RDP.RU

EcoSGE

User Guide

Руководство по установке и конфигурированию

Редакция: сентябрь 2018 г.

Sk Участник

EcoSGE. User Guide

Руководство по установке и конфигурированию

Редакция: сентябрь 2018 г.

Телефон: +7 (495) 204-9-204

http://rdp.ru/

Оглавление

Введение

В настоящем руководстве описан порядок установки и первичной настройки универсальной сервисной платформы EcoSGE. Данное оборудование является многофункциональным программно-аппаратным комплексом. Существует несколько наименований данного оборудования в зависимости от активного функционала: EcoNAT, EcoFILTER, EcoBRAS, Eco3in1 (устаревшее название EcoNATDPI). В настоящем документе описан максимальный набор функциональных возможностей данного оборудования.

Настоящее руководство действительно для встроенного программного обеспечения версии 3.1. Некоторые команды и значения параметров могут отличаться для более поздних или более ранних версий программного обеспечения. Для получения информации об актуальной версии программного обеспечения и документации обратитесь на сайт производителя http://rdp.ru/ или в службу технической поддержки.

Рекомендации по настройке, сопровождающиеся словами «ВНИМАНИЕ» или «ВАЖНО», обязательны к исполнению для корректной работы оборудования и встроенного программного обеспечения. При невыполнении этих рекомендаций, EcoSGE может работать некорректно.

Условные обозначения

Для наглядности в тексте документации используются различные стили оформления. Области применения стилей указаны в Таблица 1.

Таблица 1 – Стили оформления в документе

Стиль оформления	Область применения	Пример
Полужирный шрифт	Названия элементов пользовательского интерфейса (команды, кнопки клавиатуры, символы консоли)	Используйте команду **end**.
Полужирный курсив	Рекомендуемые значения вводимых параметров	Используйте тип терминала: ***vt100***.
Шрифт `Courier New`	Примеры кода. Примеры вывода консоли	Заводские настройки серийной консоли: `baud rate = 115200`
Курсив	Примечания	*Предварительно рекомендуется отключить автоматическое обновление списка…*

`Рамка, голубой цвет фона`	Примеры вывода консоли	Также доступна синхронизация времени по NTP протоколу настраиваемая через следующий раздел конфигурации:
		`system`
		`{ ntp { disable`
		`primary_server`
		`"131.131.249.19"`

Серый цвет фона	Примеры кода	После чего формируется файл запроса вида:
		`<?xml version="1.0"`
		`encoding="windows-1251"?>`
		`<request>`

В Таблица 2 приведены условные обозначения, используемые при описании консоли.

Таблица 2 – Условные обозначения при описании консоли

Условное обозначение	Расшифровка	Пример
Описание консоли		
< >	Пользовательские значения параметров	<часть команды>?
[ ]	Кнопки клавиатуры	<часть команды>[TAB]
Примеры		
Шрифт `Courier New`	Вывод консоли	`Welcome to EcoNAT console`
Полужирный шрифт	Вводимые значения параметров и команды	`EcoNAT:1:> configure`
Полужирный курсив	Пользовательские значения параметров	`1:# no use myacl mypool`

Список терминов и сокращений

Сокращение		Расшифровка
ACL	Access Control List	Список управления доступом
ALG	Application Layer Gateway	Интерфейс (шлюз) прикладного уровня, позволяющий транслировать определенные протоколы через NAT
ARP	Address Resolution Protocol	Протокол преобразования логического адреса в физический
BGP	Border Gateway Protocol	Протокол граничного шлюза
BRAS	Broadband Remote Access Server	Широкополосный сервер удалённого доступа
CGNAT	Carrier-grade NAT	NAT операторского класса
CLI	Command Line Interface	Интерфейс командной строки
CR	Carriage return	ASCII символ возврата каретки
DDM	Digital Diagnostics Monitoring	Цифровой контроль параметров (для SFP-модулей)
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки IP-узлов
DNS	Domain Name System	Система доменных имен
DPI	Deep Packet Inspection	Технология глубокой проверки содержимого сетевых пакетов
FTP	File Transfer Protocol	Протокол передачи файлов
GRE	Generic Routing Encapsulation	Протокол общей инкапсуляции
ICMP	Internet Control Message Protocol	Протокол управляющих сообщений Интернет
IP	Internet Protocol	Протокол сетевого уровня стека TCP/IP
IPTV	Internet Protocol Television	Телевидение по протоколу интернета
LF	Line Feed	ASCII символ новой строки
LLDP	Link Layer Discovery Protocol	Протокол обнаружения устройств, канального уровня
NAPT	Network Address Port Translation	Трансляция сетевых адресов и номеров портов транспортного уровня
NAT	Network Address Translation	Преобразование сетевых адресов
NTP	Network Time Protocol	Протокол синхронизации времени (версии 4)

Сокращение	Расшифровка	
OEM	Original Equipment Manufacturer	Оригинальный производитель оборудования
OSPF	Open Shortest Path First	Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала
PPTP	Point-to-Point Tunneling Protocol	Туннельный протокол типа точка-точка
RST	Reset the connection	Флаг сброса соединения в TCP протоколе
SFP	Small Form-factor Pluggable	Стандарт модульных компактных приёмопередатчиков, 1Gb Ethernet
SFP+	Small Form-factor Pluggable Plus	Стандарт модульных компактных приёмопередатчиков, 10Gb Ethernet
SNI	Server Name Indication	Идентификатор имени сервера для HTTPS
SNMP	Simple Network Management Protocol	Протокол сетевого управления и мониторинга
SSH	Secure Shell	Протокол защищенной консоли
TACACS	Terminal Access Controller Access Control System	Сервер контроля доступа
TCP	Transmission Control Protocol	Протокол управления передачей данных
TFTP	Trivial File Transfer Protocol	Простой протокол обмена файлами
ToS	Type of Service	Тип обслуживания
TTL	Time to Live	Время жизни IP-пакетов
UDP	User Datagram Protocol	Протокол пользовательских дейтаграмм
URL	Uniform Resource Locator	Единый указатель ресурса
UTC	Coordinated Universal Time	Всемирное координированное время
WAN	Wide Area Network	Глобальная компьютерная сеть
ИНН	Идентификационный номер налогоплательщика	
ОГРН	Основной государственный регистрационный номер	

1 борудование

ВНИМАНИЕ: Во избежание повреждения аппаратной платформы не рекомендуется устанавливать 1GB SFP модули в разъемы, предназначенные для 10GB SFP+.

Для оборудования старших серий 10GB сетевые интерфейсы для трафика имеют номера TE1-TE12 (TE8/TE16 – в зависимости от модели). Порт для логирования имеет скорость 1GB и маркировку LOG (см. рисунок ниже).

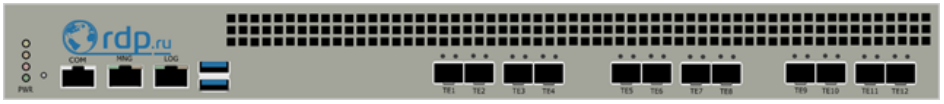

Рисунок 1

Для оборудования 2-тысячной серии 10G сетевые интерфейсы для трафика располагаются в правой части передней панели устройства (см. рисунок ниже).

EcoNAT 2020

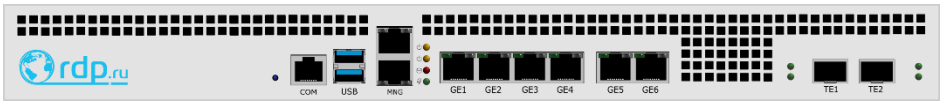

Рисунок 2

Оптические сетевые интерфейсы, промаркированные как TE1, TE2, в CLI называются **te7**, **te8**.

EcoNAT 2040

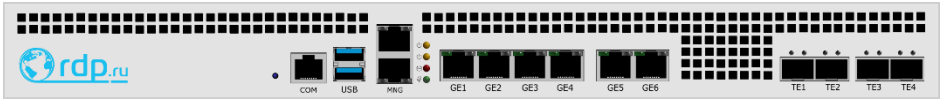

Рисунок 3

Оптические сетевые интерфейсы, промаркированные как TE1-TE4, в CLI называются **te7-te10**.

Также можно использовать «медные» сетевые интерфейсы 1GB Copper с номерами 1, 2 и 3, 4. На устройствах 2020 в черном корпусе (старая модель) сетевые интерфейсы для логирования имеют скорость 1GB и маркировку 5, 6.

На устройствах 2020, 2040 в синем корпусе сетевой интерфейс для логирования имеет скорость 1GB и расположен над MNG-интерфейсом.

Оборудование управляется при помощи CLI консоли.

2 Вход в систему

Существуют два варианта для входа в консоль EcoNAT: через последовательный порт или по сети через SSH протокол.

2.1 Подключение по последовательному порту

Разъем для последовательного порта находится с левой стороны передней панели устройства и помечен надписью “Console” или “COM” (Рисунок 3). Подсоедините кабель к разъему “COM”. Переходник для серийного порта EcoNAT с RJ-45 на DB-9 прилагается к устройству.

Рисунок 4

Заводские настройки серийной консоли по умолчанию (в последствии их можно будет сменить):

- скорость передачи (baud rate) 115200 бод;
- биты данных (data bits) 8;
- стоповые биты (stop bits) 1;
- бит контроля по чётности (parity bits) none;
- контроль потока (flow control) none.

Настройки терминала: используйте тип терминала ***vt100***.

Серийная консоль защищена локальным паролем (сохранённым на самом устройстве). Вход по серийной консоли не логируется через TACACS+.

Серийную консоль нельзя запретить – она будет всегда доступна.

По умолчанию для входа используется имя пользователя ***admin*** и пароль ***econat***.

2.2 Подключение через SSH

Консоль управления EcoNAT доступна по SSH протоколу через управляющий сетевой интерфейс, который находится с левой стороны передней панели устройства в нижнем ряду и помечен надписью “LOG/MGMT” или “MNG”.

Заводские настройки управляющего интерфейса:

- IP-адрес и маска (ip address/mask) 192.168.100.200/255.255.255.0;
- шлюз (gateway) 192.168.100.1;
- серверы DNS (DNS servers) 8.8.8.8;
- разрешенные IP-адреса (allowed IP) any.

Заводские настройки сетевой консоли: используйте имя пользователя ***admin*** и пароль ***econat***, используется стандартный порт 22.

В EcoNAT поддерживается отправка команд в строке SSH-соединения. Пример: **ssh admin@<IP-address> show counters all** или **ssh admin@<IP-address> "uptime ; who ; show interface te10"**. При отправке нескольких команд их необходимо заключить в кавычки ". В качестве разделителя между перечисляемыми командами используется точка с запятой с пробелами по обе стороны знака.

2.3 Режимы работы консоли

Сразу после входа Вы оказываетесь в операционном режиме (подсказка командной строки заканчивается символом ' >'), в котором можно просматривать настройки, но нельзя изменять конфигурацию. Для того чтобы войти в конфигурационный режим, надо выполнить команду **configure**. После этого действующая (активная) конфигурация будет загружена для редактирования, а символ приглашения командной строки (prompt) изменится на символ ' #'.

```
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:#
```

Для выхода из конфигурационного режима используйте команду **end** или **exit** (если вы находитесь в корне конфигурации). В случае если редактируемая конфигурация отличается от текущей активной, вам будет предложено применить конфигурацию **[a]**, сохранить под некоторым именем **[s]**, или потерять редактируемую конфигурацию **[d]**. При сохранении конфигурации появится запрос на ввод имени конфигурации.

Разрыв сеанса, или закрытие соединения автоматически приводит к потере всех не сохранённых изменений в редактируемой конфигурации.

```
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:>
```

3 Подсказки и горячие клавиши

В любой момент можно использовать подсказки и горячие клавиши, представленные в таблице ниже.

Таблица 3

Команда/сочетание клавиш	Действие
?	Показывает перечень команд и/или аргументов, доступных в текущем контексте, а также подсказки по их назначению
<часть команды>?	Показывает перечень команд с таким началом
<часть команды>[TAB]	Пытается выполнить автозаполнение
стрелка вверх [↑]	Возврат к ранее введенной команде (история)
стрелка вниз [↓]	Возврат к команде, введенной позднее (история)
..	Перейти на уровень выше
/	Вернуться в корень конфигурационного дерева
helpme %	Вывод на консоль описания параметров и веток дерева, доступных на текущем уровне
!	Вывод на консоль веток, доступных на текущем уровне дерева конфигурации

Примеры:

```
EcoNAT:1:> w ?
```

Какие команды начинаются на «w»?

```
whoami
write
```

Команды, недоступные на текущем уровне пользовательских привилегий, выделяются цветом.

```
EcoNAT:2:>
EcoNAT:1:system.loopback> helpme
system loopback ip: IPv4 address used for loopback packets
system loopback mac: MAC address used for loopback packets
```

4 Конфигурация

EcoNAT использует конфигурационное дерево для хранения настроек. Структура дерева показана на рисунке ниже.

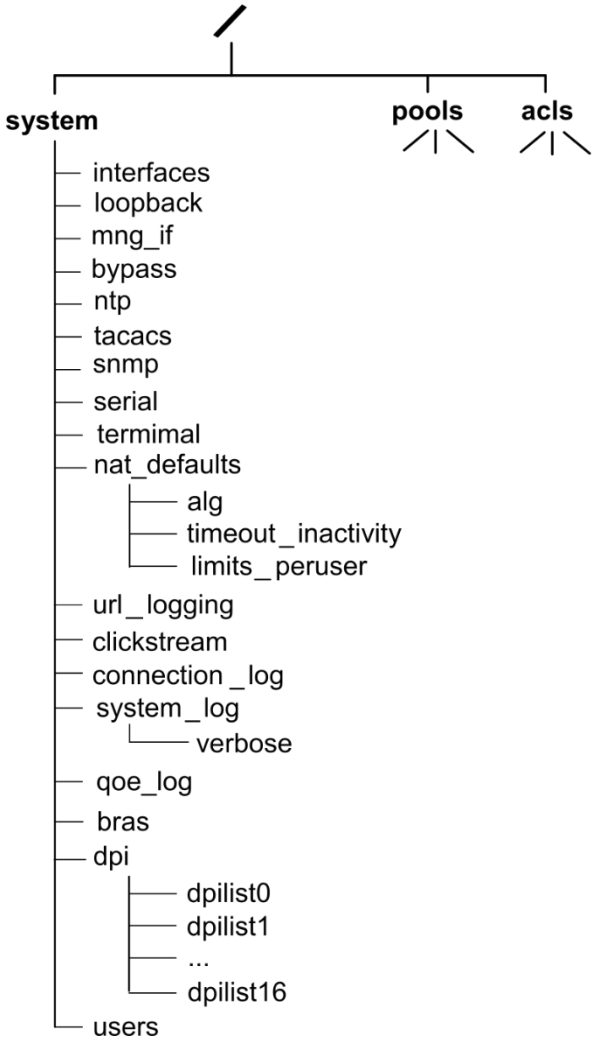

Рисунок 5

ПРИМЕЧАНИЕ: В реальном устройстве возможны дополнительные ветки в дереве, связанные с дополнительной функциональностью, и не показанные в этом дереве. Описание веток дерева конфигурации приведено в таблице ниже.

Таблица 4

Название ветки	Описание
system	Контейнер для настроек
interfaces	Включение/выключение сетевых интерфейсов
loopback	IP- и MAC-адреса, используемые для генерации ошибок
mng_if	Настройки управляющего сетевого интерфейса
bypass	Настройки интерфейсов, подключенных к EcoBypass
ntp	Настройки NTP
tacacs	Настройки TACACS
snmp	Настройки SNMP
serial	Настройки последовательного порта
terminal	Настройки терминала

Название ветки	Описание
nat_defaults	Параметры NAT по умолчанию (общие параметры для всех пулов, в том числе, параметры, используемые при создании новых пулов)
url_logging	Настройки логирования. Настройки логирования URL
connection_log	Настройки логирования аллокации адресов
system_log	Настройки системного логирования
clickstream	Настройки сбора проходящих GET-запросов
bras	Настройки BRAS
dpi	Настройки URL-фильтрации (DPI)
users	Информация о пользователях
pools	Здесь содержатся пулы, созданные пользователем
acls	Здесь содержатся ACL (Access Control List), созданные пользователем

Изменение конфигурации возможно только в конфигурационном режиме (см. раздел "Вход в систему").

Фактическое изменение настроек системы происходит только после успешного выполнения команды **apply**, завершающей правку конфигурации администратором. Команда **apply** может быть выполнена только в конфигурационном режиме. Непосредственно при выходе из конфигурационного режима также будет предложено применить изменения.

При успешном выполнении команды **apply** в консоли выводится подтверждение применения изменений конфигурации.

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

Навигация по дереву конфигурации возможна как в операционном, так и в конфигурационном режиме. По умолчанию после авторизации в системе вы оказываетесь в корне конфигурационного дерева. При навигации по дереву в командной строке отображается, в какой ветке дерева вы находитесь в данный момент. Путь отображается перед символом приглашения, названия веток отображаются иерархически, начиная с родительской, разделяемые символом '**.**'.

Вернуться в корень конфигурационного дерева можно в любой момент при помощи команды **root** или символа '/'.Перейти на уровень можно при помощи команд **exit** или **up**, или символов '**..**'.

ПРИМЕР:

```
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:#
```

Маршрут следования по дереву показан на рисунке ниже.

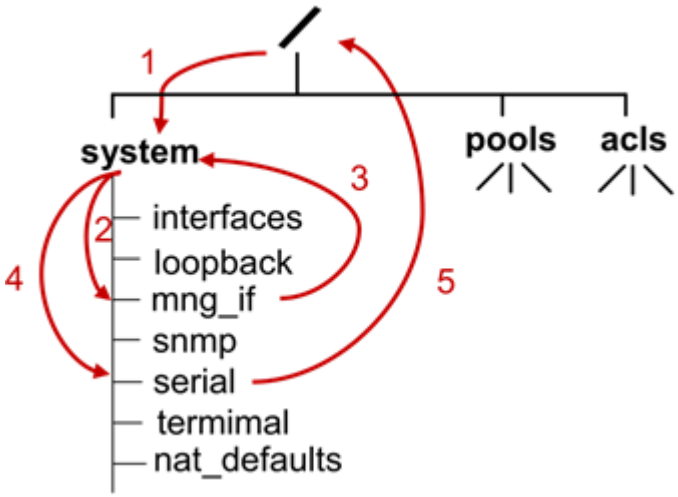

Рисунок 6

Для того, чтобы сразу перейти в конкретную поддиректорию конфигурации (ветку дерева), необходимо указать путь, используя в качестве разделителя **пробел**.

Для быстрой навигации по поддиректориям первого уровня директории **system** можно использовать команду **goto *<имя ветки>***. Например, команда **goto serial** переводит в конфигурационную директорию **system serial**.

Аналогично, для быстрого перехода к ветке NAT **pools** используется команда **goto *<имя пула>*** (подробнее о правилах именования пулов см. в разделе "Пулы и ACL"). А для быстрого перехода к одной из веток ACL служит команда **goto *<имя ACL>*** (подробнее о правилах именования ACL см. в разделе "Пулы и ACL").

ПРИМЕР:

```
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#
```

Для просмотра конфигурации, начиная от текущего уровня вглубь используйте команду **ls** или **show**.

Для просмотра веток, доступных на текущем уровне дерева конфигурации, используйте короткую команду '**!**'.

```
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)
```

Команды для просмотра конфигураций и управления ими описаны в разделе " Конфигурация".

4.1 Управление конфигурациями

Предопределённые имена конфигураций:

- **startup** – конфигурация, автоматически используемая после перезагрузки устройства;
- **effective** – текущая конфигурация (последняя применённая на устройстве). Можно загрузить в текущую консоль командой **load effective**,
- **lastapply** – конфигурация, которая была применена последней,
- **factory** – заводская конфигурация (не подлежит изменению).

4.1.1 Просмотр конфигураций

Для просмотра списка сохранённых конфигураций используйте команду **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
…
```

Для просмотра произвольной конфигурации из сохраненных используйте команду **show config file <имя конфигурации>**.

Для просмотра действующей, ранее применённой конфигурации, используйте команду **show config effective** в любом режиме.

Для просмотра конфигурации, которая будет применена после перезагрузки, используйте команду **show config startup** в любом режиме.

4.1.2 Применение и сохранение конфигурации

При внесении изменений в конфигурацию, изменяется только локальная конфигурация, связанная с текущим экземпляром консоли. Таким образом, при завершении сеанса все изменения в конфигурации будут утеряны, если они не были применены или сохранены.

Для того чтобы записать текущую редакцию конфигурации в файл, используется команда: **save <CONF_NAME>**, где **CONF_NAME** - имя конфигурации. Команда **save** не применяется к конфигурациям **factory** и **effective**.

Для применения изменений в конфигурации используется команда **apply**.

Если в секции конфигурационного дерева указано значение параметра **disable**, то секция считается отключенной. При внесении изменений в такую секцию и дальнейшей попытке применения изменений будет выдано сообщение: «**NO NEED FOR APPLY: CONFIGURATION IS THE SAME**», - указывающее на отсутствие требующих применения настроек.

Исключение составляют секции **system_log verbosity** и **dpi shortlist**.

В секции **system_log verbosity** указывается подробность ведения системных журналов той или иной подсистемы (см. раздел Логирование). Данные журналы дублируются локально. Изменения в настройке данной секции применяются, независимо от отключения удаленного сервера логирования системных журналов.

В секции **dpi shortlist** присутствует параметр **servers_ip_and_port**, в котором хранится адрес сервера логирования, общего для всей подсистемы URL-фильтрации (см. раздел Shortlist). Изменения в настройке данного сервера применяются даже при отключенной секции **shortlist**.

4.1.3 Загрузка конфигурации

Для загрузки конфигурации из файла необходимо вызвать команду: **load <CONF_NAME>**.

ВНИМАНИЕ! Во время внесения изменений в конфигурацию с одной консоли, другой пользователь мог применить свои настройки с другой консоли. Для загрузки на редактирование текущей активной конфигурации в конфигурационном режиме необходимо ввести команду **load effective**.

Для сохранения или загрузки конфигурации на/из TFTP-сервер, используются следующие формы команд **save** и **load**:

- **save tftp://<HOSTNAME>:<PORT>/<CONF_NAME>**,
- **load tftp://<HOSTNAME>:<PORT>/<CONF_NAME>**.

Параметры команд приведены в таблице ниже.

Таблица 5

Параметр	Описание
HOSTNAME	Адрес TFTP-сервера
PORT	Порт обращения к TFTP-серверу

Параметр	Описание
CONF_NAME	Имя конфигурации

Пример:

```
MyEcoNAT:1:# load tftp://192.168.0.12:69/myconfig
```

4.1.4 Копирование конфигурации

Для того чтобы скопировать конфигурацию в новый файл необходимо вызвать команду: **copy** ***<источник><назначение>***. EcoNAT поддерживает следующие схемы копирования файла конфигурации:

- из одного локального файла конфигурации в другой локальный файл конфигурации,

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

- из локального файла конфигурации на tftp-сервер,

```
MyEcoNAT:4:# copy config2 tftp://1.1.1.1/1/copyname
```

- с tftp-сервера в локальный файл.

```
MyEcoNAT:5:# copy tftp://1.1.1.1/1/copyname config4
```

Команда **copy** не применяется к конфигурациям **factory** и **effective**.

Для того чтобы скопировать конфигурацию на tftp-сервер необходимо сначала создать на сервере файл с названием соответствующим копируемому файлу. Формат названия файла конфигурации **<имя конфигурации>.econat.profile**. Для файла необходимо установить права на запись.

4.1.5 Удаление конфигурации

Для того чтобы удалить конфигурацию необходимо вызвать команду: **erase** ***<имя конфигурации>*** . Команда **erase** не применяется к конфигурациям **factory** и **effective**.

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

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

Также существует команда **clear config**. Данная команда очищает (обнуляет) редактируемую конфигурацию, не удаляя ее. То есть, удаляются все введенные пулы, ACL, обнуляются настройки интерфейсов, удаляются пользователи и так далее.

Измененная конфигурация применяется только после выполнения команды ***apply*** .

4.1.6 Запись конфигурации, которая будет использована при старте EcoNAT

Для того чтобы сделать текущую эффективную конфигурацию стартовой, используется команда **write**. Сделать текущую редактируемую конфигурацию стартовой можно непосредственно в конфигурационном режиме вызовом команды **save startup**, однако, так делать не рекомендуется.

ВАЖНО: после выполнения команды write, при перезагрузке системы будет загружена конфигурация, действовавшая на момент запуска команды write, или конфигурация, записанная при помощи команды save startup, если она была выполнена позже. Это конфигурация, для которой был выполнен последний apply, даже если он был выполнен не в текущей консоли и другим пользователем!

Во избежание коллизий рекомендуется, чтобы возможность редактировать конфигурацию EcoNAT была у одного человека. Также рекомендуется выходить из конфигурационного режима сразу после изменения конфигурации, чтобы при следующем запуске автоматически войти в последнюю версию конфигурации.

5 Быстрая первоначальная настройка

В настоящем разделе описаны общесистемные настройки и команды управления устройством.

5.1 Настройка управляющего сетевого интерфейса

Для управления EcoNAT по сети необходимо сконфигурировать параметры управляющего сетевого интерфейса.

Ниже приведен пример присвоения управляющему интерфейсу IP 192.168.100.12/24, основной шлюз 192.168.100.1, адреса DNS серверов: 10.0.8.1, 10.0.8.3. Доступ к управляющему интерфейсу разрешить только тем, кто находится в сети 192.168.100.12, а также хосту 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 )
```

Для разрешения доступа к управляющему интерфейсу с любого компьютера можно присвоить **allowed_ip** значение ***0.0.0.0/0***.

Если после изменений параметров сетевого интерфейса выполнить команду **safe apply**, то изменения именно настроек сетевого интерфейса применятся на несколько минут (в остальных случаях изменения применяются командой **apply** сразу). Это связано с тем, что ошибочное конфигурирование сетевого интерфейса приводит к невозможности конфигурирования EcoNAT по сети.

За эти две минуты имеет смысл проверить подключение путем ещё одного соединения с консолью, и если соединение прошло успешно, то для закрепления изменений можно использовать команду **commit**.

