

EcoSGE

v. 3.1.4.0.80

Руководство пользователя

Установка и конфигурирование

Редакция: декабрь 2021 г.

EcoSGE v. 3.1.4.0.80. Руководство пользователя.
Установка и конфигурирование
Редакция: декабрь 2021 г.

© RDP

Телефон: +7 (495) 204-9-204

<http://rdp.ru/>

Оглавление

Введение	7
Условные обозначения	8
Список терминов и сокращений	9
1 Оборудование.....	11
2 Вход в систему.....	12
2.1 Подключение через последовательный порт.....	12
2.2 Подключение по протоколу SSH	12
3 Режимы работы консоли.....	14
4 Подсказки и горячие клавиши.....	15
5 Конфигурация	16
6 Управление конфигурациями.....	20
6.1 Просмотр конфигураций	20
6.2 Применение и сохранение конфигурации	20
6.3 Загрузка конфигурации.....	21
6.4 Копирование конфигурации.....	21
6.5 Удаление конфигурации.....	22
6.6 Запись конфигурации, которая будет использована при старте EcoNAT	23
7 Первичная настройка	24
7.1 Настройка управляющего сетевого интерфейса	24
7.2 Настройка подключения к EcoBypass	25
7.3 Настройка терминала	26
7.4 Настройка loopback	27
7.5 Настройка времени.....	27
7.6 Логирование.....	29
7.6.1 Настройка логирования абонентских соединений	29
7.6.2 Настройка системного логирования	35
7.6.3 Логирование протоколов	38
7.6.4 QoE.....	39
7.6.5 Логирование подключений к web-серверам	40
7.7 Создание и удаление пользователей	42
7.8 Остановка и перезагрузка системы	43
7.9 Помощь пользователям.....	44
7.10 Сервисные команды	44

7.10.1	Информация о системной памяти.....	44
7.10.2	Информация о ресурсах системы.....	45
7.10.3	Проверка температуры процессора и состояния блоков питания и вентиляторов	46
7.10.4	Сбор и выгрузка диагностической информации	47
7.10.5	Ошибки выделения портов.....	47
7.10.6	Счетчики.....	50
7.11	Операции с прошивкой.....	52
7.11.1	Обновление прошивки	52
7.11.2	Изменение параметров перезагрузки	53
7.12	Настройка TACACS	54
7.13	Настройка SNMP.....	55
7.14	Параметры LLDP.....	56
8	Конфигурирование NAT.....	57
8.1	Интерфейсы	57
8.1.1	Интерфейс "on a stick"	58
8.1.2	Команды просмотра интерфейсов	59
8.2	Принципы работы NAT	62
8.3	Пулы и ACL	62
8.3.1	Общие настройки.....	63
8.3.2	Создание пула	65
8.3.3	Создание ACL.....	70
8.3.4	Порядок определения пула для пакета.....	72
8.3.5	CGNAT-пул.....	72
8.3.6	Nat пул	73
8.3.7	Static пул (1_to_1)	74
8.3.8	Fake пул	75
8.3.9	IPv6 ACL.....	75
8.4	Типовые конфигурации NAT	76
8.4.1	NAT для доступа в Интернет	76
8.4.2	Участие в пиринговой сети с пересекающимися диапазонами адресов	78
8.5	Управление объектами конфигурации.....	79
8.5.1	Клонирование ACL	79
8.5.2	Отвязывание ACL от пула	79
8.5.3	Удаление пула.....	79

8.5.4	Удаление правил в ACL	79
8.5.5	Удаление всего ACL	79
8.6	Команды просмотра	80
8.6.1	Просмотр трансляций	80
8.6.2	Просмотр сессий	81
8.6.3	Удаление сессий	82
8.6.4	Просмотр привязок	83
8.6.5	Ошибки выделения порта	84
9	Функциональность BRAS	87
9.1	Настройки BRAS	87
9.2	Консоль биллинга и протокол EcoBRAS	88
9.2.1	Команда testRID	89
9.2.2	Команда add	89
9.2.3	Команда ads	90
9.2.4	Команда remove	91
9.2.5	Команда statall	92
9.2.6	Команда clearall	92
9.3	Команды CLI для мониторинга и управления BRAS	92
9.3.1	Команды просмотра	93
9.3.2	Команды закрытия сессий	96
9.3.3	Команды очистки веток конфигурации BRAS	97
9.4	Политики и сервисы	97
9.4.1	Сервисы	97
9.4.2	Создание и настройка политики	99
9.5	Настройка RADIUS	101
9.5.1	Настройка подключения к RADIUS-серверу	102
9.5.2	Группы RADIUS-серверов	104
9.5.3	Авторизация пользователя на RADIUS-сервере	106
9.5.4	Счетчики	108
9.6	Создание BRAS-сессии по DHCP пакетам	109
9.7	Общие контракты	110
9.7.1	Общие контракты и протокол RADIUS	110
9.7.2	Общие контракты и протокол EcoBRAS	111
10	Функциональность URL-фильтрации (DPI)	112

10.1	Настройка URL-фильтрации	113
10.2	Загрузка списков	119
10.3	Ручная загрузка списков сайтов для URL-фильтрации	119
10.4	Автоматическая загрузка списков по расписанию	120
10.5	Обновление базы сайтов	120
10.6	Автоматическая загрузка реестра Роскомнадзора	120
10.7	Выгрузка файла реестра Роскомнадзора на FTP/TFTP-сервер	121
10.8	Настройка URL-фильтрации для адресов, не подвергающихся NAT	122
10.9	Управление списками	124
10.10	Команды управления списками	124
10.10.1	Show dpirecords	124
10.10.2	Dpiview	125
10.10.3	Show dpimatch	125
10.10.4	Show dpistate	126
10.11	Настройка исключений	127
10.12	Перенаправление пользователей	128
10.13	Shortlist	130
10.13.1	Настройка shortlist	130
10.13.2	Настройка логирования URL-фильтрации	131
10.13.3	Настройка сервера shortlist	131
10.14	Фильтрация по базе ЦАИР	133
10.15	Фильтрация по базе SkyDNS	136
10.16	Фильтрация протоколов	138
ПРИЛОЖЕНИЕ А		140

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
<i>Курсив</i>	Примечания	<i>Предварительно рекомендуется отключить автоматическое обновление списка...</i>
Рамка, голубой цвет фона	Примеры вывода консоли	Также доступна синхронизация времени по NTP протоколу настраиваемая через следующий раздел конфигурации: <pre>system { ntp { disable primary_server "131.131.249.19"</pre>
Серый цвет фона	Примеры кода	После чего формируется файл запроса вида: <pre><?xml version="1.0" encoding="windows-1251"?> <request></pre>

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:# <i>no use myacl mypool</i>

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 Оборудование

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

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



Рисунок 1

Для оборудования 2-тысячной серии 10GbE 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 1GbE Copper. В CLI они называются **ge1 - ge6**. На устройствах 2020 в черном корпусе (старая модель) сетевые интерфейсы для логирования имеют скорость 1GbE и маркировку 5, 6.

На устройствах 2020, 2040 в синем корпусе сетевой интерфейс для логирования имеет скорость 1GbE и расположен над MNG-интерфейсом. В CLI он называется **ge0**. При этом все 6 интерфейсов могут быть использованы для трафика.

Оборудование управляется при помощи CLI консоли.

2 Вход в систему

Предусмотрены два варианта доступа к консоли управления EcoSGE: через последовательный порт или по протоколу SSH.

2.1 Подключение через последовательный порт

Разъём последовательного порта находится с левой стороны передней панели устройства и обозначен надписью "COM" (см. рисунок ниже). В комплект поставки устройства входит переходник с RJ-45 на DB-9.



Рисунок 4

Заводские настройки последовательного порта:

- 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 (т. е. сохранённым на самом устройстве). Вход по серийной консоли не логируется через TACACS+.

Серийную консоль нельзя запретить – она будет всегда доступна.

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

2.2 Подключение по протоколу SSH

Консоль управления EcoSGE доступна по протоколу SSH через управляющий сетевой интерфейс, который находится с левой стороны передней панели устройства и обозначен надписью "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.

EcoSGE может принимать команды, отправляемые в строке SSH-подключения. Пример: **ssh admin@<IP-address> show counters all**. Для отправки нескольких команд их необходимо заключить в кавычки, а в качестве разделителя использовать точку с запятой с пробелами по обе стороны от неё. Пример: **ssh admin@<IP-address> "uptime ; who ; show interface te10"**.

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:>
```

4 Подсказки и горячие клавиши

Для упрощения работы пользователя в консоли управления EcoSGE предусмотрены подсказки и горячие клавиши, описанные в таблице ниже.

Таблица 4.1

Команда/сочетание клавиш	Действие
?	Вывод списка команд/параметров, доступных в текущем контексте, а также подсказок по их назначению
<начальные символы команды или параметра>?	Вывод списка команд/параметров, начинающихся с данных символов. Команды, выполнение которых запрещено на текущем уровне привилегий, выделяются цветом
<начальные символы команды или параметра>[TAB] <начальные символы команды или параметра>[Ctrl+i]	Автодополнение, если возможный вариант только один, или вывод списка доступных команд/параметров
стрелка вверх [↑] или [Ctrl+P]	Вызов предыдущей команды (история выполненных команд)
стрелка вниз [↓] или [Ctrl+N]	Вызов следующей команды (история выполненных команд)
..	Переход на один уровень выше
/	Переход в корень конфигурационного дерева
helpme или %	Вывод описания веток и параметров, доступных на текущем уровне дерева конфигурации
!	Вывод списка веток и параметров, доступных на текущем уровне дерева конфигурации
[Home] или [Ctrl+A]	Переместить курсор в начало строки
[End] или [Ctrl+E]	Переместить курсор в конец строки
[Ctrl]+[→]	Переместить курсор на одно слово вперёд
[Ctrl]+[←]	Переместить курсор на одно слово назад
[Ctrl+U]	Удалить все символы слева от курсора
[Ctrl+K]	Удалить все символы справа от курсора
[Ctrl+W]	Удалить слово слева от курсора
[Ctrl+C]	Переход на новую чистую строку без ввода данных, содержащихся в текущей строке
[Ctrl+J]	Перевод строки без возврата каретки
[Ctrl+M]	Аналогично нажатию [Enter]
[Ctrl+B]	Аналогично нажатию [←]
[Ctrl+F]	Аналогично нажатию [→]
[Ctrl+H]	Аналогично нажатию [Backspace]
[Ctrl+L]	Очистить консоль
[Ctrl+Q]	Завершить сеанс работы с консолью EcoSGE. Аналогично команде quit

ПРИМЕЧАНИЕ

Если при наборе команды изменить размер окна терминала, то после этого необходимо завершить набор команды без навигации по строке и нажатий клавиши Backspace и затем отправить команду нажатием клавиши Enter. В противном случае будет нарушено позиционирование курсора, и завершить набор текущей команды не удастся. Восстановить правильное позиционирование курсора можно нажатием клавиши Enter или комбинации Ctrl+C.

5 Конфигурация

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

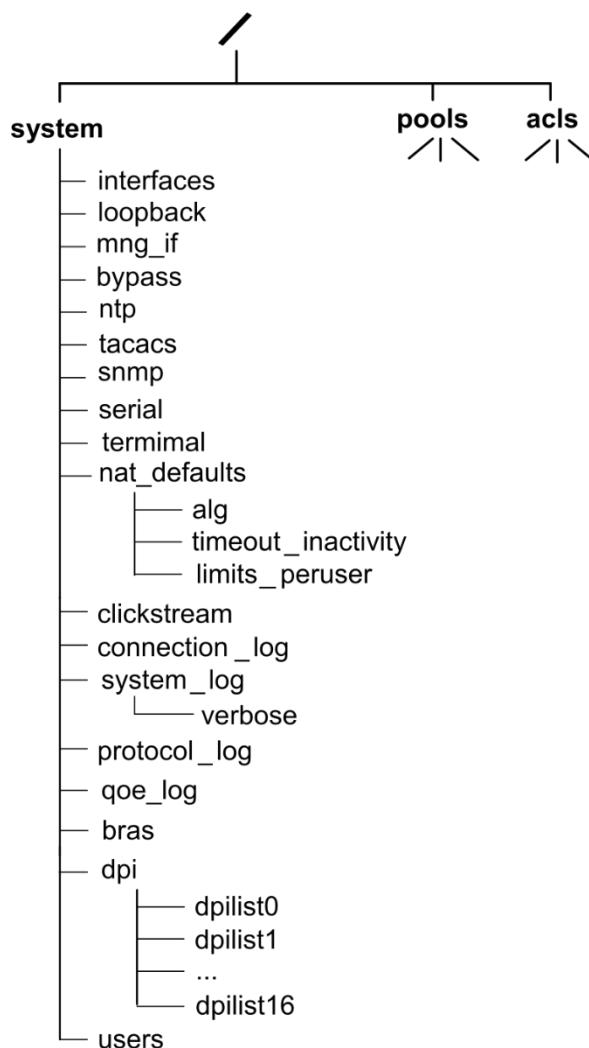


Рисунок 5

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 5.1

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

Название ветки	Описание
serial	Настройки последовательного порта
terminal	Настройки терминала
nat_defaults	Параметры NAT по умолчанию (общие параметры для всех пулов, в том числе, параметры, используемые при создании новых пулов)
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.

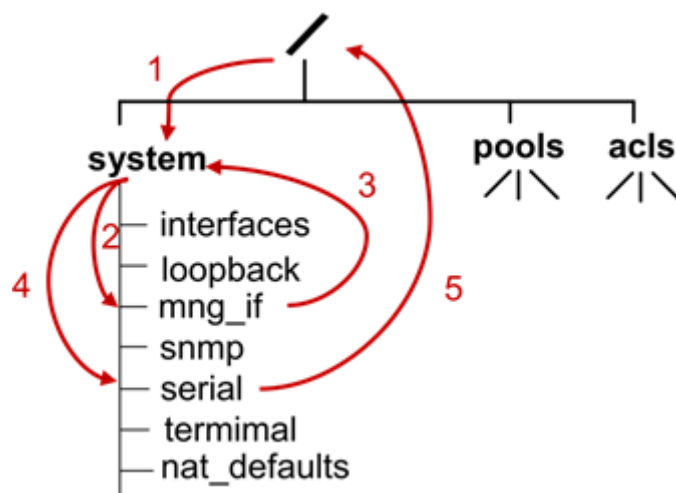


Рисунок 6

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**".

6 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).

6.1 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 сохранённых 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.

6.2 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 сохранения текущей редакции конфигурации в локальный файл используется команда **save <имя конфигурации>**.

Конфигурацию можно также сохранить на TFTP или FTP-сервер. Примеры синтаксиса команд:

save tftp://<IP-адрес>:<порт>/<имя файла>

save ftp://<IP-адрес>:<порт>/<имя файла>

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

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

Если в ветке конфигурационного дерева указано значение параметра **disable**, то данная ветка конфигурации считается отключенной. При попытке применения изменений в отключенной ветке и её дочерних ветках будет выведено сообщение «**NO NEED FOR APPLY: CONFIGURATION IS THE SAME**», указывающее на отсутствие требующих применения настроек. Исключение составляют ветки **verbose** и **shortlist**.

В ветке **verbose** задаётся уровень детализации ведения системных журналов различных подсистем (см. раздел Логирование). Данные журналы дублируются локально. Изменения настроек данной ветки применяются даже при отключенной родительской ветке **system_log**.

Ветка **shortlist** содержит параметр **server_ip_and_port**, в котором хранится адрес общего сервера логирования для всей подсистемы URL-фильтрации (см. раздел Shortlist). Изменение значения данного параметра применяется даже при отключенной ветке **shortlist** (при условии, что родительская ветка **dpi** включена).

6.3 Загрузка конфигурации

Загрузка конфигурации из локального файла выполняется командой **load <имя файла>**.

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 необходимо в конфигурационном режиме ввести команду **load effective**.

Конфигурацию можно загрузить из файла, хранящегося на TFTP, FTP или HTTP-сервере. Примеры синтаксиса команд:

load tftp://<IP-адрес>:<порт>/<имя файла>

load ftp://<IP-адрес>:<порт>/<имя файла>

load http://<IP-адрес>:<порт>/<имя файла>

6.4 Копирование конфигурации

Команда копирования конфигурации из одного файла в другой имеет следующий синтаксис:

copy <источник> <назначение>

Ниже даны примеры синтаксиса команд для всех возможных схем копирования конфигурации:

- из одного локального файла в другой локальный файл:

copy <имя файла 1> <имя файла 2>

```
MyEcoNAT:1:# dir
config1
```

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

- из локального файла в файл на TFTP-, FTP- или HTTP-сервере:

copy <имя локального файла> **tftp://**<IP-адрес>:<порт>/<имя файла>

copy <имя локального файла> **ftp://**<IP-адрес>:<порт>/<имя файла>

copy <имя локального файла> **http://**<IP-адрес>:<порт>/<имя файла>

- из файла на TFTP-, FTP- или HTTP-сервере в локальный файл:

copy **tftp://**<IP-адрес>:<порт>/<имя файла> <имя локального файла>

copy **ftp://**<IP-адрес>:<порт>/<имя файла> <имя локального файла>

copy **http://**<IP-адрес>:<порт>/<имя файла> <имя локального файла>

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

6.5 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**.*

6.6 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.

7 Первичная настройка

В настоящем разделе описаны общесистемные настройки и команды управления устройством.

7.1 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
```

Для завершения выполнения команды **ping** или **traceroute** необходимо нажать **[Ctrl+C]** или **[Backspace]**.

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.

7.2 Настройка подключения к EcoVypass

Устройство EcoNAT может быть подключено в сеть через активный оптический байпас серии EcoVypass. Взаимодействие с EcoVypass осуществляется путем отправки heartbeat-сообщений по протоколу UDP. В случае, если heartbeat-сообщения перестают приходить, EcoVypass 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 EcoVypass. В свою очередь, пары интерфейсов EcoNAT подключаются к спаренным оптическим портам EcoVypass.

