RDP
Research & Development Partners

EcoSGE

User Guide

Installation and configuration guide

Резиденты
ИТ кластера
«Сколково»

EcoSGE. User Guide
Installation and configuration guide

Tel: +7 (495) 204-9-204
http://rdp.ru/

Index

Introduction

This manual covers the installation procedure and initial configuration of universal service platform EcoSGE. This equipment is a multifunctional software and hardware complex. There are several names of this equipment, depending on the active functionality: EcoNAT, EcoFILTER, EcoBRAS, Eco3in1 (obsolete name EcoNATDPI). This document describes the maximum functionality of this equipment.

This manual is valid for firmware version 3.1. Some of the commands and parameter values may vary for later or earlier versions of the firmware. For information about the current version of the firmware and documentation, visit the manufacturer's website http://rdp.ru/ or contact 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 EcoSGE 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)	Use **end** command.
Bold Italics	Recommended values of the input parameters	Use the terminal type: ***vt100***.
`Courier New font`	Examples of code. Examples of the console output	`Factory settings of the serial console:` `baud rate = 115200`
Italics	Notes	*It is recommended to disable the automatic update of the list at first ...*

`Frame, blue background color`	Examples of the console output	Time synchronization via NTP is also available and is configured via the following configuration section:`system`
		`{ ntp { disable`
		`primary_server "131.131.249.19"`

Grey background color	Examples of the code	Which then generates the request file kind:
		`<?xml version="1.0" encoding="windows-1251"?>`
		`<request>`

The 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]
Examples		
Font `Courier New`	The console output	`Welcome to EcoNAT console`
Bold font	Input values of parameters and commands	`EcoNAT:1:> configure`
Bold Italics	Custom settings	`1:# no use myacl mypool`

A list of terms and abbreviations

Abbreviation	Transcription
ACL	Access Control List
ALG	Application Layer Gateway
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BRAS	Broadband Remote Access Server
CGNAT	Carrier-grade NAT
CLI	Command Line Interface
CR	Carriage return
DDM	Digital Diagnostics Monitoring
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPI	Deep Packet Inspection
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPTV	Internet Protocol Television
LF	Line Feed
LLDP	Link Layer Discovery Protocol
NAPT	Network Address Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OSPF	Open Shortest Path First
PPTP	Point-to-Point Tunneling Protocol
RST	Reset the connection
SFP	Small Form-factor Pluggable
SFP+	Small Form-factor Pluggable Plus
SNI	Server Name Indication
SNMP	Simple Network Management Protocol
SSH	Secure Shell

Abbreviation	Transcription
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
ToS	Type of Service
TTL	Time to Live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
WAN	Wide Area Network
TIN	Taxpayer Identification Number (INN for Russia)
PSRN	Primary State Registration Number (OGRN for Russia)

1 Hardware

CAUTION: To avoid damage to the hardware platform it is not recommended to install 1GB SFP modules in slots that are designed for 10GB SFP+.

In 4000th hardware series the 10GbE network interfaces for traffic are marked TE1-TE12 (TE8 / TE16 – depending on the model). The logging port has 1GbE speed and is marked LOG (see figure below).

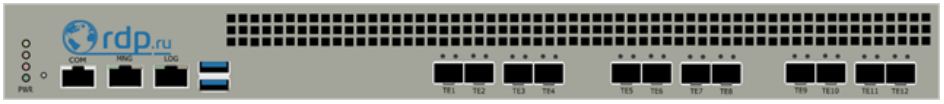

Figure 1

In 2000th hardware series the 10GbE network interfaces for the traffic are located in the right side of the front panel (see figure below).

EcoNAT 2020

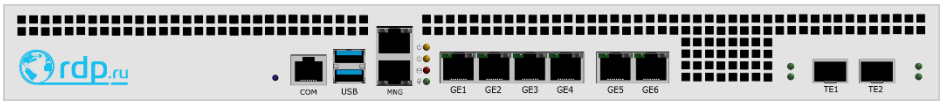

Figure 2

Fiber network interfaces marked TE1, TE2, in CLI are named **te7**, **te8**.

EcoNAT 2040

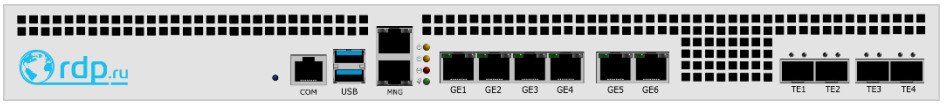

Figure 3

Fiber network interfaces marked TE1-TE4, in CLI are named **te7-te10**.

You can also use the Copper 1GbE network interfaces marked GE1-GE6. In CLI they are named as **ge1 - ge6**. On 2020 devices in a black case (the old model), the network interfaces for logging have a speed of 1GbE and are marked 5 and 6.

On 2020, 2040 devices in a blue case all 6 network interface are used for traffic, and the network interface for logging has a speed of 1GbE and is located above the MNG interface. It's name in CLI is **ge0**.

Hardware is managed using the CLI of the terminal console.

2 Log on

There are two options to log on to the terminal console of EcoNAT: via serial port or over the network via SSH protocol.

2.1 Logon via serial port

The serial port connector is located on the left side of the front panel and is marked "Console" or "COM" (Figure 3). Connect the cable to the "COM" connector. RJ-45 to DB-9 adapter for EcoNAT serial port is supplied with the device.

Figure 4

The factory default settings for the serial console (can be changed later):

- baud rate: 115200;
- data bits: 8;
- stop bits: 1;
- parity bits: none;
- flow control: none.

Terminal Settings: use ***vt100*** terminal type.

The serial console is protected by a local password (stored on the device itself). Logging on with the serial console does not logged through TACACS +.

The serial console cannot be disabled – it will always be available.

The login is ***admin*** and the password ***econat*** by default.

2.2 Logon via SSH

The EcoNAT console is accessible via SSH with the network management interface, which is located on the left side of the front panel of the unit in the lower row and is marked with the inscription "LOG / MGMT" or "MNG".

Management interface factory settings:

- IP-address and mask (ip address/mask): 192.168.100.200/255.255.255.0;
- gateway: 192.168.100.1;
- DNS servers: 8.8.8.8;
- allowed IP: any.

Network console factory settings: use the username ***admin*** and the password ***econat***, should use standard port 22.

EcoNAT supports sending commands to the SSH connection string. Example: ssh admin @ <IP-address> show counters all or ssh admin @ <IP-address> "uptime; who; show interface te10". When sending multiple commands, you must enclose them in quotation marks ". A semicolon with spaces on both sides of the character is used as a separator between the enumerated commands.

3 Operation modes of console

Immediately upon the entering you will find yourself in the operating mode (command prompt ends with the symbol '>'), where you can view the settings, but you cannot change the configuration.

To enter the configuration mode, you have to execute the **configure** command. After that, the current (active) configuration will be loaded for editing; the command prompt symbol will change to a '#'.

```
Welcome to EcoNAT console
Enter username: econat
Enter terminal type: vt100
Your privilege is 3
Applied configuration used...done
Hint: use '?' for common help available
EcoNAT:1:> configure
EcoNAT:2:#
```

To exit the configuration mode, use the **end** or **exit** (if you are in the root of the configuration). If you are editing a configuration that is differ from the currently active one, you will be asked to apply the configuration with **[a]**, save it under a certain name with **[s]**, or lose the edited configuration with **[d]**. When you are saving the configuration, you will be asked to enter a name of the configuration.

Braking the session or closing the connection automatically causes the loss of all the changes of the editable configuration that wasn't saved.

```
EcoNAT:4:# end
Current configuration is not applied. Apply, Save or Discard [a/d/s]? s
Enter profile name to save into: ecoprofile1
Save profile ok
EcoNAT:5:>
```

4 Hints and hotkeys

In order to simplify user operations, the EcoSGE CLI provides hints and shortcuts listed in the table below.

Table 1

Command/shortcut	Action
?	Lists all commands, config tree branches and parameters available in the current context, as well as hints for their intended purpose
<initial character(s) of a command or parameter>**?**	Lists all commands, config tree branches and parameters that start with these characters. The commands that cannot be executed at the current privilege level are highlighted in different color
<initial character(s) of a command or parameter>**[TAB]** <initial character(s) of a command or parameter>**[Ctrl+i]**	Performs auto-complete, if only a single match is found, or lists the available commands and/or parameters, if there are multiple matches
Up arrow **[↑]** or **[Ctrl+P]**	Recalls the previous command from the command history
Down arrow **[↓]** or **[Ctrl+N]**	Recalls the next command from the command history
..	Move up one level in the configuration hierarchy
/	Back to the root of the configuration tree
helpme or **%**	Shows the description of parameters and config tree branches available at the current level
!	Lists the parameters and config tree branches available at the current level
[Home] or **[Ctrl+A]**	Moves the cursor to the start of a line
[End] or **[Ctrl+E]**	Moves the cursor to the end of the line
[Ctrl]+[→]	Moves the cursor forward one word at a time
[Ctrl]+[←]	Moves the cursor back one word at a time
[Ctrl+U]	Deletes all text from the cursor to the beginning of the line
[Ctrl+K]	Deletes all text from the cursor to the end of the line
[Ctrl+W]	Deletes the word to the left of the cursor
[Ctrl+C]	Discard the current entry and move to a new line
[Ctrl+J]	Line feed without carriage return
[Ctrl+M]	Equivalent to pressing **[Enter]**
[Ctrl+B]	Equivalent to pressing **[←]**
[Ctrl+F]	Equivalent to pressing **[→]**
[Ctrl+H]	Equivalent to pressing **[Backspace]**
[Ctrl+L]	Clear the screen
[Ctrl+Q]	Exit the EcoSGE console session. Equivalent to the **quit** command

5 Configurations

5.1 Configuration tree

EcoNAT uses the configuration tree to store the settings. The tree structure is shown at the figure below.

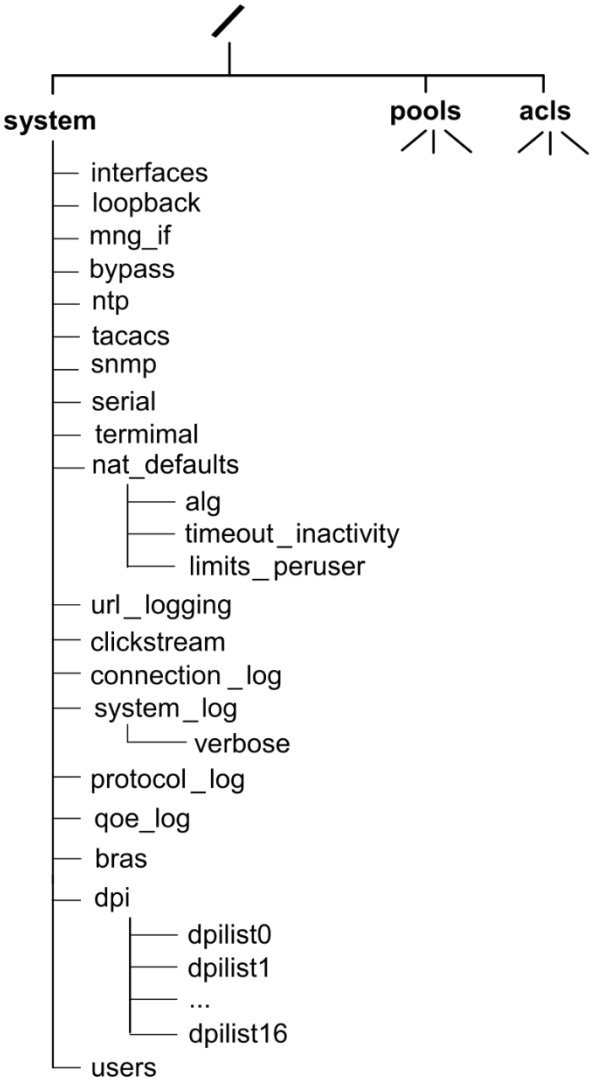

Figure 5

NOTE: The actual device may contain additional branches in the tree that are associated with additional functionality and are not shown in this tree. The description of the configuration tree branches is considered in the following table.

Table 2

Name of branch	Description
system	System settings container
interfaces	Enable/disable of network interfaces
loopback	IP- and MAC-addresses that are used to generate errors
mng_if	Network management interface settings
bypass	Settings of interfaces connected to EcoBypass
ntp	NTP settings

Name of branch	Description
tacacs	TACACS settings
snmp	SNMP settings
serial	Serial port settings
terminal	Terminal settings
nat_defaults	NAT settings by default (general settings for all pools, including the parameters used when creating new pools)
url_logging	Logging settings. URL-logging
clickstream	Collection settings for passing GET requests
connection_log	Allocation of addresses logging settings
system_log	System logging settings
bras	BRAS settings
dpi	URL filtering settings (DPI)
users	User information
pools	Contains the pools created by the user
acls	Contains the ACL (Access Control List), created by the user

Changing the configuration is only possible in the configuration mode (see paragraph Log on).

The actual change of the system settings only occurs after successful completion **apply** command, finalizing the editing of the configuration by administrator. **Apply** command can only be executed in the configuration mode. Directly when you are exiting the configuration mode you will also be prompted to apply the changes.

Upon successful completion of the **apply** command the console displays a confirmation of configuration changes applied.

```
EcoNAT:37:# apply
FIRST TIME CONFIGURATION APPLY
RECONFIG FUNCTION PROCESSING
EconatEngineReconfig output success
APPLY SUCCESS
Save applied configuration into profile 'lastapply'
EcoNAT:38:#
```

Navigating through the configuration tree is possible both in operational and in configuration mode. After logon, you are placed in the root of the configuration tree by default. At the command prompt is displayed in which branch of the tree you're currently on when you are navigating the tree. The path is displayed in the front of the invitation symbol, the names of branches are displayed hierarchically, starting from the parent and separated by '**.**'.

You may use at any time the **root** command or the symbol '/' to return to the root of the configuration tree.

You may use the commands **exit** or **up**, or characters '**..**' to switch the current level of the configuration tree.

EXAMPLE:

```
EcoNAT:1:# system
EcoNAT:2:system# mng_if
EcoNAT:3:system.mng_if# exit
EcoNAT:4:system# serial
EcoNAT:5:system.serial# root
EcoNAT:6:#
```

The example of route through the configuration tree is shown at the figure below.

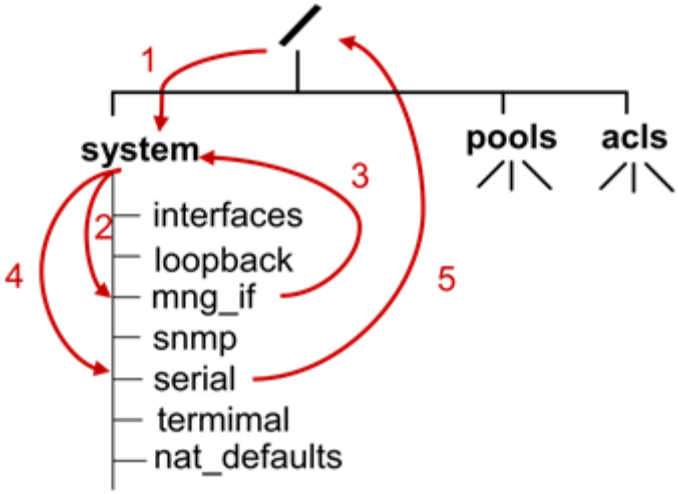

Figure 6

To go directly to a specific sub-directory of the configuration (tree branch), you have to specify the path using a **space** as a separator.

For quick navigation through the first level subdirectories of **system** directory, you may use the command **goto <*branch name*>**. For example, **goto serial** command sets the configuration directory in the system serial.

Similarly, for quick access to the branch NAT **pools**, use the command **goto <*pool name*>** (for details of the pools naming rules, see paragraph "Pools and ACL"). Also, for quick access to the one of the ACL's branches, use the command **goto <*ACL name* >** command (for more information about ACL naming rules, see paragraph "Pools and ACL").

EXAMPLE:

```
EcoNAT:1:# goto acla
EcoNAT:2:acls.acla# show
acla {
10 permit ip src host 10.0.0.1 dst any
}
EcoNAT:3:acls.acla#
```

Use the **ls** or **show** command to view the configuration, from the current level and deeper.

To view the branches that are available on the current level of the configuration tree, use the short command '**!**'.

```
EcoNAT:1:system.dpi> !
enable
functionality_mode normal_nat
certificate_file "cert.pem"
redirect_interval 600
redirect_interval_url 2592000
dpilist0  {}  # inload namespace (not show)
dpilist1  {}  # inload namespace (not show)
dpilist2  {}  # inload namespace (not show)
dpilist3  {}  # inload namespace (not show)
dpilist4  {}  # inload namespace (not show)
dpilist5  {}  # inload namespace (not show)
```

```
dpilist6  {}  # inload namespace (not show)
dpilist7  {}  # inload namespace (not show)
dpilist8  {}  # inload namespace (not show)
dpilist9  {}  # inload namespace (not show)
dpilist10  {}  # inload namespace (not show)
dpilist11  {}  # inload namespace (not show)
dpilist12  {}  # inload namespace (not show)
dpilist13  {}  # inload namespace (not show)
dpilist14  {}  # inload namespace (not show)
dpilist15  {}  # inload namespace (not show)
dpilist16  {}  # inload namespace (not show)
```

Commands for view and managing of the configuration are described in the section "Configurations".

The predefined configuration names:

- **startup** – configuration is automatically used after a reboot;
- **effective** – the current configuration (last applied on the device). To load in the current console use command **load effective**,
- **lastapply** – last applied configuration on the device,
- **factory** – the factory configuration (cannot be changed).

5.2 Viewing configuration

To view the list of saved configurations use command **dir**.

```
MyEcoNAT:1:# dir
config1
config2
lastapply
startup
MyEcoNAT:2:acls.acla# show config file config1
# config1.econat.profile – Econat Profile Script
# saved 09-Feb-2016 12^47^43 UTC, on host MyEcoNAT by user 'admin'
root
droppools
dropacls
…
```

To view the one of saved configurations, use command **show config file <configuration name>**.

To view the current configuration that had been previously applied, use the command **show config effective** in any mode.

To view the current configuration that would applied after restart, use the command **show config startup** in any mode.

5.3 Saving and applying configuration

When one make changes to the configuration, only the local configuration that is associated with the current console instance is changed. Thus, at the end of the session, all configuration changes will be lost if they have not been applied or saved.

To save the current edition of the configuration to a local file, use the **save <configuration name>** command.

It is also possible to save configuration data to a file on TFTP or FTP server. The command syntax is as follows:

save tftp://<IP address>:<port>/<filename>

save ftp://<IP address>:<port>/<filename>

The **save** command is not applicable to **factory** and **effective** configurations.

The **apply** command is used to apply configuration changes.

When attempting to apply changes in any configuration branch which is set to "**disable**" or in its descendant branches, the following message is displayed: «**NO NEED FOR APPLY: CONFIGURATION IS THE SAME**», which means that there are no changes that could be applied. The exceptions are **verbose** and **shortlist** branches.

The **verbose** branch is used to set logging verbosity for a particular subsystem (see section Logging). These logs are duplicated locally. Any changes made in this branch can be applied even if its ancestor branch **system_log** is set to "**disable**".

The **shortlist** branch contains **server_ip_and_port** parameter, which stores the address of the log server for URL filtering subsystem (see section Shortlist configuration). Changes of this parameter can be applied even if the **shortlist** branch is set to "**disable**" (provided that its ancestor branch **dpi** is enabled).

5.4 Loading configuration

To load a configuration from a local file, use the command **load <configuration filename>**.

ATTENTION! While editing the configuration, the other user may apply other settings from another terminal. To load the currently active configuration to edit, enter the command **load effective** in configuration mode.

It is also possible to load configuration data from a file stored on an FTP, TFTP or HTTP server. The command syntax is as follows:

load tftp://<IP address>:<port>/<filename>

load ftp://<IP address>:<port>/<filename>

load http://<IP address>:<port>/<filename>

5.5 Copying configuration

The command for copying configuration data from one file to another has the following syntax:

copy <source> <destination>

Below are examples of command syntax for all possible cases of configuration copying:

- from one local file to another local file:

copy <source filename> <destination filename>

```
MyEcoNAT:1:# dir
config1
config2
lastapply
startup
MyEcoNAT:2:# copy config2 config3
MyEcoNAT:3:# dir
config1
config2
config3
lastapply
startup
```

from local file to TFTP, FTP or HTTP server:

copy <local filename> tftp://<IP address>:<port>/<destination filename>

copy <local filename> ftp://<IP address>:<port>/<destination filename>

copy <local filename> http://<IP address>:<port>/<destination filename>

from TFTP, FTP or HTTP server to local file:

copy tftp://<IP address>:<port>/<source filename> <local filename>

copy ftp://<IP address>:<port>/<source filename> <local filename>

copy http://<IP address>:<port>/<source filename> <local filename>

The **copy** command is not applicable to **factory** and **effective** configurations.

5.6 Delete configuration

To remove the configuration, you have to call the command: **erase <configuration name>**. **Erase** command does not apply to **factory** and **effective** configurations.

```
MyEcoNAT:1:# dir
config1
config2
config3
config4
lastapply
startup
MyEcoNAT:2:# erase config4
MyEcoNAT:3:# dir
config1
config2
config3
lastapply
startup
```

Also there is **clear config** command. By this command one can clean (set to zero) edited configuration without deleting it. So all pools and ACLs will be deleted, all interfaces configurations will be set to zero, all users will be deleted and so on.

*Edited configuration will be applied only after **apply** command .*

5.7 Save startup configuration

To set the current effective configuration as starting use the command **write**. To set the current editable configuration as starting use command **save startup** in the configuration mode, however, it is not recommended.

> **IMPORTANT: after you run the command write, when you restart the system will be loaded the active configuration at the time of starting the write command, or configuration saved with the command save startup if it was done later. This is the configuration for which last apply was implemented, even if it was not done in the current terminal console and by another user!**

To avoid conflicts it is recommended that only the one person have the ability to edit the configuration of EcoNAT. Also it is recommended to exit the configuration mode immediately after changing the configuration so that automatically log into the latest version of the configuration at the next startup.

6 Quick system start

The system settings and management commands are described in this section.

6.1 Management interface setup

To manage the EcoNAT through the network, you must configure the parameters of the management network interface.

Suppose that we want to assign an IP 192.168.100.12/24 to the management interface, default gateway 192.168.100.1, DNS server addresses: 10.0.8.1, 10.0.8.3 and allow the access only to those who are in the network 192.168.100.12, as well as a host 10.0.22.33.

```
EcoNAT:1:# configure
EcoNAT:2:# system mng_if
EcoNAT:3:system.mng_if# ip_address 192.168.100.12/255.255.255.0
EcoNAT:3:system.mng_if# gateway 192.168.100.1
EcoNAT:4:system.mng_if# name_servers ( 10.0.8.1 10.0.8.3 )
EcoNAT:5:system.mng_if# allowed_ip ( 192.168.10.12/24 10.0.22.33 )
```

To allow the access to the management interface from any computer, you can assign **allowed_ip** a value ***0.0.0.0/0***.

If you execute **safe apply** after the changes of the network interface settings, the changes specifically of the network interface settings will be applied for a few minutes (in other cases, the changes are applied immediately after the **apply** command). This is due to the fact that the erroneous configuration of the network interface cause to inability to configure EcoNAT through the network.

During these two minutes, it makes sense to test the connection by opening another terminal, and if the connection is successful, then you can use the **commit** command to consolidate the changes.

To view information about the control settings interface, you can use the **show ipif** command.

```
EcoNAT:6:# show ipif
MAC 00:0d:48:28:1a:6e
IP: 192.168.100.12
GW: 192.168.100.1
Mask: 255.255.255.0
```

Standard commands **ping** and **traceroute** may be run with the management interface.

```
EcoNAT:7:# ping 1.2.1.5
PING 1.2.1.5 (1.2.1.5): 56 data bytes
64 bytes from 1.2.1.5: seq=0 ttl=64 time=0.632 ms
64 bytes from 1.2.1.5: seq=1 ttl=64 time=0.340 ms
64 bytes from 1.2.1.5: seq=2 ttl=64 time=0.332 ms
64 bytes from 1.2.1.5: seq=3 ttl=64 time=0.331 ms
--- 1.2.1.5 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.331/0.408/0.632 ms
EcoNAT:8:# traceroute 4.1.1.1
traceroute to 4.1.1.1 (4.1.1.1), 30 hops max, 46 byte packets
1  10.210.1.1 (10.210.1.1)  0.735 ms  0.382 ms  0.398 ms
2  1.1.5.2 (1.1.5.2)  1.027 ms  1.079 ms  0.725 ms
3  4.1.1.2 (4.1.1.2)  0.445 ms  0.535 ms  0.483 ms
```

To terminate **ping** or **traceroute** command, press **[Ctrl+C]** or **[Backspace]**.

The address of the management interface can be specified statically (see example above) or dynamically. To enable autodetection of a dynamically issued address (DHCP), you need to set the value of the **ip_address** parameter in the format **0.0.0.0/***, where * is any subnet.

6.2 Configuring the EcoBypass connection

The EcoNAT device can be connected to the network via the active optical bypass of the EcoBypass series. Interaction with EcoBypass is carried out by sending heartbeat messages by UDP. In the event that heartbeat messages cease to arrive, EcoBypass switches to transparent mode. After that traffic is bypassed by EcoNAT until communication with it is resumed.

For the correct operation of this scheme, the IP connection between the EcoNAT **MNG** interface and the EcoBypass **ETH** interface must be configured. In turn, pairs of EcoNAT interfaces are connected to the paired optical ports EcoBypass.

The connection scheme for a pair of **TE1, TE2** network interfaces via EcoBypass is shown in the figure below.

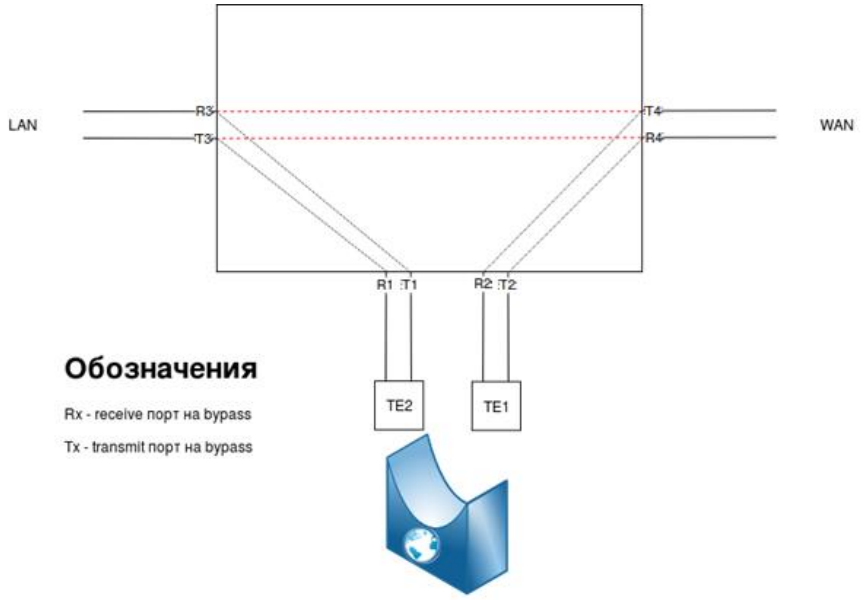

Figure 7

Hearbeat messages have the form **<BP01_XX_BP>**, where **XX** is the number of the EcoBypass network card to which the EcoNAT device is connected. In response, EcoBypass sends messages like **<BP01_XX_BP_OK>**.

Heartbeat messages are always sent, unless one of the pair interfaces has been administratively turned off, or the device has malfunctioned.

In addition to the total absence of heartbeat messages, EcoBypass can monitor the drop in the Tx signal level from the device. At a critical drop in the level, EcoBypass switches to transparent mode.

EcoBypass is configured in the **system bypass** branch of the configuration tree.

The parameters configured in this branch are shown in the table below.

Table 3

Parameter	Description
enable/disable	Enable/disable sending heartbeat messages to EcoBypass
bypass_ip	IP address of EcoBypass. For proper operation, the IP connection between the EcoNAT **MNG** interface and the EcoBypass **ETH** interface must be configured
bypass_tos	The value of the Type of Service (ToS) field for sent messages. Possible values are from 0 to 255 (0 by default)
bypass_interval	Interval for sending heartbeat messages to EcoBypass. Set in milliseconds. Possible values are from 1 to 2000 (10 by default)
teN1_teN2	Setting for a pair of interfaces. Possible values are: **disabled** - EcoBypass is not connected; number of the network card (slot) EcoBypass, to which the pair is connected. In the case of the 1U EcoBypass model, the numbering of the slots will be from 1 to 8. In the case of the 4U EcoBypass model, the slots will be numbered from 01 to 32

Setting example:

```
EcoNAT:2:system.bypass> ls
enable
bypass_ip 10.210.1.199
bypass_tos 0
bypass_interval 10
te1_te2 disabled
te3_te4 disabled
te5_te6 1
te7_te8 2
te9_te10 3
te11_te12 4
te13_te14 disabled
te15_te16 disabled
EcoNAT:3:system.bypass>
```

6.3 Terminal settings

It is recommended for initial setup of the EcoNAT to set the system prompt and the time of automatic logout on idle (for closing the session if it is inactive for the specified time). The time of automatic logout is specified in seconds.

```
EcoNAT:1:# root
EcoNAT:2:# system terminal
EcoNAT:3:system.terminal# type vt100
EcoNAT:4:system.terminal# autologoff_timeout never
EcoNAT:5:system.terminal# max_consoles 20
EcoNAT:6:system.terminal# prompt “MyEcoNAT”
EcoNAT:7:system.terminal# apply
…
APPLY SUCCESS
Save applied configuration into profile ‘lastapply’
MyEcoNAT:9:system.terminal#
```

Edited parametrs **max_consoles** and **prompt** will be applied only after reboot.

After a system boot the prompt parameter is taken from the **system terminal prompt**, that is in the launch configuration. This invitation can be changed in the relevant branch of the configuration

tree and then applying the changes with **apply** command. When you make changes via the **system terminal prompt** parameter, they will be displayed at the next system boot.

It is possible to enable / disable the counter of strings and commands using the **print_line_num** command.

print_line_num off – disable.

print_line_num on – enable (default settings).

EcoNAT:1# system terminal

EcoNAT:2:system.terminal# print_line_num off

EcoNAT:3:system.terminal# apply

…

APPLY SUCCESS

Save applied configuration into profile ‘lastapply’

EcoNAT:system.terminal# ..

