RDP
Research & Development Partners

EcoSGE

v3.1.7.0.0

Руководство пользователя

Редакция: сентябрь 2024 г.

Sk IT
Резиденты
ИТ кластера
«Сколково»

EcoSGE v3.1.7.0.0
Руководство пользователя
Редакция: сентябрь 2024 г.

Телефон: +7 (495) 204-9-204
https://www.rdp.ru/

Оглавление

Введение

Настоящий документ содержит описание функциональных возможностей и указания по настройке универсальной сервисной платформы EcoSGE. Данное оборудование является многофункциональным программно-аппаратным комплексом. В настоящем документе описан максимальный набор функциональных возможностей EcoSGE.

Некоторые команды и значения параметров могут отличаться в более поздних или более ранних версиях программного обеспечения. Информацию об актуальной версии программного обеспечения и документации можно найти на сайте компании RDP или запросить в службе технической поддержки.

Указания, сопровождающиеся словами «ВНИМАНИЕ» или «ОСТОРОЖНО», обязательны для выполнения. Невыполнение таких указаний может вызвать нарушение работы оборудования и/или встроенного программного обеспечения.

Условные обозначения

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

Таблица 1 – Стили оформления в документе

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

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

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

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

Таблица 2 – Условные обозначения при описании консоли

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

Список терминов и сокращений

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

Сокращение		Расшифровка
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

Линейка оборудования EcoSGE представлена шестью моделями устройств: 2020, 2040, 4080, 4120 и 4160 (в двух исполнениях).

Ниже рассмотрено соответствие между обозначениями интерфейсов на передней панели устройств и их нумерацией в CLI.

ВНИМАНИЕ! Во избежание повреждения оборудования не рекомендуется устанавливать модули 1 GbE SFP в разъёмы, предназначенные для 10GbE SFP+.

EcoSGE 2020

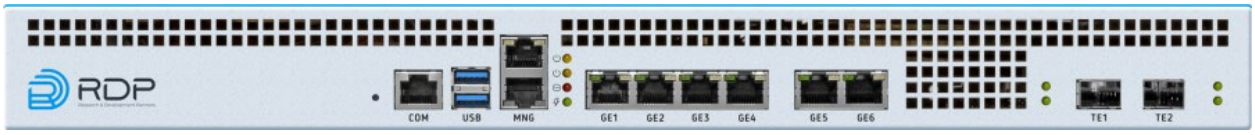

Рисунок 1

Интерфейсы GE1-GE6 (1 GbE RJ-45) в CLI называются **ge1-ge6**. На устройствах 2020 в черном корпусе (старая модель) сетевые интерфейсы для логирования имеют скорость 1GbE и маркировку 5, 6.

Оптические интерфейсы TE1 и TE2 (10 GbE SFP+) в CLI называются **te7** и **te8**.

Интерфейс для логирования (1 GbE RJ-45) находится над интерфейсом MNG и называется в CLI **ge0**.

EcoSGE 2040

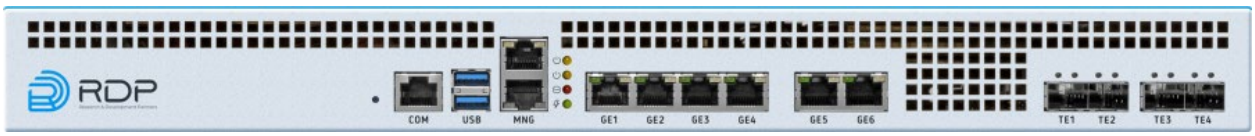

Рисунок 2

Интерфейсы GE1-GE6 (1 GbE RJ-45) в CLI называются **ge1-ge6**.

Оптические интерфейсы TE1-TE4 (10 GbE SFP+) в CLI называются **te7-te10**.

Интерфейс для логирования (1 GbE RJ-45) находится над интерфейсом MNG и называется в CLI **ge0**.

EcoSGE 4080

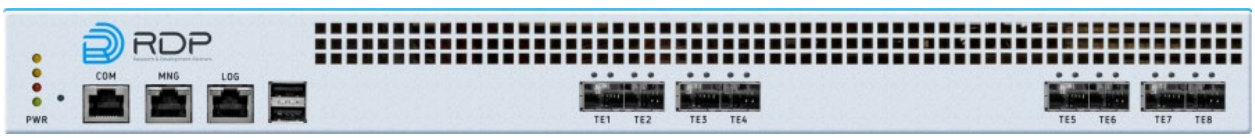

Рисунок 3

Оптические интерфейсы TE1-TE8 (10 GbE SFP+) в CLI называются **te1-te8**.

EcoSGE 4120

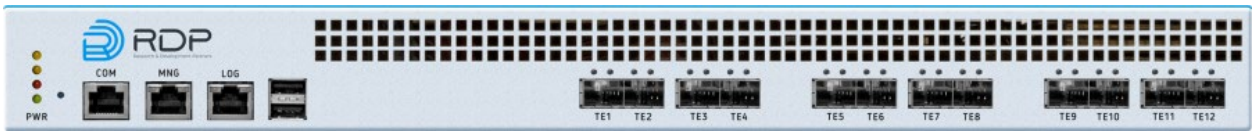

Рисунок 4

Оптические интерфейсы TE1-TE12 (10 GbE SFP+) в CLI называются **te1-te12**.

EcoSGE 4160

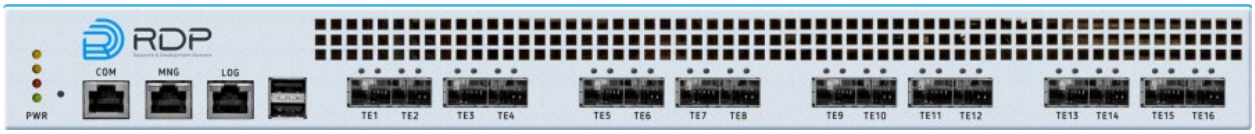

Рисунок 5

Оптические интерфейсы TE1-TE16 (10 GbE SFP+) в CLI называются **te1-te16**.

EcoSGE 4160 (новое исполнение с 2020 года)

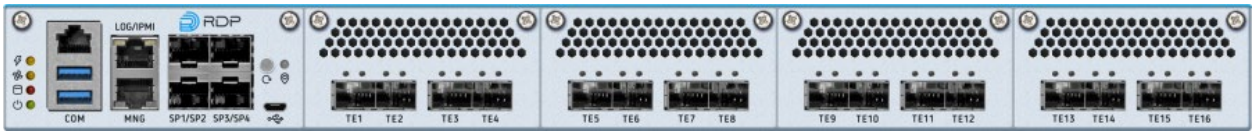

Рисунок 6

Оптические интерфейсы TE1-TE16 (10 GbE SFP+) в CLI называются **te1-te16**. Дополнительные оптические интерфейсы для логирования SP1-SP4 (10 GbE SFP+) в CLI называются **te17-te20**.

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 7

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 интерфейс управления, который находится с левой стороны передней панели устройства и обозначен надписью “MNG” (см. рисунок выше).

Заводские настройки интерфейса управления:

- IPv4-адрес и сетевой префикс 192.168.100.200/24;
- IPv6-адрес и сетевой префикс FD00::192:168:100:200/96
- основной шлюз IPv4 192.168.100.1;

- основной шлюз IPv6 FD00::192:168:0:1;
- серверы DNS 8.8.8.8 и 2001:4860:4860::8888;
- доступ разрешён с любого IPv4/IPv6-адреса.

Заводские настройки сетевой консоли: имя пользователя **admin**, 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"**.

2.3 Режимы консоли

Для консоли управления EcoSGE предусмотрено два режима: операционный и конфигурационный.

После авторизации пользователя консоль доступна в операционном режиме (приглашение командной строки заканчивается символом '>'), в котором можно просматривать настройки, но нельзя изменять конфигурацию. Переключение в конфигурационный режим производится командой **configure**. После выполнения команды действующая (активная) конфигурация будет загружена для редактирования, а символ приглашения командной строки изменится на '#'.

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

Для пользователей с уровнем привилегий 8 и выше допускается только один сеанс консоли в конфигурационном режиме. Если какой-либо пользователь с уровнем привилегий 8 и выше открыл сеанс консоли в конфигурационном режиме, то при попытке другого пользователя с уровнем привилегий 8 и выше переключить консоль в конфигурационный режим ему будет выведено сообщение:

'Another privileged user already edits configuration file. Use 'configure force' command to enter configuration mode.'

(Конфигурацию уже редактирует другой привилегированный пользователь. Для переключения в конфигурационный режим используйте команду 'configure force'.)

Узнать, какой пользователь работает в конфигурационном режиме, можно командой **who**:

```
EcoSGE:> who
Console instance 0:  username 'test', ip 185.42.125.232, rights 8 [configure]
Console instance 1:  username 'support', ip 185.42.125.232, rights 8
```

Если пользователь отправит команду **configure force**, и при этом его уровень привилегий не ниже уровня привилегий того пользователя, который работает в конфигурационном режиме, то сеанс последнего будет принудительно закрыт, и ему будет выведено сообщение:

'Your terminal session was terminated by another privileged user.'

(Ваш сеанс консоли был закрыт другим привилегированным пользователем.)

Если же у отправителя команды **configure force** уровень привилегий ниже, чем у пользователя, который работает в конфигурационном режиме, то в ответ на данную команду будет выведено сообщение:

'ERROR: Insufficient privileges to complete the operation (need 15, yours 8)'

(Ошибка! Недостаточный уровень привилегий для выполнения операции (нужен 15, ваш 8)

Альтернативой команде **configure force** является команда **clear console_instance N**, где N – номер сеанса консоли (Console instance) в выводе команды **who** (см. пример выше).

Для выхода из конфигурационного режима необходимо отправить команду **end**. При нахождении в корне конфигурации можно также использовать команду **exit**. Если при этом редактируемая конфигурация отличается от текущей активной, то будет предложено применить изменения **[a]**, сохранить конфигурацию под новым именем **[s]** или отменить изменения **[d]**. При выборе "сохранить" появится запрос на ввод имени конфигурации.

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

В случае разрыва соединения или аварийного завершения сеанса консоли все несохранённые изменения редактируемой конфигурации будут потеряны.

3 Подсказки и горячие клавиши

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

Таблица 3

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+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 консоли, 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.

4 Работа с общей конфигурацией устройства

В данной главе рассмотрены приёмы работы с общей конфигурацией устройства.

4.1 Дерево конфигурации

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

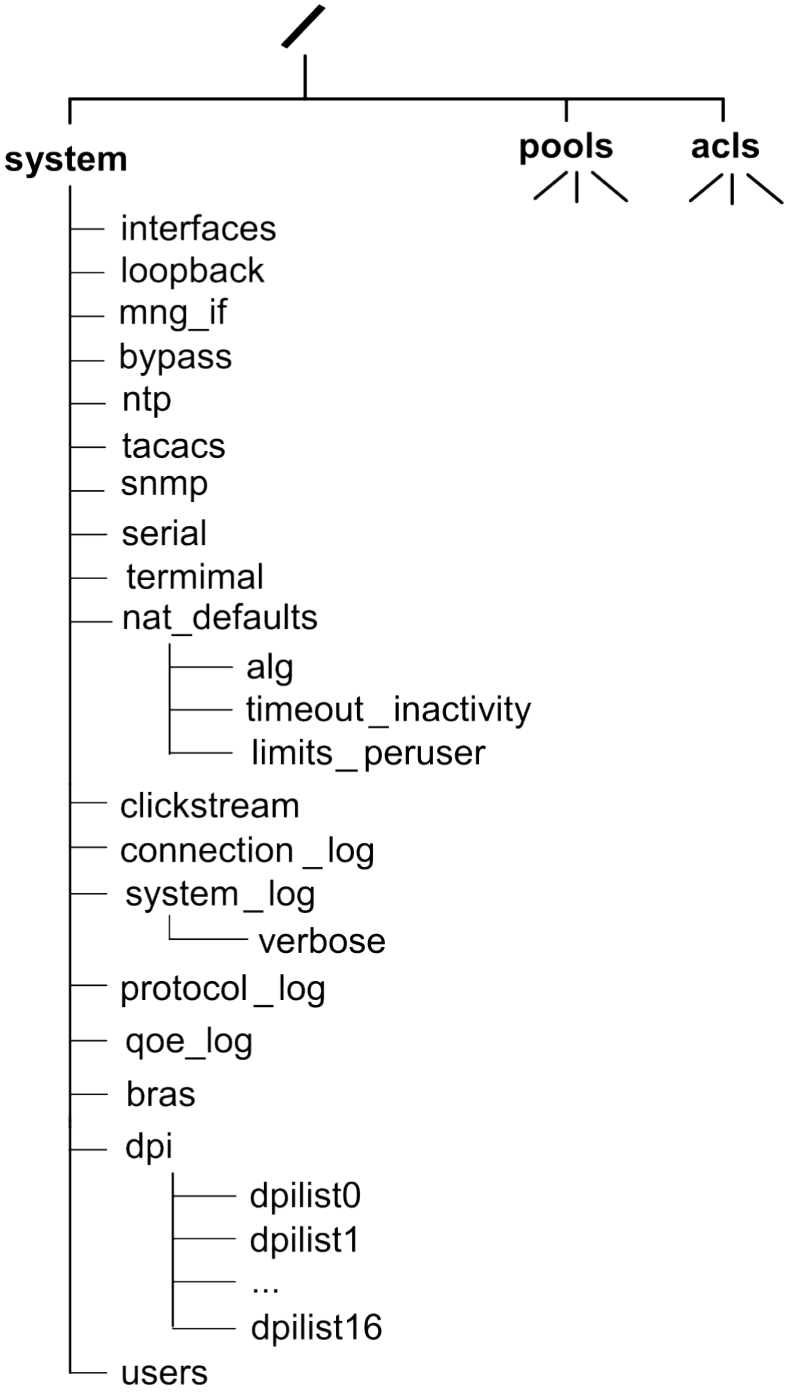

Рисунок 8

Примечание. Дерево конфигурации реального устройства может отличаться от представленного на рисунке. Это зависит от заложенной в устройство функциональности. Описание веток дерева конфигурации приведено в таблице ниже.

Таблица 4

Название ветки	Описание
system	Контейнер для настроек
interfaces	Включение/выключение сетевых интерфейсов
loopback	IP- и MAC-адреса, используемые для генерации ошибок
mng_if	Настройки сетевого интерфейса управления
bypass	Настройки интерфейсов, подключенных к EcoBypass
ntp	Настройки NTP
tacacs	Настройки TACACS
snmp	Настройки SNMP
serial	Настройки последовательного порта
terminal	Настройки терминала
nat_defaults	Параметры подсистемы NAT по умолчанию (общие параметры для всех пулов, в том числе параметры, используемые при создании новых пулов)
connection_log	Настройки логирования абонентских сессий
system_log	Настройки логирования системных событий
clickstream	Настройки логирования подключений к web-серверам
bras	Настройки подсистемы BRAS (Broadband Remote Access Server)
dpi	Настройки подсистемы DPI (Deep Packet Inspection)
users	Информация о пользователях
pools	Контейнер пулов, созданных пользователем
acls	Контейнер ACL (Access Control List), созданных пользователем

Изменение конфигурации возможно только в конфигурационном режиме (см. раздел "Режимы консоли").

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.

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

В системе есть конфигурации с предопределёнными именами:

- **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).

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, и разделяются точкой.

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:

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

Маршрут следования по дереву показан на рисунке ниже.

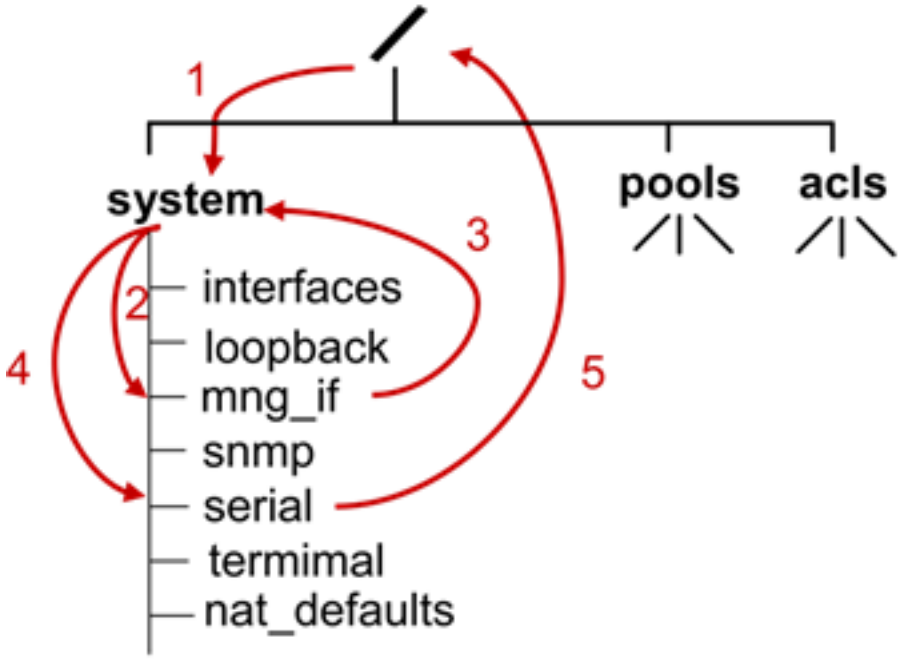

Рисунок 9

Для того чтобы сразу перейти в определённую 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 поддиректорию **system.serial**.

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

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

Для просмотра конфигурации с текущего уровня вглубь используйте команду **ls** или **show**.

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

```
EcoSGE:1:system.dpi> !
enable
functionality_mode normal_nat
dpilist0  {}  # inload namespace (not show)
dpilist1  {}  # inload namespace (not show)
```

4.2 Просмотр конфигураций

Предусмотрены команды для вывода списка сохранённых конфигураций и их просмотра по отдельности (см. таблицу ниже).

Таблица 5

Команда	Действие

dir	Вывод списка сохранённых на устройстве файлов конфигурации. Пример:
	
	`EcoSGE:# dir`
	`config1`
	`config2`
	`lastapply`
	`startup`

show config file <имя конфигурации>	Вывод указанной конфигурации в развёрнутом виде. Пример:
	
	`EcoSGE:# show config file config1`
	`# config1.econat.profile - Econat Profile Script`
	`# saved 06-Sep-2023 16:51:04 UTC, on host EcoSGE`
	`by user 'admin'`
	`root`
	`droppools`
	`dropacls`
	`...`

show config effective	Вывод действующей применённой конфигурации
show config startup	Вывод конфигурации, которая будет применена после перезагрузки

Для файла конфигурации **lastapply** можно запросить хеш-сумму в CLI и по SNMP. Для запроса хеш-суммы в CLI необходимо отправить команду **show config file hash lastapply**.

```
EcoSGE:# show config file hash lastapply
346815ef0d091697e0d0a4554d45148bd1329ac97cbde74958148fb970424ba91253236494
dd41db2765b688348aeb956e9c5e8fc509d689d303796aef188a06
```

Пример запроса хеш-суммы по SNMP:

```
$ snmpwalk -v2c -c public 192.168.5.2 iso.3.6.1.4.1.45555.1.2.886.0
iso.3.6.1.4.1.45555.1.2.886.0 = STRING:
"0057a444e3f5dd3d5b407ac91d1faf962baa20d04880fb02b6821481f053c04ebcf4197c9
4191cf139ae315bd4af61febfd3a136afe3f4221c6ef8a14fb732b4"
```

Примечание. При применении изменённой конфигурации рассчитывается новая хеш-сумма файла **lastapply** с отсчётом от состояния конфигурации в момент поступления команды **apply**.

4.3 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 необходимо отправить команду **save <имя конфигурации>**.

Конфигурацию можно также сохранить на FTP или TFTP-сервере. Для FTP поддерживается базовая аутентификация. Синтаксис команд:

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

save ftp://[<имя_пользователя>:<пароль>@]<IP-адрес>:<порт>/<имя файла>

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

Для применения изменений конфигурации необходимо отправить команду **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 системных журналов различных подсистем (см. раздел Логирование системных событий). 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 DPI (см. раздел Shortlist). Изменение значения данного параметра применяется даже при отключенной ветке **shortlist** (при условии, что родительская ветка **dpi** включена).

4.4 Сохранение конфигурации в качестве стартовой

Для того чтобы сделать текущую эффективную конфигурацию стартовой, необходимо отправить команду **write**. Сделать текущую редактируемую конфигурацию стартовой можно

непосредственно в конфигурационном режиме командой **save startup**, однако так делать не рекомендуется.

Внимание! После выполнения команды **write** при перезагрузке системы будет загружена конфигурация, действовавшая на момент запуска команды **write**, или конфигурация, записанная с помощью команды **save startup**, если она была выполнена позже. Это конфигурация, для которой была выполнена последняя команда **apply**, даже если она была отправлена не в текущей консоли и другим пользователем! Во избежание коллизий рекомендуется, чтобы возможность редактирования конфигурации EcoSGE была у одного человека. Также рекомендуется выходить из конфигурационного режима сразу после изменения конфигурации, чтобы при следующем запуске автоматически войти в последнюю версию конфигурации.

4.5 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://[<имя_пользователя>:<пароль>@]<IP-адрес>:<порт>/<имя файла>

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

4.6 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>

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

```
config3
lastapply
startup
```

- из локального файла в файл на TFTP/FTP-сервере:

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

copy <имя локального файла> ftp://[<имя_пользователя>:<пароль>@]<IP-адрес>:<порт>/<имя файла>

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

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

copy ftp://[<имя_пользователя>:<пароль>@]<IP-адрес>:<порт>/<имя файла> <имя локального файла>

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

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

4.7 Удаление конфигурации

Для удаления конфигурации необходимо отправить команду **erase <имя конфигурации>**. Команда **erase** не применяется к конфигурациям **factory** и **effective**.

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

Также предусмотрена команда **clear config**, которая очищает (обнуляет) редактируемую конфигурацию, не удаляя её. То есть удаляются все созданные пулы, ACL, сбрасываются настройки интерфейсов, удаляются пользователи и т. п.

5 Первичная настройка

В данной главе рассмотрены действия по первичной настройке, которую, как правило, выполняют на месте установки устройства EcoSGE для обнаружения его в сети и обеспечения удалённого доступа.

5.1 Настройка сетевого интерфейса управления

Для управления EcoSGE по сети необходимо правильно настроить сетевой интерфейс управления (MNG). Его параметры хранятся в ветке конфигурации **system.mng_if.System**. Ниже показано содержимое данной ветки в заводской конфигурации устройства и дано описание её параметров.

```
EcoSGE:system.mng_if.System# show
enable
vlan none
ip_address 192.168.100.200/24
gateway 192.168.100.1
allowed_ip ( any )
ipv6_address [FD00::192:168:100:200]/96
gateway_v6 [FD00::192:168:0:1]
allowed_ipv6 ( any )
name_servers (
  8.8.8.8
  [2001:4860:4860::8888]
)
```

Таблица 6

Параметр	Описание
{ enable | disable }	Включение/выключение интерфейса управления
vlan	Номер VLAN от 1 до 4094. По умолчанию **none**, т. е. интерфейс не принадлежит какой-либо VLAN. **Примечание.** Если номер VLAN задан, то он будет указан в выводе команды **show interface brief** в столбце "Interface" (например, **mng.100**). При значении **none** в выводе команды **show interface brief** будет указано **mng** (см. раздел "Просмотр информации об интерфейсах").
ip_address	IPv4-адрес и сетевой префикс интерфейса управления. По умолчанию **192.168.100.200/24**. Значение **none** отключает адресацию по IPv4
gateway	IPv4-адрес основного шлюза. По умолчанию **192.168.100.1**. Значение **none** отключает передачу через основной шлюз IPv4.
allowed_ip ( )	IPv4-адреса, с которых разрешён доступ к интерфейсу управления. По умолчанию **any** (любой IPv4-адрес)
ipv6_address	IPv6-адрес и сетевой префикс интерфейса управления. По умолчанию **[FD00::192:168:100:200]/96**. Значение **none** отключает адресацию по IPv6
gateway_v6	IPv6-адрес основного шлюза. По умолчанию **[FD00::192:168:0:1]**. Значение **none** отключает передачу через основной шлюз IPv6
allowed_ipv6 ( )	IPv6-адреса, с которых разрешён доступ к интерфейсу управления. По умолчанию **any** (любой IPv6-адрес)
name_servers ( )	IPv4/IPv6-адреса DNS-серверов. Опрос серверов производится в порядке указания их адресов. По умолчанию **8.8.8.8** и **[2001:4860:4860::8888]**

Предусмотрена возможность настройки дополнительных логических интерфейсов управления – субинтерфейсов. Такое решение позволяет организовать доступ к устройству из разных сетей и VLAN или, например, обеспечить связь с серверами (SNMP, RADIUS, Syslog и др.), находящимися в разных сетях или VLAN.

Для создания субинтерфейса необходимо отправить команду **create sub_if <имя>**. В ветку конфигурации **system.mng_if** будет добавлен объект **sub_if<имя>**. Пример:

```
EcoSGE:system.mng_if# create sub_if _test
EcoSGE:system.mng_if# show
System
{
  enable
  vlan none
  ip_address 192.168.100.200/24
  gateway 192.168.100.1
  allowed_ip ( any )
  ipv6_address [FD00::192:168:100:200]/96
  gateway_v6 [FD00::192:168:0:1]
  allowed_ipv6 ( any )
  name_servers (
    8.8.8.8
    [2001:4860:4860::8888]
  )
}
sub_if_test
{
  disable
  vlan none
  ip_address none
  gateway none
  allowed_ip ( any )
  ipv6_address none
  gateway_v6 none
  allowed_ipv6 ( any )
  name_servers ( )
}
```

Набор параметров созданного субинтерфейса такой же, как у основного интерфейса управления "System" (см. описание параметров в таблице выше). Отличие в том, что параметрам **ip_address**, **gateway**, **ipv6_address**, **gateway_v6**, **name_servers** не присвоены значения по умолчанию.

Любые изменения в ветке конфигурации **system.mng_if** вступают в силу только после успешного выполнения команды **apply**.

Необходимо отметить следующие особенности реализации субинтерфейсов в системе EcoSGE:

- значения параметров **vlan**, включая **none**, не должны совпадать даже при разных IP-адресах. При попытке применения конфигурации интерфейсов управления с одинаковыми значениями **vlan** поступит сообщение об ошибке;
- выключение основного интерфейса управления "System" приведёт к выключению всех субинтерфейсов.

Для удаления субинтерфейса из конфигурации необходимо отправить команду **no sub_if <имя>**, а затем команду **apply**. Основной интерфейс управления "System" удалить нельзя.

Текущие параметры интерфейса управления можно вывести командой **show ipif**. Команда выводит параметры как основного интерфейса (всегда первая группа параметров), так и всех созданных субинтерфейсов. Пример:

```
EcoSGE:# show ipif
MAC 00:0d:48:28:1a:6e
VLAN: none
IP: 192.168.100.200/24
GW: 192.168.0.1
IP6: fd00::192:168:100:200/96
GW6: fd00::192:168:0:1
VLAN: 1
IP: 5.5.5.2/24
GW: 5.5.5.1
IP6: fd00::192:168:5:2/96
GW6: fd00::192:168:0:1
EcoSGE:system.mng_if#
```

Предусмотрено ещё несколько команд для вывода информации об интерфейсах устройства (см. раздел "Просмотр информации об интерфейсах").

С интерфейса управления могут быть отправлены стандартные команды **ping** и **traceroute**. Для обеих команд предусмотрен как упрощённый, так и расширенный синтаксис:

- упрощённый синтаксис: { ping | traceroute } { <IPv4-адрес> | <IPv6-адрес> | <доменное имя> }
- расширенный синтаксис: { ping | traceroute } { <IPv4-адрес> | <IPv6-адрес> | <доменное имя> } [inet { 4 | 6 }] [source <имя интерфейса>] ; порядок указания опций имеет значение.

Команды с упрощённым синтаксисом всегда выполняются на основном интерфейсе "System". Если узел имеет два адреса, IPv4 и IPv6, то при его опросе командой **ping** по доменному имени сначала используется протокол IPv4. В случае успешного опроса по IPv4 выполнение команды завершается. В противном случае будет произведён опрос по IPv6.

Расширенный синтаксис позволяет явно указать, какой протокол и интерфейс управления использовать для выполнения команды (опции **inet** и **source** соответственно).

Для команды **ping** можно задать домен по умолчанию. Это позволит опрашивать хосты в этом домене, указывая только их имена вместо полного доменного имени.

Домен по умолчанию можно указать в ветке конфигурации **system.domain_lookup**.
Содержимое ветки в заводской конфигурации:

```
EcoSGE:system.domain_lookup# show
domain_lookup
{
  enable
  domain "rdp.ru"
```

```
}
```

Например, для опроса хоста с именем "test" в домене по умолчанию "rdp.ru" (т. е. test.rdp.ru) в команде вместо полного доменного имени достаточно указать имя хоста: **ping test**.