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

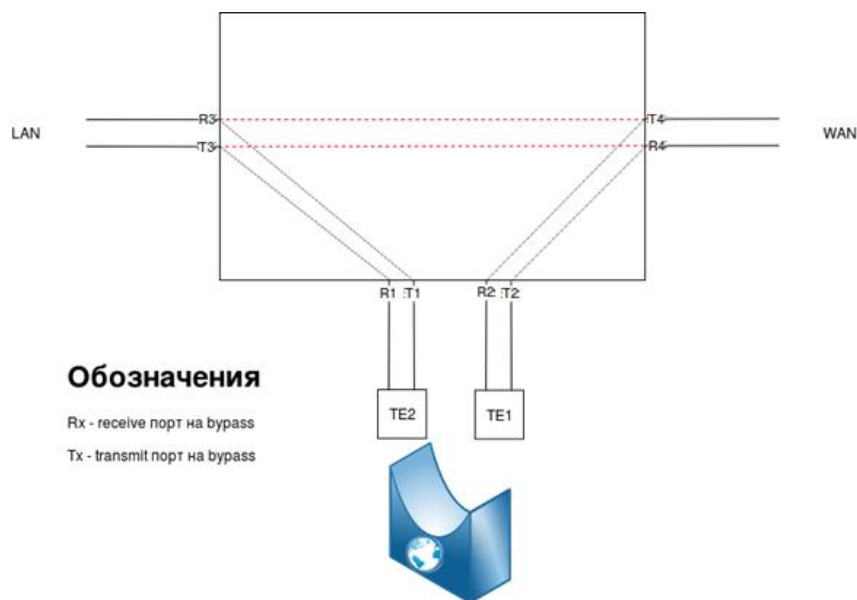


Рисунок 7

Heartbeat-сообщения имеют вид **<BP01_XX_BP>**, где **XX** - номер сетевой платы EcoVypass, к которой подключено устройство EcoNAT. В ответ EcoVypass 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. Помимо полного отсутствия heartbeat-сообщений EcoBypass может отслеживать падение уровня Tx-сигнала от устройства. При критическом падении уровня сигнала EcoBypass переключится в прозрачный режим.

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

Настраиваемые в данной ветке параметры представлены в таблице ниже.

Таблица 7.1

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
bypass_tos	Значение поля Type of Service (ToS) для отправляемых сообщений. Допустимые значения - от 0 до 255. По умолчанию 0
bypass_interval	Периодичность отправки heartbeat-сообщений на EcoBypass. Задаётся в миллисекундах. Допустимые значения - от 1 до 2000. По умолчанию 10 мс
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
bypass_tos 0
bypass_interval 10
te1_te2 disabled
te3_te4 disabled
te5_te6 1
te7_te8 2
te9_te10 3
te11_te12 4
te13_te14 disabled
te15_te16 disabled
EcoNAT:3:system.bypass>
```

7.3 Настройка терминала

Настройка терминала производится в ветке **system.terminal**. В таблице ниже дано описание доступных параметров.

Таблица 7.2

Параметр	Описание
autologoff_timeout	Максимальное время простоя (отсутствие действий пользователя и/или обновления информации в CLI), по истечении которого сеанс CLI будет автоматически завершён. Допустимые значения:

Параметр	Описание
	2_minutes, 5_minutes (по умолчанию), 10_minutes, 15_minutes, never (автозавершение сеанса выключено).
max_consoles	Максимально допустимое количество одновременных сеансов CLI для данного устройства. По умолчанию 20
prompt	Текст, выводимый в начале каждого приглашения CLI на ввод команды. Допустимые символы: прописные и строчные латинские буквы, цифры, точка, дефис. Приглашение не может начинаться с точки или дефиса и содержать следующие подряд точки; может быть пустым
print_line_num	Включение/выключение нумерации строк (on off). По умолчанию нумерация включена

Для применения внесённых изменений и добавления их в стартовую конфигурацию необходимо отправить команды **apply** и **write** соответственно. Изменения всех параметров, кроме **max_consoles**, вступают в силу сразу после выполнения команды **apply**. Новое значение параметра **max_consoles** вступит в силу только после перезагрузки устройства командой **reboot**.

ВНИМАНИЕ! Изменение значения параметра **autologoff_timeout** вступает в силу сразу после выполнения команды **apply**. Если для одного устройства открыты несколько сеансов CLI, и время их простоя больше нового значения **autologoff_timeout**, то эти сеансы будут автоматически завершены.

7.4 Настройка loopback

Настройки, хранящиеся в ветке конфигурационного дерева **loopback**, используются EcoNAT для отправки ICMP-сообщений абонентам. 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#
```

7.5 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 12-Jul-2019T13:20:52 (UTC)
Current time is 12-Jul-2019T13:50:52 (Local)
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
```

7.6 Логирование

7.6.1 Настройка логирования абонентских соединений

Информация о выделении IP-адреса и/или порта или блока портов должна сохраняться в соответствии с требованиями законодательства Российской Федерации. В качестве стандартного механизма система EcoSGE 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 и при попытке выполнить на этот адрес команду ping, ICMP запросы, попавшие на логирующий интерфейс EcoSGE, останутся без ответа (кроме случаев логирования через **mng**-интерфейс). Пакеты с логами отправляются по алгоритму Round-Robin по всем подключенным сетевым интерфейсам логирования. Номера сетевых интерфейсов для логирования указаны в разделе "Оборудование".

Базовые параметры **connection_log** описаны в таблице ниже.

Таблица 7.3

Параметр	Описание
enable или disable	Включение и выключение логирования соединений
log_servers	Адреса и порты syslog серверов, на которые будут передаваться log-сообщения (логирование будет идти параллельно на все доступные сервера из списка, то есть каждый из серверов будет получать информацию обо всех соединениях). На данный момент максимальное количество серверов ограничено двумя
log_interface	Интерфейс, через который будет производиться логирование. Возможные значения: default – через интерфейс LOG (используется по умолчанию); mng – через интерфейс MNG
ip_address	IP-адрес и маска подсети (через '/') источника виртуального канала, в который объединены логирующие сетевые интерфейсы
mac	MAC-адрес источника 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	MAC-адрес syslog-сервера в параметре log_servers , являющегося ближайшим L3 соседом. <u>Параметр необязательный.</u>

Параметр	Описание
	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). 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
pack_msgs	Разрешает упаковывать несколько информационных сообщений о логируемых событиях в одно сообщение. Это уменьшает размер логов и нагрузку на сеть

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).

EcoSGE поддерживает различные протоколы логирования. Ниже описаны параметры, необходимые для настройки логирования по протоколу syslog.

Таблица 7.4

Параметр	Описание
log_format	Параметр показывает тип логирования: syslog – логирование по протоколу syslog; netflow – логирование по протоколу NetFlow v9
log_on_release	Включение (on) / выключение (off) отправки сообщений при освобождении трансляции или блока портов. При создании трансляции сообщение отправляется в любом случае. Если включён параметр log_individual_conn , то сообщение формируется при освобождении каждой трансляции, в противном случае – только при освобождении блока портов
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 на сеть
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.

Параметр	Описание
	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 7.5

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:

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



```
MyEcoSGE:8:system.connection_log# enable
```

Формат syslog-сообщения: <Дата и время syslog-сервера> <IP-адрес EcoSGE> <Дата и время EcoSGE> <Системное имя EcoSGE> | <IP-адрес назначения (Dst)>:<Порт> <A | F> <IP-адрес, на который осуществляется трансляция>:<Порт> <E | I> <IP-адрес источника (Src)>:<Порт> <Идентификатор протокола>, где A – открытие сессии (Allocate), F – закрытие сессии (Free), E – исходящая сессия (Egress), I – входящая сессия (Ingress).

Примеры сообщений об открытии и закрытии сессии:

```
2020-09-04T15:57:53.411971+00:00 10.210.1.234 2020-09-04T18:57:52+03:00
ecosge | 192.168.008.008:01024 A 060.000.000.226:01024 E
010.000.003.254:01024 UDP
2020-09-04T16:00:13.883270+00:00 10.210.1.234 2020-09-04T19:00:12+03:00
ecosge | 192.168.008.008:01024 F 060.000.000.226:01024 E
010.000.003.254:01024 UDP
```

Предусмотрена возможность передачи в сообщении о закрытии сессии времени её открытия. Данная возможность добавляется по отдельному запросу. За дополнительной информацией следует обратиться в службу технической поддержки.

После добавления данной возможности в настройках логирования при **log_on_release on** появляется дополнительный параметр **stamp_on_free** (возможные значения – **on** | **off**). Данный параметр определяет, будет ли в сообщении о закрытии сессии передаваться время её открытия. При **stamp_on_free on** сообщение о закрытии сессии будет иметь следующий вид:

```
2020-09-04T16:00:13.883270+00:00 10.210.1.234 2020-09-04T19:00:12+03:00
ecosge | 192.168.008.008:01024 F 060.000.000.226:01024 E
010.000.003.254:01024 UDP 2020-09-04T18:57:52+03:00
```

Как видно из примера выше, в конец сообщения добавлено время открытия сессии.

IP-адреса записываются в трехзначном формате. Например, адрес 10.1.1.200 будет представлен как 010.001.001.200. Ниже приведены примеры 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 7.6

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 7.7

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

7.6.2 Настройка системного логирования

EcoSGE 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 EcoSGE будет отправлять системные логи, указывается в параметре **log_servers**.

Имя устройства EcoSGE, передаваемое в логах, задаётся в параметре **hostname**. Данное имя передаётся не только при логировании системных событий, но и при логировании абонентских соединений и подключений к web-серверам. Изменение параметра **hostname** вступает в силу сразу после команды **apply** и не требует перезагрузки устройства. Однако следует учесть, что в течение короткого периода реконфигурации после команды **apply** (не более 10 секунд) возможна отправка логов с неправильным значением в поле **hostname**. В частности, это касается логирования абонентских соединений.

```
EcoSGE:system.system_log# verbose defrag 1
EcoSGE: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**.

```
EcoSGE:# 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.

```
EcoSGE:system.system_log.verbose# setlog all fatal
EcoSGE: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
EcoSGE: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**.

```
EcoSGE:> 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 (allocated/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:

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

7.6.3 Логирование протоколов

EcoSGE ведёт запись всех проходящих протоколов. Логи распознанных протоколов в бинарном виде передаются на сервер. Настройки логирования протоколов находятся в ветке **system.protocol_log**. Для того чтобы включить логирование, в данной ветке должен быть установлен параметр **enable**. Для работы данного типа логирования необходима лицензия на функционал URL-фильтрации (см. раздел "Настройка URL-фильтрации").

```
MyEcoNAT:19:system.protocol_log# show
disable
log_interface default
server_ip_and_port 0.0.0.0:0
```

```
ip_address 0.0.0.0/0.0.0.0
gateway 0.0.0.0
source_port 1089
```

Параметры логирования протоколов приведены в таблице ниже.

Таблица 7.8

Параметр	Описание
enable disable	Включение/отключение логирования протоколов
log_interface	Интерфейс, через который будет производиться логирование. Возможные значения: default – через интерфейс LOG (используется по умолчанию); mng – через интерфейс MNG
server_ip_and_port	IP-адрес и порт syslog-сервера
ip_address	IP-адрес и маска подсети (через ‘/’) источника виртуального канала, в который объединены логирующие сетевые интерфейсы
gateway	Шлюз по умолчанию для виртуального канала, в который объединены логирующие сетевые интерфейсы. Требуется в том случае, если syslog-сервер, указанный в параметре server_ip_and_port , не находится в подсети, указанной в параметре ip_address
source_port	Порт для отправки сообщений на syslog-сервер Данный параметр необходимо задать в том случае, если для логирования выбран интерфейс LOG (log_interface default). Если для логирования выбран интерфейс MNG (log_interface mng), то используется случайный порт, и параметр source_port не учитывается

7.6.4 QoE

Quality of Experience (QoE, оценка пользователем качества услуги) – интегральный параметр, представляющий собой общую приемлемость качества услуги, субъективно воспринимаемую конечным пользователем. В контексте EcoSGE под QoE понимается сводная информация о соединениях абонентов. Данная сводка содержит показатели, характеризующие качество этих соединений. Эти показатели помогают выявлять проблемы с соединениями у отдельных абонентов, что может использоваться оператором как инструмент повышения качества предоставляемых услуг и удержания абонентов.

Подсистема QoE подразделяется на следующие модули, которые могут быть включены как вместе, так и по отдельности, в зависимости от лицензии:

- базовый функционал с бинарными логами;
- функционал аккаунтинга сессии (логирование количества переданных байт/пакетов);
- функционал ОТТ, позволяющий анализировать параметры предоставления видеосервисов: подсчёт байтов подсессии ОТТ, время последнего PSH пакета в подсессии от сервера, дельта времени между GET пакетом от клиента и PSH пакетом от сервера в подсессии.

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

Параметры настройки QoE описаны в таблице ниже.

Таблица 7.9

Параметр	Описание
enable disable	Включение/отключение логирования QoE
log_interface	Интерфейс, через который будет производиться логирование. Возможные значения: default – через интерфейс LOG (используется по умолчанию); mng – через интерфейс MNG
syn_log	Возможные значения: on, off Если значение on , то проходящий пакет SYN вместе с Ethernet заголовком будет упакован в log-пакет с фиксированным размером поля DATA = 256 байт, после чего данный log-пакет будет отправлен на log-коллектор
server_ip_and_port	<IP-адрес>:<Порт> log-коллектора
ip_address	IP-адрес и маска подсети (через '/') источника виртуального канала, в который объединены логирующие сетевые интерфейсы
gateway	Шлюз по умолчанию для виртуального канала, в который объединены логирующие сетевые интерфейсы. Требуется в том случае, если syslog-сервер, указанный в параметре server_ip_and_port , не находится в подсети, указанной в параметре ip_address
source_port	Порт для отправки сообщений на syslog-сервер
mtu	Величина MTU для пакета syslog

Пример настройки:

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

Логи QoE передаются в бинарном виде с использованием проприетарного протокола. При использовании оборудования совместно с EcoQoE (Log Collector) расшифровка логов на коллекторе происходит автоматически.

7.6.5 Логирование подключений к web-серверам

В системе EcoSGE предусмотрена возможность логирования на внешний сервер проходящих HTTP GET-запросов, ответов web-серверов (HTTP) и запросов на установление SSL/TLS соединений. Эта возможность доступна при наличии лицензии Clickstream.

Настройка данного типа логирования производится в ветке **system.clickstream**. Параметры настройки описаны в таблице ниже.

Таблица 7.10

Параметр	Описание
enable или disable	Включение/отключение логирования подключений к web-серверам
server_ip_and_port	IP-адрес и порт syslog-сервера
ip_address	IP-адрес и маска подсети (через '/') источника виртуального канала, в который объединены логирующие сетевые интерфейсы
gateway	Шлюз по умолчанию для виртуального канала, в который объединены логирующие сетевые интерфейсы. Требуется в том случае, если syslog-сервер,

Параметр	Описание
	указанный в параметре server_ip_and_port , не находится в подсети, указанной в параметре ip_address
source_port	Порт для отправки сообщений на syslog-сервер
mtu	Величина MTU для пакета syslog

Пример настройки:

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

Ниже даны примеры записей на syslog-сервере. Запись 1 - для HTTP GET-запроса абонента, запись 2 - для ответа web-сервера, запись 3 - для запроса на установление SSL/TLS соединения.

```
2019-07-11T10:35:58.202901+00:00 192.168.1.1 192.168.000.002:34904
192.168.000.003:00080 1522071357 econat GET / HTTP/1.1#015#012Host:
google.ru#015#012User-Agent: curl/7.55.0#015#012Accept: */*#015#012#015
2019-07-12T09:33:02.370234+00:00 192.168.1.1 065.208.228.223:00080
145.254.160.237:03372 1562934780 econat HTTP/1.1 200 OK
2019-07-15T14:50:01.810583+00:00 192.168.1.1 192.168.000.002:41016
192.168.000.003:00080 1532627400 econat SSL: 3.3 hostname: vk.com
```

В таблице ниже дано описание полей записи для HTTP GET-запроса на примере записи 1 (см. выше).

Таблица 7.11

№	Поле	Пример
1	Временная метка syslog-сервера (не посылается устройством EcoNAT)	2018-03-26T10:35:58.202901+00:00
2	IP-адрес устройства EcoNAT (параметр ip_address)	192.168.1.1
3	IP-адрес и порт отправителя	192.168.000.002:34904
4	IP-адрес и порт получателя	192.168.000.003:00080
5	Временная метка устройства EcoNAT (POSIX time)	1522071357
6	Имя устройства EcoNAT, заданное в параметре hostname ветви system_log	econat
7	Содержимое HTTP GET-запроса	GET / HTTP/1.1#015#012Host: google.ru#015#012User-Agent: curl/7.55.0#015#012Accept: */*#015#012#015

Описание полей 1-6 в записи для ответа web-сервера (см. запись 2 выше) аналогично описанию для HTTP GET-запроса. Поле 7 содержит версию HTTP и код ответа.

В таблице ниже дано описание полей 7, 8 в записи для запроса на установление SSL/TLS соединения на примере записи 3 (см. выше). Описание полей 1-6 аналогично описанию для HTTP GET-запроса.

Таблица 7.12

№	Поле	Пример
7	Версия SSL	SSL: 3.3
8	Доменное имя	hostname: vk.com

Статистика по пакетам, относящимся к логированию подключений к web-серверам, выводится командой **show counters all | include clickstream**. В таблице ниже дано описание счётчиков.

Таблица 7.13

Счетчик	Описание
cr_clickstream_url_for_log	Подготовлено пакетов syslog
cr_clickstream_send_one_packet	Отправлено пакетов syslog
cr_clickstream_send_fragmented_packet	Отправлено фрагментированных пакетов syslog
cr_clickstream_error_general	Количество ошибок при клонировании TCP-пакета
cr_clickstream_error_create_header	Количество ошибок при формировании пакета syslog
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
cr_clickstream_no_ssl_tmp_buffer	Выделение буфера для фрагментированного ClientHello
cr_clickstream_ssl_without_hostname	Количество полученных SSL или TLS handshake, в которых нет доменного имени

Пример:

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

7.7 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.IaryKF7jSpS1ZKnmXydvG3AURTTQvJY152R2s/
user myuser level 15 secret 5
5$00$P2c.IaryKF7jSpS1ZKnmXydvG3AURTTQvJY152jgfhgfhg
user user1 level 5 secret 5
5$00$P2c.IaryKF7jSpS1ZKnmXydvG3AURTTQvJY152mXydvS12
}
```

Эта же команда используется для изменения конфигурации пользователя, в том числе и пароля.