EcoNAT# terminal

EcoNAT:system.terminal# print_line_num on

EcoNAT:system.terminal# apply

…

APPLY SUCCESS

Save applied configuration into profile ‘lastapply’

EcoNAT:7:system.terminal#

6.4 Loopback settings

The settings stored in the The settings stored in the loopback configuration tree branch are used by EcoNAT to send ICMP messages to subscribers. configuration tree branch are used by EcoNAT to send ICMP messages to subscribers.. In the current version of the software these messages are generated by EcoNAT only in one case – if the user for some reason cannot allocate another port on the global address. EcoNAT sends ICMP error type = 3, code = 13 (Destination unreachable (Communication administratively filtered)).

The **loopback** settings are available in the **system loopback** branch of the configuration. For loopback, it is possible to specify the displayed IP address and MAC. If the IP address for the **loopback** is not set, then it will be 100.64.97.116 by default.

```
EcoNAT:1:system.loopback# show
ip 0.0.0.0
mac 00:00:00:00:00:00
EcoNAT:2:system.loopback# ip 1.1.1.1
EcoNAT:3:system.loopback# show
ip 1.1.1.1
mac 00:00:00:00:00:00
EcoNAT:3:system.loopback#
```

6.5 Time settings

Setting the system time is very important for the proper functioning of EcoNAT, because the timestamps in the logged messages are based on this time.

EcoNAT is using only UTC (Universal Time Coordinated) time zones.

Time can be viewed using the **show time** command. You can also set the time manually via the **edit datetime** command (the date and time must be entered in UTC).

```
MyEcoNAT:1:# show time
```

Current time is 12-Jul-2019T13:20:52 (UTC)

Current time is 12-Jul-2019T13:50:52 (Local)

```
MyEcoNAT:2:# edit datetime 17-Jun-2014T09:00:00
```

Time synchronization via NTP may de configured in the following configuration branch:

```
system
{
ntp
{
disable
primary_server "131.131.249.19"
secondary_server "185.21.78.23"
tertiary_server "183.143.51.50"
interval 600
}
}
```

To enable NTP time synchronization, you have to go to the ***system ntp*** branch and execute the ***enable*** command.

```
MyEcoNAT:1:# root
MyEcoNAT:2:# system ntp
MyEcoNAT:3:system.ntp# enable
```

Synchronization status with NTP server can be seen with the command **show ntp**.

```
MyEcoNAT:1:# show ntp
SERVER |offset |delay |status |strat |refid |rootdelay |reach |
-------------------------------------------------------------------------
-------------------------
83.143.51.50 |+0.025177 |0.069693 |0x24 |1 |0x00535050|0.000000 |0x7f |
85.21.78.23 |+0.053309 |0.012691 |0x24 |2 |0x169024c0|0.019104 |0xff |
```

System logs and connections logs can display the local time. Use the parameter **system system_log timeskew** to set the local time. This parameter contains the offset of the local time zone relative to UTC in minutes. For example, to configure the time zone of Moscow (UTC + 3), you must set the value ***180*** (3x60) minutes.

```
MyEcoNAT:1:# root
MyEcoNAT:2:# system system_log timeskew 180
```

6.6 Logging

6.6.1 *Subscriber's connection log settings*

It is required by the legislation of some countries that all the information about the allocation of IP-addresses and/or port or block of ports must be saved. For maintaining this feature EcoNAT uses the syslog protocol as standard mechanism of logging.

In the branch **system connection_log** you can set the settings for the connection log. To start logging you should set the parameter ***enable***.

In the case of using the platform with multiple network interfaces allocated for connection log, these interfaces are combined in a static virtual channel through which one are sent log packets. For the platforms with a single log interface virtual static channel is set on a single interface. In both cases for virtual channel will be assigned a synthetic IP-address of the source, so when you try to run ping command on this address, ICMP requests will remain unanswered (except of logging throught the **mng** interface case). Log packets will be sent by all connected network logging interfaces using Round-Robin algorithm.

The names of the network interfaces for logging are specified in section Hardware.

Connection_log basic parameters are described in a table below.

Table 4

Parameter	Description
enable or disable	Enable or disable connection logging
log_servers	Syslog servers addresses and ports for which logging will be carried out (logging would proceed in parallel on all available servers from the list, that is, each server will obtain information about all connections). Currently, the maximum number of servers is limited to two
log_interface	The interface through which logging will be carried out. Possible values: **default** - through the logging interface, **mng** - via **mng** interface
ip_address	Source IP-address and subnet mask (use '/') of the virtual channel in which logging network interfaces are merged
mac	Source MAC-address of the virtual channel in which logging network interfaces are merged (if not specified, the MAC-address one of a network interfaces will be set)
gateway	Default gateway for the virtual channel in which logging network interfaces are merged. Required if not all syslog server specified in **log_servers** parameter are on the subnet specified in the parameter **ip_address**
strip_tags	In the mirroring mode, EcoNAT sends a connection interrupt packet (for HTTPS) or a redirection packet (for HTTP) to the subscriber via the network interface. When receiving tagged traffic and when the parameter is on, the tag (or double-tag) is cut off. When the parameter is off, the redirect or interrupt packet is sent to the logging network interface with the same parameters of the processed traffic
that_mac	Syslog server MAC address in the **log_servers** section for the nearest L3 neighbour. The parameter is optional. If the option is not set, the MAC-address is calculated by the ARP protocol. must contain the MAC-address of the first syslog server (in the case when the first syslog server is on the same subnet) or MAC-address of the default gateway (if the first syslog server on a different subnet). *Using this option reduces the chance of data loss at the start of logging provided a large load. EcoNAT able to process and log the more than 5 million connections per second at*

Parameter	Description
	a full load. If a syslog server will respond to the ARP request, for example in 10 ms, in the queue may accumulate 50,000 connections waiting to be sent
timeskew	Shift of the time indicated in the logs relative to Greenwich. Set in minutes. For example, for Moscow, the parameter value must be 180
pack_msgs	Enables packaging several reports in one message. This reduces the size of the logs and the network load

Logging modes. Syslog logging

Ports for address translation for subscribers in CGNAT mode are allocated in blocks of 128 ports at a time. The next block is issued only when the exhaustion ports occurs in the previous block. Due to the block allocation, you may reduce volume of logs, as with the proper settings, instead of the number of reports on the allocation of ports to subscribers, will only one allocating the range of 128 ports (block) message.

EcoNAT supports multiple formats logging. The following describes the appropriate settings **connection_log** when logging in the syslog format.

Table 5

Parameter	Description
log_format	Parameter indicates the type of logging: **syslog** – syslog logging, **netflow** – connections logging with NetFlow v9 protocol
log_on_release	The parameter indicates whether or not to send a message to connection_log if translation or block is released. The message is always sent when translation or block is created. If **log_individual_conn** enabled, a message is generated when occurs the release of each translation, otherwise – in case of releasing the block
log_individual_conn	Parameter specifies whether to log individual connections, or you may log blocks of ports only
use_hex_format	Allows to use hexadecimal format for the output log, which reduces the size of the log, while preserving the informational component. If disabled, the fixed decimal format is used, for example:010.210.000.012:00080
pack_msgs	Enables packaging several reports in one syslog message. This reduces the size of the logs and the network load
facility	For the generated syslog messages sets a category of entity that generates the message for further processing and filtering. Possible values are from 16 to 23. These values relevant to the codes in the RFC 5424, indicating the subjects of local origin (local use 0 (local0) local use 7 (local7)). The default value – 16
severity	For the generated syslog messages sets severity for the convenience of further processing and filtering. Possible values are from 0 to 7, recommended – from 5 to 7. These values relevant to the codes in the RFC 5424, indicating the importance levels of messages: **5** – Notice, messages about general but significant events; **6** – Informational message; **7** – Debug message. Default value – 6

The main modes of connection logging and recommended settings are presented in the table below .

Table 6

The ratio of size/ readability of logs	log_on_release	log_individual_conn	use_hex_format	pack_msgs
The minimum log size (Ports blocks)	No	No	**Yes**	**Yes**
The small size of the log,	No	No	No	No

The ratio of size/ readability of logs	log_on_release	log_individual_conn	use_hex_format	pack_msgs
but it is more readable				
The small size of the log (connections)	No	**Yes**	**Yes**	**Yes**
More readable logs (connections)	**Yes**	**Yes**	No	**Yes**
Debug mode (most readable logs, but the large size)	**Yes**	**Yes**	No	No

If you want to log WHO VISITED FROM SUCH ADDRESS AND PORT:

- If the providers logging storage system is well established (that is, everything is logged and stored without losses), then it is recommended to set for the four above parameters, the value ***No***.
- If there are losses in the providers logging system, it makes sense to enable the **log_on_release**. Then, in case of loss of the opening of the connection message will be additionally sent the message about the closure, which will reduce the probability of loss of message.

If you want to log WHO VISITED TO SUCH ADDRESS AND PORT:
You need to enable **log_individual_conn** mode. In this case, the log will reflect the REMOTE_IP and REMOTE_PORT – host and the port which communicates with your subscriber.

To enable logging, do not forget to set the **connection_log** option in ***enable***.

CONFIGURATION EXAMPLE:

```
MyEcoNAT:1:# root
MyEcoNAT:2:# system connection_log
MyEcoNAT:3:system.connection_log# log_servers ( 10.0.22.78:514 )
MyEcoNAT:4:system.connection_log# ip_address 10.0.22.33/255.255.255.0
MyEcoNAT:5:system.connection_log# log_on_release on
MyEcoNAT:6:system.connection_log# log_individual_conn on
MyEcoNAT:7:system.connection_log# pack_msgs off
MyEcoNAT:8:system.connection_log# enable
```

The syslog logging format: **<Syslog server date time > < EcoNAT IP address> <EcoNAT date time> <EcoNAT name> |<Destination IP address (DST)>:<Port> < IP address to which the translation is done >:<Port> <Source IP address (SRC)> <Protocol identifier>**.

Example:

```
Mar  3 14:36:58 10.210.1.234  2016-03-03T11:39:55+00:03
eco101     |  192.168.008.008:01024 A 060.000.000.226:01024 E
010.000.003.254:01024  UDP
```

IP addresses are recorded in the three-digit format, for example, the address of 10.1.1.200 will be presented as 010.001.001.200.Below are a few examples of the log format settings. For convenience, some of the lines before the vertical bar is not shown.

Port blocks logging by packaging multiple network event messages to one syslog message. In this case, the log includes the NAT translation address, with used block of ports and IP address of the source.

Settings:

log_on_release off

log individual off use_

hex_format off

pack_msgs on

```
| 060.000.000.020:01024-01278 EA 010.000.003.250 UDP
060.000.000.018:01024-01278 EA 010.000.001.251 UDP
060.000.000.017:01024-01278 EA 010.000.002.251 UDP
060.000.000.015:01024-01278 EA 010.000.000.252 UDP
060.000.000.012:01024-01278 EA 010.000.003.252 UDP
060.000.000.010:01024-01278 EA 010.000.001.253 UDP
060.000.000.009:01024-01278 EA 010.000.002.253 UDP
060.000.000.007:01024-01278 EA 010.000.000.254 UDP
060.000.000.004:01024-01278 EA 010.000.003.254 UDP
060.000.000.002:01024-01278 EA 010.000.001.255 UDP
060.000.000.001:01024-01278 EA 010.000.002.255 UDP
```

Logging of each connection with the packaging of multiple network event messages to one syslog message. In this case, the log includes three addresses (destination, translation, source) specifying the port. Several events are packed into a single message.

Settings:

log_on_release off

log individual on

use_hex_format off

pack_msgs on

```
| 192.168.008.008:01024 A 060.000.000.006:01024 E 010.000.001.254:01024
UDP 192.168.008.008:01024 A 060.000.000.005:01024 E
010.000.002.254:01024 UDP 192.168.008.008:01024 A 060.000.000.003:01024
E 010.000.000.255:01024 UDP 192.168.008.008:01024 A
060.000.000.000:01024 E 010.000.003.255:01024 UDP
| 192.168.008.008:01024 A 060.000.000.010:01024 E 010.000.001.253:01024
UDP 192.168.008.008:01024 A 060.000.000.009:01024 E
010.000.002.253:01024 UDP 192.168.008.008:01024 A 060.000.000.007:01024
E 010.000.000.254:01024 UDP 192.168.008.008:01024 A
060.000.000.004:01024 E 010.000.003.254:01024 UDP 192.168.008.008:01024
A 060.000.000.002:01024 E 010.000.001.255:01024 UDP
192.168.008.008:01024 A 060.000.000.001:01024 E 010.000.002.255:01024
UDP
```

Logging of each connection without packaging. In this case, the log includes all three addresses (destination, translation, source) specifying the port. For each event a new message is created.

Settings:

log_on_release off

log individual on

use_hex_format off

pack_msgs off

```
| 192.168.008.008:01024 A 060.000.000.226:01024 E 010.000.003.254:01024
UDP
| 192.168.008.008:01024 A 060.000.000.102:01024 E 010.000.001.255:01024
UDP
| 192.168.008.008:01024 A 060.000.001.098:01024 E 010.000.002.255:01024
UDP
| 192.168.008.008:01024 A 060.000.002.234:01024 E 010.000.001.254:01024
UDP
| 192.168.008.008:01024 A 060.000.003.238:01024 E 010.000.002.254:01024
UDP
| 192.168.008.008:01024 A 060.000.001.230:01024 E 010.000.000.255:01024
UDP
```

Logging blocks of ports without packaging. In this case, the log includes the NAT translation address, with used block of ports and IP address of the source. For each event a new message is created.

Settings:

log_on_release off

log individual off

use_hex_format off

pack_msgs off

```
| 060.000.000.179:01024-01278 EA 010.000.001.253 UDP
| 060.000.003.096:01024-01278 EA 010.000.002.253 UDP
| 060.000.000.034:01024-01278 EA 010.000.000.254 UDP
| 060.000.002.245:01024-01278 EA 010.000.003.254 UDP
| 060.000.001.249:01024-01278 EA 010.000.001.255 UDP
| 060.000.000.108:01024-01278 EA 010.000.002.255 UDP
| 060.000.001.104:01024-01278 EA 010.000.000.255 UDP
| 060.000.000.253:01024-01278 EA 010.000.003.255 UDP
```

Logging the messages about blocks of ports release and the translation release. In this case, the last message in the example notifies of the releasing of the port 1.

Settings:

log_on_release on

log_individual_conn on

use_hex_format off

pack_msgs off

```
| 207.046.113.078:05443 F 060.000.003.112:01043 E 010.000.002.015:02542
TCP
| 172.016.255.001:00001 F 060.000.003.176:00001 E 067.215.065.132:00001
ICM
| 077.001.001.254:00000 A 000.000.000.000:00000 E 077.001.001.002:00001
047
```

Logging in hexadecimal format.

Settings:

log_on_release on

log_individual_conn on

use_hex_format on

pack_msgs off

```
|  c0a800c10015 06 3c0002e80400 EA c0a800720471
|  c0a800c11c56 06 3c0002e80401 EA c0a800720474
```

NetFlow logging

EcoNAT allows you to configure connection logging with NetFlow v9 protocol. In this case is logged the connection but not the amount of transferred traffic. Additional settings of **connection_log** branch used for this are described in the table below.

Table 7

Parametr	Description
netflow_template_rate	It indicates after how many packets will be transmitted the netflow template package. Possible values: once, 128, 512, 1K, 4K, 16K, 64K
netflow_options_rate	It indicates after how many packets will be transmitted netflow options and netflow options template package. Possible values: once, 128, 512, 1K, 4K, 16K, 64K

Required to configure NetFlow logging parameter values are shown in the table below. It is recommended to strictly adhere to the specified settings.

Table 8

Parametr	Value
log_format	netflow
log_on_release	on
log_individual_conn	on
use_hex_format	off
pack_msgs	on
log_server	NetFlow server address and the right port number
ip_address gateway	Address/mask of the subnet and gateway

6.6.2 *System logging setup*

EcoNAT keeps the recordings of all user actions in the terminal console. Logs of these actions are sent to the server through the management interface.

System logging settings can be found in a **system system_log** branch. To turn logging on set the parameter to ***enable***. The server on which EcoNAT will send system logs, specified in **log_servers** parameter.

EcoNAT name that appears in the logs is set in the **hostname** parameter using the command **hostname "name"**. This name is added not only in the system log, but also in EcoNAT connection log.

```
MyEcoNAT:18:system.system_log# verbose defrag 1
MyEcoNAT:19:system.system_log# show
enable
log_servers ( )
hostname "econat"
timeskew 180
verbose
{
```

```
 all 3
 basic_nat 3
 conn_track 3
 defrag 1
 dpi 3
 fast_path 3
 gc 3
 health_check 3
 main 3
 session 3
 reconfig 3
 services 3
 sniffer 3
 snmp 3
 syslogger 3
 trans_tbl 3
 alg 3
 bras_tbl 3
}
```

The level of detail is set by **verbose** parameter, which can vary, depending on the subsystems and to be one for all subsystems (**all**).

Logging levels :

0 – FATAL – critical messages only,

1 – ERROR – errors,

2 – WARN – warnings,

3 – INFO – information.

To view the logging levels that are set in the configuration, you should use **show verboselvl** command.

```
MyEcoNAT:20:# show verboselvl
ALL = 3
BASIC_NAT = 1
CONN_TRACK = 1
DEFRAG = 1
DPI = 1
FAST_PATH = 1
GC = 1
HEALTH_CHECK = 1
MAIN = 1
RECONFIG = 1
SERVICE = 1
SNIFFER = 1
SNMP = 1
SYSLOGGER = 1
TRANS_TBL = 1
SESSION = 1
ALG = 1
BRAS_TBL = 1
```

Subsystems (**facility** parameter): basic_nat, conn_track, defrag, dpi, fast_path, gc, health_check, main, reconfig, service, sniffer, snmp, syslogger, trans_tbl, session, alg, bras_tbl.

That is, if configured parameter **verbose all** equal to ***3***, it will benefit from logging messages of all levels. If the subsystem is set to the **verbose** parameter, different from **all**, so the higher of these two values will be taken.

The values displayed by **show verboselvl** command may differ from the set in the current configuration.

In order to quickly change the logging level for some subsystem (or all subsystems), use the command **setlog <subsystem> <logging rate>**. Here logging levels are set no figures, as in the configuration change, but names. The changes take effect immediately. After the reboot, the logging levels values will be reset to the specified in the active configuration.

In the example below, the logging level for all subsystems is changed to FATAL, respectively, lower priority events (WARNING, INFO, ERROR) will not benefit from logging. In the configuration level of logging for all subsystems is INFO, and to after reboot will again log all events.

Example.

```
MyEcoNAT:21:system.system_log.verbose# setlog all fatal
MyEcoNAT:22:system.system_log.verbose# show verboselvl
ALL = 0
BASIC_NAT = 1
CONN_TRACK = 1
DEFRAG = 1
DPI = 1
FAST_PATH = 1
GC = 1
HEALTH_CHECK = 1
MAIN = 1
RECONFIG = 1
SERVICE = 1
SNIFFER = 1
SNMP = 1
SYSLOGGER = 1
TRANS_TBL = 1
SESSION = 3
ALG = 1
BRAS_TBL = 1
MyEcoNAT:23:system.system_log.verbose# ls
all 3
basic_nat 1
conn_track 1
defrag 1
dpi 1
fast_path 1
gc 1
health_check 1
main 1
session 3
reconfig 1
services 1
sniffer 1
snmp 1
```

```
syslogger 1
trans_tbl 1
alg 1
bras_tbl 1
```

Log messages are presented in the following format: **<Date, time> <Subsystem> [<Logging level>]: <Message>**.

Use **show logs** command to view the system log. By default, the command displays all the log entries. In order for the output records to the screen was by portions, is used the conveyor | **more**. In this logs viewing mode, at the touch of any key, the screen displays several messages, by pressing the key combination **[Ctrl + C]** or **[Backspace]** system exits the viewing logs.

To see a specific level messages, you need to specify the desired level in the command. This will show all messages pertaining to the specified severity level and higher. That is, if you specify ERROR, that will display messages of level ERROR and FATAL.

```
MyEcoNAT:24:> show logs info | more
Mar 09 09:27:25 MAIN [FATAL]: User admin logged with 3
Mar 09 09:27:12 DPI [INFO]: Performed checks for short list https: total
0.00/s, allowed 0.00/s, banned 0.00/s
Mar 09 09:27:12 DPI [INFO]: buffers (min-max): state 7f3eada42980-
7f3eada42980, host 0-0, path 0-0
Mar 09 09:27:12 DPI [INFO]: buffers (alloced/freed): state 1/1, host
0/0, path 0/0
Mar 09 09:27:03 GC [INFO]: abonents_table_GC_CORE_2 calls: 0, ticks: 0,
ticks/entry: -nan, processed: 0, freed 0
Press any key
```

In order to filter the messages by subsystem you should specified the desired subsystem in the command **show logs**, the command will then be as follows: **show logs facility <subsystem>**.

Example:

```
MyEcoNAT:25:> show logs facility snmp
May 11 12:32:50 SNMP [INFO]: Launched snmp agent on port 161 for
community public
```

EcoNAT records all passing protocols. Logs of the recognized protocols with indication of the VLAN id in binary form are transmitted to the server. Logging logging settings are located in the **system.protocol_log** branch. In order to enable logging, the **enable** parameter must be set in this branch. This type of logging requires a license for URL filtering functionality (see the “URL Filtering configuration” section).

```
MyEcoNAT: 19: system.protocol_log # show
disable
log_interface default
server_ip_and_port 0.0.0.0
ip_address 0.0.0.0/0.0.0.0
gateway 0.0.0.0
source_port 1089
```

Parameters of the protocol logging are given in the table below.

Table 9

Parameter	Description
enable disable	Enabling / disabling protocol logging

Parameter	Description
log_interface	The interface through which logging will be carried out. Possible values: **default** - through the logging interface, **mng** - via **mng** interface
server_ip_and_port	The syslog server IP address and port
ip_address	Source IP-address and subnet mask (use '/') of the virtual channel in which logging network interfaces are merged
gateway	The default gateway for a virtual channel, into which the logging network interfaces are merged. This setting is r equired if the syslog server specified in the **server_ip_and_port** parameter is not on the subnet specified in the **ip_address** parameter
source_port	The port used for sending syslog packets

6.6.3 *Quality of Experience*

Quality of Experience (QoE) is an integral parameter representing the general acceptability of quality or service subjectively perceived by the end user. In the context of EcoNAT, QoE is a summary of information about subscriber connections. In this summary, the indicators characterizing the quality of this connection are presented. These indicators help identify connection problems for each individual subscriber, which can be used by the operator as a tool to increase the subjective quality of the services provided and to retain subscribers.

EcoNAT QoE is divided into the following modules, which can be included both together and separately, depending on the license:

- basic functionality with binary logs;
- session accounting functionality (the number of bytes/packets transmitted is logged);
- OTT functionality, which allows analyzing the parameters for providing video services: counting bytes of the OTT sub-session, time of the last PSH packet in the sub-session from the server, delta time between the GET packet from the client and PSH from the server in the sub-session.

The QoE settings are located in the branch of the configuration tree **system.qoe_log**.

The QoE settings are described in the table below .

Table 10

Parameter	Description
enable disable	Enabling / disabling QoE Logging
log_interface	The interface through which logging will be carried out. Possible values: **default** - through the logging interface, **mng** - via **mng** interface
syn_log	Possible values: on, off If the value is "on", then the passing SYN packet (including Ethernet header) will be encapsulated into a log packet with fixed DATA field length of 256 bytes, which is then forwarded to the log collector
server_ip_and_port	<IP Address>:<Port> of Log Collector
ip_address	Source IP-address and subnet mask (use '/') of the virtual channel in which logging network interfaces are merged
gateway	The default gateway for a virtual channel, into which the logging network interfaces are merged. This setting is r equired if the syslog server specified in the **server_ip_and_port** parameter is not on the subnet specified in the **ip_address** parameter

Parameter	Description
source_port	The port used for sending syslog packets
mtu	MTU of syslog packets

Settings example:

```
2:7:system.qoe_log# ls
enable
log_interface default
syn_log on
server_ip_and_port 192.168.1.2:514
ip_address 192.168.1.1/255.255.255.0
gateway 192.168.1.1
source_port 1089
mtu 1500
```

QoE logs are transmitted in binary form using a proprietary protocol. When using equipment in conjunction with EcoQoE (Log Collector), the logs are automatically decrypted at the collector.

6.6.4 *Logging subscribers requests to web servers*

The EcoNAT system provides the capability to use a remote syslog server to log HTTP GET requests, web servers HTTP responses and SSL/TLS connection requests.

This functionality is configured in the **system clickstream** configuration branch. The table below describes the parameters available in this branch.

Table 11

Parameter	Description
enable disable	Enabling / disabling logging of requests to web servers
server_ip_and_port	The syslog server IP address and port
ip_address	Source IP-address and subnet mask (use '/') of the virtual channel in which logging network interfaces are merged
gateway	The default gateway for a virtual channel, into which the logging network interfaces are merged. This setting is r equired if the syslog server specified in the **server_ip_and_port** parameter is not on the subnet specified in the **ip_address** parameter
source_port	The port used for sending syslog packets
mtu	MTU of syslog packets

Settings example:

```
EcoNAT:43:system.clickstream# ls
enable
server_ip_and_port 192.168.2.2:514
ip_address 192.168.1.1/255.255.255.0
gateway 192.168.1.254
source_port 1088
mtu 1500
```

Below is an example of records on the syslog server. The 1st record is for HTTP GET request, the 2nd is for web server HTTP response, and the 3rd is for SSL connection request.

```
2019-07-11T10:35:58.202901+00:00 192.168.1.1 192.168.000.002:34904
192.168.000.003:00080 1522071357 econat     GET / HTTP/1.1#015#012Host:
google.ru#015#012User-Agent: curl/7.55.0#015#012Accept: */*#015#012#015
2019-07-12T09:33:02.370234+00:00 192.168.1.1 065.208.228.223:00080
145.254.160.237:03372 1562934780 econat     HTTP/1.1 200 OK
```

```
2019-07-15T14:50:01.810583+00:00 192.168.1.1 192.168.000.002:41016
192.168.000.003:00080 1532627400 econat     SSL: 3.3 hostname: vk.com
```

The table below describes the values in the fields of the record for HTTP GET request (see the 1st string in the example above).

Table 12

#	Field	Example
1	Syslog server timestamp	2018-03-26T10:35:58.202901+00:00
2	EcoNAT device IP address	192.168.1.1
3	Source IP-address:port	192.168.000.002:34904
4	Destination IP address:port	192.168.000.003:00080
5	EcoNAT device timestamp (POSIX time)	1522071357
6	Hostname specified in the **system_log** branch	econat
7	HTTP GET request content	GET / HTTP/1.1#015#012Host: google.ru#015#012User-Agent: curl/7.55.0#015#012Accept: */*#015#012#015

The description of fields 1-6 in the record for web server HTTP response (see the 2nd string in the example above) is the same as for HTTP GET request. The field 7 contains HTTP version and response status code.

The table below describes the fields 7 and 8 of the record for SSL connection request (see the 3rd string in the example above). The description of fields 1-6 is the same as for HTTP GET request.

Table 13

#	Field	Example
7	SSL version	SSL: 3.3
8	Domain name	hostname: vk.com

To view the statistics on packets for logging of requests to web servers, use the command **show counters all | include clickstream**. The counters displayed by this command are described in the table below.

Table 14

Counter	Description
cr_clickstream_url_for_log	Prepared syslog packets
cr_clickstream_send_one_packet	Sent syslog packets
cr_clickstream_send_fragmented_packet	Sent fragmented syslog packets
cr_clickstream_error_general	The number of errors occured when cloning a TCP packet
cr_clickstream_error_create_header	The number of errors occured when creating a syslog packet
cr_clickstream_warn_invalid_sequence	The number of received TCP packets with invalid sequence number
cr_clickstream_error_no_session	The number of received TCP packets for which a record in the session table was not found
cr_clickstream_no_ssl_tmp_buffer	The size of buffer dedicated for ClientHello
cr_clickstream_ssl_without_hostname	The number of received SSL or TLS handshakes without hostname

Example:

```
EcoNAT:10:> show counters all | include clickstream
Core total, cr_clickstream_url_for_log: 11
Core total, cr_clickstream_send_one_packet: 11
Core total, cr_clickstream_error_no_session: 11
```

6.7 Create and remove user accounts

At any time of configuration, you can create a user (in the configuration mode). Users are created with the command **create user <username> level <permission> secret <password> "<password>"**.

Permissions (level):

- 0 – view only;
- 3 – the ability to execute the command **write**;
- 4 – editing and loading configuration;
- 5 – saving configuration with specific name, but not applying it;
- 8 – applying configuration, run/shutdown EcoNAT;
- 15 – full access, including user management.

Password submission types (secret):

- 0 – plain text;
- 5 – SHA-256 w/salt.

The user information in the configuration is always displayed with encrypted password (type 5).

Also you can create a user by going to the **system users** branch of a configuration tree. Command syntax in this case would be: **<username> level <permission> secret <password> "<password>"**.

EXAMPLE:

```
MyEcoNAT:1:# create user myuser level 15 secret 0 "mypassword"
MyEcoNAT:2:# system users
MyEcoNAT:3:system.users# user1 level 5 secret 0 "password1"
MyEcoNAT:3:system.users# show
users {
user admin level 15 secret 5
5$00$p2c.IaryKF7jSpS1ZKnnmXydvG3AURTTQvJYl52R2s/
user myuser level 15 secret 5
5$00$p2c.IaryKF7jSpS1ZKnnmXydvG3AURTTQvJYl52jgfhgfhg
user user1 level 5 secret 5
5$00$p2c.IaryKF7jSpS1ZKnnmXydvG3AURTTQvJYl52mXydvS12
}
```

To change the level of user permission access, it is not necessarily to change its configuration. You may use the command **grant <username> <permission>**. Changes to user permissions take effect immediately after entering the command.

```
MyEcoNAT:4:# grant user1 8
Use no user <username> command to remove a user.
MyEcoNAT:1:# no user myuser
MyEcoNAT:2:# system users
MyEcoNAT:3:system.users# show
users {
```

```
user admin level 15 secret 5
5$00$p2c.IaryKF7jSpS1ZKnnmXydvG3AURTTQvJYl52R2s/
}
```

If user password is lost, the password can be changed, for performing that you should connect to EcoNAT serial console through port "Console" or "COM", when booting press [i] button. After that console is loaded with a CHPASS username. In this console mode, you may change user passwords and save the settings.