Примеры выполнения команд **ping** и **traceroute**:

```
EcoSGE:# 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
EcoSGE:# 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]**.

5.2 Настройка терминала

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

Таблица 7

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: • 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.

5.3 Установка даты и времени

Настройка системного времени очень важна для правильного функционирования системы EcoSGE. В частности, на системном времени основаны временные метки в log-сообщениях.

В первую очередь необходимо задать часовой пояс. Для этого в ветке **nat_defaults** предусмотрен параметр **timezone**. Данный параметр принимает значения от **utc-12** до **utc+14**. По умолчанию задано значение **utc+3** (при наличии лицензии СОРМ – **utc**). Список всех часовых поясов выводится командой **timezone ?** непосредственно в ветке **nat_defaults**. Текущий часовой пояс можно узнать командой **show timezone**:

```
EcoSGE:# show timezone
Current timezone: utc+3 - Russia [MSK], Belarus, Turkey, Iraq
```

Текущие дату, время и часовой пояс можно узнать командой **show time**.

```
EcoSGE:> show time
Current time is 29-Jun-2020T14:40:09 utc+3
```

Можно задать дату и время вручную или настроить синхронизацию с NTP-сервером.

Вручную дата и время задаются командой **edit datetime <ДД-Месяц-ГГГГТЧЧ:ММ:СС>**. Следует помнить, что в этой команде указываются дата и время UTC, а корректировка с учётом заданного часового пояса отображается в выводе команды **show time**. Пример:

```
EcoSGE:# edit datetime 23-Jul-2020T12:30:00
EcoSGE:# show time
Current time is 23-Jul-2020T15:30:10 utc+3
```

Месяц в команде должен быть указан в виде сокращённого английского названия, а не числом (см. таблицу ниже).

Таблица 8

Январь	**Jan**
Февраль	Feb
Март	Mar
Апрель	Apr
Май	May
Июнь	Jun
Июль	Jul
Август	Aug
Сентябрь	Sep

Январь	Jan
Октябрь	Oct
Ноябрь	Nov
Декабрь	Dec

Синхронизация с NTP-сервером настраивается в ветке конфигурации **system.ntp**:

```
EcoSGE:system.ntp# ls
disable
primary_server "31.131.249.19"
secondary_server "85.21.78.23"
tertiary_server "83.143.51.50"
update_schedule 600
```

В заводской конфигурации уже заданы три NTP-сервера (основной и два резервных) и периодичность синхронизации 600 секунд. Можно указывать как IPv4, так и IPv6-адреса NTP-серверов. Включение и выключение синхронизации по NTP производится непосредственно в ветке **system.ntp** командами **enable** и **disable** соответственно. По умолчанию синхронизация выключена.

Состояние синхронизации с NTP-серверами можно узнать командой **show ntp**.

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

5.4 Учётные записи 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>"**. Имя пользователя может содержать только латинские буквы (регистр учитывается), цифры и знак подчёркивания.

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:

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

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

```
EcoSGE:4:# grant user1 8
```

Для удаления пользователей используется команда **no user <имя пользователя>**.

```
EcoSGE:1:# no user myuser
EcoSGE:2:# system users
EcoSGE:3:system.users# show
users {
user admin level 15 secret 5
5$00$p2c.IaryKF7jSpS1ZKnnmXydvG3AURTTQvJYl52R2s/
}
```

Если пароль пользователя утерян, то его можно изменить. Для этого необходимо подключиться через порт Console или COM к серийной консоли EcoSGE, и при загрузке нажимать клавишу **[i]**. При этом загружается консоль с именем пользователя CHPASS. В данном режиме работы консоли можно изменить пароли пользователей и сохранить настройки.

5.5 Настройка взаимодействия с сервером TACACS+

Настройка взаимодействия с сервером TACACS+ производится в ветке конфигурации **system.tacacs**. Можно настроить подключение к двум TACACS-серверам – основному **server1** и резервному **server2**.

В таблице ниже дано описание параметров взаимодействия с сервером TACACS+.

Таблица 9

Группа параметров	Параметр	Описание
Общие	timeout	Период в секундах для попытки авторизации пользователя через основной сервер. Если в течение заданного периода авторизация через основной сервер не выполнена, то запрос авторизации будет направлен на резервный сервер. **Примечание.** Если до истечения данного периода поступит ICMP-сообщение о недоступности основного сервера (destination host unreachable), то сразу произойдёт переключение на резервный сервер
	fallback { on | off }	Включение/выключение поиска пользователя в локальной базе в случае неудачной попытки авторизации через серверы TACACS+. По умолчанию включён
	accounting { on | off }	Включение/выключение аккаунтинга пользователей, авторизующихся по TACACS+. По умолчанию выключен Если **accounting on** и **auth_cmd on**, то при аккаунтинге будут учитываться только авторизованные команды CLI
	auth_cmd { on | off }	Включение/выключение авторизации через сервер TACACS+ каждой команды, вводимой в CLI EcoSGE. По умолчанию выключена
	service_type <type>	Тип сервиса. Должен совпадать с типом сервиса, указанным в конфигурации сервера. При выключенной авторизации команд CLI (**auth_cmd off**) данному параметру по умолчанию присвоено значение **shell**. При включенной авторизации команд CLI (**auth_cmd on**) данный параметр скрыт в конфигурации EcoSGE, а на сервер TACACS+ всегда передаётся значение **shell**. Однако в конфигурации сервера TACACS+ необходимо для группы задать **service = exec**.
	protocol <proto>	Протокол взаимодействия с сервером TACACS+. Должен совпадать с протоколом, указанным в конфигурации сервера. При включенной авторизации команд CLI (**auth_cmd on**) данный параметр скрыт в конфигурации EcoSGE, а на сервер TACACS+ всегда передаётся значение **exec**
server1 server2	enable | disable	Использовать или нет подключение к серверу TACACS+
	server <IP address>	Адрес сервера TACACS+. Можно указать IPv4-адрес, IPv6-адрес или доменное имя
	secret { text <string> | hash <hex string> }	Пароль для подключения к серверу TACACS+. Можно указать в текстовом или хешированном виде. После указания пароля в текстовом виде производится его хеширование

Пример настроек:

```
EcoSGE:system.tacacs# ls
timeout 5
fallback on
accounting on
```

```
auth_cmd off
service_type "shell"
protocol ""
server1
{
  enable
  server "fb00::2"
  secret
"3f024a93509581e777db9c4701a6a1492f30a38e7349199508467b626d4c1fa5"
}
server2
{
  enable
  server "192.168.7.2"
  secret
"3f024a93509581e780eeb803e93d63f3c194a8eccbfd3b5608467b626d4c1fa5"
}
```

Для просмотра информации о текущей сессии TACACS+ необходимо отправить команду **show tacacs**. Команда выводит информацию о текущей сессии и времени с момента последнего обращения к серверу TACACS+.

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

5.6 Параметры SNMP

Система EcoSGE поддерживает протоколы SNMP v1, v2c и, с ограничениями, v3. Предусмотрена возможность считывания значений переменных MIB (GET-запросы) и отправки Trap-сообщений. SET-запросы не поддерживаются.

Trap-сообщения всегда передаются в формате SNMPv1 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 10

Параметр	Описание
{ enable | disable }	Включение / выключение протокола SNMP. По умолчанию выключен
trap { true | false } или trap { on | off }	Включение (true) или выключение (false) отправки Trap-сообщений. По умолчанию выключена
trap_host	IPv4-адрес или доменное имя сервера, принимающего Trap-сообщения
trap_host6	IPv6-адрес или доменное имя сервера, принимающего Trap-сообщения
trap_port	Номер UDP-порта сервера, принимающего Trap-сообщения. По умолчанию 162
allowed_ip ( )	IPv4-адреса, с которых EcoSGE будет принимать SNMP-запросы. Допустимые значения: • **any**, т. е. любые адреса (по умолчанию);

Параметр	Описание
	• отдельный адрес; • диапазон адресов через дефис; • подсеть. 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
allowed_ipv6 ( )	IPv6-адреса, с которых EcoSGE будет принимать SNMP-запросы. Допустимые значения: • **any**, т. е. любые адреса (по умолчанию); • отдельный адрес, • диапазон адресов через дефис, • подсеть. Можно задать любую комбинацию значений через пробел, а также добавлять и удалять отдельные значения с помощью операторов += и -= соответственно
port	Номер UDP-порта EcoSGE для приёма SNMP-запросов. По умолчанию 161
description	Текстовая строка, которая описывает систему (объект sysDescr группы System в MIB-II, RFC1213). По умолчанию **"EcoSGE"**
hostname	Текстовая строка, которая содержит имя системы (объект sysName группы System в MIB-II, RFC1213). По умолчанию **"EcoSGE"**
contact	Текстовая строка, которая содержит контактную информацию администратора системы (объект sysContact группы System в MIB-II, RFC1213)
hostlocation	Текстовая строка, которая описывает местонахождение системы (объект sysLocation группы System в MIB-II, RFC1213)
viewCommon	Определяет список OID, доступных для просмотра. Формируется с помощью двух вложенных параметров: • **oid_included** – список доступных OID. По умолчанию **all** (доступны все) • **oid_excluded** – список недоступных OID. Действие параметров распространяется не только на указанные OID, но и на все их дочерние OID. Данный список может быть привязан к одному или нескольким профилям доступа (по умолчанию привязан к профилю **communityCommon**). Можно создавать дополнительные списки доступных OID и привязывать их к разным профилям доступа
communityCommon	Встроенный профиль доступа. Содержит следующие параметры: • **security** – строка Community для SNMP-запросов (по умолчанию **public**); • **view** – имя привязанного к профилю списка доступных OID (по умолчанию **viewCommon**); • **authorization** – режим доступа; текущая версия программного обеспечения поддерживает только доступ с правами **read-only** (только чтение). Можно создавать и настраивать дополнительные профили доступа

Пример настройки:

```
EcoSGE:system.snmp# ls
enable
trap true
trap_host "192.168.10.100"
trap_host6 "fd00::1"
trap_port 162
allowed_ip (
  10.10.0.10-10.10.0.20
  10.100.0.0/24
  192.168.10.11
)
allowed_ipv6 ( any )
port 161
description "EcoSGE Test"
hostname "EcoSGE-4120"
contact "admin@company.ru"
hostlocation "Tech Support Dept"
viewCommon
{
  oid_included (
    "all"
  )
  oid_excluded ( )
}
communityCommon
{
  security "public"
  view "viewCommon"
  authorization read-only
}
```

5.6.1 Создание и настройка дополнительных профилей доступа и списков доступных OID

Для создания нового списка доступных OID необходимо отправить команду **create view <name>**. В ветку **system.snmp** будет добавлена секция **view<name>**, в которой необходимо задать параметры **oid_included** и **oid_excluded**. Для удаления какого-либо созданного списка доступных OID необходимо отправить команду **no view view<name>**. Встроенный список **viewCommon** удалить нельзя.

Для того чтобы создать новый профиль доступа, необходимо отправить команду **create community <name>**. В ветку **system.snmp** будет добавлена секция **community<name>**, в которой необходимо задать параметры **security** и **view**. Для удаления какого-либо созданного профиля доступа необходимо отправить команду **no community community<name>**. Встроенный профиль доступа **communityCommon** удалить нельзя.

5.7 Параметры LLDP

Устройство EcoSGE поддерживает протокол LLDP (Link Layer Discovery Protocol) и с периодичностью 60 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). Изменение **lldp_hostname** вступает в силу после перезагрузки устройства.

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

```
EcoSGE:# 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
```

5.8 Настройка подключения к EcoBypass

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

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

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

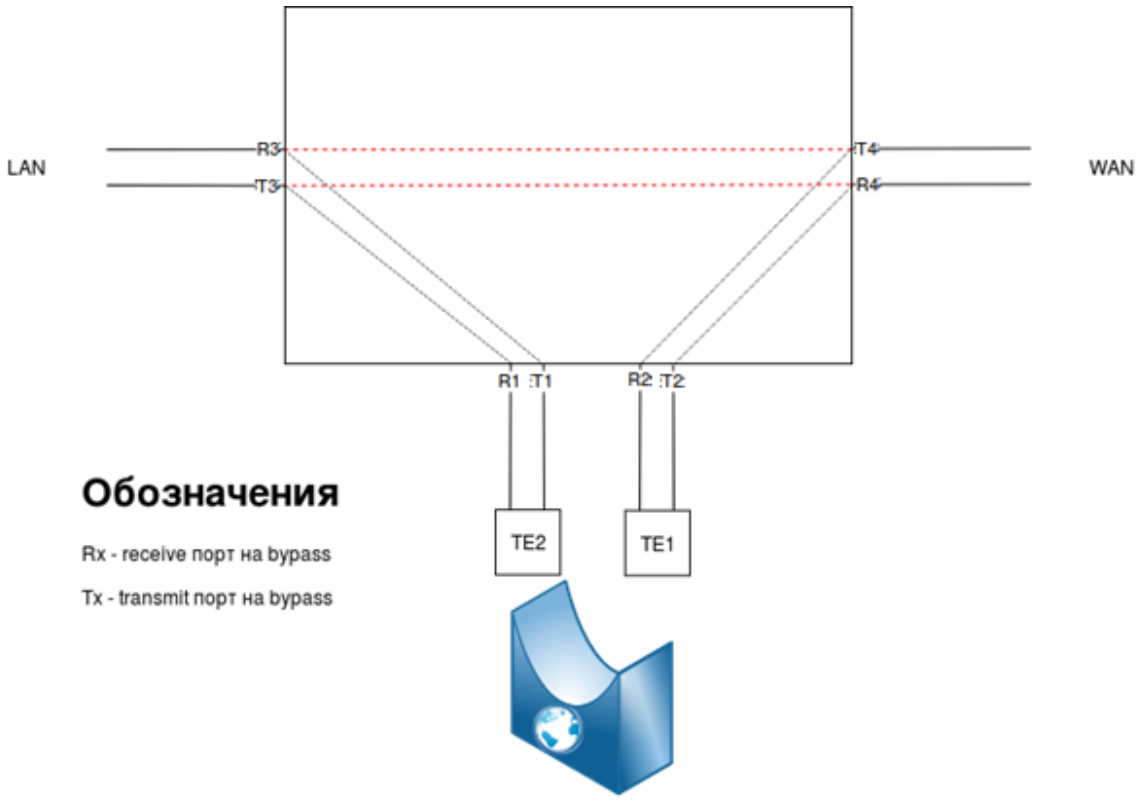

Рисунок 10

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

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

Параметры подключения к EcoBypass задаются в ветке конфигурации **system.bypass**. Настраиваемые в данной ветке параметры представлены в таблице ниже.

Таблица 11

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 EcoSGE 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 значения: • **disabled** - EcoBypass не подключен;

Параметр	Описание
	• 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:

```
EcoSGE: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
EcoSGE:system.bypass>
```

5.9 Параметры loopback

Параметры, хранящиеся в ветке конфигурации **system.loopback**, используются EcoSGE для отправки ICMP-сообщений абонентам. В текущей версии ПО такие сообщения генерируются EcoSGE только в одном случае – если для абонента по какой-либо причине не удалось выделить очередной порт на глобальном адресе. EcoSGE отправит ICMP error type=3 code=13 (Destination unreachable (Communication administratively filtered)). Можно указать отображаемый IP-адрес и MAC. Если IP-адрес для **loopback** не задан, то по умолчанию он будет 100.64.97.116.

```
EcoSGE:system.loopback# show
ip 0.0.0.0
mac 00:00:00:00:00:00
EcoSGE:system.loopback# ip 1.1.1.1
EcoSGE:system.loopback# show
ip 1.1.1.1
mac 00:00:00:00:00:00
EcoSGE:system.loopback#
```

5.10 Информация о версии ПО и установленных лицензиях

При обращении в службу технической поддержки необходимо сообщать следующую информацию об оборудовании:

- тип платформы,
- версия программного обеспечения,
- установленные лицензии.

Тип платформы и версию программного обеспечения можно узнать с помощью команды **show version**:

```
EcoSGE:# show version
EcoNAT 4160L (2020 year) series v3.1 (C) RDP.RU Ltd. 2013-2022. All rights
reserved.
Firmware version: 3.1.5.2.0
S/N: 0C7DC8549F00
```

Команда **show version detail** выводит более подробную информацию о версии ПО:

```
EcoSGE:# show version detail
EcoNAT 4160L (2020 year) series v3.1 (C) RDP.RU Ltd. 2013-2022. All rights
reserved.
Firmware version: 3.1.5.2.0
H1: ea9fbdc
H2: 21418ca
S/N: 0C7DC8549F00
```

Для вывода информации о лицензиях ПО на активном разделе необходимо отправить команду **show license**:

```
EcoSGE:# show license
CGNAT: Ok
BRAS: Ok
DPI: Ok
RADIUS: Ok
CAIR: Not installed
Content filter: Not installed
IPv6: Not installed
ClickStream: Ok
QOE: Ok
ACCOUNTING: Ok
OTT: Not installed
ONSTICK: Not installed
Multivlan: Not installed
```

Для вывода информации о лицензиях ПО на любом интересующем разделе необходимо дополнительно указать имя раздела (регистр символов учитывается):

```
EcoSGE:# show license PRIM2
CGNAT: Ok
BRAS: Ok
DPI: Ok
RADIUS: Ok
CAIR: Not installed
Content filter: Not installed
IPv6: Ok
ClickStream: Ok
QOE: Ok
ACCOUNTING: Ok
OTT: Not installed
ONSTICK: Ok
Multivlan: Ok
```

Имена разделов можно узнать из подсказки к команде **show license ?** или с помощью команды **firmware status** (см. раздел "Действия с прошивкой").

5.11 Перезагрузка и выключение

EcoSGE 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 системы необходимо отправить команду **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 устройства (например, в случае 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.

6 Хранилище сертификатов SSL

Для выполнения различных файловых операций с HTTPS-серверами предусмотрена возможность локального хранения SSL-сертификатов в системе EcoSGE и их администрирования. В частности, сертификат SSL необходим для загрузки хранящегося на HTTPS-сервере списка фильтрации в подсистему DPI.

Команда загрузки сертификата имеет вид **certload <локальное_имя_сертификата> <URL>**. Загрузка возможна по HTTP, FTP и TFTP. Пример команды:

```
EcoSGE:# certload ecosge_cert http://10.20.30.40/certificates/cert1.pem
```

Список загруженных сертификатов можно вывести командой **certlist**:

```
EcoSGE:# certlist
ecosge_cert
my_cert
```

Одного только наличия локальных сертификатов недостаточно для файловых операций с HTTPS-серверами. Требуется указать, какой сертификат использовать при подключении к тому или иному HTTPS-серверу. Для этого предусмотрена ветка конфигурации **system.ca_certs**, где можно задавать привязки сертификатов к IP-адресам или доменным именам HTTPS-серверов. Привязку следует задавать в виде **<IP-адрес или доменное имя сервера> <имя сертификата>**. Пример:

```
EcoSGE:# go ca_certs
EcoSGE:system.ca_certs# 10.11.12.13 ecosge_cert
EcoSGE:system.ca_certs# dpilistserver.ru my_cert
EcoSGE:system.ca_certs# show
"10.11.12.13" "ecosge_cert"
"dpilistserver.ru" "my_cert"
```

Удаление привязки сертификата к серверу производится командой **no <IP-адрес или доменное имя сервера>** непосредственно в ветке **system.ca_certs**.

Для удаления локального сертификата необходимо отправить команду **certerase <имя сертификата>**.

7 Настройки интерфейсов

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 "Оборудование".

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
}
```

Интерфейсы EcoSGE можно включать и отключать, не переходя в ветку настроек интерфейса. Для этого предусмотрены команды **interface <INT_NAME> enable** и **interface <INT_NAME> disable**, где **INT_NAME** – имя одного интерфейса, несколько имён интерфейсов или диапазон через дефис. Например, **interface ge1 ge3 ge6 te2-te4 disable**. После данных команд необходимо отправить команду **apply**, чтобы изменения вступили в силу.

При изменении состояния интерфейса в журнал системных событий добавляются следующие записи:

- информация об административном изменении состояния интерфейса

```
RECONFIG [FATAL] Setting administrative link status UP on port ge2
RECONFIG [FATAL] Setting administrative link status DOWN on port ge2
```

- информация о разрыве/восстановлении соединения

```
MAIN [FATAL] Port ge2 Link Up - speed 1000 Mbps - full-duplex
MAIN [FATAL] Port ge2 Link Down
```

Аналогичная информация передаётся в SNMP Trap:

```
1.3.6.1.4.1.45555 = STRING: "Port ge1 Link Down"
```

```
1.3.6.1.4.1.45555 = STRING: "Port ge2 Link Up - speed 1000 Mbps - full-
duplex"
Link Down Trap (2) Uptime: 0:03:03.93, SNMPv2-SMI::enterprises.45555 =
STRING: "Port ge1 Link Down"
Link Up Trap (3) Uptime: 0:03:03.93, SNMPv2-SMI::enterprises.45555 =
STRING: "Port ge2 Link Up - speed 1000 Mbps - full-duplex"
```

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:

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

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

```
EcoSGE:# show interface brief
Interface    MAC-Address     MTU   Speed   Status  Loading(rx/tx)  Last change    Description
  mng    00:71:00:C0:9E:00  1518  1 Gbps  active    -             -              -
  ge1    00:71:00:C0:9E:01  1522  1 Gbps  active    -       0 days 00:00:10 ago  connect to router
  ge2    00:71:00:C0:9E:02  1522  1 Gbps  active  0/0       0 days 00:00:10 ago  -
  ge3    00:71:00:C0:9E:03  1522  1 Gbps  active  0/0       0 days 00:00:10 ago  -
  ge4    00:71:00:C0:9E:04  1522  1 Gbps  active  0/0       0 days 00:00:10 ago  -
  ge5    00:71:00:C0:9E:05  1522  1 Gbps  active  0/0       0 days 00:00:10 ago  -
```

Отображение в команде **show interface ge1**:

```
EcoSGE:# show interface ge1
Interface name: ge1
Description: connect to router
L2MTU: 1522
Packets droped because of L2MTU: 0
MAC address: 00:71:00:C0:9E:01
Link state: active
Last state change: Tue Sep 1 12:55:36 2020 (0 days 00:03:22 ago)
Link speed: 1 Gbps
Bytes In: 0
Bytes Out: 3060
Packets In: 0
Packets Out: 36
Errors In: 0
Errors Out: 0
Packets Received Imissed: 0
Packets Received Nombuf: 0
```

7.1 Режим On-a-Stick

В режиме On-a-Stick каждый физический Ethernet-порт устройства EcoSGE (кроме MNG и LOG) может одновременно служить в качестве LAN и WAN интерфейса. Разделение трафика на исходящий и входящий в этом режиме производится по одному из двух независимых условий:

- принадлежность VLAN (требуется лицензия Onstick);
- соответствие ACL (требуется лицензия IP_Onstick).

Параметры режима On-a-Stick хранятся в ветке **system.onstick**. Включение и выключение данного режима производится непосредственно в данной ветке командами **enable** и **disable** соответственно. Режим применяется сразу ко всем интерфейсам, кроме MNG. Для активации режима также требуется перезагрузка устройства.

7.1.1 Разделение трафика по принадлежности VLAN

Для разделения трафика на исходящий и входящий на основании его принадлежности VLAN пакеты должны иметь один (802.1Q, Dot1q) или два (802.1ad, QinQ) дополнительных заголовка VLAN. Во втором случае учитывается VLAN ID (VID) внешнего заголовка.

Для того чтобы устройство EcoSGE анализировало содержимое заголовков VLAN, необходимо в ветке **system.nat_defaults** присвоить параметру **vlan_mode** значение **vlan** или **qinq**. В первом случае анализируется один тег, во втором – оба.

Порядок настройки режима On-a-Stick с данным методом разделения трафика:

1. Подготовить список пар Local VID <-> Global VID, по которым трафик будет разделяться на исходящий (egress) и входящий (ingress) соответственно. Список должен учитывать все возможные значения для данного линка. В противном случае пакет будет проигнорирован. При прохождении через EcoSGE происходит замена VID на парный. **Внимание!** Лицензия Onstick позволяет задать только одну пару VID. Возможность задания нескольких пар VID доступна при наличии дополнительной лицензии MultiVLAN. Максимально допустимое количество пар VID – 2048.
2. Для пары VID создать запись в ветке **system.onstick** командой **create vpair <NAME>**. Будет создана запись vpairNAME. Удаление пары VID производится командой **no vpair vpairNAME**.
3. Перейти к созданной записи и задать значения параметров **local** и **global** (VID).
4. Повторить шаги 2 и 3 для остальных пар VID.
5. Включить разделение трафика по VID командой **mode vlan**.
6. Включить режим On-a-Stick командой **enable**.
7. Применить конфигурацию командой **apply**.
8. Сделать конфигурацию стартовой командой **write**.
9. Перезагрузить устройство командой **reboot**.

Пример последовательности команд:

```
system nat_defaults vlan_mode vlan
system onstick
create vpair A
create vpair B
vpairA local 10
global 20
vpairB local 30
global 40
mode vlan
enable
```

```
apply
write
reboot
```

Пример содержимого конфигурации:

```
onstick
{
  enable
  mode vlan
  vpairA
  {
   local 10
   global 20
  }
  vpairB
  {
   local 30
   global 40
  }
}
```

7.1.2 Разделение трафика по соответствию ACL

В данном методе разделения трафика на исходящий и входящий производится сверка IPv4- и IPv6-адресов источников в пакетах с ACL и ACLv6, связанных с режимом On-a-Stick. Пакеты, которые соответствуют ACL и ACLv6, интерпретируются как исходящие (egress), а остальные – как входящие (ingress).

Если трафик имеет заголовки VLAN, то они игнорируются данным методом (но не базовой функциональностью, отвечающей за распределение трафика по пулам NAT).

Настройка режима On-a-Stick с данным методом разделения трафика выполняется в следующем порядке:

1. Создать ACL/ACLv6.
2. Включить разделение трафика по соответствию ACL/ACLv6 (команда **mode ip**).
3. Указать созданные ACL и ACLv6 в ветке конфигурации **system.onstick**.
4. Включить режим On-a-Stick (команда **enable**).
5. Применить конфигурацию (команда **apply**).
6. Сделать конфигурацию стартовой (команда **write**).
7. Перезагрузить устройство (команда **reboot**).

Пример содержимого конфигурации:

```
onstick
{
  enable
  mode ip
  acl aclonstick
  aclv6 aclv6onstick
}
```

ВНИМАНИЕ! Любые изменения настроек режима On-a-Stick будут применены только после перезагрузки устройства. Поэтому после внесения изменений необходимо отправить команды **apply**, **write**, **reboot**.

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

7.2 Агрегирование интерфейсов

Для режима On-a-Stick предусмотрена возможность объединения двух или более физических интерфейсов EcoSGE в один логический интерфейс – Link Aggregation Group (LAG) – с пропорционально большей пропускной способностью. LAG может включать в себя до 16 физических портов Ethernet одного типа. Можно создать до 16 LAG. Для создания и контроля работы LAG используется протокол LACP (IEEE 802.1AX). При работе EcoSGE в обычном режиме, когда в качестве WAN и LAN интерфейсов используются разные физические порты, необходимость в создании LAG отсутствует, так как пакеты протокола LACP проходят через устройство без обработки.

LAG создаётся командой **create lag ID** (где ID – значение от 1 до 65535), после выполнения которой в секцию конфигурации **system.lag_if** добавляется подсекция **lagID**:

```
lag_if
{
  lagID
  {
   disable
   description ""
    min_links 0
   iflist ( )
  }
}
```

В параметре **iflist** необходимо указать интерфейсы, задействованные в LAG (например, **iflist (te1 te2)**). Включение и отключение LAG производится непосредственно в подсекции lagID командами **enable** и **disable** соответственно.

Параметр **min_links** устанавливает минимально допустимое количество исправных каналов через интерфейсы из списка **iflist**, при котором LAG считается работоспособным и находится в состоянии 'Activated'. При меньшем количестве исправных каналов LAG рассматривается как неработоспособный, переводится в состояние 'Deactivated' и перестаёт отправлять LACPDU до тех пор, пока не будет выполнено условие **min_links**. Состояние LAG можно узнать с помощью команды **show lacp { ID | all } local** (см. примеры 1 и 2 ниже).

Настройки протокола LACP, заданные по умолчанию, обеспечивают правильное взаимодействие EcoSGE с сетевыми устройствами основных производителей. При необходимости можно изменить настройки LACP на уровне интерфейса. Для этого в настройках каждого интерфейса предусмотрены параметры **lacp_mode** и **lacp_rate**. По умолчанию настройки интерфейса имеют следующий вид:

```
teN
{
  enable
  description ""
  lacp_mode passive
  lacp_rate fast
}
```

В таблице ниже дано описание параметров LACP в настройках интерфейса.