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.IaryKF7jSpS1ZKnmXydvG3AURTTQvJY152R2s/
}
```

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 SHPASS. В данном режиме работы консоли можно изменить пароли пользователей и сохранить настройки.

7.8 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.

7.9 Помощь пользователям

При обращении в службу технической поддержки необходимо сообщать версию прошивки оборудования (выводится командой **show version**) и информацию о лицензии (выводится командой **show license**). Пример выводимой информации:

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

Для вывода подробной информации о версии используется команда **show version detail**.

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

7.10 Сервисные команды

Предусмотрен ряд команд, которые позволяют провести общую диагностику системы: получить информацию об использовании системной памяти, загрузке процессора и буферов подсистем, проверить температуру процессора и состояние блоков питания и вентиляторов. Также предусмотрена возможность сбора и выгрузки подробной диагностической информации на внешний сервер.

7.10.1 Информация о системной памяти

Информация об использовании системной памяти устройства выводится командой **show memstat**.

```
EcoSGE:# show memstat
Data plane free/total memory: 21515 MiB / 30064 MiB
Control plane free/total memory: 2559 MiB / 3475 MiB
```

При отправке данной команды с ключевым словом **detail** объём памяти будет указан в байтах.

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

7.10.2 Информация о ресурсах системы

Информация об использовании ресурсов системы выводится командой **show resources**.

```
EcoSGE:# show resources
CPU load: 97% (te7, te8, te9, te10, te11, te12)
Avg egress burst: 10.8 (4.2%)
Avg ingress burst: 11.6 (4.5%)
Session table used/total: 0/33554432 (0.0%)
Translation table used/total: 0/41943040 (0.0%)
Abons table used/total: 0/131072 (0.0%)
Mbufs number on socket 0 used/total: 15372/2097151 (0.7%)
Block allocation log size: 0 (0.0%)
Bras table used/total: 0/524288 (0.0%)
DPI host buffers used/total: 0/65535 (0.0%)
DPI path buffers used/total: 0/65535 (0.0%)
DPI state buffers used/total: 0/4194303
Awaiting syslog messages: 0 (0.0%)
```

Описание выводимых данных представлено в таблице ниже.

Таблица 7.14

Параметр	Описание
CPU load	Загрузка процессора и перечисление интерфейсов в порядке убывания их нагрузки на процессор
Avg egress burst	Среднее значение всплесков egress направления
Avg ingress burst	Среднее значение всплесков ingress направления
Session table used/total	Счётчик заполнения таблицы сессий (текущее/максимальное)
Translation table used/total	Счётчик заполнения таблицы трансляций (текущее/максимальное)
Abons table used/total	Счётчик заполнения таблицы уникальных пользователей (текущее/максимальное)
Mbufs number on socket 0 used/total	Количество используемых data plane буферов процессора / общее количество
Block allocation log size	Счётчик заполнения буфера сообщений connection_log (процент используемых)
Bras table used/total	Счётчик заполнения таблицы пользователей, зарегистрированных на BRAS (текущее/максимальное)
DPI host buffers used/total	Счётчик заполнения буфера информации по доменному имени (текущее/максимальное)

Параметр	Описание
DPI path buffers used/total	Счётчик заполнения буфера информации по URL, идущей после знака "?" (текущее/максимальное)
DPI state buffers used/total	Счётчик заполнения буфера информации по сессии (текущее/максимальное)
Awaiting syslog messages	Счётчик заполнения буфера сообщений syslog

7.10.3 Проверка температуры процессора и состояния блоков питания и вентиляторов

Информация о температуре процессорных ядер выводится командой **show temperature**.

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

Информация о частоте вращения вентиляторов выводится командой **show fan**. У моделей EcoSGE 2020/2040 и 4080/4120/4160 выводимая информация немного отличается. Пример для моделей 2020/2040:

```
EcoSGE:> show fan
CPU fan : 12500
System fan: 12616
System fan(AUX0) : 12500
System fan(AUX1) : 12616
System fan(AUX2) : 6521
```

Пример для моделей 4080/4120/4160:

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

В выводе команды:

- NIC<N> – вентиляторы на сетевых картах. При нормальной работе частота вращения вентилятора должна быть в диапазоне 6000-6400 RPM;

- System fan <N> – вентиляторы в корпусе устройства. Частота вращения вентилятора зависит от температуры в корпусе устройства. При минимальной нагрузке частота вращения вентилятора должна быть в диапазоне 2600-4800 RPM, а при максимальной нагрузке – в диапазоне 16700-22300 RPM.

7.10.4 Сбор и выгрузка диагностической информации

Если по каким-либо причинам сотруднику технической поддержки компании RDP не может быть предоставлен удалённый доступ к устройству для его диагностики, то можно сгенерировать зашифрованный архив с подробной диагностической информацией и выгрузить его на HTTP, FTP или TFTP-сервер. Для этого предусмотрена команда **tech_support [backtrace] <URL>**.

Замечания по использованию команды:

- команда с ключевым словом **backtrace** может быть выполнена только в конфигурационном режиме CLI с уровнем привилегий 15. При выполнении команды с данным ключевым словом в архив будет добавлено несколько дополнительных файлов с отладочной информацией, которая позволит разработчикам определить, в каком именно месте кода возникает ошибка;
- если URL содержит дефис, то такой URL необходимо заключить в двойные кавычки;
- если используется нестандартный порт протокола передачи, то его номер необходимо явно указать в URL. Стандартные номера портов: HTTP – 80, FTP – 21, TFTP – 69.

В ходе выполнения команды в консоли отображается информация о производимых действиях. Пример:

```
EcoSGE:> tech_support ftp://192.168.5.1:2121/shared
[#####] 100.0% (Copying logs 3/3)
[#####] 100.0% (Preparing / (Compressing))
[#####] 100.0% (File transfer)
Debug info uploaded.
```

Если команда выполнена успешно, то на хосте в указанной директории должен появиться зашифрованный архив **tech_support.enc** объёмом приблизительно 23 МБ. Этот архив необходимо предоставить запросившему его сотруднику технической поддержки компании RDP.

7.10.5 Ошибки 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 7.15

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 7.16

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 удастся 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)

Обозначение	Причина
0x[PP]33	acl INGRESS трансляции не соответствует пулу PP (номер пула где произошла ошибка)
0x34	Трансляция не соответствует настройкам
0x35	Адрес не соответствует глобальным настройкам BNAT пула
0x36	Превышено количество соединений BNAT пула
0x37	Запрещены INGRESS соединения

Для сброса счётчика ошибок необходимо выполнить команду **clear cgnat errors**

7.10.6 Счетчики

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 gel counters
Interface name: gel
rx_good_packets: 0
tx_good_packets: 0
rx_good_bytes: 0
tx_good_bytes: 0
```

...

Для просмотра информации о трафике, проходящем через определённый интерфейс или все интерфейсы, используется команда **show interface {all | <INT_NAME>} traffic [monitor]**, где **all** - все интерфейсы, **INT_NAME** - имя интересующего интерфейса, **monitor** - просмотр в режиме реального времени. В режиме **monitor** выводится информация о трафике за последнюю секунду. Для выхода из режима **monitor** необходимо нажать на клавиатуре **[Ctrl+C]** или **[Esc]**, или **[Q]**. В строке Subtotal указана общая статистика трафика для всех линейных интерфейсов, т. е. не являющихся интерфейсами управления или логирования.

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

Для удобства просмотра используются десятичные приставки "К, М, Г, Т" [в системе СИ](#).

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
```

7.11 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.

7.11.1 Обновление 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**.

7.11.2 Изменение 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*    .         .
```

7.12 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 7.17

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 зашифрованным 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
```

7.13 Настройка SNMP

Система EcoSGE поддерживает протоколы SNMP v1 и v2c. Реализована возможность считывания значений переменных MIB (GET-запросы) и отправки Trap-сообщений. SET-запросы не поддерживаются.

Trap-сообщения всегда передаются в формате SNMPv1 на UDP-порт 162 с использованием community "public". В данных сообщениях передаётся информация обо всех системных событиях уровня FATAL.

Параметры SNMP находятся в ветке конфигурации **system.snmp**. В таблице ниже дано описание всех доступных параметров.

Таблица 7.18

Параметр	Описание
enable disable	Включение / выключение протокола SNMP
trap { true false } или trap { on off }	Включение (true) или выключение (false) отправки Trap-сообщений
trap_host	IP-адрес или доменное имя сервера, которому должны передаваться Trap-сообщения
port	Номер UDP-порта, через который EcoSGE будет принимать GET-запросы. По умолчанию 161
allowed_ip ()	IP-адреса, с которых система EcoSGE будет принимать GET-запросы. Допустимые значения: отдельный адрес, диапазон адресов через дефис (например, 10.10.0.10-10.10.0.20), адрес сети/подсети. Можно задать любую комбинацию значений через пробел (например, allowed_ip (192.168.10.11 10.10.0.10-10.10.0.20 10.100.0.0/24)), а также добавлять и удалять отдельные значения с помощью операторов += и -= соответственно.
read_community	Community String для операций чтения (GET-запросов)
description	Текстовая строка, которая описывает систему EcoSGE (объект sysDescr группы System в MIB-II, Настройка URL-фильтрации)
hostname	Текстовая строка, которая содержит имя системы EcoSGE (объект sysName группы System в MIB-II, RFC1213)

Параметр	Описание
contact	Текстовая строка, которая содержит контактную информацию администратора системы EcoSGE (объект sysContact группы System в MIB-II, Настройка URL-фильтрации)
hostlocation	Текстовая строка, которая описывает местонахождение системы EcoSGE (объект sysLocation группы System в MIB-II, RFC1213)

Пример настройки:

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

7.14 Параметры LLDP

Устройство EcoNAT поддерживает протокол LLDP (Link Layer Discovery Protocol) и с периодичностью 30 секунд рассылает через все задействованные интерфейсы LLDP-сообщения с информацией о себе и своих характеристиках.

При необходимости можно выключить рассылку LLDP-сообщений. Для этого необходимо в ветке **system.nat_defaults** присвоить параметру **lldp** значение **off**. В этой же ветке можно изменить значение параметра **lldp_hostname**, которое будет передаваться в LLDP-сообщении в поле System Name (TLV Type 5).

Кроме того, можно получить информацию о соседних узлах, использующих LLDP. Для этого необходимо выполнить команду **show neighbours <имя интерфейса>** для определённого интерфейса или **show neighbours all** для всех интерфейсов.

```
EcoNAT:# 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
```


8 Конфигурирование NAT

В настоящем разделе описаны настройки функционала CG-NAT.

8.1 Интерфейсы

В логике EcoSGE 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 1GbE начинаются с префикса **ge**, например, **ge3**.

Названия в системе соответствуют названиям сетевых интерфейсов, представленным в разделе "Настройка URL-фильтрации".

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

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

В EcoSGE можно включать или отключать интерфейсы, не переходя в ветку настроек интерфейса для внесения соответствующих изменений (**enable** | **disable**). Для включения и отключения интерфейсов предусмотрены команды **interface <INT_NAME> up** и **interface <INT_NAME> down**, где **INT_NAME** – имя интерфейса. После данных команд необходимо отправить команду **apply**, чтобы изменения вступили в силу.

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 dropped 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
```

8.1.1 Интерфейс "on a stick"

В EcoNAT реализована поддержка режима интерфейсов "on a stick" (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 "on a stick" 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 8.1

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 интерфейса "on a stick"
vlan_global	Глобальный тег для интерфейса "on a stick"
description	Описание интерфейса. От 1 до 240 символов

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

ВНИМАНИЕ, любые изменения в настройках режима "on a stick" будут применены только после перезагрузки устройства. Даже изменения номеров **vlan_local** и **vlan_global** на интерфейсах не будут применены после выполнения команды **apply** до тех пор, пока устройство не будет перезагружено.

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.

8.1.2 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 dropped 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 all transceiver** (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 all transceiver
Interface name: te1
Module Vendor Name: OEM
Module Part Number: SFP+-10G-LR
Module Serial Number: P1309040348
Module Revision: A
Module Manufacturing 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 Manufacturing 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 *te18* transceiver**.

Для просмотра информации о MNG-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 tel8
Interface tel8 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
```

8.2 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").

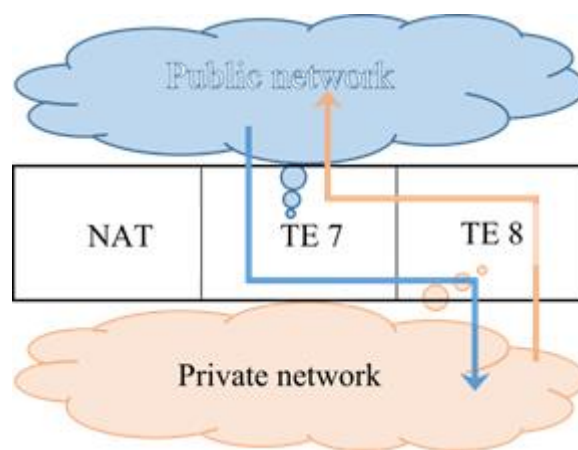


Рисунок 8

8.3 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**.

8.3.1 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 8.2

Параметр	Описание
<code>vlan_mode</code>	Обработка и анализ пакетов до указанного уровня инкапсуляции. Возможные значения: <code>untagged</code> , <code>vlan</code> , <code>qinq</code> .
<code>alg ftp</code>	Включает опцию ALG для протокола FTP. Возможные значения: <code>on</code> , <code>off</code>
<code>alg pptp</code>	Включает опцию ALG для протокола PPTP. Возможные значения: <code>on</code> , <code>off</code>
<code>alg rtsp</code>	Включает опцию ALG для протокола RTSP. Возможные значения: <code>on</code> , <code>off</code>
<code>alg sip</code>	Включает опцию ALG для протокола SIP. Возможные значения: <code>on</code> , <code>off</code>
<code>alg alg_on_bnat</code>	Включает опцию ALG для статического NAT. Возможные значения: <code>on</code> , <code>off</code>
<code>sessions_per_translation</code>	Количество активных сессий на трансляцию
<code>udp_inbound_refresh</code>	Включает обновление UDP-трансляций входящими (ingress) пакетами. Возможные значения: <code>on</code> , <code>off</code>
<code>l2mtu</code>	Величина MTU на входе. Значение задаётся для L2 с учётом заголовка (по умолчанию 1522, макс. значение 9692)
<code>port_block_size</code>	Размер блока портов. Значение по умолчанию – 128. Не рекомендуется изменять значение данного параметра
<code>portlimit_low</code>	Значение используемого диапазона "нижних" портов (до 1024) для каждого пользователя. Варианты значений параметра: <code>nolimit</code> , 64, 128, 256, 512
<code>low_to_all_udp</code>	Позволяет использовать порты из верхнего диапазона, если порты из нижнего диапазона исчерпаны. Варианты значений параметра: <code>on/off</code>
<code>lldp</code>	Включение (<code>on</code>) / выключение (<code>off</code>) протокола LLDP. По умолчанию on
<code>lldp_hostname</code>	Имя хоста, которое будет использоваться в LLDP-сообщениях
<code>permit_invalid_flow</code>	Включить (<code>on</code>) / отключить (<code>off</code>) функцию заведения сессий по TCP-сегментам, у которых не выставлен флаг SYN. Значение по умолчанию: off . TCP-сессия всегда начинается с сегмента с выставленным SYN-флагом, и такие пакеты могут быть ошибочными или вредоносными, поэтому по умолчанию новые сессии по таким сегментам не заводятся, а сами сегменты отбрасываются. Однако в некоторых случаях данное поведение может быть полезным. Например, когда часть трафика идёт по другому маршруту или для корректной работы TCP-соединений, по которым длительное время не передаются данные. Этот параметр является глобальным: он влияет на поведение всего устройства и не может быть переопределён в пулах. Для применения изменений требуется выполнить команду apply
<code>timeouts_inactivity {}</code>	В этом разделе задаются параметры времени неактивности (в секундах) для разных протоколов и состояний TCP, по истечении которого неиспользуемое соединение будет закрыто принудительно.
<code>timeouts_inactivity translation</code>	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 udp	Таймаут неактивности в секундах для UDP соединений. По истечении этого таймаута порт на глобальном IP высвобождается. По умолчанию 300
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 (в секундах) для трансляции, созданной TCP-пакетом с флагом SYN (запрос на установление TCP-соединения). 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 протоколу IP (например, для GRE). По истечении заданного времени 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-адресу). 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 создать отдельный CGNAT-пул с меньшим коэффициентом уплотнения (меньше локальных IP-адресов на один глобальный), либо использовать NAT-пул для выделения пользователю целого IP-адреса со всеми портами на период его активности

Параметр **vlan_mode** может принимать значения **untagged**, **vlan**, **qinq**. При значении **untagged** устройство EcoSGE будет обрабатывать только нетегированный трафик, при **vlan** – нетегированный и с одной меткой, при **qinq** – нетегированный, с одной и с двумя метками.

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

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

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 sessions all**.

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

8.3.2 Создание пула

Для создания пула используется команда **create pool <имя пула>**. При этом создаётся CGNAT-пул с типовыми параметрами (см. описание в разделе "Пулы и ACL") 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 находиться 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 создания пула можно приступить к заданию его параметров. Для этого необходимо перейти в ветку конфигурации с именем данного пула (приёмы навигации по дереву конфигурации описаны 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, к созданному пулу не привязан ACL (у параметра **acl** значение **none**). Привязка ACL выполняется вручную.

Параметры пула описаны в таблице ниже.

Таблица 8.3

Параметр	Описание
type	Тип пула: cgnat, static, nat, fake
enable disable	Состояние пула
acl	Связанный с пулом ACL
priority	Приоритет пула
global_ip ()	Глобальные IP-адреса, относящиеся к пулу. Во избежание ARP-запросов от маршрутизатора к WAN-интерфейсу EcoNAT не рекомендуется назначать global_ip из подсети интерфейсов маршрутизаторов, между которыми включен EcoNAT
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>[~vid]-<глобальный адрес>. Параметр действителен для пулов типа Static. VID – идентификатор VLAN от 0 до 4094 (необязательный параметр). Значение VID задаётся с префиксом "~" (тильда) без пробела после адреса
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

Параметр	Описание
	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
timeouts_inactivity tcp_handshake	Таймаут (в секундах) для трансляции, созданной TCP-пакетом с флагом SYN (запрос на установление TCP-соединения). 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-адресу). 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. Значения более 32256 могут привести к тому, что один пользователь сможет исчерпать порты IP-адреса. Для пользователей, особенно требовательных к числу портов, имеет смысл создать отдельный CGNAT-пул с меньшим коэффициентом уплотнения (меньше локальных IP-адресов на один глобальный) или использовать NAT-пул для выделения пользователю отдельного IP-адреса 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 8.4

Параметры	cgnat	nat	static	fake
type	+	+	+	+

Параметры	cgnat	nat	static	fake
enable	+	+	+	+
acl	+	+	+	+
priority	+	+	+	+
global_ip ()	+	+		
port_range	+			
global_map ()			+	
hairpin	+	+	+	+
allow_external_connect		+	+	
connection_logging	+	+	+	+
randomize_ports	+	+	+	+
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 **+=**. При внесении изменений в параметр **global _ ip**, CLI не выйдет из режима редактирования параметра до тех пор, пока не будет введена закрывающая скобка.