Для просмотра информации о настройках управляющего интерфейса можно использовать команду **show ipif**.

```
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
```

С управляющего интерфейса могут быть выполнены стандартные команды **ping** и **traceroute**.

```
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
```

Адрес управляющего интерфейса может быть задан статически (см. пример выше) или динамически. Для включения автоопределения динамически выдаваемого адреса (DHCP) необходимо задать значение параметра **ip_address** в формате **0.0.0.0/***, где * - любая подсеть.

5.2 Настройка подключения к EcoBypass

Устройство EcoNAT может быть подключено в сеть через активный оптический байпас серии EcoBypass. Взаимодействие с EcoBypass осуществляется путем отправки heartbeat-сообщений в рамках одной TCP-сессии. В случае, если heartbeat-сообщения перестают приходить, EcoBypass переключается в прозрачный режим. После чего трафик пропускается в обход EcoNAT до тех пор, пока связь с ним не возобновится.

Для корректной работы данной схемы должна быть настроена IP-связность между **MNG**-интерфейсом EcoNAT и **ETH**-интерфейсом EcoBypass. В свою очередь, пары интерфейсов EcoNAT подключаются к спаренным оптическим портам EcoBypass.

Схема подключения пары сетевых интерфейсов **TE1, TE2** через EcoBypass представлена на рисунке ниже.

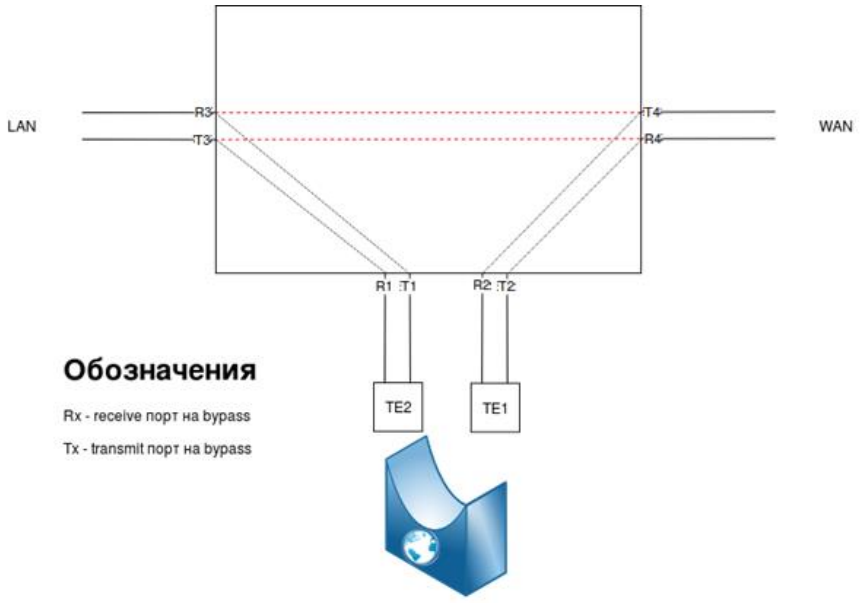

Рисунок 7

Hearbeat-сообщения имеют вид **<BP01_XX_BP>**, где **XX** - номер сетевой платы EcoBypass, к которой подключено устройство EcoNAT. В ответ EcoBypass отправляет сообщения вида **<BP01_XX_BP_OK>**.

Heartbeat-сообщения отправляются всегда, кроме случаев когда был административно выключен один из интерфейсов пары, или возник сбой в работе устройства.Кроме полного отсутствия heartbeat-сообщений, EcoBypass может отслеживать падение уровня Tx-сигнала от устройства. При критическом падении уровня, EcoBypass переключится в прозрачный режим.

Настройка EcoBypass осуществляется в ветке конфигурационного дерева **system bypass**.

Настраиваемые в данной ветке параметры представлены в таблице ниже.

Таблица 6

Параметр	Описание
enable/disable	Включение/выключение отправки heartbeat-сообщений на EcoBypass
bypass_ip	IP-адрес EcoBypass. Для корректной работы должна быть настроена IP-связность между MNG-интерфейсом EcoNAT и ETH-интерфейсом EcoBypass
teN1_teN2	Настройка для пары интерфейсов. Возможные варианты значений: **disabled** - EcoBypass не подключен; номер сетевой платы (слота) EcoBypass, к которому подключена пара. В случае 1U модели EcoBypass нумерация слотов будет от 1 до 8. В случае 4U модели EcoBypass нумерация слотов будет от 01 до 32

Пример настройки:

```
EcoNAT:2:system.bypass> ls
enable
bypass_ip 10.210.1.199
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>
```

5.3 Настройка терминала

Рекомендуется при первичной настройке EcoNAT выставить системное приглашение и время автоматического завершения сеанса по неактивности (то есть, если сеанс будет неактивен, то спустя указанное время он будет закрыт). Время автоматического завершения сеанса указывается в секундах.

```
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#
```

Для вступления в силу изменений параметров **system terminal** (**autologoff_timeout**, **max_consoles**, **prompt**) требуется перезагрузка устройства.

После загрузки системы системное приглашение берётся из параметра **system terminal prompt**, находящегося в стартовой конфигурации. Это приглашение можно изменить в

соответствующей ветке дерева конфигурации с последующим применением изменений командой **apply**. При внесении изменений через параметр **system terminal prompt**, они будут отображены только при следующей загрузке системы.

Предусмотрена возможность включения/выключения счетчика строк и команд с использованием команды **print_line_num**.

print_line_num off – выключить.

print_line_num on – включить (установлено по умолчанию).

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#

5.4 Настройка loopback

Адрес loopback интерфейса используется EcoNAT для отправки ICMP-сообщений пользователям. В текущей версии ПО данные сообщения генерируются EcoNAT только в одном случае – если пользователю по каким-либо причинам не удалось выделить очередной порт на глобальном адресе. EcoNAT отправит ICMP error type=3 code=13 (Destination unreachable (Communication administratively filtered)).

Настройка **loopback** доступна в ветке конфигурации **system loopback**. Для loopback возможно указать отображаемый IP-адрес и MAC. Если IP-адрес для **loopback** не установлен, то по умолчанию он будет 100.64.97.116.

```
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#
```

5.5 Настройка времени

Настройка системного времени очень важна для правильного функционирования EcoNAT, поскольку временные метки в сообщениях, которые логируются, основаны именно на этом времени.

EcoNAT понимает время только во временной зоне UTC (Universal Time Coordinated).

Время можно посмотреть с помощью команды **show time**. Также можно установить время вручную через команду **edit datetime** (при этом дата и время должны вводиться в формате UTC).

```
MyEcoNAT:1:# show time
Current time is 16-Jun-2014T09:07:28
MyEcoNAT:2:# edit datetime 17-Jun-2014T09:00:00
```

Также доступна синхронизация времени по NTP протоколу, настраиваемая через следующий раздел конфигурации:

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

Чтобы включить синхронизацию времени по NTP, необходимо зайти в ветку ***system ntp*** и выполнить команду ***enable***.

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

Состояние синхронизации с NTP серверами можно увидеть с помощью команды **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 |
```

Системные логи и логи соединений могут выводить локальное время. Для установки локального времени используется параметр **system system_log timeskew**. Это параметр содержит смещение локальной временной зоны относительно UTC в минутах. Например, для настройки временной зоны Москвы (UTC+3) необходимо выставить значение параметра ***180*** (3x60) минут.

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

5.6 Логирование

5.6.1 Настройка логирования абонентских соединений

Информация о выделении IP-адреса и/или порта или блока портов в нём должна сохраняться в соответствии с требованиями законодательства Российской федерации. В качестве стандартного механизма EcoNAT использует логирование по syslog протоколу.

Настройки логирования соединений находятся в ветке **system connection_log**. Для того, чтобы включить логирование, в данной ветке должен быть установлен параметр ***enable***.

В случае платформы с несколькими сетевыми интерфейсами, выделенными для логирования соединений, данные интерфейсы объединяются в виртуальный статический канал, по которому отправляются пакеты логов. Для платформ с одним интерфейсом для логирования соединений, виртуальный статический канал организуется на единственном интерфейсе. Для виртуального канала в обоих случаях указывается синтетический IP-адрес источника, который не является фактическим, поэтому при попытке выполнить на этот адрес команду ping, ICMP запросы, попавшие на логирующий интерфейс EcoNAT, останутся без ответа. Пакеты с логами отправляются по очереди по всем подключенным сетевым интерфейсам логирования, балансировки или разделения трафика при этом не происходит. Номера сетевых интерфейсов для логирования указаны в разделе "Shortlist".

Параметры **connection_log** описаны в таблице ниже.

Таблица 7

Параметр	Описание
enable или disable	Включение и выключение логирования соединений
log_servers	Адреса и порты syslog серверов, на которые будет осуществляться логирование (логирование будет идти параллельно на все доступные сервера из списка, то есть каждый из серверов будет получать информацию обо всех соединениях). В настоящее время максимальное количество серверов ограниченно двумя
ip_address	IP-адрес и маска подсети (через ‘/’) для виртуального канала, в который объединены логирующие сетевые интерфейсы
mac	MAC-адрес для виртуального канала, в который объединены логирующие сетевые интерфейсы (если не указан, то в качестве его будет выбран MAC-адрес одного из сетевых интерфейсов)
gateway	Шлюз по умолчанию для виртуального канала, в который объединены логирующие сетевые интерфейсы. Требуется в случае, если не все syslog сервера, указанные в параметре **log_servers**, находятся в подсети, указанной в параметре **ip_address**
strip_tags	В режиме зеркалирования EcoNAT отправляет абоненту через логирующий сетевой интерфейс пакет прерывания соединения (для HTTPS) или пакет перенаправления (для HTTP) – при получении тегированного трафика и при включенном параметре (on), срезается метка (или двойная метка). При выключенном параметре (off) пакет перенаправления или прерывания отправляется в логирующий сетевой интерфейс с аналогичными параметрами обрабатываемого трафика
that_mac	Статическая ARP запись для первого syslog-сервера в параметре log_servers. Параметр необязательный. Если параметр не установлен, то MAC-адрес будет определяться по ARP протоколу. Должен содержать MAC-адрес первого syslog сервера (в случае, когда первый syslog сервер находится в той же подсети) или MAC-адрес default gateway (если первый syslog сервер в другой подсети).

Параметр	Описание
	Использование этого параметра уменьшает вероятность потери данных логирования на старте при условии большой нагрузки. EcoNAT способен обработать и залогировать более 5 миллионов соединений в секунду при полной нагрузке. Если syslog сервер ответит на ARP запрос, например, через 10 ms, в очереди может скопиться 50,000 соединений, ждущих отправки
timeskew	Сдвиг указываемого в логах времени относительно Гринвича. Задается в минутах. Например, для Москвы значение параметра должно быть - 180

Режимы логирования. Логирование в формате Syslog

Порты для трансляции адресов в режиме CGNAT абонентам выделяются блоками по 128 портов за один раз. Следующий блок выдаётся только при исчерпании портов в предыдущем блоке. За счёт блочного выделения можно многократно уменьшить объем логов, так как при соответствующих настройках, вместо множества сообщений о выделении абонентам портов, будет лишь одно сообщение о выделении диапазона в 128 портов (блока).

EcoNAT поддерживает логирование в различных форматах. Ниже описаны соответствующие параметры **connection_log** при логировании в формате syslog.

Таблица 8

Параметр	Описание
log_format	Параметр показывает тип логирования: **syslog** – логирование по syslog, **netflow** – логирование соединений по NetFlow v9 протоколу
log_on_release	Параметр показывает, надо ли посылать в **connection_log** сообщение в случае освобождения трансляции или блока. В случае создания сообщение посылается всегда. Если параметр **log_individual_conn** включен, то сообщение формируется при освобождении каждой трансляции, в противном случае – при освобождении блока
log_individual_conn	Параметр указывает, надо ли логировать индивидуальные соединения или можно логировать только блоки портов
use_hex_format	Разрешает использовать шестнадцатеричной формат для вывода логов, что позволяет уменьшить размер логов, при полном сохранении информационной составляющей. Если запрещено, то используется десятичный фиксированный формат, например: 010.210.000.012:00080
pack_msgs	Разрешает упаковывать несколько информационных сообщений о логируемых событиях в одно syslog сообщение. Это уменьшает размер логов и нагрузку сети
facility	Устанавливает для формируемых сообщений формата syslog категорию субъекта, формирующего сообщение, для удобства дальнейшей обработки и фильтрации. Допустимые значения параметра от 16 до 23. Эти значения соответствуют кодам стандарта RFC 5424, обозначающим субъекты локального происхождения (local use 0 (local0) – local use 7 (local7)). Значение по умолчанию – 16
severity	Устанавливает для формируемых сообщений формата syslog уровень важности для удобства дальнейшей обработки и фильтрации. Допустимые значения параметра от 0 до 7, рекомендуемые – от 5 до 7. Эти значения соответствуют кодам стандарта RFC 5424, обозначающим уровни важности сообщений: **5** – замечание (Notice), сообщения о нормальных, но важных событиях; **6** – информационное (Informational) сообщение; **7** – отладочное (Debug) сообщение. Значение по умолчанию – 6

Основные режимы для логирования соединений и рекомендуемые настройки представлены в таблице ниже.

Таблица 9

Соотношение размер/читаемость логов	log_on_release	log_individual_conn	use_hex_format	pack_msgs
Минимальный размер логов (блоки портов)	No	No	**Yes**	**Yes**
Малый размер логов, но более читаемые	No	No	No	No
Минимальный размер логов (соединения)	No	**Yes**	**Yes**	**Yes**
Более читаемые логи (соединения)	**Yes**	**Yes**	No	**Yes**
Отладочный режим (самые читаемые логи, но большой размер)	**Yes**	**Yes**	No	No

Если нужно логировать, КТО ХОДИЛ С ТАКОГО-ТО АДРЕСА И ПОРТА:

- Если система хранения логов у оператора хорошо налажена (то есть, всё логируется и хранится без потерь), то рекомендуются задать для четыре вышеописанных параметров значение ***No***.
- Если возникают потери в системе логирования провайдера, то имеет смысл включить опцию **log_on_release**. Тогда в случае потери сообщения об открытии соединения будет дополнительно направлено сообщение о закрытии, что снизит вероятность потери сообщения.

Если нужно логировать, КТО ХОДИЛ НА ЗАДАННЫЙ АДРЕС И ПОРТ:
Необходимо включить режим **log_individual_conn**. В этом случае в логе будет отражаться REMOTE_IP и REMOTE_PORT – хост и порт, с которым осуществлял обмен данными ваш абонент.

Для включения логирования, не забудьте установить для **connection_ log** параметр ***enable***.

ПРИМЕР НАСТРОЕК:

```
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
```

Формат логов syslog: **<Дата время syslog сервера> <IP-адрес EcoNAT> <Дата время EcoNAT> <Имя EcoNAT> | <IP-адрес назначения (DST)>:<Порт> <IP-адрес, на который осуществляется трансляция>:<Порт> <IP-адрес источника (SRC)> <Идентификатор протокола>**.

Например:

```
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-адреса записываются в трехзначном формате, например, адрес 10.1.1.200 будет представлен как 010.001.001.200.Ниже приведены несколько примеров настроек формата логов. Для удобства восприятия, часть строк до вертикальной черты не показана.

Логирование блоков портов с упаковкой нескольких информационных сообщений о событиях в сети в одно сообщение syslog. В данном случае в лог включается адрес на NAT, на который идет трансляция с используемым блоком портов и IP-адрес источника.

Настройки:

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
```

Логирование каждого соединения с упаковкой нескольких информационных сообщений о событиях в сети в одно сообщение syslog. В данном случае в лог включаются все три адреса (назначения, трансляции, источника) с указанием порта. События упаковываются по несколько в одно сообщение.

Настройки:

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
```

Логирование каждого соединения без упаковки. В данном случае в лог включаются все три адреса (назначения, трансляции, источника) с указанием порта. Для каждого события создается новое сообщение.

Настройки:

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
```

Логирование блоков портов без упаковки. В данном случае в лог включается адрес на NAT, на который идет трансляция с используемым блоком портов и IP-адрес источника. Для каждого события создается новое сообщение.Настройки:

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
```

Логирование сообщений об освобождении блоков портов и трансляций. В данном случае последнее сообщение в примере говорит об освобождении порта 1.

Настройки:

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
```

Логирование в шестнадцатеричном формате.

Настройки:

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
```

Логирование в формате NetFlow

В EcoNAT есть возможность настроить логирование соединений по NetFlow v9 протоколу, при этом логируются соединения, но не логируется объем переданного по ним трафика. Используемые для этого дополнительные параметры ветки **connection_log** описаны в таблице ниже.

Таблица 10

Параметр	Описание
netflow_template_rate	Показывает, через какое количество пакетов передавать netflow template пакет. Возможные значения: once, 128, 512, 1K, 4K, 16K, 64K
netflow_options_rate	Показывает, через какое количество пакетов будут переданы netflow options и netflow options template пакеты. Возможные значения: once, 128, 512, 1K, 4K, 16K, 64K

Необходимые для настройки NetFlow логирования значения параметров, приведены в таблице ниже. Рекомендуется строго придерживаться указанных настроек.

Таблица 11

Параметр	Значение
log_format	netflow
log_on_release	on
log_individual_conn	on
use_hex_format	off
pack_msgs	on
log_server	Адрес netflow сервера и правильный номер порта
ip_address gateway	Адрес/маска подсети и шлюз

5.6.2 Настройка системного логирования

EcoNAT ведет запись всех действий пользователя в консоли. Логи этих действий передаются на сервер по управляющему интерфейсу. Настройки системного логирования находятся в ветке **system system_log**. Для того, чтобы включить логирование, в данной ветке должен быть установлен параметр ***enable***. Сервер, на который EcoNAT будет отправлять системные логи, указывается в параметре **log_servers**.

Имя EcoNAT, отображающееся в логах задаётся в параметре **hostname** с помощью команды **hostname “имя”**. Данное имя добавляется не только в системные логи, но и в логи соединений EcoNAT.

```
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
}
```

Степень подробности логов устанавливается параметром **verbose** который может как варьироваться, в зависимости от подсистем, так и быть одним для всех подсистем (**all**).

Уровни логирования:

- 0 – FATAL – только критические сообщения,
- 1 – ERROR – ошибки,
- 2 – WARN – предупреждения,
- 3 – INFO – информация.

Просмотр установленных в системе уровней логирования доступен по команде **show verboselvl**.

```
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
```

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

То есть, если настроен параметр **verbose all** равный ***3***, то будут логироваться сообщения всех уровней. Если для подсистемы указано значение параметра **verbose**, отличное от **all**, то будет приниматься в расчет наибольшая из этих двух величин.

Значения, выводимые командой **show verboselvl** могут отличаться от установленных в текущей конфигурации.

Для того чтобы оперативно изменить уровень логирования для какой-то подсистемы (или всех подсистем), используется команда **setlog <подсистема> <уровень логирования>**. Здесь уровни логирования задаются не цифрами, как при изменении конфигурации, а названиями. Изменения вступают в силу немедленно. После перезагрузки установки уровней логирования будут возвращены к значениям, указанным в активной конфигурации.

В приведенном ниже примере уровень логирования для всех подсистем изменяется на FATAL, соответственно, менее приоритетные события (WARNING, INFO, ERROR) логироваться не будут. При этом в конфигурации уровень логирования для всех подсистем остается INFO, и после перезагрузки системы будут снова логироваться все события.

Пример.

```
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
```

Сообщения логов представлены в формате: **<Дата, время> <Подсистема> [<Уровень логирования>]: <Сообщение>**.

Для просмотра системных логов используется команда **show logs**. По умолчанию, команда выводит на экран все записи логов. Для того чтобы вывод записей на экран шел порционно, используется конвейер **| more**. В таком режиме просмотра логов по нажатию любой клавиши на экран выводится несколько сообщений, по нажатию сочетания клавиш **[Ctrl+ C]** или **[Backspace]** система выходит из режима просмотра логов.

Для того чтобы увидеть сообщения определенного уровня, нужно указать желаемый уровень в команде. При этом будут выведены все сообщения, относящиеся к указанному уровню критичности и к более высоким. То есть, если указать ERROR, на просмотр будут выведены сообщения уровня ERROR и 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
```

Для того чтобы отфильтровать сообщения по подсистеме, нужно указать в команде **show logs** желаемую подсистему, команда при этом будет выглядеть следующим образом: **show logs facility <подсистема>**.

Пример:

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

5.6.3 QoE

Quality of Experience (QoE, оценка пользователем качества услуги) - интегральный параметр, представляющий собой общую приемлемость качества услуги, субъективно воспринимаемую конечным пользователем. В контексте EcoNAT под QoE понимается сводка информации о соединениях абонента. В данной сводке представлены показатели, характеризующие качество этого соединения. Эти показатели помогают выявлять проблемы с соединением у каждого конкретного абонента, что может использоваться оператором как инструмент повышения качества предоставляемых услуг и удержания абонентов.

Настройки QoE находятся в ветке конфигурационного дерева **system.qoe_log**.

Параметры настройки QoE описаны в таблице ниже.

Таблица 12

Параметр	Описание
enable / disable	Включение/отключение логирования QoE
server_ip_and_port	Адрес и порт syslog сервера, на который будет осуществляться логирование
ip_address	IP-адрес и маска подсети (через ‘/’) для виртуального канала, в который объединены логирующие сетевые интерфейсы
gateway	Шлюз по умолчанию для виртуального канала, в который объединены логирующие сетевые интерфейсы. Требуется в случае, если syslog-сервер, указанный в параметре **server_ip_and_port**, не находится в подсети, указанной в параметре **ip_address**

Пример настройки:

```
2:7:system.qoe_log# ls
enable
server_ip_and_port 192.168.1.2:514
ip_address 192.168.1.1/255.255.255.0
gateway 192.168.1.1
```

Пример записей на syslog-сервере:

```
2018-03-06T15:59:34+03:00 econat S 192.168.0.2 42650 192.168.0.2 42650
192.168.0.4 80   1 693620 0 3 1 5 0 0 0 0
2018-03-06T15:59:34+03:00 econat T 192.168.0.2 42650 192.168.0.2 42650
192.168.0.3 8080   1 698021 0 3 1 5 0 3 1 4
2018-03-06T16:02:28+03:00 econat S 192.168.0.2 42650 192.168.0.2 42650
192.168.0.4 80   1 698455 0 3 1 5 0 0 0 0
2018-03-06T16:02:28+03:00 econat T 192.168.0.2 42650 192.168.0.2 42650
192.168.0.3 8080   1 701788 0 3 1 5 0 3 1 4
```

В таблице ниже представлены значения полей записей на примере первой строки.

Таблица 13

№	Поле	Пример
1	Дата и время в формате UTC	2018-03-06T15:59:34+03:00
2	Hostname, указанный в **system_log**	econat
3	Тип записи: **T** - трасляция, **S** - сессия	S
4	Локальный IP-адрес абонента	192.168.0.2
5	Локальный порт абонента	42650
6	Глобальный IP-адрес абонента	192.168.0.2
7	Глобальный порт абонента	42650

№	Поле	Пример
8	IP-адрес назначения	192.168.0.4
9	Порт назначения	80
10	RTT между SYN/ACK и ACK в секундах	1
11	RTT между SYN/ACK и ACK в микросекундах	693620
12	Зарезервировано	0
13	Количество исходящих TCP пакетов с опцией 5	3
14	Количество групп подряд идущих исходящих TCP пакетов с опцией 5. Что с достаточной точностью равно количеству повторных передач исходящих TCP пакетов - TCP retransmissions	1
15	Общее количество исходящих TCP пакетов	5
16	Зарезервировано	0
17	Количество входящих TCP пакетов с опцией 5. Для записей типа S значение равно 0	0
18	Количество групп подряд идущих входящих TCP пакетов с опцией 5. С достаточной точностью равно количеству повторных передач входящих TCP пакетов - TCP retransmissions. Для записей типа S значение равно 0	0
19	Общее количество входящих TCP пакетов. Для записей типа S значение равно 0	0

5.6.4 Настройка сбора проходящих GET-запросов

На EcoNAT можно настроить сбор проходящих GET-запросов и их отправку в формате syslog.

Настройка сбора проходящих GET-запросов осуществляется в секции конфигурационного дерева **system clickstream**. В таблице ниже описаны параметры настройки, доступные в данной секции дерева.

Таблица 14

Параметр	Описание
enable или disable	Включение/отключение логирования GET-запросов
servers_ip_and_port	Адрес и порт syslog-сервера, на который будет осуществляться логирование
ip_address	IP-адрес и маска подсети (через ‘/’) для виртуального канала, в который объединены логирующие сетевые интерфейсы
gateway	Шлюз по умолчанию для виртуального канала, в который объединены логирующие сетевые интерфейсы. Требуется в случае, если syslog-сервер, указанный в параметре **server_ip_and_port**, не находится в подсети, указанной в параметре **ip_address**
source_port	Порт, с которого на syslog-сервер будут приходить сообщения
mtu	Размер MTU для отправки логирующих сообщений

Пример настройки:

```
EcoNAT:43:system.clickstream# ls
enable
servers_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
```

Пример записей на syslog-сервере.