Таблица 12

Параметр	Описание
lacp_mode	Режим LACP для порта. Возможные значения: • **passive** – устройство EcoSGE не инициирует создание LAG (значение по умолчанию). LAG создаётся при поступлении LACPDU от соседнего устройства и успешном согласовании. • **active** – устройство EcoSGE отправляет LACPDU соседнему устройству и инициирует согласование и создание LAG
lacp_rate	Периодичность отправки LACPDU после создания LAG. Возможные значения: • **slow** – раз в 30 секунд; • **fast** – раз в секунду (значение по умолчанию)

Для просмотра текущего состояния протокола и контролируемого им LAG предусмотрены следующие команды:

- **show lacp { ID | all } counters** – показывает количество отправленных и полученных LACPDU;
- **show lacp { ID | all } local** – показывает состояние портов EcoSGE, объединённых в LAG, флаги и другие параметры, отправляемые в LACPDU соседнему узлу;
- **show lacp { ID | all } remote** – показывает флаги и другие параметры, получаемые от соседнего узла.

Пример 1. Информация о работоспособном lag1 из интерфейсов ge2-ge9 при условии min_links 8.

```
EcoSGE:system.lag_if.lag1# show lacp 1 local
Port
E.|d. - enable: port is configured for LACP | disable
.S|.w - sending LACPDU's | wait LACPDU from neighbor
Flags:
...C .... = Collecting is Enabled    .... ...A = Active
..D. .... = Distributing is Enabled   .... ..F. = Fast Timeout
.F.. .... = Defaulted          .... .G.. = Aggregatable
E... .... = Expired           .... S... = In Sync

Actors's information:
LACP for lag1 is enabled
min_links 8
```

```
state Activated
Iface  Port  Flags   State   Priority Dev ID     Key
ge2    Ew 2  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge3    Ew 3  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge4    Ew 4  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge5    Ew 5  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge6    Ew 6  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge7    Ew 7  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge8    Ew 8  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge9    Ew 9  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
```

Пример 2. Информация о неработоспособном lag1 из интерфейсов ge2-ge9 при условии min_links 8 и неисправном канале на интерфейсе ge2.

```
EcoSGE:system.lag_if.lag1# show lacp 1 local
Port
E.|d. - enable: port is configured for LACP | disable
.S|.w - sending LACPDU's | wait LACPDU from neighbor
Flags:
...C .... = Collecting is Enabled    .... ...A = Active
..D. .... = Distributing is Enabled   .... ..F. = Fast Timeout
.F.. .... = Defaulted          .... .G.. = Aggregatable
E... .... = Expired           .... S... = In Sync

Actors's information:
LACP for lag1 is enabled
min_links 8
state Dectivated
Iface  Port  Flags   State   Priority Dev ID     Key
ge2    Ew 2  EF-- -GF- 0xC6   65535   0cae.68f6.6300 0x0001
ge3    Ew 3  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge4    Ew 4  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge5    Ew 5  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge6    Ew 6  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge7    Ew 7  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge8    Ew 8  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
ge9    Ew 9  --DC SGF- 0x3E   65535   0cae.68f6.6300 0x0001
```

7.3 Просмотр информации об интерфейсах

Предусмотрен ряд команд для вывода информации об интерфейсах EcoSGE и установленных SFP-модулях, а также для мониторинга трафика.

7.3.1 Краткая информация об интерфейсах

Для вывода краткой информации обо всех интерфейсах необходимо отправить команду **show interface brief**. Пример вывода команды:

```
EcoSGE:# show interface brief
 Interface    MAC-Address     MTU     Speed    Status    Loading(rx/tx)
Last change           Description
   mng    00:71:00:C0:9E:00   1518    1 Gbps    active      -      -
-
```

```
  mng.100   00:71:00:C0:9E:00   1518    1 Gbps    active      -      -
-
  mng.200   00:71:00:C0:9E:00   1518    1 Gbps    active      -      -
-
   ge1    00:71:00:C0:9E:01   9216    1 Gbps    active      -      0 days
00:00:10 ago      -
   ge2    00:71:00:C0:9E:02     9216       1 Gbps    active      0/0     0
days 00:00:10 ago      LAG1
   ge3    00:71:00:C0:9E:03     9216       1 Gbps    active      0/0     0
days 00:00:10 ago      LAG1
   ge4    00:71:00:C0:9E:04     9216       1 Gbps    active      0/0     0
days 00:00:10 ago      LAG2
   ge5    00:71:00:C0:9E:05     9216       1 Gbps    active      0/0     0
days 00:00:10 ago      LAG2
```

Описание вывода команды

Таблица 13

Поле	Описание
Interface	Для всех интерфейсов, кроме интерфейса управления, выводятся их системные имена (см. раздел "Настройки интерфейсов"). Для основного интерфейса управления (System) и всех настроенных субинтерфейсов управления выводится обозначение **mng** или **mng.vlan_id**. Подробная информация о настройке основного интерфейса управления и субинтерфейсов содержится в разделе "Настройка сетевого интерфейса управления"
MAC Address	MAC-адрес интерфейса
MTU	Установленное для интерфейса значение MTU. Для всех интерфейсов, кроме MNG, значение MTU можно изменить через параметр **l2mtu** в ветке конфигурации **nat_defaults**
Speed	Согласованная пропускная способность соединения с интерфейсом
Status	Состояние соединения с интерфейсом: • active – соединение установлено • down – соединение не установлено (не подключен или повреждён кабель, неисправен порт, удалённое устройство не отвечает, плохой канал связи и другие подобные причины) • disabled – интерфейс выключен в конфигурации устройства
Loading (rx/tx)	Входящая (rx) и исходящая (tx) нагрузка на интерфейс в процентах от согласованной пропускной способности соединения
Last change	Время, прошедшее с момента последнего изменения состояния интерфейса
Description	Комментарий к интерфейсу

7.3.2 Подробная информация об интерфейсах

Подробная информация об интерфейсах выводится командой **show interface { <имя_интерфейса> | all }**. Вывод команды содержит общую информацию об интерфейсе (имя, MAC-адрес, MTU, состояние и пропускная способность соединения, дата и время последнего изменения состояния соединения) и группу счётчиков "Software Counters" (программные счётчики), которые позволяют проанализировать работу интерфейса. Пример:

```
EcoSGE:> show interface ge1
Interface name: ge1
L2MTU: 1522
```

```
Packets droped because of L2MTU: 0
MAC address: 00:0D:48:28:1A:6D
Link state: active
Last state change: 28-Nov-2022T19:07:26 (0 days 01:49:15 ago)
Link speed: 10 Gbps
SOFTWARE COUNTERS
Last reset time: 28-Nov-2022T19:46:43
Bytes rx: 5730486
Bytes tx: 111945
Packets rx: 93360
Packets tx: 1317
Errors rx: 0
Errors tx: 0
Errors rx int: 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
```

Для сброса программных счётчиков необходимо отправить команду **clear interface { <имя_интерфейса> | all }**. Дата и время последнего сброса счётчиков указаны в поле "Last reset time". Программные счётчики не обнуляются при выключении интерфейсов в конфигурации EcoSGE через CLI.

Для интерфейса MNG вывод команды **show interface mng** незначительно отличается от вывода для других интерфейсов. Кроме того, к интерфейсу MNG не применяется команда **clear interface**.

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

7.3.3 Аппаратные счётчики на интерфейсах

Для считывания и вывода значений аппаратных счётчиков (Hardware Counters) на интерфейсах предусмотрена команда **show interface { <имя_интерфейса> | all } counters**. Пример:

```
EcoSGE:> show interface ge1 counters
Interface name: ge1
HARDWARE COUNTERS
rx_good_packets: 0
tx_good_packets: 0
rx_good_bytes: 0
tx_good_bytes: 0
...
```

К аппаратным счётчикам не применяется команда **clear interface**. Обнуление данных счётчиков происходит при перезагрузке устройства, прерывании электропитания, а также при административном выключении интерфейса (**disable** в ветке **system/interfaces/<имя_интерфейса>** и последующей команде **apply**).

7.3.4 Мониторинг трафика

Для вывода информации о трафике, проходящем через какой-либо интерфейс или все интерфейсы, предусмотрена команда **show interface { <имя_интерфейса> | all } traffic [monitor]**, где **monitor** – опция для вывода с посекундным обновлением. Для выхода из режима **monitor** необходимо нажать **Ctrl+C**. В строке "Subtotal" указана общая статистика трафика для всех интерфейсов, кроме LOG и MNG. Статистика трафика через интерфейс LOG выводится под строкой "Subtotal". Для удобства просмотра используются десятичные приставки "K, M, G, T" в системе СИ.

```
EcoSGE:> 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 to stop.
```

7.3.5 Информация об установленных SFP-модулях

С помощью команды **show interface { <имя_интерфейса> | all } transceiver** или **show sfp all** можно вывести информацию об установленных SFP и SFP+ модулях, включая данные DDM (Digital Diagnostics Monitoring). Для модулей под витую пару данная информация недоступна.

```
EcoSGE:# show interface all transceiver
Interface name: te1
Module Vendor Name: OEM
Module Part Number: SFP+-10G-LR
Module Serial Number: P1309040348
Module Revision: A
Module Manufactoring Date: 130904
Module supports DDM: yes
Module temperature: 39.00 C
Module voltage: 3.25 Volt
```

```
Module TX power: 0.69 mW (-1.60 dBm)
Module RX power: 0.28 mW (-5.50 dBm)
Interface name: te2
Module Vendor Name: OEM
Module Part Number: SFP+-10G-LR
Module Serial Number: P1309040335
Module Revision: A
Module Manufactoring Date: 130904
Module supports DDM: yes
Module temperature: 37.00 C
Module voltage: 3.25 Volt
Module TX power: 0.61 mW (-2.12 dBm)
Module RX power: 0.30 mW (-5.13 dBm)
Interface name: ge3
SFP details are not accessible, code -14
...
```

7.3.6 Информация ARP

Для интерфейсов логирования и управления можно вывести информацию, полученную по протоколу ARP. Для этого предусмотрена команда **show arp { <имя_интерфейса> | mng | all }**. Ниже рассмотрены примеры вывода команд.

Пример 1. Вывод информации ARP для интерфейса LOG.

```
EcoSGE:# show arp ge0
Interface ge0 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) = 00:0D:48:10:7D:2E
    Last ARP reply: 16 seconds ago
```

Вывод команды содержит:

- реальный MAC-адрес интерфейса;
- IP-адрес и MAC-адрес, указываемые в качестве адресов источника логов (EcoNAT EtherChannel); MAC-адрес источника может отличаться от реального MAC-адреса интерфейса – это зависит от настроек логирования;
- IP-адрес и MAC-адрес log-сервера и/или шлюза для log-сервера;
- время, прошедшее с момента получения последнего ARP-ответа.

Пример 2. Вывод информации ARP для всех интерфейсов управления

```
EcoSGE:# show arp mng
Interface System
    Interface MAC              0C:3B:C0:16:11:00
    vlan id 4094
    fd00::3                 4e:72:71:9f:32:8b STALE
```

```
    fe80::4c72:71ff:fe9f:328b        4e:72:71:9f:32:8b STALE
Interface sub_ifclickstream
    Interface MAC              0C:3B:C0:16:11:00
    vlan id 1
    192.168.5.3               56:eb:cf:c4:73:e4 STALE
Interface sub_iflog_server
    Interface MAC              0C:3B:C0:16:11:00
    172.16.1.3                72:d7:41:78:df:e0 STALE
```

Вывод команды содержит:

- MAC-адрес интерфейса;
- номер VLAN (если задан в настройках интерфейса);
- IP-адрес и MAC-адрес соседа.

8 ACL

Access Control List (ACL) представляет собой список правил, которые определяют, какой абонентский трафик должен поступать на обработку в ту или иную подсистему EcoSGE (NAT, BRAS, DPI). Также ACL используется и другими функциями, которые не связаны непосредственно с подсистемами EcoSGE (например, режим интерфейсов On-a-Stick и защита от TCP SYN Flooding).

Можно создавать два типа ACL: для трафика IPv4 или IPv6. Для обработки трафика IPv6 требуется дополнительная лицензия.

8.1 Создание ACL

Для создания ACL необходимо отправить команду **create acl <name>** или **create aclv6 <name>**. Имя ACL может содержать только латинские буквы (регистр учитывается), цифры и знак подчёркивания. В результате выполнения команды в ветке конфигурации **acls** создаётся объект (пустой список) **aclname** или **aclv6name** соответственно. Для перехода к созданному списку необходимо отправить команду **edit acl<name>** или **goto acl<name>** (**edit aclv6<name>** или **goto aclv6<name>**), после чего можно приступить к формированию списка правил.

Общий синтаксис команды для задания правила ACL:

[<num>] <type> <protocol> <src>[~<vid>] [port <src_port>] <dst>[~<vid>] [port <dst_port>]

В квадратных скобках указаны необязательные параметры. Следует указывать только значения параметров (без имени). Исключением является параметр **port**: перед значением, через пробел, должно идти слово "port". Описание всех параметров команды дано в таблице ниже.

Таблица 14

Имя параметра	Описание
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. При задании правил ACL без указания номера система автоматически присваивает номера: • кратные 10, начиная с 10, если ACL изначально пустой; • ближайший больший номер, кратный 10, если ACL уже содержит одно или несколько правил. 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 194.85.16.0/24~10-50 dst any** и требуется исключить из обработки пулом, к которому привязан ACL, весь трафик VLAN 20 данной подсети, то следует задать запрещающее правило вида **9 deny ip src 194.85.16.0/24~20 dst any**, т. е. с номером меньше 10.
type	Тип правила: разрешающее (**allow** или **permit**) или запрещающее (**deny**).

Имя параметра	Описание
	Пакеты, соответствующие разрешающему правилу, будут обрабатываться подсистемой или функцией, в настройках которой указан данный ACL (например, пул или DPI-список). Пакеты, соответствующие запрещающему правилу, исключаются из обработки на текущем уровне подсистемы или функции, в настройках которой указан данный ACL, и передаются на анализ на следующий уровень (например, в другой пул или DPI-список).
protocol	Протокол передачи данных. Допустимые значения: • **ip** – весь стек TCP/IP • **tcp** • **udp** • **icmp** Если не указать значение параметра **protocol**, то ему будет присвоено значение **ip**.
src	IP-адрес отправителя. Допустимые значения (с примерами): • любой адрес: **any** или **0.0.0.0/0** для IPv4, **any** или **::/0** для IPv6; • один адрес (10.10.0.100); • диапазон адресов (10.10.0.100-10.10.0.150); • адрес сети/подсети (10.10.10.0/24). Адреса IPv6 можно указывать в полной или сокращённой форме, но в списке правил они всегда отображаются в сокращённой форме. Если не указать значение параметра **src**, то ему будет присвоено значение **any**. При этом в команде обязательно должно быть указано значение параметра **dst** (см. пример 1 ниже).
vid	Идентификатор VLAN (от 0 до 4094). 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 в явном виде, т. е. 0.0.0.0/0 или ::/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.
src_port и **dst_port**	Номера портов отправителя и получателя. Только для протоколов TCP и UDP. Можно задать одно значение или диапазон через дефис.
dst	IP-адрес получателя. Допустимые значения (с примерами): • любой адрес: **any** или **0.0.0.0/0** для IPv4, **any** или **::/0** для IPv6; • один адрес (11.12.13.100) • диапазон адресов (11.12.13.100-11.12.13.150) • адрес сети/подсети (11.12.13.0/24) Адреса IPv6 можно указывать в полной или сокращённой форме, но в списке правил они всегда отображаются в сокращённой форме. Если не указать значение параметра **dst**, то ему будет присвоено значение **any** (см. пример 3 ниже).

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
}
```

8.2 Действия с ACL

8.2.1 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:#
```

8.2.2 Отвязывание ACL от пула

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

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

8.2.3 Удаление правил в ACL

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

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

8.2.4 Удаление ACL

Чтобы удалить ACL, воспользуйтесь командой **no acl <имя ACL>.**

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

8.2.5 Удаление всех ACL

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

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

9 Карты классов трафика

Карты классов трафика предназначены для классификации трафика по значению поля DSCP (первые 6 бит октета ToS) в заголовке IP-пакетов. Они могут использоваться как дополнительное условие применения сервисов BRAS к исходящему и входящему трафику (см. раздел "Создание и настройка сервиса"). Таким образом, применение сервиса к трафику может зависеть не только от IP-адреса (проверка по ACL), но и от значения поля DSCP в заголовке IP-пакетов (проверка по картам классов). Карты классов трафика хранятся в ветке конфигурации **classmaps**.

Конфигурирование карты классов состоит из двух этапов:

1. Создание пустой карты классов командой **create classmap <name>**. Имя может содержать только символы A-Z, a-z, 0-9 и _.
2. Задание требуемых значений DSCP командой **goto classmap<name> dscp (<список dscp>)**. Значения DSCP задаются в виде шестизначных двоичных чисел (например, 011001). Всего возможно 64 значения DSCP – от 000000 до 111111. Несколько значений в команде указываются через пробел. Порядок указания не важен, так как учитываются все значения.

Для добавления и удаления отдельных значений DSCP можно использовать операторы += и -=.

Пустую карту классов нельзя указать в настройках сервиса BRAS. Указание карты классов, состоящей из всех 64 возможных значений DSCP, равнозначно отсутствию в сервисе карт классов (т. е. DSCP в этом случае не проверяется).

Удаление карты классов из конфигурации производится командой **no classmap<name>**.

По завершении конфигурирования необходимо применить изменения командой **apply**.

10 Подсистема NAT

В этой главе описаны настройки, принцип работы и типовые сценарии применения подсистемы NAT.

10.1 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 "Создание и настройка пула").

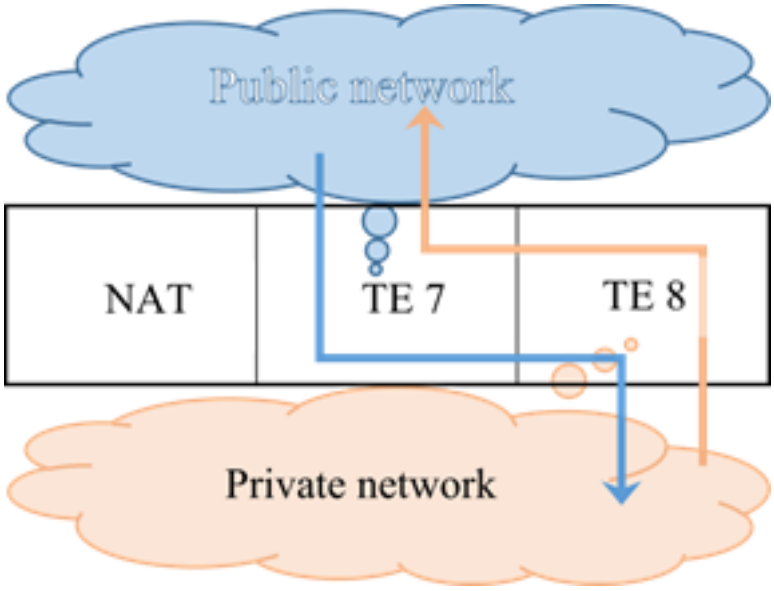

Рисунок 11

EcoNAT поддерживает следующие типы трансляции IPv4 адресов: CG-NAT/PAT, Basic NAT, статическую трансляцию 1:1.

BNAT

BNAT (Basic NAT) – классический NAT режим, при котором абоненту на время работы выделяется публичный IPv4 адрес, и транслируются только адреса (порты остаются неизменными). У этого режима есть два варианта: прозрачный, разрешающий входящие внешние соединения на любые порты, и закрытый, допускающий соединения извне лишь на порты, открытые сессиями изнутри.

1:1

В статическом режиме (он ещё именуется трансляцией 1:1) за каждым абонентским IP адресом закреплен публичный IP адрес. Посредством данного метода оператор связи может оперативно выдавать абонентам статические публичные IP без изменения настроек CPE абонента.

CG-NAT / PAT (Port Address Translation) – основный режим работы EcoNAT, допускающий использование публичного IPv4 адреса одновременно несколькими абонентами. В этом режиме транслируется не только адреса, но и порты. Количество портов TCP и UDP, одновременно используемых абонентом, можно ограничивать.

Для всех режимов работы EcoNAT поддерживаются следующие технологии:

EIM/EIF (Endpoint Independent Mapping / Endpoint Independent Filtering)

EIM/EIF (ранее такой режим работы CG-NAT назывался Full Cone NAT) позволяет любым внешним хостам устанавливать соединения с абонентом извне по тем TCP/UDP портам, для которых трансляция была ранее инициирована самим абонентом. Поддержка EIM/EIF в EcoNAT обеспечивает максимально прозрачную работу всех протоколов и приложений, в том числе мобильных, P2P, торрентов, голосовых и видео сообщений, игр и др. EIM/EIF позволяет работать приложениями, которые используют механизмы STUN (Session Traversal Utilities for NAT).

IP pairing

С целью обеспечения наилучшей прозрачности EcoNAT все соединения абонента, относящиеся к одному пулу, привязаны к одному и тому же публичному IP адресу.

Hairpinning

Hairpinning позволяет абонентам внутри NAT взаимодействовать друг с другом через NAT, не посылая пакеты вовне.

10.2 Пулы

Основным элементом конфигурации подсистемы NAT являются так называемые пулы (pool), которые характеризуются типами трансляции и набором внешних (глобальных) IPv4-адресов. Каждому пулу присваивается приоритет. Чем меньше числовое значение приоритета, тем раньше данный пул обрабатывается. Можно присвоить одинаковый приоритет нескольким пулам, но в этом случае только один из них может быть задействован. С каждым пулом связан ACL, который содержит в себе критерии выбора данного пула в зависимости от содержимого полей поступившего IP-пакета.

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

10.2.1 Общие настройки

Ветка конфигурации **system.nat_defaults** содержит общие настройки системы и настройки, применяемые по умолчанию ко всем создаваемым пулам (блоки timeouts_inactivity и limits_peruser копируются в пул при его создании). В таблице ниже дано описание параметров данной ветки конфигурации.

Таблица 15

Параметр	Описание
vlan_mode	Обработка и анализ пакетов до указанного уровня инкапсуляции. Возможные значения: **untagged**, **vlan**, **qinq**
inner_vlan outer_vlan	Значение поля TPID внутреннего тега 802.1Q (C-VLAN). По умолчанию 0x8100. Значение поля TPID внешнего тега 802.1Q (S-VLAN). По умолчанию 0x8100. Данные параметры доступны в конфигурации устройств EcoSGE с сетевыми контроллерами Intel серий 710/810 и необходимы для правильной обработки трафика QinQ
alg dns	Опция ALG для DNS запросов и ответов при трансляциях из IPv4 в IPv4 (NAT44). Возможные значения: on, off. **Примечание.** Если опция включена, то при получении ответа DNS-сервера таймер неактивности соответствующей исходящей UDP-сессии (timeouts_inactivity udp_session) сразу устанавливается в 0, и сессия помечается как подлежащая немедленному удалению (статус "To be deleted right now")
alg dns64	Опция ALG для DNS запросов и ответов при трансляциях из IPv6 в IPv4 (NAT64). Возможные значения: on, off. При включенной опции: • запрос типа AAAA будет преобразован в тип A; • ответ типа A будет преобразован в тип AAAA; • запросы типа A и ответы типа AAAA не преобразовываются
alg ftp	Опция ALG для протокола FTP при трансляциях из IPv4 в IPv4 (NAT44). Возможные значения: on, off
alg ftp64	Опция ALG для протокола FTP при трансляциях из IPv6 в IPv4 (NAT64). Возможные значения: on, off
alg pptp	Опция ALG для протокола PPTP. Возможные значения: on, off
alg rtsp	Опция ALG для протокола RTSP. Возможные значения: on, off
alg sip	Опция ALG для протокола SIP при трансляциях из IPv4 в IPv4 (NAT44). Возможные значения: on, off
alg sip64	Опция ALG для протокола SIP при трансляциях из IPv6 в IPv4 (NAT64). Возможные значения: on, off
alg alg_on_bnat	Опция ALG для трансляций из IPv4 в IPv4 (NAT44) в пулах **nat** и **static**. Возможные значения: on, off
alg alg64_on_bnat	Опция ALG для трансляций из IPv6 в IPv4 (NAT64) в пулах **static64**. Возможные значения: on, off
sessions_per_translation	Количество активных сессий на трансляцию
udp_inbound_refresh	Включает обновление UDP-трансляций входящими (ingress) пакетами. Возможные значения: on, off
forward_traffic	Включить (**on**) / отключить (**off**) пересылку пакетов через платформу EcoSGE. Значение по умолчанию: **on**. Отключение пересылки пакетов может потребоваться, когда, например, платформа EcoSGE используется только для анализа и логирования зеркалированного трафика
l2mtu	Максимальный размер (в байтах) кадра Ethernet на входе, включая заголовки и исключая поле контрольной суммы. Диапазон допустимых значений – от 576 до 9692. По умолчанию 9216

Параметр	Описание
port_block_size	Размер блока портов для пулов CGNAT и CGNAT64. Не рекомендуется изменять значение данного параметра. По умолчанию 128. Допустимые значения в стандартной конфигурации: 64, 128, 256, 512. По запросу заказчика набор допустимых значений может быть расширен: 8, 16, 32, 64, 128, 256, 512. Для применения нового значения необходимо перезагрузить устройство
portlimit_low	Значение используемого диапазона "нижних" портов (до 1024) для каждого пользователя. Варианты значений параметра: nolimit, 64, 128, 256, 512
low_to_all_udp	Позволяет использовать порты из верхнего диапазона, если порты из нижнего диапазона исчерпаны. Варианты значений параметра: on/off
lldp	Включение (on) / выключение (off) протокола LLDP. По умолчанию **on**
lldp_hostname	Имя хоста, которое будет передаваться в LLDP-сообщениях. По умолчанию **"ecosge"**
permit_invalid_flow	Включить (on) / отключить (off) 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**
pppoe_analyzer	Включить (**on**) / выключить (**off**) обработку трафика PPPoE. По умолчанию **off**
timeouts_inactivity {}	В этом разделе задаются тайм-ауты неактивности (в секундах) для разных протоколов и состояний TCP. По истечении тайм-аута неиспользуемая трансляция/сессия принудительно закрывается
timeouts_inactivity translation	Время в секундах, до истечения которого абоненту, даже в случае его неактивности, будет гарантировано выделение портов на одном и том же глобальном IP-адресе. Рекомендованное значение по умолчанию 86400
timeouts_inactivity udp	Тайм-аут неактивности в секундах для UDP-соединений. По истечении заданного времени порт на глобальном IP-адресе освобождается. По умолчанию 300
timeouts_inactivity icmp	Тайм-аут неактивности в секундах для ICMP-соединений. По истечении заданного времени порт на глобальном IP-адресе освобождается. По умолчанию 60
timeouts_inactivity tcp_handshake	Тайм-аут неактивности в секундах, устанавливаемый для TCP-соединений при получении пакета с флагом SYN или SYN-ACK. По умолчанию 4
timeouts_inactivity tcp_active	Тайм-аут неактивности в секундах, устанавливаемый для TCP-соединений при получении пакета с флагом ACK. По истечении заданного времени порт на глобальном IP-адресе освобождается. 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	Тайм-аут неактивности в секундах для активных UDP-сессий. По умолчанию

Параметр	Описание
udp_session	120
timeouts_inactivity icmp_session	Тайм-аут неактивности в секундах для активных ICMP-сессий. По умолчанию 120
timeouts_inactivity other	Тайм-аут неактивности в секундах для прочих соединений по протоколу IP (например, для GRE). По истечении заданного времени протокол на глобальном IP-адресе освобождается. По умолчанию 300. Применимо только к пулам NAT и Static
timeouts_inactivity special	Тайм-аут неактивности в секундах для протоколов, которым требуется большее значение тайм-аута. По умолчанию 600
timeouts_inactivity special_tcp_ports ( )	TCP-порты, к которым применяется увеличенное значение тайм-аута
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
timezone	Часовой пояс. Принимает значения от **utc-12** до **utc+14**. По умолчанию задано значение **utc+3** (при наличии лицензии COPM – **utc**). Список всех часовых поясов выводится командой **timezone ?** непосредственно в ветке **nat_defaults**

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 натирования.