```
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 **analyze** *<имя пула>* . Вывод команды покажет, чего не хватает для нормальной работы пула.

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

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

```
MyEcoNAT:1:# analyze 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 **analyze** 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:pooltest# enable
```

8.3.3 Создание ACL

После создания пула необходимо 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**. Для перехода в созданный список необходимо выполнить команду **edit <имя ACL>** или **goto <имя ACL>**, после чего можно приступить к формированию списка правил.

Общий синтаксис команды для задания правила ACL:

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

В квадратных скобках указаны необязательные параметры. Следует указывать только значения параметров (без имени). Описание всех параметров команды дано в таблице ниже.

Таблица 8.5

№	Имя параметра	Описание
1	num	Порядковый номер правила, который определяет его приоритет. Чем меньше значение, тем выше приоритет. ACL не может содержать правила с одинаковыми номерами. При добавлении правила с номером, который уже присутствует в списке, новое правило заменит существующее с данным номером. Если номер не указан, то при добавлении правила в ACL номер присваивается автоматически. ПРИМЕЧАНИЕ Правила применяются в порядке убывания приоритета (возрастания номера), поэтому приоритет частных правил должен быть выше, чем приоритет общих. Например, если в ACL задано разрешающее правило вида 10 permit ip src net 194.85.16.0/24 dst any и требуется исключить из обработки пулом, к которому привязан ACL, весь трафик VLAN 2 данной подсети, то следует задать запрещающее правило вида 9 deny ip src net 194.85.16.0/24~2 dst any , т. е. с номером меньше 10.
2	type	Тип правила: разрешающее (allow или permit) или запрещающее (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.
3	protocol	Протокол передачи данных. Допустимые значения: ip – весь стек TCP/IP tcp udp icmp
4	src	IP-адрес отправителя. Допустимые значения (с примерами): any или 0.0.0.0/0 (любой адрес); один адрес (10.10.0.100); диапазон адресов (10.10.0.100-10.10.0.150); адрес сети/подсети (10.10.10.0/24). Если значение параметра src не указано, то ему по умолчанию присваивается значение any . При этом в команде обязательно должно быть указано значение параметра dst (см. пример 1 ниже).

№	Имя параметра	Описание
		При выводе содержимого ACL командой show или ls в правилах будет также указан тип заданного значения: any – любой адрес, host – определённый адрес, range – диапазон адресов, net – адрес сети/подсети
5	vid	Идентификатор VLAN (от 0 до 4094). Необязательный параметр. Используется в связке с параметром src . Значение vid задаётся с префиксом "~" (тильда) без пробела после значения src . Можно задать одно значение или диапазон (например, <src>~10-20). Для того чтобы задать vid для всех IP-адресов, значение параметра src должно быть задано <u>в явном виде</u> , т. е. 0.0.0.0/0 (см. пример 2 ниже). ПРИМЕЧАНИЕ Для того чтобы тегированный трафик обрабатывался в соответствии с заданными правилами, необходимо в ветке system.nat_defaults присвоить параметру vlan_mode значение vlan или qinq . В противном случае весь тегированный трафик будет проходить через EcoSGE без обработки.
6	dst	IP-адрес получателя. Допустимые значения (с примерами): any или 0.0.0.0/0 (любой адрес) один адрес (11.12.13.100) диапазон адресов (11.12.13.100-11.12.13.150) адрес сети/подсети (11.12.13.0/24) Если значение параметра dst не указано, то ему по умолчанию присваивается значение any (см. пример 3 ниже). При выводе содержимого ACL командой show или ls в правилах будет также указан тип заданного значения: any – все адреса, host – определённый адрес, range – диапазон адресов, net – адрес сети/подсети

Пример 1. Задание правила без значения **src**:

```
EcoSGE:acls.acltest# 10 allow dst 10.20.30.40
EcoSGE:acls.acltest# ls
acltest {
    10 permit ip src any dst host 10.20.30.40
}
```

Пример 2. Задание **vid** для всех IP-адресов:

```
EcoSGE:acls.acltest# 10 allow ip 0.0.0.0/0~10-20
EcoSGE:acls.acltest# ls
acltest {
    10 permit ip src 0.0.0.0/0~10-20 dst any
}
```

Пример 3. Задание правила без значения **dst**:

```
EcoSGE:acls.acltest# 10 allow ip 10.0.0.1
EcoSGE:acls.acltest# ls
acltest {
    10 permit ip src host 10.0.0.1 dst any
}
```

Сам по себе список правил не имеет значения, поэтому он должен быть привязан к определённому пулу. Привязка выполняется командой **use <имя ACL> <имя пула>**.

Пример последовательности команд для создания ACL и привязки к пулу:

```
EcoSGE:1:# create acl test
EcoSGE:2:# go acltest
EcoSGE:3:acls.acltest# show
```



```
acltest {  
}  
EcoSGE:4:acls.acltest# 10 allow ip 194.85.16.0/24~1-10 any  
EcoSGE:5:acls.acltest# show  
acltest {  
    10 permit ip src net 194.85.16.0/24~1-10 dst any  
}  
EcoSGE:6:acls.acltest# use acltest pooltest  
EcoSGE:7:acls.acltest# goto pooltest  
EcoSGE:8:pools.pooltest# show  
type cgnat  
enable  
acl acltest  
priority 100  
global_ip ( )  
...
```

8.3.4 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).

8.3.5 CGNAT-пул

CGNAT-пул осуществляет Carrier-grade NAT 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 пула данного типа, и их описание приведены выше, в разделе "Пулы и ACL".

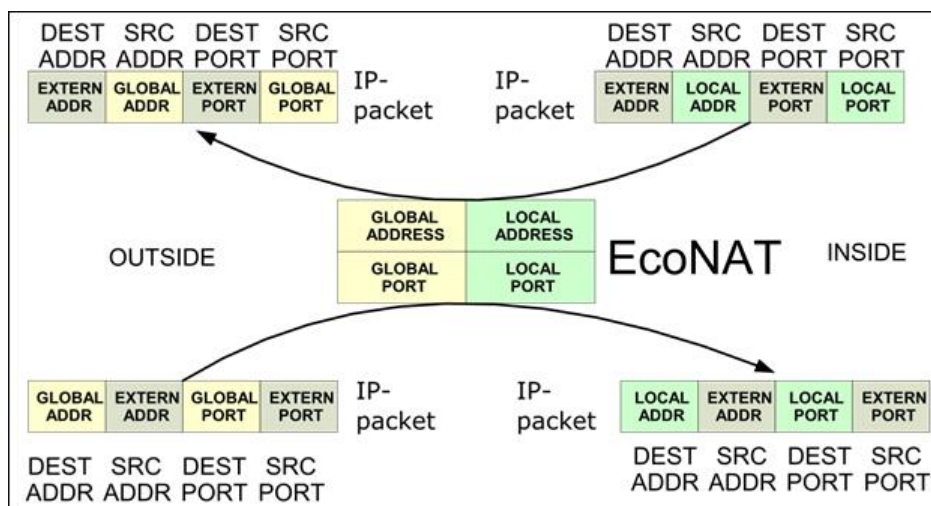


Рисунок 9

8.3.6 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".

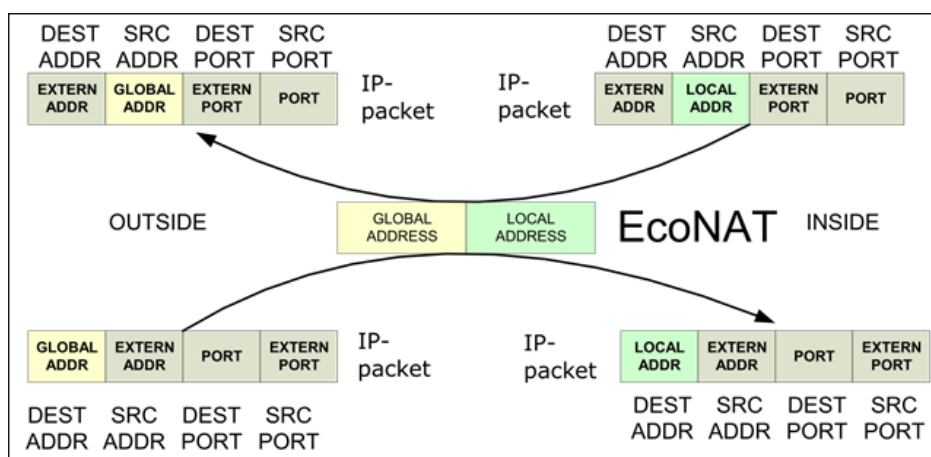


Рисунок 10

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 (хотя бы 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#
```

8.3.7 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>[~vid]-<глобальный адрес>. **Vid** - идентификатор VLAN (от 0 до 4094). Необязательный параметр. Значение vid задаётся с префиксом "~" (тильда) без пробела после адреса.

```
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:poools.poolc# global_map += 192.168.0.5-200.0.0.3
MyEcoNAT:6:poools.poolc# global_map += (192.168.1.2~102-3.3.3.3)
MyEcoNAT:7:poools.poolc#
```

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

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

ВНИМАНИЕ! Если к пулу типа **static** привязана ACL, то в списке не должно быть строчки **permit any any**.

8.3.8 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".

8.3.9 IPv6 ACL

Для того чтобы система EcoSGE обрабатывала трафик IPv6 (создавала сессии, применяла политики и сервисы BRAS и т. п.), необходима отдельная лицензия "IPV6". При наличии данной лицензии в конфигурации EcoSGE содержится ветка **system.ipv6** со следующими параметрами:

Таблица 8.6

Параметр	Описание
enable disable	Включение / выключение обработки трафика IPv6; по умолчанию enable
timeouts_inactivity tcp_handshake	Тайм-аут (в секундах) для сессии, созданной TCP-пакетом с флагом SYN (запрос на установление TCP-соединения). По умолчанию 4
timeouts_inactivity tcp_active	Тайм-аут неактивности в секундах для установленных TCP-соединений в состоянии ESTABLISHED. По умолчанию 300
timeouts_inactivity tcp_final	Тайм-аут для завершения TCP-сессий в секундах. По умолчанию 240
timeouts_inactivity tcp_reset	Тайм-аут для сброса TCP-сессий в секундах. По умолчанию 4
timeouts_inactivity tcp_session_active	Тайм-аут неактивности в секундах для активных TCP-сессий. По умолчанию 120
timeouts_inactivity udp_session	Тайм-аут неактивности в секундах для активных UDP-сессий. По умолчанию 120
timeouts_inactivity icmp_session	Тайм-аут неактивности в секундах для активных ICMP-сессий. По умолчанию 120
timeouts_inactivity no_acl	Тайм-аут неактивности в секундах для сессий, не попавших в ACL подсистемы DPI или BRAS. По умолчанию 2
timeouts_inactivity special	Особый тайм-аут неактивности в секундах для определённых TCP-портов. Данный параметр действует в связке с параметром timeouts_inactivity special_tcp_ports . По умолчанию 600
timeouts_inactivity special_tcp_ports ()	TCP-порты, к которым применяется значение параметра timeouts_inactivity special . Несколько портов указывать через пробел

8.4 Типовые конфигурации NAT

8.4.1 NAT для доступа в Интернет

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

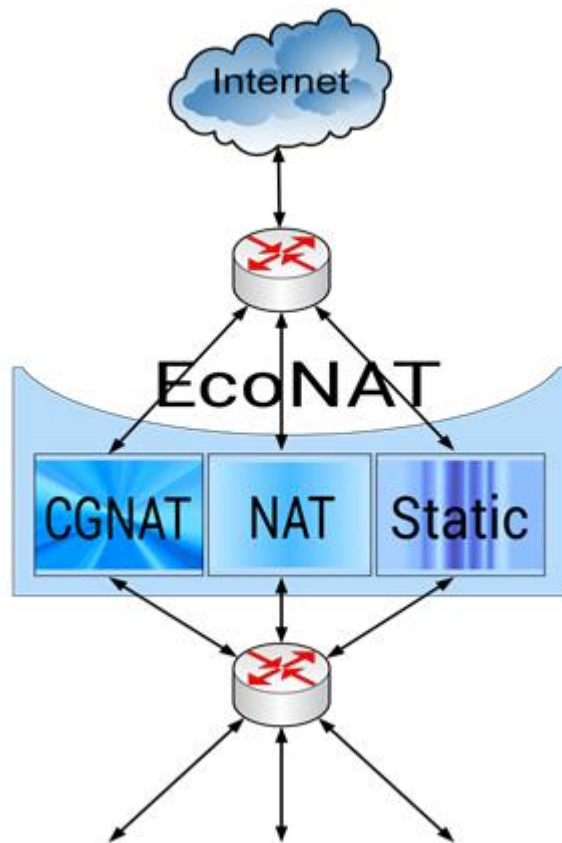


Рисунок 11

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 иницируемыми 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.

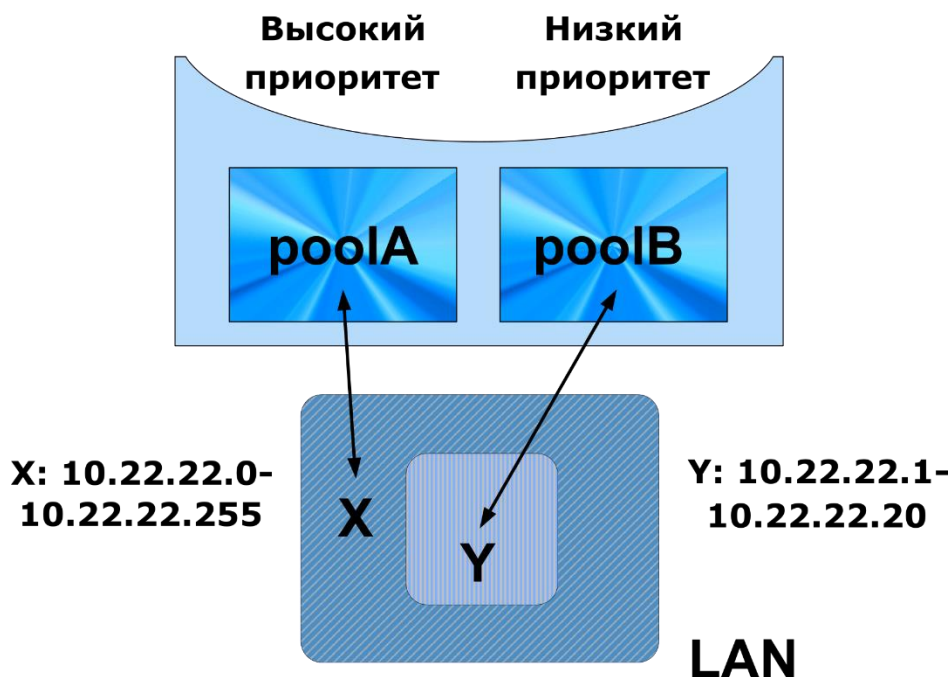


Рисунок 12

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.

8.4.2 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.

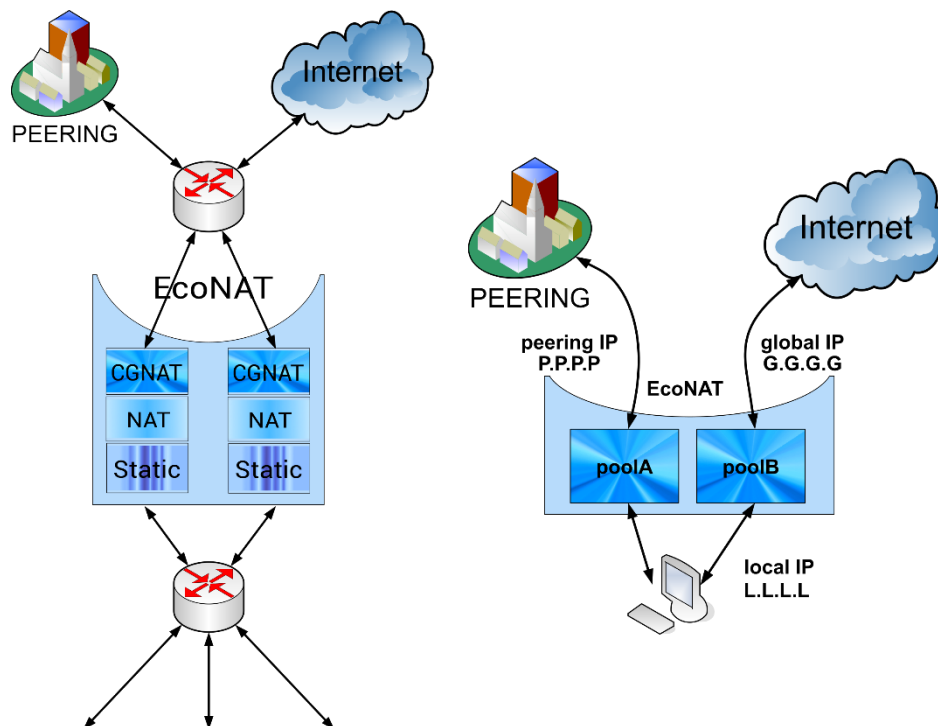


Рисунок 13

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.

8.5 Управление объектами конфигурации

8.5.1 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:#
```

8.5.2 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:#
```

8.5.3 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:#
```

8.5.4 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.mycl# no 100
MyEcoNAT:2:acls.mycl#
```

8.5.5 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:#
```


8.6 Команды просмотра

8.6.1 Просмотр трансляций

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

В таблице ниже представлены различные вариации данной команды.