6.8 TACACS Settings

The connection settings for the TACACS server are located in the **system tacacs** branch of the configuration tree. In order to activate the device connection to the TACACS server, the **enable** parameter must be set in this branch.

In EcoNAT, you can configure two TACACS servers (primary and secondary) - **server1** and **server2**.

The list of configurable parameters for connecting to a TACACS server is shown in the table below.

Table 15

Parameter	Description
enable | disable	Active or not connection to the TACACS server
server <IP address>	Address of the TACACS server. An IP address or domain name can be specified
secret <PASS>	Password to connect to the TACACS server. It is stored in an encrypted configuration
fallback {on | off}	In the event that the TACACS authorization fails, it will be attempted to find the user in the local database: **on** - local base search enabled, **off** - local base search disabled
accounting {on | off}	Enabling and disabling user account authorization through TACACS
service_type <TYPE>	Service Type. Must match the type of service specified in the settings of the TACACS server
protocol <PROTOCOL>	Protocol. Must match the specified in the settings of the TACACS server

Configuration example:

```
MyEcoNAT:44:system.tacacs# ls
timeout 5
fallback on
accounting off
service_type "shell"
protocol ""
server1
{
 disable
 server "1.1.1.1"
 secret
"b4ff371e8df242ca5f09801e8d8d8e9cf3a6cb552eb024577026f2f007bdbbdc"
}
server2
{
 enable
```

```
 server "2.2.2.2"
 secret
"e9d029b9851d3ed5334f01605e6041940960bae72c13237366edc9ce2fed432c"
}
```

The **show tacacs** command exists to view information about the current session. The command displays information about the current session on the console and about when the last connection to the TACACS server was made.

```
EcoNAT:20:> show tacacs
The current session is handled by TACACS server at 172.16.1.10:49
TACACS server was accessed 0 seconds ago
```

6.9 LLDP Settings

The EcoNAT system supports Link Layer Discovery Protocol (LLDP) and sends packets to its active ports at 30-s intervals, advertising its presence and capabilities to neighbor nodes. This can be disabled by setting the **lldp** parameter to **off** in the **system.nat_defaults** branch. Also, the value of the **lldp_hostname** parameter can be changed in the **system.nat_defaults** branch. This value is inserted in the System Name (TLV Type 5) field of an LLDP frame.

Additionally, the neighbor nodes that use LLDP protocol can be viewed. To do this, run the **show neighbours <interface name>** command for a specific interface, or **show neighbours all** for all interfaces.

```
MyEcoNAT:1:# show neighbours te6
Interface te6 neighbour:
Last time seen in 22 seconds
Chassis ID = C0:A0:BB:44:94:50
Port ID = C0:A0:BB:44:94:5A
TTL = 120
Interface Name = 'te06’
System Name = 'Dlink’
Capabilities =
 - TP Relay
Management interface address = 10.210.1.212
Maximum Frame Size = 2000
```

6.10 SNMP Settings

EcoSGE supports SNMP v1/v2c. It can respond to GET requests and send Trap messages (Traps). SET requests are not supported.

SNMP Traps are always sent in SNMPv1 format to the destination UDP port 162 using the "public" community string. These traps contain information on FATAL system events.

All available SNMP parameters are contained in the **system.snmp** configuration branch and described in the table below.

Table 16

Parameter	Description
enable | disable	Enable / disable SNMP
trap { true | false }	Enable (true) / disable (false) SNMP trap messaging

Parameter	Description
or trap { on | off }	
trap_host	Trap server IP address or domain name
port	UDP port number for accepting GET requests (161 by default)
allowed_ip ( )	IP addresses for which the system will accept GET requests. Possible values: single address, address range, e.g. 10.10.0.10-10.10.0.20 (hyphen as delimiter), net/subnet address. To set multiple values, use space as delimiter (e.g. **allowed_ip (192.168.10.11 10.10.0.10-10.10.0.20 10.100.0.0/24)**). To add new or delete existing value, use += and -= respectively.
read_community	Community String for read-only operations (GET requests)
description	A text string describing the EcoSGE system (sysDescr object in the System group of MIB-II, RFC1213)
hostname	A text string containing the name of the EcoSGE system (sysName object in the System group of MIB-II, URL Filtering configuration)
contact	A text string containing contact information on the EcoSGE system administrator (sysContact object in the System group of MIB-II, RFC1213)
hostlocation	A text string describing the EcoSGE system location (sysLocation object in the System group of MIB-II, URL Filtering configuration)

Settings example:

```
EcoSGE-4120:system.snmp# ls
enable
trap true
trap_host "192.168.10.100"
port 161
allowed_ip (
  10.10.0.10-10.10.0.20
  10.100.0.0/24
  192.168.10.11
)
trap_port 162
read_community "public"
description "EcoSGE Test"
hostname "EcoSGE-4120"
contact "admin@company.com"
hostlocation "Tech Support Dept"
```

6.11 Shutdown and restart the system

EcoNAT allows hot reconfiguration without interrupting operation. However, there are times when you need to restart the equipment. For example, you have to reboot EcoNAT to apply the version of the embedded software (firmware), as the result of update.

Use **reboot** command for restarting EcoNAT.

After entering the command, the system will ask you to confirm a reboot: «**Confirm (y / N)**» Press **[y]** to confirm, otherwise the restart will not occur.

This confirmation is accompanied by the all critical steps.

To turn off the EcoNAT (for example, in the case of physically moving the device to another site), used **poweroff** command. After entering the command, the system prompts you to confirm the shutdown: « **Confirm (y/N)**». Press **[y]** to confirm, otherwise the shutdown will not occur.

6.12 Firmware management

```
In EcoNAT there are several partitions of the hard disk (partitions) for
the firmware (firmware).  These are the two main sections in which any
firmware version can be installed: PRIM1 and PRIM2, and the FALLBACK
service section.

Using the firmware status command, you can see which firmware versions
are installed in the partitions and their status.

For example:
MyEcoNAT:2:# firmware status
Firmware status:
LABEL    VERSION   CURR    BOOT
PRIM1    0cdd03a*   X       X
PRIM2    9f03e81*   .       .
FALLBACK  bc333b6*   .       .
```

In the output of the **firmware status** command:

```
          LABEL - section,
          VERSION - the firmware version installed in this section,
          CURR - the partition from which the download was made
(current section),
          BOOT - the partition from which EcoNAT will boot when
restarting.
```

6.12.1 *Firmware Upgrade*

```
To update the firmware, you need to transfer information about the
EcoNAT device to the manufacturer.
In order to obtain the necessary information in the CLI EcoNAT, the
copy hwinfo <address> / <file name>   command is used, which generates
and copies to the remote server a file with information about the
device.  With this command, the information can be copied to an HTTP,
FTP or TFTP server.  In the event that authorization is enabled on the
server, the address must be entered along with the login and password:
ftp://user:password@myserver.ru/filename.
After downloading the information file, it must be transferred to the
manufacturer to generate the update.
When the update file is ready, it must be downloaded to the device using
the firmware download command <address> / <file name>.  With this
command, the firmware file can be copied from an HTTP, FTP or TFTP
server.  In the event that authorization is enabled on the server, the
address must be entered along with the login and password:
ftp://user:password@myserver.ru/filename.
To install the downloaded firmware update, use the firmware install
command.
         ATTENTION!    During the installation of the update, the CLI
will not respond to other commands.
```

```
The update will be installed in the inactive hard disk partition.  In
order for the update to take effect, you must reboot the device using
the reboot command.
When the update is installed, the download flag from the inactive
partition will automatically be installed, where the new version is
installed.

MyEcoNAT:5:# firmware status
Firmware status:
LABEL    VERSION   CURR    BOOT
PRIM1    0cdd03a*   X       .
PRIM2    2c758a2*   .       X
FALLBACK  bc333b6*   .       .
```

If the connection to the server is lost when the firmware is downloaded, the upgrade process will be blocked by the system. To reset the blocked process, use the **firmware unlock** command.

6.12.2 *Changing reset settings*

If you need to restart the device from the firmware that is currently inactive, use the firmware rollback command.

Example:

```
MyEcoNAT:6:# firmware status
Firmware status:
LABEL    VERSION   CURR    BOOT
PRIM1    0cdd03a*   X       X
PRIM2    2c758a2*   .       .
FALLBACK  bc333b6*   .       .
MyEcoNAT:7:# firmware rollback
Using PRIM2 as boot partition
Next boot from partition PRIM2
MyEcoNAT:8:# firmware status
Firmware status:
LABEL    VERSION   CURR    BOOT
PRIM1    0cdd03a*   X       .
PRIM2    2c758a2*   .       X
FALLBACK  bc333b6*   .
```

If after the first call of this command to try to call it again, no changes will occur. That is, EcoNAT will still receive a command to restart from the inactive firmware at the moment.

To cancel the start with inactive firmware (after updating or using the **firmware rollback** command), the **firmware revert** command is provided.

In the continuation of the previous example:

```
MyEcoNAT:9:# firmware revert
Using PRIM1 as boot partition
Next boot from partition PRIM1
MyEcoNAT:10:# firmware status
Firmware status:
LABEL    VERSION   CURR    BOOT
PRIM1    0cdd03a*   X       X
PRIM2    9f03e81*   .       .
FALLBACK  bc333b6*   .       .
```

6.13 Getting help

When contacting Technical Support, you have to report the firmware version (displayed by the **show version** command) and information about the license of your hardware (displayed by the **show license** command). Below is an example of CLI output for these commands.

```
EcoSGE:# show version
EcoNAT 4080 series v2.1 (C) Ecotelecom [RDP.RU Ltd.] 2013-2019. All
rights reserved.
Firmware version: 2.1.2.0.1
S/N: 0C7DC8549F00
EcoSGE:#
EcoSGE:# show license
CGNAT: Ok
BRAS: Ok
DPI: Not installed
URL filter: Ok
RADIUS: Ok
CAIR: Not installed
Content filter: Not installed
DPIv6: Ok
```

To display the detailed version information, use the **show version detail** command.

```
EcoSGE:# show version detail
EcoNAT 4080 series v2.1 (C) Ecotelecom [RDP.RU Ltd.] 2013-2019. All
rights reserved.
Firmware version: 2.1.2.0.1
H1: ea9fbdc
H2: 21418ca
S/N: 0C7DC8549F00
```

6.14 Service commands

6.14.1 *Information about memory resources*

To view the free volume of memory use the **show memstat** command.

```
EcoSGE:1:# show memstat
Data plane free/total memory: 19012 MiB / 30064 MiB
Control plane free/total memory: 2559 MiB / 3475 MiB
```

If using the **detail** option, the values in bytes are displayed.

```
EcoSGE:1:# show memstat detail
Data plane free/total memory: 3018025088 bytes / 4294966720 bytes
Control plane free/total memory: 1460961280 bytes / 1813062208 bytes
```

6.14.2 *Information about system resources*

To view information about system resources use the **show resources** command.

```
EcoSGE:# show resources
CPU load: 97% (te7, te8, te9, te10, te11, te12)
Avg egress burst: 10.8 (4.2%)
Avg ingress burst: 11.6 (4.5%)
Translations number: 2152808
```

```
Session table   used/total: 0/33554432 (0.0%)
Translation table used/total: 0/41943040 (0.0%)
Abons table      used/total: 0/131072 (0.0%)
Mbufs number on socket 0 used/total: 15372/2097151 (0.7%)
Block allocation log size: 0 (0.0%)
Bras table     used/total: 0/524288 (0.0%)
DPI host  buffers used/total: 0/65535 (0.0%)
DPI path  buffers used/total: 0/65535 (0.0%)
Awaiting syslog messages: 0 (0.0%)

The description of the output parameters is given in the table below.
```

Table 17

Parameter	Description
CPU load	CPU load. Interfaces, in order of decreasing % of processor load
Avg egress burst	Average egress burst
Avg ingress burst	Average ingress burst
Session table used/total	Session table filling counter (used/total)
Translation table used/total	Translation table filling counter (used/total)
Abons table used/total	Unique abonents table filling counter (used/total)
Mbufs number on socket 0 used/total	Used/total number of data plane buffers of the processor
Block allocation log size	Counter of the buffer of **connection_log** messages (% usage)
Bras table used/total	BRAS authorized abonents table filling counter (used/total)
DPI host buffers used/total	Domain name buffer filling counter (used/total)
DPI path buffers used/total	The counter of filling the information buffer by the URL after the "?" (used/total)
DPI state buffers used/total	Session information buffer filling counter (used/total)
Awaiting syslog messages	**Syslog** messages buffer filling counter

6.14.3 *Information on temperature and fans*

To view information about the temperature of the cores use the **show temperature** command.

```
EcoSGE:> show temperature
Core 0: 54C
Core 1: 53C
Core 2: 50C
Core 3: 54C
Core 4: 57C
Core 5: 54C
Core 6: 52C
Core 7: 54C
Core 8: 55C
Core 9: 56C
```

To view information about the speed of the fans available in the hardware platform use the **show fan** command (for EcoSGE 4xxx models).

In the output of the command:

- NIC <N> – fans on network cards. During normal operation, the fan speed should be within 6000-6398 RPM;
- System fan <N> – fans in the case of the device. The fan speed depends on the temperature in the enclosure of the device. With a minimum load, the fan speed should be between 2600-4800 RPM. At maximum load, the fan speed should be between 16700-22300 RPM.

Example:

```
EcoSGE:> show fan
NIC1 fan : 6308 RPM
NIC2 fan : 6279 RPM
NIC3 fan : 6398 RPM
NIC4 fan : 6081 RPM
System fan 1 : 12162 RPM
System fan 2 : 12162 RPM
System fan 3 : 12272 RPM
System fan 4 : 11946 RPM
System fan 5 : 7219 RPM
System fan 6 : 7297 RPM
System fan 7 : 7417 RPM
System fan 8 : 7297 RPM
```

6.14.4 *Port allocation errors*

To view the information about the CGNAT port allocation errors, use the **show cgnat errors** command.

Example of output of a command.

```
ECONAT:1:> show cgnat errors
Last other port allocation errors:
local ip = 10.4.33.18, global port = 0029, proto = 4, reason = 14, count
= 26
local ip = 10.4.171.19, global port = 0029, proto = 4, reason = 14,
count = 288
...
local ip = 10.4.215.165, global port = 0029, proto = 4, reason = 14,
count = 103
total 3032 other port allocation errors, 12 entries
Last PPTP_GRE port allocation errors:
total 0 PPTP_GRE port allocation errors, 0 entries
Last ICMP port allocation errors:
local ip = 10.4.192.5, global port = 33AA, proto = 3, reason = 2, count
= 506
local ip = 10.4.215.122, global port = 261B, proto = 3, reason = 2,
count = 1436
...
local ip = 10.4.10.92, global port = 0003, proto = 3, reason = 0, count
= 7
total 25520 ICMP port allocation errors, 8 entries
Last UDP port allocation errors:
```

```
local ip = 10.4.96.160, global port = D9A9, proto = 2, reason = 2, count
= 26
...
local ip = 10.4.10.225, global port = F248, proto = 2, reason = 2, count
= 56123
local ip = 10.4.10.69, global port = 837E, proto = 2, reason = 2, count
= 325840
total 20172340 UDP port allocation errors, 187 entries
Last TCP port allocation errors:
local ip = 10.4.12.38, global port = C4C6, proto = 1, reason = 2, count
= 737
local ip = 10.4.101.68, global port = BEB4, proto = 1, reason = 2, count
= 31860
...
local ip = 10.4.176.174, global port = C716, proto = 1, reason = 2,
count = 1204
total 888852360 TCP port allocation errors, 8198 entries
Last GC port freeing errors:
total 0 GC port freeing errors, 0 entries
Debug counters: c0 = 2097260570, c10 = 2097260851, c11 = 281, c14 =
2097260851, c16 = 2097260851, c18 = 2097260851, c19 = 1962724651, c1A =
129378344, c1B = 5157732, c1D = 124, c21 = 1962956737, c22 = 129423896,
c23 = 5158397, c25 = 125, c31 = 888866719, c32 = 20171823, c33 = 25513,
c34 = 3032, c41 = 1962724651, c42 = 129391431, c43 = 5157732, c45 = 124,
c60 = 2097539155, c61 = 2097273938, cE0 = 7787174454, cE3 = 7787173632,
cE4 = 7787173632, cE5 = 541, cF8 = 541, c120 = 3, c122 = 888866719, c140
= 531, c142 = 20171808, c148 = 15, c160 = 7, c162 = 25513, c1B4 = 3032,
c200 = 9528647, c201 = 3943199,
```

In the output of the command:

- **Debug counters** are debugging counters for developers,
- **proto** - type of protocol,
- **reason** is the cause of the error,
- **count** is the value of the error counter.

Legend types of protocols are presented in the table below.

Table 18

Legend	Protocol
0	UNKNOWN - protocols that are not in the categories listed below
1	TCP
2	UDP
3	ICMP
4	L4_OPAQUE (RDP, IPV4, IPV6, ESP, AH, L2TP)
5	PPTP_GRE
6	ARP

The causes of the errors are indicated in the table below.

Table 19

Legend	Cause
1	Information for developers
2	The number of ports for the user has been exceeded, the **limits_peruser** parameter

Legend	Cause
3	Information for developers
4	**Global_ip** allocation error
5	Information for developers
6	Information for developers
7	Information for developers
8	Port block allocation error
9	Information for developers
0xA	Information for developers
0xB	Information for developers
0xC	Information for developers
0xD	Information for developers
0x10	Information for developers
0x11	Information for developers
0x12	Information for developers
0x13	Information for developers
0x14	Can not recognize the protocol
0x20	Information for developers
0x21	Entries do not exist
0x22	Information for developers
0x23	The top TCP ports are out of range
0x24	Lower TCP ports are out of range
0x25	The upper odd UDP ports are out of range
0x26	Lower odd UDP ports are out of range
0x27	Upper even UDP ports out of range
0x28	Bottom even UDP ports out of range
0x29	ICMP Ports Out of Range
0x2A	PPTP_GRE ports are out of range
0x[PP]30	EGRESS translation did not hit any PP pool (pool number where the error occurred)
0x[PP]31	INGRESS translation did not hit any PP pool (pool number where the error occurred)
0x[PP]32	acl EGRESS translation does not match the PP pool (pool number where the error occurred)
0x[PP]33	acl INGRESS translation does not match the PP pool (pool number where the error occurred)
0x34	Translation does not match settings
0x35	The address does not match the global settings of the BNAT pool
0x36	Exceeded the number of connections BNAT pool
0x37	INGRESS connections are forbidden

To clear the error counter, use the **clear cgnat errors** command.

6.14.5 *Counters*

In EcoNAT there are the counters that collect system statistics.

In order to view the status of all the counters, use the **show counters all** command.

```
MyEcoNAT:7:# show counters all
Printing counters...
Port statistics:
Port te8 | dataplane: 0/1429/0; d_bursts:1429/0/0;  arp: 0/0; lacp: 0/0;
lldp: 0/1429; unknown: 0/0; tx_drops: 0
```

```
Port te7 | dataplane: 0/1429/0; d_bursts:1429/0/0;  arp: 0/0; lacp: 0/0;
lldp: 0/1429; unknown: 0/0; tx_drops: 0
Port ge5 | dataplane: 114645/0/0; d_bursts:0/0/0;  arp: 101660/8604;
lacp: 0/0; lldp: 2864/1429; unknown: 10121/0; tx_drops: 0
Port ge4 | dataplane: 0/0/0; d_bursts:0/0/0;  arp: 0/0; lacp: 0/0; lldp:
0/1429; unknown: 0/0; tx_drops: 0
Port ge3 | dataplane: 0/0/0; d_bursts:0/0/0;  arp: 0/0; lacp: 0/0; lldp:
0/1429; unknown: 0/0; tx_drops: 0
Port ge2 | dataplane: 0/96877/0; d_bursts:94158/0/0;  arp: 0/98908;
lacp: 0/0; lldp: 0/1429; unknown: 0/57; tx_drops: 0
Port ge1 | dataplane: 100422/1429/0; d_bursts:1429/0/0;  arp: 98908/0;
lacp: 0/0; lldp: 2864/1429; unknown: 57/0; tx_drops: 0
Total statistics:
Core total, cr_l2_pass_unsupported_proto: 57
Core total, cr_pass_arp: 98908
Core total, cr_session_alloc_no_pool_ingress: 1608
Core total, cr_allocated_logger_mbufs: 3
Core total, cr_allocated_arp_mbufs: 266367
Core total, cr_allocated_lldp_mbufs: 2858
Core total, cr_avg_ingress_rx_queue: 292
Core total, cr_egress_rx_queue_void: 1254429909073
Core total, cr_ingress_rx_queue_void: 1254429805635
Core total, cr_ingress_rx_queue_medium: 103437
Core total, cr_trans_per_user_limit_exceed: 1
Core total, crs_urgent_conns.cc_void: 1441
Core total, crs_urgent_conns.cc_medium: 167
Core total, crs_lazy_conns.cc_void: 167
Core total, crs_lazy_conns.cc_medium: 1441
Displays:
free_laddrs: 65536
free_logging_mbufs: 65437
free_mbufs0: 13264
```

To view the status of the counters changes per second, use the command **show counters diff**.

```
MyEcoNAT:8:# show counters diff
Core diff statistics:
Core total-diff, cr_pass_arp: 2
Core total-diff, cr_allocated_arp_mbufs: 3
Core total-diff, cr_avg_ingress_rx_queue: 65
Core total-diff, cr_egress_rx_queue_void: 14690971
Core total-diff, cr_ingress_rx_queue_void: 14690968
Core total-diff, cr_ingress_rx_queue_medium: 3
```

To view the counters for a particular interface (or for all interfaces), use the **show interface {all | <INT_NAME>} counters** command, where **INT_NAME** is the name of the interface.

```
MyEcoNAT:9:> show interface ge1 counters
Interface name: ge1
rx_good_packets: 0
tx_good_packets: 0
rx_good_bytes: 0
tx_good_bytes: 0
```

…

To view information about traffic passing through the interface, use the **show interface {all | <INT_NAME>} traffic [monitor]** command, where **all** is "show all interfaces" option, **INT_NAME** is the name of the interface**, monitor** is a real-time view. To exit the **monitor** mode, press **[Ctrl+C]** or **[Esc]**, or **[Q]** on the keyboard. The Subtotal row shows the total values for all line interfaces, i. e. non-management/non-logging ones.

```
MyEcoNAT:10:> show interface all traffic monitor
 Interface      Packets In/Out       Bytes In/Out    Errors In/Out
 ---------      --------------       ------------    -------------
  ge2      15677 M / 21212 M     17175 G / 11090 G        0 / 0
  ge3      21307 M / 15600 M    11127 G / 17149 G        0 / 0
-------------------------------------------------------------------------
--------
  Subtotal:   36984 M / 36812 M     28302 G / 28239 G        0 / 0
-------------------------------------------------------------------------
--------
  ge1        397 K / 4105 M     24108 K / 799 G        0 / 0
Press Ctrl+C / Esc / q to stop.
```

For ease of viewing, the decimal prefixes "K, M, G, T" in the SI system are used.

To reset the counters, use the **clear counters** command.

```
MyEcoNAT:9:# clear counters
Counters has been zeroed
```

To view the general statistics for sessions, use the **show statistics** command.

```
EcoNAT:1:> show statistics
*** Total session stats:
used/optimal/total sessions tcp: 3745042 / 16777216 / 83886080
used/optimal/total sessions udp: 5363325 / 16777216 / 83886080
used/optimal/total sessions icmp: 15853 / 16777216 / 83886080
```

7 NAT configuration

This section describes the CG-NAT functionality settings.

7.1 Interfaces

In EcoSGE logic the network interfaces are represented by **interface** type objects.

Interface names begin with the prefix, depending on the transmitter type:

- names of interfaces with installed SFP+ optical modules prefixed with **te**, for example, te10;
- the name of «copper» 1GbE Interfaces begin with the prefix **ge**, for example, ge3.

Titles in the system match the names of network interfaces presented in section "Hardware".

The list of interfaces and their status may be found in the **system interfaces** branch of configuration tree.

```
EcoSGE:1:system.interfaces# !
interfaces
{
 ge1 up
 ge2 up
 ge3 up
 ge4 up
 ge5 up
 ge6 up
 te7 up
 te8 up
}
```

In EcoSGE, you can enable or disable interfaces without going into the interface settings section to make the appropriate changes (**enable | disable**) and then apply configuration changes with the **apply** command. To enable the interface, use the command**interface <INTERFACE_NAME> up**. To disable the interface use the command **interface <INTERFACE_NAME> down**.

The interface can be assigned a description. To do this, go to the configuration context of this interface and enter the **description <DESCR>** command, where **DESCR** is a description with a length of 1 to 240 characters.

Example:

```
2:6:system.interfaces.ge1# description connect to router
2:6:system.interfaces.ge1# ls
enable
description "connect to router"
```

The output of the **show interface brief** displays only the first 50 characters of the description..

```
2:53:# show interface brief
Interface    MAC-
Address     MTU     Speed    Status    Loading(rx/tx)    Description
  mng    00:71:00:C0:9E:00   1518    1 Gbps    active      -        -
  ge1    00:71:00:C0:9E:01   1522    1
Gbps    active      -        connect to router
  ge2    00:71:00:C0:9E:02   1522    1 Gbps    active      0/0      -
```

```
  ge3     00:71:00:C0:9E:03    1522     1 Gbps     active       0/0        -
  ge4     00:71:00:C0:9E:04    1522     1 Gbps     active       0/0        -
  ge5     00:71:00:C0:9E:05    1522     1 Gbps     active       0/0        -
```

Display in the **show interface ge1** command:

```
2:54:# show interface ge1
Interface name: ge1
Description: connect to router
L2MTU: 1522
Packets droped because of L2MTU: 0
MAC address: 00:71:00:C0:9E:01
Link state: active
Link speed: 1 Gbps
Bytes In: 0
Bytes Out: 3060
Packets In: 0
Packets Out: 36
Errors In: 0
Errors Out: 0
```

7.1.1 *Interface "on a stick"*

EcoNAT supports the interface "on a stick" mode (LAN and WAN to one port).

To enable the functional, required an appropriate license (see section "Getting help").

In the configuration section **interfaces** of the configuration tree, the "on a stick" mode is enabled and the interface settings for this mode are stored. This mode is applied directly to all EcoNAT interfaces.

```
system.interfaces# show
 interface_mode onstick
 ge1
 {
   enable
   vlan_local 10
   vlan_global 20
   description ""
 }
ge2
 {
   enable
   vlan_local 10
   vlan_global 20
   description ""
 }
...
```

Table 20

Parameter	Description
interface_mode	A required parameter that indicates which mode will be used. Parameter values: **default** - EcoNAT works in a mode of separation of interfaces into global and local; **onstick** - all EcoNAT interfaces work in the mode of combining LAN and WAN
geN	Enumeration of EcoNAT interfaces
enable/disable	Administrative on/off interface
vlan_local	Local tag for interface "on a stick"

Parameter	Description
vlan_global	Global Tag for interface "on a stick"
description	Description of the interface. 1 to 240 characters

To use the "on a stick" mode, one need to specify the **vlan_mode vlan** in the **nat_defaults** section (see the "Pools and ACL" section) to enable support for tagged traffic.

ATTENTION, any changes in the settings of the "on a stick" mode will be applied only after the device is rebooted. Even changes to the **vlan_local** and **vlan_global** numbers on the interfaces will not be applied after the execution of the **apply** command, until the device is rebooted.

Therefore, after these settings, you must execute the following commands:

- apply the configuration with the **apply** command,
- save the changes with the **write** command,
- reboot the device with the **reboot** command.

It is possible that on a router connected to the EcoNAT, you will need two static ARP entries for each VLAN interface: local and global, respectively. This situation can occur if one MAC address is allocated on the connected router for both VLAN interfaces of the same port or group of ports that are connected to the LAG.

7.1.2 *Show interface commands*

To view a summary of the state of the interfaces, use the **show interface brief** command. The command displays a table on the console, where the Status column shows the current status of the interface:

- active – interface in active state,
- down – the interface is not connected,
- disabled – the interface is disabled through EcoNAT CLI.

```
MyEcoNAT:2:# interface ge6 up
MyEcoNAT:3:# interface ge6 down
MyEcoNAT:4:# show interface brief
Interface    MAC-Address      MTU      Speed    Status    Loading(rx/tx)
  mng    00:0D:48:31:EB:54   1518    100 Mbps   active       -
  ge1    00:0D:48:31:EB:53   1522   unknown/error  down       -
  ge2    00:0D:48:31:EB:52   1522   unknown/error  down       -
  ge3    00:0D:48:31:EB:51   1522   unknown/error  down       -
  ge4    00:0D:48:31:EB:50   1522   unknown/error  down       -
  ge5    00:0D:48:31:EB:4F   1522   unknown/error  down       -
  ge6    00:0D:48:31:EB:4E   1522   unknown/error  down       -
  te7    00:0D:48:31:EB:4D   1522    10 Gbps   active      70/100
  te8    00:0D:48:31:EB:4C   1522    10 Gbps   active     100/75
  te9    00:0D:48:31:EB:4B   1522    10 Gbps   active     88/100
  te10   00:0D:48:31:EB:4A   1522    10 Gbps   active     100/94
  te11   00:0D:48:31:EB:49   1522    10 Gbps   active     35/34
  te12   00:0D:48:31:EB:48   1522    10 Gbps   active     33/44
```

For complete information about the interfaces, use **show interface all** command.

```
MyEcoNAT:5:> show interface all
```

```
Interface name: ge1
L2MTU: 1522
Packets droped because of L2MTU: 0
MAC address: 00:0D:48:28:1A:6D
Link state: active
Link speed: 100 Mbps
Bytes In: 5730486
Bytes Out: 111945
Packets In: 93360
Packets Out: 1317
Errors In: 0
Errors Out: 0
Broadcast Packets Received: 2526
Multicast Packets Received: 0
Valid Packets Received: 552239826119
Packets Received [64 Bytes]: 12168186116
Packets Received [65-127 Bytes]: 69833219845
Packets Received [128-255 Bytes]: 18352133279
Packets Received [256-511 Bytes]: 8100120469
Packets Received [512-1023 Bytes]: 9285356600
Packets Received [1024 to Max Bytes]: 435328201814
Receive Oversize Count: 0
Interface name: ge2
MTU: 1522
...
```

You may view information about the SFP and SFP+ modules, including DDM information with the **show interface all transceiver** (or **show sfp all**) command. This information is not available for ports with a "copper" interface.

```
MyEcoNAT:6:# show interface all transceiver
Interface name: te1
Module Vendor Name: OEM
Module Part Number: SFP+-10G-LR
Module Serial Number: P1309040348
Module Revision: A
Module Manufactoring Date: 130904
Module supports DDM: yes
Module temperature: 39.00 C
Module voltage: 3.25 Volt
Module TX power: 0.69 mW (-1.60 dBm)
Module RX power: 0.28 mW (-5.50 dBm)
Interface name: te2
Module Vendor Name: OEM
Module Part Number: SFP+-10G-LR
Module Serial Number: P1309040335
Module Revision: A
Module Manufactoring Date: 130904
Module supports DDM: yes
Module temperature: 37.00 C
Module voltage: 3.25 Volt
Module TX power: 0.61 mW (-2.12 dBm)
Module RX power: 0.30 mW (-5.13 dBm)
Interface name: ge3
```

```
SFP details are not accessible, code -14
…
```

You may also select a specific interface to display information about the relevant SFP module. Example: **show interface *te18* transceiver**.