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

10.2.2 Создание и настройка пула

Для создания пула необходимо отправить команду **create pool <имя>**. Имя пула может содержать только латинские буквы (регистр учитывается), цифры и знак подчёркивания. Будет создан CGNAT-пул с типовыми параметрами (см. описание в разделе "Пул CGNAT") и именем **poolИМЯ** (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 "Работа с общей конфигурацией устройства"). Пример:

```
EcoSGE:# create pool test
EcoSGE:# goto pooltest
EcoSGE:pools.pooltest# show
type cgnat
 enable
 nat_filtering_mode endpoint_independent
 acl none
 priority 100
 global_ip ( )
 port_range 1024-65535
 hairpin on
 connection_logging on
 connection_log none
 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.

В таблице ниже дано описание параметров пула.

Таблица 16

Параметр	Описание
type	Тип пула: cgnat, cgnat64, static, static64, nat, fake, fake6, port_fwd. Настройка пула port_fwd описана в разделе "Пул port_fwd"
enable | disable	Включение / выключение пула
nat_filtering_mode	Режим фильтрации входящего трафика для пула CGNAT: • **endpoint_independent** – пропускать весь входящий трафик, поступающий на глобальный адрес существующей трансляции, независимо от того, с какого внешнего адреса/порта этот трафик отправлен (режим по умолчанию); • **address_dependent** – пропускать только тот входящий трафик, который поступает на глобальный адрес существующей трансляции с того же внешнего адреса, для которого была открыта исходящая сессия. При этом внешний порт может меняться. Для каждого нового внешнего порта создаётся новая входящая сессия; • **address_and_port_dependent** – пропускать только тот входящий трафик, который поступает на глобальный адрес существующей трансляции с того же внешнего адреса и порта, для которого была открыта исходящая сессия.
acl	Связанный с пулом ACL для абонентского трафика IPv4. Параметр присутствует в настройках пулов cgnat, nat, static, fake
aclv6	Связанный с пулом ACL для абонентского трафика IPv6. Параметр присутствует в настройках пулов cgnat64, static64, fake6
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
global_map ( )	Присутствует в настройках пула Static. Задаёт соответствие между локальными и глобальными IPv4-адресами и/или подсетями (правила трансляции). Правила трансляции задаются в формате **{ <локальный адрес> | <подсеть> }[~vid]-{ <глобальный адрес> | <подсеть> }**. VID – идентификатор VLAN от 0 до 4094 (необязательный параметр). Значение VID задаётся с префиксом "~" (тильда) без пробела после адреса. **Внимание!** Параметр задаёт строгое соответствие локального адреса **и** локального VLAN определённому глобальному адресу. Если VID не указан, то это подразумевает, что трафик будет нетегированным. Трансляция локальной подсети в глобальную возможна только при одинаковой длине префикса подсетей. Например, global_map (10.10.10.0/**24**-101.102.103.0/**24**)
global_map_64 ( )	Присутствует в настройках пула Static64. Задаёт соответствие между локальными IPv6-адресами и глобальными IPv4-адресами (правила

Параметр	Описание
	трансляции). Можно указать несколько правил трансляции через пробел. Например, global_map_64 ([2001:DB8::1]-192.0.2.1 [2001:DB8::2]-198.51.100.2)
v6_remote_prefix ( )	IPv6-префикс для NAT64. Параметр присутствует в настройках пулов CGNAT64 и Static64. В RFC 6052 определён так называемый "хорошо известный" префикс (Well-Known Prefix, WKP) 64:FF9B::/96, рекомендуемый к использованию в типовых случаях. В общем случае можно использовать любой префикс, но при одном условии: он должен иметь длину /96
tos2tc_mapping	Присутствует в настройках пулов CGNAT64 и Static64. Определяет действия с полями Type of Service (ToS) и Traffic Class (TC) в заголовках пакетов при трансляциях IPv6 → IPv4 и IPv4 → IPv6. По умолчанию задано значение **on**. При трансляциях IPv6 → IPv4 в поле ToS создаваемого IPv4-заголовка копируется значение поля TC из заголовка IPv6. При трансляциях IPv4 → IPv6 в поле TC создаваемого IPv6-заголовка копируется значение поля ToS из заголовка IPv4. Если инфраструктура IPv4 использует устаревшую семантику "Type of Service and Precedence", то копирование значений полей ToS и TC можно выключить, присвоив данному параметру значение **off**. В этом случае при трансляциях IPv6 → IPv4 значение поля ToS создаваемого IPv4-заголовка всегда будет равно нулю (поле TC заголовка IPv6 игнорируется). При трансляциях IPv4 → IPv6 значение поля TC создаваемого IPv6-заголовка всегда будет равно нулю (поле ToS заголовка IPv4 игнорируется).
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
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 сессий: включено (on) или выключено (off)
connection_log	Имя раздела настроек логирования сессий (см. раздел "Логирование абонентских сессий"). По умолчанию **none**, т. е. настройки логирования не привязаны к пулу
randomize_ports	Разрешает выделение портов из блока в случайном порядке (on). Если выключено (off), то порты выделяются поочередно
timeouts_inactivity	В этом разделе задаются параметры времени неактивности (в секундах) для разных протоколов и состояний TCP, по истечении которого неиспользуемое соединение будет закрыто принудительно. Эти параметры не рекомендуется настраивать без необходимости, можно использовать оптимальные значения «по умолчанию»
timeouts_inactivity translation	Задаёт время в секундах до истечения которого, даже в случае неактивности пользователя, ему будет гарантировано выделение портов из одного и того же глобального IP. Рекомендованное значение по умолчанию 86400
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	Таймаут для завершения TCP сессий в секундах. По умолчанию 240

Параметр	Описание
tcp_final	
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 17

Параметры	cgnat	nat	static	fake	fake6
type	+	+	+	+	+
enable	+	+	+	+	+
acl	+	+	+	+	
aclv6					+
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:#
```

10.2.3 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).

10.2.4 Пул Basic NAT

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 "Создание и настройка пула".

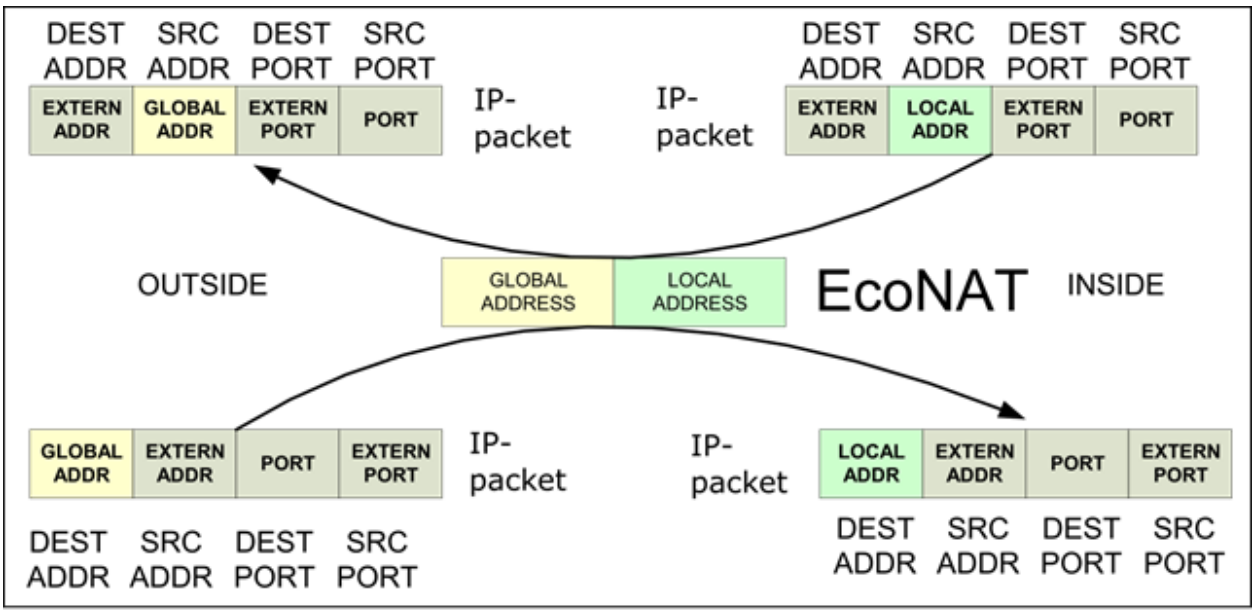

Рисунок 12

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

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

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

```
MyEcoNAT:1:# create pool b
MyEcoNAT:2:# goto poolb
MyEcoNAT:3:pools.poolb# type nat
MyEcoNAT:4:pools.poolb# show
type nat
enable
acl none
priority 200
global_ip ( )
hairpin on
allow_external_connect on
connection_logging on
randomize_ports off
timeouts_inactivity
{
 translation 86400
 udp 300
 icmp 60
 tcp_handshake 4
```

```
 tcp_active 300
 tcp_final 240
 tcp_reset 4
 other 300
 special 600
 special_tcp_ports ( )
}
MyEcoNAT:5:pools.poolb#
```

10.2.5 Пул CGNAT

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

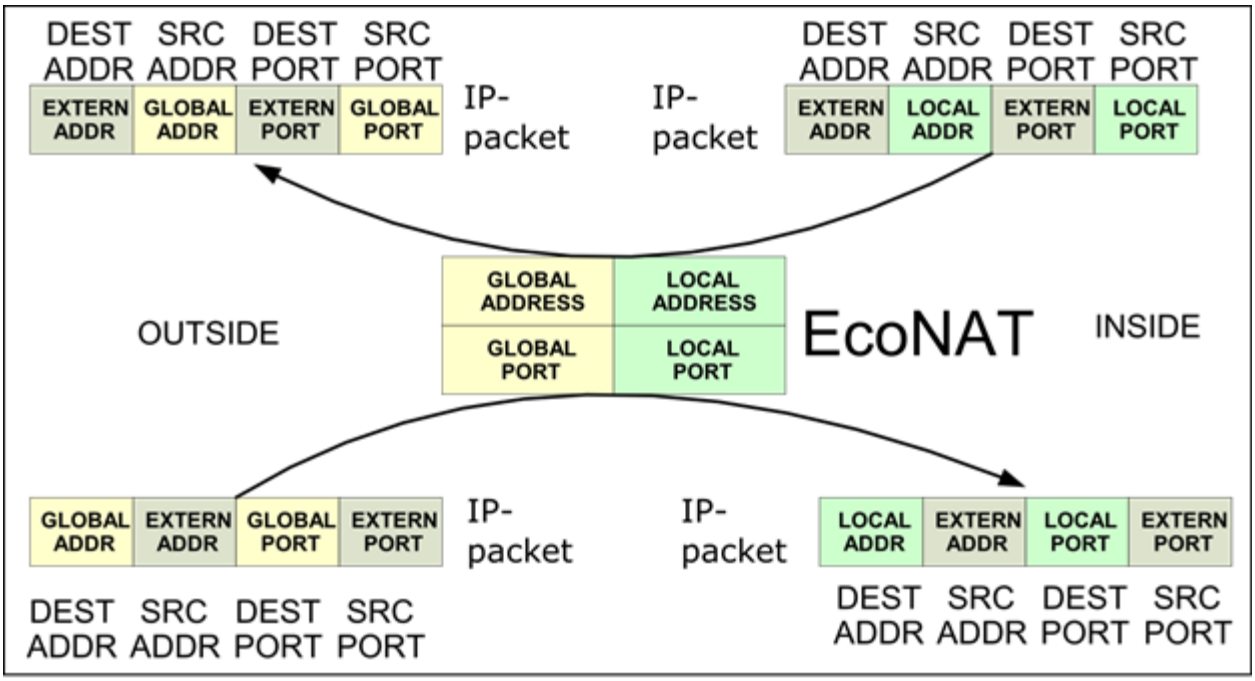

Рисунок 13

10.2.6 Пул CGNAT64

Технология NAT64 обеспечивает возможность доступа из сети, использующей только IPv6, к устройствам, использующим только IPv4. В системе EcoSGE реализованы Stateful NAT64 (RFC 6146) и Stateless NAT64 (RFC 7915). Соответствующие типы пулов – CGNAT64 и Static64. Если в NAT для IPv4 (NAT44) транслируется только IP-адрес отправителя пакета, то в NAT64 происходит также преобразование IP-адреса получателя. ALG в NAT64 расширен для поддержки работы протоколов, в которых информация об адресах и портах содержится в полезной нагрузке TCP-сегментов и UDP-дейтаграмм.

Пул CGNAT64 выполняет в NAT64 ту же роль, что и пул CGNAT в NAT44. По сравнению с CGNAT, для адресации к устройствам за EcoSGE, использующим только IPv4, в настройках пула CGNAT64 необходимо задать дополнительный параметр **v6_remote_prefix**. EcoSGE

добавляет этот префикс к IPv4-адресам ingress-пакетов и удаляет его из адресов назначения IPv6 egress-пакетов. В RFC 6052 определён так называемый "хорошо известный" префикс (Well-Known Prefix, WKP) 64:FF9B::/96, рекомендуемый к использованию в типовых случаях. В общем случае можно использовать любой префикс, но при одном условии: он должен иметь длину /96.

Ещё одно отличие пула CGNAT64 от CGNAT – вместо параметра **acl** используется параметр **aclv6**, в котором необходимо указать ACL для абонентского трафика IPv6.

10.2.7 Пул Static NAT

Пул Static NAT определяет правила статической трансляции сетевых адресов. Каждому локальному адресу однозначно сопоставляется глобальный адрес. Трансляция портов не производится. Вместо списка глобальных адресов, принадлежащих пулу (параметр **global_ip** в пулах CGNAT и Basic NAT) создаётся список правил трансляции адресов 1 в 1 (параметр **global_map**). Описание всех параметров, доступных для настройки пула Static NAT, содержится в разделе "Создание и настройка пула".

В параметре **global_map** можно задавать два типа правил трансляции:

- адрес в адрес. Правила задаются в виде **<локальный адрес>[~vid]-<глобальный адрес>**, где **vid** – идентификатор VLAN от 0 до 4094 (необязательный параметр). Значение **vid** задаётся с префиксом "~" (тильда) без пробела после адреса;
- подсеть в подсеть. Правила задаются в виде **<локальная подсеть>[~vid]-<глобальная подсеть>**. Обязательное условие для трансляций данного типа – одинаковая длина префикса локальной подсети и сопоставленной ей глобальной подсети. Трансляции выполняются строго по порядку адресов в подсетях. Например, A.A.A.1 → B.B.B.1, A.A.A.2 → B.B.B.2 и т. д.

Примечание. Для выполнения трансляций с учётом VLAN ID необходима лицензия на функциональность VLAT (VLAN+NAT).

```
EcoSGE:1:# create pool c
EcoSGE:2:# goto poolc
EcoSGE:3:pools.poolc# type static
EcoSGE: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
EcoSGE:5:pools.poolc# global_map += 192.168.0.5-200.0.0.3
EcoSGE:6:pools.poolc# global_map += (192.168.1.2~102-3.3.3.3)
EcoSGE:7:pools.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 всё же задан и настроен, то сначала проверяется он, а затем неявно предполагаемый.

ВНИМАНИЕ! Если к пулу типа **static** привязан ACL, то в этом ACL не должно быть правила **permit any any**.

10.2.8 Пул Static NAT64

Пул Static NAT64 (static64) выполняет в NAT64 ту же роль, что и пул static в NAT44. По сравнению с пулом static, для адресации к устройствам за EcoSGE, использующим только IPv4, в настройках пула static64 необходимо задать дополнительный параметр **v6_remote_prefix**. EcoSGE добавляет этот префикс к IPv4-адресам ingress-пакетов и удаляет его из адресов назначения IPv6 egress-пакетов. В RFC 6052 определён так называемый "хорошо известный" префикс (Well-Known Prefix, WKP) 64:FF9B::/96, рекомендуемый к использованию в типовых случаях. В общем случае можно использовать любой префикс, но при одном условии: он должен иметь длину /96.

Ещё два отличия пула static64 от static:

- вместо параметра **acl** используется параметр **aclv6** для указания ACL для абонентского трафика IPv6. 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 всё же задан и настроен, то сначала проверяется он, а затем неявно предполагаемый. **Внимание!** Если к пулу типа static привязан ACL, то в этом ACL не должно быть правила **permit any any**.
- вместо параметра **global_map** используется параметр **global_map_64** для задания отображений локальных IPv6-адресов в глобальные IPv4-адреса, какими они будут видны хостам на стороне WAN. Пример: global_map_64 ([2001:DB8::1]-192.0.2.1 [2001:DB8::2]-198.51.100.2)

10.2.9 Пулы Fake и Fake6

Пулы **fake** и **fake6** предназначены для обслуживания абонентского трафика IPv4 и IPv6*, к которому не требуется применять NAT, но при этом необходимо применять, например, сервисы BRAS или URL-фильтрацию. Параметры указанных пулов описаны в разделе "Создание и настройка пула". Единственное отличие в настройках этих пулов – параметры **acl** и **aclv6**.

* Для обработки трафика IPv6 требуется отдельная лицензия.

Пример применения этих пулов рассмотрен в разделе "Фильтрация абонентского трафика, к которому не применяется NAT".

10.2.10 Пул port_fwd

Пул типа **port_fwd** предназначен для обеспечения доступа извне к ресурсам абонентов, находящихся со стороны LAN-порта EcoSGE. Данная функциональность аналогична часто используемым в корпоративных и домашних сетях технологиям DNAT, DMZ, Port Forwarding.

Для задания пула типа port_fwd необходимо определить отображение (mapping) пары локальных IP-адреса и TCP/UDP-порта в пару глобальных IP-адреса и порта. Это отображение задаётся непосредственно в ветке конфигурации пула, поэтому, в отличие от пулов других типов, в пуле типа port_fwd не используется ACL.

Сразу после создания пула командой **create pool** и выбора типа **port_fwd** ветка конфигурации данного пула выглядит следующим образом:

```
type port_fwd
enable
port_map ( )
hairpin on
connection_logging on
```

Назначение параметров **hairpin** и **connection_logging** аналогично назначению одноимённых параметров в других типах пулов. Уникальный для данного типа пула параметр **port_map** задаётся в виде **(proto:local_ip:local_port-global_ip:global_port[~vid])**, где:

- **proto** – протокол (**tcp** или **udp**);
- **local_ip:local_port** – локальные IPv4-адрес и порт абонентского хоста, на котором запущен соответствующий сервис;
- **global_ip:global_port** – глобальные IPv4-адрес и порт во внешней сети, к которым обращаются клиентские приложения;
- **vid** – VLAN ID, необязательный параметр, указывается при наличии лицензии на функциональность VLAT.

При использовании пула типа **port_fwd** следует учитывать две особенности:

1. При соответствии трафика одновременно параметру **port_map** данного пула и ACL других типов пулов трафик попадёт в данный пул.
2. При простое сессии в течение времени, превышающего таймауты, заданные в ветке конфигурации **system.nat_defaults**, данная сессия будет закрыта. Если для какого-либо приложения (например, SSH) важно поддерживать сессию открытой независимо от её активности, то необходимо обеспечить периодическую отправку пакетов keep-alive.

10.2.11 Действия с пулами

10.2.11.1 Отвязывание пула от ACL

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

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

10.2.11.2 Удаление пула

Для удаления пула необходимо отправить команду **no pool <имя пула>**.

```
EcoSGE:1:# no pool pooltest
```

```
EcoSGE:2:#
```

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

```
EcoSGE:1:# droppools
EcoSGE:2:#
```

10.2.11.3 Особенности применения изменений

Порядок применения любых изменений конфигурации, относящихся к пулам (включая их создание и удаление), а также поведение системы касательно существующих и новых трансляций и сессий зависит от типа и количества задействованных пулов, в которых должны быть применены изменения. Предусмотрены два режима перенастройки пулов: **one-by-one** и **all-at-once**.

Если изменения затрагивают не более четырёх задействованных пулов типа **nat**, **static**, **static64**, **fake**, **fake6**, **port_fwd** (в любой комбинации), то перенастройка выполняется в режиме **one-by-one**. В данном режиме:

- система поочерёдно применяет изменения в каждом пуле;
- сохраняются существующие трансляции и сессии, которые соответствуют изменённым настройкам пулов; относящийся к данным трансляциям и сессиям трафик не прерывается;
- возможно создание новых трансляций и сессий;
- возможно прерывание логирования трансляций и сессий.

Если изменения затрагивают более четырёх задействованных пулов типа **nat**, **static**, **static64**, **fake**, **fake6**, **port_fwd** (в любой комбинации) или хотя бы один задействованный пул другого типа (например, **cgnat**), то перенастройка выполняется в режиме **all-at-once**. В данном режиме:

- система применяет изменения одновременно во всех пулах;
- сохраняются существующие трансляции и сессии, которые соответствуют изменённым настройкам пулов; относящийся к данным трансляциям и сессиям трафик не прерывается;
- невозможно создание новых трансляций и сессий.

10.2.12 Особенности работы с трафиком ICMP в режиме NAT64

Помимо трансляции абонентского трафика устройство EcoSGE в режиме NAT64 обеспечивает трансляцию следующих типов ICMP-сообщений, попадающих в пулы cgnat64 и static64:

- входящих и исходящих сообщений Echo Request;
- входящих сообщений Echo Reply;
- входящих сообщений ICMP Error следующих типов:
  - network unreachable;
  - host unreachable;
  - port unreachable;
  - fragmentation is needed and "Don't Fragment" was set;

- time exceeded;

- исходящих сообщений ICMP Error следующих типов:
  - network unreachable;
  - host unreachable;
  - port unreachable;
  - fragmentation is needed and "Don't Fragment" was set;
  - time exceeded;
  - parameter problem;
  - packet too big.

10.2.13 NAT для доступа в Интернет

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

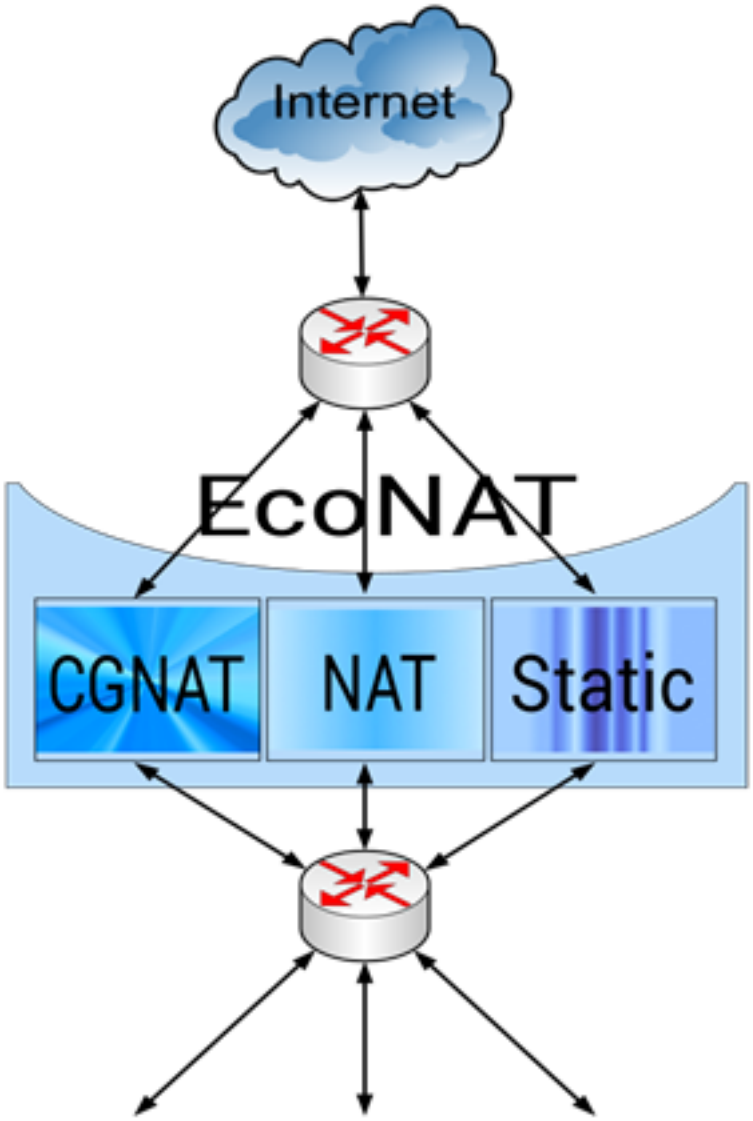

Рисунок 14

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

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.

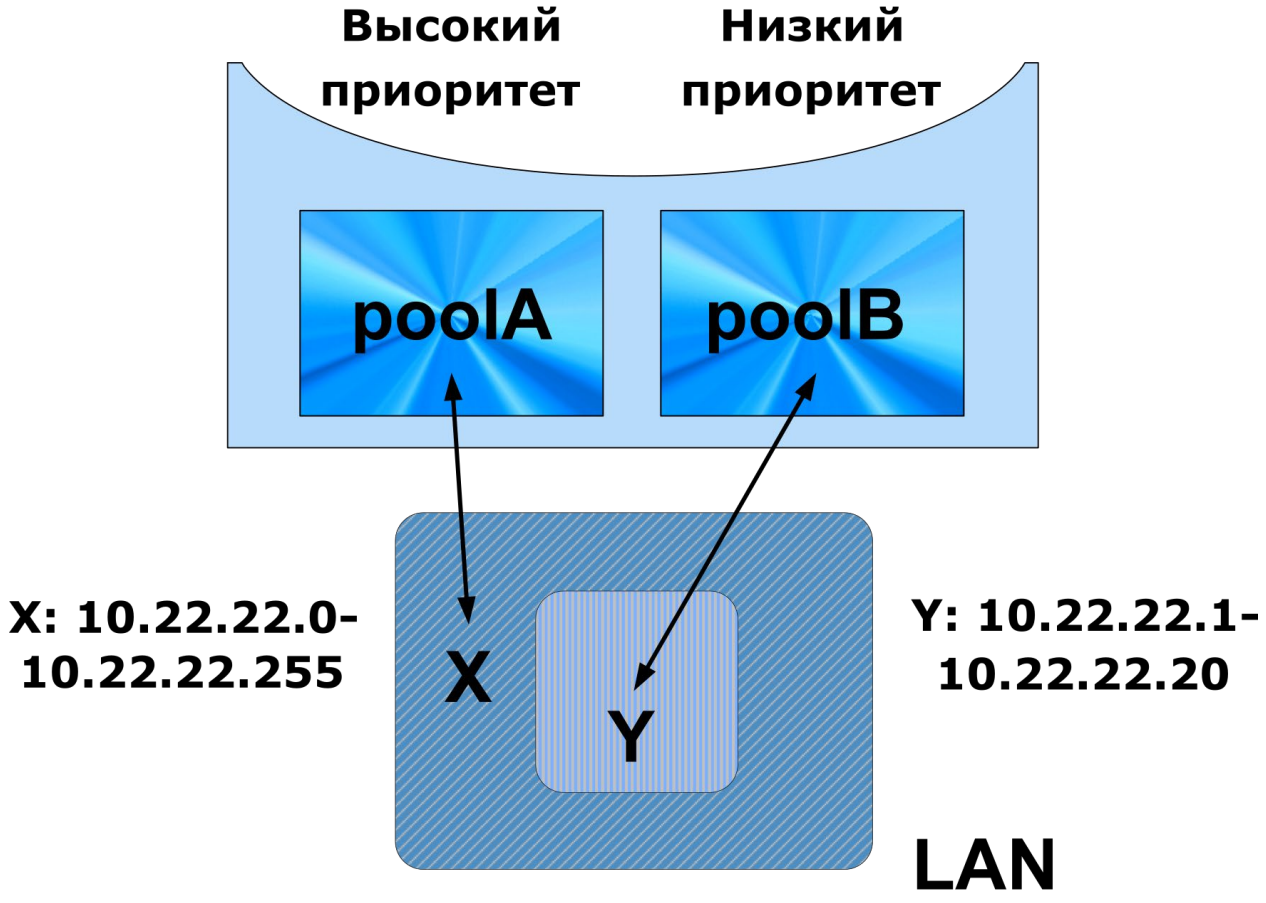

Рисунок 15

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.

10.2.14 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.

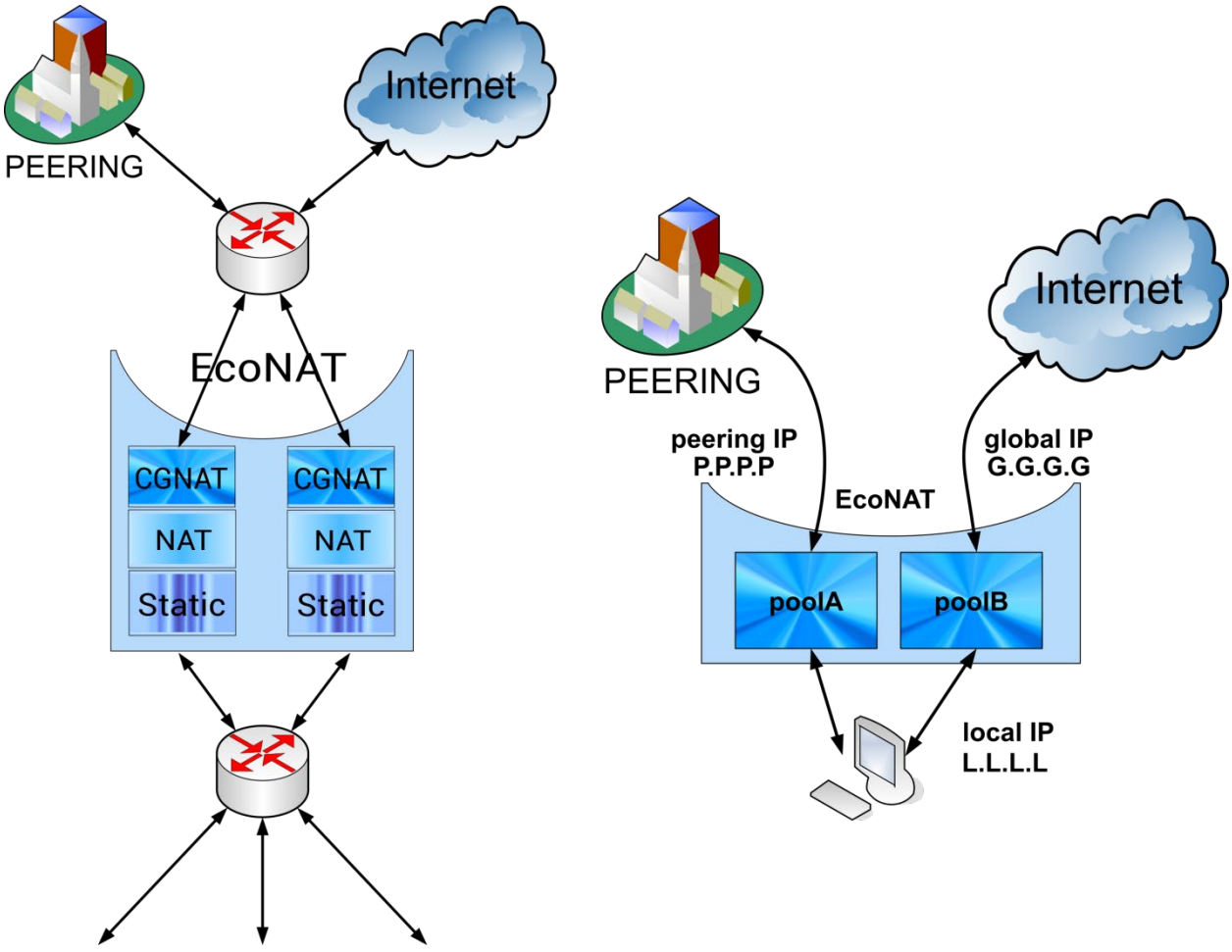

Рисунок 16

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.

10.3 Статистика NAT

В данном разделе описаны команды для вывода информации о трансляциях и сессиях, привязках адресов в пулах CGNAT и CGNAT64 и ошибках выделения портов в этих пулах.

10.3.1 Трансляции

Для просмотра существующих в данный момент трансляций предусмотрена подгруппа команд **show xlate**. Ниже описаны действия и даны примеры вывода команд этой подгруппы.

Таблица 18

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

Примеры вывода команд:

```
EcoSGE:1:> 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.
```

```
EcoSGE:2:# 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
EcoSGE:3:> 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.
EcoSGE:4:> 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.
EcoSGE:5:> 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.
EcoSGE:6:> 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
EcoSGE:7:> 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.
EcoSGE:8:> 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.
EcoSGE:9:> 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.
```

Для подгруппы команд **show xlate** предусмотрена возможность фильтрации вывода. Подробная информация содержится в разделе "Фильтрация вывода команд группы Show".

Для очистки таблицы трансляций используется команда **clear sessions all**.