Таблица 8.7

Команда	Описание
show xlate gap ADDR:PORT	Вывод всех текущих трансляций для указанной пары: глобальный адрес+ глобальный порт
show xlate gastat ADDRANGE	Вывод статистики трансляций для указанного глобального адреса
show xlate global ADDRANGE	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 ADDRANGE	Вывод статистики трансляций для указанного локального адреса
show xlate local ADDRANGE	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; UDP 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; UDP 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; UDP 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; UDP 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.
```

8.6.2 Просмотр сессий

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

В таблице ниже представлены различные вариации данной команды.

Таблица 8.8

Команда	Описание
show sessions gap ADDR:PORT	Вывод всех текущих сессий для указанной пары: глобальный адрес+ глобальный порт
show sessions global ADDR RANGE	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 ADDR RANGE	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 ADDR RANGE	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 100.64.0.4~2
egress UDP 100.64.0.4~2:1024-100.64.0.4:1024 4.4.4.4:53; Last packet 8.27
seconds ago; To be deleted in 291.73 seconds of inactivity

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

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

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

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

8.6.3 Удаление сессий

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

В таблице ниже представлены различные вариации данной команды.

Таблица 8.9

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

Команда	Описание
clear sessions global ADDRANGE	Удаление всех текущих сессий для указанного глобального адреса
clear sessions gport PORT	Удаление всех текущих сессий для указанного глобального порта (независимо от адреса)
clear sessions lap ADDR:PORT	Удаление всех текущих сессий для указанной пары: локальный адрес + локальный порт
clear sessions local ADDRANGE	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 ADDRANGE	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.
```

8.6.4 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 8.10

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
```

8.6.5 Ошибки выделения порта

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 8.11

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 8.12

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

Для сброса счётчика ошибок необходимо выполнить команду **clear cgnat errors**

9 Функциональность BRAS

Данная функциональность доступна при наличии 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 счёт, а также для демонстрации абонентам информационных сообщений путём переадресации на портал.

Предполагается следующая сервисная модель IPoE:

- отсутствие инкапсуляции PPTP, PPPoE и др., т. е. 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);
- абоненту может выдаваться либо статический IP-адрес, либо динамический (сторонним устройством, не EcoSGE) от DHCP сервера, связанного с системой биллинга.

BRAS допускает кратковременное превышение (burst) скорости трафика над расчётной. Продолжительность burst ограничена объёмом трафика, соответствующего первой секунде на законтрактованной скорости абонента.

9.1 Настройки BRAS

Настройки BRAS хранятся в ветке **system.bras**.

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

```

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

```

Включение и выключение BRAS производится непосредственно в ветке **system.bras** командами **enable** и **disable** соответственно.

Описание параметров настройки BRAS дано в таблице ниже.

Таблица 9.1

Параметр	Описание
acl	Список IP-адресов абонентов, трафик которых необходимо обрабатывать BRAS. Значение по умолчанию - none , что эквивалентно 0.0.0.0/0 , т. е. трафик любого абонента, попадающий в какой-либо пул, будет передаваться на обработку BRAS
pass_multicast	Пропускать multicast трафик прозрачно, не применяя к нему политики (рекомендуемое значение: true)
pass_routing_protocols	Пропускать трафик протоколов маршрутизации (OSPF и BGP), не применяя к ним политики (рекомендуемое значение: true)
pass_bgp_port bgp_port	Пропускать трафик BGP на выбранном TCP-порту, не применяя к нему политики (рекомендуемое значение: true)
no_shape no_shape_v6	Внешние глобальные адреса IPv4 и IPv6, для которых не ограничивается скорость (для абонентов, разрешённых системой биллинга). Здесь можно указать IP-адреса игровых серверов, серверов IPTV и других ресурсов, которые должны быть доступны абонентам без ограничения скорости
policies services	Совокупность настроек, позволяющих ограничивать скорость приёма и передачи данных, выполнять перенаправление на портал для пополнения счёта абонента и применять другие различные действия. Подробная информация содержится в разделе "Политики и сервисы"
radius	Совокупность параметров RADIUS. Подробная информация содержится в разделе "Настройка RADIUS"

Изменения настроек применяются только после выполнения команды **apply**.

9.2 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

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

remove

clearall

9.2.1 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**.

9.2.2 Команда add

```
B: add 24372 {oid} LIM10M/LIM10M 10.21.0.208, 10.210.0.207, // 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 9.2

№	Поле	Содержание поля	Описание поля
1	add	3 символа	Команда – добавить контракт
2		TAB	Разделитель
3	24372	Любая комбинация цифр и прописных и строчных латинских букв (не более 16 символов)	Идентификатор 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 К/М/Г или UNLIM	Скорость upstream (в Интернет). К/М/Г – 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	
14		SPACE	Разделитель
15	RULE	4 символа	
16	43	Число	Номер тарифа абонента (ID тарифа в биллинге)
17		LF	Конец строки запроса

9.2.3 Команда ads

Команда **ads** добавляет абонентов в общий контракт.

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

Синтаксис команды **ads** описан в таблице ниже.

Таблица 9.3

№	Поле	Содержание поля	Описание поля
1	ads	3 символа	Команда – добавить общий контракт
2		TAB	Разделитель
3	24372	Любая комбинация цифр и прописных и строчных латинских букв (не более 16 символов)	Идентификатор контракта
4		TAB	Разделитель

№	Поле	Содержание поля	Описание поля
5	{oid}	Строка 5 символов	Тип контракта (в нашем случае всегда фиксированная строка '{oid}')
6		SPACE	Разделитель
7	LIM10M	Строка: LIM значение скорости К/М/Г или UNLIM	Скорость downstream (из Интернета). К/М/Г – 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

9.2.4 Команда remove

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

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

Таблица 9.4

№	Поле	Содержание поля	Описание поля
1	remove	6 символов	Команда – удалить контракт
2		TAB	Разделитель
3	24372	Любая комбинация цифр и прописных и строчных латинских букв (не более 16 символов)	Идентификатор 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 К/М/Г или UNLIM	Скорость upstream (в Интернет). К/М/Г – 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).

9.2.5 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
```

9.2.6 Команда **clearall**

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

9.3 Команды CLI для мониторинга и управления BRAS

Для подсистемы EcoSGE BRAS предусмотрен ряд команд, которые позволяют выводить краткую и подробную информацию об обслуживаемых IP-адресах и контрактах, применяемых политиках и сервисах, а также производить сброс абонентских сессий и очистку веток конфигурации BRAS. В таблице ниже дано краткое описание всех предусмотренных команд. Подробное описание команд следует после таблицы.

Таблица 9.5

Команда	Действие
clear brascontract <id>	Закрытие сессии абонента с указанным номером персонального контракта или всех сессий абонентов с указанным номером общего контракта.
clear brasinfo { <IP-адрес> all }	Удаление информации об абонентских сессиях из таблицы BRAS. Аргументами команды могут быть IP-адрес или ключевое слово all . При указании IP-адреса соответствующая абонентская сессия будет закрыта.
droppolicies	Очистка ветки конфигурации system.bras.policies
dropradius	Очистка ветки конфигурации system.bras.radius
dropservices	Очистка ветки конфигурации system.bras.services
show brascontract <id>	Вывод информации о контракте и связанных с ним абонентах
show brascontracts	Вывод списка активных контрактов, т. е. тех, в которых есть хотя бы одна открытая абонентская сессия
show brasinfo { <IP-адрес_1>[-<IP-адрес_2>] all }	Вывод подробной или краткой информации об абонентских сессиях. Аргументами команды могут быть IP-адрес, диапазон IP-адресов или ключевое слово all .

Команда	Действие
show brasinfo summary	Вывод информации о созданных политиках и состоянии базы данных BRAS
show brasstate	Вывод информации о состоянии BRAS

9.3.1 Команды просмотра

- **show brascontract <id>**

Данная команда выводит информацию о контракте и связанных с ним абонентах: тип контракта (Shared/Not Shared, т. е. общий или персональный), IP-адрес абонента, статус авторизации и статистика принятых и отправленных байтов и пакетов. Если контракт общий, то также выводится сводная статистика байтов и пакетов по всем абонентам данного контракта. Ниже дан пример выводимой информации для общего контракта.

```
EcoSGE:# show brascontract qq
Shared      192.168.55.6      Authorized      Bytes rx/tx:
7832582/115571751; Packets rx/tx: 45613/119596
Shared      192.168.55.7      Authorized      Bytes rx/tx:
7951843/99673922; Packets rx/tx: 47917/199925
Shared      192.168.55.5      Authorized      Bytes rx/tx:
7595493/95415626; Packets rx/tx: 49795/92433
===== Shared Configuration
=====
Maximum data rate upstream total
1022 Kb/s
Maximum data rate downstream total
1022 Kb/s
Bytes downstream total
23289918
Bytes upstream total
328286141
Packets downstream total
133335
Packets upstream total
315275
```

- **show brascontracts**

Данная команда выводит список активных контрактов (персональных и общих), то есть тех контрактов, в которых имеется хотя бы одна открытая абонентская сессия.

```
EcoSGE:# show brascontracts
sh1
sh2
pers1
pers2
```

- **show brasinfo { <IP-адрес_1>[-<IP-адрес_2>] | all }**

Данная команда, в зависимости от аргумента, выводит подробную или краткую информацию об абонентских сессиях. Аргументами команды могут быть IP-адрес, диапазон IP-адресов или ключевое слово **all**.

При отправке команды с ключевым словом **all** выводится краткая информация обо всех абонентских сессиях. Пример вывода:

```
EcoSGE:# 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
...
```

При указании IP-адреса выводится подробная информация о сессии и применённых сервисах для данного абонента. Пример вывода:

```
EcoSGE:# show brasinfo 10.210.0.125
Bras info for address 10.210.0.125:
=====
Subscriber 10.210.0.125
=====
Status                               Authorized
Maximum data rate upstream total      unlim Kb/s
Maximum data rate downstream total    unlim Kb/s
Bytes downstream total                404843
Bytes upstream total                  0
Packets downstream total              5272
Packets upstream total                0
Session timeout expires in            32499 s
Idle timeout expires in               28798 s
Interim interval expires in           6 s
-----
1. serviceredi "serviceredi"
Enabled
Maximum data rate upstream            55 Kb/s
Maximum data rate downstream          55 Kb/s
Bytes downstream                      0
Bytes upstream                        0
Packets downstream                    0
Packets upstream                      0
-----
2. service20m "service20m"
Enabled
Maximum data rate upstream            20479 Kb/s
Maximum data rate downstream          20479 Kb/s
Bytes downstream                      404695
Bytes upstream                        0
Packets downstream                    5270
Packets upstream                      0
```

Если для указанного IP-адреса нет сессий, то будет выведено следующее сообщение:

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

При указании диапазона, включающего в себя не более миллиона IP-адресов, выводится подробная информация об абонентских сессиях для указанных адресов (как для команды **show brasinfo <IP-адрес>**). Если указанный диапазон содержит более миллиона адресов IP-адресов, то выводится краткая информация об абонентских сессиях (как для команды **show brasinfo all**).

Вывод информации для большого количества IP-адресов может занять некоторое время. Выполнение команды можно прервать нажатием **[Backspace]** или **[Ctrl+C]**.

В таблице ниже приведено описание данных, выводимых командой **show brasinfo <IP-адрес>**.

Таблица 9.6

Поле	Описание
Status	Статус абонента
Maximum data rate upstream total	Установленные для абонента ограничения пропускной способности исходящего канала (кбит/с)
Maximum data rate downstream total	Установленные для абонента ограничения пропускной способности входящего канала (кбит/с)
Bytes downstream total	Общее количество принятых байтов
Bytes upstream total	Общее количество отправленных байтов
Packets downstream total	Общее количество принятых пакетов
Packets upstream total	Общее количество отправленных пакетов
Session timeout expires in	Время (в секундах), оставшееся до автоматического завершения сессии. По истечении данного времени сессия удаляется и создаётся новая
Idle timeout expires in	Время (в секундах), оставшееся до автоматического завершения сессии по причине неактивности
Interim interval expires in	Время (в секундах), оставшееся до завершения интервала аккаунтинга
Информация о сервисах	
Enabled/Disabled	Состояние сервиса: включен/выключен
Maximum data rate upstream	Установленные сервисом ограничения пропускной способности исходящего канала (кбит/с)
Maximum data rate downstream	Установленные сервисом ограничения пропускной способности входящего канала (кбит/с)
Bytes downstream	Количество байтов, полученных абонентом
Bytes upstream	Количество байтов, отправленных абонентом
Packets downstream	Количество пакетов, полученных абонентом
Packets upstream	Количество пакетов, отправленных абонентом

- **show brasinfo summary**

Данная команда выводит информацию о созданных политиках BRAS, количестве абонентов, к которым применены эти политики, статусе авторизации абонентов, а также информацию о состоянии базы данных BRAS. Пример вывода:

```
EcoSGE:system# show brasinfo summary
```

```
=====
brasinfo summary
```

Policy	Subscribers
policya	3
policyb	3
Status sum for policies	
Authorization	0
Authorized	4
Rejected	0
Error	2
Deleting	0
Total	6
Database queue used/total: 0 / 524288 (0.0%)	
Database strings used/total: 0 / 1572864 (0.0%)	
Database contract data used/total: 0 / 524288 (0.0%)	
Database ip entries used/fair/total: 0 / 104857 / 2621440 (0.0%)	
Database used contract: 0 / used connection: 0 / total: 1048576 (0.0%)	

- **show brasstate**

Данная команда предназначена для просмотра состояния BRAS. Пример вывода:

```
EcoSGE:# show brasstate
Default access: BLOCK
State      : ENABLED
```

Вывод команды содержит два поля:

Default access – действие по умолчанию (BLOCK или PASS),

State – состояние BRAS (включен/выключен).

Сразу после загрузки BRAS работает в режиме пропускания всего трафика, чтобы выполнялось обслуживание абонентов в то время, пока ещё не загружена информация из системы 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**).

9.3.2 Команды закрытия сессий

- **clear brascontract <id>**

Данная команда закрывает сессию абонента с указанным номером персонального контракта или все сессии абонентов с указанным номером общего контракта. При выполнении команды выводятся IP-адреса абонентов, чьи сессии были закрыты. Этим абонентам потребуется повторная авторизация через RADIUS-сервер. Пример вывода:

```
EcoSGE:# clear brascontract sh1
Process...
```



```
66.77.88.99
1.2.3.4
5.6.7.8
Done
```

- **clear brasinfo { <IP-адрес> | all }**

Данная команда предназначена для удаления информации об абонентских сессиях из таблицы BRAS. Аргументами команды могут быть IP-адрес или ключевое слово **all**. При указании IP-адреса соответствующая абонентская сессия будет закрыта. Примеры выполнения команды:

```
EcoSGE:# clear brasinfo 10.210.30.4
Success
EcoSGE:# clear brasinfo all
Bras table purged
```

Если настроен аккаунтинг, то при выполнении команды **clear brasinfo <IP-адрес>** сначала на RADIUS-сервер отправляется запрос **Accounting Stop**, чтобы закрыть сессию, и только потом сессия удаляется из таблицы BRAS. При выполнении **clear brasinfo all** происходит только удаление записей о сессиях из таблицы BRAS.

9.3.3 Команды очистки веток конфигурации BRAS

Для очистки веток конфигурации BRAS предусмотрены следующие команды:

droppolicies – очистка ветки конфигурации **system.bras.policies**

dropradius – очистка ветки конфигурации **system.bras.radius**

dropservices – очистка ветки конфигурации **system.bras.services**

После выполнения любой из трёх вышеуказанных команд необходимо отправить команду **apply**, чтобы изменения конфигурации вступили в силу.

9.4 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.

9.4.1 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 9.7

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; 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. EcoSGE 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_NAME>=<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 попытается 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

Параметр	Описание
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 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.bras.services.service1# disable
```

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

9.4.2 Создание и настройка политики

Для создания политики необходимо отправить команду **create policy <имя политики>**. При создании политики её имя формируется аналогично имени пула или ACL. Затем необходимо перейти в ветку параметров созданной политики командой **goto policy<имя**

политики> и задать значения её параметров. Доступные параметры политики описаны в таблице ниже.

Таблица 9.8

Параметр	Описание
enable disable	Включение / выключение политики
priority	Приоритет политики. Чем меньше значение, тем выше приоритет. Политики применяются в порядке убывания приоритета. По умолчанию первой созданной политике присваивается приоритет 100, второй – 200, третьей – 300 и т. д.
local_ip ()	IPv4-адреса абонентов, к которым будет применяться политика
local_ip_v6 ()	IPv6-адреса абонентов, к которым будет применяться политика
type	Тип политики: static – к абонентам применяются сервисы, указанные в параметре services ; dynamic – для авторизации абонентов используется протокол RADIUS (должен быть настроен RADIUS-сервер)
session_timeout	Максимальное время существования сессии (в секундах). По истечении данного времени текущая сессия закрывается и создаётся новая. Значение по умолчанию – 86400
idle_monitor_direction	Данный параметр определяет, по каким пакетам будет происходить сброс таймера простоя сессии (параметр idle_timeout). Возможные значения: both – сброс таймера будет происходить по исходящим и входящим пакетам (по умолчанию); egress – сброс таймера будет происходить только по исходящим пакетам
idle_timeout	Максимальное время простоя сессии (в секундах). При отсутствии активности в течение данного времени сессия будет закрыта. Значение по умолчанию – 28800
interim_interval	Периодичность аккаунтинга (в секундах). Применяется при включённом функционале RADIUS. Значение по умолчанию – 15
ingress_auth	Разрешить (on) / запретить (off) авторизацию абонента по входящему пакету с Destination IP-адресом абонента. Применимо только к абонентам из пулов типа Static и Fake.
services ()	Имя сервиса, привязываемого к политике. Можно указать до 6 сервисов через пробел. Порядок указания сервисов определяет их приоритет (по убыванию). Параметры, настраиваемые в случае type dynamic , описаны в разделе "Настройка RADIUS"
Параметры динамической политики	
auth	Параметры авторизации. Имя подключения к RADIUS-серверу или имя группы RADIUS-серверов
reauthorization_timeout	Периодичность (в секундах) повторной отправки запроса авторизации абонента при отсутствии ответа от RADIUS-сервера (BRAS-сессия абонента при этом находится в статусе Error). Значение по умолчанию – 180
acct	Параметры аккаунтинга. Имя подключения к RADIUS-серверу или имя группы RADIUS-серверов

ВНИМАНИЕ! Перед применением изменений значение параметра **auth** не должно быть **none**. В противном случае команда **apply** завершится ошибкой.