```
2018-03-26T10:35:58.202901+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
```

```
2018-03-26T10:36:19.032814+00:00 192.168.1.1 192.168.000.002: 34906
192.168.000.003:00080 1522071378 econat     GET / HTTP/1.1#015#012Host:
mail.ru#015#012User-Agent: curl/7.55.0#015#012Accept: */*#015#012#015
2018-03-26T10:36:21.915058+00:00 192.168.1.1 192.168.000.002: 34908
192.168.000.003:00080 1522071381 econat     GET / HTTP/1.1#015#012Host:
ya.ru#015#012User-Agent: curl/7.55.0#015#012Accept: */*#015#012#015
```

В таблице ниже представлены значения полей записей на примере первой строки.

Таблица 15

№	Поле	Пример
1	Дата и время в формате UTC	2018-03-26T10:35:58.202901+00:00
2	IP-адрес устройства, с которого пришло сообщение	192.168.1.1
3	Локальный IP-адрес абонента	192.168.000.002
4	Локальный порт абонента	34904
5	Удаленный IP-адрес	192.168.000.003
6	Удаленный порт	00080
7	Timestamp	1522071357
8	Hostname, указанный в **system_log**	econat
9	Содержание GET-запроса	GET / HTTP/1.1#015#012Host: google.ru#015#012User-Agent: curl/7.55.0#015#012Accept: */*#015#012#015

Статистика по обработке пакетов с GET-запросами доступна по команде **show counters all** (подробнее см. в разделе Сервисные команды).

Данные счетчики описаны в таблице ниже.

Таблица 16

Счетчик	Описание
cr_clickstream_url_for_log	Подготовлено логирующих пакетов
cr_clickstream_send_one_packet	Отправлено логирующих пакетов
cr_clickstream_send_fragmented_packet	Отправлено фрагментированных логирующих пакетов
cr_clickstream_error_general	Количество ошибок при клонировании TCP-пакета
cr_clickstream_error_create_header	Количество ошибок при создании лог-пакета
cr_clickstream_warn_invalid_sequence	Количество полученных TCP-пакетов с некорректным значением поля sequence
cr_clickstream_error_no_session	Количество полученных TCP-пакетов, для которых не найдена запись в таблице сессий

Пример:

```
EcoNAT:10:> sh counters all
Printing counters...
Port statistics:
Port ge1 | dataplane: 38/0/0; d_bursts:0/0/0;  arp: 13/10; lacp: 0/0;
lldp: 0/4; unknown: 25/0; tx_drops: 0
Port ge2 | dataplane: 103/85/0; d_bursts:75/0/0;  arp: 2/2; lacp: 0/0;
lldp: 0/4; unknown: 21/21; tx_drops: 0
Port ge3 | dataplane: 81/107/0; d_bursts:87/0/0;  arp: 2/2; lacp: 0/0;
lldp: 0/4; unknown: 21/21; tx_drops: 0
Total statistics:
Core total, cr_l2_pass_unsupported_proto: 42
Core total, cr_pass_arp: 4
Core total, cr_translated_tcp: 138
Core total, cr_sess_tcp_alloc: 14
Core total, cr_sess_tcp_free: 3
Core total, cr_translated_egress_tcp_syn: 14
```

```
Core total, cr_translated_ingress_tcp_rst: 3
Core total, cr_translated_egress_tcp_fin: 11
Core total, cr_translated_ingress_tcp_fin: 11
Core total, cr_tcpstate_established: 14
Core total, cr_tcpstate_close_timeout: 3
Core total, cr_session_alloc: 14
Core total, cr_session_early_free_ingress: 14
Core total, cr_session_free: 3
Core total, cr_dpi_state_alloced: 1
Core total, cr_dpi_state_freed: 1
Core total, cr_allocated_logger_mbufs: 3
Core total, cr_allocated_arp_mbufs: 10
Core total, cr_allocated_lldp_mbufs: 4
Core total, cr_sent_logger_mbufs: 11
Core total, cr_egress_rx_queue_void: 1037129416
Core total, cr_egress_rx_queue_medium: 87
Core total, cr_ingress_rx_queue_void: 1037129432
Core total, cr_ingress_rx_queue_medium: 71
Core total, crs_urgent_conns.cc_medium: 14
Core total, crs_lazy_conns.cc_void: 14
Core total, cr_clickstream_url_for_log: 11
Core total, cr_clickstream_send_one_packet: 11
Core total, cr_clickstream_error_no_session: 11
Displays:
free_laddrs: 65536
free_logging_mbufs: 32669
free_mbufs0: 28477
```

5.7 Создание и удаление пользователей

В любой момент работы с конфигурацией можно создать пользователя (в конфигурационном режиме). Пользователи создаются при помощи команды **create user *<имя пользователя>* level *<права>* secret *<тип пароля>* “*<пароль>*”**.

Права (level):

- 0 – только просмотр;
- 3 – возможность выполнения команды **write**;
- 4 – редактирование конфигурации, загрузка конфигурации;
- 5 – сохранение конфигурации под отдельным именем, но не применение;
- 8 – применение конфигурации, запуск/остановка EcoNAT;
- 15 – полный доступ, включая управление пользователями.

Типы представления пароля (secret):

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

В конфигурации информация о пользователях выводится всегда с зашифрованным паролем (тип 5).

Также пользователя можно создать, перейдя в ветку дерева конфигурации **system users**. Синтаксис команды при этом будет: ***<имя пользователя>*** **level** ***<права>*** **secret** ***<тип пароля>*** **"*<пароль>*"**.

ПРИМЕР:

```
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
}
```

Для изменения уровня прав доступа пользователя, не обязательно менять его конфигурацию. Для этого можно воспользоваться командой **grant** ***<имя пользователя>*** ***<права>*** . Изменения в правах пользователя вступают в силу сразу после ввода команды.

```
MyEcoNAT:4:# grant user1 8
Для удаления пользователей используется команда no user <имя
пользователя>.
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/
}
```

В случае, если утерян пароль пользователя EcoNAT, пароль можно поменять, для этого необходимо подключиться через порт "Console" или "COM" к серийной консоли EcoNAT, и при загрузке нажимать кнопку **[i]**. При этом загружается консоль с именем пользователя CHPASS. В данном режиме работы консоли можно изменить пароли пользователей и сохранить настройки.

Для просмотра информации о соединении с сервером TACACS и текущей сессии пользователя используется команда **show tacacs .**

```
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
```

5.8 Остановка и перезагрузка системы

EcoNAT позволяет осуществлять горячую реконфигурацию без прекращения работы. Тем не менее, бывают случаи, когда необходимо перезагрузить оборудование. Например, понадобится перезагрузка EcoNAT, чтобы применить версию встроенного программного обеспечения (firmware), полученную в результате обновления.

Для перезагрузки EcoNAT используется команда **reboot**.После ввода команды, система попросит подтвердить перезагрузку: «**Confirm (y/N)**». Для подтверждения необходимо нажать **[y]**, в противном случае перезагрузка не будет выполнена.

Данный запрос подтверждения сопровождает все критичные действия.

Для выключения EcoNAT (например, в случае физического перемещения устройства на другую площадку), используется команда **poweroff**. После ввода команды, система попросит подтвердить выключение: «**Confirm (y/N)**». Для подтверждения необходимо нажать **[y]**, в противном случае выключение не будет выполнено.

5.9 Помощь пользователям

При обращении в техническую поддержку необходимо сообщать версию прошивки проблемного оборудования (отображается по вводу команды **show version**), а также информацию о лицензии проблемного оборудования (отображается по вводу команды **show license**). Пример вывода консоли по этим командам представлен ниже.

```
MyEcoNAT:1:# show version
EcoNAT 4080 series v2.1 (C) Ecotelecom [RDP.RU Ltd.] 2013-2016. All
rights reserved.
Firmware version: 2.1.2.0.1
S/N: 1C87764002B7
MyEcoNAT:2:# show license
CGNAT: Ok
BRAS: Not installed
DPI: Ok
RADIUS: Not installed
```

Для отображения детальной информации о версии используется команда **show version detail**.

```
EcoNAT:2:> show version detail
EcoNAT 4080 series v2.1 (C) Ecotelecom [RDP.RU Ltd.] 2013-2016. All
rights reserved.
Firmware version: 2.1.2.0.1
H1: b5ba452
H2: 5b80a1e
S/N: 1C87764002B7
```

5.10 Сервисные команды

5.10.1Информация о ресурсах памяти

Для просмотра информации об объеме свободной памяти устройства, воспользуйтесь командой **show memstat**.

```
MyEcoNAT:1:# show memstat
Data plane free/total memory: 21515MB / 30064MB
Control plane free/total memory: 2559MB / 3475MB
```

5.10.2Информация о ресурсах системы

Для просмотра информации об использовании ресурсов системы используется команда **show resources**.

```
EcoNAT:179:# 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%)
Session table   used/total: 0/33554432 (0.0%)
Translation table used/total: 0/41943040 (0.0%)
Abons table      used/total: 0/131072 (0.0%)
Free mbufs number on socket 0: 28642
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%)
```

Значение выводимых параметров представлено в таблице ниже.

Таблица 17

Параметр	Описание
CPU load	Загрузка процессора. Интерфейсы, в порядке убывания % загрузки процессора
Avg egress burst	Среднее значение всплесков egress направления
Avg ingress burst	Среднее значение всплесков ingress направления
Session table used/total	Счетчик заполнения таблицы сессий (текущее/максимальное)
Translation table used/total	Счетчик заполнения таблицы трансляций (текущее/максимальное)
Abons table used/total	Счетчик заполнения таблицы уникальных пользователей (текущее/максимальное)
Free mbufs number on socket 0	Количество свободных data-plane буферов на процессоре
Block allocation log size	Счетчик заполнения буфера сообщений **connection_log** (процент используемых)
Bras table used/total	Счетчик заполнения таблицы пользователей зарегистрированных на BRAS (текущее/максимальное)
DPI host buffers used/total	Счетчик заполнения буфера информации по доменному имени (текущее/максимальное)
DPI path buffers used/total	Счетчик заполнения буфера информации по URL, идущей после знака "?" (текущее/максимальное)
DPI state buffers used/total	Счетчик заполнения буфера информации по сессии (текущее/максимальное)
Awaiting syslog messages	Счетчик заполнения буфера сообщений **syslog**

5.10.3Информация о температурном режиме и вентиляторах

Для просмотра информации о температуре ядер используется команда **show temperature**.

```
EcoNAT:1:> 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
```

Для просмотра информации о скорости имеющихся в аппаратной платформе вентиляторов используется команда **show fan** (для моделей EcoNAT 4xxx). В выводе команды:

NIC<N> - вентиляторы на сетевых картах. При нормальной работе скорость вентилятора должна быть в пределах 6000-6398 RPM;

System fan <N> - вентиляторы в корпусе устройства. Скорость вентилятора зависит от температуры в корпусе устройства. При минимальной нагрузке скорость вентилятора должна быть в пределах 2600-4800 RPM. При максимальной нагрузке скорость вентилятора должна быть в пределах 16700-22300 RPM.

Пример:

```
EcoNAT:1:> 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
```

5.10.4Команды остановки/возобновления обработки пакетов

Для остановки приема/передачи EcoNAT пакетов используется команда **stop**. После ввода команды система попросит подтвердить остановку передачи пакетов: « **Confirm (y/ N)**». Для подтверждения необходимо нажать **[y]** , в противном случае остановка не будет выполнена. После выполнения команды **stop** устройство не выключается, команды конфигурации продолжают работать.

Для того чтобы EcoNAT возобновил обработку пакетов, необходимо ввести команду **start**.

5.10.5Ошибки выделения портов

Для просмотра информации об ошибках выделения порта cgnat пулов используется команда **show cgnat errors**.

Пример вывода команды.

```
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,
```

В выводе команды:

- **Debug counters** - отладочные счетчики для разработчиков,
- **proto** - тип протокола,
- **reason** - причина возникновения ошибки,
- **count** - значение счетчика ошибок.

Обозначения типов протоколов приведены в таблице ниже.

Таблица 18

Обозначение	Протоколы
0	UNKNOWN - протоколы, не вошедшие в перечисленные ниже категории
1	TCP
2	UDP
3	ICMP
4	L4_OPAQUE (RDP, IPV4, IPV6, ESP, AH, L2TP)
5	PPTP_GRE
6	ARP

Обозначения причин ошибок приведены в таблице ниже.

Таблица 19

Обозначение	Причина
1	Информация для разработчиков
2	Превышено количество портов для пользователя, параметр **limits_peruser**
3	Информация для разработчиков
4	Ошибка выделения **global_ip**
5	Информация для разработчиков
6	Информация для разработчиков
7	Информация для разработчиков
8	Ошибка выделения блока портов
9	Информация для разработчиков
0xA	Информация для разработчиков
0xB	Информация для разработчиков
0xC	Информация для разработчиков
0xD	Информация для разработчиков
0x10	Информация для разработчиков
0x11	Информация для разработчиков
0x12	Информация для разработчиков
0x13	Информация для разработчиков
0x14	Не удается распознать протокол
0x20	Информация для разработчиков
0x21	Записи не существует
0x22	Информация для разработчиков
0x23	Верхние TCP порты за пределами допустимого диапазона
0x24	Нижние TCP порты за пределами допустимого диапазона
0x25	Верхние нечетные UDP порты за пределами допустимого диапазона
0x26	Нижние нечетные UDP порты за пределами допустимого диапазона
0x27	Верхние четные UDP порты за пределами допустимого диапазона
0x28	Нижние четные UDP порты за пределами допустимого диапазона
0x29	ICMP порты за пределами допустимого диапазона
0x2A	PPTP_GRE порты за пределами допустимого диапазона
0x[PP]30	EGRESS трансляция не попала ни в один пул PP (номер пула где произошла ошибка)
0x[PP]31	INGRESS трансляция не попала ни в один пул PP (номер пула где произошла ошибка)
0x[PP]32	acl EGRESS трансляции не соответствует пулу PP (номер пула где произошла ошибка)
0x[PP]33	acl INGRESS трансляции не соответствует пулу PP (номер пула где произошла ошибка)

Обозначение	Причина
0x34	Трансляция не соответствует настройкам
0x35	Адрес не соответствует глобальным настройкам BNAT пула
0x36	Превышено количество соединений BNAT пула
0x37	Запрещены INGRESS соединения

5.10.6Счетчики

В EcoNAT действуют счетчики сбора системной статистики.

Для того чтобы просмотреть состояние всех счетчиков используется команда **show counters all**.

```
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
```

Для просмотра изменения состояния счетчиков за секунду используется команда **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
```

Для просмотра счетчиков по конкретному интерфейсу (или по всем интерфейсам) используется команда **show interface {all | <INT_NAME>} counters**, где **INT_NAME** - имя интерфейса.

```
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
```

...

Для просмотра информации о проходящем через интерфейс трафике используется команда **show interface <INT_NAME> traffic [monitor]**, где **INT_NAME** - имя интерфейса**, monitor** - просмотр в режиме реального времени. Для выхода из режима **monitor** необходимо нажать на клавиатуре **[Ctrl+C]** или **[Esc]**, или **[Q]**.

```
MyEcoNAT:10:> show interface all traffic monitor
Interface  Packets In/Out per sec   Bytes In/Out per sec  Errors In/Out
per sec
---------  ----------------------   --------------------  --------------
-------
  ge1            0 / 0           0 / 0          0 / 0
  ge2            0 / 0           0 / 0          0 / 0
  ge3            0 / 0           0 / 0          0 / 0
  ge4            0 / 0           0 / 0          0 / 0
  ge5            0 / 0           0 / 0          0 / 0
  ge6            0 / 0           0 / 0          0 / 0
  te7            0 / 0           0 / 0          0 / 0
  te8            0 / 0           0 / 0          0 / 0
Press Ctrl+C / Esc / q to stop.
```

Для того, чтобы сбросить значения счетчиков, используется команда **clear counters**.

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

Для просмотра общей статистики по сессиям используется команда **show statistics**.

```
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
```

5.11 Операции с прошивкой

В EcoNAT предусмотрено несколько разделов жесткого диска (партиций) для встроенного программного обеспечения (прошивки). Это два основных раздела, в которых

может быть установлена какая-либо версия прошивки: PRIM1 и PRIM2, - и служебный раздел FALLBACK.

При помощи команды **firmware status** можно увидеть, какие версии прошивки установлены в партициях и их статус.

Например:

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

В выводе команды **firmware status**:

- LABEL - раздел,
- VERSION - версия прошивки, установленная в этом разделе,
- CURR - раздел, с которого произведена загрузка (текущий раздел),
- BOOT - раздел, с которого EcoNAT загрузится при перезапуске.

5.11.1Обновление прошивки

Для обновления прошивки необходимо передать информацию об обновляемом устройстве EcoNAT производителю.

Для того чтобы получить необходимую информацию в CLI EcoNAT используется команда **copy hwinfo <адрес>/<имя файла>**, которая формирует и копирует на удаленный сервер файл с информацией об устройстве. При помощи данной команды информация может быть скопирована на HTTP, FTP или TFTP-сервер. В случае, если на сервере включена авторизация, адрес необходимо вводить вместе с логином и паролем: **ftp://user:password@myserver.ru/filename** .

После выгрузки информационного файла, он должен быть передан производителю для генерации обновления.

Когда файл обновления готов, его необходимо загрузить в устройство при помощи команды **firmware download <адрес>/<имя файла>**. При помощи данной команды файл прошивки может быть скопирован с HTTP, FTP или TFTP-сервера. В случае, если на сервере включена авторизация, адрес необходимо вводить вместе с логином и паролем: **ftp://user:password@myserver.ru/filename** .

Для установки скачанного обновления прошивки используется команда **firmware install**.

ВНИМАНИЕ! Во время инсталляции обновления, CLI не будет реагировать на другие команды.

Обновление будет установлено в неактивном разделе жесткого диска. Для того, чтобы обновление вступило в силу, необходима перезагрузка устройства при помощи команды **reboot**.

При инсталляции обновления будет автоматически установлен флаг загрузки с неактивного раздела, куда установлена новая версия.

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

Если в момент скачивания прошивки будет потеряна связь с сервером, процесс обновления будет заблокирован системой. Для сброса заблокированного процесса используется команда **firmware unlock**.

5.11.2Изменение параметров перезагрузки

В случае, если необходимо перезапустить устройство с прошивки, которая не активна на данный момент, используется команда **firmware rollback**.

Например:

```
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*    .       .
```

Если после первого вызова данной команды попытаться вызвать ее повторно, то никаких изменений не произойдет. То есть EcoNAT все так же будет получать команду перезапуститься с неактивной в данный момент прошивкой.

Для отмены запуска с неактивной прошивкой (после обновления или использования команды **firmware rollback**) предусмотрена команда **firmware revert**.

В продолжение предыдущего примера:

```
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*    .       .
```

5.12 Настройка TACACS

Настройки соединения с TACACS-сервером находятся в ветке конфигурационного дерева **system tacacs**. Для того, чтобы активировать подключение устройства к TACACS-серверу, в данной ветке необходимо установить параметр **enable**.

В EcoNAT можно настроить два TACACS-сервера (primary и secondary) - **server1** и **server2**.

Список настраиваемых параметров подключения к TACACS-серверу приведен в таблице ниже.

Таблица 20

Параметр	Описание
enable | disable	Активно или нет подключение к TACACS-серверу
server <IP address>	Адрес TACACS-сервера. Может быть указан IP-адрес или доменное имя
secret <PASS>	Пароль для подключения к TACACS-серверу. Хранится в конфигурации зашифрованном виде
fallback {on | off}	В случае, если авторизация по TACACS не прошла, будет ли выполнена попытка найти пользователя в локальной базе: **on** - поиск по локальной базе включен, **off** - поиск по локальной базе выключен
accounting {on | off}	Включение и выключение аккаунтинга пользователей, авторизующихся через TACACS
service_type <TYPE>	Тип сервиса. Должен совпадать с типом сервиса, указанным в настройках TACACS-сервера
protocol <PROTOCOL>	Протокол. Должен совпадать с указанным в настройках TACACS-сервера

Пример настроек:

```
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"
}
```

Для просмотра информации о текущей сессии существует команда **show tacacs**. Команда выводит на консоль информацию о текущей сессии и о том, когда было последнее подключение к TACACS-серверу.

```
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 Конфигурирование NAT

В настоящем разделе описаны настройки функционала CG-NAT.

6.1 Интерфейсы

В логике EcoNAT сетевые интерфейсы представлены объектами типа **interface**.

Имена интерфейсов начинаются с префикса, зависящего от типа передатчика:

- названия интерфейсов с установленными оптическими модулями SFP+ начинаются с префикса te, например, te10;
- названия «медных» интерфейсов 1GB начинаются с префикса **ge**, например, ge3.

Названия в системе соответствуют названиям сетевых интерфейсов, представленным в разделе "".

Список интерфейсов и их состояние можно посмотреть в ветке конфигурационного дерева **system interfaces**.

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

В EcoNAT возможно как физическое, так и административное включение/отключение интерфейса. Для включения интерфейса используется команда **interface <INT_NAME> up**, где **INT_NAME** - имя интерфейса. Для выключения интерфейса используется команда **interface <INT_NAME> down**, где **INT_NAME** - имя интерфейса.

Интерфейсу может быть присвоено описание. Для этого необходимо перейти в контекст настройки данного интерфейса и ввести команду **description <DESCR>**, где **DESCR** - описание длиной от 1 до 240 символов.

Пример:

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

В выводе команды **show interface brief** отображаются только первые 50 символов описания.

```
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       -
```

Отображение в команде **show interface ge1**:

```
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
```

6.1.1 Onstick

В EcoNAT реализована поддержка функционала Onstick (объединение LAN и WAN в один порт).

Для включения функционала необходимо наличие соответствующей лицензии (подробнее о проверке лицензии, см. раздел "Помощь пользователям").

В секции конфигурационного дерева **interfaces** осуществляется включение режима Onstick и хранятся настройки интерфейсов для данного режима. Данный режим применяется сразу ко всем интерфейсам EcoNAT.

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

Таблица 21

Параметр	Описание
interface_mode	Обязательный параметр, который указывает, какой режим будет использован. Значения параметра: **default** - EcoNAT работает в режиме разделения интерфейсов на глобальные и локальные; **onstick** - все интерфейсы EcoNAT работают в режиме объединения LAN и WAN
geN	Перечисление интерфейсов EcoNAT
enable/disable	Административное включение/выключение интерфейса
vlan_local	Локальный тег для Onstick
vlan_global	Глобальный тег для Onstick
description	Описание интерфейса. От 1 до 240 символов

Для работы функционала Onstick, необходимо в секции **nat_defaults** указать **vlan_mode vlan** (см. раздел "Пулы и ACL"), чтобы включить поддержку тегированного трафика.

ВНИМАНИЕ, режим Onstick будет применен только после перезагрузки.

Поэтому после данных настроек необходимо выполнить следующие команды:

- применить конфигурацию командой **apply**,
- сохранить внесенные изменения командой **write**,
- перезагрузить устройство командой **reboot**.

Возможна ситуация, когда на подключенном к EcoNAT маршрутизаторе понадобится две статические ARP-записи для каждого VLAN-интерфейса: локального и глобального соответственно. Такая ситуация может возникнуть, если на подключенном маршрутизаторе выделяется один MAC-адрес для обоих VLAN-интерфейсов одного порта или группы портов, объединенных в LAG.

6.1.2 Команды просмотра интерфейсов

Для просмотра краткой информации о состоянии интерфейсов, используется команда **show interface brief**. Команда выводит на консоль таблицу, где в колонке Status отображается текущее состояние интерфейса:

- active – интерфейс в активном состоянии,
- down – интерфейс не подсоединен,
- disabled – интерфейс выключен через CLI EcoNAT.

```
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
```

Полную информацию об интерфейсах можно получить, воспользовавшись командой **show interface all**.

```
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
…
```

С помощью команды **show interface transceiver all** (или **show sfp all**) можно посмотреть информацию о SFP и SFP+ модулях, включая DDM информацию. Для портов с «медным» интерфейсом данная информация недоступна.

```
MyEcoNAT:6:# show interface transceiver all
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
…
```

Также можно указать конкретный интерфейс, чтобы вывести информацию о соответствующем SFP модуле. Например: **show interface transceiver *te18***. Для просмотра информации о MNGT-интерфейсе используется команда **show interface mng**.

```
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
```

Для просмотра информации о ARP используется команда **show arp all** или команда **show arp <INTERFACE>** (для просмотра информации о конкретном интерфейсе). Команда выводит на консоль информацию о MAC-адресе интерфейса, информацию о виртуальном канале, в который объединены логирующие сетевые интерфейсы (EcoNAT EtherChannel), и информацию о сервере, на который отправляются логи.

Пример.

```
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
```

6.2 Принципы работы NAT

EcoNAT осуществляет трансляцию адресов, передавая данные между сетевыми интерфейсами, которые объединены в пары. В каждой паре сетевых интерфейсов, один из них,

принадлежащий private (локальной) стороне NAT, имеет чётный номер, а второй, принадлежащий public (глобальной) стороне NAT – нечётный номер.

Например, интерфейс 8 является private (соединён с внутренней сетью), а интерфейс 7 – public (на нём размещаются глобальные адреса).

Данные, пришедшие на один из сетевых интерфейсов пары, покидают NAT через другой интерфейс из этой же пары (см. рисунок ниже). В случае, если настроен hairpinning, данные могут покинуть NAT через тот же интерфейс, на который они поступили (см. раздел "Пулы и ACL").

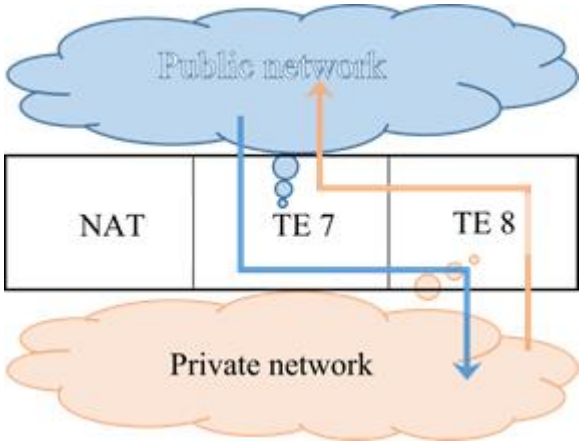

Рисунок 8

EcoNAT поддерживает LLDP протокол и регулярно высылает в порты LLDP пакеты, уведомляющие о присутствии EcoNAT.

При этом, можно посмотреть соседние устройства, использующие LLDP протокол. Для этого выполните команду **show neighbours <*имя интерфейса*>** для конкретного интерфейса, или **show neighbours all** для всех интерфейсов сразу.