For viewing the MNG interface status use the **show interface mng** command.

```
MyEcoNAT:7:#  show interface mng
Managment interface name: mng
MTU: 1500
MAC address: 00:0D:48:28:1A:6E
Link state: active
Link speed: 100 Mbps
Bytes In: 62190
Bytes Out: 101668
Packets In: 710
Packets Out: 967
Errors In: 0
Errors Out: 0
Multicast: 7
```

For viewing ARP information use the **show arp all** command or **show arp <INTERFACE>** command (for the certain interface). This command shows the interface MAC address, virtual channel information (merged logging interfaces - EcoNAT EtherChannel) and the log server information.

Example.

```
MyEcoNAT:7:# show arp te18
Interface te18 neighbour:
   Interface MAC      = 00:0D:48:31:EB:42
  EcoNAT EtherChannel:
   EtherChannel IP     = 172.16.5.253
   EtherChannel MAC    = 00:0D:48:31:EB:4E
  connection log server 0:
   target ip (network)   = 172.16.5.254
   target ip (link level) = 172.16.5.254
   target MAC (linklevel) = 00:00:00:00:00:00
   Last ARP reply: never
```

7.2 The principles of NAT

EcoNAT performs address translation, transferring data between the network interfaces that are combined into pairs. In each pair of network interfaces, one of them belonging to the private (local) side of the NAT, has an even number, and the other belonging to the public (global) of the NAT – has an odd number.

For example, the interface 8 is private (connected to the internal network), and the interface 7 – public (global addresses are placed on it).

The data that arrive at one of a pair of network interfaces, leaving NAT through another interface of the same pair (see figure below). If hairpinning is configured, data can leave the NAT through the same interface on which they arrived (see paragraph "Pools and ACL").

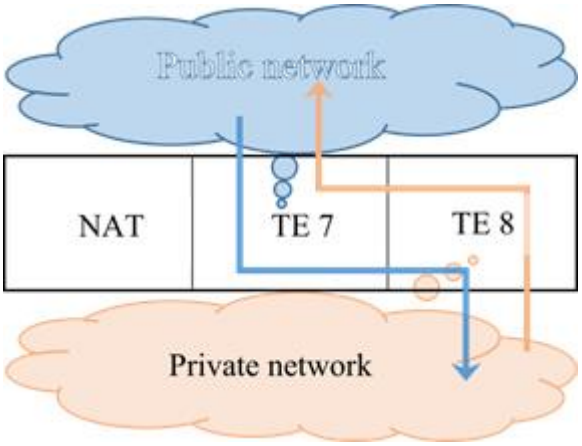

Figure 8

7.3 Pools and ACL

7.3.1 *The concept of pools*

EcoNAT main configuration element are the so-called pools, characterized by a type of translations and a set of external (global) IPv4 address. Each pool is assigned its priority. The smaller the numerical value of the priority, the earlier the pool is processed. Each pool is associated with an ACL, which contains the selection criteria for a given pool depending on the content fields of the received IP packet.

NOTE: You should not assign the same priority to several pools! This will lead that only the one pool, which was created first, will be used. The rest of the pools will be ignored.

Each pool can be either active (***enable***), or inactive (***disable***). Pool names always begin with the **pool** prefix.

7.3.2 *General settings*

In the **system nat_defaults** configuration branch there are common settings and system settings that are applied by default to all newly created pools (timeouts_inactivity and limits_peruser blocks are copied to the pool when it is created). Description of the parameters of this configuration branch is shown in the table below.

Table 21

Parametr	Description
vlan_mode	Processes/analyzes packets to a specified level of encapsulation. Possible parameter values: **untagged, vlan, qinq**
alg ftp	Enables ALG option for FTP protocol. Possible values: on/off
alg pptp	Enables ALG option for PPTP protocol. Possible values: on/off
alg rtsp	Enables ALG option for RTSP protocol. Possible values: on/off
alg sip	Enables ALG option for SIP protocol. Possible values: on/off
alg alg_on_bnat	Enables ALG option for static NAT. Possible values: on/off
sessions_per_translation	Number of active sessions per translation
udp_inbound_refresh	Enables updating the UDP translations with ingress (incoming) packets. Possible parameter values: on/off
l2mtu	The maximum size of MTU for incoming The value is specified for L2 with the L2-header. Default - 1522, maximum - 9692
port_block_size	The size of port block. Default 128. It is strongly recommended not to change this value

Parametr	Description
portlimit_low	The value of used range "lower" ports (up to 1024-th) for each user. Possible parameter values: nolimit, 64, 128, 256, 512
low_to_all_udp	Allows to use ports from the upper range if the ports from the lower range are exhausted. Possible parameter values: on/off
lldp	Enable (on) / disable (off) LLDP (**on** by default)
lldp_hostname ""	Hostname that will be used in LLDP advertisements
permit_invalid_flow	Enable (on) / disable (off) the function of establishing sessions on TCP segments for which the SYN flag is not set. The default value is **off**. A TCP session always starts with a segment with the SYN flag set, and such packets can be erroneous or malicious, therefore, by default, new sessions on such segments do not start, and the segments themselves are discarded. However, in some cases, this behavior can be useful, for example, in cases where part of the traffic goes along a different route or for the correct operation of TCP connections over which data is not transmitted for a long time. The functionality affects the behavior of the entire device and cannot be redefined in pools. To apply the changes, you must run the **apply** command
timeouts_inactivity {}	In this section is defined the inactivity time (in seconds) for different protocols and TCP states, after which an unused session will be closed forcibly
timeouts_inactivity translation	Sets the time in seconds before the expiry of which, even in the case of user inactivity, he will be guaranteed the allocation of ports of the same global IP. The recommended default value 86400
timeouts_inactivity udp	Inactivity timeout in seconds for UDP sessions. The port on the global IP is released after this timeout. Default 300
timeouts_inactivity icmp	Inactivity timeout in seconds for ICMP sessions. The port on the global IP is released after this timeout. Default 60
timeouts_inactivity tcp_handshake	Timeout in seconds for a translation established by TCP packet with SYN flag set (unsteady TCP session). Default 4
timeouts_inactivity tcp_active	Inactivity timeout in seconds for established TCP sessions in ESTABLISHED state. The port on the global IP is released after this timeout. Default 300
timeouts_inactivity tcp_final	Inactivity timeout in seconds for TCP sessions. Default 240
timeouts_inactivity tcp_reset	Timeout in seconds to reset TCP sessions. Default 4
timeouts_inactivity tcp_session_active	Inactivity timeout in seconds for active TCP sessions. Default 120
timeouts_inactivity udp_session	Inactivity timeout in seconds for active UDP sessions. Default 120
timeouts_inactivity icmp_session	Inactivity timeout in seconds for active ICMP sessions. Default 120
timeouts_inactivity other	Inactivity timeout in seconds for other IP-sessions (GRE for example). The protocol on the global IP is released after this timeout. Default 300. (applicable to NAT and 1:1 types of pools only)
timeouts_inactivity special	Inactivity timeout in seconds for protocols that require a larger timeout value. Default 600
timeouts_inactivity special_tcp_ports ( )	TCP ports to which to apply the increased timeout value
limits_peruser {}	Limit the number of ports to users
limits_peruser portlimit_icmp	This parameter describes the maximum number of simultaneously existing ICMP sessions for a user
limits_peruser portlimit_tcp limits_peruser portlimit_udp	Limit the number of global (external) ports that can be assigned to one user (the local IP). It is recommended to set the values that are multiples of 64, from 64 to 32256.

Parametr	Description
	It makes sense to service providers to assign to ordinary users (individuals): from 1024 to 4096. Values less than 1024 may cause problems with the performance of some applications. Value greater than 32256 may result in that a user will be able to exhaust ports of IP addresses. For users, who are most demanding about the number of ports, it makes sense to create a separate CGNAT pool with a lower compression ratio (less local IP to one global), or use the NAT pool for allocation to a user of the whole IP with all the ports for the period of its activity

Tcp_session_timeout, udp_session_timeout, icmp_session_timeout parameters triggered in the occasion when the translation is created and the first session appears. All other sessions will be created with the same parameters from **timeouts_inactivity** section (copied automatically from **system nat_defaults**).

Vlan_mode parameter may have the values: **untagged**, **vlan**, **qinq**. Where, **untagged** means that EcoNAT will process only untagged traffic, untagged and with one label – **vlan**, untagged, with one or two tags – **qinq**.

By default (**untagged** parameter value), EcoNAT passes transparently all traffic that are different from the standard IP, in order to smoothly transmit traffic on protocols such as BFD, OSPF, BGP, and so on. In particular, IP-packets with options (except for fragmented IP-packages with options), and also, tagged traffic are passed also without NAT.

If **vlan** mode is activated, EcoNAT will see label in the L2 header, look in to it and redirect the IP in accordance with the existing rules with the same label. Thus IP addresses under different labels should not overlap, because EcoNAT will see it as the same user. For example, if the packet comes with the IP address 192.168.1.100 and Tagged VLAN 100 and comes the packet with IP address 192.168.1.100 and Tagged VLAN 200, in fact it will be different users, but for EcoNAT, it will be the same address of the user. Therefore, the traffic may be disrupted.

To clear the translation table, use the **clear sessions all** command.

```
MyEcoNAT:1# clear sessions all
Sessions table purged
Translation table purged
```

7.3.3 *Creating a pool*

To create a pool, use the **create pool <pool name>** command. This creates a CGNAT pool with typical parameters (more about CGNAT pools, see paragraph 6.2.5) and named ***poolPOOL_NAME*** (prefixed «pool»). If the specified pool name already starts with the prefix «pool», eg, «pooltest», the name does not change, and in the future, this pool will be located in a **pools** configuration branch named **pooltest**. When you try to create a pool with an existing name, the pool will not be created. For example, if after changing the pooltest settings you try to create the pool named «test» (which will be automatically changed to «pooltest»), pooltest configuration will not be changed, and the new pool will not be created.

Then the values of pool parameters may be changed by going to the branch of a configuration tree corresponding to this pool (for details see the section Configurations).

EXAMPLE:

```
MyEcoNAT:1:# create pool test
MyEcoNAT:2:# goto pooltest
MyEcoNAT:3:pools.pooltest# show
type cgnat
enable
acl none
priority 100
global_ip ( )
port_range 1024:65535
hairpin on
connection_logging on
 randomize_ports off
timeouts_inactivity
{
 translation 86400
 udp 300
 icmp 60
 tcp_handshake 4
 tcp_active 300
 tcp_final 240
 tcp_reset 4
 tcp_session_active 120
 udp_session 120
 icmp_session 120
 other 300
 special 600
 special_tcp_ports ( )
}
limits_peruser
{
 portlimit_icmp 1024
 portlimit_tcp 1024
 portlimit_udp 1024
}
```

As you can see in example, the ACL bindings is not performed when you are creating a new pool.

Pool parameters are described in the table below.

Table 22

Parameter	Description
type	Pool type: cgnat, static, nat, fake
enable или disable	Pool state
acl	ACL associated with the pool
priopity	Pool priority
global_ip ( )	Global IP-addresses associated with the pool. To avoid ARP requests from the router to the EcoNAT WAN interface, it is not recommended to assign **global_ip** from the subnet of interfaces of routers between which EcoNAT is enabled
port_range	The range of external ports available for use on each global IP address owned by cgnat pool. The recommended value (range): 1024:65535. With these settings in each global IP will be available 64512 UDP and TCP ports as well

Parameter	Description
global_map ( )	Consistency between global and local IP addresses. Addresses are set in pairs in the format <**local address**>**[~vid]** – <**global address**>. The parameter is valid for the **static** pool. The parameter is valid for pools of type static. **Vid** - VLAN identifier (from 0 to 4094). Optional parameter. The **vid** value is prefixed with "~" (tilde) without a space after the address
hairpin	Allows hairpinning. If the address on the external network coincides with the global address of one of the pools, EcoNAT will perform double translation without sending a packet outside (on the WAN). Hairpinning works only if it is allowed in both pools where users are connected in such a way
allow_external_connect	Allow external connection. The parameter is valid for the **nat** pool
connection_logging	Connection logging: (on) or (off)
randomize_ports	Allows port assignments from a block in a random order (on). Ports are allocated one-be-one if (off)
timeouts_inactivity	In this section is defined the inactivity time (in seconds) for different protocols and TCP states, after which an unused session will be closed forcibly. It is recommended not to change this parameters without purpose, one can use default settings instead
timeouts_inactivity translation	Sets the time in seconds before the expiry of which, even in the case of user inactivity, he will be guaranteed the allocation of ports of the same global IP. The recommended default value 86400
timeouts_inactivity tcp_handshake	Timeout in seconds for a translation established by TCP packet with SYN flag set (unsteady TCP session). Default 4
timeouts_inactivity tcp_active	Inactivity timeout in seconds for established TCP connections in the ESTABLISHED state. After this timeout port on the global IP is released. Default 300
timeouts_inactivity tcp_final	Inactivity timeout in seconds for TCP sessions. Default 240
timeouts_inactivity tcp_reset	Timeout in seconds to reset TCP sessions. Default 4
timeouts_inactivity tcp_session_active	Inactivity timeout in seconds for active TCP sessions. Default 120
timeouts_inactivity udp_session	Inactivity timeout in seconds for active UDP sessions. Default 120
timeouts_inactivity icmp_session	Inactivity timeout in seconds for active ICMP sessions. Default 120
timeouts_inactivity other	Inactivity timeout in seconds for other IP-sessions (GRE for example). The protocol on the global IP is released after this timeout. Default 300. (applicable to NAT and 1:1 types of pools only)
timeouts_inactivity special	Inactivity timeout in seconds for protocols that require a larger timeout value. Default 600
timeouts_inactivity special_tcp_ports ( )	TCP ports to which to apply the increased timeout value
limits_peruser	Limit the number of ports to users
limits_peruser portlimit_tcp limits_peruser portlimit_udp	Limit the number of global (external) ports that can be assigned to one user (the local IP). It is recommended to set the values that are multiples of 64, from 64 to 32256. It makes sense to service providers to assign to ordinary users (individuals): from 1024 to 4096. Values less than 1024 may cause problems with the performance of some applications. Value greater than 32256 may result in that a user will be able to exhaust ports of IP addresses. For users, who are most

Parameter	Description
	demanding about the number of ports, it makes sense to create a separate pool cgnat with a lower compression ratio (less local IP to one global), or use the nat pool for allocation to a user of the whole IP with all the ports for the period of its activity
limits_peruser portlimit_icmp	This parameter describes the maximum number of simultaneously existing ICMP sessions for a user

These options are available depending on the pool type. The table below shows the parameters available for each type of pool.

Table 23

Parameters	cgnat	nat	static	fake
type	+	+	+	+
enable	+	+	+	+
acl	+	+	+	+
priority	+	+	+	+
global_ip ( )	+	+		
port_range	+			
global_map ( )			+	
hairpin	+	+	+	+
allow_external_connect		+	+	
connection_logging	+	+	+	+
randomize_ports	+	+	+	+
timeouts_inactivity	+	+	+	+
limits_peruser	+			

After the pool is created, it needs to add a global IPv4 address, this pool will use. To do this, enter the pool edit mode using the **goto <pool name>** or **edit <pool name>** command and type the **global_ip add <global IP address>** command. Type the **global_ip remove <global IP address>** command to remove the IP address in the pool edit mode.

```
MyEcoNAT:4:pools.pooltest# global_ip add 200.0.2.0/24
MyEcoNAT:5:pools.pooltest# show global_ip
global_ip ( 200.0.2.0/24 )
MyEcoNAT:6:pools.pooltest#
```

For the convenience of working with IP addresses arrays the alternative way of modifying **global_ip** parameter is provided. Go into editable pool in the configuration tree branch, next to the **global_ip** parameter and use **add** and **remove** commands or a **'+='** character command to add an address, **'-='** to remove the addresses. To add/remove multiple addresses at once, you may type them inside the parentheses, separated by **[Enter]**. In order to add the address in the empty array or to completely replace the existing array enter the address list in parentheses with no **add** command or **'+ ='** character command. When making changes to the **global _ ip** parameter, the CLI will not exit the parameter edit mode until the closing parenthesis is entered.

```
MyEcoNAT:4:pools.pooltest# global_ip
MyEcoNAT:5:(pools.pooltest.global_ip)# (
MyEcoNAT:6:(pools.pooltest.global_ip)# 10.11.22.1
MyEcoNAT:7:(pools.pooltest.global_ip)# 2.3.4.5
MyEcoNAT:8:(pools.pooltest.global_ip)# 188.165.1.1
MyEcoNAT:9:(pools.pooltest.global_ip)# )
MyEcoNAT:10:pools.pooltest# show
 type cgnat
 enable
```

```
 acl none
 priority 100
 global_ip (
  2.3.4.5
  10.11.22.1
  188.165.1.1
 )
 port_range 1024:65535
 …
 }
MyEcoNAT:11:pools.pooltest# global_ip -=(188.165.1.1 2.3.4.5)
MyEcoNAT:12:pools.pooltest# show
 type cgnat
 enable
 acl none
 priority 100
 global_ip (
  10.11.22.1
 )
 port_range 1024:65535
 …
 }
MyEcoNAT:13:pools.pooltest# global_ip +=(
MyEcoNAT:14:(pools.pooltest.global_ip)# 188.165.1.1
MyEcoNAT:15:(pools.pooltest.global_ip)# 111.1.1.255
MyEcoNAT:16:(pools.pooltest.global_ip)# 77.7.7.7
MyEcoNAT:17:(pools.pooltest.global_ip)# )
MyEcoNAT:18:pools.pooltest# show
 type cgnat
 enable
 acl none
 priority 100
 global_ip (
  10.11.22.1
  77.7.7.7
  111.1.1.255
  188.165.1.1
 )
 port_range 1024:65535
 …
 }
```

You may verify the created pool with **analyze <pool name>** command. The output of the will show what is missing for normal operation of the pool.

```
MyEcoNAT:1:# analyze pooltest
# --- During processing pool 'pooltest' ----:
# No ACL associated with the pool
# use command 'use ACLNAME POOLNAME' to associate acl with a pool
MyEcoNAT:2:#
```

If all is well with the pool, no messages will be displayed.

```
MyEcoNAT:1:# analyze pooltest
MyEcoNAT:2:#
```

Pool can be deactivated using the **disable** command. In this case, its configuration information remains, and the pool will not be applied. A deactivated pool is considered to be good anyway with the **analyze** command.

```
MyEcoNAT:1:# edit pooltest
MyEcoNAT:2:pools.pooltest# disable
```

Use **enable** command to activate the pool:

```
MyEcoNAT:1:# edit pooltest
MyEcoNAT:2:pools.pooltest# enable
```

7.3.4 *Creating an ACL*

After creating a pool, it is necessary to create an ACL determining which packets should be handled by that pool. Use the **create acl** <**ACL name**> command to create an ACL. This command creates an empty rule list called **aclACL_NAME**. Use the **edit <ACL name>** or **goto <ACL name>** command to open the rule list for editing.

The command for setting up a rule has the following syntax:

<num> <type> <protocol> <src>[~<vid>] <dst>

Optional parameters are enclosed in square brackets. Only values of the parameters are required in the command.

The table below describes all the parameters of the command.

Since the list of rules itself does not matter, it must be tied to a particular pool. The binding is done by applying **use <ACL name> <pool name>**.

EXAMPLE:

```
MyEcoNAT:1:# create acl a
MyEcoNAT:2:# goto acla
MyEcoNAT:3:acls.acla# show
acla {
}
MyEcoNAT:4:acls.acla# 10 allow ip 194.85.16.0/24 any
MyEcoNAT:5:acls.acla# show
acla {
 10 permit ip src net 194.85.16.0/24 dst any
}
MyEcoNAT:6:acls.acla# use acla pooltest
MyEcoNAT:7:acls.acla# goto pooltest
MyEcoNAT:8:pools.pooltest# show
type cgnat
enable
acl acla
priority 100
global_ip ( )
…
```

Destination address is ***any*** by default.

```
MyEcoNAT:1:acls.acla# 10 allow ip 10.0.0.1
MyEcoNAT:2:acls.acla# show
acla {
10 permit ip src host 10.0.0.1 dst any
```

```
}
MyEcoNAT:3:acls.acla#
```

Source address is ***any*** by default, if you don't specify other value, it is necessarily to use keyword ***dst*** in a command.

```
MyEcoNAT:1:acls.acla# 10 allow dst 40.0.0.1
MyEcoNAT:2:acls.acla# show
acla {
10 permit ip src any dst host 40.0.0.1
}
MyEcoNAT:3:acls.acla#
```

If you want to allow all possible addresses, the command will look like: ***10 allow any any***.

7.3.5 *The procedure for determining the pool for the packet*

When you receive a new IP packet (at the beginning of a new session), the pools are processed in the order of their priority: the priority value is smaller, the earlier this pool is processed. For example, if there are pools with the priorities of: 200, 150, 250, the first pool will be handled with priority 150.

Then will be analyzed the ACL, associated with a processed pool and the rules contained in the ACL are tested.

If the parameters of the received packet satisfy the **allow** rule, the packet will be processed by this pool. If the parameters of the received packet satisfy the conditions of a **deny** rule, then this pool will not be considered for this packet, and following pools will be considered in the priority order. If the packet does not satisfy the conditions of the current ACL rules, it examines the next rule of the pool or (if there are no rules anymore) moving on to the next pool in order of priority. If there are no more pools, the IPv4 packet will be transmitted without translation (like through the wire).

7.3.6 *CGNAT pool*

CGNAT pool provides Carrier-grade NAPT translation, in which the addresses and the ports are translated. Addresses and blocks of ports for client connections are allocated dynamically. Addresses allocation policy aims to equal ports filling of each global address. This gives the maximum benefit for the efficient use of IP addresses. Available parameters for this type of pools are represented in the table above in the section "Pools and ACL".

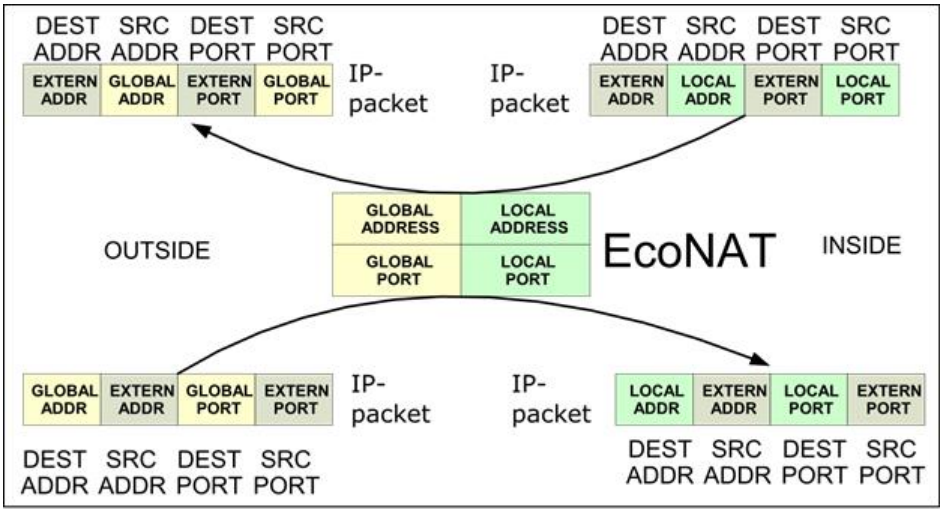

Figure 9

7.3.7 *Nat pool*

Nat pool, otherwise referred to as the basic-NAT, provides only address translation (ports are not translated). Available parameters for this type of pools are represented in the section "Pools and ACL".

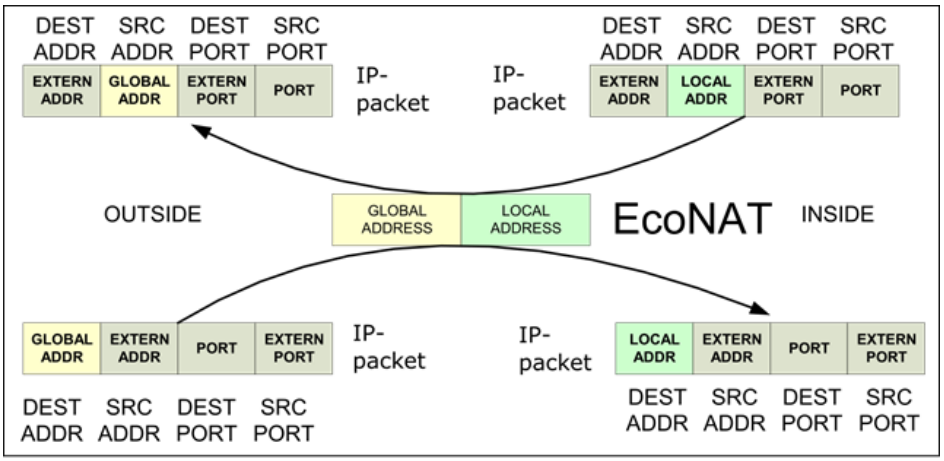

Figure 10

The ***cgnat*** pool type is generated by default when you are creating a pool, but you may change a pool type after its creating, assigning the corresponding value of the **type** parameter, located in the pool (***nat*** for example).

Some of the parameters connected to ***cgnat*** pool disappears after changing its type to ***nat***. Also, there a new option **allow_external_connect** appear, which allows outside connections. If you switch **allow_external_connect** to ***on***, the translation may be established "by the initiative of" external hosts. This increases accessibility for peer-to-peer networks, as it will be able to connect from the outside at any ports to your users (unless, of course, the port is open on the host).

Usually, it makes sense to do two types of ***nat*** pool: one for those users who need connections initiated from outside (want to share torrents actively), and the other – for those customers who want to initiate connections only on their own initiative.

```
MyEcoNAT:1:# create pool b
MyEcoNAT:2:# goto poolb
```

```
MyEcoNAT:3:pools.poolb# type nat
MyEcoNAT:4:pools.poolb# show
type nat
enable
acl none
priority 200
global_ip ( )
hairpin on
allow_external_connect on
connection_logging on
randomize_ports off
timeouts_inactivity
{
 translation 86400
 udp 300
 icmp 60
 tcp_handshake 4
 tcp_active 300
 tcp_final 240
 tcp_reset 4
 other 300
 special 600
 special_tcp_ports ( )
}
MyEcoNAT:5:pools.poolb#
```

7.3.8 *Static pool (1_to_1)*

Static pool – is a pool in which the address translation is set administratively. Available parameters for this type of pools are represented in the section "Pools and ACL".

Each local address pool is uniquely mapped to a global address, port translation is not performed. Instead of a list of IPv4 global addresses that belong to a pool (instead of the **global_ip** parameter) there is a list of 1:1 translations (**global_map** parameter).

Translations in **global_map** parameter are defined as: <**local address**>**[~vid]** – <**global address**>. The parameter is valid for pools of type static. **Vid** - VLAN identifier (from 0 to 4094). Optional parameter. The **vid** value is prefixed with "~" (tilde) without a space after the address.

```
MyEcoNAT:1:# create pool c
MyEcoNAT:2:# goto poolc
MyEcoNAT:3:pools.poolc# type static
MyEcoNAT:4:pools.poolc# show
type static
enable
acl none
priority 100
global_map ( )
hairpin on
allow_external_connect on
connection_logging on
randomize_ports off
MyEcoNAT:5:pools.poolc# global_map += 192.168.0.5-200.0.0.3
MyEcoNAT:6:pools.poolc# global_map += (192.168.1.2~102-3.3.3.3)
```

```
MyEcoNAT:7:pools.poolc#
```

You may not specify the ACL for a static pool, in this case, it is implicitly assumed that the ammount of rules will be applied to the pool: **allow ip src <*local address*> dst any**.

If the ACL is still defined and configured, it is first checked, and then those which is implicitly assumed.

ATTENTION! If an ACL is attached to a **static** pool, then the list should not include the line **permit any any**.

7.3.9 *Fake pool*

Fake pool type intended for handling addresses that do not need translation (for example, if you need URL filtering, but do not need NAT translation for the addresses). The use of this type of pool is described in paragraph "Configuring URL Filtering for addresses that do not fall under the NAT". Available parameters for this type of pools are represented in the section "Pools and ACL".

7.4 Typical configurations

7.4.1 *NAT for Internet access*

Typical scheme of how EcoNAT used for network address translation for Internet access, is shown in the figure below.