Пример создания и настройки политики:

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

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

```
EcoSGE:system.bras.policies.policy1# enable
EcoSGE:system.bras.policies.policy1# disable
```

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

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

9.5 Настройка RADIUS

Настройки RADIUS находятся в ветке **system.bras.radius**. Данная ветка содержит следующие разделы и параметры:

- **request_burst_interval** – интервал в миллисекундах между отправками блоков пакетов Access-Request и Accounting-Request. Допустимые значения: от 1 до 1000 (по умолчанию 10);
- **request_burst_size** – максимальное количество пакетов Access-Request и Accounting-Request в отправляемом блоке. Допустимые значения: от 1 до 1000 (по умолчанию 64);

coa – раздел параметров RADIUS Change of Authorization;

radius_groups – раздел параметров групп RADIUS-серверов;

radius_servers – раздел параметров подключения к RADIUS-серверам.

Ниже описаны структура и команды конфигурирования перечисленных разделов.

9.5.1 Настройка подключения к RADIUS-серверу

В первую очередь необходимо создать новое подключение к RADIUS-серверу командой **create radius <имя подключения>**. При создании подключения его название формируется аналогично имени нового пула (см. раздел "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 9.9

Параметр	Описание
enable disable	Включен или выключен доступ к RADIUS-серверу
server	IP-адрес RADIUS-сервера. По умолчанию: 0.0.0.0
acct_port	Порт RADIUS-сервера для аккаунтинга. По умолчанию: 1813
auth_port	Порт RADIUS-сервера для аутентификации и авторизации. По умолчанию: 1812
secret	Пароль для аутентификации на RADIUS-сервере

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

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

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 9.10

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 т.д.
local_ip local_ip_v6	Задаются адреса или подсети клиентов, к которым будет применяться данная политика
type dynamic	Включает авторизацию абонентов по протоколу RADIUS
auth	Параметры авторизации. Имя группы RADIUS-серверов или ключевое слово none
acct	Параметры аккаунтинга. Имя группы RADIUS-серверов или ключевое слово none
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. Примечание: по истечении заданного интервала отправляется повторный Access-Request (RADIUS-сервер может переопределить длительность данного интервала параметром Session-Timeout). То же происходит и для абонентов, на попытку авторизации которых получен Access-Reject от RADIUS-сервера
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 60 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

ВНИМАНИЕ! Перед применением изменений значение параметра **auth** не должно быть **none**, иначе команда **apply** завершится с ошибкой.

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 )
```

9.5.2 Группы RADIUS-серверов

Для повышения надёжности RADIUS-серверы объединяются в группы, в которых можно распределять нагрузку между серверами и реализовывать резервирование. В динамических политиках BRAS указываются именно группы, а не отдельные серверы.

В текущей реализации допускается до 16 групп RADIUS-серверов. При этом один и тот же сервер может принадлежать к нескольким группам одновременно.

Для создания группы RADIUS-серверов используется команда конфигурационного режима **create radiusgroup** <RADIUS_GROUP>, где <RADIUS_GROUP> - имя создаваемой группы RADIUS-серверов.

По умолчанию конфигурация только что созданной группы выглядит следующим образом.

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

Для удаления группы RADIUS-серверов используется команда конфигурационного режима **no radiusgroup** <RADIUS_GROUP>, где <RADIUS_GROUP> - имя удаляемой группы RADIUS-серверов. Также может использоваться команда **dropradius**, в результате которой будут удалены все группы и сервера RADIUS.

В режиме конфигурации группы RADIUS-серверов можно отредактировать или удалить описание группы, настроить режим ее работы, добавить или удалить выбранный RADIUS-сервер из группы. Данные команды и параметры описаны в таблице ниже.

Таблица 9.11

Команда/параметр	Описание
description <TEXT>	Задание описания группы RADIUS-серверов. <TEXT> - строка описания. Описания радиус-групп, содержащие пробелы, должны заключаться в кавычки
no description	Удаление описания группы RADIUS-серверов
type <MODE>	Настройка режима работы группы RADIUS-серверов. Допустимые значения режима работы группы RADIUS-серверов - <MODE>: active_standby - для всех запросов используется RADIUS-сервер с наибольшим приоритетом в группе. Приоритет определяется порядком указания серверов в параметре servers (). Этот сервер является активным (active), остальные при этом находятся в режиме ожидания (standby). Если RADIUS-сервер с наибольшим приоритетом перестает отвечать на запросы, то запросы начинают поступать на следующий по приоритету сервер. По истечении определенного периода времени производится попытка повторить отправку запросов на наиболее приоритетный сервер. Если такая попытка удачна, то он снова становится активным; round_robin - запросы распределяются между всеми RADIUS-серверами группы. Например, если группа состоит из 3 RADIUS-серверов, пришло 5 запросов от клиентов. 1-ый запрос отправляется на 1-ый сервер, 2-ой - на 2-ой сервер, 3-ий - на 3-ий сервер, 4-ый запрос - снова на 1-ый сервер, 5-ый на 2-ой и т.д. Значение по умолчанию - active_standby
Настройка таймеров	
request_max <NUMBER>	Количество запросов, после отсутствия ответа на которые сервер будет считаться недоступным (DEAD). Значение по умолчанию - 3
request_timeout <INTERVAL>	Временной интервал между отправкой запросов в секундах. Значение по умолчанию - 3 секунды
dead_time_min <MIN> dead_time_max <MAX>	Временной интервал в секундах, в течение которого сервер будет находиться в состоянии DEAD. Задаются минимальное <MIN> и максимальное <MAX> значения. По умолчанию <MIN> - 15 секунд, <MAX> - 300 секунд. Допустимые значения <MIN> и <MAX> - от 0 до 65535. Принцип использования dead_time После отсутствия ответа RADIUS-сервера на <NUMBER> запросов (параметр request_max), ранее отмеченного как ACTIVE, такой сервер помечается как DEAD на период <MIN>, и роутер, посылающий запросы, перенаправляет их на резервный RADIUS-сервер внутри группы. По окончании этого интервала запросы будут вновь посланы на ставший неактивным RADIUS-сервер. Если он ответит, то вновь станет ACTIVE. Если RADIUS-сервер не ответит, то останется помеченным как DEAD. Интервал для такого его состояния будет увеличен на <MIN> (то есть после первой неудачной попытки интервал составит <MIN>, после второй - 2*<MIN>, после третьей - 3*<MIN> и т.д.). Так будет продолжаться до того момента, пока интервал назначения отметки DEAD не достигнет значения <MAX>. После этого попытки обращения к такому RADIUS-серверу будут делаться раз в интервал <MAX> до первого успешного перехода RADIUS-сервера в состояние ACTIVE. Если <MAX> не кратен <MIN>, то интервал станет равным <MAX> после первого его превышения в результате увеличения на очередной <MIN>

Добавление серверов в группу (параметр servers)

Серверы включаются в группу командой **add <имя сервера>**, символьной командой **'+='** или перечислением через пробел в скобках в параметре **servers ()**.

Пример:

```
2:2:# create radiusgroup 1
2:3:# create radius 1
2:4:# create radius 2
2:5:# create radius 3
2:6:# create radius 4
2:7:# go radiusgroup1
2:8:system.bras.radius.radius_groups.radiusgroup1# servers (radius1
radius2)
2:9:system.bras.radius.radius_groups.radiusgroup1# servers add radius3
2:10:system.bras.radius.radius_groups.radiusgroup1# servers += radius4
2:11:system.bras.radius.radius_groups.radiusgroup1# show servers
servers ( radius1 radius2 radius3 radius4 )
```

Порядок серверов в списке имеет значение! Он определяет порядок опроса серверов. Нельзя включать в группу сервер, который ещё не создан.

Для удаления RADIUS-сервера из группы используется символьная команда '-='.

9.5.3 Авторизация пользователя на RADIUS-сервере

Для авторизации пользователя на RADIUS-сервере BRAS отправляет RADIUS Access-Request со следующей информацией:

- User_Name = <IP-адрес пользователя | MAC-адрес пользователя (для DHCP Option 82)>
- User-Password = <EcoSGE hostname>
- Framed-Protocol = <PPP>

Framed-IP-Address = <IP-адрес пользователя>

- Calling-Station-Id = <MAC-адрес пользователя>
- NAS-IP-Address = <IP-адрес MNG-интерфейса EcoSGE>

Атрибут User-Password используется только для обеспечения совместимости с некоторыми системами биллинга. Такими системами предъявляются требования только к наличию данного атрибута в сообщениях Access-Request, поэтому 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-Асcept от RADIUS сервера пользователю назначается сервис, указанный в параметре **if_auth_accept**, и соответствующие ему ограничения скорости. Сессия пользователя регулируется таймаутами, заданными в параметрах **session_timeout**, **idle_timeout**, **interim_interval**. Однако в том случае, если Access-Асcept от RADIUS-сервера содержит дополнительные атрибуты с сервисами и/или таймаутами, то пользователю автоматически назначаются именно они, а соответствующие настройки политик и сервисов BRAS игнорируются.

Для IPv6-сетей, в которых для назначения IPv6-адресов используется технология DHCPv6 Prefix Delegation, в BRAS реализована обработка атрибута Delegated-IPv6-Prefix (<https://tools.ietf.org/html/rfc4818>), которая заключается в следующем: если ответ Access-Accept содержит атрибуты

- Cisco-Account-Info := "P<string>",
- Cisco-Account-Info += "VU;<integer>;D;<integer>",
- Delegated-IPv6-Prefix = "<OctetString>",

то BRAS запоминает делегированный префикс IPv6, после чего всех пользователей с данным префиксом BRAS будет авторизовывать без обращения к RADIUS-серверу и применять к ним атрибуты общего контракта и все остальные атрибуты из ответа Access-Accept. Допускается не более пяти атрибутов Delegated-IPv6-Prefix на одного пользователя.

BRAS обрабатывает следующие атрибуты, содержащиеся в RADIUS Access-Accept:

- Cisco-Account-Info – ограничение скорости Upload/Download (бит/с) для персонального (QU/D) или общего (VU/D) контракта, тип значения – Integer; идентификатор общего контракта P, тип значения – String
- Cisco-Service-Info – принудительное назначение сервиса, настроенного на BRAS. Имя сервиса задается в виде: **A<имя сервиса>**
- Framed-Callback-Id – уникальный идентификатор пользователя, который подставляется в **redirect_url** через спецификатор **%c**
- Framed-IP-Address
- RDP_SHARED_SERVICES
- Idle-Timeout
- Session-Timeout
- Acct-Interim-Interval
- Delegated-IPv6-Prefix – делегированный префикс IPv6, тип значения – OctetString

Например:

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

ПРИМЕЧАНИЕ

В определённых случаях при очень большом количестве абонентских соединений RADIUS-сервер может не справляться с обработкой запросов на авторизацию и/или аккаунтинг. Во избежание перегрузки RADIUS-сервера предусмотрена возможность ограничения скорости отправки запросов. Для этого в ветке **system.bras.radius** есть параметры

request_burst_size и **request_burst_interval**, которые позволяют задать максимальное количество пакетов Access-Request и Accounting-Request, передаваемых в одном блоке, и интервал между отправками таких блоков (см. раздел Логирование).

9.5.4 Счетчики

Для просмотра счетчиков по RADIUS используется команда **show counters all | include radius**.

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

В таблице ниже приведено описание существующих счетчиков данного раздела.

Таблица 9.12

Счетчик	Описание
radius_authorization_success	Количество принятых Access_Response пакетов со статусом Accept
radius_authorization_reject	Количество принятых Access_Response пакетов со статусом Reject
radius_authorization_bad_response	Количество принятых Access_Response пакетов из-за проблем настроек EcoNAT и RADIUS-сервера (например, несовпадающий пароль)
radius_authorization_error	Количество отправленных Access_Request пакетов с возникновением проблем, отличных от описанных выше
radius_accounting_send_try	Количество попыток провести RADIUS-аккаунтинг пользователя
radius_accounting_success	Количество принятых Accounting_Response пакетов
radius_accounting_reject	Количество ответов reject при отправке/приеме RADIUS-пакетов
radius_accounting_error	Количество ответов error при отправке/приеме RADIUS-пакетов
radius_accounting_bad_response	Количество ответов bad_response при отправке/приеме RADIUS-пакетов
radius_accounting_default_handler	Количество аккаунтинг-запросов через RADIUS с возникновением проблем, отличных от описанных выше
radius_accounting_session_timeout	Количество срабатываний session_timeout
radius_accounting_idle_timeout	Количество срабатываний idle_timeout
radius_coa_get_packet	Количество принятых пакетов на CoA-порт EcoNAT
radius_coa_bad_packet	Количество принятых на CoA-порт пакетов, непригодных для обработки
radius_coa_no_entry	Количество принятых на CoA-порт пакетов, для которых не найден абонент
radius_coa_request	Количество принятых на CoA-порт пакетов типа coa_request
radius_coa_ack	Количество пакетов типа coa_request , по которым отправлен пакет типа coa_ack
radius_coa_nak	Количество пакетов типа coa_request , по которым отправлен пакет типа coa_nak
radius_coa_disconnect_request	Количество принятых на CoA-порт пакетов типа coa_disconnect_request
radius_coa_disconnect_ack	Количество пакетов типа coa_disconnect_request , по которым отправлен пакет типа coa_disconnect_ack
radius_coa_disconnect_nak	Количество пакетов типа coa_disconnect_request , по которым отправлен пакет типа coa_disconnect_nak

9.6 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.

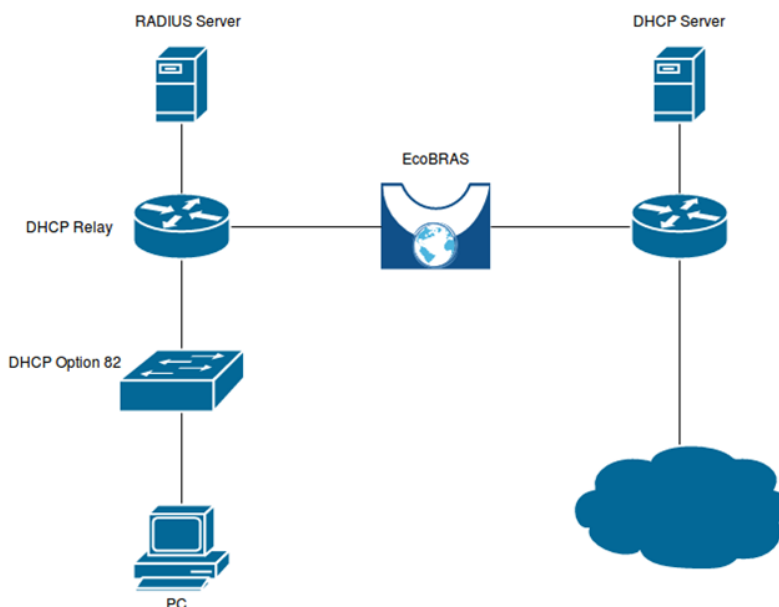


Рисунок 14

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\0330
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.

9.7 Общие контракты

BRAS может обслуживать несколько абонентов в рамках общего контракта (shared contract). Абонентам с таким контрактом предоставляется общий логический канал, пропускная способность которого распределяется между участниками контракта пропорционально их активности. Как и в случае с персональными контрактами, аутентификация и авторизация абонентов с общим контрактом возможна по протоколу RADIUS или проприетарному протоколу EcoBRAS в зависимости от версии встроенного программного обеспечения и установленных лицензий.

9.7.1 Общие контракты и протокол RADIUS

Если для аутентификации и авторизации абонентов используется протокол RADIUS, то для обслуживания нескольких абонентов в рамках общего контракта необходимо добавить в базу данных RADIUS-сервера записи обо всех абонентах с общим контрактом. Например, при использовании FreeRADIUS и файла 'users' записи для общего контракта должны иметь следующий вид:

```
<IP-адрес>      Auth-Type := Accept
                  Cisco-Account-Info += "P<string>",
                  Cisco-Account-Info += "VU;<integer>;D;<integer>"
```

где:

P<string> – идентификатор общего контракта (например, P123); допускается использование комбинации цифр и прописных и строчных латинских букв (не более 16 символов);

VU;<integer>;D;<integer> – пропускная способность канала Upstream и Downstream для общего контракта. Задаётся в битах в секунду.

При необходимости можно дополнительно задать для абонента персональные ограничения пропускной способности. Для этого следует добавить атрибут Cisco-Account-Info с переменными QU | D. Пример:

```
<192.168.55.5>   Auth-Type := Accept
                  Cisco-Account-Info := "QU;500000000;D;500000000",
                  Cisco-Account-Info += "P123",
                  Cisco-Account-Info += "VU;10000000000;D;10000000000"
```

В связи с определёнными особенностями работы BRAS необходимо при конфигурировании общего контракта следить за тем, чтобы у всех абонентов значения VU | D были одинаковыми. Для пояснения рассмотрим простой пример. В общий контракт включено 5 абонентов. Для первых четырёх из них задано "VU;10000000000;D;10000000000", т. е. контракт подразумевает предоставление общего канала 1 Гбит/с. Для пятого абонента ошибочно задано "VU;500000000;D;500000000", т. е. 50 Мбит/с. Предположим, что первые четыре абонента уже авторизованы и смотрят потоковое видео в разрешении 4K. При авторизации пятого абонента BRAS применит его значения VU | D и к остальным четырём абонентам (всегда применяются последние поступившие от RADIUS-сервера значения VU | D). Таким образом, пять абонентов станут использовать общий канал 50 Мбит/с, чего явно недостаточно для просмотра 4K-видео. Это может вызвать претензии со стороны абонентов.

9.7.2 Общие контракты и протокол EcoBRAS

Общие контракты можно сконфигурировать непосредственно на устройстве EcoSGE с помощью проприетарного протокола EcoBRAS. Добавление абонентов в общий контракт производится командой **ads**. Описание синтаксиса команды дано в разделе Консоль биллинга и протокол EcoBRAS.

В отличие от общих контрактов, сконфигурированных на RADIUS-сервере, протокол EcoBRAS позволяет задать только пропускную способность общего канала. Возможность задания персональных ограничений для отдельных абонентов не предусмотрена. Но при этом можно одной командой добавить в общий контракт сразу несколько абонентов.

Как и в случае с общими контрактами, сконфигурированными на RADIUS-сервере, при добавлении абонентов в общий контракт по протоколу EcoBRAS следует помнить, что значения переменных LIM в команде **ads** должны быть одинаковыми у всех абонентов в рамках одного контракта, поскольку BRAS будет применять последнее считанное значение ко всем абонентам.

10 Функциональность URL-фильтрации (DPI)

Данная функциональность доступна при наличии лицензии EcoDPIxxxx-LIC. Информация об установленных лицензиях выводится командой **show license** (см. раздел "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. Данная функциональность соответствует всем требованиям и прошла 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») задаётся отдельно для каждого списка фильтрации. Поддерживается фильтрация по подсетям.

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

Основной список запрещённых сайтов – это Единый реестр Роскомнадзора (РКН), который имеет предопределённое имя **dpilist0** в конфигурационном пространстве **system.dpi**. Кроме того, поддерживаются до 16 списков сайтов, задаваемых пользователем (**dpilist1 ... dpilist16**), каждый из которых может быть либо чёрным (список запрещённых сайтов), либо белым (список разрешённых сайтов).

Возможна фильтрация абонентских соединений одновременно по нескольким спискам. При одновременном срабатывании нескольких списков будет выполняться действие, заданное для списка с наивысшим приоритетом (с наименьшим номером).

Срабатывание по чёрному списку означает запрет доступа к странице. В этом случае HTTP-соединение будет перенаправлено на заданную в конфигурации страницу, а HTTPS-соединение будет закрыто по RST.

Срабатывание по белому списку означает разрешение доступа к странице. Отсутствие события по белому списку означает, что доступ по умолчанию запрещён (и будет выполнено перенаправление или закрытие). Однако абонент может быть подписан на несколько белых списков одновременно, и в таком случае для доступа к странице достаточно, чтобы сработал хотя бы один из них.

Формат загружаемых списков: текстовый файл с перечнем URL, начинающихся со схемы “http://” или “https://”, в которых также может быть указан номер порта. 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, а если только один из протоколов, то перед '*' указывается схема “http://” или “https://”. Кроме URL в списках могут быть указаны IP-адреса (v4 и v6), подсети и диапазоны адресов (через дефис, только для IPv4). IPv6-адреса должны быть заключены в квадратные скобки. IP-адреса могут быть указаны в связке с портом или диапазоном портов.

Разделителем строк в файле выступает CR или CR LF (конец строки и переход на новую строку). Имя и расширение файла не регламентируются.

В списках допускается использование комментариев. Например, для логического разделения Интернет-ресурсов на группы по тематикам. Каждая строка комментария должна начинаться с символа решётки '#'. Кроме того, этим же символом можно при необходимости "закомментировать" определённые строки в списке, чтобы они не обрабатывались при построении или обновлении базы данных.

Пример содержимого файла:

```
http://www.badsite.com:8080/badpath.htm
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
# ip:port
22.48.50.55:2020
149.154.1.5/16:3000-9000
[2001:67c:4e8:f002::0:0001]/112:3000-9000
```

Если URL в списке указан без схемы “http://” или “https://”, то по умолчанию считается, что в списке он фигурирует с обеими схемами. При этом фильтр для HTTPS-соединений будет срабатывать только на указанное доменное имя. То есть при указанном в примере выше 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, то в списке должно быть указано “http://ru.wikipedia.org/wiki/GRE_(протокол)”.

10.1 Настройка URL-фильтрации

Настройки 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 EcoSGE называются **dpilistN**, где **N** - порядковый номер от 0 до 16.

```
EcoSGE:# go dpi
EcoSGE:system.dpi# ls
enable
extra_analyze off
functionality_mode normal_nat
revisors ( )
dpilist0
{
  enable
```

```
rkn_source rkn
rkn_login "0123456789"
rkn_password "qlw2e3r4t5y6u7i8o9p0"
rkn_proxy ""
upload_dump_server ""
whitelist_mode off
log_matches off
log_pictures off
exceptions off
behaviour block
redirect_use_interval off
redirect_interval 600
redirect_interval_url 2592000
redirect_url "http://www.provider.ru/blocked/block0.html"
color_direction both
color_tos_byte 32
download_url "http://192.168.10.1/dump.xml"
update_schedule interval 600
protocols ( )
no_ip ( 10.210.0.123~0-4095 )
no_ip_remote ( )
ip (
    10.0.0.0/8~1-10
    61.216.14.0/23~0-4095
)
no_ipv6 ( )
ipv6 ( )
}
dpilist1
{
    disable
    whitelist_mode off
    log_matches off
    log_pictures off
    exceptions off
    behaviour block
    redirect_use_interval off
    redirect_interval 600
    redirect_interval_url 2592000
    redirect_url http://www.provider.ru/blocked/block1.html
    color_direction both
    color_tos_byte 32
    download_url http://www.provider.ru/blacklists/list1.txt
    update_schedule never
    protocols ( )
    no_ip ( )
    no_ip_remote ( )
    ip ( )
    no_ipv6 ( )
    ipv6 ( )
}...
```

Включение и выключение URL-фильтрации выполняется в ветке **system.dpi** командами **enable** и **disable** соответственно.

Кроме того, каждый из списков сайтов может быть отдельно включен или выключен командами **enable** и **disable**, выполненными в конфигурационном пространстве списка.

Возможны две схемы подключения устройства EcoSGE:

- в разрыв соединения (на первом рисунке ниже),
- с двойным зеркалированием трафика (на втором рисунке ниже).

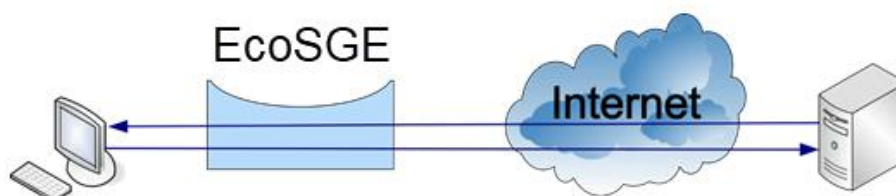


Рисунок 15

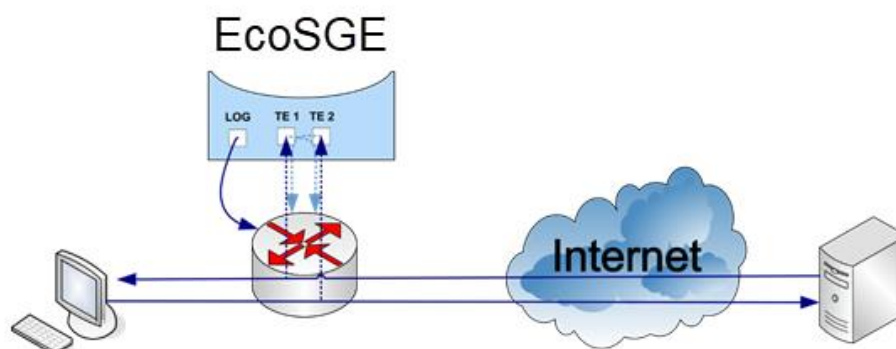


Рисунок 16

Каждой схеме подключения соответствует определённый режим функционирования EcoSGE, который задаётся параметром **functionality_mode** в ветке **system.dpi**. Для схемы "в разрыв" необходимо задать значение **normal_nat**, а для схемы с зеркалированием – **double_mirrored_traffic**.

В режиме зеркалирования EcoSGE анализирует входящий и исходящий трафик и выполняет его трансляцию, как и в обычном режиме. Для этого исходящий от абонентов трафик зеркалируется на локальные (чётные) интерфейсы EcoSGE, а входящий из Интернета к абонентам – на глобальные (нечётные) интерфейсы EcoSGE (см. раздел "Помощь пользователям"). Если EcoSGE 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 EcoSGE использует логирующий интерфейс или интерфейсы (см. раздел "Оборудование"), тогда как в обычном режиме для этого используются те же сетевые интерфейсы, через которые проходит абонентский трафик. Поэтому для корректной работы схемы зеркалирования в EcoSGE 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 EcoSGE.

Если на EcoSGE 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 EcoSGE и интерфейса маршрутизатора (IP-адрес которого указан как шлюз по умолчанию в контексте конфигурации **connection_log**). При этом можно настроить EcoSGE таким образом, чтобы из логирующего интерфейса отправлялся нетегированный трафик. Для этого необходимо в ветке конфигурационного дерева **connection_log** присвоить параметру **strip_tags** значение **on**.

В таблице ниже приведены параметры **dpilist**.

Таблица 10.1

Параметр	Описание
enable / disable	Определяет состояние списка: enable – включён, disable – выключен
whitelist_mode	Задаёт тип списка: белый или чёрный. Чёрный список (значение off) определяет, к каким сайтам доступ запрещён. Белый список (значение on), наоборот, разрешает доступ только к перечисленным в нём сайтам и может быть использован, например, для организации «детского интернета». ВНИМАНИЕ! При использовании белого списка возможна полная блокировка доступа (см. пояснение под таблицей)
log_matches	Определяет, будет ли выполняться логирование обращений к запрещённым сайтам. Значения: on , off
log_pictures	Определяет, будет ли выполняться логирование изображений на сайте. Учитываются форматы *.bmp, *.gif, *.jpeg, *.jpg, *.png, *.tif, *.tiff. Значения: on , off
exceptions	Применяет список исключений к данному списку. Значения: on , off
behaviour	Определяет действие, выполняемое при срабатывании условия чёрного списка или несрабатывании условия белого списка: block – блокировка HTTPS, перенаправление HTTP на страницу, заданную в параметре redirect_url ; redirect – перенаправление HTTP на страницу, заданную в параметре redirect_url , пропускание HTTPS; color – подкраска; ignore – нет определенного действия
redirect_use_interval	Включает использование таймеров перенаправления. При выключении этого параметра перенаправление будет выполняться при каждой 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 минут открываться в обычном режиме
redirect_interval_url	Интервал между перенаправлениями одной и той же страницы, в секундах. 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. Затем снова сработает перенаправление
redirect_url	URL, на который будет перенаправлено HTTP-соединение. Если задано behaviour block , то в строку URL можно добавлять спецификаторы, указывающие на абонента, что позволяет, например, персонифицировать страницу переадресации. Допустимые спецификаторы: %c – передавать callback-id, полученный от RADIUS-сервера; %i – передавать IP-адрес абонента; %m – передавать MAC-адрес абонента;

Параметр	Описание
	%u – передавать URL, к которому обратился абонент; %v1 – передавать первый (верхний) VLAN ID абонента; %v2 – передавать второй (нижний) VLAN ID абонента. При использовании спецификаторов значение параметра redirect_url задаётся в виде <code><URL>/?<var_1>=<spec_1>&<var_2>=<spec_2>...<var_n>=<spec_n></code>, где: URL – адрес страницы, на которую производится перенаправление; var_1 ... var_n – имена переменных, определённых на сервере, на который производится перенаправление; spec_1 ... spec_n – спецификаторы. Например, если указан redirect_url <code>http://example.com/?var1=%u&ip=%i&qwe=%v2</code>, то при обращении абонента с IP-адресом 10.1.1.10 к запрещённому ресурсу forbidden.com будет произведено перенаправление на страницу <code>http://example.com/?var1=forbidden.com&ip=10.1.1.10&qwe=0</code>. Если задано behaviour redirect, то всегда используется URL вида <code>http://domain/?list=%dpilist_number%&ip=%client_ip_address%&hash=%user_agent_hash%&src_url=%URL%</code>, где: domain – доменное имя или IP-адрес хоста, на который производится перенаправление; list – номер DPI-списка, в котором выполнено условие перенаправления; ip – IP-адрес абонента; hash – CRC32 хеш из поля User-Agent в клиентском HTTP-пакете; если User-Agent отсутствует, то hash=0; src_url – URL, к которому обратился клиент. Для правильной обработки дополнительной информации, передаваемой в строке URL, соответствующие переменные должны быть предварительно определены на сервере, на который производится перенаправление.
color_direction	Маркируемое направление трафика: egress – маркируется трафик от пользователя в Интернет; ingress – маркируется трафик из Интернета к пользователю; both – маркируется трафик в обоих направлениях; no – трафик не маркируется
color_tos_byte	Значение, которое будет устанавливаться в поле type of service в заголовке пакета. Задаётся в десятичном формате
download_url	URL, откуда будет скачиваться список в случае автообновления (поддерживаются протоколы HTTP, FTP, TFTP). Для списка dpilist0 - адрес, по которому будет храниться предварительно скачанный 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)
protocols	Блокируемые протоколы (см. раздел "Фильтрация протоколов"). Можно задать несколько протоколов через пробел
no_ip	IPv4-адреса абонентов (source), исключаемые из сферы действия списка (параметр no_ip обрабатывается раньше, чем ip). Можно задать один адрес, диапазон или адрес сети/подсети. С префиксом "~" (тильда) без пробела после адреса можно также указать VLAN ID (одно значение или диапазон). Примеры допустимых значений: один адрес: 10.0.10.2 диапазон адресов: 10.0.10.2-10.0.10.100 адрес сети: 10.0.0.0/8

Параметр	Описание
	один адрес + VID: 10.0.10.2~5 диапазон адресов + VID: 10.0.10.2-10.0.10.100~5 адрес сети + диапазон VID: 10.0.0.0/24~2-10 Можно ввести несколько значений через пробел: no_ip (10.0.10.2 10.0.10.50-10.0.10.100~3 10.0.0.0/24~10-20)
no_ip_remote	IPv4-адреса назначения (destination), исключаемые из сферы действия списка.
ip	IPv4-адреса абонентов (source), попадающие под действие списка. Допустимые значения те же, что и для параметра no_ip . Для обработки трафика со всех адресов необходимо задать значение 0.0.0.0/0 или any
no_ipv6	IPv6-адреса абонентов (source), исключаемые из сферы действия списка (параметр no_ipv6 обрабатывается раньше, чем ipv6). Допустимые значения те же, что и для параметра no_ip
ipv6	IPv6-адреса абонентов (source), попадающие под действие списка. Допустимые значения те же, что и для параметра no_ip . Для обработки трафика со всех адресов необходимо задать значение ::/0 или any
Параметры только dpilist0 (списка Роскомнадзора)	
rkn_source	Источник для загрузки списка Роскомнадзора: rkn – сервер Роскомнадзора, grfc – сервер ГРЧЦ (ФГУП "Главный Радиочастотный Центр")
rkn_login	Логин для авторизации в системе Роскомнадзора.
rkn_password	Пароль для авторизации в системе Роскомнадзора. Хранится в зашифрованном виде. Копирование на другое устройство недопустимо
rkn_proxy	Прокси-сервер. Указывается в формате [<PROTOCOL>://[<USER>:<PASSWORD>@]<URL>[:<PORT>] , где: PROTOCOL – протокол прокси-сервера: SOCKS4, SOCKS5 или HTTP(S); если не указан, то используется HTTP; USER - имя пользователя для неанонимного прокси-сервера; PASSWORD - пароль для неанонимного прокси-сервера; URL - IP-адрес или доменное имя прокси-сервера; PORT - порт прокси-сервера; если не указан, то используется TCP-порт 1080

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**, то создаются соответствующие абонентские сессии. Состояние этих сессий можно проверить при помощи команды **show sessions local any**.

```
EcoSGE:system.dpi# show sessions local any
```



```

ipv6 egress UDP [2001:DB8:3333:4::5]:58712-[2001:DB8:3333:4::10]:33435;
Last packet 6.10 seconds ago; To be deleted in 293.90 seconds of
inactivity.
ipv6 ingress UDP [2001:DB8:3333:4::5]:33435-[2001:DB8:3333:4::10]:63607;
Last packet 37.46 seconds ago; To be deleted in 262.54 seconds of
inactivity.

```

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

Таблица 10.2

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

10.2 Загрузка списков

10.3 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>* **ftp://<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**.

Команда **dpiload 0** инициирует обновление реестра с сервера Роскомнадзора или ГРЧЦ, в зависимости от значения параметра **rkn_source** в ветке **system.dpi**. Если в настройках списка

dpilist0 указан параметр **download_url**, и при этом сервер Роскомнадзора или ГРЧЦ недоступен, 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").

10.4 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**.

10.5 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**.

10.6 Автоматическая загрузка реестра Роскомнадзора

Для автоматической загрузки 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 HTTP(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 прокси-сервера: SOCKS4, SOCKS5 или HTTP(S); если не указан, то используется HTTP;

USER - имя пользователя для неанонимного прокси-сервера;

PASSWORD - пароль для неанонимного прокси-сервера;

URL - IP-адрес или доменное имя прокси-сервера;

PORT - порт прокси-сервера; если не указан, то используется TCP-порт 1080

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

Авторизация по логину

Для включения автоматической загрузки 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 загрузке реестра Роскомнадзора по логину/паролю загрузка производится дельта-пакетами. В этом случае рекомендуется установить значение параметра **update_scheduler 60** (ежеминутная загрузка).

Авторизация по сертификату

Для включения автоматической загрузки 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.

10.7 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 10.3

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

Параметр	Описание
	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 Роскомнадзора (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
```

10.8 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 попадают 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
```

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
            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.

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

10.9 Управление списками

10.10 Команды управления списками

Для удаления списков или файлов, используемых 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**.