```
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
```

6.3 Пулы и ACL

Основным элементом конфигурации EcoNAT являются так называемые пулы (pool), которые характеризуются типами трансляции и набором внешних (глобальных) IPv4 адресов. Каждому пулу назначается его приоритет, причем, чем меньше численное значение приоритета, тем раньше данный пул обрабатывается. С каждым пулом связан ACL, который

содержит в себе критерии выбора данного пула в зависимости от содержимого полей поступившего IP-пакета.

ВНИМАНИЕ: Нельзя назначать одинаковый приоритет нескольким пулам! Это приведёт к тому, что будет использоваться только тот пул, который был создан первым. Остальные пулы будут игнорироваться.

Каждый пул может быть либо активен (***enable***), либо неактивен (***disable***). Имена пулов всегда начинаются с префикса **pool**.

6.3.1 Общие настройки

В ветке конфигурации **system nat_defaults** находятся общие настройки системы и настройки, применяемые по умолчанию ко всем вновь создаваемым пулам (блоки timeouts_inactivity и limits_peruser копируются в пул при его создании). Описание параметров данной ветки конфигурации приведено в таблице ниже.

Таблица 22

Параметр	Описание
vlan_mode	Обрабатывает/анализирует пакеты до указанного уровня инкапсуляции. Варианты значений параметра: untagged, vlan, qinq.
alg ftp	Включает опцию ALG для протокола FTP. Варианты значений параметра: on/off
alg pptp	Включает опцию ALG для протокола PPTP. Варианты значений параметра: on/off
alg rtsp	Включает опцию ALG для протокола RTSP. Варианты значений параметра: on/off
alg sip	Включает опцию ALG для протокола SIP. Варианты значений параметра: on/off
alg alg_on_bnat	Включает опцию ALG для статического NAT. Варианты значений параметра: on/off
sessions_per_translation	Количество активных сессий на трансляцию
udp_inbound_refresh	Включает обновление UDP трансляций ingress (входящими) пакетами. Варианты значений параметра: on/off
l2mtu	Максимальный размер MTU на входе. Значение указывается для L2 с учетом заголовка. Значение по умолчанию - 1522, максимальное значение - 9692
port_block_size	Размер блока портов. Значение по умолчанию – 128. Изменять значение параметра не рекомендуется
portlimit_low	Значение используемого диапазона "нижних" портов (до 1024-го) для каждого пользователя. Варианты значений параметра: nolimit, 64, 128, 256, 512
low_to_all_udp	Позволяет использовать порты из верхнего диапазона, если порты из нижнего диапазона исчерпаны. Варианты значений параметра: on/off
lldp_hostname ""	Имя хоста, которое будет использоваться для LLDP оповещений
timeouts_inactivity {}	В этом разделе задаются параметры времени неактивности (в секундах) для разных протоколов и состояний TCP, по истечении которого неиспользуемое соединение будет закрыто принудительно.
timeouts_inactivity translation	Задаёт время в секундах до истечения которого, даже в случае неактивности пользователя, ему будет гарантировано выделение портов из одного и того же глобального IP. Рекомендованное значение по умолчанию 86400
timeouts_inactivity udp	Таймаут неактивности в секундах для UDP соединений. По истечении этого таймаута порт на глобальном IP высвобождается. По умолчанию 300

Параметр	Описание
timeouts_inactivity icmp	Таймаут неактивности в секундах для ICMP соединений. По истечении этого таймаута порт на глобальном IP высвобождается. По умолчанию 60
timeouts_inactivity tcp_handshake	Таймаут трансляции, созданной пакетом TCP с флагом SYN (неустановившееся TCP соединение) секундах. По умолчанию - 4
timeouts_inactivity tcp_active	Таймаут неактивности в секундах для установленных TCP-соединений в состоянии ESTABLISHED. По истечении этого таймаута порт на глобальном IP высвобождается. По умолчанию 300
timeouts_inactivity tcp_final	Таймаут для завершения TCP сессий в секундах. По умолчанию 240
timeouts_inactivity tcp_reset	Таймаут для сброса TCP сессий в секундах. По умолчанию 4
timeouts_inactivity tcp_session_active	Таймаут неактивности в секундах для активных TCP-сессий. По умолчанию 120
timeouts_inactivity udp_session	Таймаут неактивности в секундах для активных UDP-сессий. По умолчанию 120
timeouts_inactivity icmp_session	Таймаут неактивности в секундах для активных ICMP-сессий. По умолчанию 120
timeouts_inactivity other	Таймаут неактивности в секундах для прочих соединений по IP протоколу (например, для GRE). По истечении этого параметра протокол на глобальном IP высвобождается. По умолчанию 300. (Применимо только к NAT и 1:1 типам пулов)
timeouts_inactivity special	Таймаут неактивности в секундах для протоколов, которым требуется большее значение таймаута. По умолчанию 600
timeouts_inactivity special_tcp_ports ( )	TCP порты, к которым применяется увеличенное значение таймаута
limits_peruser {}	Ограничения числа портов для пользователей
limits_peruser portlimit_icmp	Этот параметр описывает максимальное количество одновременно существующих ICMP сессий для пользователя
limits_peruser portlimit_tcp limits_peruser portlimit_udp	Лимит числа глобальных (внешних) портов, которые могут быть выделены одному пользователю (локальному IP). Рекомендуется задавать значения, кратные 64, от 64 до 32256. Операторам связи имеет смысл назначать для обычных пользователей (физических лиц): от 1024 до 4096. Значения менее 1024 могут приводить к проблемам с работоспособностью некоторых приложений. Значение более 32256 может привести к тому, что один пользователь сможет исчерпать порты IP-адреса. Для пользователей, особенно требовательных к числу портов, имеет смысл завести отдельный cgnat пул с меньшим коэффициентом уплотнения (меньше локальных IP на один глобальный), либо использовать nat пул для выделения пользователю целого IP со всеми портами на период его активности

Параметры **tcp_ session_ timeout** , **udp_ session_ timeout** , **icmp_ session_ timeout** срабатывают, когда создается новая трансляция и в ней появляется сессия. Все последующие сессии в данной трансляции создаются с параметрами из раздела **timeouts_inactivity** (автоматически копируемыми из **system nat_defaults**) .

Параметр **vlan_mode** может принимать значения: **untagged**, **vlan**, **qinq**. Где **untagged** означает, что EcoNAT будет обрабатывать только нетегированный трафик, **vlan** – нетегированный и с одной меткой, **qinq** – нетегированный, с одной либо с двумя метками.

По умолчанию (значение параметра **untagged**) EcoNAT пропускает прозрачно всё, что отличается от стандартного IP, для того чтобы беспрепятственно передавался трафик по протоколам типа BFD, OSPF, BGP и так далее. В том числе, IP-пакеты с опциями (кроме

фрагментированных IP-пакетов с опциями), а также, тегированный трафик пропускаются без натирования.

При включении режима **vlan**, EcoNAT увидит метку в L2 заголовке, заглянет под неё и перенаправит IP в соответствии с имеющимися правилами с той же меткой. При этом IP-адреса под различными метками не должны пересекаться, так как для EcoNAT это будет восприниматься как один и тот же абонент. Например, если придет пакет с IP-адресом 192.168.1.100 и с меткой VLAN 100 и пакет с IP-адресом 192.168.1.100 и с меткой VLAN 200, то фактически это будут разные абоненты, но для EcoNAT, это будет один и тот же адрес абонента. Таким образом может быть нарушена передача трафика.

Для очистки таблицы трансляций используется команда clear session**s all**.

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

6.3.2 Создание нового пула

Для создания пулов используется команда **create pool <*имя пула*>**. При этом создаётся cgnat пул с типовыми параметрами (подробнее о cgnat пулах см. в соответствующем разделе) и именем ***poolИМЯ_ПУЛА*** (добавляется префикс «pool»). Если заданное имя пула уже начинается с префикса «pool», например, «pooltest», то имя не меняется, и в дальнейшем этот пул будет располагаться в ветке конфигурации **pools** с именем **pooltest**. При попытке создать пул с уже существующим именем, пул не будет создан. Например, если после изменения параметров **pooltest** попытаться создать пул с названием «test» (которое будет автоматически изменено на «pooltest»), конфигурация пула **pooltest** не изменится, а новый пул не будет создан.

После чего значения параметров пула можно изменить, перейдя в ветку дерева конфигурации, соответствующую данному пулу (подробнее о дереве конфигурации см. в разделе "Конфигурация").

ПРИМЕР:

```
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
}
```

Как видно из примера, при создании нового пула к нему не осуществляется привязки ACL.

Параметры пула описаны в таблице ниже.

Таблица 23

Параметр	Описание
type	Тип пула: cgnat, static, nat, fake
enable или disable	Состояние пула
acl	Связанные с пулом ACL
priopity	Приоритет пула
global_ip ( )	Глобальные IP-адреса, относящиеся к пулу
port_range	Диапазон внешних портов, доступных для использования на каждом глобальном IP-адресе, принадлежащем cgnat пулу. Рекомендованное значение (диапазон): 1024:65535. При таких настройках в каждом глобальном IP будет доступно 64512 UDP и столько же TCP портов
global_map ( )	Соответствие между глобальными и локальными IP-адресами. Адреса задаются парами в формате <локальный адрес>-<глобальный адрес>. Параметр действителен для пулов типа static
hairpin	Разрешает hairpinning. Если адрес во внешней сети совпадает с глобальным адресом одного из пулов, EcoNAT выполнит двойную трансляцию, не отправляя пакет вовне (на WAN). Hairpinning работает только в случае, если он разрешён в обоих пулах, где находятся пользователи, связанные таким образом
allow_external_connect	Разрешить соединения извне. Параметр действителен для пулов типа nat
connection_logging	Логирование соединений: включено (on) или выключено (off)
randomize_ports	Разрешает выделение портов из блока в случайном порядке (on). Если выключено (off), то порты выделяются поочередно
timeouts_inactivity	В этом разделе задаются параметры времени неактивности (в секундах) для разных протоколов и состояний TCP, по истечении которого неиспользуемое соединение будет закрыто принудительно. Эти параметры не рекомендуется настраивать без необходимости, можно использовать оптимальные значения «по умолчанию»
timeouts_inactivity translation	Задаёт время в секундах до истечения которого, даже в случае неактивности пользователя, ему будет гарантировано выделение портов из одного и того же глобального IP. Рекомендованное значение по умолчанию 86400

Параметр	Описание
timeouts_inactivity tcp_handshake	Таймаут трансляции, созданной пакетом TCP с флагом SYN (неустановившееся TCP соединение) секундах. По умолчанию 4
timeouts_inactivity tcp_active	Таймаут неактивности в секундах для установленных TCP соединений в состоянии ESTABLISHED. По истечении этого таймаута порт на глобальном IP высвобождается. По умолчанию 300
timeouts_inactivity tcp_final	Таймаут для завершения TCP сессий в секундах. По умолчанию 240
timeouts_inactivity tcp_reset	Таймаут для сброса TCP сессий в секундах. По умолчанию 4
timeouts_inactivity tcp_session_active	Таймаут неактивности в секундах для активных TCP-сессий. По умолчанию 120
timeouts_inactivity udp_session	Таймаут неактивности в секундах для активных UDP-сессий. По умолчанию 120
timeouts_inactivity icmp_session	Таймаут неактивности в секундах для активных ICMP-сессий. По умолчанию 120
timeouts_inactivity other	Таймаут неактивности в секундах для прочих соединений по IP протоколу (например, для GRE). По истечении этого параметра протокол на глобальном IP высвобождается. По умолчанию 300. (Применимо только к NAT и 1:1 типам пулов)
timeouts_inactivity special	Таймаут неактивности в секундах для протоколов, которым требуется большее значение таймаута. По умолчанию 600
timeouts_inactivity special_tcp_ports ( )	TCP порты, к которым применяется увеличенное значение таймаута
limits_peruser	Ограничения числа портов для пользователей
limits_peruser portlimit_tcp limits_peruser portlimit_udp	Лимит числа глобальных (внешних) портов, которые могут быть выделены одному пользователю (локальному IP). Рекомендуется задавать значения, кратные 64, от 64 до 32256. Операторам связи имеет смысл назначать для обычных пользователей (физических лиц): от 1024 до 4096. Значения менее 1024 могут приводить к проблемам с работоспособностью некоторых приложений. Значение более 32256 может привести к тому, что один пользователь сможет исчерпать порты IP-адреса. Для пользователей, особенно требовательных к числу портов, имеет смысл завести отдельный cgnat пул с меньшим коэффициентом уплотнения (меньше локальных IP на один глобальный), либо использовать nat пул для выделения пользователю целого IP со всеми портами на период его активности
limits_peruser portlimit_icmp	Этот параметр описывает максимальное количество одновременно существующих ICMP сессий для пользователя

Данные параметры доступны в зависимости от типа пула. Ниже представлена таблица параметров, доступных для каждого типа пула.

Таблица 24

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

Параметры	cgnat	nat	static	fake
timeouts_inactivity	+	+	+	+
limits_peruser	+			

После создания пула, ему нужно добавить глобальные IPv4 адреса, которые будет использовать этот пул. Для этого войдите в режим редактирования пула с помощью команды **goto *<имя пула>*** или **edit *<имя пула>*** и вызовите команду **global_ip add *<глобальный IP-адрес>***. Для того чтобы удалить IP-адрес, в режиме редактирования пула вызовите команду **global_ip remove *<глобальный IP-адрес>***.

```
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#
```

Для удобства работы с массивами IP-адресов предусмотрен альтернативный вариант изменения параметра **global _ ip .** Для этого необходимо перейти в редактируемый пул в ветке конфигурационного дерева, войти в параметр **global _ ip** и воспользоваться командами **add** и **remove** или символьными командами **+=** для добавления адресов, **-=** для удаления адресов. Для того чтобы добавить/удалить несколько адресов сразу, их можно ввести внутри скобок, разделяя переводом строки. Для того чтобы внести адреса в пустой массив или полностью заменить имеющийся массив, введите список адресов в скобках, как указано выше, без команды **add** или символьной команды **+=**.

```
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
 …
 }
```

Созданный пул можно продиагностировать с помощью команды **analize <*имя пула*>**. Вывод команды покажет, чего не хватает для нормальной работы пула.

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

Если с пулом все хорошо, не будет выведено никаких сообщений:

```
MyEcoNAT:1:# analize pooltest
MyEcoNAT:2:#
```

Пул можно деактивировать при помощи команды **disable**. В этом случае его конфигурационная информация остается, а сам пул не будет применён. Деактивированный пул считается командой **analize** хорошим в любом случае.

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

Чтобы активировать пул, вызовите команду **enable**:

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

6.3.3 Создание нового ACL

После того как пул создан, надо создать ACL, который будет определять, какие пакеты будут попадать в этот пул. Для создания ACL используется команда **create acl <*имя ACL*>**. При этом создаётся пустой список с именем ***aclИМЯ_ACL***, имя которого форматируется аналогично имени пула (см. выше). Для дальнейшего редактирования списка используется команда **edit <*имя ACL*>** или **goto <*имя ACL*>**.

После перехода к конкретной ACL начинается формирование списка правил (синтаксис правил условно изображен на рисунке ниже).

номер правила	разрешить/ запретить	протокол	источник	получатель
10	allow	ip	194.85.16.0/24	any

Рисунок 9

Каждое правило вводится, начиная с его номера, определяющего порядок применения правила. Рекомендуется, чтобы сначала шли номера частных правил, а потом – общих, иначе возможно нежелательное срабатывание правил. Если порядок создаваемого правила совпадет с уже существующим правилом в этом ACL, то правило будет заменено новой версией.

Следующим элементом правила является режим обработки пакета (тип правила). Правила делятся на разрешающие (***allow*** или ***permit***) и запрещающие (***deny***). Разрешающее правило указывает на то, что пакеты данного типа будут транслироваться данным пулом. Запрещающее правило указывает на то, что пакеты данного типа не обрабатываются данным пулом и происходит переход к следующему пулу для обработки.

Далее указывается протокол, пакеты которого обрабатываются. Если протокол не указан, то по умолчанию считается что это протокол IPv4. Указываемое значение ***ip*** означает любые протоколы 4го уровня модели OSI внутри IPv4 пакетов. В текущей версии продукта работает только ***ip***. Остальные варианты (***tcp***, ***udp***, ***icmp***, ***proto 17***) являются синонимами ***ip***.

Далее указывается адрес источника пакетов (source) и адрес получателя (destination). В начале каждого блока могут ставиться ключевые слова **src** и **dst**. Задавать диапазон адресов для ACL можно в виде одиночного адреса ***host*** (например, 1.1.1.1), адреса сети ***net*** (например, 10.10.10.0/24) или путем указания непрерывного диапазона адресов ***range*** (например, 12.12.12.1-12.12.12.5) либо ***any***. ***Any*** – означает множество всех возможные адресов, т.е. 0.0.0.0/0. Ключевые слова ***host***, ***net***, ***range*** не являются обязательными при вводе правила, в этом случае они добавляются в созданное правило автоматически, исходя из заданного диапазона адресов (см. пример ниже).

Так как сам по себе список правил не имеет значения, он должен быть привязан к конкретному пулу. Установка привязки осуществляется с помощью команды **use *<имя ACL>* *<имя пула>***.

ПРИМЕР:

```
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 ( )
…
```

В случае, если не указан destination адрес, то по умолчанию считается, что он ***any***.

```
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#
```

В случае, если не указан source адрес, то по умолчанию считается, что он ***any***, при этом в команде обязательно должно быть использовано ключевое слово ***dst***.

```
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#
```

В случае, если нужно разрешить все возможные адреса, команда будет выглядеть: ***10 allow any any***.

6.3.4 Порядок определения пула для пакета

При поступлении нового IP-пакета (начале новой сессии), пулы обрабатываются в порядке их приоритета: чем значение приоритета меньше – тем раньше обрабатывается данный пул. Например, если имеются пулы с приоритетами: 200, 150, 250, – то первым будет обрабатываться пул с приоритетом 150.

Далее анализируется ACL, связанный с обрабатываемым пулом и проверяются правила, содержащиеся в этом ACL.

Если параметры полученного пакета удовлетворяют условиям правила с типом **allow** (разрешить), то пакет будет обработан данным пулом. Если же параметры полученного пакета удовлетворяют условиям правила с типом **deny**, то этот пул больше не будет рассматриваться для данного пакета, а будут рассматриваться следующие в порядке приоритета пулы. Если пакет не удовлетворяет условиям текущего правила ACL, то анализируется следующее правило для данного пула, или (если правил больше нет) происходит переход к следующему пулу в порядке приоритета. Если же пулов больше не осталось, то пакет IPv4 передаётся без трансляции (как через провод).

6.3.5 Cgnat пул

Cgnat пул осуществляет Carrier-grade NAPT трансляцию, при которой транслируются и адреса, и порты. Адреса и блоки портов для клиентских соединений распределяются динамически. Политика распределения адресов стремится к равномерному заполнению портов каждого глобального адреса. Это дает максимальный выигрыш по эффективности использования IP-адресов. Параметры, доступные для настройки данного типа пулов, и их описание приведены выше, в разделе "Пулы и ACL".

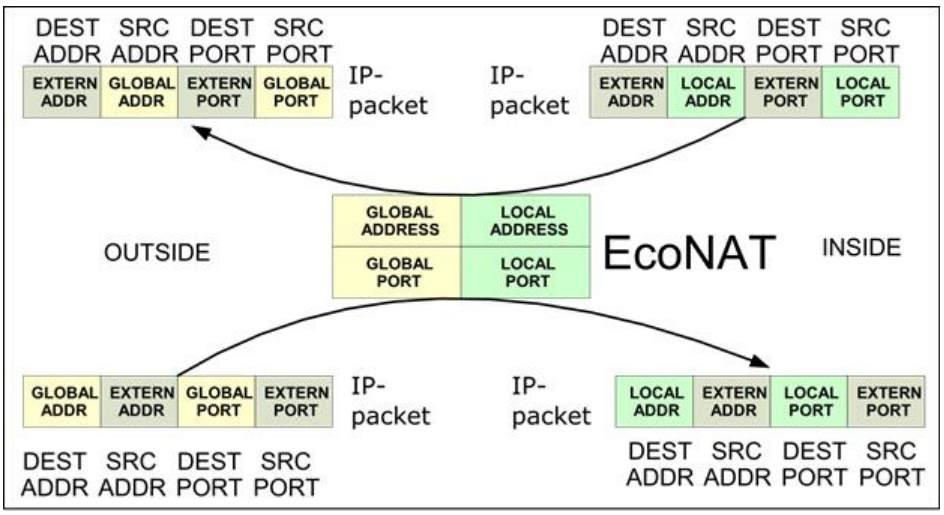

Рисунок 10

6.3.6 Nat пул

Nat пул, иначе именуемый как basic-NAT, осуществляет только трансляцию адресов (порты не транслируются). Параметры, доступные для настройки данного типа пулов, и их описание приведены выше, в разделе "Пулы и ACL".

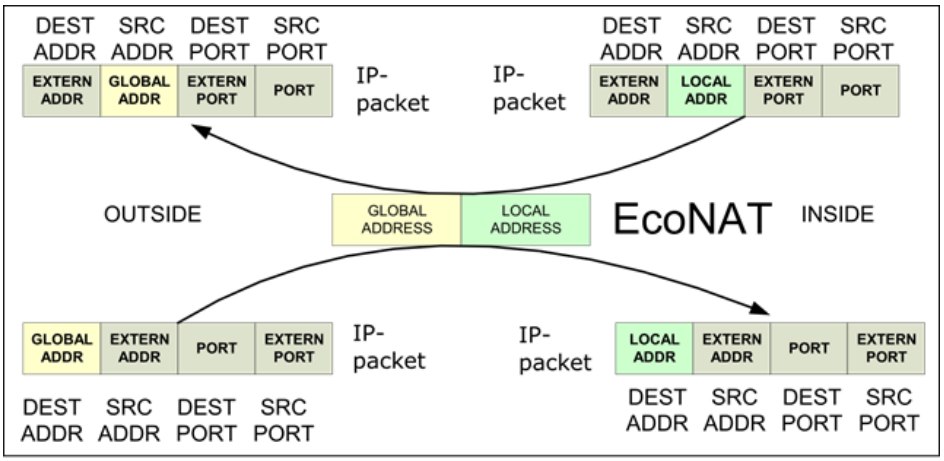

Рисунок 11

По умолчанию при создании пула создаётся пул типа ***cgnat***, но мы можем после создания изменить тип пула, присваивая соответствующие значения параметру **type**, находящемуся в пуле (например, ***nat***).

Часть параметров, характерная для ***cgnat*** пула, исчезает после изменения его типа на тип ***nat***. Также, появляется новый параметр **allow_external_connect**, который разрешает соединения снаружи. Если включить **allow_external_connect *on***, то трансляции смогут создаваться «по инициативе» внешних хостов. Это увеличивает доступность для peer-to-peer сетей, так как к вашим абонентам смогут подсоединяться извне по любым портам (если, конечно, порт открыт на хосте).

Обычно имеет смысл делать два пула типа ***nat***: один для тех абонентов, которым нужны соединения, инициируемые снаружи (хотят активно раздавать торренты), а другой – для тех абонентов, кто хочет инициировать соединения только по собственной инициативе.

```
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#
```

6.3.7 Static пул (1_to_1)

Статический пул – это такой пул, в котором трансляции адресов заданы административно. Параметры, доступные для настройки данного типа пулов, и их описание приведены выше, в разделе "Пулы и ACL".

Каждому локальному адресу пула однозначно сопоставлен глобальный адрес, при этом трансляции портов не производится. Вместо списка IPv4 глобальных адресов, принадлежащих пулу (вместо параметра **global_ip**) находится список 1:1 трансляций (параметр **global_map**).

Трансляции в параметре **global_map** задаются в виде: ***<локальный адрес>-<глобальный адрес>***.