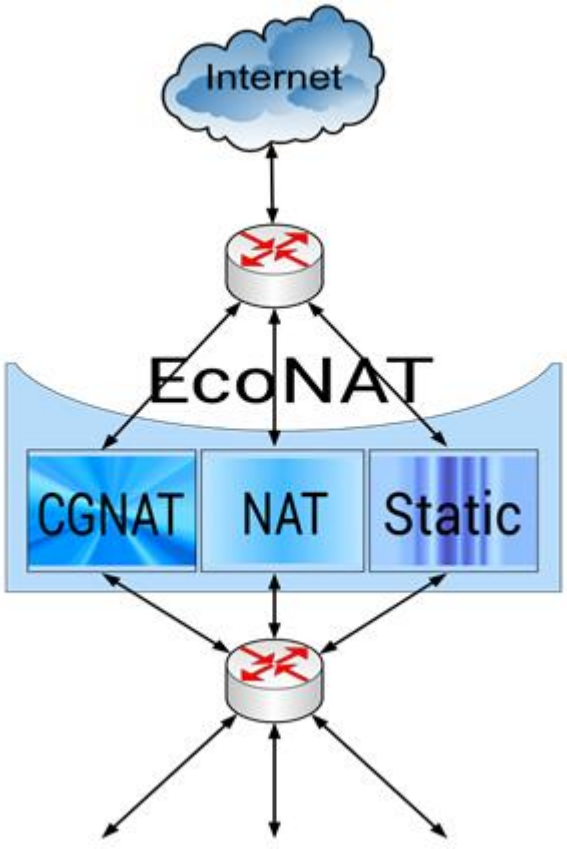

Figure 11

EcoNAT typical configuration includes three type of pools for different types of traffic. Pools are recommended to enter in the following order:

1. Static IP addresses are allocated administratively in a static pool (see Pools and ACL).
2. NAT pool (see Pools and ACL) – is needed when using protocols that do not support ports (for example, GRE). An exception is the PPTP protocol (**cgnat** pool is created for its processing and **alg pptp** parameter is switched on in NAT general settings). If you need a basic NAT with permitted externally-initiated connections and independently basic NAT with banned connections – it is possible to have two NAT pool differing with **allow_external_connect** parameter value.
3. Most of the subscribers have an Internet access through CGNAT pool (see Pools and ACL).

If you have a situation when you need to adjust the translation of overlapping IP address ranges in two different pools (see figure below), it is important to set the rule priorities. Keep in mind, however, that the first rule with a lower number would be handled, in case of the triggering the rest are not checked.

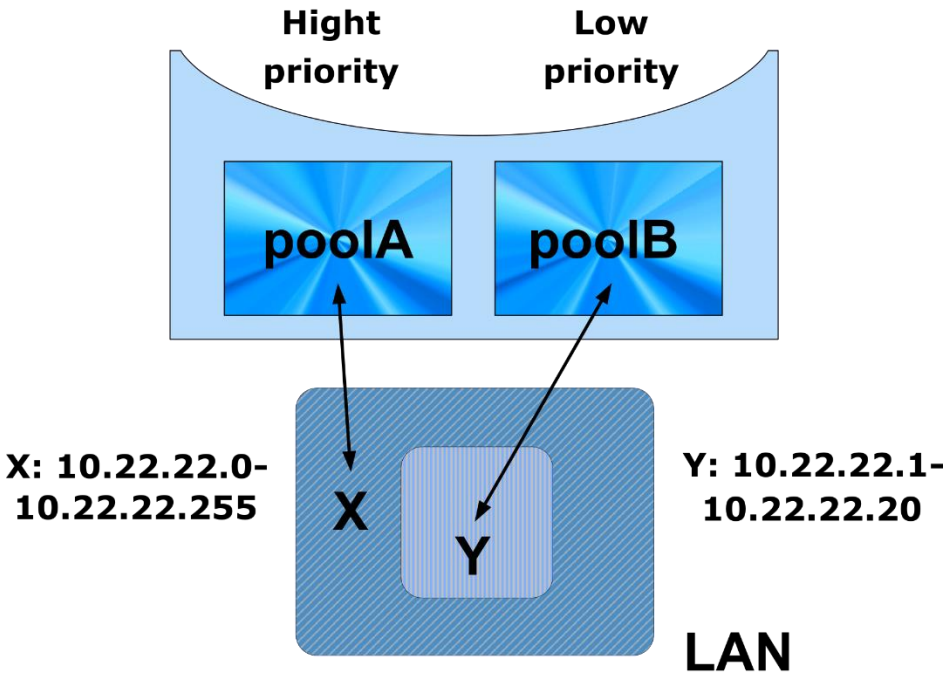

Figure 12

In the situation shown in the figure ACL must be formed for the two pools with the following rules (with the proviso that ***poolA*** has higher priority than ***poolB***):

for ***poolA:***

```
acla {
 10 deny ip src range 10.22.22.1-10.22.22.20 dst any
 20 allow ip src net 10.22.22.0/24 dst any
}
```

for ***poolB:***

```
aclb {
 10 allow ip src range 10.22.22.1-10.22.22.20 dst any
}
```

In this case, whether the source IP belongs to the range of Y (10.22.22.1-10.22.22.20) will be checked at first for ***poolA***. If belongs, the packet will be rejected by ***poolA*** pool, and then ***poolB*** and

his list of rules will be examined. If not belongs, the rule whether the source IP belongs to the range X (10.22.22.0/24) will be tested, and in this case, the packet will be passed ***poolA*** pool.

The rule whether the source IP belongs to the range of Y for ***poolB*** will be checked, and in this case, the packet will be passed.

7.4.2 *Implementation in peer to peer networks with overlapping address ranges*

A typical usage EcoNAT pattern for the network address translation peering is shown below. On the left there is EcoNAT implementation in the service provider network diagram, and on the right is point of view of the end user diagram.

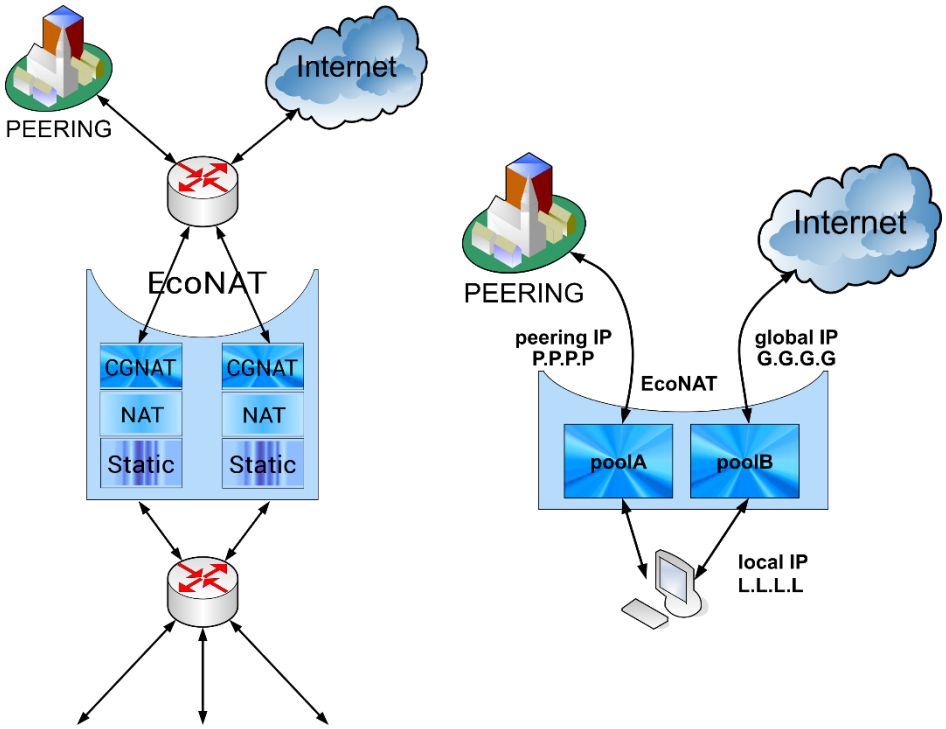

Figure 13

If the subscriber address space of service provider overlaps with addresses used his peering partners, for the implementation of peering into a traffic exchange points (with addresses kind of 10.0.0.0/8, or other type of private addresses) you need to implement the translation of users IP into free address space.

EcoNAT is ready to solve this problem. For this purpose, create additional NAT pools and set the rules for the selection of these pools in associated with them ACL.

In most peering cases, it is created a single NAT pool with allowed external connections (for maximum transparency) and a higher than for pools serving the Internet access priority. The criterion for the choosing of the pool may serve the DST field of the IP packet for which in the ACL rules indicates the network of peering partners in the **dst** field. Thus, packets bound for the peer-to-peer network, will be translated with selected pool to the address space allocated to provider.

7.5 Configuration objects management

7.5.1 *ACL cloning*

When configuring EcoNAT you have the ability to clone the ACL, creating a copy of the list of rules under a different name. To do this, use **cloneacl <*name of the copied ACL*> <*name of the new ACL*>** command.

```
MyEcoNAT:1:# cloneacl myoldacl mynewacl
MyEcoNAT:2:#
```

7.5.2 *Unbind the ACL from the pool*

To remove the link between the pool and the ACL, simply apply **no use <*pool name*> <*name of the ACL*>** command.

```
MyEcoNAT:1:# no use myacl mypool
MyEcoNAT:2:#
```

7.5.3 *Remove pool*

To remove the pool use **no pool <*pool name*>** command.

```
MyEcoNAT:1:# no pool pooltest
MyEcoNAT:2:#
```

If you want to delete all the pools in the configuration, use **droppools** command.

```
MyEcoNAT:1:# droppools
MyEcoNAT:2:#
```

7.5.4 *Remove ACL rules*

To remove the rules, you must first start editing a specific ACL that contains these rules with the **edit <*ACL name*>** command. The **no rule <*ACL rule number*>** command that deletes the rule is contextual and can only be run from within an editable configuration ACL.

```
MyEcoNAT:1:acls.myacl# no 100
MyEcoNAT:2:acls.myacl#
```

7.5.5 *Remove entire ACL*

Use **no acl** command to delete entire ACL **.**

```
MyEcoNAT:1:# no acl acla
MyEcoNAT:2:#
```

Use **dropacls** to erase all ACLs from the configuration.

```
MyEcoNAT:1:# dropacls
MyEcoNAT:2:#
```

7.6 Show commands

7.6.1 *Show translations*

Use the **show xlate** commands to view the currently available translations.

The table below shows the various variations of this command.

Table 24

Command	Description
show xlate gap ADDR:PORT	Output of all current translations for the specified pair: global address + global port
show xlate gastat ADDRRANGE	Output of translation statistics for the specified global address
show xlate global ADDRRANGE	Output of all current translations for the specified global address
show xlate gport PORT	Output of all current translations for the specified global port (regardless of address)
show xlate lap ADDR:PORT	Output of all current translations for the specified pair: local address + local port
show xlate lastat ADDRRANGE	Output of translation statistics for the specified local address
show xlate local ADDRRANGE	Output of all current translations for the specified local address
show xlate lport PORT	Output of all current translations for the specified local port (regardless of address)
show xlate pool POOLNAME	Output of the translations for the specified pool

Examples of output are shown below.

```
EcoNAT:3:> sh xlate gap 10.4.5.136:56575
egress UDP 1.10.0.167:56575-10.4.5.136:56575 pool: poolx; Last packet
93.15 seconds ago; To be deleted in 206.85 seconds of inactivity.

EcoNAT:14:# sh xlate gastat 7.0.165.80
Pool type cgnat; gaddr: 7.0.165.80; ; TCP: Free blocks: 4294967294; UDP
even: Free blocks: 4294967294; UPD odd: Free blocks: 4294967294; ICMP:
Free blocks: 4294967295

EcoNAT:5:> sh xlate global 10.4.5.136
egress UDP 1.10.0.167:5221-10.4.5.136:5221 pool: poolx; Last packet
323.87 seconds ago; To be deleted right now.

EcoNAT:10:> sh xlate gport 56575
egress UDP 1.10.0.167:56575-10.4.5.136:56575 pool: poolx; Last packet
160.79 seconds ago; To be deleted in 139.21 seconds of inactivity.

EcoNAT:13:> sh xlate lap 1.10.0.167:43656
egress TCP 1.10.0.167:43656-10.4.5.136:43656 pool: poolx; Last packet
4.41 seconds ago; To be deleted in 295.59 seconds of inactivity.

EcoNAT:14:> sh xlate lastat 1.10.0.0/24
Pool type cgnat; laddr: 1.10.0.2, gaddr: 1.4.4.215; ; TCP: Blocks: 0;
Conns: 0 of 4096; UDP even: Blocks: 0; Conns: 0 of 2048; UPD odd:
Blocks: 0; Conns: 0 of 2048; ICMP: Blocks: 0; Conns: 0 of 4096
Pool type cgnat; laddr: 1.10.0.3, gaddr: 1.4.4.115; ; TCP: Blocks: 4;
Conns: 42 of 4096; UDP even: Blocks: 0; Conns: 0 of 2048; UPD odd:
Blocks: 0; Conns: 0 of 2048; ICMP: Blocks: 0; Conns: 0 of 4096
```

```
Pool type cgnat; laddr: 1.10.0.11, gaddr: 1.4.4.235; ; TCP: Blocks: 0;
Conns: 0 of 4096; UDP even: Blocks: 0; Conns: 0 of 2048; UPD odd:
Blocks: 0; Conns: 0 of 2048; ICMP: Blocks: 0; Conns: 0 of 4096

EcoNAT:51:> sh xlate local 10.10.0.167
egress UDP 1.10.0.167:13446-10.4.5.136:13446 pool: poolx; Last packet
285.09 seconds ago; To be deleted in 14.91 seconds of inactivity.

EcoNAT:18:> sh xlate lport 55700:55744
egress TCP 1.10.0.167:55744-10.4.5.136:55744 pool: poolx; Last packet
249.57 seconds ago; To be deleted right now.
egress TCP 1.10.0.43:55719-10.4.4.211:1029 pool: poolreserve; Last
packet 2.12 seconds ago; To be deleted in 297.88 seconds of inactivity.
egress UDP 1.10.0.35:55718-10.4.4.247:1040 pool: poolreserve; Last
packet 327.97 seconds ago; To be deleted right now.

EcoNAT:58:> sh xlate pool poolx
egress UDP 1.10.0.175:32407-10.4.5.134:32407 pool: poolx; Last packet
143.45 seconds ago; To be deleted in 156.55 seconds of inactivity.
egress TCP 1.10.0.196:54468-10.4.5.133:54468 pool: poolx; Last packet
1.22 seconds ago; To be deleted in 298.78 seconds of inactivity.
```

7.6.2 *Show sessions*

Use the **show sessions** commands to view the currently available sessions.

The table below shows the various variations of this command.

Table 25

Command	Description
show sessions gap ADDR:PORT	Output of all current sessions for the specified pair: global address + global port
show sessions global ADDRRANGE	Output of all current sessions for the specified global address
show sessions gport PORT	Output of all current sessions for the specified global port (regardless of address)
show sessions lap ADDR:PORT	Output of all current sessions for the specified pair: local address + local port
show sessions local ADDRRANGE	Output of all current sessions for the specified local address
show sessions lport PORT	Output of all current sessions for the specified local port (regardless of address)
show sessions rap ADDR:PORT	Output of all current sessions for the specified pair: remote address + remote port
show sessions remote ADDRRANGE	Output of all current sessions for the specified remote address
show sessions rport PORT	Output of all current sessions for the specified remote port

Examples of output are shown below.

```
EcoNAT:83:> sh sessions gap 10.4.125.134:43057
egress UDP 1.10.0.175:43057-10.4.125.134:43057 173.194.44.80:443; Last
packet 7.78 seconds ago; To be deleted in 292.22 seconds of inactivity.
```

```
EcoNAT:84:> sh sessions global 10.4.125.134
egress UDP 1.10.0.175:26228-10.4.125.134:26228 8.8.8.8:53; Last packet
17.09 seconds ago; To be deleted in 282.91 seconds of inactivity.

EcoNAT:95:> sh sessions gport 41656:42000
egress TCP 1.10.0.175:41656-10.4.125.134:41656 87.240.165.80:443; Last
packet 31.62 seconds ago; To be deleted in 208.38 seconds of inactivity.
egress UDP 1.10.0.175:41669-10.4.125.134:41669 8.8.8.8:53; Last packet
29.12 seconds ago; To be deleted in 270.88 seconds of inactivity.

EcoNAT:108:> sh sessions lap 1.10.0.175:5060
ingress UDP 1.10.0.175:5060-10.4.125.134:5060 163.172.91.161:5067; Last
packet 272.29 seconds ago; To be deleted in 27.71 seconds of inactivity.
EcoNAT:109:> sh sessions local 100.64.0.4~2
egress UDP 100.64.0.4~2:1024-100.64.0.4:1024 4.4.4.4:53; Last packet 8.27
seconds ago; To be deleted in 291.73 seconds of inactivity

EcoNAT:115:> sh sessions lport 30556:31000
egress UDP 1.10.0.167:30556-10.4.125.136:30556 8.8.8.8:53; Last packet
159.33 seconds ago; To be deleted in 140.67 seconds of inactivity.
egress UDP 1.10.0.175:30894-10.4.125.134:30894 8.8.8.8:53; Last packet
133.56 seconds ago; To be deleted in 166.44 seconds of inactivity.

EcoNAT:116:> sh sessions rap 8.8.8.8:53
egress UDP 1.10.0.167:6148-10.4.125.136:6148 8.8.8.8:53; Last packet
265.48 seconds ago; To be deleted in 34.52 seconds of inactivity.

EcoNAT:122:> sh sessions remote 8.8.8.8
egress UDP 1.10.0.167:6148-10.4.125.136:6148 8.8.8.8:53; Last packet
282.31 seconds ago; To be deleted in 17.69 seconds of inactivity.

EcoNAT:136:> sh sessions rport 2000:2100
egress UDP 1.10.0.169:35881-10.4.124.251:1027 111.71.62.156:2075; Last
packet 27.07 seconds ago; To be deleted in 92.93 seconds of inactivity.
```

7.6.3 *Deleting the sessions*

To delete sessions, use the **clear sessions** command.

The table below shows the various variations of this command.

Table 26

Command	Description
clear sessions all	Deleting of all current sessions
clear sessions gap ADDR:PORT	Deleting of all current sessions for the specified pair: global address + global port
clear sessions global ADDRRANGE	Deleting of all current sessions for the specified global address
clear sessions gport PORT	Deleting of all current sessions for the specified global port (regardless of address)
clear sessions lap ADDR:PORT	Deleting of all current sessions for the specified pair: local address + local port
clear sessions local ADDRRANGE	Deleting of all current sessions for the specified local address
clear sessions lport PORT	Deleting of all current sessions for the specified local port (regardless of address)

Command	Description
clear sessions rap ADDR:PORT	Deleting of all current sessions for the specified pair: remote address + remote port
clear sessions remote ADDRRANGE	Deleting of all current sessions for the specified remote address
clear sessions rport PORT	Deleting of all current sessions for the specified remote port

Example.

```
EcoNAT:126:> clear sessions gap 10.4.125.134:43057
egress UDP 1.10.0.175:43057-10.4.125.134:43057 173.194.44.80:443; Last
packet 9.86 seconds ago; To be deleted right now.
```

7.6.4 *Show binds*

To see the currently existing bindings of local IP addresses to global bindings, use **show bind** commands.

The table below shows the various variations of this command.

Table 27

Command	Description
show bind global IPRANGE | any	Output of all bindings for the specified global address
show bind local IPRANGE | any	Output of all bindings for the specified local address
show bind summary	Output of the counters for global ports
show bind usage	Output of the counters for g_abons_table filling

Examples of output are shown below.

```
EcoNAT:137:pools.poolx# show bind local any
CGNAT pool 'poolx'
Global IP usage: 4 out of 4
1.1.1.0 -> 2.2.2.3 | 86211 sec
1.1.1.1 -> 2.2.2.2 | 86211 sec
1.1.1.2 -> 2.2.2.1 | 86211 sec
1.1.1.3 -> 2.2.2.0 | 86211 sec
1.1.1.4 -> 2.2.2.0 | 86211 sec
1.1.1.5 -> 2.2.2.1 | 86211 sec
1.1.1.6 -> 2.2.2.2 | 86211 sec
1.1.1.7 -> 2.2.2.3 | 86211 sec
1.1.1.8 -> 2.2.2.3 | 86211 sec
1.1.1.9 -> 2.2.2.2 | 86211 sec
1.1.1.10 -> 2.2.2.1 | 86211 sec
1.1.1.11 -> 2.2.2.0 | 86211 sec
1.1.1.12 -> 2.2.2.0 | 86211 sec
1.1.1.13 -> 2.2.2.1 | 86211 sec
1.1.1.14 -> 2.2.2.2 | 86211 sec
1.1.1.15 -> 2.2.2.3 | 86211 sec
1.1.1.100 -> 2.2.2.3 | 86244 sec
EcoNAT:138:pools.poolx# show bind global any
CGNAT pool 'poolx'
Global IP usage: 4 out of 4
```

```
1.1.1.3 -> 2.2.2.0 | 86205 sec
1.1.1.4 -> 2.2.2.0 | 86205 sec
1.1.1.11 -> 2.2.2.0 | 86205 sec
1.1.1.12 -> 2.2.2.0 | 86205 sec
1.1.1.2 -> 2.2.2.1 | 86205 sec
1.1.1.5 -> 2.2.2.1 | 86205 sec
1.1.1.10 -> 2.2.2.1 | 86205 sec
1.1.1.13 -> 2.2.2.1 | 86205 sec
1.1.1.1 -> 2.2.2.2 | 86205 sec
1.1.1.6 -> 2.2.2.2 | 86205 sec
1.1.1.9 -> 2.2.2.2 | 86205 sec
1.1.1.14 -> 2.2.2.2 | 86205 sec
1.1.1.0 -> 2.2.2.3 | 86205 sec
1.1.1.7 -> 2.2.2.3 | 86205 sec
1.1.1.8 -> 2.2.2.3 | 86205 sec
1.1.1.15 -> 2.2.2.3 | 86205 sec
1.1.1.100 -> 2.2.2.3 | 86238 sec
2:146:pools.poolx# show bind usage
g_abons_table usage is 17 out of 65536
```

7.6.5 *Port allocation errors*

7.6.6 *Port allocation errors*

To view the information about the CGNAT port allocation errors, use the **show cgnat errors** command.

Example of output of a command.

```
ECONAT:1:> show cgnat errors
Last other port allocation errors:
local ip = 10.4.33.18, global port = 0029, proto = 4, reason = 14, count
= 26
local ip = 10.4.171.19, global port = 0029, proto = 4, reason = 14,
count = 288
...
local ip = 10.4.215.165, global port = 0029, proto = 4, reason = 14,
count = 103
total 3032 other port allocation errors, 12 entries
Last PPTP_GRE port allocation errors:
total 0 PPTP_GRE port allocation errors, 0 entries
Last ICMP port allocation errors:
local ip = 10.4.192.5, global port = 33AA, proto = 3, reason = 2, count
= 506
local ip = 10.4.215.122, global port = 261B, proto = 3, reason = 2,
count = 1436
...
local ip = 10.4.10.92, global port = 0003, proto = 3, reason = 0, count
= 7
total 25520 ICMP port allocation errors, 8 entries
Last UDP port allocation errors:
local ip = 10.4.96.160, global port = D9A9, proto = 2, reason = 2, count
= 26
...
```

```
local ip = 10.4.10.225, global port = F248, proto = 2, reason = 2, count
= 56123
local ip = 10.4.10.69, global port = 837E, proto = 2, reason = 2, count
= 325840
total 20172340 UDP port allocation errors, 187 entries
Last TCP port allocation errors:
local ip = 10.4.12.38, global port = C4C6, proto = 1, reason = 2, count
= 737
local ip = 10.4.101.68, global port = BEB4, proto = 1, reason = 2, count
= 31860
...
local ip = 10.4.176.174, global port = C716, proto = 1, reason = 2,
count = 1204
total 888852360 TCP port allocation errors, 8198 entries
Last GC port freeing errors:
total 0 GC port freeing errors, 0 entries
Debug counters: c0 = 2097260570, c10 = 2097260851, c11 = 281, c14 =
2097260851, c16 = 2097260851, c18 = 2097260851, c19 = 1962724651, c1A =
129378344, c1B = 5157732, c1D = 124, c21 = 1962956737, c22 = 129423896,
c23 = 5158397, c25 = 125, c31 = 888866719, c32 = 20171823, c33 = 25513,
c34 = 3032, c41 = 1962724651, c42 = 129391431, c43 = 5157732, c45 = 124,
c60 = 2097539155, c61 = 2097273938, cE0 = 7787174454, cE3 = 7787173632,
cE4 = 7787173632, cE5 = 541, cF8 = 541, c120 = 3, c122 = 888866719, c140
= 531, c142 = 20171808, c148 = 15, c160 = 7, c162 = 25513, c1B4 = 3032,
c200 = 9528647, c201 = 3943199,
```

In the output of the command:

- **Debug counters** are debugging counters for developers,
- **proto** - type of protocol,
- **reason** is the cause of the error,
- **count** is the value of the error counter.

Legend types of protocols are presented in the table below.

Table 28

Legend	Protocol
0	UNKNOWN - protocols that are not in the categories listed below
1	TCP
2	UDP
3	ICMP
4	L4_OPAQUE (RDP, IPV4, IPV6, ESP, AH, L2TP)
5	PPTP_GRE
6	ARP

The causes of the errors are indicated in the table below.

Table 29

Legend	Cause
1	Information for developers
2	The number of ports for the user has been exceeded, the **limits_peruser** parameter
3	Information for developers
4	**Global_ip** allocation error
5	Information for developers

Legend	Cause
6	Information for developers
7	Information for developers
8	Port block allocation error
9	Information for developers
0xA	Information for developers
0xB	Information for developers
0xC	Information for developers
0xD	Information for developers
0x10	Information for developers
0x11	Information for developers
0x12	Information for developers
0x13	Information for developers
0x14	Can not recognize the protocol
0x20	Information for developers
0x21	Entries do not exist
0x22	Information for developers
0x23	The top TCP ports are out of range
0x24	Lower TCP ports are out of range
0x25	The upper odd UDP ports are out of range
0x26	Lower odd UDP ports are out of range
0x27	Upper even UDP ports out of range
0x28	Bottom even UDP ports out of range
0x29	ICMP Ports Out of Range
0x2A	PPTP_GRE ports are out of range
0x[PP]30	EGRESS translation did not hit any PP pool (pool number where the error occurred)
0x[PP]31	INGRESS translation did not hit any PP pool (pool number where the error occurred)
0x[PP]32	acl EGRESS translation does not match the PP pool (pool number where the error occurred)
0x[PP]33	acl INGRESS translation does not match the PP pool (pool number where the error occurred)
0x34	Translation does not match settings
0x35	The address does not match the global settings of the BNAT pool
0x36	Exceeded the number of connections BNAT pool
0x37	INGRESS connections are forbidden

To clear the error counter, use the **clear cgnat errors** command.

8 BRAS functionality

This functionality is available in EcoBRASxxxx-LIC license.

BRAS functionality allows the service provider to implement the so-called Services Gateway to restrict users access speed to IP services and data transmission services in both directions, to disconnect subscribers to forward them to the portal or web-page with the notice about the need to refill their account, as well as to demonstrate the information to subscribers by forwarding to the specified information portal.

An expected IPoE service model:

- the absence of encapsulation PPP, PPPoE, etc., means clean IPoE ;
- subscriber is uniquely identified by its IPv4 address within the provider network;
- aggregation or core (L3-connected subscribers) switch is a gateway for subscribers -not the BRAS;
- IP address to the subscriber may be issued statically or dynamically (by a third-party device, not EcoSGE) – using DHCP server associated with the billing system;
- device puts the speed limit of traffic(policing) the whole IP traffic, including the one that misses the NAT pools and is not subject to NAT translation. Non-IP traffic passes transparently.

BRAS permits to carry out short-term excess of traffic speed over the settlement (burst), duration of burst is limited by traffic volume corresponding to the first second to the contracted subscriber rate.

8.1 BRAS configuration

BRAS settings are located in the **system.bras** configuration branch.

```
EcoSGE:# go bras
EcoSGE:system.bras# ls
enable
pass_multicast true
pass_routing_protocols true
pass_bgp_port true
bgp_port 179
acl none
no_shape ( )
no_shape_v6 ( )
policies
{
}
services
{
}
radius
{
  request_burst_interval 10
  request_burst_size 64
  coa
```

```
  {
    disable
    port 3799
    secret ""
  }
  radius_groups
  {
  }
  radius_servers
  {
  }
}
```

BRAS functionality can be enabled and disabled using the **enable** and **disable** commands directly in the **system.bras** branch.

The table below describes the available BRAS settings.

Table 30

Parameter	Description
acl	List of IP addresses of subscribers that need to process with BRAS. The default value is **none**, which is equivalent to **0.0.0.0/0**. Thus, all subscribers entering any pool will also be transferred to BRAS processing
pass_multicast	Passing multicast traffic transparently, not performing the speed limit for it (recommended value: true)
pass_routing_protocols	Passing the traffic routing protocols (the OSPF and BGP), not performing speed limits for them (recommended value: true)
pass_bgp_port bgp_port	Passing BGP traffic on the selected TCP port and not performing its control (recommended value: true)
no_shape no_shape_v6	The external global IPv4 or IPv6 address, for which the data rate is not limited (for the subscribers allowed by the billing system). Here you may enter the IP addresses of game servers, IPTV servers and other resources that should be available to users at maximum speed
policies services	The set of settings that limit the speed of receiving and transmitting data also redirect to the portal to refill subscriber's account. More will be described in section "Policies and services"
radius	The set of RADIUS settings. More will be described in the section "RADIUS server settings"

*The modified configuration is applied only after the **apply** command.*

8.2 Billing console and EcoBRAS protocol

Specialized EcoBRAS proprietary protocol is used to download information from billing to the EcoNAT. It is a simple text protocol.

For its work, you need to establish a connection to port 2225 of the EcoNAT control interface. Then there is the exchange of query strings (to EcoNAT) and answers by EcoNAT. In the case of an incorrect query string EcoNAT immediately and forcibly closes the connection without sending a response string.

The query string cannot exceed 64 kilobytes.

Request and response string are ended with ASCII LF (code 0x0A) symbol.

Request string may contain ASCII CR (code 0x0D) symbol, but they will be ignored.

The protocol supports the following commands:

testRID

add

- **ads**
- **statall**

remove

clearall

8.2.1 *TestRID*

```
B: testRID
E: 1-40 18-8 19-8 24-8 26-21 27-16 31-41 35-21 37-28 40-21 41-8 55-28
82-34 135-21 143-40 146- 40 147-31 155-34 163-45 182-34 202-41 207-40
209-16 212-34 213-34 215-41 217-43 220-34 227-16
228-31 231-40 232-16 240-34 242-28 244-34
```

On **testRID** request you are given in a row a list of pairs of **CONTRACTNUMBER-TARIFNUMBER**. Billing uses this information to sync lists to determine which number of the contract is not in EcoNAT, and which is superfluous.

```
B: testRID
E:
```

If EcoNAT not offer contracts (for example, if he had just loaded), it responds with an empty string.