```
EcoSGE:# clear sessions all
Sessions table purged
Translation table purged
```

10.3.2 Сессии

Для просмотра существующих в данный момент сессий предусмотрена подгруппа команд **show sessions**. Ниже описаны действия и даны примеры вывода команд этой подгруппы.

Таблица 19

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

Примеры вывода команд:

```
EcoSGE:1:> 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.
EcoSGE:2:> 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.
EcoSGE:3:> 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.
EcoSGE:4:> 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.
EcoSGE:5:> 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
EcoSGE:6:> 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.
EcoSGE:7:> 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.
EcoSGE:8:> 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.
EcoSGE:9:> 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.
```

Для подгруппы команд **show sessions** предусмотрена возможность фильтрации вывода. Подробная информация содержится в разделе "Фильтрация вывода команд группы Show".

10.3.2.1 Удаление сессий

Удаление сессий производится командами из подгруппы **clear sessions**. Ниже описаны действия команд этой подгруппы.

Таблица 20

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

Пример:

```
EcoSGE:1:> 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.
```

10.3.3 Привязки адресов

Для вывода информации о существующих в данный момент привязках локальных IP-адресов к глобальным для пулов CGNAT и CGNAT64 предусмотрена подгруппа команд **show bind**. Ниже описаны действия и даны примеры вывода команд этой подгруппы.

Таблица 21

Команда	Действие
show bind { local | global } { <IP-адрес> | <диапазон> | <подсеть> | any }	Вывод списка привязок указанных локальных или глобальных IP-адресов с указанием времени жизни каждой привязки
show bind summary	Вывод счётчиков количества локальных адресов, привязанных к каждому глобальному адресу
show bind usage	Вывод счётчиков заполнения таблиц абонентов

Примеры вывода команд:

```
EcoSGE:# show bind local any
CGNAT pool 'pool44'
```

```
Global IP usage: 4 out of 4
1.1.1.0 -> 2.2.2.0 | 86211 sec
1.1.1.1 -> 2.2.2.1 | 86211 sec
1.1.1.2 -> 2.2.2.2 | 86211 sec
1.1.1.3 -> 2.2.2.3 | 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
CGNAT64 pool 'pool64'
Global IP usage: 1 out of 1
fc00::1 -> 3.3.3.3 | 86211 sec
fc00::2 -> 3.3.3.3 | 86211 sec
EcoSGE:# show bind global any
CGNAT pool 'pool44'
Global IP usage: 4 out of 4
1.1.1.0 -> 2.2.2.0 | 86205 sec
1.1.1.4 -> 2.2.2.0 | 86205 sec
1.1.1.1 -> 2.2.2.1 | 86205 sec
1.1.1.5 -> 2.2.2.1 | 86205 sec
1.1.1.2 -> 2.2.2.2 | 86205 sec
1.1.1.6 -> 2.2.2.2 | 86205 sec
1.1.1.3 -> 2.2.2.3 | 86205 sec
1.1.1.7 -> 2.2.2.3 | 86205 sec
CGNAT64 pool 'pool64'
Global IP usage: 1 out of 1
fc00::1 -> 3.3.3.3 | 86205 sec
fc00::2 -> 3.3.3.3 | 86205 sec
EcoSGE:# show bind summary
CGNAT pool 'pool44'
2.2.2.0 -> 2
2.2.2.1 -> 2
2.2.2.2 -> 2
2.2.2.3 -> 2
CGNAT64 pool 'pool64'
3.3.3.3 -> 2
EcoSGE:# show bind usage
Abons table used/total: 8/245760 (0.0%)
Abons table NAT64 used/total: 2/245760 (0.0%)
```

10.3.4 Ошибки выделения портов

Для вывода информации об ошибках выделения портов в пулах CGNAT и CGNAT64 предусмотрены команды **show cgnat errors** и **show cgnat64 errors**.

Пример вывода команды:

```
EcoSGE:> 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:

- **proto** – тип протокола,
- **reason** – причина ошибки,
- **count** – общее количество ошибок,
- **Debug counters** – отладочные счётчики для разработчиков.

Для команды **show cgnat errors** предусмотрена возможность фильтрации вывода. Подробная информация содержится в разделе "Фильтрация вывода команд группы Show".

Обозначения типов протоколов приведены в таблице ниже.

Таблица 22

Обозначение	Протокол
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 23

Обозначение	Причина
0	Ошибка выделения порта или блока портов для исходящей сессии в пуле **cgnat**. При этом срабатывает счётчик **cr_session_alloc_error_egress**
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
0x1E	Ошибка выделения порта или блока портов для исходящей сессии в пуле **port_fwd**. При этом срабатывает счётчик **cr_session_alloc_error_egress**
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

Для сброса счётчиков ошибок выделения портов в пулах CGNAT или CGNAT64 необходимо отправить команду **clear cgnat errors** или **clear cgnat64 errors** соответственно.

11 Подсистема 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.

11.1 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
aclv6 none
always_pass none
always_pass_v6 none
no_shape none
no_shape_v6 none
graceful_reload false
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 24

Параметр	Описание
acl	ACL, которому должен соответствовать трафик IPv4 для поступления на обработку в BRAS. Значение по умолчанию – **none**, что эквивалентно правилу ACL **allow ip src any dst any**, т. е. любой абонентский трафик IPv4, попадающий в какой-либо пул подсистемы NAT, будет поступать на обработку в BRAS
aclv6	ACL, которому должен соответствовать трафик IPv6 для поступления на обработку в BRAS. Значение по умолчанию – **none**, что эквивалентно правилу ACL **allow ip src any dst any**, т. е. любой абонентский трафик IPv6, попадающий в какой-либо пул подсистемы NAT, будет поступать на обработку в BRAS. Параметр доступен при наличии лицензии на работу с трафиком IPv6
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)
always_pass always_pass_v6	ACL для трафика IPv4 и IPv6, который необходимо исключить из обработки в BRAS. Правила данных ACL суммируются с правилами ACL, указанных в одноимённых параметрах сервиса. Параметр **always_pass_v6** доступен при наличии лицензии на работу с трафиком IPv6
no_shape no_shape_v6	ACL для трафика IPv4 и IPv6, к которому не должно применяться ограничение скорости передачи данных. Правила данных ACL суммируются с правилами ACL, указанных в одноимённых параметрах сервиса. Параметр **no_shape_v6** доступен при наличии лицензии на работу с трафиком IPv6
graceful_reload { false | true }	Определяет действия BRAS, связанные с повторной авторизацией абонентов при замене ACL в общих настройках, политиках и сервисах, а также при

Параметр	Описание
	изменении правил самих ACL. Если задано значение **false**, то при применении нового/изменённого ACL будут отправлены запросы на повторную авторизацию всех активных абонентов, авторизованных на момент применения, за исключением тех, чей трафик не соответствует ACL ни одной из динамических политик и/или новому/изменённому общему ACL. При значении **true** применение нового/изменённого ACL не влияет на абонентов, авторизованных на момент применения, независимо от того, соответствует их трафик новому/изменённому ACL или нет. Запросы на повторную авторизацию абонентов, чей трафик соответствует изменённому ACL, будут отправлены по истечении тайм-аутов их сессий (если сессия остаётся активной). По умолчанию **false**
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**.

11.2 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.

11.2.1 Создание и настройка политики

В подсистеме BRAS предусмотрены три типа политик:

- **static** – простая статическая политика. Действия с трафиком абонентов определяются постоянным сервисом или набором сервисов (см. раздел "Создание и настройка сервиса");
- **static_shared** – групповая статическая политика. Отличие от простой статической политики – возможность задания групповых ограничений в отдельном, более приоритетном сервисе. Например, можно задать пропускную способность общего канала для группы абонентов;
- **dynamic** – динамическая политика. Требует взаимодействия с внешним RADIUS-сервером. Для каждого возможного ответа RADIUS-сервера (Access-Accept, Access-Reject, Authentication-Failed) можно задать свой сервис или набор сервисов, определяющий действия с трафиком. Можно назначить сервис, применяемый по умолчанию к трафику абонентов, которые ещё не прошли авторизацию. Кроме того,

возможно обслуживание группы абонентов в рамках одного контракта с общей пропускной способностью канала по аналогии с политикой **static_shared**.

Для создания политики необходимо отправить команду **create policy <имя>**. Имя политики может содержать только латинские буквы (регистр учитывается), цифры и знак подчёркивания. В ветке конфигурации **system.bras.policies** будет создан объект **policy<имя>** (обратить внимание – без пробела между словами). Затем необходимо перейти в ветку параметров созданной политики командой **goto policy<имя>** и задать значения её параметров. В первую очередь следует указать тип политики в параметре **type**, который может принимать значения **static** (по умолчанию), **static_shared** или **dynamic**. От выбранного типа политики зависит набор параметров настройки.

11.2.1.1 Простая статическая политика

В таблице ниже описаны параметры простой статической политики.

Таблица 25

Параметр	Описание
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.
enable | disable	Включение / выключение политики
ingress_auth	Разрешить (**on**) / запретить (**off**) авторизацию абонента и создание абонентской сессии по входящему пакету с Destination IP-адресом абонента
acl	ACL, которому должен соответствовать трафик IPv4 для применения политики
aclv6	ACL, которому должен соответствовать трафик IPv6 для применения политики. Параметр доступен при наличии лицензии на работу с трафиком IPv6
acct	Имя подключения к RADIUS-серверу или группы RADIUS-серверов для аккаунтинга (см. разделы "Настройка доступа к RADIUS-серверу" и "Группы RADIUS-серверов"). По умолчанию **none**, т. е. аккаунтинг не используется
session_timeout	Максимальное время существования сессии в секундах. По истечении данного времени текущая сессия закрывается и создаётся новая. 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. По умолчанию 28800
interim_interval	Периодичность аккаунтинга в секундах. Применяется при настроенном подключении к RADIUS-серверу. По умолчанию 60
services ( )	Имя сервиса, привязываемого к политике. Можно указать до 6 сервисов через пробел. Порядок указания сервисов определяет их приоритет (по убыванию)

Пример создания и настройки статической политики:

```
EcoSGE:1:system.bras.policies# create policy 1
EcoSGE:2:system.bras.policies# policy1
EcoSGE:3:system.bras.policies.policy1# enable
```

```
EcoSGE:4:system.bras.policies.policy1# acl acltestv4
EcoSGE:5:system.bras.policies.policy1# aclv6 acltestv6
EcoSGE:6:system.bras.policies.policy1# type static
EcoSGE:7:system.bras.policies.policy1# services service1
EcoSGE:8:system.bras.policies.policy1# ls
  priority 100
  enable
  ingress_auth off
  acl acltestv4
  aclv6 acltestv6
  type static
  acct none
  session_timeout 86400
  idle_monitor_direction both
  idle_timeout 28800
  interim_interval 60
  services ( service1 )
```

11.2.1.2 Групповая статическая политика

Групповая статическая политика содержит те же параметры, что и простая статическая политика (см. таблицу выше), а также дополнительный параметр **common_service**. Данный параметр позволяет указать сервис, который будет устанавливать групповые ограничения для абонентского трафика, соответствующего правилам ACL данного сервиса. Например, можно задать пропускную способность общего канала для группы абонентов.

11.2.1.3 Динамическая политика

Динамическая политика содержит те же параметры, что и простая статическая политика (см. таблицу выше), за исключением параметра **services**, а также дополнительные параметры, описанные в таблице ниже.

Таблица 26

Параметр	Описание
auth	Имя подключения к RADIUS-серверу или имя группы RADIUS-серверов для отправки запросов авторизации абонентов (см. разделы "Настройка доступа к RADIUS-серверу" и "Группы RADIUS-серверов"). **ВНИМАНИЕ!** Перед применением настроек динамической политики значение параметра **auth** не должно быть **none**. В противном случае выполнение команды **apply** завершится с ошибкой
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). По умолчанию 180
default ( )	Сервис (или сервисы), который применяется для абонента, попавшего в политику, но ещё 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 для абонента, если RADIUS-сервер не ответил на Access-Request по истечении соответствующего тайм-аута

Примечание. В динамической политике по истечении времени **session_timeout** BRAS отправляет повторный запрос Access-Request (RADIUS-сервер может переопределить данный тайм-аут параметром Session-Timeout). То же самое происходит и в том случае, если на запрос авторизации абонента был получен ответ Access-Reject.

Пример создания и настройки динамической политики:

```
EcoSGE:1:system.bras.policies# create policy 2
EcoSGE:2:system.bras.policies# policy2
EcoSGE:3:system.bras.policies.policy2# enable
EcoSGE:4:system.bras.policies.policy2# acl acltestv4
EcoSGE:5:system.bras.policies.policy2# type dynamic
EcoSGE:6:system.bras.policies.policy2# auth radius1
EcoSGE:7:system.bras.policies.policy2# default (service5M)
EcoSGE:8:system.bras.policies.policy2# if_auth_accept (service1 service5M)
EcoSGE:9:system.bras.policies.policy2# if_auth_reject (service2)
EcoSGE:10:system.bras.policies.policy2# if_auth_fail (service2)
EcoSGE:11:system.bras.policies.policy2# show
  priority 200
  enable
  ingress_auth off
  acl aclv4test
  aclv6 none
  auth radius1
  acct none
  reauthorization_timeout 180
  session_timeout 86400
  idle_timeout 28800
  idle_monitor_direction both
  interim_interval 60
  default ( service5M )
  if_auth_accept ( service1 service5M )
  if_auth_reject ( service2 )
  if_auth_fail ( service2 )
```

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

11.2.2 Создание и настройка сервиса

Для создания сервиса необходимо отправить команду **create service <имя сервиса>**. Имя сервиса может содержать только латинские буквы (регистр учитывается), цифры и знак подчёркивания. При создании сервиса его название формируется так же, как описано в разделе "Создание и настройка пула".

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 27

Параметр	Описание
enable | disable	Включение / выключение сервиса

Параметр	Описание
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. "Настройка периодического перенаправления"). При указании данного действия происходит перенаправление HTTP-трафика (HTTPS проходит). Для правильного выполнения в параметрах DPI-списка, привязанного к данному сервису, необходимо указать **redirect_use_interval on**
acl	ACL для трафика IPv4, к которому необходимо применять сервис. Параметр игнорируется, если сервис связан с динамической политикой, а она в свою очередь применяется к трафику абонентов из общего контракта.
aclv6	ACL для трафика IPv6, к которому необходимо применять сервис. Параметр игнорируется, если сервис связан с динамической политикой, а она в свою очередь применяется к трафику абонентов из общего контракта.
tethering	Данный параметр указывает, к трафику какого абонентского устройства – основного или дополнительного – применять сервис (см. раздел "Функция Tethering Detection"). Допустимые значения: • **any** (по умолчанию) – применять сервис к любому абонентскому трафику; • **main** – применять сервис к трафику основного устройства; • **secondary** – применять сервис к трафику дополнительного устройства
redirect_url	Адрес, на который будет происходить переадресация клиента, если используется **action redirect**. Как правило, здесь задаётся адрес портала оператора связи, куда переадресовывается абонент в случае необходимости пополнения счёта, 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;

Параметр	Описание
	%u – передавать в redirect_url url, на который обратился клиент. Формат ввода параметра **redirect_url**: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>=<SPEC2>..<VAR_NAMEN>=<SPECN>** где **URL** – адрес страницы, на которую осуществляется перенаправление, **VAR_NAME1** .. **VAR_NAMEN** – имя переменной, **SPEC1** .. **SPECN** – спецификатор. Например, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. Если при таком значении параметра клиент попробует обратиться на адрес **forbidden.com**, то он будет перенаправлен на адрес: **http://example.com/?var1=forbidden.com&ip=10.1.1.10&qwe=0**
egress_classmaps ( )	Карты классов трафика, по которым происходит контроль исходящих пакетов (см. раздел "Карты классов трафика"). Указываются через пробел. Учитываются все карты классов, поэтому порядок их указания не важен. Параметр игнорируется, если сервис связан с динамической политикой, а она в свою очередь применяется к трафику абонентов из общего контракта. Изменения значения поля DSCP в течение сессии не учитываются
ingress_classmaps ( )	Карты классов трафика, по которым происходит контроль входящих пакетов (см. раздел "Карты классов трафика"). Указываются через пробел. Учитываются все карты классов, поэтому порядок их указания не важен. Параметр игнорируется, если сервис связан с динамической политикой, а она в свою очередь применяется к трафику абонентов из общего контракта. Изменения значения поля DSCP в течение сессии не учитываются
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**
egress_ttl	Новое значение TTL и Hop Limit для исходящих пакетов IPv4 и IPv6 соответственно. Диапазон значений – от 0 до 255. По умолчанию **nochange** (не изменять)
ingress_ttl	Новое значение TTL и Hop Limit для входящих пакетов IPv4 и IPv6 соответственно. Диапазон значений – от 0 до 255. По умолчанию **nochange** (не изменять)
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
http_analyzer	Имя HTTP-анализатора (см. раздел "Анализ HTTP запросов и ответов"). Применяется только к трафику TCP. По умолчанию **none**, т. е. анализ не проводится

Параметр	Описание
always_pass always_pass_v6	ACL для трафика IPv4 и IPv6, к которому не должен применяться сервис. Правила данных ACL суммируются с правилами ACL, указанных в одноимённых параметрах в общих настройках BRAS (ветка конфигурации **system.bras**). Параметр **always_pass_v6** доступен при наличии лицензии на работу с трафиком IPv6
no_shape no_shape_v6	ACL для трафика IPv4 и IPv6, к которому не должно применяться ограничение скорости передачи данных. Правила данных ACL суммируются с правилами ACL, указанных в одноимённых параметрах в общих настройках BRAS (ветка конфигурации **system.bras**). Параметр no_shape_v6 доступен при наличии лицензии на работу с трафиком IPv6
dpilists ( )	Номер DPI-списка для выполнения URL-фильтрации (см. раздел "Подсистема DPI"). Если интернет-ресурс попадает под действие DPI-списка, то происходит переадресация на ресурс, указанный в параметре **redirect_url**. Параметр доступен только при установленном модуле URL-фильтрации

Пример создания и настройки сервиса:

```
EcoSGE:1:system.bras.services# create service 1
EcoSGE:2:system.bras.services# service1
EcoSGE:3:system.bras.services.service1# enable
EcoSGE:4:system.bras.services.service1# action redirect
EcoSGE:4:system.bras.services.service1# acl acltestv4
EcoSGE:4:system.bras.services.service1# aclv6 acltestv6
EcoSGE:5:system.bras.services.service1# redirect_url
"http://redirect.domen.ru"
EcoSGE:6:system.bras.services.service1# egress_speed 56
EcoSGE:7:system.bras.services.service1# ingress_speed 56
EcoSGE:8:system.bras.services.service1# time_start daily 03:00
EcoSGE:9:system.bras.services.service1# time_end daily 21:00
EcoSGE:10:system.bras.services.service1# show
  enable
  action redirect
  acl acltestv4
  aclv6 acltestv6
  redirect_url "http://redirect.domen.ru"
  egress_classmaps ( )
  ingress_classmaps ( )
  egress_speed 56
  ingress_speed 56
  egress_tos nochange
  ingress_tos nochange
  egress_ttl nochange
  ingress_ttl nochange
  time_start daily 03:00:00
  time_end daily 21:00:00
  always_pass none
  always_pass_v6 none
  no_shape none
  no_shape_v6 none
  dpilists ( )
```

Для применения изменений необходимо отправить команду **apply**.

11.3 Функция Tethering Detection

По отдельной лицензии для BRAS доступна функция Tethering Detection (обнаружение раздачи доступа в Интернет), которая может быть полезна операторам мобильной связи. Наличие данной функции позволит настраивать и применять разные сервисы к трафику основного абонентского устройства и подключенных к нему дополнительных устройств, когда абонент использует на основном устройстве режим точки доступа, USB-модема и т. п. Сервисы для основного и дополнительного трафика назначаются параметром **tethering** (см. раздел "Создание и настройка сервиса).

BRAS определяет принадлежность трафика основному или дополнительному устройству по значению поля TTL в пакетах IPv4 (Hop Limit в пакетах IPv6). При получении первого исходящего пакета первой сессии абонента BRAS запоминает значение TTL данного пакета. К трафику первой и всех следующих сессий с таким TTL применяются сервисы с настройкой **tethering main** и/или **tethering any** (при соответствии трафика остальным критериям, таким как ACL, DSCP, порядковый номер сервиса в политике и т. п.), т. е. BRAS определяет, что это сессии основного абонентского устройства. Трафик любых сессий с другим TTL пакетов считается трафиком дополнительного абонентского устройства, и к нему применяются сервисы с настройкой **tethering secondary** и/или **tethering any** из списка сервисов (при соответствии трафика остальным критериям).

Примечание. Изменение TTL в ходе сессии не учитывается.

Если сессия инициирована входящим пакетом, то сначала к ней применяется сервис с настройкой **tethering main** или **tethering any**. При поступлении первого исходящего пакета в этой сессии алгоритм действий BRAS аналогичен вышеописанному:

- если TTL абонента еще не сохранён, то BRAS сохраняет его в качестве основного и не сменяет сервис;
- если TTL уже сохранён, и при этом у исходящего пакета другой TTL, то сервис с настройкой **tethering main** сменяется сервисом с настройкой **tethering secondary** (сервис с настройкой **tethering any** продолжит действовать).

Узнать, какое значение TTL для IPv4 или Hop Limit для IPv6 сохранено в качестве основного для определённого абонента можно с помощью команды **show brasinfo <IP-адрес абонента>**. Вывод команды будет содержать строку **Main TTL <N>** для IPv4-адреса или **Main hop limit <N>** для IPv6-адреса, где N – соответствующее сохранённое значение.

При наличии функции аккаунтинга сессий (см. раздел "QoE") в логи добавляется один байт с информацией о принадлежности сессии основному устройству (значение 3), дополнительному (значение 1) или ещё не определённому (значение 0).

11.4 Анализ HTTP запросов и ответов

При использовании BRAS в связке с DPI можно вводить дополнительное условие применения сервисов к TCP-трафику: наличие определённого содержимого в HTTP запросах и ответах.

Анализ содержимого HTTP запросов и ответов выполняет подсистема DPI. В ней можно настроить несколько HTTP-анализаторов и привязать их к разным сервисам BRAS. Привязка выполняется через параметр **http_analyzer** (см. раздел "Создание и настройка сервиса").

Для создания HTTP-анализатора необходимо отправить команду **create http_analyzer <name>**. В ветке **system.dpi.http_analyzers** будет создан раздел **http_analyzer<name>**, где можно указать, какое содержимое должен искать HTTP-анализатор. Пример выполнения команды **create http_analyzer _test**:

```
dpi
{
http_analyzers
{
  http_analyzer_test
  {
     Request Method ( )
     User-agent ( )
     Content-Encoding ( )
     Answer code ( )
     Content-Type ( )
  }
}
}
```

Подробная информация о содержимом HTTP запросов и ответов приведена в RFC 9110.

Особенности настройки и алгоритм поиска содержимого:

- анализатор можно настроить на обработку либо HTTP-запросов (параметры Request Method и User-agent), либо HTTP-ответов (параметры Content-Encoding, Answer code и Content-Type);
- в каждом параметре можно задать не более 5 значений; разделитель – пробел;
- максимальная длина значения – 8 символов (3 для Answer Code);
- между значениями одного параметра – условие "ИЛИ"; между параметрами – условие "И";
- поиск ведётся по условию "СОДЕРЖИТ", регистр символов учитывается.

Для отслеживания работы HTTP-анализаторов предусмотрены следующие счётчики:

Таблица 28

Имя счётчика	Что подсчитывает	MIB OID
cr_bras_http_analyzer_try	Количество пакетов, отправленных из BRAS в DPI на анализ, включая пакеты без полезной нагрузки	.1.3.6.1.4.1.45555.1.2.598
cr_bras_http_analyzer_match	Количество обнаруженных полных совпадений	.1.3.6.1.4.1.45555.1.2.599
cr_bras_http_analyzer_result	Количество проанализированных пакетов, за исключением пакетов без полезной нагрузки	-
cr_bras_http_analyzer_reconf	Количество реконфигураций, связанных с задействованием анализаторов в сервисах BRAS. Примеры действий, на которые срабатывает счётчик: • привязка анализатора к	-

Имя счётчика	Что подсчитывает	MIB OID
	сервису; • изменение настроек анализатора, привязанного к сервису; • включение подсистемы DPI, в которой есть настроенные анализаторы, привязанные к сервисам; • и другие подобные изменения конфигурации	
cr_bras_http_analyzer_reconf_empty	Количество реконфигураций, связанных с исключением анализаторов из сервисов BRAS. Примеры действий, на которые срабатывает счётчик: • отвязка анализатора от сервиса (http_analyzer none); • выключение подсистемы DPI; • и другие подобные изменения конфигурации	-
cr_bras_http_analyzer_chunked	Количество проанализированных TCP-сегментов	-
cr_bras_http_analyzer_no_dpi	Неуспешные попытки передачи данных в анализатор из-за критической ошибки в работе подсистемы DPI	-

11.5 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.

11.5.1 Настройка доступа к RADIUS-серверу

В первую очередь необходимо создать новое подключение к RADIUS-серверу командой **create radius <имя подключения>**. Имя подключения может содержать только латинские буквы (регистр учитывается), цифры и знак подчёркивания. При создании подключения его имя формируется аналогично имени нового пула.

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 29

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:

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

11.5.2 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 необходимо отправить команду **create radiusgroup <имя>**. Имя группы RADIUS-серверов может содержать только латинские буквы (регистр учитывается), цифры и знак подчёркивания.

По умолчанию конфигурация только что созданной группы выглядит следующим образом.

```
EcoSGE: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 необходимо отправить команду **no radiusgroup <имя>**. Также можно использовать команду **dropradius**, в результате выполнения которой будут удалены все созданные группы RADIUS-серверов и подключения к ним.

В конфигурационном режиме можно изменить или удалить описание группы RADIUS-серверов, настроить режим её работы, добавить или удалить выбранный RADIUS-сервер. Данные команды и параметры описаны в таблице ниже.

Таблица 30

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.

Команда/параметр	Описание
	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>

11.5.2.1 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:

```
EcoSGE:# create radiusgroup 1
EcoSGE:# create radius 1
EcoSGE:# create radius 2
EcoSGE:# create radius 3
EcoSGE:# create radius 4
EcoSGE:# go radiusgroup1
EcoSGE:system.bras.radius.radius_groups.radiusgroup1# servers (radius1
radius2)
EcoSGE:system.bras.radius.radius_groups.radiusgroup1# servers add radius3
EcoSGE:system.bras.radius.radius_groups.radiusgroup1# servers += radius4
EcoSGE: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 '-='.