```
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#
```

Для статического пула можно не указывать ACL, в этом случае неявно предполагается, что для пула действует одно правило: **allow ip src <*локальный адрес*> dst any**.

Если ACL все же задан и настроен, то сначала проверяется он, а затем неявно предполагаемый.

6.3.8 Fake пул

Тип пулов **fake** предназначен для обслуживания адресов, не подвергающихся NAT (например, если для этих адресов необходима URL-фильтрация, но не нужна NAT трансляция). Применение данного типа пула рассмотрено в разделе "Настройка URL-фильтрации для адресов, не подвергающихся NAT". Параметры, доступные для настройки данного типа пулов, и их описание приведены выше, в разделе "Пулы и ACL".

Для корректного логирования событий и обработки URL-фильтрации для таких адресов их необходимо прописывать в настройках **global_ip** пула типа **fake**.

6.4 Типовые конфигурации NAT

6.4.1 NAT для доступа в Интернет

Типовая схема того, как EcoNAT используется для трансляции сетевых адресов при доступе в Интернет, представлена на рисунке ниже.

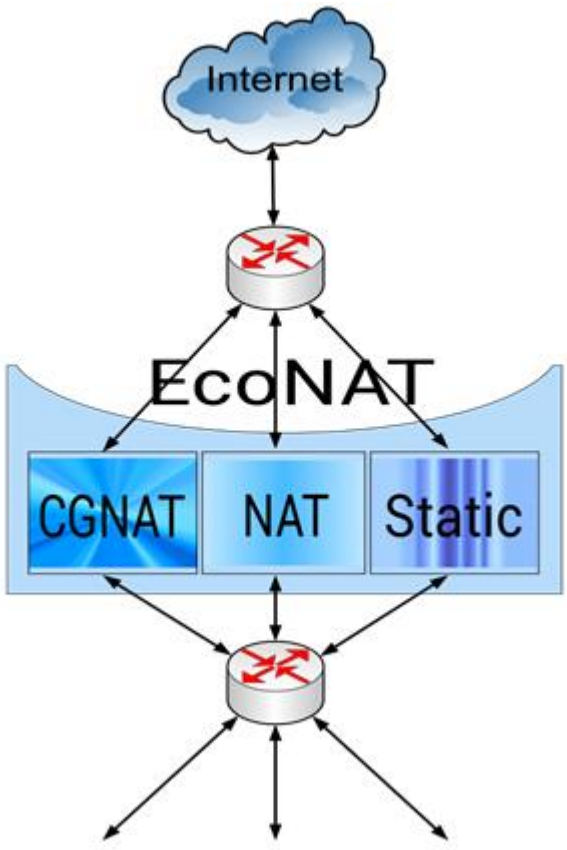

Рисунок 12

Типовая конфигурация EcoNAT включает в себя три пула различного типа для разных видов трафика. Пулы рекомендуется заводить в следующем порядке:

1. Статические IP-адреса административно выделяются в статическом пуле (см. раздел "Пулы и ACL").
2. NAT пул (см. раздел "Пулы и ACL") – необходим в случаях, когда используются протоколы, не поддерживающие портов (например, для GRE). Исключение составляет протокол PPTP (для его обработки создаются пулы типа **cgnat** и включается параметр **alg pptp** в общих настройках NAT). Если нужен basic-NAT с разрешёнными внешне инициируемыми соединениями и отдельно basic-NAT с запрещёнными – то можно завести два NAT пула, различающиеся значением параметра **allow_external_connect**.
3. Основная часть абонентов выходит в Интернет через CGNAT пул (см. раздел "Пулы и ACL").

Если возникла ситуация, когда необходимо настроить трансляцию пересекающихся диапазонов IP-адресов через два разных пула (см. рисунок ниже), то важно правильно расставить приоритеты правил. Учитывая при этом, что первым будет обрабатываться правило с меньшим номером, и что при срабатывании данного правила, остальные не проверяются.

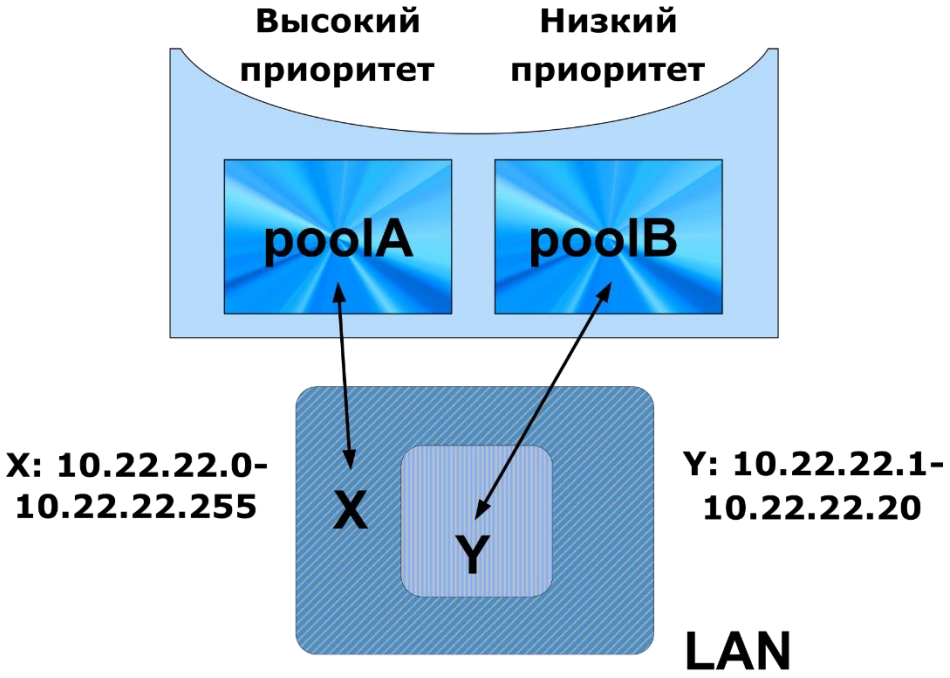

Рисунок 13

В приведенной на рисунке ситуации для двух пулов должны быть сформированы ACL со следующими правилами (при условии, что ***poolA*** имеет больший приоритет, чем ***poolB***):

для ***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
}
```

для ***poolB:***

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

В этом случае для ***poolA*** будет сначала проверяться, принадлежит ли IP источника к диапазону Y (10.22.22.1-10.22.22.20). Если принадлежит, пакет будет отклонен пулом ***poolA,*** и дальше будет рассматриваться ***poolB*** и его список правил. Если не принадлежит, будет проверяться правило, принадлежит ли IP источника к диапазону X (10.22.22.0/24), и в этом случае пакет будет пропущен пулом ***poolA***.

Для ***poolB*** будет проверяться, принадлежит ли IP источника к диапазону Y, и в этом случае пакет будет пропущен.

6.4.2 Участие в пиринговой сети с пересекающимися диапазонами адресов

Типовая схема использования EcoNAT для трансляции сетевых адресов при пиринге представлена на рисунке ниже. Слева изображена схема включения EcoNAT в операторской сети, а справа изображена схема с точки зрения конечного пользователя.

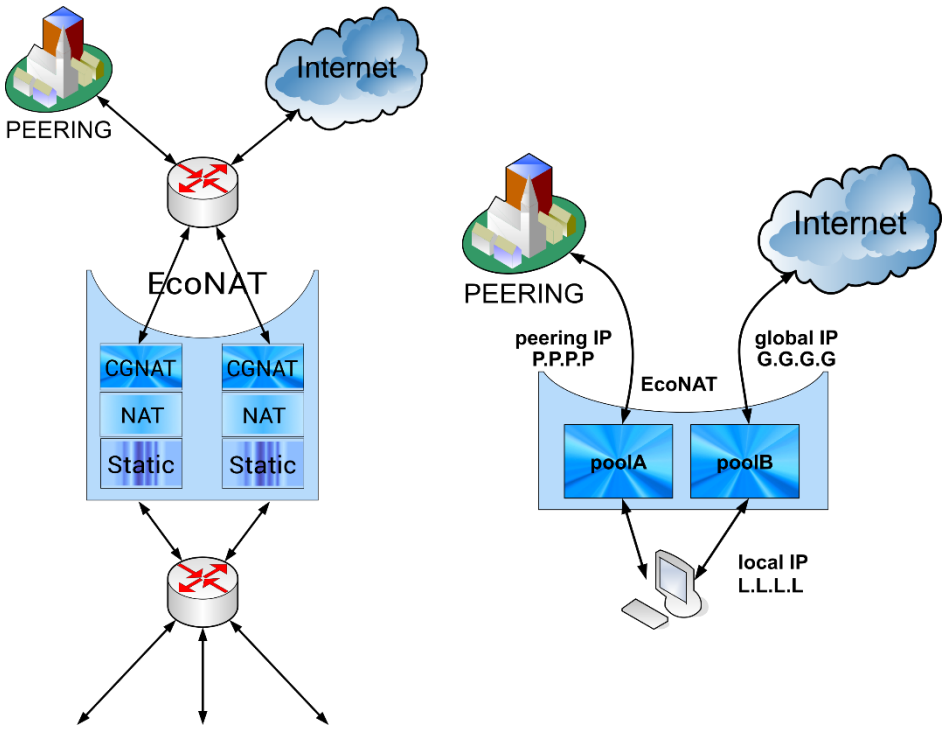

Рисунок 14

Если адресное пространство абонентов оператора связи пересекается с адресами, используемыми его пиринговыми партнерами, то для организации пиринга в точках обмена трафиком (с адресами вида 10.0.0.0/8 или другими приватными адресами) необходимо транслирование абонентских IP в не занятое адресное пространство.

Для решения этой проблемы может быть использован EcoNAT. С этой целью создаются дополнительные пулы типа NAT и в связанных с ними ACL прописываются правила для выбора этих пулов.

Как правило, в большинстве случаев для пиринга создаётся один NAT пул с разрешёнными внешними соединениями (для максимальной прозрачности) и более высоким приоритетом, чем для пулов, обслуживающих доступ в Интернет. Критерием выбора пула может служить DST поле IP пакета, для чего в правилах ACL в поле **dst** указываются сети

партнеров по пирингу. Таким образом, пакеты, направляющиеся в пиринговую сеть, будут транслироваться отдельным пулом в выделенное провайдеру адресное пространство.

6.5 Управление объектами конфигурации

6.5.1 Клонирование ACL

При конфигурировании EcoNAT есть возможность клонировать ACL, создав копию списка правил под другим именем. Для этого существует команда **cloneacl <*имя копируемого ACL*> <*имя нового ACL*>**.

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

6.5.2 Отвязывание ACL от пула

Чтобы разрушить связь между пулом и ACL, используется команда **no use <*имя пула*> <*имя ACL*>**.

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

6.5.3 Удаление пула

Для удаления пула служит команда **no pool <*имя пула*>**.

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

Если необходимо удалить все имеющиеся в конфигурации пулы, используйте команду **droppools**.

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

6.5.4 Удаление правил в ACL

Для удаления правил необходимо сначала перейти к редактированию конкретного ACL, в котором содержатся правила, с помощью команды **edit <*имя ACL*>**. Команда удаления правила **no <*номер правила ACL*>** является контекстной и может быть запущена только изнутри конфигурации редактируемой ACL.

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

6.5.5 Удаление всего ACL

Чтобы удалить ACL, воспользуйтесь командой **no acl.**

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

Если необходимо удалить все имеющиеся в конфигурации ACL, используйте команду **dropacls**.

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

6.6 Команды просмотра

6.6.1 Просмотр трансляций

Для просмотра существующих в данный момент трансляций используются команды **show xlate**.

В таблице ниже представлены различные вариации данной команды.

Таблица 25

Команда	Описание
show xlate gap ADDR:PORT	Вывод всех текущих трансляций для указанной пары: глобальный адрес+ глобальный порт
show xlate gastat ADDRRANGE	Вывод статистики трансляций для указанного глобального адреса
show xlate global ADDRRANGE	Вывод всех текущих трансляций для указанного глобального адреса
show xlate gport PORT	Вывод всех текущих трансляций для указанного глобального порта (независимо от адреса)
show xlate lap ADDR:PORT	Вывод всех текущих трансляций для указанной пары: локальный адрес + локальный порт
show xlate lastat ADDRRANGE	Вывод статистики трансляций для указанного локального адреса
show xlate local ADDRRANGE	Вывод всех текущих трансляций для указанного локального адреса
show xlate lport PORT	Вывод всех текущих трансляций для указанного локального порта (независимо от адреса)
show xlate pool POOLNAME	Вывод трансляций для указанного пула

Примеры вывода представлены ниже.

```
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.
```

6.6.2 Просмотр сессий

Для просмотра существующих в данный момент сессий используются команды **show sessions**.

В таблице ниже представлены различные вариации данной команды.

Таблица 26

Команда	Описание
show sessions gap ADDR:PORT	Вывод всех текущих сессий для указанной пары: глобальный адрес+ глобальный порт
show sessions global ADDRRANGE	Вывод всех текущих сессий для указанного глобального адреса
show sessions gport PORT	Вывод всех текущих сессий для указанного глобального порта (независимо от адреса)
show sessions lap ADDR:PORT	Вывод всех текущих сессий для указанной пары: локальный адрес + локальный порт
show sessions local ADDRRANGE	Вывод всех текущих сессий для указанного локального адреса
show sessions lport PORT	Вывод всех текущих сессий для указанного локального порта (независимо от адреса)
show sessions rap ADDR:PORT	Вывод всех текущих сессий для указанной пары: внешний адрес + внешний порт
show sessions remote ADDRRANGE	Вывод всех текущих сессий для указанного внешнего адреса
show sessions rport PORT	Вывод всех текущих сессий для указанного внешнего порта

Примеры вывода представлены ниже.

```
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 10.210.0.167
egress UDP 1.10.0.167:6148-10.4.125.136:6148 8.8.8.8:53 Last packet
222.35 seconds ago; To be deleted in 77.65 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.
```

6.6.3 Удаление сессий

Для удаления сессий используется команда **clear sessions**.

В таблице ниже представлены различные вариации данной команды.

Таблица 27

Команда	Описание
clear sessions all	Удаление всех текущих сессий
clear sessions gap ADDR:PORT	Удаление всех текущих сессий для указанной пары: глобальный адрес+ глобальный порт
clear sessions global ADDRRANGE	Удаление всех текущих сессий для указанного глобального адреса
clear sessions gport PORT	Удаление всех текущих сессий для указанного глобального порта (независимо от адреса)

Команда	Описание
clear sessions lap ADDR:PORT	Удаление всех текущих сессий для указанной пары: локальный адрес + локальный порт
clear sessions local ADDRRANGE	Удаление всех текущих сессий для указанного локального адреса
clear sessions lport PORT	Удаление всех текущих сессий для указанного локального порта (независимо от адреса)
clear sessions rap ADDR:PORT	Удаление всех текущих сессий для указанной пары: внешний адрес + внешний порт
clear sessions remote ADDRRANGE	Удаление всех текущих сессий для указанного внешнего адреса
clear sessions rport PORT	Удаление всех текущих сессий для указанного внешнего порта

Пример.

```
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.
```

6.6.4 Просмотр привязок

Для просмотра существующих в данный момент привязок локальных IP-адресов к глобальным используются команды **show bind**.

В таблице ниже представлены различные вариации данной команды.

Таблица 28

Команда	Описание
show bind global IPRANGE | any	Вывод привязок для указанных глобальных адресов
show bind local IPRANGE | any	Вывод привязок для указанных локальных адресов
show bind summary	Вывод счетчика связей для глобальных портов
show bind usage	Вывод счетчика заполнения таблицы g_abons_table

Примеры вывода представлены ниже.

```
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
```

6.6.5 Просмотр таблицы ALG

Для просмотра существующих в данный момент в таблице ALG (Application-level gateway) записей используются команды **show algtable**.

В таблице ниже представлены различные вариации данной команды.

Таблица 29

Команда	Описание
show algtable local IPRANGE | any	Вывод записей о сессиях по указанным локальным адресам
show algtable lport PORT | any	Вывод записей о сессиях по указанным локальным портам
show algtable remote IPRANGE | any	Вывод записей о сессиях по указанным удаленным адресам
show algtable rport PORT | any	Вывод записей о сессиях по указанным удаленным портам

Пример вывода представлен ниже.

```
EcoNAT:8:> show algtable local any
10.210.51.67:38434->212.22.86.99:1723 PPTP src 0.0.0.0 glb 0.0.0.0 dst
0.0.0.0 sid 0 gid 0 did 0 callserial0 !pptp0 !cherry0
10.210.224.169:60364->62.226.226.112:1723 PPTP src 0.0.0.0 glb 0.0.0.0
dst 0.0.0.0 sid 0 gid 0 did 0 callserial0 !pptp0 !cherry0
10.210.151.27:53782->130.193.124.153:1723 PPTP src 0.0.0.0 glb 0.0.0.0
dst 0.0.0.0 sid 0 gid 0 did 0 callserial0 !pptp0 !cherry0
10.254.49.45:43220->178.162.211.68:1723 PPTP src 0.0.0.0 glb 0.0.0.0 dst
0.0.0.0 sid 0 gid 0 did 0 callserial0 !pptp0 !cherry0
10.254.49.45:60528->178.162.211.68:1723 PPTP src 0.0.0.0 glb 0.0.0.0 dst
0.0.0.0 sid 0 gid 0 did 0 callserial0 !pptp0 !cherry0
10.12.163.64:5060->212.24.35.28:5060 SIP global 46.148.235.249 gport
1024 local 10.12.163.64 lport 5060
```

```
10.210.59.219:63176->99.240.144.149:1723 PPTP src 0.0.0.0 glb 0.0.0.0
dst 0.0.0.0 sid 0 gid 0 did 0 callserial0 !pptp0 !cherry0
10.254.105.110:46560->185.25.50.156:1723 PPTP src 0.0.0.0 glb 0.0.0.0
dst 0.0.0.0 sid 0 gid 0 did 0 callserial0 !pptp0 !cherry0
10.254.221.65:50078->213.33.170.11:1723 PPTP src 0.0.0.0 glb 0.0.0.0 dst
0.0.0.0 sid 0 gid 0 did 0 callserial0 !pptp0 !cherry0
```

6.6.6 Ошибки выделения порта

Для просмотра информации об ошибках выделения порта CG-NAT пулов используется команда **show cgnat errors**.

```
EcoNAT:9:> 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
```

7 Функциональность BRAS

Данная функциональность доступна на основе лицензии EcoBRASxxxx-LIC.

Функциональность BRAS позволяет оператору связи реализовать так называемый Services Gateway для ограничения скорости доступа абонентов к IP-сервисам и услугам передачи данных в обоих направлениях, отключать абонентов, переадресовывать их на портал или страницу с уведомлением о необходимости пополнить счет, а также для демонстрации абонентам информационных сообщений путем переадресации на портал.

Предполагается следующая сервисная модель IPoE:

- отсутствие инкапсуляции PPTP, PPPoE и др, чистый IPoE;
- абонент однозначно идентифицируется своим IPv4 адресом внутри сети провайдера;
- шлюзом для абонентов служит не BRAS, а коммутатор агрегации, или ядра (L3-connected абоненты);
- IP-адрес абоненту может выдаваться либо статически, либо динамически (сторонним устройством, не EcoNAT) – при помощи DHCP сервера, связанного с системой биллинга.

EcoBRAS разрешает осуществлять краткосрочное превышение (burst) скорости трафика над расчетной, продолжительность burst ограничена объемом трафика, соответствующего первой секунде на законтрактованной скорости абонента.

7.1 Настройки BRAS

Управление настройками BRAS осуществляется в ветке конфигурационного дерева **system bras**.

```
MyEcoNAT:1:# root
MyEcoNAT:2:# system bras
MyEcoNAT:3:system.bras# show
enable
pass_multicast true
pass_routing_protocols true
pass_bgp_port true
bgp_port 179
redirect_string "http://www.provider.ru/closed.html"
no_shape( )
MyEcoNAT:4:system.bras# enable # включить BRAS функциональность
MyEcoNAT:5:system.bars# disable # выключить BRAS функциональность
```

Для включения и выключения BRAS используются контекстные команды **enable** и **disable**, которые должны быть запущены в **system bras**.

Измененная конфигурация применяется только после выполнения команды **apply**.

Настройки, доступные для BRAS приведены в таблице ниже.

Таблица 30

Параметр	Описание
acl	Список IP-адресов абонентов, которые необходимо обрабатывать BRAS. Значение по умолчанию - **none**, что эквивалентно **0.0.0.0/0**. Таким образом

Параметр	Описание
	все абоненты, попадающие в любой пул, будут также передаваться на обработку BRAS
pass_multicast	Пропускать мультикаст трафик прозрачно, не применяя для него политик (рекомендуемое значение: true)
pass_routing_protocols	Пропускать трафик протоколов маршрутизации (OSPF и BGP), не применяя для них политик (рекомендуемое значение: true)
pass_bgp_port bgp_port	Пропускать трафик BGP на выбранном TCP порту, не осуществляя его контроль (рекомендуемое значение true)
no_shape	Внешние глобальные IP-адреса, для которых не ограничивается скорость (для абонентов, разрешённых биллингом). Сюда вы можете внести IP-адреса игровых серверов, серверов IPTV и других ресурсов, которые должны быть доступны абонентам на максимальной скорости
policies и services	Совокупность настроек, ограничивающих скорость приема и передачи данных или осуществляющих перенаправление на портал для пополнения счета абонента. Более подробно будет рассмотрено в разделах "Политики и сервисы", "Настройка доступа к RADIUS серверу"

7.2 Консоль биллинга и протокол EcoBRAS

Для загрузки информации из биллинга в EcoNAT используется специализированный проприетарный протокол EcoBRAS, который является простым текстовым протоколом.

Для его работы необходимо установить соединение с портом 2225 управляющего интерфейса EcoNAT, после чего происходит обмен строками запросов (к EcoNAT) и ответов EcoNAT.

В случае неверной строки запроса EcoNAT немедленно принудительно закрывает соединение, не высылая строку ответа.

Длина строки запроса не может превышать 64 килобайта. Строки запроса и ответа заканчиваются символом ASCII LF (код 0x0A).

Строка запроса может содержать в себе символы ASCII CR (код 0x0D), но они будут игнорироваться.

Протокол поддерживает следующие команды:

testRID,

add,

- **statall,**

remove

clearall.

7.2.1 Команда 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
```

По запросу **testRID** выдаётся подряд список пар **НОМЕРДОГОВОРА-НОМЕРТАРИФА**. Биллинг использует эту информацию для синхронизации списков: чтобы определить, какого номера договора нет в EcoNAT, а какой является лишним.

```
B: testRID
E:
```

В случае если в EcoNAT нет номеров договоров (например, если он только-только загрузился), то он отвечает пустой строкой.

Сразу после загрузки BRAS включается режим пропускания всего трафика (для того чтобы абоненты обслуживались в то время, пока еще не загружена информация из биллинга). После поступления первого **testRID** включается таймер, который в течение 600 секунд держит режим пропускания всего трафика (в это время могут поступать новые **testRID)**. По прошествии 10 минут действие таймера закончится, и при поступлении следующего **testRID** BRAS переключится в основной режим работы (когда запрещён трафик от тех абонентов, которые в биллинге не разрешены явно). Для того чтобы увидеть состояние таймера, используется команда **time.**

7.2.2 Команда add

```
B: add 24372 {oid} LIM10M/LIM10M 10.21.0.208, 10.210.0.207.95, // RULE43
E:
```

Команда **add** – добавляет политику для абонента с указанным номером контракта.

В случае успеха BRAS возвращает пустую строку. В случае неуспеха закрывает соединение.

Детальный формат команды **add** описан в таблице ниже.

Таблица 31

№	Поле	Содержание поля	Описание поля
1	add	3 символа	Команда – добавить контракт
2		TAB	Разделитель
3	24372	Цифры	Номер контракта
4		TAB	Разделитель
5	{oid}	Строка 5 символов	Тип контракта (в нашем случае всегда фиксированная строка '{oid}')
6		SPACE	Разделитель
7	LIM10M	Строка: LIM значение скорости K/M/G или UNLIM	Скорость upstream (в Интернет). K/M/G – означают кило/мега/гига бит. Например, LIM64K – 64 Кбит/с. UNLIM – без ограничений скорости
8	/	Символ '/'	Разделитель
9	LIM10M	строка	Скорость downstream (из Интернета)
10		SPACE	Разделитель пробел
11	10.21.0.208,	IP адрес, разделитель‘,’	IP-адрес абонента (могут следовать несколько подряд, каждый из IP-адресов получает те скорости, которые заданы для этого контракта)
12		SPACE	Разделитель
13	//	2 символа	

№	Поле	Содержание поля	Описание поля
14		SPACE	Разделитель
15	RULE	4 символа	
16	43	Число	Номер тарифа абонента (ID тарифа в биллинге)
17		LF	Конец строки запроса

7.2.3 Команда remove

```
B: remove 24372 {oid} LIM10M/LIM10M 10.21.0.208, 10.210.0.207.95,
E:
```

Команда **remove** имеет синтаксис, близкий к команде **add**, но она не добавляет, а удаляет контракт и связанные с ним адреса абонентов.

Таблица 32

№	Поле	Содержание поля	Описание поля
1	remove	6 символов	Команда – удалить контракт
2		TAB	Разделитель
3	24372	Цифры	Номер контракта
4		TAB	Разделитель
5	{oid}	Строка 5 символов	Тип контракта (в нашем случае всегда фиксированная строка '{oid}')
6		SPACE	Разделитель
7	LIM10M	Строка: LIM значение скорости K/M/G или UNLIM	Скорость upstream (в Интернет). K/M/G – означают кило/мега/гига бит. Например, LIM64K - 64 Кбит/с. UNLIM – без ограничений скорости
8	/	Символ '/'	Разделитель
9	LIM10M	строка	Скорость downstream (из Интернета)
10		SPACE	Разделитель пробел
11	10.21.0.208,	IP адрес, разделитель‘,’	IP адрес абонента (могут следовать несколько подряд, каждый из IP-адресов получает те скорости, которые заданы для этого контракта)
12		LF	Конец строки запроса

Если в запросе **remove** указан перечень IP-адресов, отличный от указанного ранее в запросе **add**, то BRAS деавторизует все IP, ранее зарегистрированные во всех командах **add** для данного номера контракта. Если команда **add** была выдана повторно (без remove), то для IP-адресов, указанных в повторном **add**, будет выставлена скорость, указанная в повторном запросе (обновление скорости).

7.2.4 Команда statall

На порту с номером 2225 также доступна сервисная команда **statall**, по вызову которой выводится информация о трафике всех абонентов.

```
$ 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
```

7.2.5 Команда clearall

Данная команда используется для удаления всех политик, добавленных через консоль биллинга.

7.3 Сервисная BRAS консоль

Для удобства работы службы поддержки, на TCP-порт с номером 2226 управляющего интерфейса EcoNAT выведена сервисная BRAS консоль, которая позволяет службе поддержки проверить состояние абонента (как по IP-адресу, так и по номеру контракта).

```
$ 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
>
```

Ниже описаны команды просмотра и очистки информации BRAS.

Команда **show brasinfo all** выдаёт краткую информацию о состоянии BRAS для всех обслуживаемых адресов.

```
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
…
```

Команда **show brasinfo**, применённая к конкретному IP-адресу, выдаёт детальную информацию о состоянии сессии и примененных сервисах для данного абонента.

```
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 recieved total                         404843
Bytes transmitted total                         0
Packets recieved total                       5272
Packets transmitted 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 recieved                              0
Bytes transmitted                             0
Packets recieved                            0
Packets transmitted                           0
-------------------------------------------------------------------------
2. service20m "service20m"
Enabled
Maximum data rate upstream                   20479 Kb/s
Maximum data rate downstream                  20479 Kb/s
Bytes recieved                         404695
Bytes transmitted                           0
Packets recieved                         5270
Packets transmitted                           0
```

Команда **show brasinfo**, применённая к диапазону до миллиона адресов (например, **show brasinfo *10.210.0.81/12***), выдаёт подробную информацию о состоянии BRAS для указанных адресов. Если данная команда применяется к большому диапазону адресов, то выдается краткая информация (как для команды **show brasinfo all**).

Команда **show brasinfo summary** выводит краткую статистику по политике.