Immediately after BRAS loading the mode of transmission of all traffic is switched on (in order to serve the users at the time, not yet loaded information from the billing). After receiving of the first **testRID** the timer, which for 600 seconds keeps the transmission of all traffic switched on. At this time, it may receive new **testRID**, and after 10 minutes finally BRAS switches to the main mode (when traffic is prohibited from those subscribers which is not allowed explicitly in the billing). To see the status of the timer use **time** command.

8.2.2 *Add*

```
B: add 24372 {oid} LIM10M/LIM10M 10.21.0.208, 10.210.0.207, // RULE43
E:
```

Add command adds policy for a subscriber with the specified contract number.

In case of success BRAS returns an empty string. In case of failure BRAS closes the connection. Detailed format of **add** command is described in a table below.

Table 31

№	Field	Content type	Description
1	add	3 symbols	Command – add a contract
2		TAB	Delimiter
3	24372	Digits	Contract number
4		TAB	Delimiter
5	{oid}	5 symbols string	Contract type (in our case, always the fixed string '{oid}')
6		SPACE	Delimiter

№	Field	Content type	Description
7	LIM10M	String: LIM speed K/M/G or UNLIM	Upstream speed (to the Internet). K/M/G – means kilo/mega/giga bit. For example: LIM64K – 64 Kbps. UNLIM – means no speed limit
8	/	Symbol '/'	Delimiter
9	LIM10M	String	Downstream speed (from the Internet)
10		SPACE	Delimiter
11	10.21.0.208,	IP address, delimiter‘,’	Subscriber IP address (may follow a few in a row, each of the IP addresses gets the speeds that are set for this contract)
12		SPACE	Delimiter
13	//	2 symbols	
14		SPACE	Delimiter
15	RULE	4 symbols	
16	43	Number	Subscriber tariff number (ID of the tariff in the billing)
17		LF	The end of the query string

8.2.3 *Ads*

With the help of the EcoBRAS protocol, the addition of clients of the shared contract is carried out by the **ads** command.

```
B: ads 24372 {oid} LIM10M/LIM10M 10.21.0.208, 10.21.0.207, // RULE43
E:
```

The syntax of the **ads** command is described in the table below.

Table 32

№	Field	Content	Description
1	ads	3 characters	Command - add a shared contract
2		TAB	Delimiter
3	24372	Figures	Number of the contract
4		TAB	Delimiter
5	{oid}	String 5 characters	Type of contract (in our case always a fixed line '{oid}')
6		SPACE	Delimiter
7	LIM10M	String: LIM speed value K/M/G or UNLIM	Downstream speed (from the Internet). K / M / G - means kilo/mega/giga bit. For example, LIM64K is 64 Kbps. UNLIM - without speed limits
8	/	Character '/'	Delimiter
9	LIM10M	String	Speed upstream (to the Internet)
10		SPACE	Delimiter
11	10.21.0.208,	IP address, delimiter ‘,’	IP-address of the subscriber (can follow a few in a row, each of the IP-addresses gets those speeds that are set for this contract)
12		SPACE	Delimiter
13	//	2 characters	
14		SPACE	Delimiter
15	RULE	4 characters	
16	43	Number	Number of the specific rule in the EcoBRAS table
17		LF	End of query string

8.2.4 *Remove*

```
B: remove 24372 {oid} LIM10M/LIM10M 10.21.0.208, 10.210.0.207,
E:
```

Syntax of **remove** command is close to the **add** command, but instead of adding it removes the contract and the associated subscriber address.

Table 33

№	Field	Content	Description
1	remove	6 symbols	Command – remove a contract
2		TAB	Delimiter
3	24372	Digits	Contract number
4		TAB	Delimiter
5	{oid}	5 symbols string	Contract type (in our case, always the fixed string '{oid}')
6		SPACE	Delimiter
7	LIM10M	String: LIM speed K/M/G or UNLIM	Upstream speed (to the Internet). K/M/G – means kilo/mega/giga bit. For example: LIM64K – 64 Kbps. UNLIM – means no speed limit
8	/	Symbol '/'	Delimiter
9	LIM10M	String	Downstream speed (from the Internet)
10		SPACE	Delimiter
11	10.21.0.208,	IP address, delimiter‘,’	Subscriber IP address (may follow a few in a row, each of the IP addresses gets the speeds that are set for this contract)
12		LF	The end of the query string

*If in the **remove** query is specified the list of IP-addresses, other than the previously specified in the **add** request, the BRAS deauthorize all IP previously registered in all **add** commands to this contract number. If **add** command was issued again (without the remove), then for IP addresses in the re-add it will be set the speed specified in the second request (update speed rate).*

8.2.5 *Statall*

At the port 2225 is also available a **statall** service command, that displays a list of all users traffic information.

```
$ telnet 2.2.2.2 2225
Trying 2.2.2.2...
Connected to 2.2.2.2.
Escape character is '^]'.
statall
10.210.0.81: rx_bytes=5630281 tx_bytes=1211117 rx_packets=6201
tx_packets=11017
10.210.0.82: rx_bytes=133560825 tx_bytes=7870065 rx_packets=109851
tx_packets=53843
10.210.0.83: rx_bytes=0 tx_bytes=0 rx_packets=0 tx_packets=0
```

8.2.6 *Clearall*

This command is used to delete all policies added through the billing console.

8.3 BRAS service console

For convenience of service support, on the TCP port number 2226 of EcoNAT management interface is functioned a BRAS service console, which allows testing the user state (as by IP-address, also by contract number) to service support team.

```
$ telnet 2.2.2.2 2226
Trying 2.2.2.2...
```

```
Connected to 2.2.2.2.
Escape character is '^]'.
Start connection...
Please use next commands:
ip ADDRESS – for show information about address contract
NUMBER – for show information about contract
> ip 10.210.0.81
IP => 5100d20a
Contract number = 54174
Upload speed limit = 102400 KB
Download speed limit = 102400 KB
>
```

The following describes the commands to view and clear BRAS information.

Show brasinfo all command gives brief information on the BRAS state for all the supported addresses.

```
ECOHOST:10:# show brasinfo all
Bras info for addresses 0.0.0.0-255.255.255.255:
10.210.1.0    Authorized Bytes rx/tx: 0/60; Packets rx/tx: 0/1
10.210.1.234   Authorized Bytes rx/tx: 0/60; Packets rx/tx: 0/1
10.210.1.89   Authorized Bytes rx/tx: 17464/0; Packets rx/tx: 118/0
…
```

Show brasinfo command applied to a specific IP address, gives detailed information on the status of the session and applied services for the IP-subscriber

```
MyEcoNAT:14:# show brasinfo 10.210.0.125
Bras info for address 10.210.0.125:
================================================================================
Subscriber 10.210.0.125
================================================================================
Status                              Authorized
Maximum data rate upstream total                unlim Kb/s
Maximum data rate downstream total               unlim Kb/s
Bytes downstream total                       404843
Bytes upstream total                           0
Packets downstream total                       5272
Packets upstream total                          0
Session timeout expires in                     32499 s
Idle timeout expires in                       28798 s
Interim interval expires in                       6 s
--------------------------------------------------------------------------------
1. serviceredi "serviceredi"
Enabled
Maximum data rate upstream                       55 Kb/s
Maximum data rate downstream                      55 Kb/s
Bytes downstream                             0
Bytes upstream                                0
Packets downstream                            0
Packets upstream                               0
--------------------------------------------------------------------------------
2. service20m "service20m"
Enabled
Maximum data rate upstream                     20479 Kb/s
```

```
Maximum data rate downstream                    20479 Kb/s
Bytes downstream                               404695
Bytes upstream                                  0
Packets downstream                              5270
Packets upstream                                0
```

Show brasinfo command, applied to the range of addresses up to the million (example, **show brasinfo** ***10.210.0.81/12***), gives detailed view of BRAS state for the specified addresses. If this command is used for bigger range of addresses, it gives a brief summary (so as **show brasinfo all** command).

Show brasinfo summary command gives brief statistics for the certain policy.

```
MyEcoNAT:17:system.bras.policies.policy1# show brasinfo summary
=========================================================
 brasinfo summary
=========================================================
 Policy                                      Subscribers
---------------------------------------------------------
 policy1                                             504
---------------------------------------------------------
 Status
---------------------------------------------------------
 Authorization                                       203
 Authorized                                            6
 Rejected                                            295
 Error                                                 0
 Deleting                                              0
---------------------------------------------------------
 Total                                               504
=========================================================
```

With a large number of addresses, information output to the console may take some time. Command execution may be interrupted by pressing **[Backspace]** or **[Ctrl+C]**.

In the case when there is no session for the specified address, one will see the message like this:

```
MyEcoNAT:1:# show brasinfo 10.210.0.212
Bras info for address 10.210.0.212: not found
```

Show brasinfo command displays parameters see in a table below.

Table 34

Field	Description
Status	Client state
Maximum data rate upstream total	Upstream speed limit (to the Internet) for the abonent, in Kbps
Maximum data rate downstream total	Downstream speed limit (from the Internet) for the abonent, in Kbps
Bytes downstream total	Total received bytes number for the abonent
Bytes upstream total	Total transmitted bytes number for the abonent
Packets downstream total	Total received packets number for the abonent
Packets upstream total	Total transmitted packets number for the abonent
Session timeout expires in	Remaining time (in seconds) to the automatically finalizing the session. When the time expires the session wiil be deleted and a new one will be created

Field	Description
Idle timeout expires in	Remaining time (in seconds) to the automatically finalizing the session because of inactivity
Interim interval expires in	Remaining time (in seconds) to the finalizing of the accaunting inteerval
Services information	
Enabled/Disabled	The service in on/off
Maximum data rate upstream	Upstream speed limit (to the Internet) by the service, in Kbps
Maximum data rate downstream	Downstream speed limit (from the Internet) by the service, in Kbps
Bytes downstream	Received bytes number
Bytes upstream	Transmitted bytes number
Packets downstream	Received packets number
Packets upstream	Transmitted packets number

Use **show brasstate** command to check the state of the BRAS.

```
MyEcoNAT:2:# show brasstate
Default access: BLOCK
State      : ENABLED
```

This command shows two fields:

- **default access** – the default action,
- **state** – BRAS state (enabled/disabled).

Immediately after BRAS loading the mode of transmission of all traffic is switched on, in order to serve the users at the time, not yet loaded information from the billing (**default access** – **pass**). After loading the database BRAS switches to the main mode, when traffic is prohibited from those subscribers which is not allowed explicitly in the billing (**default access** – **block**).

To check the status of the contract, use the **show brascontract <ID>** command, where **ID** is the contract identifier. This command displays information on the contract itself and its subscribers: status, IP-addresses, speed, as well as statistics for the subscriber and general contract.

```
2:93:# show brascontract qq
Shared     192.168.55.6    Authorized      Bytes rx/tx: 7832582/115571751; Packets rx/tx: 45613/110596
Shared     192.168.55.7    Authorized      Bytes rx/tx: 7951843/99673922; Packets rx/tx: 47017/100025
Shared     192.168.55.5    Authorized      Bytes rx/tx: 7505493/95415626; Packets rx/tx: 40705/92433

============================ Shared Configuration ============================
Maximum data rate upstream total                                    1022 Kb/s
Maximum data rate downstream total                                  1022 Kb/s
Bytes recieved total                                              23289918
Bytes transmitted total                                          328286141
Packets recieved total                                              133335
Packets transmitted total                                           315275
```

Figure 14

For one abonent session reset one can use **clear brasinfo <IP-адрес>** command, for all EcoNAT abonents sessions reset one can use **clear brasinfo all** command.

```
MyEcoNAT:3:# clear brasinfo 10.210.30.4
Success
MyEcoNAT:4:# clear brasinfo all
Bras table purged
```

If accounting is configured when you run **clear brasinfo <IP-адрес>** command, at first the **accounting STOP** request will be sent to the server to close the session and then the session will be

removed at the EcoNAT. When you run **clear brasinfo all** command, the sessions recordings will be deleted only at the EcoNAT.

Use the **dropservices**, **droppolicies**, and **dropradius** commands to clean configuration items.

8.4 Policies and services

To limit the speed of transmission and reception of data and for redirection to a portal for subscriber account refilling in BRAS functionality are used policies and services. Service is a set of activities carried out in the case of certain conditions - the source or destination of session matchs to the specified ACL. Politics can combine multiple services together.

8.4.1 *Services*

To create a service, execute the command **create service <service name>**. When creating a service, its name is formed in the same way as described in the section "Pools and ACL".

After the service is created, it is necessary to go into the configuration mode of this service with **goto bras services <service name>** and set the parameters of its parameters using context commands.

The available service parameters are described in the table below.

Table 35

Parameter	Description
enable | disable	Enabled or disabled service
name	Service name
action	The action that the service performs: **pass** – traffic passes, but is subject to speed limits (default); **drop** – the traffic is discarded; block – redirects to the portal, for example, to replenish the account. The address of the portal is specified by the parameter **redirect_url**; redirect – used when the periodic redirection feature is enabled (see "Periodic forwarding setup"). When this action is specified, HTTP traffic is redirected (HTTPS passes). To work correctly in the parameters of the dpilist that is bound to this service, one must specify **redirect_use_interval on**
acl	The list of access by which packets fall into this service
redirect_url	The address to which the client will redirect if **action redirect** is used. Typically, here you specify the address of the portal of the telecom operator, where the client is redirected in case of need to replenish the account, you can also specify other resources. EcoSGE is capable to add some client specificators to the address string. It helps to personalize the redirection site. Used specificators: **%c** - send to redirect_url the callback-id received from the RADIUS server; **%m** - give to redirect_url the client MAC address; **%i** - give to redirect_url the client IP address; **%v1** - give to redirect_url the first (upper) client vlan tag; **%v2** - give to redirect_url the second (lower) client vlan tag; **%u** - give to redirect_url the URL which was addressed by the client. The **redirect_url** parameter format: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>=<SPEC2>..<VAR_NAMEN>=<SPECN>**

Parameter	Description
	where **URL** -redirection sites address, **VAR_NAME1** .. **VAR_NAMEN** - variable name, **SPEC1** .. **SPECN** - specificator. For example, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. In this case if client will try to address to **forbidden.com**, it will be redirected to: **http://example.com/?var1= forbidden.com&ip=10.1.1.10&qwe=0**
egress_speed	Maximum egress speed (Kb/s)
ingress_speed	Maximum ingress speed (Kb/s)
egress_tos	The value to be set in the **type of service** field in the outbound packet header is specified in decimal format. In order not to mark traffic, you need to leave the value: **nochange**
ingress_tos	The value that will be set in the **type of service** field in the header of the incoming packet is specified in decimal format. In order not to mark traffic, you need to leave the value: **nochange**
time_start daily HH:MM	Service start time. If you specify the value, this service is activated daily at the specified time. Time (UTC) is indicated in the format **HH:MM**, where **HH** is the hour, **MM** is the minute
time_end daily HH:MM	The end time of the service. If you specify the value, this service is turned off daily at the specified time. Time (UTC) is indicated in the format **HH:MM**, where **HH** is the hour, **MM** is the minute
always_pass	Dst IP addresses to which the rules of this service will not be applied
no_shape	External global IP addresses, for which speed is not limited. Here you can enter the IP addresses of game servers, IPTV servers and other resources that must be available to subscribers at maximum speed
dpilists	The number of the list of sites to implement the URL filtering is indicated (see section "URL Filtering functionality (DPI) "). If the site does not satisfy the list requirement, the **redirect_url** is redirected to the resource specified. The parameter is available only when the URL filtering module is installed

Example of creating and configuring the service:

```
MyEcoNAT:1:system.bras.services# create service 1
MyEcoNAT:2:system.bras.services# service1
MyEcoNAT:3:system.bras.services.service1# enable
MyEcoNAT:4:system.bras.services.service1# action redirect
MyEcoNAT:5:system.bras.services.service1# redirect_url
"http://redirect.domen.ru"
MyEcoNAT:6:system.bras.services.service1# egress_speed 56
MyEcoNAT:7:system.bras.services.service1# ingress_speed 56
MyEcoNAT:8:system.bras.services.service1# time_start daily 03:00
MyEcoNAT:9:system.bras.services.service1# time_end daily 21:00
MyEcoNAT:10:system.bras.services.service1# show
 enable
 name "service1"
 action redirect
 acl none
 redirect_url "http://redirect.domen.ru"
 egress_speed 56
 ingress_speed 56
 egress_tos nochange
 ingress_tos nochange
  time_start daily 03:00:00
  time_end daily 21:00:00
 always_pass ( )
```

```
no_shape ( )
dpilists ( )
```

To enable and disable the service, the context mode commands **enable** and **disable**, which must be run in the service branch.

```
MyEcoNAT:5:system.bras.services.service1# enable
MyEcoNAT:6:system.bars.services.service1# disable
```

*Edited configuration will be applied only after **apply** command .*

8.4.2 *Policies*

To create a policy, you must run the **create policy <policy name>** command. When creating a policy, its name is formed in a similar manner to that described in the section "Pools and ACL".

After you create a new policy, go to the configuration mode of the policy with **goto policy<policy name>** command and using the context commands to set the values of its parameters.

The available policy options are described in the table below.

Table 36

Parameter	Description
enable disable	Policy is enabled or disabled
priority	Priority of policies applying. The less value - higher priority. By default the first created policy has priority 100, the next one - 200, the third one - 300 and so on
local_ip ( )	Specify IPv4 addresses or subnets of clients binded with this policy
local_ip_v6 ( )	Specify IPv6 addresses or subnets of clients binded with this policy
type	Type may be one of the following: **static** – the services specified by policy configuration will be applyed for clients, **dynamic** – abonents authorization is performed via the RADIUS protocol (RADIUS server must be configured)
session_timeout	Time (in seconds) to the automatically finalizing the session. When the time expires the session wiil be deleted and a new one will be created. Default value 86400
idle_timeout	Time (in seconds) to the automatically finalizing the session because of inactivity. Default value 28800
interim_interval	Time (in seconds) to the finalizing of the accaunting inteerval. Is used with enabled Radius. Default value 15
ingress_auth	Allow (**on**) / deny (**off**) client authorization by the ingress packet with the client IP address in DST field. Is used only for the clients in static and fake pools
services ( )	Specifies the name of the service that is bound to the policy. You can specify up to 6 services using space as delimiter. The order defines the priority of services from the highest to the lowest. Parameters that can be set in the case of **type dynamic**, described in the section "RADIUS server settings"
Dynamic policy parameters	
auth	Authorization options. The name of the connection to the RADIUS server or group of RADIUS servers, or the keyword **none**
reauthorization_timeout	The time (in seconds) through which the client's authorization will be retried if there is no response from the RADIUS server (the BRAS client session is in the Error status). The default value is 180 seconds

Parameter	Description
acct	Accounting options. The name of the connection to the RADIUS server or group of RADIUS servers, or the keyword **none**

*ATTENTION! Before applying the changes, the value of the **auth** parameter should not be **none**, otherwise the **apply** command will end with an error.*

Example of creating and configurating policy:

```
MyEcoNAT:1:system.bras.policies# create policy 1
MyEcoNAT:2:system.bras.policies# policy1
MyEcoNAT:3:system.bras.policies# enable
MyEcoNAT:4:system.bras.policies# type static
MyEcoNAT:5:system.bras.policies# services service1
MyEcoNAT:6:system.bras.policies.policy1# show
MyEcoNAT:7:system.bras.policies.policy1#
  priority 100
  enable
  local_ip ( )
  local_ip_v6 ( )
  type static
  session_timeout 86400
  idle_timeout 28800
  interim_interval 15
  services (service1)
```

Use the context **enable** and **disable** commands in policies branch to turn the policy on or off.

```
MyEcoNAT:5:system.bras.policies.policy1# enable
MyEcoNAT:6:system.bras.policies.policy1# disable
```

*Edited configuration will be applied only after **apply** command .*

Configured policies will be processed in order of their priority. In addition, each policy can be assigned to multiple services. Then within the same policy services will be processed in the order in which they appear in the policies configuration.

8.5 RADIUS server settings

RADIUS settings are located in the **system.bras.radius** branch. The branch contains the following sections and parameters:

- **request_burst_interval** – the time interval in milliseconds between sending bursts of Access-Request and Accounting-Request packets. The range is 1 to 1000. The default is 10;
- **request_burst_size** – the maximum number of Access-Request and Accounting-Request packets in a burst. The range is 1 to 1000. The default is 64.
- **coa** – the section of RADIUS Change of Authorization parameters;
- **radius_groups** – the section of RADIUS server groups parameters;
- **radius_servers** – the section of RADIUS server connection parameters.

The structure and configuration commands of the above listed sections are described below.

8.5.1 *General settings for connecting to a RADIUS server*

To create a new connection to the RADIUS server, you must run the **create radius <connection name>** command. When creating a connection, its name is formed in the same way as described in the section "Pools and ACL".

After creating a new connection, you need to go to the appropriate branch of the configuration tree and use the context commands to set the values of its parameters.

The connection parameters for the RADIUS server are described in the table below.

Table 37

Parameter	Description
enable disable	Enabled or disabled access to the RADIUS server
server	IP address for authentication on the RADIUS server. By default: 0.0.0.0
acct_port	RADIUS server port for account
auth_port	RADIUS server port for authentication and authorization
acc_password	Password for authentication on the RADIUS server

An example of setting up a connection to a RADIUS server:

```
MyEcoNAT:1:system.bras.radius# create radius 1
MyEcoNAT:2:system.bras.radius# radius1
MyEcoNAT:3:system.bras.radius.radius_servers.radius1# enable
MyEcoNAT:4:system.bras.radius.radius_servers.radius1# server 192.168.5.1
MyEcoNAT:5:system.bras.radius.radius_servers.radius1# secret "econat"
MyEcoNAT:6:system.bras.radius.radius_servers.radius1# acct_port 1813
MyEcoNAT:7:system.bras.radius.radius_servers.radius1# auth_port 1812
MyEcoNAT:8:system.bras.radius.radius_servers.radius1# show
   enable
     server 192.168.5.1
     acct_port 1813
     auth_port 1812
     secret ""
```

To enable or disable access to the RADIUS server, use the context commands **enable** and **disable**, which must be started in the branch to the RADIUS server.

```
MyEcoNAT:5:system.bras.radius.radius_servers.radius1# enable
MyEcoNAT:6:system.bras.radius.radius_servers.radius1# disable
```

8.5.2 *Configuring Dynamic Policies*

When connecting to a RADIUS server, you must use dynamic policies. Such a policy is created and configured similarly to the static policy described in the section "Policies and services". Only a few parameters differ. Dynamic policy settings are listed in the table below.

Table 38

Parameter	Description
enable disable	Policy enabled or disabled
priority	Priority of applying policies. The lower the value, the higher the priority. By default, the first created policy has a priority of 100, the second has 200, the third has 300, and so on
local_ip local_ip_v6	Specify the addresses or subnets of clients to which this policy will apply
type dynamic	Enables RADIUS subscriber authorization

Parameter	Description
auth	Authorization options. The name of RADIUS servers group, or the keyword **none**
acct	Accounting options. The name of RADIUS servers group, or the keyword **none**
reauthorization_timeout	The time (in seconds) through which the client's authorization will be retried if there is no response from the RADIUS server (the BRAS client session is in the Error status). The default value is 180 seconds
session_timeout	The time (in seconds) during which a session exists, after the timer expires, the session is deleted. The default value is 86400 seconds. Note: after the specified interval has elapsed, a repeated Access-Request is sent (the RADIUS server can override the duration of this interval with the Session-Timeout parameter). The same thing happens for subscribers who have received an Access-Reject from a RADIUS server to attempt authorization
idle_timeout 28800	If there is no activity for a given period of time, the session will be interrupted. Specified in seconds. The default value is 28800 seconds
interim_interval	Interval of account (in seconds). Applicable with the Radius functionality enabled. The default value is 60 seconds
Binding services to the policy	
default	Service (or services), which is applied to a subscriber who has got into a policy but has not yet been authorized
if_auth_accept	A service (or services) that is applied to a subscriber who has received an Access-Accept from a RADIUS server
if_auth_reject	A service (or services) that is applied to a subscriber who has received an Access-Reject from a RADIUS server
if_auth_fail	Service (or services) that is applied to the subscriber, if the radius of the server has not responded to the Access-Request after the timeout

*ATTENTION! Before applying the changes, the value of the **auth** parameter should not be **none**, otherwise the **apply** command will end with an error.*

Example of creating and configuring a dynamic policy:

```
MyEcoNAT:1:system.bras.policies# create policy 2
MyEcoNAT:2:system.bras.policies# policy2
MyEcoNAT:3:system.bras.policies.policy2# enable
MyEcoNAT:4:system.bras.policies.policy2# local_ip (0.0.0.0/0)
MyEcoNAT:5:system.bras.policies.policy2# type dynamic
MyEcoNAT:6:system.bras.policies.policy2# auth radius1
MyEcoNAT:7:system.bras.policies.policy2# default (service5M)
MyEcoNAT:8:system.bras.policies.policy2# if_auth_accept (service1
service5M)
MyEcoNAT:9:system.bras.policies.policy2# if_auth_reject (service2)
MyEcoNAT:10:system.bras.policies.policy2# if_auth_fail (service2)
MyEcoNAT:11:system.bras.policies.policy2# show
MyEcoNAT:12:system.bras.policies.policy2#
   priority 200
   enable
   local_ip ( 0.0.0.0/0 )
   type dynamic
   auth radius1
   reauthorization_timeout 180
   session_timeout 86400
   idle_timeout 28800
   interim_interval 15
```

```
   default ( service5M )
   if_auth_accept ( service1 service5M )
   if_auth_reject ( service2 )
   if_auth_fail ( service2 )
```

8.5.3 *RADIUS Server Groups*

To increase reliability, RADIUS servers are combined into groups in which you can distribute the load between the servers and implement redundancy. BRAS dynamic policies specify groups rather than individual servers.

In the current implementation up to 16 RADIUS server groups. One RADIUS server can be included into several groups in the same time.

Use the **create radiusgroup <RADIUS_GROUP>** command to create RADIUS server group where <RADIUS_GROUP> is the group name.

By default, the configuration of the newly created group is as follows.

```
EcoNAT:8:system.bras.radius.radius_groups.radiusgroupb# ls
type active_standby
description ""
request_max 3
request_timeout 3
dead_time_min 15
dead_time_max 300
servers ( )
```

Use the **no radiusgroup <RADIUS_GROUP>** command in configuration mode to delete RADIUS server group where <RADIUS_GROUP> is the group name to be deleted. The **dropradius** command can also be used, as a result of which all groups and RADIUS servers will be deleted.

In the configuration mode of RADIUS server group operator can edit or delete group description, edit group mode, add the specific RADIUS server or delete it form the group.

Use the commands and parameters specified in the table below to configure RADIUS server group.

Table 39

Command/parameter	Description
description <TEXT>	Set RADIUS server group description where <TEXT> is the description string. Descriptions of radius groups containing spaces must be quoted
no description	Delete RADIUS server group description
type <MODE>	Set the RADIUS server group mode where <MODE> is the group operating mode. The allowed modes of RADIUS server group operating mode are the following: **active_standby** - the RADIUS server having highest priority in the group (the minimum value of the **priority** parameter) is used for all requests. This server is **active**, all others are in the **standby** mode. If the RADIUS server having highest priority in the group stops responding, the requests begin to arrive on the next highest priority server. After a certain period of time, the retry attempt sending requests to the highest priority server is made. If such an attempt is successful, then the server becomes active again;

Command/parameter	Description
	round_robin - requests are distributed among all RADIUS servers of the group. For example, if a group consists of 3 RADIUS servers, 5 requests from customers have come. The first request is sent to the 1st server, the second one to the second server, the third one to the third server, the fourth request to the 1st server, the fifth request to the second server, etc. The default value is **active_standby**
Timer Configuration	
request_max <NUMBER>	Number of requests after no response to which the server will be marked as unavailable (DEAD). Default value is 3
request_timeout <INTERVAL>	Time interval between request sending in seconds. Default value is 3
dead_time_min <MIN> dead_time_max <MAX>	Time interval in seconds during which the server will be unavailable (DEAD). The minimum <MIN> and the maximum <MAX> values can be specified. The default <MIN> value is 15 seconds, <MAX> - 300 seconds. The valid values of <MIN> and <MAX> are from 0 to 65535. The principle of using the **dead_time** timer After the RADIUS server previously marked as ACTIVE, has not responded to <NUMBER> requests (the **request_max** parameter), such server is marked as DEAD for the <MIN> period, and the router sending requests, redirects them to the backup RADIUS server inside the same group. At the end of this interval, the requests will be sent again to the inactive RADIUS server. If it responds successively, then it becomes ACTIVE again. If the RADIUS server does not respond it remains marked as DEAD. The interval for such its state will be increased by <MIN> (that is, after the first unsuccessful attempt, the interval is <MIN>, after the second one - 2*<MIN>, after the third - 3*<MIN>, etc.). This will continue until the interval of the DEAD mark reaches the <MAX> value. After that, attempts to access such a RADIUS server will be done once in the interval <MAX> until the first successful transition of the RADIUS server to the ACTIVE state. If <MAX> is not a multiple of <MIN>, the interval will become equal to <MAX> after its first exceeding as a result of increasing for the next <MIN>

RADIUS Servers Configuration in a Group (the servers parameter)

Servers are included in the group using the **add <server name>** command, symbolic '+=' command, or by space-separated listing of server names in brackets of the **servers ()** parameter.

Settings example:

```
2:2:# create radiusgroup 1
2:3:# create radius 1
2:4:# create radius 2
2:5:# create radius 3
2:6:# create radius 4
2:7:# go radiusgroup1
2:8:system.bras.radius.radius_groups.radiusgroup1# servers (radius1
radius2)
2:9:system.bras.radius.radius_groups.radiusgroup1# servers add radius3
2:10:system.bras.radius.radius_groups.radiusgroup1# servers += radius4
```

```
2:11:system.bras.radius.radius_groups.radiusgroup1# show servers
servers ( radius1 radius2 radius3 radius4 )
```

The order of the servers in the list matters! It determines the polling order of the servers. You cannot include a server in the group that has not yet been created.

To remove a RADIUS server from a group, use the symbolic '-=' command.

8.5.4 *Client authorization on the RADIUS server*

When authorizing a client on a RADIUS server, BRAS sends a RADIUS access request with the following information:

- User_Name: <user IP address>
- Calling-Station-Id: = <user MAC address>
- User-Password = <EcoBRAS hostname>

The User-Password attribute is used only to ensure compatibility with some billing systems. Since such systems are only required to have this attribute in Access-Request messages, its value is the same for all users. The value of the parameter User-Password is automatically used as the value of the **hostname** parameter from the branch of the configuration tree **system_log** (see section "Logging"). At authorization values of this attribute are not used.