11.5.3 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 системных событий"). При авторизации значения данного атрибута не используются.

При получении Access-Accept от RADIUS сервера пользователю назначается сервис, указанный в параметре **if_auth_accept**, и соответствующие ему ограничения скорости. Сессия пользователя регулируется таймаутами, заданными в параметрах **session_timeout**, **idle_timeout**, **interim_interval**. Однако в том случае, если Access-Accept 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 "Настройка RADIUS").

11.5.4 Параметры RADIUS Change of Authorization (CoA)

Для обработки BRAS входящих запросов об изменении параметров авторизации пользователя (CoA) может быть использован код 43 (CoA-Request) и код 40 (Disconnect-Request) с указанием атрибута **User-Name**, в котором может передаваться IP-адрес абонента или номер контракта. При получении CoA-Disconnect происходит прерывание сессии (disconnect code 40). Новые параметры вступают в силу после переавторизации. При получении CoA-Request происходит изменение параметров текущей сессии без прерывания. После запроса отправляются данные Accounting-Stop и Accounting-Start.

Настройки CoA находятся в ветке конфигурации **system.bras.radius.coa**. Параметры, содержащиеся в данной ветке, представлены в таблице ниже.

Таблица 31

Параметр	Описание
enable disable	Включение / выключение функции изменения параметров авторизации пользователя
port	Порт, который будет слушать BRAS на интерфейсе управления для CoA-запросов
secret	Пароль для CoA-запросов

11.5.5 Счётчики RADIUS

Счётчики, относящиеся к RADIUS, выводятся командой **show counters all | include radius**.

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

```
Printing counters...
```

В таблице ниже приведено описание относящихся к RADIUS счётчиков, предусмотренных на момент публикации этой версии документации.

Таблица 32

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**

11.6 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.

11.6.1 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;50000000;D;50000000",
              Cisco-Account-Info += "P123",
              Cisco-Account-Info += "VU;1000000000;D;1000000000"
```

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;1000000000;D;1000000000", т. е. контракт подразумевает предоставление общего канала 1 Гбит/с. Для пятого абонента ошибочно задано "VU;50000000;D;50000000", 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.

11.6.2 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.

11.7 Создание сессий BRAS по пакетам DHCP

Сессии BRAS могут создаваться по пакетам DHCP. Данная возможность доступна по запросу и требует обновления ПО. Рассмотрим принцип работы данного механизма на примере схемы, представленной на рисунке ниже.

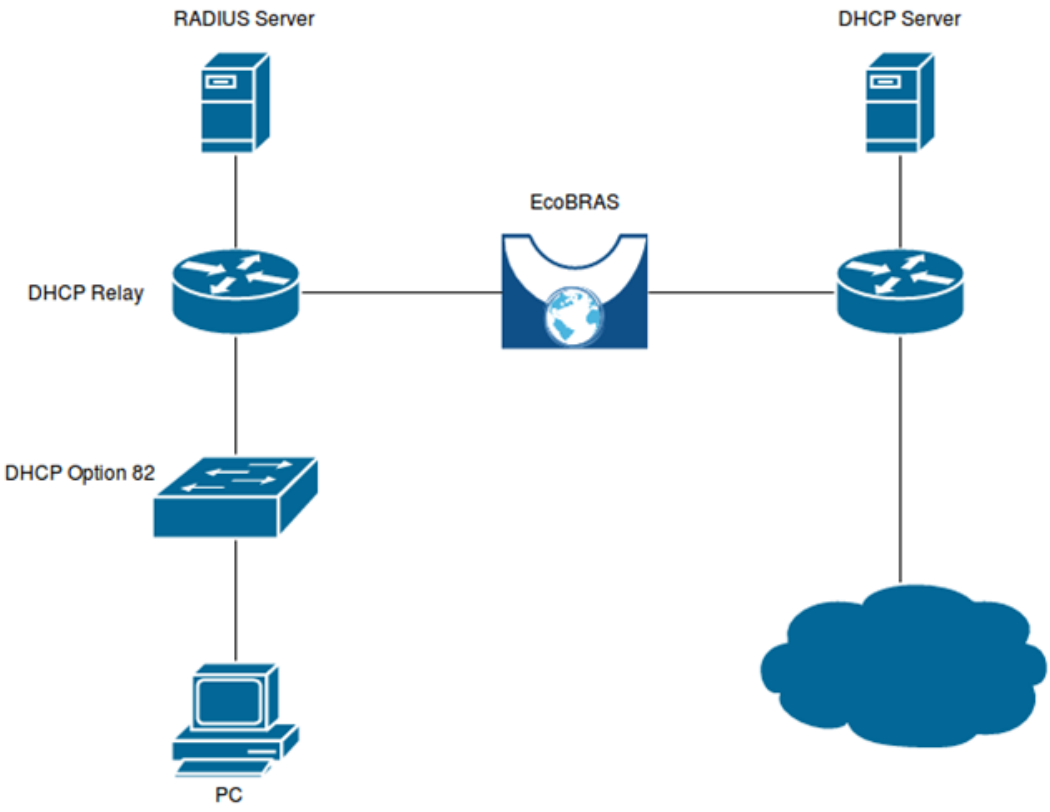

Рисунок 17

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

Когда абонент запрашивает настройки у DHCP-сервера, BRAS получает из пакета DHCP ACK следующие данные: IP-адрес, MAC-адрес, Option 82 (если присутствует). На основании этих данных создаётся сессия BRAS, а 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 пакет DHCP содержит Option 82, то в **Access-Request** добавляются дополнительные атрибуты:

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

При передаче от клиента сообщения **DHCP Release**, BRAS отправляет **Accounting-Stop** на RADIUS-сервер и закрывает сессию этого клиента.

11.8 Консоль биллинга и протокол EcoBRAS

Для взаимодействия с системой биллинга в EcoSGE используется специализированный проприетарный протокол EcoBRAS, который является простым текстовым протоколом.

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

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

Длина строки запроса не может превышать 64 килобайта. Строки запросов и ответов 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**
- **remove**
- **killcontract**
- **statall**
- **clearall**

11.8.1 Команда testRID

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

```
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
```

Если в EcoSGE отсутствуют номера договоров (например, если устройство только загрузилось), то ответом будет пустая строка.

```
B: testRID
E:
```

Сразу после загрузки подсистема BRAS работает в режиме пропускания всего трафика (для того чтобы абоненты обслуживались в то время, пока еще не загружена информация из системы 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 системе биллинга не разрешены явно). Состояние таймера можно узнать с помощью команды **time.**

11.8.2 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.

Если команда содержит IP-адреса ранее авторизованных абонентов, то к ним будут применены новые параметры, указанные в команде: номер контракта, номер тарифа, ограничения скорости.

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

Таблица 33

№	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 K/M/G или UNLIM	Скорость upstream (в Интернет). K/M/G – означают кило/мега/гига бит. Например, LIM64K – 64 Кбит/с. UNLIM – без ограничения 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

№	Поле	Содержание поля	Описание поля
			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

11.8.3 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 34

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

11.8.4 Команда remove

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

Команда **remove** позволяет удалять IP-адреса абонентов из всех контрактов, в которых они указаны. Синтаксис команды описан в таблице ниже.

Таблица 35

№	Поле	Содержание поля	Описание поля
1	`remove`	6 символов	Команда удаления IP-адресов из контрактов
2		TAB	Разделитель
3	`24372`	Любая комбинация цифр и прописных и строчных латинских букв (не более 16 символов)	**Примечание.** Данное поле в случае с командой **remove** требуется исключительно для её правильной интерпретации обработчиком команд. Можно указать любое значение.
4		TAB	Разделитель
5	`{oid}`	Строка 5 символов	Тип контракта (в нашем случае всегда фиксированная строка '{oid}')
6		SPACE	Разделитель
7	`LIM10M`	Строка: LIM значение скорости K/M/G (килобит/мегабит/гигабит) или UNLIM	**Примечание.** Данное поле в случае с командой **remove** требуется исключительно для её правильной интерпретации обработчиком команд. Можно указать любое значение.
8	`/`	Символ '/'	Разделитель
9	`LIM10M`	строка	**Примечание.** Данное поле в случае с командой **remove** требуется исключительно для её правильной интерпретации обработчиком команд. Можно указать любое значение.
10		SPACE	Разделитель пробел
11	`10.21.0.208,`	IP адрес, разделитель‘,’	IP-адрес абонента. Можно указать несколько адресов через запятую.
12		LF	Конец строки запроса

11.8.5 Команда killcontract

Команда **killcontract** позволяет деавторизовать всех абонентов, привязанных к определённому контракту.

```
B: killcontract 24372 {oid}
E:
```

Синтаксис команды описан в таблице ниже.

Таблица 36

№	Поле	Содержание поля	Описание поля
1	`killcontract`	12 символов	Команда деавторизации всех абонентов, привязанных к контракту
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

№	Поле	Содержание поля	Описание поля
			всегда фиксированная строка '{oid}')

11.8.6 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
```

11.8.7 Команда clearall

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

11.9 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 37

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>] | <имя_политики> | all }	Вывод подробной или краткой информации об абонентских сессиях. Аргументами команды могут быть IP-адрес, диапазон IP-адресов, имя политики 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

11.9.1 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, продолжительность сессии и статистика принятых и отправленных байтов и пакетов. Если в контракте есть абоненты IPv6, использующие делегированные префиксы, то эти префиксы будут включены в вывод команды, если соответствующие атрибуты Delegated-IPv6-Prefix были получены от RADIUS-сервера. Для общего контракта также выводится сводная статистика байтов и пакетов по всем абонентам данного контракта. Ниже дан пример выводимой информации для общего контракта.

```
EcoSGE:# show brascontract shared1
Shared    192.168.55.6   Authorized  2m30s   Bytes rx/tx:
7832582/115571751; Packets rx/tx: 45613/119596
Shared    192.168.55.7   Authorized  1m45s   Bytes rx/tx:
7951843/99673922; Packets rx/tx: 47917/199925
Shared    192.168.55.5   Authorized  3m20s   Bytes rx/tx:
7595493/95415626; Packets rx/tx: 49795/92433
Shared      3001::2     Authorized  1m15s    Bytes rx/tx: 0/0; Packets
rx/tx: 0/0
Shared      3001::1     Authorized  1m50s    Bytes rx/tx: 0/0; Packets
rx/tx: 0/0
Delegated IPv6 Prefixes:
3001:db8:1101::/48
3400:ca00:3000:240::/60
============================ Shared Configuration
============================
Current service: "servicesh2" (Enabled)
Configured data rate upstream                          1022 Kb/s
Configured data rate downstream                        1022 Kb/s
Policer byte drop upstream/downstream                            0/6083734
Policer packet drop upstream/downstream                             0/4019
Bytes downstream                              23379918
Bytes upstream                               328286141
Packets downstream                              133335
Packets upstream                                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>] | <имя_политики> | all }**

Данная команда, в зависимости от аргумента, выводит подробную или краткую информацию об абонентских сессиях. Аргументами команды могут быть IP-адрес, диапазон IP-адресов, имя политики 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   1m30s  Bytes rx/tx: 0/60; Packets rx/tx: 0/1
10.210.1.234   Authorized   3m20s  Bytes rx/tx: 0/60; Packets rx/tx: 0/1
10.210.1.89   Authorized   4m15s  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 1.2.3.4
Bras info for address 1.2.3.4:
================================================================================
======
Subscriber 1.2.3.4
Contract qq0
Origin RADIUS
Mac 11:11:11:11:11:11
Main TTL 12
Policy policyd
================================================================================
======
Status                                  Authorized
Accounting status                            Start
Configured data rate upstream total                    unlim Kb/s
Configured data rate downstream total                   unlim Kb/s
Policer byte drop upstream/downstream total              0/3185938
Policer packet drop upstream/downstream total               0/2105
Bytes upstream total                          471087
Bytes downstream total                        17246003
Packets upstream total                           6605
Packets downstream total                         11436
Session uptime                               158 s
Session timeout expires in                        10961 s
Idle timeout expires in                         28728 s
Interim interval expires in                        0 s
--------------------------------------------------------------------------------
------
Shared service: "servicesh2" (Enabled)
Configured data rate upstream                        4999 Kb/s
Configured data rate downstream                       4999 Kb/s
Policer byte drop upstream/downstream                 0/6083734
Policer packet drop upstream/downstream                  0/4019
Bytes upstream                               839948
Bytes downstream                              25460597
```

```
Packets upstream                              11657
Packets downstream                             16880
------------------------------------------------------------------------
------
1. "servicea" (Enabled)
Configured data rate upstream                        unlim Kb/s
Configured data rate downstream                       unlim Kb/s
Policer byte drop upstream/downstream                      0/0
Policer packet drop upstream/downstream                    0/0
Bytes upstream                                471087
Bytes downstream                              14060065
Packets upstream                                6605
Packets downstream                              9331
```

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 38

Поле	Описание
Status	Статус абонента
Accounting status	
Configured data rate upstream total	Установленные для абонента ограничения пропускной способности исходящего канала (кбит/с)
Configured data rate downstream total	Установленные для абонента ограничения пропускной способности входящего канала (кбит/с)
Policer byte drop upstream/downstream total	Количество отброшенных исходящих/входящих байтов, которые не удалось обработать при установленных ограничениях скорости передачи
Policer packet drop upstream/downstream total	Количество отброшенных исходящих/входящих пакетов, которые не удалось обработать при установленных ограничениях скорости передачи
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 uptime	Продолжительность сессии в секундах
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

Поле	Описание
Информация о сервисах	
Enabled/Disabled	Состояние сервиса: включен/выключен
Configured data rate upstream	Установленные сервисом ограничения ограничения пропускной способности исходящего канала (кбит/с)
Configured data rate downstream	Установленные сервисом ограничения ограничения пропускной способности входящего канала (кбит/с)
Policer byte drop upstream/downstream	Количество отброшенных исходящих/входящих байтов, которые не удалось обработать в данном сервисе при установленных ограничениях скорости передачи
Policer packet drop upstream/downstream	Количество отброшенных исходящих/входящих пакетов, которые не удалось обработать в данном сервисе при установленных ограничениях скорости передачи
Bytes downstream	Количество байтов, полученных абонентом
Bytes upstream	Количество байтов, отправленных абонентом
Packets downstream	Количество пакетов, полученных абонентом
Packets upstream	Количество пакетов, отправленных абонентом

Пример вывода **show brasinfo** для групповой статической политики (static_shared):

```
EcoSGE:# show brasinfo policy1
Bras info for policy policy1:
================================================================================
======
Subscriber policy1
Contract Undefined
Mac 00:00:00:00:00:00
Policy policy1
================================================================================
======
Status                                  Authorized
Accounting status                            Alive
Configured data rate upstream total                    unlim Kb/s
Configured data rate downstream total                   unlim Kb/s
Policer byte drop upstream/downstream total               0/102952
Policer packet drop upstream/downstream total                0/68
Bytes upstream total                              26508
Bytes downstream total                            699468
Packets upstream total                              394
Packets downstream total                             462
Session timeout expires in                           86393 s
Idle timeout expires in                             28800 s
Interim interval expires in                            53 s
--------------------------------------------------------------------------------
------
Common service: "serviceTotal" (Enabled)
Configured data rate upstream                          4999 Kb/s
Configured data rate downstream                         4999 Kb/s
Policer byte drop upstream/downstream                      0/0
Policer packet drop upstream/downstream                     0/0
Bytes upstream                                  26508
Bytes downstream                                699468
Packets upstream                                  394
```

```
Packets downstream                                462
------------------------------------------------------------------------
------
1. "service1" (Enabled)
Configured data rate upstream                        999 Kb/s
Configured data rate downstream                       999 Kb/s
Policer byte drop upstream/downstream                  0/102952
Policer packet drop upstream/downstream                   0/68
Bytes upstream                                 26508
Bytes downstream                               596516
Packets upstream                                 394
Packets downstream                                394
------------------------------------------------------------------------
------
2. "service2" (Enabled)
Configured data rate upstream                        1999 Kb/s
Configured data rate downstream                       1999 Kb/s
Policer byte drop upstream/downstream                    0/0
Policer packet drop upstream/downstream                   0/0
Bytes upstream                                    0
Bytes downstream                                   0
Packets upstream                                   0
Packets downstream                                  0
```

- **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
=========================================================
Shared contract stats:
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**).

11.9.2 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.

11.9.3 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.

11.10 Сервисная консоль BRAS

На TCP-порту 2226 управляющего интерфейса EcoSGE доступна сервисная консоль BRAS, которая позволяет быстро узнать параметры BRAS для абонента по IP-адресу или номеру контракта. Ниже дан пример подключения к сервисной консоли и запроса информации об абоненте по IP-адресу.

```
$ telnet 2.2.2.2 2226
Trying 2.2.2.2...
Connected to 2.2.2.2.
Escape character is '^]'.
Start connection...
Please use next commands:
ip ADDRESS - for show information about address contract
NUMBER - for show information about contract
> ip 10.210.0.81
IP => 5100d20a
Contract number = 54174
Upload speed limit = 102400 KB
Download speed limit = 102400 KB
>
```

12 Подсистема DPI

Подсистема DPI позволяет операторам связи и интернет-провайдерам выполнять требования Федерального закона № 139-ФЗ от 28 июля 2012 года, касающиеся ограничения и блокирования доступа к нежелательным и запрещённым ресурсам в сети Интернет, а также оказывать услуги типа «детский интернет». Данная функциональность соответствует всем требованиям и прошла тестирование Роскомнадзора (официальное заключение доступно по ссылке).

Функциональность DPI доступна при наличии лицензии EcoDPIxxxx-LIC. Информация об установленных лицензиях выводится командой **show license** (см. раздел "Информация о версии ПО и установленных лицензиях").

Фильтрация трафика может производиться по Единому реестру Роскомнадзора (РКН), пользовательским спискам интернет-ресурсов и/или сетевым протоколам.

В стандартной конфигурации поддерживаются до 25 настраиваемых DPI-списков, каждый из которых может быть либо чёрным (список запрещённых ресурсов), либо белым (список разрешённых ресурсов). По требованию заказчика количество поддерживаемых DPI-списков может быть увеличено (максимум – 1000).

В каждом DPI-списке можно настроить перенаправление на страницу блокировки («доступ к ресурсу запрещён»). Поддерживается фильтрация по подсетям.

Для HTTPS и QUIC version 1 (RFC 9000) 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 для HTTPS проверяется входящий сертификат сервера, на который был отправлен запрос. Если в сертификате указан запрещённый фильтрами ресурс, то соединение с сервером разрывается.

Возможна фильтрация трафика одновременно по нескольким DPI-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 или QUIC 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.

12.1 Создание и настройка DPI-списков

Настройка подсистемы DPI производится в ветке **system.dpi**. Включение и выключение подсистемы DPI производится непосредственно в ветке **system.dpi** командами **enable** и **disable** соответственно.

В заводской конфигурации ветка **system.dpi** имеет следующий вид:

```
EcoSGE:system.dpi# ls
disable
functionality_mode normal_nat
rkn
{
  source rkn
  login ""
  password ""
  list_number none
  list_number_soc none
  proxy ""
  upload_dump_server ""
}
revisors ( )
shortlist
{
  disable
  timeskew utc
  server_ip_and_port 0.0.0.0:0
}
block_fast_response on
blocked_session_timeout
{
  tcp 300
  udp 300
  icmp 60
  other 300
}
```

В таблице ниже описаны параметры ветки **system.dpi** в заводской конфигурации.

Таблица 39

Параметр	Описание
{ enable | disable }	Состояние подсистемы DPI: включена (enable) или выключена (disable)
functionality_mode	Режим работы в зависимости от схемы подключения EcoSGE: • **normal_nat** для схемы "в разрыв"; • **double_mirrored_traffic** для схемы с зеркалированием. Подробная информация содержится в разделе "Зависимость работы EcoSGE от схемы подключения"
rkn	Подгруппа параметров для настройки фильтрации по реестру Роскомнадзора
shortlist	Подгруппа параметров для настройки логирования срабатывания DPI-списков (см. раздел "Shortlist")
block_fast_response	Включение/выключение обработки незапрошенных HTTP-ответов (см. раздел "Обработка незапрошенных HTTP-ответов")
blocked_session_timeout { tcp | udp | icmp | other } <value>	Позволяет задать тайм-ауты в секундах для заблокированных сессий TCP, UDP, ICMP и других протоколов, инкапсулированных в IP (подгруппа "Other"). По истечении тайм-аута заблокированная сессия будет закрыта, а соответствующая ей запись будет удалена из общей таблицы сессий

В заводской конфигурации ветка **system.dpi** не содержит параметров, определяющих то, с каких IP-адресов подсистема DPI должна анализировать трафик и какие действия выполнять

при обнаружении этого трафика. Поэтому необходимо создать один или несколько DPI-списков.

Для создания DPI-списка необходимо отправить команду **create dpilist N**, где N – номер из установленного диапазона (в стандартной конфигурации – от 0 до 24; по требованию заказчика количество поддерживаемых DPI-списков может быть увеличено; максимум – 1000). После выполнения данной команды (например, **create dpilist 0**) в ветку **system.dpi** будет добавлена дочерняя ветка **dpilistN** со следующим набором параметров:

```
EcoSGE:system.dpi# ls
...
dpilist0
{
 disable
 whitelist_mode off
 log_matches off
 log_pictures off
 exceptions off
 direction egress
 behaviour block
 redirect_use_interval off
 redirect_interval 600
 redirect_interval_url 2592000
 redirect_url " "
 tls_esni_match on
 color_direction both
 color_tos_byte 32
 download_url " "
 update_schedule never
 protocols ( )
 quic_sni_match off
 acl none
 aclv6 none
}
```

Любой DPI-список можно отдельно включить или выключить командами **enable** и **disable**, выполненными в ветке его параметров.

При создании и настройке нескольких DPI-списков следует помнить, что они применяются в порядке убывания приоритета (возрастания номера).

Для удаления DPI-списка необходимо отправить команду **no dpilist N**, где N – номер от 0 до 24.

В таблице ниже дано описание параметров DPI-списка.

Таблица 40

Параметр	Описание
enable / disable	Определяет состояние списка: enable – включён, disable – выключен
whitelist_mode	Задаёт тип загружаемого списка интернет-ресурсов (см. параметр **download_url** ниже). Чёрный список (значение **off**) определяет, к каким ресурсам доступ запрещён. Белый список (значение **on**), наоборот, разрешает доступ только к перечисленным ресурсам и, например, может быть использован для организации «детского интернета».

Параметр	Описание
	Белый список может содержать только IP-адреса, только URL или IP-адреса и URL. Если список содержит IP-адреса и URL, то для каждого URL должен быть прописан соответствующий IP-адрес (адреса), в который он будет преобразовываться. Если список содержит только URL, то IP-адреса прописывать не надо.
log_matches	Определяет, будет ли выполняться логирование обращений к запрещённым адресам. Значения: **on**, **off**
log_pictures	Определяет, будет ли выполняться логирование изображений на сайтах. Учитываются форматы *.bmp, *.gif, *.jpeg, *.jpg, *.png, *.tif, *.tiff. Значения: **on**, **off**
exceptions	Применяет список исключений к данному DPI-списку. Значения: **on**, **off**. См. раздел "Настройка исключений".
direction	Определяет, на каком направлении необходимо анализировать трафик. Возможные значения: • **egress** – исходящий трафик (LAN → WAN, по умолчанию); • **ingress** – входящий трафик (WAN → LAN); • **both** – анализировать трафик на обоих направлениях
behaviour	Определяет действие, применяемое к трафику при срабатывании условия чёрного списка или несрабатывании условия белого списка: • **block** – блокировка HTTPS и HTTP; перенаправление HTTP, если задан параметр **redirect_url**; сессия сразу помечается как подлежащая удалению; • **redirect** – перенаправление HTTP (обязательно должен быть задан параметр **redirect_url**), пропускание HTTPS; • **drop** – блокировка HTTPS и HTTP без отправки пакетов TCP RST и перенаправления; сессия не помечается как подлежащая удалению сразу, и для неё продолжает действовать соответствующий тайм-аут, заданный в ветке конфигурации **system.nat_defaults**; • **color** – маркировка (DiffServ); • **ignore** – не применять никаких действий. Трафик поступит на анализ в следующий по приоритету DPI-список (при его наличии). Если других DPI-списков нет, то трафик сразу передаётся дальше в сеть; • **pass** – не применять никаких действий. Трафик сразу передаётся дальше в сеть. Остальные DPI-списки игнорируются.
redirect_use_interval	Включает использование таймеров перенаправления. При выключении этого параметра перенаправление будет выполняться при каждой попытке зайти на любой адрес из списка. Значения: **on**, **off**
redirect_interval	Интервал между перенаправлениями для сайтов из 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, куда будет перенаправлено HTTP-соединение, если условие списка сработало (для чёрного списка) или не сработало (для белого списка). EcoSGE позволяет добавлять в адресную строку спецификаторы, указывающие на клиента. Что позволяет персонализировать страницу переадресации.

Параметр	Описание
	Возможные спецификаторы: **%c** – передавать в redirect_url callback-id, полученный от RADIUS-сервера; **%m** – передавать в redirect_url mac адрес клиента; **%i** – передавать в redirect_url ip адрес клиента; **%v1** – передавать в redirect_url первый (верхний) vlan клиента; **%v2** – передавать в redirect_url второй (нижний) vlan клиента; **%u** – передавать в redirect_url url, на который обратился клиент. Формат ввода параметра **redirect_url**: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>=<SPEC2>..<VAR_NAMEN>=<SPECN>** где **URL** – адрес страницы, на которую осуществляется перенаправление, **VAR_NAME1** .. **VAR_NAMEN** – имя переменной, **SPEC1** .. **SPECN** – спецификатор. Например, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. Если при таком значении параметра клиент попробует обратиться на адрес **forbidden.com**, то он будет перенаправлен на адрес: **http://example.com/?var1=forbidden.com&ip=10.1.1.10&qwe=0**
tls_esni_match	Включение (**on**) / выключение (**off**) распознавания TLS-пакетов с полем ESNI (Encrypted SNI) в заголовке. По умолчанию включено
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 выгружаться список интернет-ресурсов в случае автообновления (поддерживаются протоколы HTTP, HTTPS, FTP, TFTP). Для DPI-списка, используемого для фильтрации по реестру РКН, – адрес, по которому будет храниться предварительно скачанный реестр РКН. Для работы по HTTPS требуется локальный SSL-сертификат и его привязка к адресу сервера (см. "Хранилище сертификатов SSL")
update_schedule	Периодичность автоматического обновления списка интернет-ресурсов. Возможные значения: **never** – никогда не обновлять, **interval <SECONDS>** – периодичность в секундах. Не рекомендуется задавать значения меньше 300.
protocols ( )	Обрабатываемые протоколы (см. раздел "Фильтрация протоколов"). Можно указать несколько протоколов через пробел
quic_sni_match	Включение (**on**) / выключение (**off**) фильтрации трафика QUIC на основании SNI из загруженного списка фильтрации. По умолчанию **off**.

Параметр	Описание
acl aclv6	ACL для трафика IPv4 и IPv6 соответственно. К трафику, который соответствует разрешающим правилам ACL, будут применяться действия, указанные в настройках данного DPI-списка. Трафик, соответствующий запрещающим правилам ACL, будет отправлен на анализ в следующий по приоритету DPI-список. Если других DPI-списков нет, то трафик будет передан дальше в сеть. По умолчанию обоим параметрам присвоено значение **none**. Это значение равносильно разрешающему правилу ACL **permit ip any any**, т. е. заданные действия DPI-списка будут применяться ко всему трафику.

12.2 Фильтрация по реестру Роскомнадзора

В данном разделе описана настройка подсистемы DPI для фильтрации трафика по реестрам Роскомнадзора.

12.2.1 Фильтрация по единому реестру запрещённых ресурсов и реестру социально значимых ресурсов

Для фильтрации трафика по единому реестру запрещённых ресурсов и/или реестру социально значимых ресурсов Роскомнадзора (РКН) необходимо привязать созданный, настроенный и включённый DPI-список к настройкам доступа к сервису выгрузки реестра РКН. Эти настройки находятся в ветке **system.dpi.rkn** и включают в себя параметры, описанные в таблице ниже.

Таблица 41

Параметр	Описание
source	Источник для выгрузки реестра РКН: • **rkn** – сервер Роскомнадзора, • **grfc** – сервер ГРЧЦ (ФГУП "Главный Радиочастотный Центр"); только для загрузки реестра запрещённых ресурсов
login	Логин для доступа к сервису выгрузки реестра РКН, полученный на портале https://service.rkn.gov.ru/monitoring/vigruzka
password { text <string> | hash <hex string> }	Пароль для доступа к сервису выгрузки реестра РКН, полученный на портале https://service.rkn.gov.ru/monitoring/vigruzka. Можно указать в текстовом или хешированном виде. После указания пароля в текстовом виде производится его хеширование
list_number	Номер DPI-списка, который должен использоваться для фильтрации по реестру запрещённых ресурсов РКН. Допустимые значения – от 0 до 24. Можно назначить только один DPI-список
list_number_soc	Номер DPI-списка, который должен использоваться для фильтрации по реестру социально значимых ресурсов РКН. Допустимые значения – от 0 до 24. Можно назначить только один DPI-список
proxy	Прокси-сервер, используемый для автоматической загрузки реестра РКН (см. раздел "Автоматическая загрузка реестра Роскомнадзора"). Необязательный параметр.