```
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
=========================================================
```

При большом количестве адресов, вывод информации на консоль может занять некоторое время. Выполнение команды можно прервать, нажав **[Backspace]** или **[Ctrl+C]**.

В случае если нет сессии для указанного адреса, мы получим следующее сообщение:

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

Отображаемые командой **show brasinfo** параметры приведены в таблице ниже.

Таблица 33

Поле	Описание
Status	Статус клиента
Maximum data rate upstream total	Установленные для абонента ограничения скорости upstream (в Интернет), в килобайтах
Maximum data rate downstream total	Установленные для абонента ограничения скорости downstream (из Интернета), в килобайтах
Bytes received total	Общее количество байт, полученных абонентом
Bytes transmitted total	Общее количество байт, переданных абонентом
Packets received total	Общее количество пакетов, полученных абонентом
Packets transmitted total	Общее количество пакетов, переданных абонентом
Session timeout expires in	Время (в секундах), которое осталось до автоматического завершения сессии, после истечения таймера сессия удаляется и создается новая
Idle timeout expires in	Время (в секундах), которое осталось до автоматического завершения сессии по причине неактивности
Interim interval expires in	Время (в секундах), которое осталось до завершения интервала аккаунтинга
Информация о сервисах	
Enabled/Disabled	Включен/выключен
Maximum data rate upstream	Установленные сервисом ограничения скорости upstream (в Интернет), в килобайтах
Maximum data rate downstream	Установленные сервисом ограничения скорости downstream (из Интернета), в килобайтах
Bytes received	Количество байт, полученных абонентом
Bytes transmitted	Количество байт, переданных абонентом
Packets received	Количество пакетов, полученных абонентом
Packets transmitted	Количество пакетов, переданных абонентом

Для просмотра состояния BRAS используется команда **show brasstate**.

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

Данная команда показывает два поля:

- **default access** – действие по умолчанию,
- **state** – состояние BRAS (включен/выключен).

Сразу после загрузки BRAS включается режим пропускания всего трафика для того, чтобы абоненты обслуживались в то время, пока еще не загружена информация из биллинга (**default access** – **pass**). После загрузки базы BRAS переключается в основной режим работы, когда запрещён трафик от тех абонентов, которые в биллинге не разрешены явно (**default access** – **block**).

Для проверки состояния контракта используется команда **show brascontract <ID>**, где **ID** - идентификатор контракта. Данная команда выводит информацию по самому контракту и входящих в него абонентов: состояние, IP-адреса, скорость, а также статистику по абоненту и общую по контракту.

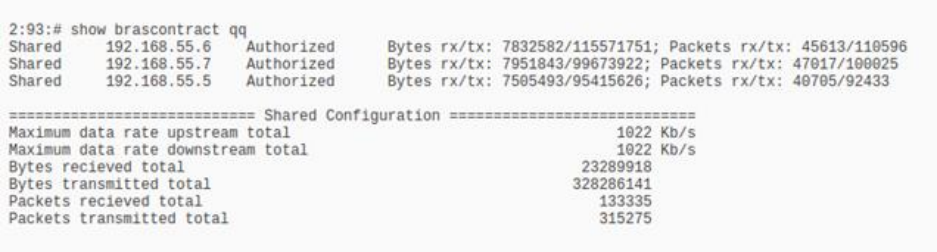

Рисунок 15

Для сброса одной абонентской сессии используется команда **clear brasinfo <IP-адрес>**, а для сброса всех сессий абонентов в EcoBRAS используется команда **clear brasinfo all**.

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

При настроенном аккаунтинге при выполнении команды **clear brasinfo <IP-адрес>,** сначала отправляется запрос **accounting STOP** на сервер для того чтобы закрыть сессию, и только потом сессия удаляется на EcoNAT. При выполнении **clear brasinfo all**, записи сессий удаляются только на EcoNAT.

Для очистки элементов конфигурации используются команды **dropservices**, **droppolicies** и **dropradius**.

7.4 Политики и сервисы

Для ограничения скорости приема и передачи данных или перенаправления на портал для пополнения счета абонента в функциональности BRAS используются политики (policy) и сервисы (service). Сервис представляет собой набор действий, выполняемых в случае выполнения определенных условий – попадания адреса источника или назначения сессии в указанный ACL. Политика может объединять несколько сервисов между собой.

7.4.1 Сервисы

Для создания сервиса необходимо выполнить команду **create service <*имя сервиса*>**. При создании сервиса, его название формируется аналогичным образом с описанным в разделе "Пулы и ACL".

После создания сервиса необходимо перейти в режим конфигурирования этого сервиса командой **goto bras services <*имя сервиса*>** и при помощи контекстных команд задать значения его параметров.

Доступные параметры сервисов описаны в таблице ниже.

Таблица 34

Параметр	Описание
enable disable	Включен или выключен сервис
name	Имя сервиса
action	Действие, которое выполняет сервис: **pass** – трафик проходит, но подвергается ограничению скорости (по умолчанию); **drop** – трафик отбрасывается;

Параметр	Описание
	block – происходит переадресация на портал, например, для пополнения счета. Адрес портала задается параметром **redirect_url**; **redirect** – используется при включенной функции периодического перенаправления (см. "Перенаправление пользователей"). При указании данного действия происходит перенаправление HTTP-трафика (HTTPS проходит). Для корректной работы в параметрах списка доступа, привязанного к данному сервису, необходимо указать **redirect_use_interval on**
acl	Список доступа, по которому пакеты попадают в данный сервис
redirect_url	Адрес, на который будет происходить переадресация клиента, если используется **action redirect**. Как правило, здесь задается адрес портала оператора связи, куда переадресовывается клиент в случае необходимости пополнения счета, также можно задать и другие ресурсы. EcoNAT позволяет добавлять в адресную строку спецификаторы, указывающие на клиента. Что позволяет персонализировать страницу переадресации. Возможные спецификаторы: **%c** - передавать в redirect_url callback-id, полученный от RADIUS-сервера; **%m** - передавать в redirect_url mac адрес клиента; **%i** - передавать в redirect_url ip адрес клиента; **%v1** - передавать в redirect_url первый (верхний) vlan клиента; **%v2** - передавать в redirect_url второй (нижний) vlan клиента; **%u** - передавать в redirect_url url, на который обратился клиент. Формат ввода параметра **redirect_url**: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>=<SPEC2>..<VAR_NAMEN>=<SPECN>** где **URL** - адрес страницы, на которую осуществляется перенаправление, **VAR_NAME1** .. **VAR_NAMEN** - имя переменной, **SPEC1** .. **SPECN** - спецификатор. Например, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. Если при таком значении параметра клиент попробует обратиться на адрес **forbidden.com**, то он будет перенаправлен на адрес: **http://example.com/?var1= forbidden.com&ip=10.1.1.10&qwe=0**
egress_speed	Максимальная исходящая скорость (Кб/с)
ingress_speed	Максимальная входящая скорость (Кб/с)
egress_tos	Значение, которое будет устанавливаться в поле **type of service** в заголовке исходящего пакета, задается в десятичном формате. Для того чтобы не маркировать трафик, необходимо оставить значение: **nochange**
ingress_tos	Значение, которое будет устанавливаться в поле **type of service** в заголовке входящего пакета, задается в десятичном формате. Для того чтобы не маркировать трафик, необходимо оставить значение: **nochange**
time_start daily HH:MM	Время начала действия сервиса. При указании значения данный сервис включается ежедневно в определенное время. Время (UTC) указывается в формате **HH:MM**, где **HH** - час, **MM** - минуты
time_end daily HH:MM	Время окончания действия сервиса. При указании значения данный сервис выключается ежедневно в определенное время. Время (UTC) указывается в формате **HH:MM**, где **HH** - час, **MM** - минуты
always_pass	Внешние глобальные IP-адреса, к которым не будут применены правила данного сервиса
no_shape	Внешние глобальные IP-адреса, для которых не ограничивается скорость. Сюда можно внести IP-адреса игровых серверов, серверов IPTV и других ресурсов, которые должны быть доступны абонентам на максимальной скорости
dpilists	Указывается номер списка сайтов для реализации URL фильтрации (см. раздел "Функциональность URL-фильтрации (DPI) "). Если сайт не

Параметр	Описание
	удовлетворяет требованию списка, происходит переадресация на ресурс, указанный в параметре **redirect_url**. Параметр доступен только при установленном модуле URL-фильтрации

Пример создания и настройки сервиса:

```
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 ( )
```

Для включения и выключения сервиса используются контекстные команды **enable** и **disable**, которые должны быть запущены в ветке сервиса.

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

Измененная конфигурация применяется только после выполнения команды ***apply*** .

7.4.2 Политики

Для создания политики необходимо выполнить команду **create policy <*имя политики*>**. При создании политики, ее название формируется аналогичным образом с описанным в разделе "Пулы и ACL".

После создания новой политики необходимо перейти в режим конфигурирования этой политики командой **goto bras policy <*имя политики*>** и при помощи контекстных команд задать значения ее параметров.

Доступные параметры политик описаны в таблице ниже.

Таблица 35

Параметр	Описание
enable disable	Включена или выключена политика

Параметр	Описание
priority	Приоритет применения политик. Чем меньше значение, тем выше приоритет. По умолчанию у первой по счету созданной политики приоритет 100, у второй – 200, у третьей по счету – 300 и так далее
local_ip	Задаются адреса или подсети клиентов, к которым будет применяться данная политика
type	Параметр принимает одно из двух значений: **static** – для клиентов применяются сервисы, определенные настройками политики, **dynamic** – авторизация абонентов осуществляется по протоколу RADIUS (должен быть настроен сервер RADIUS)
session_timeout	Время (в секундах), в течение которого существует сессия, после истечения таймера сессия удаляется и создается новая. По умолчанию принимает значение 86400 секунд
idle_timeout 28800	При отсутствии активности в течение данного промежутка времени, сессия будет прервана. Указывается в секундах. По умолчанию принимает значение 28800 секунд
interim_interval	Интервал аккаунтинга (в секундах). Применяется при включенном функционале Radius. По умолчанию принимает значение 15 секунд
ingress_auth	Разрешить/запретить авторизацию клиента по ingress-пакету с dst IP-адресом клиента. Работает только для клиентов из статического или fake пулов
services	Указывается имя сервиса, который привязывается к политике. Можно задать несколько сервисов через пробел. Параметры, настраиваемые в случае type dynamic, описаны в разделе "Настройка доступа к RADIUS серверу"

Пример создания и настройки политики:

```
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 ( )
 type static
 session_timeout 86400
 idle_timeout 28800
 interim_interval 15
 services (service1)
```

Для включения и выключения политики используются контекстные команды **enable** и **disable**, которые должны быть запущены в ветке политики.

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

*Измененная конфигурация применяется только после выполнения команды **apply**.*

Настроенные политики будут обрабатываться в порядке их приоритета. При этом, каждой политике может быть присвоено несколько сервисов. Тогда внутри одной политики сервисы будут обрабатываться в том порядке, в котором они указаны в конфигурации политики.

7.5 Настройка доступа к RADIUS серверу

7.5.1 Общие настройки подключения к RADIUS-серверу

Для доступа к RADIUS-серверу в конфигурации BRAS должны быть настроены параметры подключения к серверу. Для создания нового подключения к RADIUS серверу необходимо выполнить команду **create radius <*имя подключения*>**. При создании подключения, его название формируется аналогичным образом с описанным в разделе "Пулы и ACL".

После создания нового подключения необходимо зайти в соответствующую ветку конфигурационного дерева и при помощи контекстных команд задать значения его параметров.

Параметры подключения к RADIUS-серверу описаны в таблице ниже.

Таблица 36

Параметр	Описание
enable disable	Включен или выключен доступ к RADIUS серверу
auth_server	IP-адрес:порт для аутентификации на RADIUS сервере. Пример: 192.168.1.1:1812
auth_password	Пароль для аутентификации на RADIUS сервере
acc_server	IP-адрес:порт RADIUS сервера для аккаунтинга
acc_password	Пароль для аккаунтинга на RADIUS сервере
coa_port	Порт, который будет слушать BRAS на интерфейсе управления для CoA сообщений
coa_password	Пароль для CoA сообщений

Пример настройки подключения к RADIUS серверу:

```
MyEcoNAT:1:system.bras.radius# create radius 1
MyEcoNAT:2:system.bras.radius# radius1
MyEcoNAT:3:system.bras.radius.radius1# enable
MyEcoNAT:4:system.bras.radius.radius1# auth_server 192.168.5.1:1812
MyEcoNAT:5:system.bras.radius.radius1# auth_password "econat"
MyEcoNAT:6:system.bras.radius.radius1# acc_server 192.168.5.1:1813
MyEcoNAT:7:system.bras.radius.radius1# acc_password "econat"
MyEcoNAT:8:system.bras.radius.radius1# coa_port 702
MyEcoNAT:9:system.bras.radius.radius1# coa_password "pass22"
MyEcoNAT:10:system.bras.radius.radius1# show
   enable
   auth_server 192.168.5.1:1812
   auth_password "econat"
   acc_server 192.168.5.1:1813
   acc_password "econat"
   coa_port 702
   coa_password "pass22"
```

Для включения и выключения доступа к RADIUS-серверу используются контекстные команды **enable** и **disable**, которые должны быть запущены в ветке подключения к RADIUS-серверу.

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

7.5.2 Настройка динамических политик

При подключении к RADIUS-серверу необходимо использовать динамические политики. Такая политика создается и настраивается аналогично статической, описанной в разделе "Политики и сервисы". Отличаются только некоторые параметры. Настройки динамической политики приведены в таблице ниже.

Таблица 37

Параметр	Описание
enable disable	Включена или выключена политика
priority	Приоритет применения политик. Чем меньше значение, тем выше приоритет. По умолчанию у первой по счету созданной политики приоритет 100, у второй – 200, у третьей по счету – 300 и т.д.
local_ip	Задаются адреса или подсети клиентов, к которым будет применяться данная политика
type dynamic	Включает авторизацию абонентов по протоколу RADIUS
auth	Имя подключения к RADIUS серверу
reauthorization_timeout	Время (в секундах), через которое будет выполнена повторная попытка авторизации клиента при отсутствии ответа от RADIUS сервера (BRAS сессия клиента при этом находится в статусе Error). По умолчанию принимает значение 180 секунд
session_timeout	Время (в секундах), в течение которого существует сессия, после истечения таймера сессия удаляется. По умолчанию принимает значение 86400 секунд
idle_timeout 28800	При отсутствии активности в течение данного промежутка времени, сессия будет прервана. Указывается в секундах. По умолчанию принимает значение 28800 секунд
interim_interval	Интервал аккаунтинга (в секундах). Применяется при включенном функционале Radius. По умолчанию принимает значение 15 секунд
Привязка сервисов к политике	
default	Сервис (или сервисы), который применяется для абонента, попавшего в политику, но еще не прошедшего авторизацию
if_auth_accept	Сервис (или сервисы), который применяется для абонента, получившего Access-Accept от сервера RADIUS
if_auth_reject	Сервис (или сервисы), который применяется для абонента, получившего Access-Reject от сервера RADIUS
if_auth_fail	Сервис (или сервисы), который применяется на абонента, если радиус сервер не ответил на Access-Request по истечению таймаута

Пример создания и настройки динамической политики:

```
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 )
```

7.5.3 Авторизация клиента на RADIUS-сервере

При авторизации клиента на RADIUS-сервере, BRAS отправляет RADIUS Access-Request со следующей информацией:

- User_Name = <IP-адрес пользователя>
- Calling-Station-Id = <MAC-адрес пользователя>
- User-Password = <EcoBRAS hostname>

Атрибут User-Password используется только для обеспечения совместимости с некоторыми системами биллинга. Так как такими системами предъявляются требования только к наличию данного атрибута в сообщениях Access-Request, то его значение одинаково для всех пользователей. В качестве значения параметра User-Password автоматически используется значение параметра **hostname** из ветки конфигурационного дерева **system_log** (см. раздел "Логирование"). При авторизации значения данного атрибута не используются.

При получении Access-Accept от RADIUS сервера, пользователю назначается сервис, указанный в параметре if_auth_accept и соответствующие ему ограничения скорости. Сессия пользователя регулируется таймаутами, указанными в параметрах: session_timeout, idle_timeout, interim_interval. Однако в случае если в Access-Accept от RADIUS-сервера содержатся дополнительные атрибуты с сервисами, то к абоненту автоматически применяются именно они, несмотря на настройки политик и сервисов BRAS.

В некоторых случаях для обеспечения совместимости с системами биллинга необходимо, чтобы в сообщениях Access-Request присутствовал атрибут User-Password. При авторизации не используются значения данного атрибута

BRAS обрабатывает следующие атрибуты, содержащиеся в RADIUS24:

- Cisco-Account-Info – ограничение Upload и Download скорости в бит/с;
- Cisco-Service-Info – принудительное назначение сервиса, настроенного на BRAS. При этом имя сервиса задается в виде: **A<имя сервиса>**;
- Callback-Id – уникальный идентификатор пользователя, который подставляется в **redirect_url** через спецификатор **%c**;
- Idle-Timeout;
- Session-Timeout;
- Acct-Interim-Interval.

Например:

- Cisco-Account-Info := "QU;20240000;D;20240000",
- Cisco-Service-Info := "Aservice2",
- Callback-Id := "c6958059a295af355e5b8dfbbfcf4fd4",
- Idle-Timeout := 500,
- Session-Timeout := 500,
- Acct-Interim-Interval :=500.

Для обработки BRAS сообщения об изменении параметров авторизации пользователя (CoA), может быть использован код 43(Coa-Request) и код 40(Disconnect-Request). с указанием атрибута **User-Name=<ip пользователя>**. При получении CoA-Disconnect происходит прерывание сессии (disconnect code 40). Новые параметры вступают в действие с переавторизацией. При получении CoA-Request происходит изменение параметров текущей сессии без прерывания. После запроса отправляются данные accounting-stop и accounting-start.

7.5.4 Настройка резервного RADIUS-сервера

Можно настроить резервный RADIUS-сервер. В этом случае при отсутствии связи с основным RADIUS-сервером произойдет переключение на резервный сервер. Обнаружение доступности/недоступности основного RADIUS-сервера реализовано с помощью периодической отправки **check_state** пакетов от BRAS и получения на них ответов. Частота проверки - 1 пакет в секунду.

Настройка резервного сервера производится в разделе **system.bras.radius**.

Для этого создается второй RADIUS-сервер аналогично описанию, приведенному выше. Кроме того, в разделе **system.bras.radius** должны быть указаны значения следующих параметров, описанных в таблице ниже.

Таблица 38

Параметр	Описание
radius_timeout	Таймаут, в течении которого BRAS ожидает получить ответ от RADIUS-сервера на отправленный radius-request. Если ответ от RADIUS-сервера в течение указанного таймаута получен не был, BRAS-сессия по данному клиенту переходит в статус error.
attempt_timeout	Таймаут, по истечению которого: основной сервер, который перестал отвечать на radius-request пакеты, считается недоступным. В этом случае BRAS перенаправляет все пакеты radius-request на другой(резервный) RADIUS сервер; основной RADIUS-сервер, который стал снова отвечать на check_state пакеты, считается доступным. В этом случае BRAS возвращает все пакеты radius-request с резервного RADIUS-сервера на него.

Пример:

```
MyEcoNAT:10:system.bras.radius# ls
radius_timeout 5
attempt_timeout 10
radius1
{
 disable
 auth_server 0.0.0.0:0
```

```
 auth_password ""
 acc_server 0.0.0.0:0
 acc_password ""
 coa_port 0
 coa_password ""
}
radius2
{
 disable
 auth_server 0.0.0.0:0
 auth_password ""
 acc_server 0.0.0.0:0
 acc_password ""
 coa_port 0
 coa_password ""
}
```

7.6 Создание BRAS-сессии по DHCP пакетам

EcoBRAS имеет возможность заводить BRAS-сессии по DHCP пакетам. Данная функция доступна по запросу, требуется обновление ПО.

Рассмотрим принцип работы данного механизма на примере схеме, представленной на рисунке ниже.

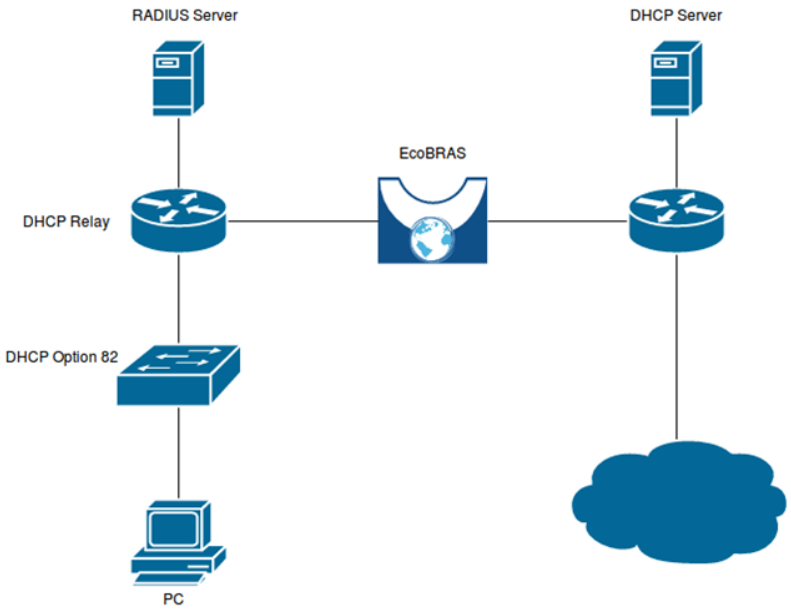

Рисунок 16

Для работы данного механизма необходимо чтобы через EcoBRAS проходили Unicast DHCP пакеты от DHCP Relay до DHCP Server. При этом IP-адрес DHCP Relay должен попадать в **pool** на EcoBRAS и не должен попадать ни в одну политику.

Когда абонент запрашивает настройки у DHCP сервера, EcoBRAS из пакета DHCP ACK получает следующие данные: IP-адрес, MAC-адрес, Option 82 (если присутствует). На основании этих данных заводится BRAS-сессия и на RADIUS-сервер отправляется запрос на аутентификацию. При отправке **Access-Request** в поле **User-Name** подставляется MAC-адрес

абонента, а в поле **Calling-Station-ID** IP адрес. Если в пакете DHCP присутствовала Option 82, тогда в **Access-Request** добавляются дополнительные атрибуты:

```
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
```

При передаче от клиента сообщения **DHCP Release**, EcoBRAS удаляет BRAS-сессию для этого клиента, отправляя **Accounting-Stop** на RADIUS-сервер.

7.7 Общие контракты

В рамках одного контракта может быть организована работа нескольких пользователей с общей максимальной полосой пропускания (общий контракт). В этом случае учитываются персональные настройки ограничения полосы пропускания, если они меньше общей максимальной полосы пропускания. В одном контракте могут быть абоненты с общей полосой пропускания и с индивидуальной.

```
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
```

При использовании максимальной пропускной способности канала, скорость между участниками контракта распределяется пропорционально их активности.

Добавление записи общего контракта возможно по протоколу RADIUS или проприориетарному протоколу EcoBRAS, в зависимости от версии и лицензии встроенного программного обеспечения.

Конфигурация записи для клиента на RADIUS-сервере должна быть аналогична приведенной ниже (в качестве примера использована запись freeRADIUS).

```
192.168.55.5   Auth-Type := Accept
        Cisco-Accout-Info := "QU;5000000;D;5000000",
        Cisco-Accout-Info += "Pqq1",
        Cisco-Accout-Info += "VU;8000000;D;8000000",
```

Где:

Pqq1 - идентификатор контракта,

QU/QD - ограничение скорости данного клиента;

VU/VD - ограничение скорости скорости общего контракта.

В том случае, если заводится клиент с индивидуальными ограничениями полосы пропускания, то последний атрибут отсутствует. Такой клиент может быть включен в контракт с общими настройками полосы пропускания.

Для COA-запроса также должны появиться параметры:

```
Cisco-Account-Info := \"Pqq1\", Cisco-Account-Info :=
\"VU;2012000;D;2012000\"
```

При помощи протокола EcoBRAS добавление клиентов общего контракта осуществляется командой **ads**.

```
B: ads 24372 {oid} LIM10M/LIM10M 10.21.0.208, 10.210.0.207.95, // RULE43
E:
```

Детальный формат команды **ads** описан в таблице ниже.

Таблица 39

№	Поле	Содержание поля	Описание поля
1	ads	3 символа	Команда – добавить общий контракт
2		TAB	Разделитель
3	24372	Цифры	Номер контракта
4		TAB	Разделитель
5	{oid}	Строка 5 символов	Тип контракта (в нашем случае всегда фиксированная строка '{oid}')
6		SPACE	Разделитель
7	LIM10M	Строка: LIM значение скорости K/M/G или UNLIM	Скорость downstream (из Интернета). K/M/G – означают кило/мега/гига бит. Например, LIM64K – 64 Кбит/с. UNLIM – без ограничений скорости
8	/	Символ '/'	Разделитель
9	LIM10M	строка	Скорость upstream (в Интернет)
10		SPACE	Разделитель пробел
11	10.21.0.208,	IP-адрес, разделитель ‘,’	IP-адрес абонента (могут следовать несколько подряд, каждый из IP-адресов получает те скорости, которые заданы для этого контракта)
12		SPACE	Разделитель
13	//	2 символа	
14		SPACE	Разделитель
15	RULE	4 символа	
16	43	Число	Идентификатор конкретного правила в таблице EcoBRAS
17		LF	Конец строки запроса

При добавлении нового абонента, входящего в общий контракт, требуется повторно указать ограничение скорости общего контракта, так как происходит замена значения, указанного при предыдущем добавлении.

8 Функциональность URL-фильтрации (DPI)

Данная функциональность доступна на основе лицензии EcoDPIxxxx-LIC (о том, как посмотреть лицензию, см. "Помощь пользователям).

Функциональность URL-фильтрации (DPI) позволяет провайдерам выполнять требования Федерального закона № 139-ФЗ от 28 июля 2012 года в отношении фильтрации нежелательных и запрещённых ресурсов в сети Интернет, а также оказывать услуги типа «детский интернет» с фильтрацией по большим спискам. Этот функционал удовлетворяет всем требованиям и прошел тестирование Роскомнадзора (официальное заключение доступно по ссылке http://www.rkn.gov.ru/docs/Izobrazhenie_29.09.2017.tiff).

Перенаправление пользователя на страницу блокировки («ресурс запрещён») задается индивидуально для каждого списка. Поддерживается фильтрация по подсетям.

Для HTTPS поддерживается фильтрация по SNI (Server Name Indication) с разрывом соединения с запрещённым ресурсом. В случае отсутствия в запросе поля SNI, запрос пропускается прозрачно. При этом проверяется входящий сертификат сервера, на который был отправлен запрос. Если в сертификате указан запрещённый фильтрами сайт, соединение с сервером обрывается.

Основной список запрещённых сайтов – это реестр Роскомнадзора (он имеет предопределенное имя **dpilist0** в конфигурационном пространстве **system dpi**).

Также поддерживаются до 16 списков сайтов, задаваемых пользователем (**dpilist1 ... dpilist16**), каждый из которых может быть либо чёрным (список запрещённых сайтов), либо белым (список разрешённых сайтов).

Формат загружаемых списков: текстовый файл с перечнем URL, начинающихся на “http://” или “https://”, в которых также может указываться номер порта. Также в записи URL может использоваться символ ***** для указания любого набора символов, например, для фильтрации нескольких сайтов-зеркал. Если необходимо фильтровать и HTTP, и HTTPS, то ***** ставится в начале URL, если только один из протоколов, то перед ***** указывается префикс. В списках могут быть указаны IP-адреса, подсети или диапазоны адресов (через дефис). Разделителем выступает CR или CR LF (конец строки и переход на новую строку). Имя и расширение файла не регламентируются.

Пример файла:

```
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/
ru.wikipedia.org/wiki/GRE_(протокол)
8.8.8.0/24
3.3.3.1
5.5.5.5-5.5.5.150
```

Если в загружаемом списке URL представлен без префикса “http://” или “https://”, то по умолчанию считается, что в списке он фигурирует и с префиксом “http://”, и “https://”.

При этом, фильтр для HTTPS соединений будет реагировать только на указанное доменное имя. То есть, при приведенном в примере написании ссылки на статью Википедии, будут закрываться все соединения, пытающиеся получить доступ к русскоязычной Википедии. Таким образом, если требуется закрыть доступ только к одной статье, в списке должно быть указано "http://ru.wikipedia.org/wiki/GRE_(протокол)".

Абонент может одновременно фильтроваться по нескольким спискам. В случае срабатывания нескольких списков одновременно, действие будет осуществляться в соответствии с наиболее приоритетным из них (тем, у которого меньше номер).

Чёрный список – список запрещённых сайтов. Срабатывание по нему означает запрещение доступа к странице. В этом случае HTTP соединение будет перенаправлено на заданную в конфигурации страницу, а HTTPS соединение будет закрыто по RST.

Белый список наоборот содержит разрешённые сайты. Срабатывание по нему означает разрешение доступа к странице. Отсутствие события по белому списку означает, что доступ по умолчанию запрещён (и будет осуществлено перенаправление или закрытие), но абонент может быть подписан на несколько белых списков одновременно, в этом случае для доступа к странице достаточно, чтобы сработал хотя бы один из них.

8.1 Настройка URL-фильтрации

Настройки функционала URL-фильтрации (DPI) хранятся в ветке конфигурационного дерева **system dpi**. В данной ветке находятся общие системные настройки URL-фильтрации и настройки списков сайтов, которые в концепции EcoNAT называются **dpilistN**, где **N** - порядковый номер от 0 до 16.