When Access-Accept is received from the RADIUS server, the user is assigned the service specified in the parameter if_auth_accept and the corresponding speed limits. The user session is controlled by the timeouts specified in the parameters: session_timeout, idle_timeout, interim_interval. However, if Access-Accept from the RADIUS server contains additional attributes with services, then they are automatically applied to the subscriber, in spite of the settings of BRAS policies and services.

BRAS processes the following attributes contained in RADIUS24:

- Cisco-Account-Info – Upload and Download speed limit in bps;
- Cisco-Service-Info – forced assignment of a service configured for BRAS. In this case, the service name is specified in the form: **A <service name>**;
- Callback-Id is a unique identifier of the user, which is substituted into **redirect_url** through the qualifier **% c **;
- Idle-Timeout;
- Session-Timeout;
- Acct-Interim-Interval;
- Framed-IP-Address.

Example:

- Cisco-Account-Info := "Pqq0",
- Cisco-Account-Info := "VU;20000000;D;20000000",
- Delegated-IPv6-Prefix := "::1:1900:0:0/125"
- Callback-Id := "c6958059a295af355e5b8dfbbfcf4fd4",
- Idle-Timeout := 500,
- Session-Timeout := 500,

- Acct-Interim-Interval :=500.

8.5.5 *Counters*

To view counters by RADIUS, use the **show counters all | include radius** command.

```
MyEcoNAT:7:# show counters all | include radius
Printing counters...
```

The table below describes the existing counters in this section.

Table 40

Counter	Description
radius_authorization_success	The number of packets accepted with Access_Response with **Accept** status
radius_authorization_reject	Number of packets received with Access_Response with **Reject** status
radius_authorization_bad_response	Number of packets received by Access_Response due to problems with EcoNAT and RADIUS server settings (for example, a mismatched password)
radius_authorization_error	Number of packets sent by Access_Request with problems other than those described above
radius_accounting_send_try	Number of attempts to perform RADIUS accounting of user
radius_accounting_success	The number of received Accounting_Response packets
radius_accounting_reject	Number of **reject** responses when sending/receiving RADIUS packets
radius_accounting_error	Number of **error** responses when sending/receiving RADIUS packets
radius_accounting_bad_response	Number of **bad_response** responses when sending/receiving RADIUS packets
radius_accounting_default_handler	Number of accounting requests via RADIUS with problems other than those described above
radius_accounting_session_timeout	Number of **session_timeout** operations
radius_accounting_idle_timeout	Number of **idle_timeout** operations
radius_coa_get_packet	Number of received packets on the EcoNAT CoA port
radius_coa_bad_packet	The number of packets received on the CoA port that are unsuitable for processing
radius_coa_no_entry	The number of packets received on the CoA port for which we did not find the abonent
radius_coa_request	The number of packets of type **coa_request** received on the CoA port
radius_coa_ack	The number of **coa_request** packets for which a **coa_ack** packet was sent
radius_coa_nak	The number of **coa_request** packets for which a **coa_nak** packet was sent
radius_coa_disconnect_request	The number of packets received on the CoA port type **coa_disconnect_request**
radius_coa_disconnect_ack	The number of packets of type **coa_disconnect_request** for which a packet of type **coa_disconnect_ack** was sent
radius_coa_disconnect_nak	The number of packets of type **coa_disconnect_request** for which a packet of type **coa_disconnect_nak** was sent

8.6 Creating a BRAS session using DHCP packages

EcoBRAS has the ability to initiate BRAS sessions over DHCP packets. This function is available on request, software update is required.

Let's consider the working principle of this mechanism using the example shown in the figure below.

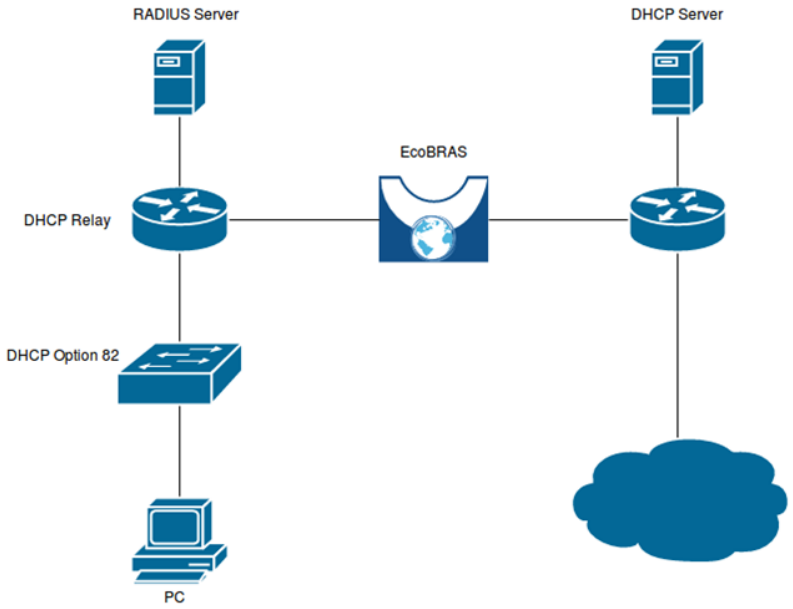

Figure 15

For this mechanism to work, it is necessary that through Unicast DHCP packets from DHCP Relay to DHCP Server pass through EcoBRAS. In this case, the IP address of the DHCP Relay must fall into the pool on EcoBRAS and should not fall into any policy.

When a subscriber requests settings from a DHCP server, EcoBRAS from the DHCP ACK receives the following data: IP address, MAC address, Option 82 (if present). Based on this data, a BRAS session is initiated and an authentication request is sent to the RADIUS server. When **Access-Request** is sent to the **User-Name** field, the subscriber's MAC address is substituted, and in the **Calling-Station-ID** IP address field. If Option 82 was present in the DHCP packet, then additional attributes are added to the **Access-Request**:

```
AVP: l=14 t=Vendor-Specific(26) v=Ericsson, Inc. (formerly 'RedBack
Networks')(2352)
  AVP Type: 26
  AVP Length: 14
  VSA: l=8 t=Agent-Remote-Id(96): \000\006\240\253\033O
AVP: l=10 t=Vendor-Specific(26) v=Ericsson, Inc. (formerly 'RedBack
Networks')(2352)
  AVP Type: 26
   AVP Length: 10
  VSA: l=4 t=Agent-Circuit-Id(97): \000\004
```

When sending a **DHCP Release** message from the client, EcoBRAS removes the BRAS session for this client by sending **Accounting-Stop** to the RADIUS server.

8.7 Shared contracts

Within one contract, the work of several users with the common maximum bandwidth can be organized (the shared contract). In this case, personal settings for the bandwidth limitation are taken into account if they are less than the common maximum bandwidth. In one contract there can be subscribers with a common bandwidth and with an individual.

```
EcoNAT:3:#show brascontract 17
 Shared   192.168.55.5  Authorized  Bytes rx/tx: 0/0; Packets rx/tx: 0/0
 Shared   192.168.55.6  Authorized  Bytes rx/tx: 0/0; Packets rx/tx: 0/0
 Not shared 192.168.55.7  Authorized  Bytes rx/tx: 0/0; Packets rx/tx:
0/0
```

When using the maximum bandwidth of the channel, the speed between the contract participants is distributed in proportion to their activity.

Adding a shared contract entry is possible using the RADIUS protocol or the proprietary EcoBRAS protocol, depending on the version and license of the firmware.

The configuration of the entry for the client on the RADIUS server should be similar to the following (for example, the record is for freeRADIUS).

```
192.168.55.5   Auth-Type := Accept
        Cisco-Account-Info := "QU;5000000;D;5000000",
        Cisco-Account-Info += "P12345678",
        Cisco-Account-Info += "VU;8000000;D;8000000",
```

Where:

P12345678 - contract identifier in the format P<contract identifier>. A combination of numbers, capital and lowercase Latin letters may be used as an identifier for a contract;

QU / QD - speed limit of this client;

VU / VD - speed limit of the general contract.

In the event that a client with individual bandwidth restrictions is launched, the last attribute is missing. Such a client can be included in the contract with the general bandwidth settings.

For the CoA request, the following parameters should also appear:

```
Cisco-Account-Info := \"P12345678\", Cisco-Account-Info :=
\"VU;2012000;D;2012000\"
```

With the help of the EcoBRAS protocol, the addition of clients of the general contract is carried out by the **ads** command (see Billing console and EcoBRAS protocol).

One must repeatedly specify the speed limit of the general contract when adding a new subscriber who is included in the general contract, because the value specified at the previous addition will be replaced.

9 URL Filtering functionality (DPI)

This functionality is available with EcoDPIxxxx-LIC license (how to view the license, see "Getting help).

URL Filtering (DPI) functionality allows service providers to filter unwanted and prohibited resources on the Internet, and also provide services such as "Child Online" with filtering for large lists. This functionality meets all requirements and has been tested by Roskomnadzor (the official conclusion is available at http://www.rkn.gov.ru/docs/Izobrazhenie_29.09.2017.tiff).

Subscriber redirection to the blocking page ("resource is prohibited") is set individually for each list. Supports subnet filtering.

In case of HTTPS supports filtering SNI (Server Name Indication) to break the connection with the forbidden resource. In there is no SNI field in the query, the request is passed transparently. It checks incoming server certificate on which the request was sent. If there is URL denied by filters in the certificate, the connection to the server is dropped.

The main list of banned sites – a register of Russian Roskomnadzor (it has a predefined name **dpilist0** in **system dpi** configuration space).

It also supports up to 16 user-defined lists of sites (**dpilist1** ... **dpilist16**), each of which can be either black (list of banned sites) or white (the list of allowed sites).

The format of the uploaded lists: a text file with list of URL beginning with “http://” or “https://” in which the port number may be setted. Also in the URL entry, the '*****' character can be used to specify any character set, for example, to filter multiple mirror sites. If you want to filter both HTTP and HTTPS, then '*****' is placed at the beginning of the URL, if only one of the protocols, then “http://” or “https://” is prefixed before '*****'. In the lists, IP addresses, subnets or ranges of addresses (via a hyphen) can be specified. The delimiter is CR or CR LF (the end of the line and the newline). The name and file extension are not regulated.

Dpilists are allowed to use comments. For example, to logically split IP addresses into groups by Internet service provider area. Each comment line must begin with the pound sign '#'. In addition, with the same character, if necessary, you can “comment out” certain lines in the list, and they will not be processed when building or updating the database.

File example:

```
http://citybus.nnov.ru:8080/login.php
https://maps.yandex.ru/213/moscow/?source=tableau_maps
http://flibusta.net
https://hh.ru
http://hh.ru
http://*.example.ru
*.badsite.ru
http://vk.com
en.wikipedia.org/wiki/Ethernet
8.8.8.0/24
3.3.3.1
# District
5.5.5.5-5.5.5.150
```

If the URL in the uploaded list is presented without the prefix "http: //" or "https: //", then the default is believed that he also figures in the list with the prefix "http: //", and "https: //". Thus, a filter for HTTPS connections will only respond to the specified domain name. That is, with the above example, writing in reference to the Wikipedia article, will close all connections, attempting to gain access to English Wikipedia. Thus, if you want to close access to only one article, in the list should be " http://en.wikipedia.org/wiki/Ethernet ".

A subscriber may be filtered according to several lists. In the case of triggering multiple lists at the same time, the action will be in accordance with the most priority of them (those which has the lower number).

Blacklist – is a list of banned sites. Triggered by it means the prohibition of access to the page. In this case, the HTTP connection will be redirected to the page specified in the configuration, and the HTTPS connection will be closed by RST.

White list contains the contrary permitted sites. Triggered by it means permission to access this page. The absence of events on the white list means that access is denied by default (and there will be redirect or closure), but the user can be subscribed to multiple white lists simultaneously, in this case, to access the page is enough to load at least one of them.

9.1 URL Filtering configuration

The settings of the URL filtering functional (DPI) are stored in the **system.dpi** branch of the configuration tree. This branch contains general system settings for URL filtering and websites lists settings, which in the EcoSGE concept are called **dpilistN**, where **N** is a sequence number from 0 to 16.

```
EcoSGE:# go dpi
EcoSGE:system.dpi# ls
enable
functionality_mode normal_nat
revisors ( )
dpilist0
{
 enable
 rkn_source rkn
 rkn_login "0123456789"
 rkn_password "q1w2e3r4t5y6u7i8o9p0"
 rkn_proxy ""
 upload_dump_server ""
 whitelist_mode off
 log_matches off
 log_pictures off
 exceptions off
 behaviour block
 redirect_use_interval off
 redirect_interval 600
 redirect_interval_url 2592000
 redirect_url "http://www.provider.ru/blocked/block0.html"
 color_direction both
 color_tos_byte 32
 download_url "http://192.168.10.1/dump.xml"
```

```
 update_schedule interval 600
 protocols ( )
 no_ip ( 10.210.0.123~0-4095 )
 no_ip_remote ( )
 ip (
   10.0.0.0/8~1-10
   61.216.14.0/23~0-4095
 )
 no_ipv6 ( )
 ipv6 ( )
}
dpilist1
{
 disable
 whitelist_mode off
 log_matches off
 log_pictures off
 exceptions off
 behaviour block
 redirect_use_interval off
 redirect_interval 600
 redirect_interval_url 2592000
 redirect_url http://www.provider.ru/blocked/block1.html
 color_direction both
 color_tos_byte 32
 download_url http://www.provider.ru/blacklists/list1.txt
 update_schedule never
 protocols ( )
 no_ip ( )
 no_ip_remote ( )
 ip ( )
 no_ipv6 ( )
 ipv6 ( )
}…
```

To enable or disable URL filtering functionality use **enable** and **disable** contextual command of the **system.dpi** branch of the configuration tree.

In addition, each of the lists may be individually enabled/disabled with the **enable** and **disable** command, running in the configuration space of the list.

EcoSGE can operate in two modes:

- standard NAT, standing "in the gap" connection (the first figure below),
- and dual-mirroring traffic mode (the second figure below).

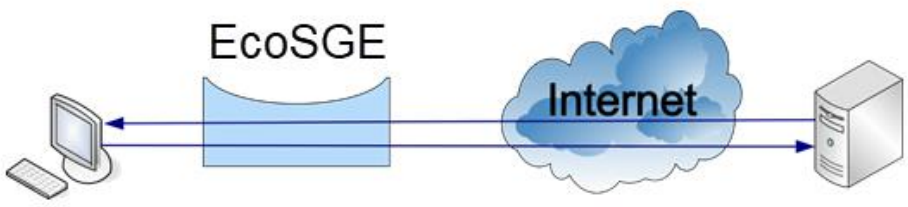

Figure 16

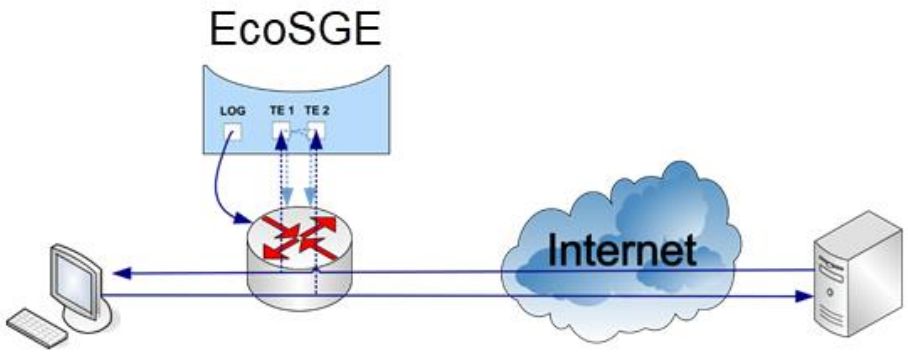

Figure 17

Modes of EcoSGE operation are switched with parameter **functionality_mode**, which may have values, respectively, **normal_nat** and **double_mirrored_traffic**. To switch between these modes you should run the command **functionality_mode normal_nat** or **functionality_mode double_mirrored_traffic** in the **system.dpi** configuration branch.

In mirroring mode EcoSGE listens to incoming and outgoing traffic, carrying out its translation, as in the normal mode. While outbound subscriber traffic is being mirrored on a local (even) EcoSGE interfaces, and the incoming from the Internet to subscribers – at the global (odd) EcoSGE interfaces (see more in "Getting help" paragraph). If EcoSGE detects the connection with the prohibited resource, it sends through a router, the interrupting connection packet (for HTTPS) or redirecting packet (for HTTP). To send redirection or interrupting connection packet EcoSGE uses log interface or interfaces (see more in "Hardware" paragraph), while normally the same network interfaces to which subscribers are connected used for this. Therefore, for the correct operation of the mirroring scheme the default gateway address in the **connection_log** context must be configured in EcoSGE (see more in "Logging" paragraph). It is also recommended to take steps to prevent the duplicated traffic back to the network through the interface from which mirrored traffic is sent to the EcoSGE.

If traffic with a tag (or double tag) is mirrored to EcoSGE, in this case the redirect packets, and the interruption of the connection packets are encapsulated accordingly. Therefore, it is necessary to provide L2 connectivity EcoSGE logged interface and the router interface (IP-address specified as the default gateway in the **connection_log** context). In this case, you can configure EcoSGE in such a way that untagged traffic will be sent from the logging interface. To do this, you must configure the value **on** of the **strip_tags** parameter in the **connection_log** branch of the configuration tree.

Parameters for the lists of sites is in a table below.

Table 41

Parameter	Description
enable or disable	Determines the activity of this list
whitelist_mode	Determines whether the white or black list. Blacklist (parameter value - **off**) shows the sites which is denied for visiting. White list (parameter value - **on**) shows the sites which allowed for visiting (it is used for "children's Internet" for example). **ATTENTION! If you use the whitelist, you can completely block access (see the explanation at the bottom of the table)**
log_matches	Specifies logging enabling of prohibited sites visiting on the server

Parameter	Description
log_pictures	Determines whether the logging of images on the site is enabled. The following formats are considered: * .bmp, * .gif, * .jpeg, * .jpg, * .png, * .tif, * .tiff
exceptions	Applies the list of exceptions to this **dpilist**. Possible values: **on**, **off**
behaviour	Determines what action will be taken when the condition is met the given list (for black or not triggered for white list): **block** - block HTTPS and redirect HTTP , **redirect** - redirect HTTP and pass HTTPS, **color** - coloring, **ignore** - all pass
redirect_use_interval	Enables redirection timers. If you turn off this setting, redirection will be triggered every time you try to access any site from the list. Possible values: **on**, **off**
redirect_interval	The interval between the redirection for the sites in the list (seconds). Default 10 minutes (600). After the first redirecting all other sites from the list will be opened within 10 min in the normal mode
redirect_interval_url	The interval between the redirections of the same page. By default, 30 days (2592000). When you try to visit the page from the list the redirection is triggered. After that, this page will be opened in the normal mode for 30 days, then redirection will occur
redirect_url	URL, where will be redirected the HTTP connection if the condition list triggered (for the black list) or didn't triggered (for the white list). EcoSGE is capable to add some client specificators to the address string. It helps to personalize the redirection site. Used specificators: **%c** - send to redirect_url the callback-id received from the RADIUS server; **%m** - give to redirect_url the client MAC address; **%i** - give to redirect_url the client IP address; **%v1** - give to redirect_url the first (upper) client vlan tag; **%v2** - give to redirect_url the second (lower) client vlan tag; **%u** - give to redirect_url the URL which was addressed by the client. The **redirect_url** parameter format: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>=<SPEC2>..<VAR_NAMEN>=<SPECN>** where **URL** -redirection sites address, **VAR_NAME1** .. **VAR_NAMEN** - variable name, **SPEC1** .. **SPECN** - specificator. For example, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. In this case if client will try to address to **forbidden.com**, it will be redirected to: **http://example.com/?var1= forbidden.com&ip=10.1.1.10&qwe=0**
color_direction	Marked direction of traffic: **egress** - the traffic from the user to the Internet is marked; **ingress** - the traffic from the Internet to the user is marked; **both** - the traffic is marked in both directions; **no** - the traffic is not marked
color_tos_byte	The value that will be set in the **type of service** field in the packet header is specified in decimal format
download_url	URL where the list will be uploaded in the case of auto-update (HTTP, FTP, TFTP protocols are supported). For **dpilist0** - the address where will be preuploaded list
update_schedule	Schedule, by which a list will be uploaded. Possible formats schedules: **never** – will never be uploaded, **interval <SECONDS>** – the number of seconds between auto-updates.

Parameter	Description
	It is recommended to put a value not less than 1 hour (3600 seconds). It is highly not recommended to set the value less than 5 minutes (300 seconds)
protocols	A list of protocols to be blocked. To specify multiple protocols, use space as delimiter.
no_ip	A list of IPv4 addresses that are excluded from the list of actions (**no_ip** parameter is processed earlier than the **ip**)
no_ip_remote	
ip	A list of IPv4 addresses that appear to be under influence of the list
no_ipv6	A list of IPv6 addresses that are excluded from the list of actions (**no_ipv6** parameter is processed earlier than the **ipv6**)
ipv6	A list of IPv6 addresses that appear to be under influence of the list. In order to specify the processing of all addresses, you must specify: **::/0**

ATTENTION!

If you use the whitelist, you can occasionally block all access!

If you set the whitelist mode on parameter and add at least one IP address to the list (for example, 127.0.0.1), all IP addresses other than 127.0.0.1 will be blocked for clients specified in the dpilist configuration.

The whitelist can contain only IP addresses, only URLs or IP addresses and URLs.

If there are IP addresses and URLs in the list, then for each URL there must be a corresponding IP-address (addresses) to which it will be converted.

If there are only URLs in dpilist, you do not need to assign IP addresses.

If the address falls within the range specified in the value of the **ipv6** parameter, the corresponding subscriber sessions are created. The status of these sessions can be checked using the **show sessions local any** command.

```
EcoSGE:system.dpi# show sessions local any
ipv6 egress UDP [2001:DB8:3333:4::5]:58712-[2001:DB8:3333:4::10]:33435;
Last packet 6.10 seconds ago; To be deleted in 293.90 seconds of
inactivity.
ipv6 ingress UDP [2001:DB8:3333:4::5]:33435-[2001:DB8:3333:4::10]:63607;
Last packet 37.46 seconds ago; To be deleted in 262.54 seconds of
inactivity.
```

For IPv6 diagnostics, a number of counters are used, as shown in the table below.

Table 42

Counter	Description
cr_ipv6_table_entries	Number of entries in the IPv6 session table
cr_ipv6_established_sessions	Total number of IPv6 sessions installed
cr_ipv6_egress_packets	Number of IPv6 packets in the egress direction
cr_ipv6_ingress_packets	Number of IPv6 packets in the ingress direction
cr_ipv6_egress_bytes	The number of bytes sent in the egress direction using the IPv6 protocol
cr_ipv6_ingress_bytes	The number of bytes sent in the ingress direction using the IPv6 protocol

9.2 Manual loading lists of sites for URL filtering

Manual loading is possible for lists with numbers from 1 to 16 (the list with the number 0 is reserved for the Russian Roskomnadzor registry). To manually upload the lists, use the **dpiload <list number> <URL>** command, where the address is entered in the **http://<server address>/<file name>.<file extension>** format (see more in "URL Filtering functionality (DPI) " paragraph).

The basic authentication for the target server and FTP-server is supported for uploading the lists. Syntax of loading commands using the authentication

dpiload <list number> http://<username>:<password>@<server address>/<filename>

dpiload <list number> ftp://<username>:<password>@<server address>/<filename>.

For example, if in order to upload ***black_list.txt*** list from the ***1.1.1.1*** http-server corresponding to the list **1** in the system is required to enter the http-server with the ***username*** name with the ***password*** password, then use the following command:

```
MyEcoNAT:1:system.dpi# dpiload 1
http://username:password@1.1.1.1/black_list.txt
```

To perform similar actions on the FTP server, then use the following command:

```
MyEcoNAT:2:system.dpi# dpiload 1
ftp://username:password@1.1.1.1/black_list.txt
```

First it is recommended to disable the automatic list update, by setting the **update_schedule** parameter to the value **never**.

When entering the **dpiload 0** command you are initiating the registry update from the Roskomnadzor server. If the **download_url** parameter is specified in the **dpilist0** list settings, and the Roskomnadzor site is not directly accessible to EcoNAT, the download will be performed from the specified in the **download_url** parameter address.

Example:

```
MyEcoNAT:2:system.dpi# dpiload 0
list0 will be updated soon
MyEcoNAT:3:system.dpi# dpiload 0
http://username:password@1.1.1.1/dump.xml
http://username:password@1.1.1.1/dump.xml to dump.xml: saved
MyEcoNAT:4:system.dpi# dpiload 0
ftp://username:password@1.1.1.1/dump.xml
ftp://username:password@1.1.1.1/dump.xml to dump.xml: saved
```

At first we recommend that you upload the list with the **dpiload** command, then enable the list in the **system dpi dpilist<number>** configuration space and configure other parameters.

The modified configuration is applied only after executing the **apply** command.

To view the dpilists and URL filtering files, use the **dpilist** command (see the "List management commands" section).

9.3 Automatically download lists on schedule

To automatically upload a list on the schedule you must **enable** the list, and the **update_schedule** parameter value must be different from never.

9.4 Updating sites base

All loaded and enabled lists are merged inside EcoNAT into a single URL database. With automatic lists loading the database update occurs immediately. In the case of manual lists loading you have to force start the process of updating the database using **dpirun** command.

9.5 Configuring URL Filtering for addresses that do not fall under the NAT

By default, the device performs URL filtering only for those IP subscribers that are included in any of the NAT pools (their IP addresses fall under to pool ACL).

In the case that some range of IP addresses of subscribers are not faced to NAT (e.g., routable to Internet the "real" addresses of subscribers, for example, from the network 194.85.16.0/24), for performing URL filtering, you have to make the following steps:

Create a new NAT pool.

```
MyEcoNAT:1:# create pool poolurl
```

To set **fake** type to the pool.

```
MyEcoNAT:2:# edit poolurl
MyEcoNAT:3:pools.poolurl# type fake
```

To set minimum priority to **poolurl** pool.

```
MyEcoNAT:4:pools.poolurl# priority 10000
```

Create an ACL.

```
MyEcoNAT:6:pools.poolurl# create acl aclurl
```

To enter rules in **aclurl**.

```
MyEcoNAT:7:pools.poolurl# use aclurl poolurl
MyEcoNAT:8:pools.poolurl# edit aclurl
MyEcoNAT:9:acls.aclurl# 10 allow ip 194.85.16.0/24 any
```

To apply a configuraion.

```
MyEcoNAT:9:acls.aclurl# apply
APPLY CONFIGURATION IS DIFFER, PROCESS APPLY
…
     }
     pools
     {
      poolurl
      {
       # pool is valid and will be activated during apply
        type fake
        enable
        acl aclurl
        priority 10000
        connection_logging on
```

```
      }
     }
     acls
     {
       aclurl {
        10 permit ip src net 194.85.16.0/24 dst any
       }
     }
RECONFIG FUNCTION PROCESSING
EconatEngineReconfig output success
APPLY SUCCESS
Save applied configuration into profile 'lastapply'
```

For this pool, it is recommended to set the minimum priority, i.e., the value of the priority parameter must be greater than all the other NAT pools (the smaller the priority value, the higher the priority). Thus, this pool will handle the traffic that is not handled by the other NAT pools.

Fake pool allows logging of connections with the relevant IP addresses for the Syslog and Netflow protocols.

9.6 List management commands

To remove lists or files that are used when setting up the URL filtering, use the **dpierase <list number or file name>** command.

To view the uploaded URL lists and DPI configuration files use **dpilist** command.

```
MyEcoNAT:1:> dpilist
     0 Thu Feb 11 13:57:50 2016 list0.dpi
     36 Mon Jan 25 10:41:37 2016 list1.dpi
     15 Tue Jan 12 15:42:28 2016 list16.dpi
     83 Thu Nov  5 10:45:39 2015 list2.dpi
     37 Thu Oct 29 14:28:31 2015 list4.dpi
     4 Thu Oct 29 13:58:27 2015 list7.dpi
     31 Thu Oct 29 13:01:43 2015 list8.dpi
     31 Thu Oct 29 12:38:15 2015 list9.dpi
     10 Mon Feb  1 14:24:22 2016 request.xml
    3.0K Tue Dec 15 14:39:08 2015 request.xml.sig
```

Use show **dpirecords** and **dpiview** commands in the EcoNAT interface to view the URL filtering lists content.

9.6.1 *Show dpirecords*

The command displays entries from the URL list.

Syntax of the command: **show dpirecords <list number> | [filters]**.

Filters, similar to the other show commands are available for this command.

Table 43

Filter	Description
| b STRING | begin STRING	Drops out a string until it reaches a line containing the specified substring

Filter	Description
| count	It counts the number of rows
| e STRING | exclude STRING	Prints only lines not containing the specified substring
| drop NUM	Пропускает указанное количество строк
| i STRING | include STRING	Prints only lines containing the specified string (If substring contains spaces or special characters such as ')', then you can use the quotation marks)
| more	Outputs with a stop after each page
| r STRING | regexp STRING	Displays only the lines that match the specified regular expression
| take NUM	Output the specified number of strings

Command output example:

```
MyEcoNAT:2:# show dpirecords 1
https://issuu.com
http://www.ya.ru
http://www.lenta.ru
http://www.rg.ru
MyEcoNAT:2:# show dpirecords 1 | include ya
http://www.ya.ru
```

9.6.2 *Dpiview*

The command displays the records of URL filtering list or the contents of files that are used to configure URL filtering. Command syntax: **dpiview <list number or filename>**.

For this command, there is no possibility of filtration, batch output or interruption of output. As a command parameter, you may specify not only the number of a specific list, but the following files:

- cert – display the contents of the certificate file,
- dump – display the contents of a file of the Roskomnadzor registry,
- request – show the contents of the certificate request file,
- sign – to show a signed certificate request file,

and other files (e.g., shortlist, exceptions), if they exist.

Command output example:

```
MyEcoNAT:3:# dpiview request
<?xml version="1.0" encoding="windows-1251"?>
<request>
<requestTime>2015-12-09T13:35:52+03:00</requestTime>
<operatorName>ABC.COM</operatorName>
<inn>1111111111</inn>
<ogrn>1111111111111</ogrn>
<email>mail@domen.ru</email>
</request>
```

9.6.3 *Show dpistate*

This command displays diagnostic information on the URL filtering functionality.