```
EcoSGE:> 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 EcoSGE используются команды **show dpirecords** и **dpiview**.

10.10.1 Show dpirecords

Команда выводит 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 10.4

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:

```
EcoSGE:# 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
```

10.10.2 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:

```
EcoSGE:# 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>111111111111</ogrn>
<email>mail@domen.ru</email>
</request>
```

10.10.3 Show dpimatch

Команда позволяет узнать, какие DPI-списки могут срабатывать для того или иного URL или IP-адреса.

Синтаксис команды: **show dpimatch** <URL> | <IP-адрес>[:<номер порта>]

URL может быть с указанием схемы (http:// или https://) или без указания. В последнем случае выводятся результаты проверки вариантов с обеими схемами. Если результаты совпадают, то выводится только один без указания схемы.

IP-адрес может быть IPv4 или IPv6. При указании IPv6-адреса с портом необходимо заключать адрес в квадратные скобки.

Вывод команды представляет собой таблицу, состоящую из трёх столбцов: LIST – номер списка, BEHAVIOUR – значение параметра **behaviour** в настройках данного списка,

WHITELIST – значение параметра **whitelist_mode** в настройках данного списка. Номер списка, который фактически сработал бы, заключается в квадратные скобки.

Примеры вывода команды:

1. Проверка для IPv4

```
EcoSGE:1:> show dpimatch 192.0.2.173
Checked IP : 192.0.2.173
LIST  BEHAVIOUR  WHITELIST
-----
1      ignore     off
2      ignore     on
[10]   block      on
14     ignore     off
-----
[<listnum>] - applied dpilist
```

2. Проверка для IPv6 с указанием номера порта

```
EcoNAT:2:> show dpimatch [2001:db8::ad94]:80
Checked IP : [2001:db8::ad94]:80
LIST  BEHAVIOUR  WHITELIST
-----
7      ignore     off
[16]   block      on
-----
[<listnum>] - applied dpilist
```

3. Проверка для URL с отсутствием результатов

```
EcoNAT:3:> show dpimatch http://www.example.com
Checked URL : http://www.example.com
LIST  BEHAVIOUR  WHITELIST
-----
no match
-----
```

10.10.4 Show dpistate

Команда выводит диагностическую информацию, относящуюся к функциональности URL-фильтрации.

Пример вывода команды:

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

DPI state buffers used/total: 161/16777215 (0.0%)

Строки вывода данной команды описаны в таблице ниже.

Таблица 10.5

Строка	Описание
IPv4 firewall table rules	Текущее/максимальное количество IPv4 записей в ACL
IPv6 firewall table rules	Текущее/максимальное количество единичных IPv6-адресов в ACL
IPv6 firewall range table rules	Текущее/максимальное количество диапазонов IPv6-адресов в ACL
Dump partition	Использование объёма дискового раздела, выделенного под хранение загруженного списка РКН, его дифференциальных обновлений, а также временных файлов, образующихся при его обработке
DPI rules size	Размер памяти, занимаемый структурами URL-фильтрации без ACL/общий (в байтах)
Summary dump size	Суммарный размер загруженного списка РКН и его дифференциальных обновлений (в байтах)
URL base rebuild at	Дата и время последнего перестроения базы данных URL-фильтрации. Формат: YYYY-MM-DDThh:mm:ss+hh:mm:ss
Last parsed dump time	Дата и время, указанные в атрибуте updateTime элемента reg:register последнего загруженного и обработанного XML-файла списка РКН (т. е. дата и время создания файла). Формат: YYYY-MM-DDThh:mm:ss+hh:mm
Actual Date for delta	Дата и время, указанные в атрибуте updateTime элемента reg:register последнего загруженного XML-файла дифференциального обновления (т. е. дата и время создания файла). Формат: YYYY-MM-DDThh:mm:ss+hh:mm
DPI host buffers used/total	Счётчик заполнения буфера информации по доменному имени (текущее/максимальное)
DPI path buffers used/total	Счётчик заполнения буфера информации по URL, идущей после знака '?' (текущее/максимальное)
DPI state buffers used/total	Счётчик заполнения буфера информации по сессии (текущее/максимальное)

Примечание

Разность **+hh:mm** между местным временем и Всемирным координированным временем (UTC) задаётся параметром **timeskew** в ветке **system_log** (см. раздел Настройка времени).

10.11 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 )
```

10.12 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 10.6

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. EcoSGE 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;

Параметр	Описание
	%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_NAME_N>=<SPECN> где URL - адрес страницы, на которую осуществляется перенаправление, VAR_NAME1 .. VAR_NAME_N - имя переменной, SPEC1 .. SPECN - спецификатор. Например, http://example.com/?var1=%u&ip=%i&qwe=%v2. Если при таком значении параметра клиент попытается 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 )
}
```

10.13 Shortlist

10.13.1 Настройка shortlist

В функционале URL-фильтрации возможна настройка логирования на внешний сервер без блокировки соединений. Для логирования используется порт MNG.

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
server_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.

10.13.2 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 ""
  ...
}
```

10.13.3 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 10.7

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"
%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 АМ (до полудня) или РМ (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

Код	Описание
%%	Знак процента

10.14 Фильтрация по базе ЦАИР

В системе EcoSGE реализована возможность URL-фильтрации по базе данных Центра Анализа Интернет-Ресурсов ([ЦАИР](#)). Для подключения базы необходима соответствующая лицензия (CAIR).

Список установленных лицензий выводится командой **show license**.

```
EcoSGE:# show license
CGNAT: Ok
BRAS: Ok
DPI: Ok
URL filter: Ok
RADIUS: Ok
CAIR: Ok
```

При наличии данной лицензии в ветке конфигурации **system.dpi** доступен элемент **cair**, который является модифицированной версией списка DPI со следующими параметрами:

```
EcoSGE: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 interval 86400
```

Где:

base_url – адрес базы ЦАИР;

uplevel_domains_url – адрес базы доменов верхнего уровня (ДВУ);

update_schedule – периодичность автоматического обновления баз в секундах; при значении **never** автоматическое обновление выключено.

Загрузка баз ЦАИР и ДВУ вручную производится командами **dpiload cair** и **dpiload uplevel** соответственно. Рекомендуется регулярно обновлять обе базы (автоматически или вручную).

Информация о сайтах в базах хранится в формате **<md5 hash hostname> <номера категорий сайтов в 16-ричном виде через двоеточие>**. Пример:

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

Базы содержат только домены, то есть, например, "www.example.com", но не "www.example.com/theme/1".

Все домены, содержащиеся в базе 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 к ресурсам "www.example.com", "help.example.com", "123.example.com" и так далее.

Для включения категорий ЦАИР в действие какого-либо списка DPI используется параметр **cair_categories**, в котором категории также указываются в 16-ричном виде через двоеточие. Пример:

```
EcoSGE: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_interval 600
redirect_interval_url 2592000
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 ( )
no_ip_remote ( )
ip ( 0.0.0.0/0 )
no_ipv6 ( )
ipv6 ( )
```

Список категорий и соответствующие им номера представлены в таблице ниже.

Таблица 10.8

Номер 10-ричный	Номер 16-ричный	Категория
1	1	Алкоголь
2	2	Эротика, порнография
3	3	Реклама
4	4	Власти, правительство
5	5	Авто
6	6	Кино, онлайн-видео
7	7	Строительство и ремонт
8	8	Предметы потребления
9	9	Кулинария
10	A	Дача
11	B	Курсы, обучение
12	C	Электроника и электротехника
13	D	Промышленное оборудование
14	E	Семья
15	F	Мода и стиль
16	10	Финансы
17	11	Изобразительное искусство
18	12	Компьютеры, аппаратное обеспечение
19	13	Здоровье
20	14	Хобби
21	15	Юмор
22	16	Интерьер
23	17	Доступ в Интернет Сайты компаний, предоставляющих услуги доступа в Интернет.
24	18	Юридические услуги
25	19	Литература, электронные книги

Номер 10-ричный	Номер 16-ричный	Категория
26	1A	СМИ
27	1B	Машиностроение
28	1C	Металлургия
29	1D	Мобильная связь
30	1E	Музыка
31	1F	Общественные организации
32	20	Компьютерные игры
33	21	Домашние животные
34	22	Фото
35	23	Афиша
36	24	Недвижимость
37	25	Религия
38	26	Школа
39	27	Наука
40	28	Спорт
41	29	Театры
42	2A	Транспорт
43	2B	Туризм
44	2C	Университеты
45	2D	Работа и вакансии
46	2E	Создание сайтов
47	2F	Чаты
48	30	Сайты знакомств
49	31	Войска и вооружение
50	32	Форумы и блоги
51	33	Сервера бесплатной электронной почты
52	34	Бесплатные хостинги
53	35	Нелегальная помощь школьникам и студентам
54	36	Убийства, насилие, трупы
55	37	Онлайн-казино
56	38	Социальные сети
57	39	Терроризм, экстремизм
58	3A	Торговля
59	3B	Нижнее белье, купальники
60	3C	Обеспечение анонимности, обход контентных фильтров
61	3D	Службы обмена сообщениями
62	3E	Файлообменные сети и сайты
63	3F	Табак
64	40	Поисковые системы
65	41	Наркотики
66	42	Злоупотребление свободой в СМИ
68	44	Вредоносные программы
69	45	Ненадлежащая реклама
70	46	Информация с ограниченным доступом
71	47	Банеры и рекламные программы
72	48	Вожделение и автомобили (негатив)
73	49	Досуг и развлечение (негатив)
74	4A	Здоровье и медицина (негатив)
75	4B	Корпоративные сайты
77	4D	Отправка СМС сообщений с помощью Интернет-ресурсов
78	4E	Доски объявлений
79	4F	Неприличный и грубый юмор

Номер 10-ричный	Номер 16-ричный	Категория
81	51	Системы поиска изображений
82	52	Программное обеспечение
83	53	Информационный мусор
84	54	Баннерные сервера
85	55	Белый список
86	56	Безопасные для детей сайты
87	57	Сервисы коротких ссылок
88	58	Спам
89	59	Нарушение авторских прав и смежных прав
90	5A	Единый реестр Роскомнадзор Сайты содержащие информацию, распространение которой в Российской Федерации запрещено (Загрузка списков http://eais.rkn.gov.ru/).
91	5B	Мошенники
92	5C	Федеральный список экстремистских материалов
93	5D	Детское порно
94	5E	Магия, колдовство, оккультизм, теургия
95	5F	Счетчики, аналитика, метрика, статистика
96	60	Женские сайты и журналы
97	61	Мужские сайты и журналы
98	62	Заработок в Интернет Сайты, заявленные для заработка в интернете, торговля бинарными опционами и прочими
100	64	Подделка документов
101	65	Служебные сайты (api, скрипты, js)
102	66	Прочие услуги
103	67	Справочники, каталоги
145	91	Реестр безопасных образовательных сайтов (РБОС). Подробная информация доступна по ссылке

Команда **show cairrecords <URL>** позволяет узнать, к каким категориям ЦАИР относится тот или иной адрес. Пример:

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

10.15 Фильтрация по базе SkyDNS

В системе EcoNAT реализована возможность URL-фильтрации по базе категоризированных ресурсов Загрузка списков. Для подключения базы необходима соответствующая лицензия (Content filter).

Список установленных лицензий вызывается командой **show license**.

```
EcoNAT:3:system.dpi> show license
CGNAT: Ok
BRAS: Ok
DPI: Ok
RADIUS: Ok
DPIv6: Ok
```

Content filter: Ok

После установки данной лицензии в ветке конфигурационного дерева **system dpi** появляется элемент **content_filter** со следующими параметрами:

```
EcoNAT:3:system.dpi.content_filter> ls
database_url "https://url2cat.skydns.ru/pubfilter/grandbase.db"
update_url "https://url2cat.skydns.ru/api/v1/update/"
login ""
password ""
update_schedule
```

Таблица 10.9

Параметр	Описание
database_url	Адрес для загрузки базы SkyDNS
update_url	Адрес для обновления базы
login	Имя учётной записи в системе SkyDNS. Необходимо для загрузки и обновления базы
password	Пароль учётной записи в системе SkyDNS. Необходим для загрузки и обновления базы
update_schedule	Периодичность обновления базы. Допустимые значения: interval <секунды> never (не обновлять)

Для того чтобы задействовать фильтрацию по базе SkyDNS, необходимо выполнить следующие действия:

1. Создать и настроить ACL и пул для трафика, подлежащего обработке (см. раздел "Пулы и ACL").
2. Задать параметры элемента **content_filter** в ветке **system dpi** (см. выше).
3. В элементе **dpilist<N>** задать IP-адреса, подлежащие обработке фильтром (<N> - номер списка DPI).
4. В параметре **content_filter_categories** списка DPI задать категории контента, который необходимо фильтровать. Список категорий вызывается командой **show cf_categories all**. Список категорий для интересующего домена вызывается командой **show cf_records <доменное имя>**. Для вывода названия категории по её ID используйте команду **show cf_categories <ID>**.
5. Задать значение параметра **behaviour** (block, ignore или redirect), чтобы назначить действие с трафиком при срабатывании фильтра.
6. Активировать настроенный **dpilist<N>**.
7. Активировать функциональность DPI.

Пример последовательности команд:

```
create acl a
go acla
10 permit ip any
create pool a
go poola
acl acla
type fake
go dpi content_filter
database_url "https://url2cat.skydns.ru/pubfilter/grandbase.db"
```

```
update_url "https://url2cat.skydns.ru/api/v1/update/"
login "login"
password "password"
update_schedule interval 86400
go dpilist1
enable
content_filter_categories "27:5"
ip (0.0.0.0/0)
behaviour redirect
go dpi
enable
```

10.16 Фильтрация протоколов

Данная функциональность позволяет блокировать трафик определённых протоколов. Для использования данной функциональности необходимо включить функциональность URL-фильтрации, а также включить и настроить **dpilist** (см. раздел «Настройка URL-фильтрации»). Допускается использование любого из 16 списков.

В настройках списка URL-фильтрации блокируемые протоколы указываются в параметре **protocols**. Можно указать один или несколько протоколов (через пробел), а также при необходимости добавлять/удалять отдельные протоколы с помощью операндов "+" и "-".

Блокирование протоколов ограничивается конкретным **dpilist**, в котором они указаны, и параметрами **ip** и **ipv6** этого **dpilist**.

Для любых операций с трафиком необходимо также настроить пулы и ACL (см. раздел «Пулы и ACL»).

Список протоколов вызывается командой **show protocols all** в ветке **system dpi**.

Для быстрого поиска протоколов по названию введите первые буквы названия после **show protocols** и нажмите клавишу **[Tab]**. При наличии нескольких вариантов будет выведен список совпадений. Если вариант один, то после нажатия клавиши **[Tab]** будет выведена аббревиатура протокола. Например:

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

Для вывода описания определённого протокола введите его аббревиатуру после команды **show protocols** и нажмите клавишу **[Enter]**. Например:

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


ПРИЛОЖЕНИЕ А

Справочник команд

Краткое описание команд приведено в таблице ниже.

Обозначения:

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

Режим:

- С – конфигурационный,
- С* – контекстные команды конфигурационного режима,
- О – операционный.

VALUE – вводимое значение параметра.

Таблица 10

Команда	Описание	Режим	Приоритет
()	Очистить редактируемый конфигурационный элемент – массив	С	4
VALUE	Присвоить значение редактируемому конфигурационному элементу	С	4
(VALUE VALUE)	Присвоить значение редактируемому конфигурационному элементу – массиву	С	4
?	Контекстная помощь	О/С	0
helpme %	Вывод на консоль описания параметров и веток дерева, доступных на текущем уровне	О/С	0
!	Вывод на консоль веток, доступных на текущем уровне дерева конфигурации	О/С	0
{	Вход в редактируемый элемент в конфигурационном дереве	О/С	0
}	Выход из редактируемого элемента в конфигурационном дереве	О/С	0
+=(VALUE VALUE)	Добавить несколько значений к редактируемому конфигурационному элементу – массиву	С	4
+= VALUE	Добавить значение к редактируемому конфигурационному элементу – массиву	С	4
-= (VALUE VALUE)	Удалить несколько значений из редактируемого конфигурационного элемента – массива	С	4
-= VALUE	Удалить значение из редактируемого конфигурационного элемента – массива	С	4
#ИМЯ?	Присвоить значение редактируемому конфигурационному элементу или массиву	С	4
add (VALUE VALUE)	Добавить несколько значений к редактируемому конфигурационному элементу – массиву	С	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 cgnat errors	Сброс счётчика ошибок выделения портов в CG-NAT пуле	C	
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 новой даты и времени на устройстве	C	14

Команда	Описание	Режим	Приоритет
edit pool POOLNAME edit POOLNAME	Переход в дереве конфигурации к указанному пулу	O/C	0
edit time TIME	Установка времени на устройстве	C	14
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

Команда	Описание	Режим	Приоритет
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
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

Команда	Описание	Режим	Приоритет
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
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

Команда	Описание	Режим	Приоритет
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 dpistate	Просмотр диагностической информации, касающейся функционала URL-фильтрации по списку Роскомнадзора	O/C	0
show fan	Вывод скорости вентиляторов	O/C	0
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 статистики входящего/исходящего трафика для определённого интерфейса (IFNAME) или всех интерфейсов (all) с момента загрузки устройства или последнего сброса счётчиков. В строке Subtotal указана общая статистика трафика для всех линейных интерфейсов, т. е. не являющихся интерфейсами управления или логирования	O/C	0
show interface IFNAME traffic monitor show interface all traffic monitor	Мониторинг текущей активности определённого интерфейса (IFNAME) или всех интерфейсов (all). Выводится объём входящего/исходящего трафика за последнюю секунду. В строке Subtotal указан суммарный трафик за последнюю секунду для всех линейных интерфейсов, т. е. не являющихся интерфейсами управления или логирования	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 в мегабайтах	O/C	0
show memstat detail	Вывод статистики использования памяти в байтах	O/C	0

Команда	Описание	Режим	Приоритет
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
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

Команда	Описание	Режим	Приоритет
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 ADDRANGE	Вывод статистики трансляций для указанного локального адреса	O/C	0
show xlate local ADDRANGE	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
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

<http://rdp.ru>

Телефон: +7(495)204-9-204

E-Mail: sales@rdp.ru