```
MyEcoNAT:1:# system dpi
MyEcoNAT:2:system.dpi# show
enable
functionality_mode normal_nat
certificate_file "cert.pem"
dpilist0
{
enable
 rkn_login "0123456789"
 rkn_password "q1w2e3r4t5y6u7i8o9p0"
 rkn_proxy ""
whitelist_mode off
log_matches off
 log_pictures off
exceptions off
behavior 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
no_ip ( 10.210.0.133 )
```

```
ip ( 10.0.0.0/8
61.216.14.0/23
)
}
dpilist1
{
disable
whitelist_mode off
log_matches off
 log_pictures off
exceptions off
behavior 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
no_ip ( )
ip ( 10.0.0.0/8 )
}…
```

Для включения и выключения функциональности URL-фильтрации используются команды **enable** и **disable** в контексте ветки **system dpi** конфигурационного дерева .

Кроме того, каждый из списков сайтов может быть индивидуально включён/выключен командами **enable** и **disable** , запущенными в конфигурационном пространстве списка, который мы хотим сконфигурировать.

EcoNAT может быть подключен в двух режимах:

- обычный NAT, стоящий «в разрыв» соединения (на первом рисунке ниже),
- режим двойного зеркалирования трафика (на втором рисунке ниже).

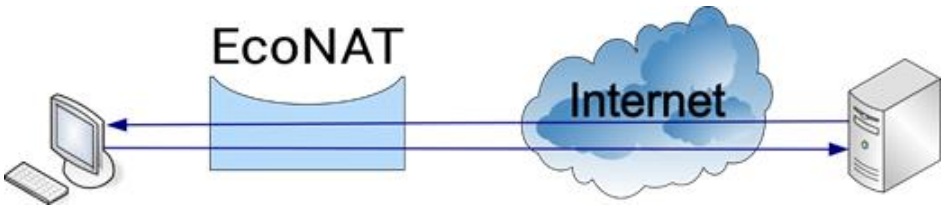

Рисунок 17

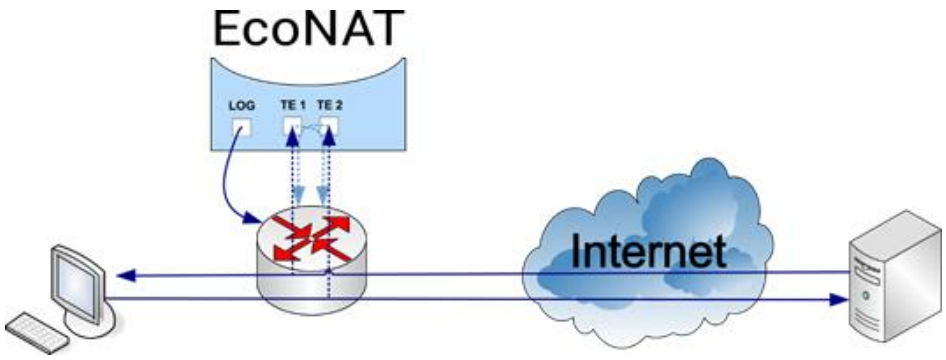

Рисунок 18

Режимы функционирования EcoNAT переключаются параметром **functionality_mode**, который может принимать значения, соответственно, **normal_nat** и **double_mirrored_traffic**. Для переключения режимов необходимо выполнить команду **functionality_mode normal_nat** или **functionality_mode double_mirrored_traffic** в ветке **system dpi** конфигурационного дерева.

В режиме зеркалирования EcoNAT слушает входящий и исходящий трафик, осуществляя его трансляцию, как и в обычном режиме. При этом исходящий от абонентов трафик зеркалируется на локальные (чётные) интерфейсы EcoNAT, а входящий из Интернета к абонентам – на глобальные (нечётные) интерфейсы EcoNAT (см. раздел "Интерфейсы"). В случае, если EcoNAT обнаруживает соединение с запрещённым ресурсом, он отправляет абоненту через маршрутизатор пакет прерывания соединения (для HTTPS) или пакет перенаправления (для HTTP). Для передачи пакетов перенаправления и прерывания соединения EcoNAT использует логирующий интерфейс или интерфейсы (см. раздел ""), тогда как в обычном режиме для этого используются те же сетевые интерфейсы, через которые проходит абонентский трафик. Поэтому для корректной работы схемы зеркалирования в EcoNAT должен быть настроен адрес шлюза по умолчанию в контексте конфигурации **connection_ log** (см. раздел "Логирование"). Также рекомендуется принять меры, чтобы предотвратить попадание дублирующего трафика обратно в сеть через интерфейсы, с которых зеркалируемый трафик направляется на EcoNAT.

Если на EcoNAT зеркалируется трафик с меткой (или с двойной меткой), то и пакеты перенаправления и прерывания соединения инкапсулируются соответствующим образом. Следовательно, необходимо обеспечить L2-связность логирующего интерфейса EcoNAT и интерфейса маршрутизатора (IP-адрес которого указан как шлюз по умолчанию в контексте конфигурации **connection_ log**). При этом можно настроить EcoNAT таким образом, чтобы из логирующего интерфейса отправлялся нетегированный трафик. Для этого необходимо в ветке конфигурационного дерева **connection_log** настроить значение параметра **strip_tags on**.

В таблице ниже приведены параметры для списков сайтов.

Таблица 40

Параметр	Описание
enable или disable	Определяет активность данного списка
whitelist_mode	Определяет, является ли список белым или чёрным. Чёрный список (значение параметра - **off**) показывает сайты, на которые нельзя ходить. Белый список (значение параметра - **on**) показывает сайты, на которые можно ходить (используется, например, для организации «детского интернета»). **ВНИМАНИЕ! При использовании белого списка возможна полная блокировка доступа (см. пояснение внизу таблицы)**

Параметр	Описание
log_matches	Определяет, включено ли логирование посещения запрещённых сайтов на сервере
log_pictures	Определяет, включено ли логирование имеющихся на сайте картинок. Учитываются файлы форматов: *.bmp, *.gif, *.jpeg, *.jpg, *.png, *.tif, *.tiff
exceptions	Применяет список исключений к данному **dpilist**. Значения: **on**, **off**
behavior	Определяет то, какое действие будет предприниматься при срабатывании условия данного списка (для чёрного) или не срабатывании (для белого списка): **block** - блокировка HTTPS (HTTP перенаправляется), **redirect** - перенаправление HTTP (HTTPS проходит), **ignore** - нет определенного действия
redirect_use_interval	Включает использование таймеров перенаправления. При выключении этого параметра, перенаправление будет срабатывать каждый раз при попытке зайти на любой сайт из списка. Значения: **on**, **off**
redirect_interval	Интервал между перенаправлениями для сайтов списка, в секундах. По умолчанию 10 минут (600). После первого перенаправления все остальные сайты из списка будут в течение 10 мин открываться в обычном режиме
redirect_interval_url	Интервал между перенаправлениями одной и той же страницы. По умолчанию 30 суток (2592000). При попытке зайти на страницу из списка срабатывает перенаправление. После этого данная страница будет открываться в обычном режиме в течение 30 суток, потом снова сработает перенаправление
redirect_url	URL, куда будет перенаправлено HTTP-соединение в случае, если условие списка сработало (для чёрного списка) или не сработало (для белого списка). EcoNAT позволяет добавлять в адресную строку спецификаторы, указывающие на клиента. Что позволяет персонализировать страницу переадресации. Возможные спецификаторы: **%c** - передавать в redirect_url callback-id, полученный от RADIUS-сервера; **%m** - передавать в redirect_url mac адрес клиента; **%i** - передавать в redirect_url ip адрес клиента; **%v1** - передавать в redirect_url первый (верхний) vlan клиента; **%v2** - передавать в redirect_url второй (нижний) vlan клиента; **%u** - передавать в redirect_url url, на который обратился клиент. Формат ввода параметра **redirect_url**: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>=<SPEC2>..<VAR_NAMEN>=<SPECN>** где **URL** - адрес страницы, на которую осуществляется перенаправление, **VAR_NAME1** .. **VAR_NAMEN** - имя переменной, **SPEC1** .. **SPECN** - спецификатор. Например, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. Если при таком значении параметра клиент попробует обратиться на адрес **forbidden.com**, то он будет перенаправлен на адрес: **http://example.com/?var1= forbidden.com&ip=10.1.1.10&qwe=0**
color_direction	Маркируемое направление трафика: **egress** - маркируется трафик от пользователя в Интернет, **ingress** - маркируется трафик из Интернета к пользователю, **both** - маркируются оба направления трафика, **no** - трафик не маркируется
color_tos_byte	Значение, которое будет устанавливаться в поле **type of service** в заголовке пакета, задается в десятичном формате. Для того чтобы не маркировать трафик, необходимо оставить значение: **nochange**
download_url	URL откуда будет выкачиваться список в случае автообновления (поддерживаются протоколы HTTP, FTP, TFTP). Для списка **dpilist0** - адрес,

Параметр	Описание
	по которому будет храниться предварительно скаченный список Роскомнадзора
update_schedule	Расписание, по которому будет автоматически обновляться список. Возможные форматы расписания: **never** – никогда не обновлять, **interval <SECONDS>** – интервал в секундах между автообновлениями. Рекомендуется ставить значения не меньше чем 1 час (3600 секунд). Крайне не рекомендуется ставить значения меньше чем 5 минут (300 секунд)
no_ip	Список IPv4-адресов, которые исключаются из сферы действия списка (параметр **no_ip** обрабатывается раньше, чем **ip**)
ip	Список IPv4-адресов, которые попадают под действие списка
no_ipv6	Список IPv6-адресов, которые исключаются из сферы действия списка (параметр **no_ipv6** обрабатывается раньше, чем **ipv6**)
ipv6	Список IPv6-адресов, которые попадают под действие списка. Для того чтобы указать обработку всех адресов необходимо указать: **::/0**
Параметры только dpilist0 (списка Роскомнадзора)	
rkn_login	Логин. Данные для авторизации в системе Роскомнадзора
rkn_password	Пароль. Хранится в зашифрованном виде. Данные для авторизации в системе Роскомнадзора
rkn_proxy	Прокси-сервер. Указывается в формате **[<PROTOCOL>://][<USER>:<PASSWORD>@]<URL>[:<PORT>]**, где: **PROTOCOL** - протокол проксирования, SOCKS4, SOCKS5 или HTTPS(S), если параметр не указан - используется HTTP; **USER** - имя пользователя для не анонимного прокси-сервера; **PASSWORD** - пароль для не анонимного прокси-сервера; **URL** - IP-адрес или доменное имя прокси-сервера, обязательный параметр; **PORT** - порт на котором слушает прокси, в случае отсутствия будет использован 1080/TCP

ВНИМАНИЕ!

При использовании белого списка возможна полная блокировка доступа!

При установке значения параметра whitelist mode on и добавлении в список хотя бы одного IP-адреса (например, 127.0.0.1), для клиентов, указанных в настройке dpilist будут заблокированы все IP-адреса, кроме 127.0.0.1.

В белом списке могут содержаться только IP-адреса, только URL или IP-адреса и URL.

В случае если в списке присутствуют IP-адреса и URL, то для каждого URL должен быть прописан соответствующий IP-адрес (адреса), в который он будет преобразовываться.

Если в dpilist присутствуют только URL, то IP-адреса прописывать не надо.

Если адрес входит в диапазон, указанный в значении параметра **ipv6**, на EcoNAT создаются соответствующие абонентские сессии. Состояние этих сессий можно проверить при помощи команды **show sessions local any**.

```
MyEcoNAT:3: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.
```

Для диагностики IPv6 используется ряд счетчиков, представленных в таблице ниже.

Таблица 41

Счетчик	Описание
cr_ipv6_table_entries	Число записей в таблице IPv6-сессий
cr_ipv6_established_sessions	Общее количество установленных IPv6-сессий
cr_ipv6_egress_packets	Количество IPv6-пакетов в egress направлении
cr_ipv6_ingress_packets	Количество IPv6-пакетов в ingress направлении
cr_ipv6_egress_bytes	Количество байт переданных в egress направлении по протоколу IPv6
cr_ipv6_ingress_bytes	Количество байт переданных в ingress направлении по протоколу IPv6

8.2 Загрузка списков

8.2.1 Ручная загрузка списков сайтов для URL-фильтрации

Ручная загрузка возможна для списков с номерами от 1 до 16 (список с номером 0 зарезервирован для реестра Роскомнадзора). Для ручной загрузки списков используется команда **dpiload** ***<номер списка>*** ***<URL>***, где **URL** вводится в формате **http://<адрес сервера>/<имя файла>.<расширение файла>** (подробнее о содержимом файла списка см. в разделе "Функциональность URL-фильтрации (DPI) ").

Для загрузки списков поддерживается базовая аутентификация на целевом и FTP серверах. Синтаксис команд загрузки с использованием аутентификации **dpiload** ***<номер списка>*** **http://<имя пользователя>:<пароль>@<адрес сервера>/<имя файла>**

dpiload ***<номер списка>*** ***f*****tp://<имя пользователя>:<пароль>@<адрес сервера>/<имя файла>**.

Например, чтобы загрузить с http-сервера ***1.1.1.1*** список ***black_list.txt***, соответствующий списку **1** в системе, требуется зайти на http-сервер под именем ***username*** с вводом пароля ***password***. В таком случае используется следующая команда:

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

Для выполнения аналогичных действий на FTP-сервере, используется следующая команда:

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

Предварительно рекомендуется отключить автоматическое обновление списка, поставив параметр **update_schedule** в значение **never**.

При вводе команды **dpiload 0** инициируется обновление реестра с сервера Роскомнадзора. Если в настройках списка **dpilist0** указан параметр **download_url**, и при этом сайт Роскомнадзора недоступен для EcoNAT, то загрузка будет производиться с указанного в параметре **download_url** адреса.

Пример:

```
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
```

Рекомендуется сначала загрузить список с помощью команды **dpiload**, затем включить список в конфигурационном пространстве **system dpi dpilist<*номер*>** и настроить прочие параметры.

Измененная конфигурация применяется только после выполнения команды **apply**.

Для просмотра списков сайтов и файлов для работы URL-фильтрации используется команда **dpilist** (см. раздел "Управление списками").

8.2.2 Автоматическая загрузка списков по расписанию

Для автоматической загрузки списка по расписанию список должен быть включён (**enable**), и значение параметра **update_schedule** должно отличаться от **never**.

8.2.3 Обновление базы сайтов

Все загруженные и включённые списки объединяются внутри EcoNAT в единую базу сайтов. При автоматической загрузке списков обновление базы происходит немедленно. В случае ручной загрузки списков необходимо принудительно запустить процесс обновления базы сайтов с помощью команды **dpirun**.

8.2.4 Автоматическая выгрузка реестра Роскомнадзора

Для автоматической выгрузки реестра Роскомнадзора можно использовать клиентский прокси-сервер. Данная настройка не является системной и не влияет на работу каких-либо других опций. В качестве протоколов проксирования возможно применение протоколов SOCKS4, SOCKS5 и HTTPS(S). Могут использоваться как анонимные, так и не анонимные прокси-сервера. Прокси-сервер можно использовать как с методом загрузки реестра полностью, так и с методом дельта-пакетов. Для включения функционала необходимо в параметре **rkn_proxy** секции **system.dpi.dpilist0** указать прокси-сервер в формате

[<PROTOCOL>://][<USER>:<PASSWORD>@]<URL>[:<PORT>], где:

PROTOCOL - протокол проксирования, SOCKS4, SOCKS5 или HTTPS(S), если параметр не указан - используется HTTP;

USER - имя пользователя для не анонимного прокси-сервера;

PASSWORD - пароль для не анонимного прокси-сервера;

URL - IP-адрес или доменное имя прокси-сервера, обязательный параметр;

PORT - порт на котором слушает прокси, в случае отсутствия будет использован 1080/TCP

На данный момент существует две схемы автоматической выгрузки из реестра Роскомнадзора: с авторизацией по по логину/паролю и с авторизацией по сертификату.

Авторизация по логину

Для включения автоматической выгрузки реестра Роскомнадзора по логину/паролю в настройках списка **dpilist0** должны быть указаны значения соответствующих параметров **rkn_login**, **rkn_password** (см. Настройка URL-фильтрации). Если данные настройки не выполнены, обновление реестра будет производиться по сертификату (см. ниже).

При автоматической выгрузке реестра Роскомнадзора по логину/паролю выгрузка производится дельта-пакетами. В этом случае рекомендуется установить значение параметра **update_scheduler 60** (ежеминутная выгрузка).

Авторизация по сертификату

Для включения автоматической выгрузки реестра Роскомнадзора по сертификатам необходимо выполнить следующие команды:

- **dpiload request <*URL*>** – Загружает *.xml файл запроса к Роскомнадзору (содержит данные о провайдере: ИНН, ОГРН и наименование);
- **dpiload sign <*URL*>** – Загружает подписанный цифровым сертификатом файл запроса к Роскомнадзору *.xml.sig.

Данные файлы необходимо заранее подготовить и выложить на каком-либо WEB или FTP сервере.

8.2.5 Выгрузка файла реестра Роскомнадзора на FTP/TFTP-сервер

Ручная выгрузка

В EcoNAT можно выгрузить уже скачанный файл реестра Роскомнадзора (вместе с дельтами) на сторонний FTP/TFTP-сервер. Для этого используется команда **copy rkn [PROTOCOL://][USER:PASSWORD@]<HOST>[:PORT][/PATH]**. Параметры данной команды описаны в таблице ниже.

Таблица 42

Параметр	Описание
PROTOCOL://	Протокол: **ftp** или **tftp**. Обязательный параметр
USER:PASSWORD@	Имя пользователя и пароль через '**:**'. Указывается, если на FTP-сервере включена авторизация
HOST	IP-адрес или доменное имя FTP/TFTP сервера. Обязательный параметр
:PORT	Порт, на котором слушает соответствующий сервис. По умолчанию будет использован стандартный порт для протокола
/PATH	Путь и имя файла, по которому файл будет сохранен на сервере. Указанная структура каталогов должна быть создана на сервере заранее. По умолчанию файл будет сохранен в корневом каталоге FTP/TFTP-сервера под именем **dumps.tar.gz**.

Файл **dumps.tar.gz** является архивом, содержащим первоначальный файл **dump.xml** и все имеющиеся на данный момент файлы дельт.

В случае проблем с копированием на сервер, будет выведено сообщение об ошибке с указанием подробностей.

Также будет выведена текущая версия файла **dump.xml** (количество дельта-обновлений, относительно первоначально скачанного **dump.xml**):

```
Actual last dump is X
```

Автоматическая выгрузка

Для автоматической выгрузки скачанного файла реестра Роскомнадзора (вместе с дельтами) на сторонний FTP/TFTP-сервер необходимо настроить параметр **upload_dump_server**. В котором указывается целевой сервер для выгрузки. Формат указания сервера, аналогичен используемому при ручной выгрузке (см. выше).

Механизм работы автовыгрузки следующий:

После добавления сервера в параметр **upload_dump_server** имеющийся **dump.xml** и дельты удаляются.

dump.xml скачивается полностью, после чего сразу же копируется на сервер в формате РКН (XML-файл сжатый ZIP).

При получении очередной дельты она так же сразу копируется на указанный сервер в таком же формате.

При возникновении ошибок автовыгрузки, в системном журнале будут появляться записи вида:

```
Jan 29 17:23:32 DPI [ERROR]: curl_easy_perform() failed: Timeout was
reached
```

8.3 Настройка URL-фильтрации для адресов, не подвергающихся NAT

По умолчанию устройство осуществляет URL-фильтрацию только для тех IP абонентов, которые попадают в какой-либо из пулов NAT (их IP адреса подпадают под ACL пула).

В случае, если какой-то диапазон IP-адресов абонентов не подвергается NAT (например, маршрутизируемые в интернет «реальные» адреса абонентов, скажем, из сети 194.85.16.0/24), для выполнения URL-фильтрации необходимо выполнить следующие действия:

Создать новый пул NAT.

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

Задать пулу тип **fake**.

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

Задать пулу **poolurl** минимальный приоритет.

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

Задать для пула те же **global_ip**, что и для соответствующего ACL.

```
MyEcoNAT:5:pools.poolurl# global_ip 194.85.16.0/24
```

Создать ACL.

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

Вписать в **aclurl** правила.

```
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
```

Применить конфигурацию.

```
MyEcoNAT:10: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
        global_ip (194.85.16.0/24)
        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'
```

*Данному вспомогательному пулу рекомендуется установить минимальный приоритет – т.е. значение параметра **priority** должно быть больше, чем у всех других пулов NAT (чем меньше значение **priority**, тем выше приоритет). Таким образом, в данном пуле будет обрабатываться трафик, который не обрабатывается другими NAT пулами.*

*Для корректного логирования событий и обработки трафика, необходимо прописывать в настройках **global_ip** пула типа **fake** те же IP-адреса, что и в привязанном к нему ACL.*

*Вспомогательный пул типа **fake** позволяет осуществлять логирование соединений с соответствующих IP-адресов по протоколам Syslog и Netflow.*

8.4 Управление списками

8.4.1 Команды управления списками

Для удаления списков или файлов, использующихся при настройке URL-фильтрации, используется команда **dpierase <номер списка или файл>**.

Для просмотра загруженных списков сайтов и файлов для работы URL-фильтрации используется команда **dpilist**.