Output example:

```
EcoSGE:# show dpistate
IPv4 firewall table rules 326812/1048576 used/max
IPv6 firewall table rules 13/1048576 used/max
IPv6 firewall range table rules 0/1048576 used/max
Dump partition: 154746880/159825920/314572800 used/free/total
DPI rules size: 31733149/35679961 url/all
Summary dump size:73804291
URL base rebuild at: 2019-10-11T10:37:00+03:00
Last dump download: 2019-10-11T07:29:00+03:00
Actual Date for delta: 2019-10-11T11:25:00+03:00
DPI host  buffers used/total: 7/65535 (0.0%)
DPI path  buffers used/total: 7/65535 (0.0%)
DPI state buffers used/total: 161/16777215 (0.0%)
```

The output strings are described in the table below.

Table 44

Строка	Описание
IPv4 firewall table rules	Current/maximum number of IPv4 rules in the ACL
IPv6 firewall table rules	Current/maximum number of single IPv6 addresses in the ACL
IPv6 firewall range table rules	Current/maximum number IPv6 addresses bands in the ACL
Dump partition	Using the volume of the disk partition allocated for storing the downloaded list of the local regulations, its differential updates, as well as temporary files generated during its processing
DPI rules size	Memory size used by URL filtering structures without ACL/total (in bytes)
Summary dump size	The total size of the downloaded list of of the local regulations and its differential updates (in bytes)
URL base rebuild at	
Last dump download	Date and time of the last successful download of the local regulations list or its differential update in the format **YYYY-MM-DD T HH: MM: SS time_offset**
Actual Date for delta	
DPI host buffers used/total	The domain name information filling buffer counter (current/maximum)
DPI path buffers used/total	The information from the URL after the '?' symbol filling buffer counter (current/maximum)
DPI state buffers used/total	Session filling buffer counter (current/maximum)

9.7 Exceptions setup

If necessary, you can configure the exceptions for lists.

To add an exception, you have to create a text file with a list of exception addresses, in the same way as described in section "URL Filtering functionality (DPI) ". Then the file is uploaded manually with the **dpiload exception <URL>** command, where the address is in **http://<server address>/<file name>.<file extension>** format. Next, you need to include an exception for a specific sites list to which they will apply, setting **exceptions on** value of list parameter. Addresses from the

list of exceptions will be prohibited if the exceptions applied to the white list, or allowed, if exceptions apply to the black list.

In a URL entry in the exception list, the * character can be used to specify any character set, for example, to filter multiple mirror sites. If you want to filter both HTTP and HTTPS, then * is placed at the beginning of the URL, if only one of the protocols, then * is prefixed before *.

Example of list parameters configuration:

```
MyEcoNAT:1:system.dpi.dpilist1# show
enable
whitelist_mode off
log_matches on
exceptions on
behaviour ignore
redirect_use_interval off
redirect_interval 600
redirect_interval_url 2592000
redirect_url "http://redirect.domen.ru/"
color_direction both
color_tos_byte 32
download_url ""
update_schedule never
no_ip ( )
ip ( 0.0.0.0/0 )
```

9.8 Periodic forwarding setup

The function of URL filtering of EcoNAT equipment allows for periodic redirection of users from certain websites (for example, competitors' websites) by a timer.

Periodic redirect configuration works only for HTTP. In the case of the use of HTTPS, the connection will be established without redirections.

To configure periodic redirects, in the **dpilist** must be manually loaded a list of sites for which you want to implement a redirection (see more in "" paragraph).

Next, you have to configure the list parameters, including redirection timers and the address to which the user will be redirected, for example, this might be the service provider’s page with a description of the services and special offers.

The redirection mechanism is activated automatically when the user first visits any page from the list. Countdown timers starts with this point. One of the timers (**redirect_interval**) counts down the time until the next redirect for all other URLs from the list, the second counts time before next redirection by the first triggered address occur (redirect_interval_url).

For example, if the list of addresses is uploaded:

- ya.ru
- lenta.ru
- rg.ru

For the list set:

- redirect_interval – day,
- redirect_interval_url – 10 minutes.

The user enters the rg.ru, and it immediately redirects to the provider's page. After that, he may visit rg.ru during the day, after that again will be redirection. At the same time, the remaining sites in the list are free to visit within 10 minutes. After that, it comes, for example, to ya.ru and it redirected again to the provider's page. Twenty-four hours after that ya.ru opens in normal mode, then again there is a redirection.

The parameters that should be configured for periodic redirects are presented in the table below.

Table 45

Parameter	Description
system dpi dpilist<NUMBER>	
redirect_interval	The interval between the redirection for the sites in the list (seconds). Default 10 minutes (600). After the first redirecting all other sites from the list will be opened within 10 min in the normal mode
redirect_interval_url	The interval between the redirections of the same page. By default, 30 days (2592000). When you try to visit the page from the list the redirection is triggered. After that, this page will be opened in the normal mode for 30 days, then redirection will occur
behaviour redirect	Specifies the behavior of the list
redirect_use_interval on	Enables redirection timers. If you turn off this setting, redirection will be triggered every time you try to access any site from the list
redirect_url	The address of the page which user will be redirected. EcoSGE is capable to add some client specificators to the address string. It helps to personalize the redirection site. Used specificators: **%c** - send to redirect_url the callback-id received from the RADIUS server; **%m** - give to redirect_url the client MAC address; **%i** - give to redirect_url the client IP address; **%v1** - give to redirect_url the first (upper) client vlan tag; **%v2** - give to redirect_url the second (lower) client vlan tag; **%u** - give to redirect_url the URL which was addressed by the client. The **redirect_url** parameter format: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>= <SPEC2>..<VAR_NAMEN>=<SPECN>** where **URL** -redirection sites address, **VAR_NAME1** .. **VAR_NAMEN** - variable name, **SPEC1** .. **SPECN** - specificator. For example, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. In this case if client will try to address to **forbidden.com**, it will be redirected to: **http://example.com/?var1= forbidden.com&ip=10.1.1.10&qwe=0**

List configuration example:

```
MyEcoNAT:2:system.dpi# show
enable
functionality_mode normal_nat
certificate_file "cert.pem"
…
dpilist1
{
```

```
 enable
 whitelist_mode off
 log_matches on
 exceptions off
 behaviour redirect
 redirect_use_interval on
 redirect_interval 600
 redirect_interval_url 2592000
 redirect_url "http://redirect.domen.ru/"
 color_direction both
 color_tos_byte 32
 download_url ""
 update_schedule never
 no_ip ( )
 ip ( 0.0.0.0/0 )
}
```

9.9 Shortlist

9.9.1 *Shortlist configuration*

In the functionality of URL filtering, it is possible to configure the logging to an external server without blocking connections. The management (MNG) port is used for sending logs to an external server.

For it you should generate a text file with a list of exceptions, similar to as described in paragraph "". Then the file is loaded manually with the **dpiload shortlist <*URL*>** command, where the **URL** is entered in a format **http://<server address>/<file name>.<file extension>**.

Next, you need to configure shortlist settings in the **system dpi shortlist** configuration branch: turn on the option (**enable**) and specify the address and port of the server on which the logs will be sent, and specify the **timeskew <MINUTES>** for logs.

```
MyEcoNAT:3:system.dpi.shortlist# show
enable
timeskew 0
server_ip_and_port 1.2.0.1:8899
```

After that all URL-filtering events will be logging on the specified server for a specific (**shortlist**) address list. This option is automatically applied to all lists.

9.9.2 *URL-filtering logging configuration*

To turn on logging in the **dpilist** parameter list, you have to set **log_matches on**. If this option is enabled, but in **system dpi shortlist** configuration branch (see the previous paragraph) is not specified server address to which will be sent all the logs, then logging will not work.

If you want to keep logging without blocking or redirection, you should to set **behaviour ignore** in the **dpilist** parameters (logging will also work when setting **behaviour** parameter with other values).

```
dpilist1
{
 enable
```

```
 whitelist_mode off
 log_matches on
  log_pictures off
  exceptions off
 behaviour ignore
 redirect_use_interval off
 redirect_url ""
…
```

9.9.3 *Shortlist server configuration*

URL filtering events entries are sent to the server that is running **shortlist_server** program (available from the vendor on request).

Interaction with the **shortlist_server** program is done by the terminal on the server where it is running with the command ./**shortlist_server** <**flags**>.

Use the following flags:

- -c – cut out pictures and other content files,
- -d – specify the file format in which the logs will be written (see. below),
- -f – log entry in one file,
- -i – IP-address, which receives the logs (if multiple interfaces are involved in the server),
- -h – show help and quit,
- -p – UDP-port, which receives logs (it should be noted in the **system dpi shortlist** configuration tree branch),
- -t – output logs directly to the terminal.

You may specify multiple flags simultaneously (for example, to write logging to a file and display it on the terminal).

Since there can be a lot of URL filtering events, there is an opportunity to record groups of logs generated on a temporary basis in the program. For example, create a different file every day or every hour. To set this format of the logs record use **-d** flag. The possible flag codes and corresponding formats are shown in the table below. If the **–f %F.log** flag is specified, the log files will be generated daily, and the format of their names will be YYYY-MM-SS.log, for example, 2016-05-10.log.

Table 46

Code	Description
%a	Abbreviated weekday name
%A	Full weekday name
%b	Abbreviated month name
%B	Full month name
%c	Standard string of date and time
%C	The last two digits of the year
%d	Day of the month as a decimal number (1-31)
%D	Date in a month/day/year
%e	Day of the month as a decimal number (1-31) in two-character field
%F	Date in the form "year-month-day"
%g	The last two digits of the year with weekly year
%G	Year using a weekly year
%h	Abbreviated month name

Code	Description
%H	Hour (0-23)
%j	Hour (1-12)
%j	Day of the year as a decimal number (1-366)
%m	The month as a decimal number (1-12)
%M	The minutes as a decimal number (0-59)
%n	Delimeter of strings
%p	The local equivalent of AM (before noon) or PM (afternoon)
%r	12-hour time
%R	Time in the form hh:mm
%S	The seconds as a decimal number (0-60)
%T	Horizontal tab
%T	Time in the form hh:mm:ss
%u	Day of the week; Monday – the first day of the week (0-6)
%U	Week of the year; Sunday – the first day of the week (0-53)
%V	Week of the year with weekly year
%w	Day of the week as a decimal number (0-6, Sunday – day 0)
%W	Week of the year; Monday – the first day of the week (0-53)
%x	The standard date string
%X	Standard time string
%y	Year as a decimal number without a century (0-99)
%Y	Year as a decimal number, including a century
%z	Offset relative to Coordinated Universal Time(UTC)
%Z	The name of the time zone
%%	The percent sign

9.10 CAIR

The EcoNAT system supports the Center for Analyzing Internet Resources database (CAIR). A license is required to connect the database.

The list of connected licenses is available with the **show license** command.

```
EcoNAT:4:system.dpi# show license
CGNAT: Ok
BRAS: Ok
DPI: Ok
RADIUS: Ok
CAIR: Ok
```

When this license is installed, the **cair** element appears in the **system dpi** branch of the configuration tree. This element is a modified version of the DPI list, with the following available options:

```
EcoNAT:7:system.dpi.cair# ls
base_url "http://md5.base.cdn.cair.ru/last.txt"
uplevel_domains_url "http://md5.base.cdn.cair.ru/uplevel_domains.txt"
update_schedule never
```

Where:

base_url - CAIR base address,

uplevel_domains_url - address of the top-level domain database ,

update_schedule - automatic update schedule .

To manually download the CAIR database, use the **dpiload cair** command.

To download the top-level domain database, use the **dpiload uplevel** command.

For correct operation of the filter, you must periodically update both databases.

In the above-mentioned databases, information about sites is stored in the form **<md5 hash hostname> <category numbers in hexadecimal form via a colon>**. The database contains only domains, i.e. "www.example.com", but not "www.example.com/theme/1".

Example:

```
# head cair.txt -1
823211830251a3d40804125cdf1a1b13 2
```

All domains listed in the CAIR list are blocked in a manner similar to the principle of blocking records of the domain-mask type. For example, if there is an entry in the CAIR database of the form "example.com", then http and https resource requests will be filtered: "www.example.com", "help.example.com", "123.example.com" etc.

To include categories in the action of one of the DPI lists, the parameter **cair_categories** is used in which categories are also indicated in hexadecimal form via a colon.

Example.

```
EcoNAT:5:system.dpi.dpilist1# ls
enable
bittorrent off
whitelist_mode off
log_matches off
log_pictures off
exceptions off
behaviour ignore
redirect_use_interval off
redirect_url "http://blocked.operator.ru"
color_direction both
color_tos_byte 32
download_url ""
update_schedule never
cair_categories
"1:2:20:30:35:36:37:38:39:3c:3e:3f:41:44:49:4e:4f:54:5c:5d:5e:63"
no_ip ( )
ip ( 0.0.0.0/0 )
```

The list of categories and the corresponding numbers are presented in the table below.

Table 47

Decimal number	Hex number	Categorie
1	1	Alcohol
2	2	Erotica, pornography
3	3	Advertising
4	4	Authorities, government
5	5	Auto
6	6	Cinema, online video
7	7	Construction and repair
8	8	Consumables
9	9	Cooking
10	A	Country house
11	B	Courses, training

Decimal number	Hex number	Categorie
12	C	Electronics and Electrical Engineering
13	D	Industrial equipment
14	E	Family
15	F	Fashion & Style
16	10	Finance
17	11	art
18	12	Computers, hardware
19	13	Health
20	14	Hobby
21	15	Humor
22	16	Interior
23	17	Internet access Websites of companies providing Internet access services.
24	18	Legal services
25	19	Literature, e-books
26	1A	mass media
27	1B	Engineering
28	1C	Metallurgy
29	1D	mobile connection
30	1E	Music
31	1F	Community organizations
32	20	Computer games
33	21	Pets
34	22	A photo
35	23	Poster
36	24	The property
37	25	Religion
38	26	School
39	27	The science
40	28	Sport
41	29	Theaters
42	2A	Transport
43	2B	Tourism
44	2C	Universities
45	2D	Jobs & Jobs
46	2E	Website development
47	2F	Chats
48	30	Dating websites
49	31	Troops and weapons
50	32	Forums and blogs
51	33	Free Email Server
52	34	Free hosting
53	35	Illegal assistance to schoolchildren and students
54	36	Killings, violence, corpses
55	37	Online casino
56	38	Social networks
57	39	Terrorism, extremism
58	3A	Trade
59	3B	Underwear, swimwear
60	3C	Ensuring anonymity, crawling content filters
61	3D	Messaging services
62	3E	File exchange networks and sites
63	3F	Tobacco
64	40	Search engines

Decimal number	Hex number	Categorie
65	41	Drugs
66	42	Abuse of media freedom
68	44	Malicious programs
69	45	Improper advertising
70	46	Restricted Information
71	47	Banners and advertising programs
72	48	Driving and cars (negative)
73	49	Leisure and entertainment (negative)
74	4A	Health and medicine (negative)
75	4B	Corporate sites
77	4D	Sending SMS using Internet resources
78	4E	Bulletin Board
79	4F	Indecent and rude humor
81	51	Image Search Systems
82	52	Software
83	53	Information trash
84	54	Banner servers
85	55	White list
86	56	Safe for children sites
87	57	Short Link Services
88	58	Spam
89	59	Infringement of copyright and related rights
90	5A	Unified Register of Roskomnadzor Sites containing information, the distribution of which is prohibited in the Russian Federation (http://eais.rkn.gov.ru).
91	5B	Scammers
92	5C	Federal list of extremist materials
93	5D	Child porn
94	5E	Magic, witchcraft, occultism, theurgy
95	5F	Counters, analytics, metrics, statistics
96	60	Women's sites and magazines
97	61	Men's websites and magazines
98	62	Earnings on the Internet Sites declared for earnings on the Internet, trade in binary options and other
100	64	Forgery of documents
101	65	Service sites (api, scripts, js)
102	66	Other services
103	67	Directories, catalogs
145	91	The registry of secure educational sites. Click for more info

For viewing the information about the CAIRs categories for the specifyed sites one may use **show cairrecords <URL>** command.

Example

```
EcoNAT:12:system.dpi.dpilist1# show cairrecords example1.com
domain example1.com is present in CAIR categorie(s) 30:2f:38
EcoNAT:13:system.dpi.dpilist1# show cairrecords example2.com
domain example2.com is present in CAIR categorie(s) 37:5a
EcoNAT:14:system.dpi.dpilist1# show cairrecords example3.com
domain example3.com is not present in CAIR categories
```

9.11 Protocol filtering

This functionality allows you to block the traffic of certain protocols. To use this functionality, you must enable the URL filtering functionality, as well as enable and configure **dpilist** (see the "URL Filtering configuration" section). You can use any of the 16 lists.

In the URL filtering list settings, blocked protocols are specified in the protocols parameter. You can specify one or several protocols (separated by a space), and also add/delete individual protocols using the "+=" and "-=" operands if necessary.

Protocol blocking is limited to **dpilist**, in which they are specified, and by the **ip** and **ipv6** parameters of that **dpilist**.

For any traffic operations, you must also configure pools and ACLs (see the section "Pools and ACL").

The list of protocols is invoked by the show protocols all command in the system dpi branch.

To quickly search for protocols by name, enter the first letters of the name after the show protocols and press the **[Tab]** key. If there are several options, a list of matches will be displayed. If there is one option, then after pressing the **[Tab]** key, the protocol abbreviation will be displayed. For example:

```
ECOHOST:7:system.dpi# show protocols ss [TAB]
# There are several choices:
ssdp
ssh
ssl
sscopmce
ss
```

To display a description of a specific protocol, enter its abbreviation after the **show protocols** command and press the **[Enter]** key. For example:

```
ECOHOST:7:system.dpi# show protocols ssh
        name ssh
   full name Secure Shell
 description Secure Shell (SSH), sometimes known as Secure Socket Shell,
is a UNIX-based command interface and a protocol for obtaining secure
access to a remote computer.
```

APPENDIX A

Command summary

A brief description of the commands shown in the table below.

Descriptions:

Priority – the minimum level of user access rights, in which the command is available.

Mode: C – configuration, C * – context commands of configuration mode, O – operational.

VALUE – entered value of the parameter.

Table 48

Command	Description	Mode	Priority
( )	Clear the edited configuration item – array	C	4
VALUE	Assign the value to the edited configuration item	C	4
(VALUE VALUE)	Assign the value to the edited configuration item – array	C	4
?	Context help	O/C	0
helpme %	Console output parameter descriptions and tree branches available at the current level	O/C	0
!	Console output branches available at the current level of the configuration tree	O/C	0
{	Access to the editable item of the configuration tree	O/C	0
}	Exit from the editable item of the configuration tree	O/C	0
+= (VALUE VALUE)	Add multiple values to the edited configuration item – array	C	4
+= VALUE	Add value to the edited configuration item – array	C	4
-= (VALUE VALUE)	Delete multiple values of editable configuration item – array	C	4
-= VALUE	Delete the value of the edited configuration item – array	C	4
#NAME?	Assign the values to the edited configuration item or array	C	4
add (VALUE VALUE)	Add more values to the edited configuration item – array	C	4
add VALUE	Add value to the edited configuration item – array	C	4
apply	Configuration applying (unquestionable)	C	8
clear brasdb all	Erase all the subscriber records in BRAS	C	4
clear cgnat errors	Clear cgnat port allocation error counter	C	
clear config	Clear running config	C	
clear counters	Reset counters	O/C	0
clear sessions all	Clear the translations table	C	4
cloneacl SRCNAME NEWNAME	Create a copy of ACL containing all the rules, but having a different name	C	4
commit	Confirm the application of the configuration. If the configuration of the network management interface is changed, its settings are applied temporarily and rolled back if the **commit** command is not called within two minutes. This	O/C	1

Command	Description	Mode	Priority
	allows you to not lose the ability to communicate with the device remotely over the network in case of an erroneous configuration		
CONFIGITEMNAME	Select the current configuration element	O/C	0
configure	Go to the configuration mode	O	0
copy SRC_PROFILENAME DST_PROFILENAME	Copy the configuration to the specified. Not applicable to the factory and effective	C	5
copy hwinfo URL	Copy hardware information to the specified file on the remote server	O	
create acl ACLNAME	Create an ACL	C	4
create pool POOLNAME	Create a pool	C	4
create user USERNAME level LEVEL secret SECRETTYPE SECRETSTRING	Create a user	C	15
dir	View the list of configurations	C	4
disable	Disable the configuration object (e.g. pool)	C	4
dpilist	View uploaded URL filtering files lists	O/C	0
dpirun	Update the sites database from downloaded and enabled URL filtering lists	C	4
dropacls	Delete all ACLs	C	4
droppools	Delete all pools	C	4
droppolicies	Delete all policies at once	C	4
dropradius	Delete all RADIUS server settings at once	C	4
dropservices	Delete all services at once	C	4
edit acl ACLNAME edit ACLNAME	Go to the specified ACL in the configuration tree	O/C	0
edit date DATE	Set a new date on the device	C	14
edit datetime DATETIME	Set a new date and time on the device	C	14
edit pool POOLNAME edit POOLNAME	Go to the specified pool in the configuration tree	O/C	0
edit time TIME	Set time on the device	C	14
enable	Enable the configuration object (e.g. pool)	C	4
end	Exit the configuration mode	C	0
erase PROFILENAME	Delete profile with the specified name. Factory and effective profiles are not removed. If you delete a profile startup, then after loading, the system will wait until the user enters the console and apply any configuration	C	4
exit ..	Go to an upper level in the configuration or exit from configuration mode (if we are at the root of the configuration tree in configuration mode)	O/C	0
firmware download URL	Download the firmware upgrade from the remote server	O	
firmware install	Install downloaded firmware upgrade	O	
firmware revert	Set the reboot with inactive firmware	O	
firmware rollback	Discard the reboot with inactive firmware	O	
firmware status	Information about the installed firmwares and its state	O	
firmware unlock	Reset the blocked process of updating the firmware	O	
goto pool POOLNAME	Go to the specified pool in the configuration tree	O/C	0
grant USERNAME LEVEL	Change the level of user access rights	C	15

Command	Description	Mode	Priority
interface IFNAME down	Disable network interface	C	4
interface IFNAME up	Enable network interface	C	4
list	View the configurations list	C	4
load effective	Load an effective configuration for editing	C	4
load factory	Load default factory configuration	C	4
load PROFILENAME	Load selected configuration to edit	C	4
load startup	Load startup configuration to edit	C	4
no acl ACLNAME	Delete specified ACL	C	4
no pool POOLNAME	Delete specified pool	C	4
no RULEPRIOIRTY	Delete rule in ACL (contextual command is allowed only within the ACL itself)	C*	4
no use ACLNAME POOLNAME	Unbind pool and ACL	C	4
no user USERNAME	Delete the user	C	15
poweroff	Shut down the power and EcoNAT	C	8
profiles	View the configurations list	C	4
quit	Terminate the console session. Exits from the console (the edited configuration is not saved in the configuration mode)	O/C	0
reboot	Restart EcoNAT	C	8
remove (VALUE VALUE)	Delete the specified multiple values from the content of the current configuration item – array		4
remove VALUE	Delete the specified value from the content of the edited configuration item – array	C	4
renum ACLNAME	The forced numbering of the rules in the ACL. The first rule will be assigned the number 100. The remaining number will be 10 more than the previous	C	4
renum pools	The forced numbering of priorities of all the pools. The first pool (highest priority) will be assigned a priority of 100. The priority of each of the following will be 100 more than the previous	C	4
rollback	Cancel the last applied settings of the control network interface	O/C	1
root top /	Go to the root of the configuration tree	O/C	0
RULEPRIORITY allow [ip] [src] SRCADDR [dst] DSTADDR	Enter the ACL rule (contextual command is allowed only within the ACL itself)	C*	4
RULEPRIORITY deny [ip] [src] SRCADDR [dst] DSTADDR	Enter the ACL rule (contextual command is allowed only within the ACL itself)	C*	4
safe apply	Apply the configuration. In the case of changing the management interface configuration it will be applied temporary. If there won't be commit command within two minutes it will be rolled back. This allows not to lose the ability to connect to the device remotely in case of an erroneous configuration	C	8

Command	Description	Mode	Priority
save PROFILENAME	Save currently edited configuration under the specified name. Not applicable to the factory and effective	C	5
save startup	Save currently edited configuration as a startup (not recommended, it is better to apply the configuration using the apply, and if their work is satisfying then set it startup with the write command)	C	5
setlog SUBSYSTEM LEVEL setlog all LEVEL	Setting the logging level. It changes the system configuration. The running configuration won't be changed	C	
show	Show the configuration tree in depth from the current configuration element	O/C	0
| b STRING | begin STRING	Filter of show command. Throw a strings until it reaches a line containing the specified substring	O/C	0
| count	Filter of show command. It counts the number of strings	O/C	0
| e STRING | exclude STRING	Filter of show command. Print only lines not containing the specified substring	O/C	0
| i STRING | include STRING	Filter of show command. Print only lines containing the specified string (If the substring contains spaces or special characters such as ')', then you should use the quotation marks)	O/C	0
| more	Filter of show command. Print with a stopping through each page	O/C	0
| r STRING | regexp STRING	Filter of show command. Display only the strings that matches the specified regular expression	O/C	0
show acl ACLNAME	Show the rules contained in this ACL	O/C	0
show algtable	Show the information about ALG sessions	O/C	0
show arp all show arp IFNAME	Show the ARP information	O/C	0
show bind	Show information about binding local IP addresses to global	O/C	0
show brasinfo IPADDR show brasinfo IPADDRRANGE	Show BRAS information about the specified address	O/C	0
show brasinfo summary	View brief BRAS statistics	O/C	0
show brasstate	Show information about BRAS state	O/C	0
show cairrecords URL	Output CAIR categories for URL	O/C	0
show cgnat errors	Viewing port allocation errors in a CG-NAT pool	O/C	0
show config effective	Show the contents of the effective configuration (editable configuration remains unchanged)	O/C	0
show config file PROFILENAME	Show the contents of the specified configuration (editable configuration remains unchanged)	O/C	4
show config startup	Show the startup configuration (editable configuration remains unchanged)	O/C	0
show counters	Show system counters	O/C	0
show cps	Show current connection establishing speed	O/C	0
show dpistate	Show diagnostic information related to the URL filtering functionality in the Roskomnadzor list	O/C	0
show interface all	Show information about all network interfaces	O/C	0
show interface brief	Show brief information about network interfaces	O/C	0

Command	Description	Mode	Priority
show interface mng	Show the MGMT interface information	O/C	0
show interface IFNAME	Show information about a specific network interface (IFNAME – interface name, for example, TE7 interface name matches the interface number on the front of the device)	O/C	0
show interface IFNAME counters show interface all counters	View counters on the specified interface	O/C	0
show interface IFNAME traffic show interface all traffic	View incoming/outgoing traffic statistics for a particular interface (IFNAME) or all interfaces since the last system boot or the last counters reset. The Subtotal row shows the total values for all line interfaces, i. e. non-management/non-logging ones	O/C	0
show interface IFNAME traffic monitor show interface all traffic monitor	Real-time interface activity monitoring. Shows incoming/outgoing traffic per second for a particular interface (IFNAME) or all interfaces. The Subtotal row shows the total values for all line interfaces, i. e. non-management/non-logging ones	O/C	0
show interface transceiver IFNAME show interface transceiver all show sfp all	Show information about the transceivers	O/C	0
show ipif	Show information about the management interface settings	O/C	0
show memstat	Show memory usage statistics in Megabytes	O/C	0
show memstat detail	Show memory usage statistics in bytes	O/C	0
show neighbours IFNAME show neighbours all	Show the information received from neighbors via LLDP protocol	O/C	0
show ntp	Show status of time synchronization via NTP	O/C	0
show pool POOLNAME	Show the contents of the pool configuration	O/C	0
show pool usage	Show information about the usage of pools	O/C	0
show pools	Show the contents of all pools	O/C	0
show pool brief	Show summary of editable pools	O/C	0
show power	Show status of power supplies	O/C	0
show resources	Show resources statistics	O/C	0
show sessions gap ADDR:PORT	Show the sessions for the pair: global address + global port	O/C	0
show sessions global ADDRRANGE	Show the sessions for the specified global address	O/C	0
show sessions gport PORT	Show the sessions for the specified global port	O/C	0
show sessions lap ADDR:PORT	Show the sessions for the pair: a local address + local port	O/C	0
show sessions local ADDRRANGE	Show the sessions for the specified local address	O/C	0
show sessions lport PORT	Show the sessions for the specified local port	O/C	0
show sessions rap ADDR:PORT	Show the sessions for the pair: external address + external port	O/C	0
show sessions remote ADDRRANGE	Show the sessions for the specified external address	O/C	0
show sessions rport PORT	Show the sessions for the specified external port	O/C	0

Command	Description	Mode	Priority
show statistics	Shows statistics used/unused blocks of ports	O/C	0
show tacacs	Show the information about the connection to the TACACS server	O/C	0
show temperature	Show the temperature information on processor cores	O/C	0
show time	Show the current device time (always in UTC)	O/C	0
show version	Show software version information	O/C	0
show version detail	Show detailed software version information	O/C	0
show xlate gap ADDR:PORT	Show all current translations for the pair: global address + global port	O/C	0
show xlate gastat ADDRRANGE	Show translations statistics for the specified global address	O/C	0
show xlate global ADDRRANGE	Show all current translations to the specified global address	O/C	0
show xlate gport PORT	Show all current translations to the specified global port (regardless of address)	O/C	0
show xlate lap ADDR:PORT	Show all current translations for the pair: local address + local port	O/C	0
show xlate lastat ADDRRANGE	Show translations statistics for the specified local address	O/C	0
show xlate local ADDRRANGE	Show all current translations to the specified local address	O/C	0
show xlate lport PORT	Show all current translations to the specified local port (regardless of address)	O/C	0
show xlate pool POOLNAME	Show translations of the specified pool	O/C	0
start	Start to receive/send packets	C	15
stop	Stop to receive/send packets	C	15
up	Go one level up in the configuration tree	O/C	0
uptime	Show the time of operation of the system	O/C	0
use ACLNAME POOLNAME	Binding pool and ACL	C	4
who	Show authenticated user sessions	O/C	0
whoami	Output to the console information about the current user of the console and its privilege level	O/C	0
write	Save the effective configuration as the startup	O/C	0

http://rdp.ru
Phone: +7(495)204-9-204
E-Mail: sales@rdp.ru