```
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
```

Для просмотра содержимого списков сайтов в интерфейсе EcoNAT используются команды **show dpirecords** и **dpiview**.

8.4.2 Show dpirecords

Команда выводит на консоль записи из списка сайтов.

Синтаксис команды: **show dpirecords <номер списка> | [фильтры]**.

Для данной команды доступны фильтры, аналогично другим командам группы show (см. таблицу ниже).

Таблица 43

Фильтр	Описание
| b STRING | begin STRING	Пропускает строки, пока не дойдет до строки, содержащей указанную подстроку
| count	Считает количество строк
| e STRING | exclude STRING	Выводит только строки, не содержащие указанную подстроку
| drop NUM	Пропускает указанное количество строк
| i STRING | include STRING	Выводит только строки, содержащие указанную подстроку. Если подстрока содержит пробелы или специальные символы типа ‘)’, то можно использовать кавычки
| more	Осуществляет вывод с остановкой через каждую страницу
| r STRING | regexp STRING	Выводит только строки, удовлетворяющие указанному регулярному выражению
| take NUM	Выводит указанное количество строк

Пример вывода команды:

```
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
```

8.4.3 Dpiview

Команда выводит на консоль записи из списка URL-фильтрации или содержимое файлов, использующихся при настройке URL-фильтрации.

Синтаксис команды: **dpiview <номер списка или название файла>**. Для данной команды нет возможности фильтрации, частичного вывода или прерывания вывода. В качестве параметра команды можно указывать не только номер конкретного списка, но и следующие файлы:

- cert – показать содержимое файла сертификата,
- dump – показать содержимое файла реестра Роскомнадзора,
- request – показать содержимое файла запроса сертификата,
- sign – показать подписанный файл запроса сертификата,

и других файлов (например, shortlist, exceptions), если они есть.

Пример вывода команды:

```
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>
```

8.4.4 Настройка исключений

При необходимости, для списков можно настроить исключения.

Для того чтобы добавить исключения, необходимо сформировать текстовый файл со списком адресов-исключений, аналогично тому, как описано в разделе "Функциональность URL-фильтрации (DPI) ". После чего файл загружается вручную командой **dpiload exception <URL>,** где **URL** вводится в формате **http://<адрес сервера>/<имя файла>.<расширение файла>**. Далее необходимо включить исключения для конкретного списка сайтов, к которому они будут применяться, установив значение параметра списка **exceptions on**. Адреса из списка исключений будут запрещены, если исключения применяются к белому списку, или разрешены, если исключения применяются к чёрному списку.

В записи URL в списке исключений может использоваться символ ***** для указания любого набора символов, например, для фильтрации нескольких сайтов-зеркал. Если необходимо фильтровать и HTTP, и HTTPS, то ***** ставится в начале URL, если только один из протоколов, то перед ***** указывается префикс.

Пример настройки параметров списка:

```
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 )
```

8.5 Перенаправление пользователей

Функционал URL-фильтрации оборудования EcoNAT позволяет осуществлять периодическое перенаправление пользователей с определенных сайтов (например, сайтов конкурентов) по таймеру.

Настройка периодического перенаправления пользователей работает только для HTTP. В случае использования HTTPS, соединение будет установлено без перенаправлений.

Для настройки периодических перенаправлений, в соответствующий **dpilist** должен быть вручную загружен список сайтов, для которых необходимо осуществлять перенаправление. Подробнее о формировании и загрузке такого списка, см. в разделе "Загрузка списков".

Далее необходимо настроить параметры списка, в том числе, таймеры перенаправлений и адрес, на который будет перенаправлен пользователь, например, это может быть страница оператора с описанием услуг и специальных предложений.

Механизм перенаправления автоматически срабатывает, когда пользователь в первый раз заходит на любой сайт из списка. С этого момента начинают свой отсчет таймеры. Один из таймеров (**redirect_interval**) отсчитывает время до следующего перенаправления по всем остальным адресам из списка, второй – время до следующего перенаправления по первому сработавшему адресу (**redirect_interval_url**).

Например, если загружен список адресов:

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

Для списка установлены:

- redirect_interval – 10 минут,
- redirect_interval_url – сутки.

Пользователь заходит на rg.ru, и его сразу перенаправляет на страницу оператора. После этого он может в течение суток заходить на rg.ru, после чего снова сработает перенаправление. В то же время, на остальные сайты из списка он может свободно заходить в течение 10 минут. После этого он заходит, допустим, на ya.ru, и его перенаправляет на сайт

оператора. Сутки после этого ya.ru открывается в нормальном режиме, потом снова идет перенаправление.

Параметры, которые необходимо настроить для периодических перенаправлений представлены в таблице ниже.

Таблица 44

Параметр	Описание
system dpi dpilist<NUMBER>	
redirect_interval	Интервал между перенаправлениями для сайтов списка, в секундах. По умолчанию 10 минут (600). После первого перенаправления все остальные сайты из списка будут в течение 10 мин открываться в обычном режиме
redirect_interval_url	Интервал между перенаправлениями одной и той же страницы. По умолчанию 30 суток (2592000). При попытке зайти на страницу из списка срабатывает перенаправление. После этого данная страница будет открываться в обычном режиме в течение 30 суток, потом снова сработает перенаправление
behaviour redirect	Задаёт поведения списка – перенаправление
redirect_use_interval on	Включает использование таймеров перенаправления. При выключении этого параметра, перенаправление будет срабатывать каждый раз при попытке зайти на любой сайт из списка
redirect_url	Адрес страницы, на которую будет производиться перенаправление. EcoNAT позволяет добавлять в адресную строку спецификаторы, указывающие на клиента. Что позволяет персонализировать страницу переадресации. Возможные спецификаторы: **%c** - передавать в redirect_url callback-id, полученный от RADIUS-сервера; **%m** - передавать в redirect_url mac адрес клиента; **%i** - передавать в redirect_url ip адрес клиента; **%v1** - передавать в redirect_url первый (верхний) vlan клиента; **%v2** - передавать в redirect_url второй (нижний) vlan клиента; **%u** - передавать в redirect_url url, на который обратился клиент. Формат ввода параметра **redirect_url**: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>=<SPEC2>..<VAR_NAMEN>=<SPECN>** где **URL** - адрес страницы, на которую осуществляется перенаправление, **VAR_NAME1** .. **VAR_NAMEN** - имя переменной, **SPEC1** .. **SPECN** - спецификатор. Например, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. Если при таком значении параметра клиент попробует обратиться на адрес **forbidden.com**, то он будет перенаправлен на адрес: **http://example.com/?var1= forbidden.com&ip=10.1.1.10&qwe=0**

Пример настройки списка:

```
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 )
}
```

8.6 Shortlist

8.6.1 Настройка shortlist

В функционале URL-фильтрации возможна настройка логирования на внешний сервер без блокировки соединений.

Для этого необходимо сформировать текстовый файл со списком адресов, аналогично тому, как описано в разделе Загрузка списков. После чего файл загружается вручную командой **dpiload shortlist <*URL*>**, где **URL** вводится в формате **http://<адрес сервера>/<имя файла>.<расширение файла>**.

Далее необходимо настроить параметры **shortlist** в ветке конфигурации **system dpi shortlist**: включить опцию (**enable**), указать адрес и порт сервера, на который будут отправляться логи, а также указать сдвиг времени в минутах (**timeskew <MINUTES>**) для логов.

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

После этого для определенного списка адресов (**shortlist**) будет вестись логирование всех событий URL-фильтрации на указанный сервер. Эта опция автоматически применяется ко всем спискам.

8.6.2 Настройка логирования URL-фильтрации

Для включения логирования в параметрах списков сайтов, нужно установить **log_matches on.** Если данный параметр будет включен, но в ветке конфигурации **system dpi shortlist** (см. предыдущий пункт) не указан адрес сервера, на который отправляются логи, логирование работать не будет.

Если необходимо вести логирование без блокировки или перенаправления, то в параметрах списка сайтов нужно установить **behaviour ignore** (при установке других значений параметра **behaviour**, логирование также будет работать).

```
dpilist1
{
 enable
```

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

8.6.3 Настройка сервера shortlist

Записи событий URL-фильтрации направляются на сервер, на котором запущена программа **shortlist_server** (предоставляется производителем по запросу).

Взаимодействие с программой-сервером осуществляется в терминале сервера, на котором она установлена, при помощи команды **./shortlist_server <флаги>**.

Используются следующие флаги:

- -c – вырезать картинки и прочие контентные файлы,
- -d – задать формат файлов, в которые будут писаться логи (см. ниже),
- -f – запись лога в один файл,
- -i – IP-адрес, на который приходят логи (если у сервера задействовано несколько интерфейсов),
- -h – показать помощь и выйти,
- -p – UDP-порт, на который приходят логи (его нужно указать в ветке конфигурационного дерева **system dpi shortlist**),
- -t – выводить логи непосредственно на терминал.

Можно указывать несколько флагов одновременно (например, чтобы велась запись логов в файл и выводилась на терминал).

Так как логируемых событий URL-фильтрации может быть много, в программе есть возможность вести запись логов группами, формируемыми по временному признаку. Например, создавать отдельный файл каждый день или каждый час. Для задания формата такой записи логов служит флаг -d. В таблице ниже представлены возможные коды этого флага и соответствующие им форматы. Если указан флаг **-d %F.log**, то файлы логов будут формироваться по дням, а формат их названий будет YYYY-MM-SS.log, например, 2016-05-10.log.

Таблица 45

Код	Описание
%a	Сокращенное название дня недели
%A	Полное название дня недели
%b	Сокращенное название месяца
%B	Полное название месяца
%c	Стандартная строка даты и времени
%C	Две последние цифры года
%d	День месяца в виде десятичного числа (1-31)
%D	Дата в виде месяц/день/год
%e	День месяца в виде десятичного числа (1-31) в двух-символьном поле
%F	Дата в виде "год-месяц-день"

Код	Описание
%g	Последние две цифры года с использованием понедельного года
%G	Год с использованием понедельного года
%h	Сокращенное название месяца
%H	Час (0-23)
%j	Час (1-12)
%j	День года в виде десятичного числа (1-366)
%m	Месяц в виде десятичного числа (1-12)
%M	Минуты в виде десятичного числа (0-59)
%n	Разделитель строк
%p	Местный эквивалент AM (до полудня) или PM (после полудня)
%r	12-часовое время
%R	Время в виде чч:мм
%S	Секунды в виде десятичного числа (0-60)
%T	Горизонтальная табуляция
%T	Время в виде чч:мм:сс
%u	День недели; понедельник – первый день недели (0-6)
%U	Неделя года; воскресенье – первый день недели (0-53)
%V	Неделя года с использованием понедельного года
%w	День недели в виде десятичного числа (0-6, воскресенье – 0-й день)
%W	Неделя года; понедельник – первый день недели (0-53)
%x	Стандартная строка даты
%X	Стандартная строка времени
%y	Год в виде десятичного числа без столетия (0-99)
%Y	Год в виде десятичного числа, включающего столетие
%z	Сдвиг относительно координированного всемирного (UTC) времени
%Z	Название часового пояса
%%	Знак процента

8.7 ЦАИР

В системе EcoNAT реализована поддержка базы ЦАИР (Центра Анализа Интернет-Ресурсов). Для подключения базы необходима соответствующая лицензия.

Список подключенных лицензий доступен по команде **show license**.

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

При установке данной лицензии в ветке конфигурационного дерева **system dpi** появляется элемент **cair**. Этот элемент является модифицированной версией списка DPI, со следующими доступными параметрами:

```
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
```

Где:

base_url - адрес базы ЦАИР,

uplevel_domains_url - адрес базы доменов верхнего уровня,

update_schedule - расписание автоматического обновления базы.

Для скачивания базы ЦАИР вручную используется команда **dpiload cair**.

Для скачивания базы доменов верхнего уровня используется команда **dpiload uplevel**.

Для корректной работы фильтра необходимо периодически обновлять обе базы.

В упомянутых выше базах информация о сайтах хранится в виде **<md5 хеш hostname> <номера категорий в 16-ричном виде через двоеточие>**. В базе содержатся только домены, т.е. "www.example.com", но не "www.example.com/theme/1".

Например:

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

Все домены, указанные в списке ЦАИР, блокируются аналогично принципу блокировки записей типа «domain-mask». Например, если в базе ЦАИР есть запись вида "example.com", то будет осуществляться фильтрация http и https запросов на ресурсы: "www.example.com", "help.example.com", "123.example.com" и так далее.

Для включения категорий в действие одного из списков DPI используется параметр **cair_categories** в котором категории также указываются в 16-ричном виде через двоеточие.

Пример.

```
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 )
```

Список категорий и соответствующие им номера представлены в таблице ниже.

Таблица 46

Номер 10-ричный	Номер 16-ричный	Категория
1	1	алкоголь
2	2	эротика, порнография
32	20	компьютерные игры
48	30	сайты знакомств
53	35	нелегальная помощь школьникам и студентам
54	36	убийства, насилие, самоубийство
55	37	онлайн-казино

Номер 10-ричный	Номер 16-ричный	Категория
56	38	социальные сети
57	39	терроризм, экстремизм
60	3c	обеспечение анонимности, обход контентных фильтров
62	3e	файлообменные сети и сайты
63	3f	табак
65	41	наркотики
68	44	вредоносные программы
73	49	досуг и развлечения (негатив)
78	4e	доски объявлений
79	4f	неприличный и грубый юмор
84	54	баннерные сервера
92	5c	федеральный список экстремистских материалов
93	5d	детское порно
94	5e	магия, колдовство, оккультизм, теургия
99	63	ненужные (вредные) для школы

Для просмотра информации о категориях ЦАИР для отдельных адресов используется команда **show cairrecords <URL>**.

Пример.

```
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
```

ПРИЛОЖЕНИЕ А

Справочник команд

Краткое описание команд приведено в таблице ниже.

Обозначения:

Приоритет – минимальный уровень прав доступа пользователя, при котором команда доступна.

Режим:

- C – конфигурационный,
- C* – контекстные команды конфигурационного режима,
- O – операционный.

VALUE – вводимое значение параметра.

Таблица 47

Команда	Описание	Режим	Приоритет
( )	Очистить редактируемый конфигурационный элемент – массив	C	4
VALUE	Присвоить значение редактируемому конфигурационному элементу	C	4
(VALUE VALUE)	Присвоить значение редактируемому конфигурационному элементу – массиву	C	4
?	Контекстная помощь	O/C	0
helpme %	Вывод на консоль описания параметров и веток дерева, доступных на текущем уровне	O/C	0
!	Вывод на консоль веток, доступных на текущем уровне дерева конфигурации	O/C	0
{	Вход в редактируемый элемент в конфигурационном дереве	O/C	0
}	Выход из редактируемого элемента в конфигурационном дереве	O/C	0
+= (VALUE VALUE)	Добавить несколько значений к редактируемому конфигурационному элементу – массиву	C	4
+= VALUE	Добавить значение к редактируемому конфигурационному элементу – массиву	C	4
-= (VALUE VALUE)	Удалить несколько значений из редактируемого конфигурационного элемента – массива	C	4
-= VALUE	Удалить значение из редактируемого конфигурационного элемента – массива	C	4
#ИМЯ?	Присвоить значение редактируемому конфигурационному элементу или массиву	C	4
add (VALUE VALUE)	Добавить несколько значений к редактируемому конфигурационному элементу – массиву	C	4

Команда	Описание	Режим	Приоритет
add VALUE	Добавить значение к редактируемому конфигурационному элементу – массиву	C	4
apply	Применение конфигурации (безусловное)	C	8
clear brasdb all	Очистка записей об абонентах в BRAS	C	4
clear config	Обнуление текущей конфигурации	C	
clear counters	Сброс значений счетчиков	O/C	0
clear sessions all	Очистка таблицы трансляций	C	4
cloneacl SRCNAME NEWNAME	Создание копии ACL содержащую все правила, но имеющую другое имя	C	4
commit	Подтверждение применения конфигурации. В случае изменения конфигурации управляющего сетевого интерфейса его настройки применяются временно и откатываются назад если в течении двух минут не вызвана команда commit. Это позволяет не потерять возможность связь с устройством удаленно по сети в случае применения ошибочной конфигурации	O/C	1
CONFIGITEMNAME	Выбор текущего конфигурационного элемента	O/C	0
configure	Переход в конфигурационный режим	O	0
copy SRC_PROFILENAME DST_PROFILENAME	Копирование конфигурации в указанную. Неприменимо к factory и effective	C	5
copy hwinfo URL	Копирование информации об устройстве в файл на удаленном сервере	O	
create acl ACLNAME	Создание ACL	C	4
create pool POOLNAME	Создание пула	C	4
create user USERNAME level LEVEL secret SECRETTYPE SECRETSTRING	Создание пользователя	C	15
dir	Просмотр списка конфигураций	C	4
disable	Логическое выключение объекта конфигурации (например, пула)	C	4
dpilist	Просмотр загруженных файлов списков URL-фильтрации	O/C	0
dpirun	Обновление базы сайтов из загруженных и включённых списков URL-фильтрации	C	4
dropacls	Удаление всех ACL сразу	C	4
droppools	Удаление всех пулов сразу	C	4
droppolicies	Удаление всех политик сразу	C	4
dropradius	Удаление настроек RADIUS-сервера	C	4
dropservices	Удаление всех сервисов сразу	C	4
edit acl ACLNAME edit ACLNAME	Переход к указанному ACL в дереве конфигурации	O/C	0
edit date DATE	Установка новой даты на устройстве	C	14
edit datetime DATETIME	Установка новый даты и времени на устройстве	C	14
edit pool POOLNAME edit POOLNAME	Переход в дереве конфигурации к указанному пулу	O/C	0
edit time TIME	Установка времени на устройстве	C	14

Команда	Описание	Режим	Приоритет
enable	Логическое включение объекта конфигурации (например, пула)	C	4
end	Выход из конфигурационного режима	C	0
erase PROFILENAME	Удаление профиля с указанным именем. Профили factory и effective не удаляются. Если удалить профиль startup, то после загрузки система будет ждать пока пользователь зайдет в консоль и применит какую-нибудь конфигурацию	C	4
exit ..	Выход на уровень выше в конфигурации или выход из конфигурационного режима (в случае если мы находимся в корне конфигурационного дерева в конфигурационном режиме)	O/C	0
firmware download URL	Скачивание обновления прошивки с указанного сервера	O	
firmware install	Установка скачанного обновления прошивки	O	
firmware revert	Установка перезапуска с неактивной прошивки	O	
firmware rollback	Отмена перезапуска с неактивной прошивки	O	
firmware status	Вывод информации об установленных прошивках и их статусе	O	
firmware unlock	Сброс заблокированного процесса обновления прошивки	O	
goto pool POOLNAME	Переход в дереве конфигурации к указанному пулу	O/C	0
grant USERNAME LEVEL	Изменение уровня прав доступа пользователя	C	15
interface IFNAME down	Выключение сетевого интерфейса	C	4
interface IFNAME up	Включение сетевого интерфейса	C	4
list	Просмотр списка конфигураций	C	4
load effective	Загрузка эффективной конфигурации для редактирования	C	4
load factory	Загрузка заводской конфигурации по умолчанию	C	4
load PROFILENAME	Загрузка указанной конфигурации для редактирования	C	4
load startup	Загрузка стартовой конфигурации для редактирования	C	4
no acl ACLNAME	Удаление ACL	C	4
no pool POOLNAME	Удаление пула	C	4
no RULEPRIOIRTY	Удаление правила ACL (контекстная команда, допускается только внутри самой ACL)	C*	4
no use ACLNAME POOLNAME	Разорвать связь между пулом и ACL	C	4
no user USERNAME	Удаление пользователя	C	15
poweroff	Завершение работы EcoNAT и выключение питания	C	8

Команда	Описание	Режим	Приоритет
profiles	Просмотр списка конфигураций	C	4
quit	Закончить сеанс работы с консолью. Происходит выход из консоли (в конфигурационном режиме редактированная конфигурация не сохраняется)	O/C	0
reboot	Перезагрузка EcoNAT	C	8
remove (VALUE VALUE)	Удалить указанные несколько значений из содержимого текущего конфигурационного элемента – массива		4
remove VALUE	Удалить указанное значение из содержимого редактируемого конфигурационного элемента – массива	C	4
renum ACLNAME	Принудительная нумерация правил в ACL. Первому правилу будет присвоен номер 100. Номера остальных будут на 10 больше предыдущего	C	4
renum pools	Принудительная нумерация приоритетов всех пулов. Первому пулу (самому приоритетному) будет присвоен приоритет 100. Приоритет каждого следующего будет на 100 больше предыдущего	C	4
rollback	Отмена последних применённых настроек управляющего сетевого интерфейса	O/C	1
root top /	Переход к корню конфигурационного дерева	O/C	0
RULEPRIORITY allow [ip] [src] SRCADDR [dst] DSTADDR	Ввод правила ACL (контекстная команда, допускается только внутри самой ACL)	C*	4
RULEPRIORITY deny [ip] [src] SRCADDR [dst] DSTADDR	Ввод правила ACL (контекстная команда, допускается только внутри самой ACL)	C*	4
safe apply	Применение конфигурации (в случае изменения конфигурации управляющего сетевого интерфейса его настройки применяются временно и откатываются назад если в течении двух минут не вызвана команда commit). Это позволяет не потерять возможность связь с устройством удаленно по сети в случае применения ошибочной конфигурации	C	8
save PROFILENAME	Сохранение текущей редактируемой конфигурации под указанным именем. Неприменимо к factory и effective	C	5
save startup	Сохранение текущей редактируемой конфигурации как стартовой (не рекомендуется использовать, лучше применить конфигурацию с помощью apply, и если ее работа будет устраивать сделать ее стартовой с помощью команды write	C	5

Команда	Описание	Режим	Приоритет
setlog SUBSYSTEM LEVEL setlog all LEVEL	Установка уровня логирования. Изменяет системные значения. Не изменяет значения в текущей конфигурации	C	
show	Вывод на консоль дерева конфигурации в глубину от текущего конфигурационного элемента	O/C	0
| b STRING | begin STRING	Фильтр для команды show. Выбрасывает строки пока не дойдет до строки, содержащей указанную подстроку	O/C	0
| count	Фильтр для команды show. Считает количество строк	O/C	0
| e STRING | exclude STRING	Фильтр для команды show. Выводит только строки не содержащие указанную подстроку	O/C	0
| i STRING | include STRING	Фильтр для команды show. Выводит только строки содержащие указанную подстроку (Если подстрока содержит пробелы или специальные символы типа ‘)’, то можно использовать кавычки)	O/C	0
| more	Фильтр для команды show. Осуществляет вывод с остановкой через каждую страницу	O/C	0
| r STRING | regexp STRING	Фильтр для команды show. Выводит только строки, удовлетворяющие указанному регулярному выражению	O/C	0
show acl ACLNAME	Вывод на консоль правил, содержащихся в данном ACL	O/C	0
show algtable	Вывод информации о сессиях ALG	O/C	0
show arp all show arp IFNAME	Вывод информации об ARP	O/C	0
show bind	Вывод информации о привязке локальных IP-адресов к глобальным	O/C	0
show brasinfo IPADDR show brasinfo IPADDRRANGE	Вывод BRAS информации об указанном адресе	O/C	0
show brasinfo summary	Просмотр краткой статистики BRAS	O/C	0
show brasstate	Вывод информации о состоянии BRAS	O/C	0
show cairrecords URL	Вывод категорий ЦАИР по адресу	O/C	0
show cgnat errors	Просмотр ошибок выделения портов в CG-NAT пуле	O/C	0
show config effective	Просмотр содержимого примененной конфигурации (редактируемая конфигурация остается неизменной)	O/C	0
show config file PROFILENAME	Просмотр содержимого указанной конфигурации (редактируемая конфигурация остается неизменной)	O/C	4
show config startup	Просмотр стартовой конфигурации (редактируемая конфигурация остается неизменной)	O/C	0
show counters	Просмотр системных счетчиков	O/C	0
show cps	Вывод текущей скорости установления соединений	O/C	0
show fan	Вывод скорости вентиляторов	O/C	0

Команда	Описание	Режим	Приоритет
show interface all	Вывод информации обо всех сетевых интерфейсах	O/C	0
show interface brief	Вывод краткой информации о сетевых интерфейсах	O/C	0
show interface mng	Вывод информации о MGMT-интерфейсе	O/C	0
show interface IFNAME show interface all	Вывод информации об указанном сетевом интерфейсе (IFNAME – имя интерфейса, например, te7. Имя интерфейса соответствует номеру интерфейса на передней панели устройства)	O/C	0
show interface IFNAME counters show interface all counters	Просмотр счетчиков на указанном интерфейсе	O/C	0
show interface IFNAME traffic show interface all traffic	Просмотр информации о трафике, проходящем через интерфейс	O/C	0
show interface IFNAME traffic monitor show interface all traffic monitor	Просмотр информации о трафике, проходящем через интерфейс, в режиме реального времени	O/C	0
show interface transceiver IFNAME show interface transceiver all show sfp all	Вывод информации о трансиверах	O/C	0
show ipif	Вывод информации о настройках управляющего интерфейса	O/C	0
show memstat	Вывод статистики использования памяти	O/C	0
show neighbours IFNAME show neighbours all	Вывод информации, полученной от соседей по протоколу LLDP	O/C	0
show ntp	Вывод состояния синхронизации времени по протоколу NTP	O/C	0
show pool POOLNAME	Вывод содержимого конфигурации пула на консоль	O/C	0
show pool usage	Вывод информации об использовании пулов	O/C	0
show pools	Вывод содержимого всех пулов на консоль	O/C	0
show pool brief	Вывод краткой информации о редактируемых пулах	O/C	0
show power	Вывод состояния блоков питания	O/C	0
show resources	Вывод статистики ресурсов	O/C	0
show sessions gap ADDR:PORT	Вывод соединений для указанной пары: глобальный адрес + глобальный порт	O/C	0
show sessions global ADDRRANGE	Вывод соединений для указанного глобального адреса	O/C	0
show sessions gport PORT	Вывод соединений для указанного глобального порта	O/C	0
show sessions lap ADDR:PORT	Вывод соединений для указанной пары: локальный адрес + локальный порт	O/C	0
show sessions local ADDRRANGE	Вывод соединений для указанного локального адреса	O/C	0

Команда	Описание	Режим	Приоритет
show sessions lport PORT	Вывод соединений для указанного локального порта	O/C	0
show sessions rap ADDR:PORT	Вывод соединений для указанной пары: внешний адрес + внешний порт	O/C	0
show sessions remote ADDRRANGE	Вывод соединений для указанного внешнего адреса	O/C	0
show sessions rport PORT	Вывод соединений для указанного внешнего порта	O/C	0
show statistics	Вывод статистики занятых/свободных блоков портов	O/C	0
show tacacs	Вывод информации о соединении с TACACS сервером	O/C	0
show temperature	Вывод информации о температуре на ядрах процессоров	O/C	0
show time	Вывод текущего времени устройства (всегда в UTC)	O/C	0
show version	Вывод информации о версии установленного ПО	O/C	0
show version detail	Вывод детальной информации о версии установленного ПО	O/C	0
show xlate gap ADDR:PORT	Вывод всех текущих трансляций для указанной пары: глобальный адрес+ глобальный порт	O/C	0
show xlate gastat ADDRRANGE	Вывод статистики трансляций для указанного глобального адреса	O/C	0
show xlate global ADDRRANGE	Вывод всех текущих трансляций для указанного глобального адреса	O/C	0
show xlate gport PORT	Вывод всех текущих трансляций для указанного глобального порта (независимо от адреса)	O/C	0
show xlate lap ADDR:PORT	Вывод всех текущих трансляций для указанной пары: локальный адрес + локальный порт	O/C	0
show xlate lastat ADDRRANGE	Вывод статистики трансляций для указанного локального адреса	O/C	0
show xlate local ADDRRANGE	Вывод всех текущих трансляций для указанного локального адреса	O/C	0
show xlate lport PORT	Вывод всех текущих трансляций для указанного локального порта (независимо от адреса)	O/C	0
show xlate pool POOLNAME	Вывод трансляций для указанного пула	O/C	0
start	Запуск приема/передачи пакетов	C	15
stop	Остановка приема/передачи пакетов	C	15
up	Переход на один уровень выше в конфигурационном дереве	O/C	0
uptime	Вывод времени работы системы	O/C	0
use ACLNAME POOLNAME	Связать пул и ACL	C	4
who	Вывод аутентифицированных пользовательских сессий	O/C	0

Команда	Описание	Режим	Приоритет
whoami	Вывод на консоль информации о текущем пользователе данной консоли и его уровне привилегий	O/C	0
write	Сохранение эффективной конфигурации как стартовой	O/C	0