Параметр	Описание
	Указывается в формате * **[<PROTOCOL>://][<USER>:<PASSWORD>@]<HOST>[:<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; • **HOST** – IP-адрес или доменное имя прокси-сервера; обязательный параметр; • **PORT** – порт прокси-сервера; если не указан, то используется TCP-порт 1080. * В квадратных скобках указаны необязательные параметры.
upload_dump_server	FTP/TFTP-сервер, на который EcoSGE будет автоматически выгружать скачанный файл реестра РКН вместе с дифференциальными обновлениями. Необязательный параметр. Подробная информация содержится в разделе "Выгрузка файла реестра Роскомнадзора на FTP/TFTP-сервер". Указывается в формате * **<PROTOCOL>://[<USER>:<PASSWORD>@]<HOST>[:<PORT>][/<PATH>]**, где: • **PROTOCOL** – протокол: **ftp** или **tftp**. Обязательный параметр; • **USER:PASSWORD** – имя пользователя и пароль через двоеточие. Указываются, 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 сохранения и имя файла. Указанная структура каталогов должна быть создана на сервере заранее. По умолчанию файл будет сохранён в корневом каталоге FTP/TFTP-сервера; имя файла – **dumps.tar.gz**. * В квадратных скобках указаны необязательные параметры.

После задания всех требуемых параметров необходимо применить настройки командой **apply**.

Если в DPI-списке настроено автоматическое обновление (**update_schedule <секунды>**), то после команды **apply** будет выполнена загрузка файла реестра запрещённых ресурсов **dump.xml** и/или реестра социально значимых ресурсов **dumpsoc.xml**, а также дифференциальных обновлений. Из загруженных данных будет сформирован файл **listN.dpi** (где N – значение параметра **list_number** или **list_number_soc**). Наличие данных файлов можно проверить командой **dpilist**. При отключенном автоматическом обновлении (**update_schedule never**) потребуется вручную загрузить файл реестра запрещённых ресурсов **dump.xml** и/или реестра социально значимых ресурсов **dumpsoc.xml** (см. раздел "Ручная загрузка реестра Роскомнадзора"), после чего отправить команду **dpirun** для формирования файла listN.dpi.

Если DPI-списки с номерами, указанными в параметрах **list_number** или **list_number_soc**, не созданы, то в ответ на команду **apply** будет выведено сообщение об ошибке "DPI list for RKN (N) is missing", и конфигурация не будет применена. При совпадении номеров будет выведено сообщение об ошибке "RKN list and social RKN dump have the same list number", и команда **apply** также не будет выполнена.

Чтобы назначить для фильтрации по реестру РКН другой DPI-список, достаточно:

1. Создать новый DPI-список.
2. Указать его номер в параметре **list_number** или **list_number_soc**.
3. Применить настройки командой **apply**.

Будет создан новый файл listN.dpi, в который будут перенесены все данные из старого файла. Если в использовавшемся ранее DPI-списке не задан параметр **download_url**, то старый файл listN.dpi будет удалён.

12.2.2 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 неанонимные прокси-серверы. Прокси-сервер можно использовать как с методом загрузки реестра полностью, так и с методом дельта-пакетов. Для включения функционала необходимо в параметре **proxy** секции **system.dpi.rkn** указать прокси-сервер в формате* **[<PROTOCOL>://|[<USER>:<PASSWORD>@]<HOST>[:<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;
- **HOST** – IP-адрес или доменное имя прокси-сервера; обязательный параметр;
- **PORT** – порт прокси-сервера; если не указан, то используется TCP-порт 1080.

* В квадратных скобках указаны необязательные параметры.

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

12.2.2.1 Авторизация по логину

Для включения автоматической загрузки реестра Роскомнадзора по логину/паролю в настройках **system.dpi.rkn** должны быть указаны значения соответствующих параметров **login** и **password**. 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_schedule 60** (ежеминутная загрузка).

12.2.2.2 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 HTTP/FTP-сервере.

12.2.3 Ручная загрузка реестра Роскомнадзора

Ручная загрузка реестра Роскомнадзора (РКН) возможна как с сервера РКН или ГРЧЦ, так и с пользовательского HTTP/FTP-сервера.

Для ручной загрузки реестра запрещённых ресурсов и реестра социально значимых ресурсов с сервера РКН или ГРЧЦ предусмотрено несколько команд, описание которых дано в таблице ниже. Предварительно необходимо настроить доступ к серверу РКН и/или ГРЧЦ в ветке конфигурации **system.dpi.rkn**.

Таблица 42

Команда	Действие
dpiload <list_number>	Загрузка реестра запрещённых ресурсов с сервера РКН или ГРЧЦ в DPI-список с номером, указанным в параметре **list_number** в ветке **system.dpi.rkn**. Если сервер РКН или ГРЧЦ недоступен, и при этом в настройках DPI-списка задан параметр **download_url**, то загрузка будет производиться с URL, указанного в данном параметре.
dpiload dump	Аналогично команде **dpiload <list_number>**
dpiload delta	Загрузка дифференциальных обновлений реестра запрещённых ресурсов с сервера РКН или ГРЧЦ в DPI-список с номером, указанным в параметре **list_number** в ветке **system.dpi.rkn**. Если предварительно не загружен основной файл реестра dump.xml, то действие команды аналогично **dpiload <list_number>** и **dpiload dump**
dpiload <list_number_soc>	Загрузка реестра социально значимых ресурсов с сервера РКН в DPI-список с номером, указанным в параметре **list_number_soc** в ветке **system.dpi.rkn**. Если сервер РКН недоступен, и при этом в настройках DPI-списка задан параметр **download_url**, то загрузка будет производиться с URL, указанного в данном параметре.
dpiload dumpsoc	Аналогично команде **dpiload <list_number_soc>**

Команда для ручной загрузки реестра РКН с пользовательского HTTP/HTTPS/FTP-сервера имеет вид **dpiload <list_number> <URL>**, где **URL** указывается в формате **{ http | https | ftp }://<адрес сервера>/<путь к файлу>**. Для загрузки по HTTPS требуется локальный SSL-сертификат и его привязка к адресу сервера (см. "Хранилище сертификатов SSL").

Поддерживается базовая аутентификация на серверах. Синтаксис команды загрузки с использованием аутентификации:

dpiload <list_number> { http | https | ftp }://<имя пользователя>:<пароль>@<адрес сервера>/<путь к файлу>

Например, для загрузки с HTTP-сервера **1.1.1.1** файла реестра РКН **dump.xml** в DPI-список **0** требуется зайти на сервер под именем **username** с вводом пароля **password**. В этом случае команда загрузки будет иметь вид:

```
EcoSGE:system.dpi# dpiload 0 http://username:password@1.1.1.1/dump.xml
```

Примеры выполнения команд:

```
EcoSGE:system.dpi# dpiload 0
list0 will be updated soon
EcoSGE: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
EcoSGE: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
```

Для вывода списка загруженных файлов, используемых в работе URL-фильтрации, необходимо отправить команду **dpilist** (см. раздел "Команды для работы со списками фильтрации").

12.2.4 Выгрузка файла реестра Роскомнадзора на FTP/TFTP-сервер

12.2.4.1 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 43

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

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

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

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

```
Actual last dump is X
```

12.2.4.2 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:

1. После добавления сервера в параметр **upload_dump_server** имеющийся **dump.xml** и дельты удаляются.
2. **dump.xml** скачивается полностью, после чего сразу же копируется на сервер в формате Роскомнадзора (XML-файл сжатый ZIP).
3. 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

12.3 Фильтрация по пользовательским спискам

В данном разделе описана настройка подсистемы DPI для фильтрации трафика по пользовательским спискам интернет-ресурсов.

12.3.1 Подготовка списков фильтрации

Пользовательский список фильтрации должен представлять собой простой текстовый файл, который может содержать:

- URL,
- отдельные адреса IPv4 и IPv6,
- диапазоны адресов IPv4,
- подсети IPv4 и IPv6,
- Perl-совместимые регулярные выражения (PCRE).

При подготовке файла со списком фильтрации необходимо учитывать следующее:

1. Каждая запись (URL, IP-адрес и др.) должна быть представлена отдельной строкой. Разделителем строк в файле должен быть управляющий символ CR или CR LF.
2. URL можно указать со схемой (“http://” или “https://”) или без неё. URL без схемы означает, что в списке он присутствует с обеими схемами. При этом фильтр для HTTPS-соединений будет учитывать только доменное имя в URL. То есть при указанном в примере ниже написании ссылки на статью Википедии будут блокироваться все соединения с русскоязычной версией Википедии. Таким образом, если требуется закрыть доступ только к одной статье, то в списке должно быть указано “http://ru.wikipedia.org/wiki/GRE_(протокол)”

3. В записи URL можно использовать замещающий символ '*' (звёздочка), который означает любое количество символов доменного имени от первого до какой-либо точки. Например, можно указать ***.example.ru** или ***.org**, но нельзя указать **www.*.com**. 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://”.
4. IPv6-адреса необходимо указывать в квадратных скобках.
5. IP-адреса можно указывать в связке с портом или диапазоном портов.
6. Перед регулярным выражением необходимо ставить знак **'~'** (тильда). Например, **~^((http|https|ftp):\/\/)?.*\.qwe\..*$**. В противном случае регулярное выражение не будет идентифицировано подсистемой DPI при обработке загруженного файла.
7. Нельзя указывать IP-адреса в виде регулярных выражений.
8. Имя и расширение файла не регламентированы.
9. Можно использовать комментарии. Например, для именования групп записей. Каждая строка комментария должна начинаться с символа **'#'** (решётка). Этим же символом можно при необходимости "закомментировать" определённые строки в списке, чтобы они не обрабатывались при построении или обновлении базы данных.

Пример содержимого файла:

```
# URLs
http://www.badsite.com:8080/badpath.htm
http://flibusta.net
https://*.example.ru
*.badsite.ru
http://vk.com
ru.wikipedia.org/wiki/GRE_(протокол)
# ip
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
# PCRE
~^((http|https|ftp):\/\/)?.*\.boo\..*$
```

12.3.2 Автоматическая загрузка списков фильтрации

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

12.3.3 Ручная загрузка списков фильтрации

Ручная загрузка пользовательских списков фильтрации производится командой **dpiload <номер DPI-списка> <URL>**, где **URL** указывается в формате **{ http | https | ftp }://<адрес сервера>/<путь к файлу>**. Для загрузки по HTTPS требуется локальный SSL-сертификат и его привязка к адресу сервера (см. "Хранилище сертификатов SSL"). Содержимое файла со списком фильтрации описано в разделе "Подготовка списков фильтрации".

Поддерживается базовая аутентификация на серверах. Синтаксис команды загрузки с использованием аутентификации:

dpiload <номер DPI-списка> { http | https | ftp }://<имя пользователя>:<пароль>@<адрес сервера>/<путь к файлу>

Например, для загрузки с HTTP-сервера **1.1.1.1** списка фильтрации **black_list.txt** в DPI-список **1** требуется зайти на сервер под именем **username** с вводом пароля **password**. В этом случае команда загрузки будет иметь вид:

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

Предварительно рекомендуется отключить автоматическое обновление списка фильтрации, задав в настройках DPI-списка **update_schedule never**.

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

Для вывода списка загруженных файлов, используемых в работе URL-фильтрации, необходимо отправить команду **dpilist** (см. раздел "Команды для работы со списками фильтрации").

12.4 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 44

Номер 10-ричный	Номер 16-ричный	Категория
1	1	Алкоголь

Номер 10-ричный	Номер 16-ричный	Категория
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
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

Номер 10-ричный	Номер 16-ричный	Категория
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	Вождение 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
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 (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
```

12.5 Фильтрация по базе SkyDNS

В системе EcoSGE реализована возможность URL-фильтрации по базе категорированных ресурсов SkyDNS. 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 45

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 загрузки базы вручную предусмотрена команда **dpiload skydns**

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

1. Создать и настроить ACL и пул для трафика, подлежащего обработке (см. разделы "Создание и настройка пула" и "Создание 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"
acl acla
behaviour redirect
go dpi
enable
```

12.6 Обновление внутренней базы фильтрации

Все загруженные задействованные списки фильтрации объединяются в единую внутреннюю базу фильтрации. Если настроена автоматическая загрузка списков, то процесс обновления внутренней базы фильтрации начинается сразу после загрузки списков. Если загрузка списков фильтрации производится вручную, то после их загрузки необходимо принудительно запустить процесс обновления внутренней базы фильтрации с помощью команды **dpirun**.

Внимание! Продолжительность обновления внутренней базы фильтрации зависит от общего количества записей в загруженных списках. До завершения обновления будет использоваться текущая версия базы.

12.7 Настройка исключений

При необходимости для DPI-списков можно настроить исключения.

Для того чтобы добавить исключения, необходимо сформировать текстовый файл со списком ресурсов-исключений, аналогично тому, как описано в разделе "Подготовка списков фильтрации". После чего файл загружается вручную командой **dpiload exception <URL>,** где **URL** вводится в формате **http://<адрес сервера>/<имя файла>.<расширение файла>**. Далее необходимо активировать исключения в DPI-списке, к которому они будут применяться, задав значение **on** для параметра **exceptions**. Доступ к ресурсам из списка исключений будет запрещён, если исключения применяются к белому списку, или разрешён, если исключения применяются к чёрному списку.

Пример настройки DPI-списка:

```
EcoSGE: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
acl ( aclmain )
```

12.8 Фильтрация абонентского трафика, к которому не применяется NAT

По умолчанию подсистема DPI выполняет фильтрацию трафика только тех абонентов, IP-адреса которых попадают в какой-либо из пулов NAT.

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

Создать новый пул NAT.

```
MyEcoNAT:1:# create pool url
```

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 url
```

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.*

12.9 Команды для работы со списками фильтрации

12.9.1 dpilist

Для просмотра загруженных списков фильтрации и прочих файлов, необходимых для работы 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
```

12.9.2 show dpirecords

Команда выводит записи определённого списка фильтрации.

Синтаксис команды: **show dpirecords <номер списка>**

Для данной команды предусмотрена возможность фильтрации вывода (см. раздел "Фильтрация вывода команд группы Show".

Пример вывода команды:

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

12.9.3 dpiview

Команда выводит записи из списка фильтрации или содержимое файлов, использующихся при настройке фильтрации.

Синтаксис команды: **dpiview <номер DPI-списка или имя файла>**. Команда не поддерживает опции после символа **|** (вертикальная черта) и прерывание вывода. Можно также указывать следующие файлы:

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

и другие файлы (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>1111111111111</ogrn>
<email>mail@domen.ru</email>
</request>
```

12.9.4 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.

Предусмотрена возможность поиска по маске. Для этого в команде следует использовать символ '*****', который будет интерпретирован как набор любых символов до какой-либо точки в URL или IP-адресе. Например, **show dpimatch *.example.com** или **show dpimatch *.100.10.1**.

Примечание. Поиск по маске отрабатывает только по записям со схемой 'https://' или без схемы.

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
------------------------------
```

Для удаления списков или файлов, используемых при настройке URL-фильтрации, используется команда **dpierase <номер DPI-списка или имя файла>**.

Удаление всех файлов ***.dpi** из базы фильтрации производится командой **dpierase all**.

12.9.5 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
Last RKN update time: no request yet
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 46

Строка	Описание

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
Last RKN update time	Дата и время последнего успешного обращения к серверу РКН. Регистрируется даже при отсутствии очередных обновлений на сервере
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**.

12.10 Настройка периодического перенаправления

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

Настройка периодического перенаправления пользователей работает только для HTTP. При использовании HTTPS соединение будет установлено без перенаправления.

Для настройки периодических перенаправлений, в соответствующий **dpilist** должен быть вручную загружен список ресурсов, для которых необходимо осуществлять перенаправление.

Подробнее о формировании и загрузке такого списка, см. в разделе "Подготовка списков фильтрации".

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.

В таблице ниже указаны параметры, которые необходимо задать в DPI-списке, чтобы срабатывало периодическое перенаправление.

Таблица 47

Параметр	Описание
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.

Параметр	Описание
	Возможные спецификаторы: **%c** – передавать в redirect_url callback-id, полученный от RADIUS-сервера; **%m** – передавать в redirect_url mac адрес клиента; **%i** – передавать в redirect_url ip адрес клиента; **%v1** – передавать в redirect_url первый (верхний) vlan клиента; **%v2** – передавать в redirect_url второй (нижний) vlan клиента; **%u** – передавать в redirect_url url, на который обратился клиент. Формат ввода параметра **redirect_url**: **<URL>/?<VAR_NAME1>=<SPEC1>&<VAR_NAME2>= <SPEC2>..<VAR_NAMEN>=<SPECN>** где **URL** – адрес страницы, на которую осуществляется перенаправление, **VAR_NAME1** .. **VAR_NAMEN** – имя переменной, **SPEC1** .. **SPECN** – спецификатор. Например, **http://example.com/?var1=%u&ip=%i&qwe=%v2**. Если при таком значении параметра клиент попробует обратиться на адрес **forbidden.com**, то он будет перенаправлен на адрес: **http://example.com/?var1= forbidden.com&ip=10.1.1.10&qwe=0**

Пример настройки списка:

```
MyEcoNAT:2:system.dpi# show
enable
functionality_mode normal_nat
certificate_file "cert.pem"
…
dpilist1
{
 enable
 whitelist_mode off
 log_matches on
 exceptions off
 behaviour redirect
 redirect_use_interval on
 redirect_interval 600
 redirect_interval_url 2592000
 redirect_url "http://redirect.domen.ru/"
 color_direction both
 color_tos_byte 32
 download_url ""
 update_schedule never
 no_ip ( )
```

```
 ip ( 0.0.0.0/0 )
}
```

12.11 Shortlist

12.11.1 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 "Подготовка списков фильтрации". 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.

Время, указываемое в log-сообщениях, зависит от значения параметра **timeskew**. Возможные значения:

- **utc** – указывать время UTC (значение по умолчанию);
- **system** – указывать локальное системное время.

Пример настройки:

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

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

12.11.2 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 ""
…
```

12.11.3 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 48

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

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

12.12 Фильтрация протоколов

Подсистема DPI способна избирательно обрабатывать трафик определённых протоколов. Для этого необходимо в настройках DPI-списка указать обрабатываемые протоколы в параметре **protocols**. Можно указать один или несколько протоколов (через пробел), а также при необходимости добавлять/удалять отдельные протоколы с помощью операторов **+=** и **-=**.

Список поддерживаемых протоколов выводится командой **show protocols all**.

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:

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

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

```
EcoSGE: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.
```

По каждому распознанному протоколу подсистема DPI ведёт подсчёт исходящих и входящих сессий, байтов и пакетов. Счётчики можно вывести в CLI или опросить по SNMP.

Для вывода счётчиков в CLI необходимо отправить команду **show protocounters { all | diff }** :

- с аргументом **all** команда покажет суммарные значения с момента запуска системы EcoSGE;
- с аргументом **diff** будут показаны только изменения за последнюю минуту.

Счётчики в выводе команд сгруппированы по протоколам, а группы счётчиков, в свою очередь, упорядочены по убыванию суммарного количества байт.

Примеры вывода:

```
EcoSGE:# show protocounters all
Printing proto counters...
Core total, cr_dpi_total_base_egress_bytes: 1750
Core total, cr_dpi_total_base_ingress_bytes: 948
Core total, cr_dpi_total_base_egress_pkts: 25
Core total, cr_dpi_total_base_ingress_pkts: 14
Core total, cr_dpi_total_ip_egress_bytes: 1688
Core total, cr_dpi_total_ip_ingress_bytes: 948
Core total, cr_dpi_total_ip_egress_pkts: 24
Core total, cr_dpi_total_ip_ingress_pkts: 14
Core total, cr_dpi_total_tcp_egress_bytes: 1688
Core total, cr_dpi_total_tcp_ingress_bytes: 948
Core total, cr_dpi_total_tcp_egress_pkts: 24
Core total, cr_dpi_total_tcp_ingress_pkts: 14
Core total, cr_dpi_total_smpp_egress_sessions: 1
Core total, cr_dpi_total_smpp_egress_bytes: 848
Core total, cr_dpi_total_smpp_ingress_bytes: 678
Core total, cr_dpi_total_smpp_egress_pkts: 12
Core total, cr_dpi_total_smpp_ingress_pkts: 10
Core total, cr_dpi_total_imaps_egress_sessions: 2
Core total, cr_dpi_total_imaps_egress_bytes: 280
Core total, cr_dpi_total_imaps_egress_pkts: 4
EcoSGE:# show protocounters diff
Printing proto counters diff...
Core total-diff, cr_dpi_total_base_egress_bytes: 906
Core total-diff, cr_dpi_total_base_ingress_bytes: 474
Core total-diff, cr_dpi_total_base_egress_pkts: 13
Core total-diff, cr_dpi_total_base_ingress_pkts: 7
Core total-diff, cr_dpi_total_ip_egress_bytes: 844
Core total-diff, cr_dpi_total_ip_ingress_bytes: 474
Core total-diff, cr_dpi_total_ip_egress_pkts: 12
Core total-diff, cr_dpi_total_ip_ingress_pkts: 7
Core total-diff, cr_dpi_total_tcp_egress_bytes: 844
Core total-diff, cr_dpi_total_tcp_ingress_bytes: 474
```

```
Core total-diff, cr_dpi_total_tcp_egress_pkts: 12
Core total-diff, cr_dpi_total_tcp_ingress_pkts: 7
Core total-diff, cr_dpi_total_smpp_egress_bytes: 424
Core total-diff, cr_dpi_total_smpp_ingress_bytes: 339
Core total-diff, cr_dpi_total_smpp_egress_pkts: 6
Core total-diff, cr_dpi_total_smpp_ingress_pkts: 5
Core total-diff, cr_dpi_total_imaps_egress_sessions: 1
Core total-diff, cr_dpi_total_imaps_egress_bytes: 140
Core total-diff, cr_dpi_total_imaps_egress_pkts: 2
```

Для опроса счётчиков по SNMP следует использовать шаблон запроса 1.3.6.1.4.1.45555.1.6.**<a>**.**<b>**.**<c>**, где:

<a> – определяет запрашиваемое значение:

- 0 – суммарное значение с момента запуска системы;
- 1 – изменение за последнюю минуту;

<b> – номер (id) протокола в MIB;

<c> – подсчитываемые единицы:

- 0 – исходящие сессии,
- 1 – входящие сессии,
- 2 – исходящие байты,
- 3 – входящие байты,
- 4 – исходящие пакеты,
- 5 – входящие пакеты.

Пример SNMP-опроса счётчиков для протокола SMPP (ID 738):

```
snmpwalk -v2c -c public 192.168.5.2:161 1.3.6.1.4.1.45555.1.6.0.738
iso.3.6.1.4.1.45555.1.6.0.738.0.0 = Counter64: 1
iso.3.6.1.4.1.45555.1.6.0.738.1.0 = Counter64: 0
iso.3.6.1.4.1.45555.1.6.0.738.2.0 = Counter64: 848
iso.3.6.1.4.1.45555.1.6.0.738.3.0 = Counter64: 678
iso.3.6.1.4.1.45555.1.6.0.738.4.0 = Counter64: 12
iso.3.6.1.4.1.45555.1.6.0.738.5.0 = Counter64: 10
```

Если в SNMP Manager загружен MIB-файл счётчиков для протоколов, то в SNMP-ответах вместо OID будут указаны имена счётчиков. Пример:

```
snmpwalk -v2c -m Proto-MIB -c public 192.168.5.2:161
1.3.6.1.4.1.45555.1.6.0.738
Proto-MIB::econatTotalSmppEgressSessions.0 = Counter64: 1
Proto-MIB::econatTotalSmppIngressSessions.0 = Counter64: 0
Proto-MIB::econatTotalSmppEgressBytes.0 = Counter64: 848
Proto-MIB::econatTotalSmppIngressBytes.0 = Counter64: 678
Proto-MIB::econatTotalSmppEgressPkts.0 = Counter64: 12
Proto-MIB::econatTotalSmppIngressPkts.0 = Counter64: 10
```

Все счётчики подсистемы DPI являются скалярными объектами в MIB, поэтому при опросе таких счётчиков по отдельности необходимо после OID указывать **".0"**. Пример запроса суммарного количества исходящих пакетов протокола SMPP:

```
snmpget -v2c -m Proto-MIB -c public 192.168.5.2:161
1.3.6.1.4.1.45555.1.6.0.738.4.0"
Proto-MIB::econatTotalSmppEgressPkts.0 = Counter64: 12
```

Для сброса счётчиков необходимо отправить команду **clear counters**.

При распознавании какого-либо протокола по базе сигнатур подсистема DPI сохраняет уникальный набор данных об этом протоколе (5-tuple) в специальную таблицу – DPI flow table. Если в дальнейшем будет обнаружена попытка открытия сессии, у которой 5-tuple совпадает с сохранённым в таблице, то подсистема DPI уже по первому пакету определит протокол. Это оптимизирует производительность DPI.

Каждая запись 5-tuple хранится в таблице в течение фиксированного времени, которое нельзя изменить. Однако предусмотрена возможность принудительной очистки DPI flow table. Для этого необходимо отправить команду **clear dpi_worker_flows**. С данной командой связаны два счётчика:

- **cr_dpi_worker_flush_try** регистрирует каждую попытку очистки таблицы;
- **cr_dpi_worker_flush** регистрирует количество удалённых записей.

12.13 Обработка незапрошенных HTTP-ответов

Возможен случай, когда HTTP-сервер отправляет ответ сразу после успешного завершения процедуры TCP Handshake без получения соответствующего запроса от клиента. Для подсистемы DPI такой порядок обмена данными является неправильным. Незапрошенный HTTP-ответ и соответствующая TCP-сессия будут заблокированы. За блокировку отвечает параметр **block_fast_response** в ветке **system.dpi**, которому по умолчанию присвоено значение **on** (блокировка включена). Для того чтобы пропускать такие незапрошенные HTTP-ответы и не блокировать сессии, необходимо задать **block_fast_response off** и применить новую настройку командой **apply**.

Примечание. Блокировка не применяется к незапрошенным ответам, которые следуют за надлежащим ответом сервера на запрос клиента (технология Server Push, описанная в RFC 7540).

Для подсчёта сессий, в ходе которых незапрошенные HTTP-ответы поступили сразу после процедуры TCP Handshake, предусмотрен счётчик **cr_sess_http_wo_get**. Этот счётчик срабатывает только при отключенной блокировке. OID счётчика в MIB: **1.3.6.1.4.1.45555.1.2.685.0**.

12.14 Функция DPI Redirect

Функция DPI Redirect отвечает за перенаправление абонентских HTTP-соединений при попытке обращения к запрещённым интернет-ресурсам. Алгоритм работы данной функции зависит от того, есть ли в пакетах абонентского трафика метки MPLS и в какой интерфейс – LAN или Log

– производится перенаправление. Таким образом, возможны четыре алгоритма работы DPI Redirect, которые рассмотрены ниже.

- Метка MPLS отсутствует, перенаправление в LAN-интерфейс

При поступлении в LAN-интерфейс GET-запроса к запрещённому ресурсу данный запрос блокируется, после чего генерируется ответ "307 Temporary Redirect", который передаётся в тот же LAN-интерфейс. Заголовок Location данного ответа содержит URL, заданный в параметре redirect_url в настройках dpilist (см. раздел "Создание и настройка DPI-списков").

- Метка MPLS отсутствует, перенаправление в Log-интерфейс

При поступлении в LAN-интерфейс GET-запроса к запрещённому ресурсу данный запрос блокируется, после чего генерируется ответ "307 Temporary Redirect", который передаётся в Log-интерфейс. Заголовок Location данного ответа содержит URL, заданный в параметре redirect_url в настройках dpilist (см. раздел "Создание и настройка DPI-списков"). Затем ответ передаётся на маршрутизатор и далее следует до абонента. Для данного алгоритма необходимо предварительно задать все необходимые параметры в ветке **connection_log** (см. раздел "Логирование абонентских сессий"). В частности, необходимо в параметре **log_servers** задать IP-адрес интерфейса маршрутизатора, с которым соединён Log-интерфейс.

- Метка MPLS присутствует, перенаправление в LAN-интерфейс

При поступлении в LAN-интерфейс GET-запроса к запрещённому ресурсу данный запрос не блокируется. В ответе запрещённого Web-сервера содержимое полезной нагрузки заменяется сообщением "307 Temporary Redirect", в котором заголовок Location содержит URL, заданный в параметре redirect_url в настройках dpilist (см. раздел "Создание и настройка DPI-списков"). Затем данный изменённый ответ передаётся в тот же LAN-интерфейс.

- Метка MPLS присутствует, перенаправление в Log-интерфейс

При поступлении в LAN-интерфейс GET-запроса к запрещённому ресурсу данный запрос не блокируется. В ответе запрещённого Web-сервера содержимое полезной нагрузки заменяется сообщением "307 Temporary Redirect", в котором заголовок Location содержит URL, заданный в параметре redirect_url в настройках dpilist (см. раздел "Создание и настройка DPI-списков"). Данный изменённый ответ передаётся в Log-интерфейс, затем на маршрутизатор, где ему присваивается соответствующая метка MPLS, и далее следует до абонента. Для данного алгоритма необходимо предварительно задать все необходимые параметры в ветке **connection_log** (см. раздел "Логирование абонентских сессий"). В частности, необходимо в параметре **log_servers** задать IP-адрес интерфейса маршрутизатора, с которым соединён Log-интерфейс.

ПРИМЕЧАНИЕ

В системе EcoSGE перенаправление HTTP-соединений может быть реализовано как средствами DPI, так и средствами BRAS. Следует помнить, что политики и сервисы BRAS применяются к абонентскому трафику раньше, чем параметры DPI.

12.15 Зависимость работы EcoSGE от схемы подключения

Возможны две схемы подключения устройства EcoSGE:

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

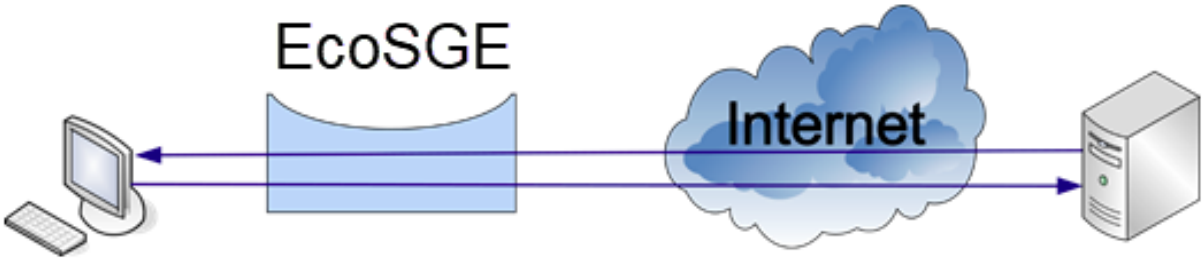

Рисунок 18

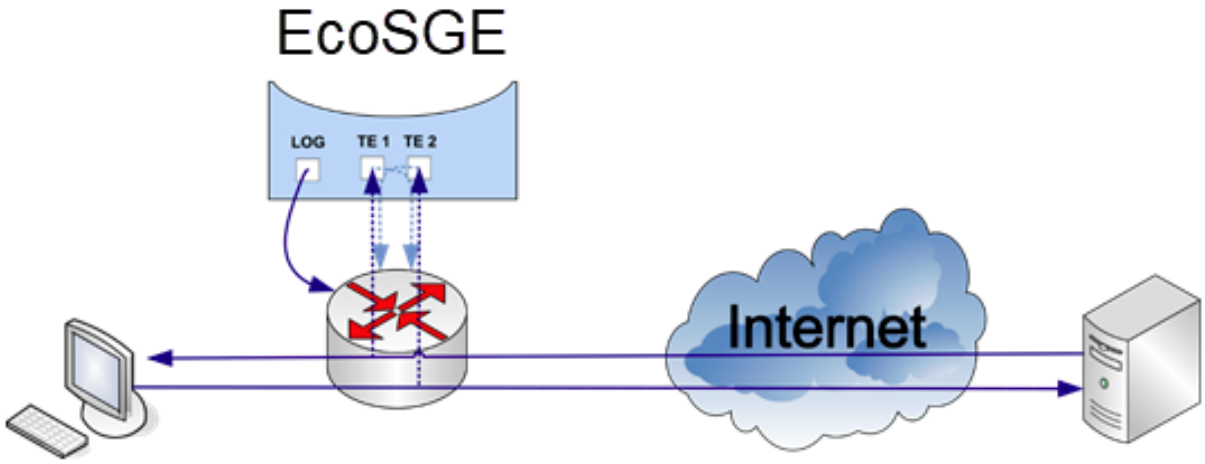

Рисунок 19

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 "Настройки интерфейсов"). 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 задан адрес шлюза по умолчанию в ветке конфигурации **connection_log** (см. раздел "Логирование абонентских сессий"). 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 ветке конфигурации **connection_log**). При этом можно настроить EcoSGE таким образом, чтобы из логирующего интерфейса отправлялся нетегированный трафик. Для этого необходимо в ветке конфигурации **connection_log** присвоить параметру **strip_tags** значение **on**.

13 Подсистема логирования

Подсистема логирования обеспечивает передачу на внешний сервер следующей информации:

- системные события (базовая функция);
- абонентские сессии (базовая функция);
- протоколы, распознанные механизмом DPI (доп. лицензия);
- подключения к web-серверам: HTTP запросы и ответы, запросы на установление SSL/TLS соединений (доп. лицензия);
- DNS-запросы (доп. лицензия);
- статистика Quality of Experience: общая информация о сессиях, аккаунтинг, данные для анализа качества сервисов OTT (доп. лицензия).

Для отправки логов может использоваться интерфейс LOG или MNG. Исключение – логирование системных событий, где используется только интерфейс MNG.

Существуют устройства EcoSGE с несколькими интерфейсами LOG. На таких устройствах отправка логов происходит по алгоритму Round-Robin.

13.1 Логирование системных событий

EcoSGE может вести логирование системных событий и действий пользователя в CLI и передавать логи на syslog-сервер через интерфейс управления (MNG). Настройки системного логирования находятся в ветке **system.system_log**. Включение и выключение логирования производится непосредственно в данной ветке командами **enable** и **disable** соответственно. Серверы, на которые должны передаваться системные логи, указываются в параметрах **log_servers** в виде **<IPv4-адрес>:<порт>** и **log_servers6** в виде **[<IPv6-адрес>]:<порт>**.

Время, указываемое в log-сообщениях, зависит от значения параметра **timeskew**. Возможные значения:

- **utc** – указывать время UTC (значение по умолчанию);
- **system** – указывать локальное системное время.

Имя устройства, передаваемое в логах, задаётся в параметре **hostname** (по умолчанию **"ecosge"**). Данное имя передаётся не только при логировании системных событий, но и при логировании абонентских сессий 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 сессий.

```
EcoSGE:18:system.system_log# verbose defrag 1
EcoSGE:19:system.system_log# show
enable
log_servers ( )
log_servers6 ( )
hostname "ecosge"
timeskew utc
```

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

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

Уровни логирования:

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

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

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

Подсистемы (параметр **facility**): basic_nat, conn_track, defrag, dpi, fast_path, gc, health_check, main, reconfig, service, sniffer, snmp, syslogger, trans_tbl, session, alg, bras_tbl.
То есть, если настроен параметр **verbose all** равный ***3***, то будут логироваться сообщения всех уровней. Если для подсистемы указано значение параметра **verbose**, отличное от **all**, то будет приниматься в расчет наибольшая из этих двух величин.
Значения, выводимые командой **show verboselvl** могут отличаться от установленных в текущей конфигурации.
Для того чтобы оперативно изменить уровень логирования для какой-то подсистемы (или всех подсистем), используется команда **setlog <подсистема> <уровень логирования>**. Здесь уровни логирования задаются не цифрами, как при изменении конфигурации, а названиями. Изменения вступают в силу немедленно. После перезагрузки установки уровней логирования будут возвращены к значениям, указанным в активной конфигурации.
В приведенном ниже примере уровень логирования для всех подсистем изменяется на FATAL, соответственно, менее приоритетные события (WARNING, INFO, ERROR) логироваться не будут. При этом в конфигурации уровень логирования для всех подсистем остается INFO, и после перезагрузки системы будут снова логироваться все события.
Пример.

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

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

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

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

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

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

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

Пример:

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

Формат сообщений о системных событиях, передаваемых на syslog-сервер, соответствует RFC 5424. Пример:

```
2020-06-26T20:40:59+03:30 test econat: 9B20C43C9CFEC103 1593204059 GC
[INFO] SESSION_TABLE_GC_CORE_1 calls: 0, ticks: 0, ticks/entry: -nan,
processed: 0, freed 0
2020-06-26T20:41:35+03:30 test econat: 9B20C43C0C6BC103 1593204095 GC
[INFO] abonents_table_GC_CORE_3 calls: 0, ticks: 0, ticks/entry: -nan,
processed: 0, freed 0
```

13.2 Логирование абонентских сессий

В соответствии с требованиями законодательства Российской Федерации оператор связи обязан хранить информацию о выделении абонентам IP-адресов и портов, а также об адресах ресурсов, к которым обращаются абоненты. Для сбора такой информации предусмотрена функция логирования абонентских сессий IPv4 и IPv6 по протоколу Syslog или NetFlow v9 (IPFIX).

Настройка логирования абонентских сессий производится в ветке конфигурации **connection_log** и включает в себя три шага:

1) создание раздела настроек логирования;

2) задание параметров в созданном разделе;

3) привязка созданного раздела настроек логирования к пулу (см. раздел "Создание и настройка пула").

В стандартной поставке системы EcoSGE можно создать два раздела настроек логирования, в специальной поставке – до восьми.

Для создания раздела настроек логирования абонентских сессий необходимо отправить команду **create conlog <name>**. В ветку **connection_log** будет добавлен раздел **conlogname** указанного ниже вида (пример):

```
connection_log
{
    conlogtest
    {
      disable
      log_interface mng
      log_servers ( )
      strip_tags off
      num_copies 1
      log_on_release off
      log_individual_conn off
      use_hex_format off
      pack_msgs on
      log_format syslog
      facility 16
      severity 6
      timeskew utc
    }
}
```

В таблице ниже дано описание параметров логирования абонентских сессий.

Таблица 49

Параметр	Описание
enable | disable	Включение и выключение логирования абонентских сессий
log_interface	Интерфейс для отправки log-сообщений. Возможные значения: • **dedicated** – интерфейс LOG; с данным параметром связаны параметры **mac**, **that_mac**, **ip_address**, **gateway**; • **mng** – интерфейс MNG (используется по умолчанию)
log_servers ( )	**<IP-адрес>:<порт>** сервера, на который должны передаваться log-сообщения. Если указать несколько серверов, то log-сообщения будут передаваться параллельно на все доступные серверы из списка. То есть каждый сервер будет получать информацию обо всех сессиях. Можно указать не более 10 серверов
mac	MAC-адрес источника, который будет передаваться в log-пакетах. Если не

Параметр	Описание
	указан, то будет выбран MAC-адрес одного из логирующих интерфейсов. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
that_mac	MAC-адрес syslog-сервера в параметре **log_servers**, являющегося ближайшим L3 соседом. Параметр необязательный. Если параметр не задан, то MAC-адрес будет определяться по протоколу ARP. Должен содержать MAC-адрес первого syslog-сервера, если первый syslog-сервер находится в той же подсети, или MAC-адрес default gateway, если первый syslog-сервер находится в другой подсети. Использование этого параметра снижает вероятность потери данных логирования на старте при большой нагрузке. EcoSGE может обрабатывать и логировать более 5 миллионов сессий в секунду при полной нагрузке. Если syslog-сервер ответит на ARP-запрос, например, через 10 мс, то в очереди может накопиться до 50000 сессий, ожидающих отправки. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
ip_address	**<IP-адрес>/<маска подсети>** источника, которые будут передаваться в log-пакетах. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
gateway	Адрес шлюза, который будет передаваться в log-пакетах. Требуется в том случае, если не все syslog-серверы, указанные в параметре **log_servers**, находятся в подсети, указанной в параметре **ip_address**. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
strip_tags	В режиме зеркалирования EcoSGE отправляет абоненту через логирующий сетевой интерфейс пакет прерывания соединения (для HTTPS) или пакет перенаправления (для HTTP). При поступлении 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
num_copies	Количество экземпляров одного и того же log-сообщения, посылаемого каждому серверу из списка **log_servers**. По умолчанию 1
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	**on** – отправлять данные по каждой абонентской сессии **off** – отправлять только данные о выделении блока портов для абонентов Примеры логов при включенном и выключенном параметре даны в разделе "Логирование по протоколу Syslog"

Параметр	Описание
use_hex_format	Формат вывода логов: • **on** – шестнадцатеричный формат; позволяет уменьшить размер логов при полном сохранении информационной составляющей; • **off** – десятичный фиксированный формат (например, 010.210.000.012:00080)
pack_msgs	Разрешает упаковывать несколько log-сообщений в одно. Это уменьшает размер логов и нагрузку на сеть. Упаковываются все сообщения, которые поступили за период 200 мс. Примеры логов при включенном и выключенном параметре даны в разделе "Логирование по протоколу Syslog"
log_format	Формат логирования: • **syslog** – логирование по протоколу syslog; с данным параметром связаны параметры **facility**, **severity**, **timeskew**; • **netflow** – логирование по протоколу NetFlow v9 (IPFIX); с данным параметром связаны параметры **netflow_template_rate**, **netflow_options_rate**, **multiple_receivers**
multiple_receivers	Определяет режим рассылки логов в формате NetFlow на несколько серверов (см. раздел "Балансировка сообщений NetFlow") Данный параметр действует только при **log_format netflow** и скрыт в выводе конфигурации при **log_format syslog**
netflow_template_rate	Указывает, через какое количество пакетов должны передаваться пакет netflow template. Возможные значения: once, 128, 512, 1K, 4K, 16K, 64K. Данный параметр действует только при **log_format netflow** и скрыт в выводе конфигурации при **log_format syslog**
netflow_options_rate	Указывает, через какое количество пакетов должны передаваться пакеты netflow options и netflow options template. Возможные значения: once, 128, 512, 1K, 4K, 16K, 64K. Данный параметр действует только при **log_format netflow** и скрыт в выводе конфигурации при **log_format syslog**
facility	Задаёт 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. Данный параметр действует только при **log_format syslog** и скрыт в выводе конфигурации при **log_format netflow**
severity	Задаёт для формируемых сообщений формата syslog уровень важности для удобства дальнейшей обработки и фильтрации. Допустимые значения параметра от 0 до 7, рекомендуемые – от 5 до 7. Эти значения соответствуют кодам стандарта RFC 5424, обозначающим уровни важности сообщений: • **5** – замечание (Notice), сообщения о нормальных, но важных событиях; • **6** – информационное (Informational) сообщение;

Параметр	Описание
	• **7** – отладочное (Debug) сообщение. Значение по умолчанию – 6. Данный параметр действует только при **log_format syslog** и скрыт в выводе конфигурации при **log_format netflow**
timeskew	Данный параметр определяет, какое время будет указано в log-сообщениях. Возможные значения: • **utc** – указывать время UTC (значение по умолчанию); • **system** – указывать локальное системное время. Данный параметр действует только при **log_format syslog** и скрыт в выводе конфигурации при **log_format netflow**

После задания всех необходимых параметров в созданном разделе настроек логирования необходимо привязать данный раздел настроек к пулу (см. раздел "Создание и настройка пула") и применить конфигурацию командой **apply**.

Для удаления созданного раздела настроек логирования абонентских сессий необходимо отправить команду **no conlog conlog<name>**.

13.2.1 Логирование по протоколу Syslog

Порты для трансляции адресов в режиме CGNAT выделяются блоками. Следующий блок выдаётся только при исчерпании портов в текущем блоке. Блочное выделение портов позволяет многократно уменьшить объём логов, так как при соответствующих настройках вместо множества сообщений о выделении отдельных портов будет лишь одно сообщение о выделении диапазона (блока) портов. Количество портов в блоке задаётся параметром **port_block_size** в ветке конфигурации **system.nat_defaults**. Значение по умолчанию – 128. Изменение параметра возможно, но не рекомендуется.

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

Таблица 50

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 рекомендуется задать для четырех 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 о сессии из пула CGNAT:

<Дата и время syslog-сервера> <IP-адрес EcoSGE> <Дата и время EcoSGE> <Системное имя EcoSGE> | <IP-адрес назначения>:<Порт> <A | F> <IP-адрес, на который произведена трансляция>:<Порт> <E | I> <IP-адрес источника>:<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.

Формат сообщений о сессиях из пулов CGNAT64 и Fake6 отличается от формата для пула CGNAT. Сообщения содержат следующие поля:

<Дата и время syslog-сервера> <IP-адрес EcoSGE> <Дата и время EcoSGE> <Системное имя EcoSGE> | <IPv6-адрес источника>:<Порт> <A | F> <IPv4-адрес, на который произведена трансляция (post-NAT source)>:<Порт> <E | I> <IPv6-адрес назначения>:<Порт> <IPv4-адрес назначения (post-NAT destination)>:<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 для пула CGNAT64:

```
2022-10-31T11:57:57.723636+00:00 192.168.5.2  2022-10-31T11:57:56+00:00
econat     |  fc00:0000:0000:0000:0000:0000:0001:01024 A
003.003.003.003:01024 E 0064:ff9b:0000:0000:0000:0000:0202:0202:00053
002.002.002.002:00053  UDP
2022-10-31T11:58:03.914193+00:00 192.168.5.2  2022-10-31T11:58:02+00:00
econat     |  fc00:0000:0000:0000:0000:0000:0001:01024 F
003.003.003.003:01024 E 0064:ff9b:0000:0000:0000:0000:0202:0202:00053
002.002.002.002:00053  UDP  2022-10-31T11:57:56+00:00
```

Примеры сообщений об открытии и закрытии сессии для пула Fake6:

```
2022-10-31T20:03:45.723636+03:00 192.168.5.2  2020-10-31T20:03:45+03:00
econat     |  fd00:0000:0000:0000:0000:0000:0000:0001:01024 A
000.000.000.000:00000 E aaaa:0000:0000:0000:0000:0000:0000:aaaa:00053
000.000.000.000:00000  UDP
2022-10-31T20:03:50.914193+03:00 192.168.5.2  2020-10-31T20:03:50+03:00
econat     |  fd00:0000:0000:0000:0000:0000:0000:0001:01024 F
000.000.000.000:00000 E aaaa:0000:0000:0000:0000:0000:0000:aaaa:00053
000.000.000.000:00000  UDP  2022-10-31T20:03:45+03:00
```

Следует обратить внимание на то, что в сообщениях о сессиях из пула Fake6 поля **post-NAT source** и **post-NAT destination** будут всегда содержать нули.

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
```

13.2.2 Логирование по протоколу NetFlow v9 (IPFIX)

При логировании абонентских сессий по протоколу NetFlow v9 (IPFIX) передаётся только информация о сессиях. Логирование объёма трафика, переданного в ходе сессий, не ведётся.

Для работы логирования по протоколу NetFlow настройки должны быть такими, как указано ниже.

Таблица 51

Параметр	Значение
log_format	netflow
log_on_release	on
log_individual_conn	on
use_hex_format	off
pack_msgs	on
log_servers	IP-адрес и порт NetFlow-сервера
ip_address	IP-адрес/маска подсети источника (при **log_interface dedicated**)
gateway	IP-адрес шлюза (при **log_interface dedicated**)

В таблицах ниже описаны используемые шаблоны сообщений при логировании по протоколу NetFlow. Подробное описание полей сообщения доступно по ссылке.

Шаблон сообщений для сессий IPv4 (NAT44)

Таблица 52

Поле	Размер (бит)	IANA ID	Описание
observationTimeMilliseconds	64	323	Unix-время открытия или закрытия сессии в миллисекундах
sourceIPv4Address	32	8	Локальный IPv4-адрес отправителя
postNATSourceIPv4Address	32	225	Глобальный IPv4-адрес отправителя
protocolIdentifier	8	4	Идентификатор протокола (полная таблица идентификаторов доступна по ссылке)
sourceTransportPort	16	7	Локальный порт отправителя

Поле	Размер (бит)	IANA ID	Описание
postNAPTsourceTransportPort	16	227	Глобальный порт отправителя
destinationIPv4Address	32	12	Локальный IPv4-адрес получателя
postNATDestinationIPv4Address	32	226	Глобальный IPv4-адрес получателя
destinationTransportPort	16	11	Локальный порт получателя
postNAPTdestinationTransportPort	16	228	Глобальный порт получателя
natOriginatingAddressRealm	8	229	Направление сессии: 1 – исходящая, 2 – входящая
natEvent	8	230	Событие NAT: 1 – создание трансляции, 2 – удаление трансляции

Шаблон сообщений для сессий IPv6 (NAT64)

Таблица 53

Поле	Размер (бит)	IANA ID	Описание
observationTimeMilliseconds	64	323	Unix-время открытия или закрытия сессии в миллисекундах
sourceIPv6Address	128	27	Локальный IPv6-адрес отправителя
postNATSourceIPv4Address	32	225	Глобальный IPv4-адрес отправителя
protocolIdentifier	8	4	Идентификатор протокола (полная таблица идентификаторов доступна по ссылке)
sourceTransportPort	16	7	Локальный порт отправителя
postNAPTsourceTransportPort	16	227	Глобальный порт отправителя
destinationIPv6Address	128	28	Локальный IPv6-адрес получателя
postNATDestinationIPv4Address	32	226	Глобальный IPv4-адрес получателя
destinationTransportPort	16	11	Локальный порт получателя
postNAPTdestinationTransportPort	16	228	Глобальный порт получателя
natOriginatingAddressRealm	8	229	Направление сессии: 1 – исходящая, 2 – входящая
natEvent	8	230	Событие NAT: 1 – создание трансляции, 2 – удаление трансляции

Если для приёма логов указано несколько серверов (параметр **log_servers**), то можно выбрать режим рассылки через параметр **multiple_receivers**:

- **mirror** – параллельная рассылка (режим по умолчанию); рассылка логов ведётся на все доступные серверы из списка, т. е. каждый сервер будет получать информацию обо всех сессиях;
- **balance** – режим балансировки; система будет распределять логи в зависимости от выбранного типа балансировки, который определяется параметром **balance_type**:
  - **round_robin** – распределение между приёмниками по кругу в порядке очереди;
  - **hash_src_ip** – распределение между приёмниками по IP-адресам источников. Система запоминает, на какой сервер был отправлен первый лог с определённым адресом источника, и в дальнейшем будет отправлять на этот сервер все логи, относящиеся к этому адресу;
  - **hash_5_tuple** – распределение между приёмниками по набору данных 5-tuple (IP-адрес и порт источника, IP-адрес и порт назначения, протокол), по которому однозначно идентифицируется сессия. Система запоминает, на какой сервер был отправлен первый лог с определённым набором данных 5-tuple, и в дальнейшем будет отправлять на этот сервер все логи с таким 5-tuple.

13.3 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 функциональность DPI (см. раздел "Подсистема DPI").

```
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 54

Параметр	Описание
enable | disable	Включение/выключение логирования протоколов
log_interface	Интерфейс для отправки log-сообщений. Возможные значения: • **dedicated** – интерфейс LOG; с данным параметром связаны параметры **ip_address**, **gateway**, **source_port**; • **mng** – интерфейс MNG (используется по умолчанию)
server_ip_and_port	**<IP-адрес>:<порт>** log-сервера
ip_address	**<IP-адрес>/<маска подсети>** источника, которые будут передаваться в log-пакетах. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
gateway	Адрес шлюза, который будет передаваться в log-пакетах. Требуется в том случае, если log-сервер, указанный в параметре **server_ip_and_port**, не находится в подсети, указанной в параметре **ip_address**. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
source_port	Номер порта источника для отправки сообщений на log-сервер. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**. По умолчанию 1089. Если для логирования выбран интерфейс MNG (**log_interface mng**), то используется случайный порт

13.4 Логирование подключений к web-серверам

Система EcoSGE способна вести логирование проходящих HTTP GET-запросов, ответов web-серверов (HTTP) и запросов на установление SSL/TLS соединений, включая сообщения ClientHello и ServerHello и сертификаты TLS. Данная возможность доступна при наличии лицензии "Clickstream".

Настройка данного типа логирования производится в ветке **system.clickstream**. Настраиваемые параметры описаны в таблице ниже.

Таблица 55

Параметр	Описание
enable | disable	Включение/выключение логирования
log_interface	Интерфейс для отправки log-сообщений. Возможные значения: • **dedicated** – интерфейс LOG; с данным параметром связаны параметры **ip_address**, **gateway**, **source_port**, **mtu**; • **mng** – интерфейс MNG (используется по умолчанию)
server_ip_and_port	**<IP-адрес>:<порт>** log-сервера
ip_address	**<IP-адрес>/<маска подсети>** источника, которые будут передаваться в log-пакетах. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
gateway	Адрес шлюза, который будет передаваться в log-пакетах. Требуется в том случае, если log-сервер, указанный в параметре **server_ip_and_port**, не находится в подсети, указанной в параметре **ip_address**. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
source_port	Номер порта источника для отправки сообщений на log-сервер. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**. По умолчанию 1088. Если для логирования выбран интерфейс MNG (**log_interface mng**), то используется случайный порт
mtu	Значение MTU для пакетов, отправляемых на log-сервер. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**. По умолчанию 1500
log_format	Формат логов: • **syslog** – текстовый, • **binary** – двоичный
tls_client_h	Включение (on) / выключение (off) логирования сообщений ClientHello. По умолчанию выключено
tls_server_h	Включение (on) / выключение (off) логирования сообщений ServerHello. По умолчанию выключено
tls_certificate	Включение (on) / выключение (off) логирования сертификатов TLS. По умолчанию выключено
http_get	Включение (on) / выключение (off) логирования запросов HTTP GET. По умолчанию включено
tls_sni	Включение (on) / выключение (off) логирования запросов на установление SSL/TLS-соединения. По умолчанию включено
send_tls_version { on | off }	Добавлять (on) / не добавлять (off) поле "Максимальная поддерживаемая версия TLS" в логи запросов на установление SSL/TLS-соединений. По умолчанию **off**.

Параметр	Описание
	Данный параметр связан с параметром **tls_sni**. При значении **off** параметра **tls_sni** данный параметр скрыт в выводе ветки конфигурации **system.clickstream**.

Пример настройки:

```
EcoSGE:system.clickstream# ls
enable
log_interface default
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
log_format syslog
tls_client_h on
tls_server_h on
tls_certificate on
http_get on
tls_sni on
send_tls_version on
```

Ниже даны примеры записей на сервере при логировании в текстовом формате (**log_format syslog**). 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 34567345673456734567
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 56789567895678956789
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 12345678900987654321
192.168.000.002:41016 192.168.000.003:00080 1532627400 econat     SSL: 3.3
0x0304 hostname: vk.com
```

Для логирования в двоичном формате (**log_format binary**) используется проприетарный протокол, для парсинга которого требуется устройство EcoQoE.

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

Таблица 56

№ поля	Что содержит	Пример
1	Временная метка log-сервера (не посылается устройством EcoSGE)	2018-03-26T10:35:58.202901+00:00
2	IP-адрес устройства EcoSGE (параметр **ip_address**)	192.168.1.1
3	20-значный идентификатор сессии.	34567345673456734567

№ поля	Что содержит	Пример
	Опция лицензии Clickstream. Для получения необходимо обратиться в службу технической поддержки	
4	IP-адрес и порт отправителя	192.168.000.002:34904
5	IP-адрес и порт получателя	192.168.000.003:00080
6	Временная метка устройства EcoSGE (POSIX time)	1522071357
7	Имя устройства EcoSGE, заданное в параметре **hostname** ветки **system_log**	econat
8	Содержимое HTTP GET-запроса	GET / HTTP/1.1#015#012Host: google.ru#015#012User-Agent: curl/7.55.0#015#012Accept: */*#015#012#015

Описания полей 1-7 в записи для ответа web-сервера (см. запись 2 выше) аналогичны описаниям для HTTP GET-запроса. Поле 8 содержит версию HTTP и код ответа.

В таблице ниже дано описание полей 8, 9, 10 в записи для запроса на установление SSL/TLS соединения (см. запись 3 выше). Описания полей 1-7 аналогичны описаниям для HTTP GET-запроса (см. таблицу выше).

Таблица 57

№ поля	Что содержит	Пример
8	Версия SSL	SSL: 3.3
9	Максимальная поддерживаемая версия TLS: • 1.0 – 0x0301 • 1.1 – 0x0302 • 1.2 – 0x0303 • 1.3 – 0x0304 Данное поле передаётся в логах в том случае, если в настройках EcoSGE **system.clickstream** задано **tls_sni on** и **send_tls_version on**	0x0304
10	Доменное имя	hostname: vk.com

Статистика логирования подключений к web-серверам выводится командой **show counters all | include clickstream** . В таблице ниже дано описание счётчиков.

Таблица 58

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

Счетчик	Описание
	доменного имени
cr_clickstream_certificate	Количество сессий, для которых была получена информация о сертификате TLS
cr_clickstream_client_hello	Количество отправленных пакетов ClientHello
cr_clickstream_server_hello	Количество полученных пакетов ServerHello

Пример:

```
EcoSGE:> 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
```

13.5 Логирование DNS-запросов

Система EcoSGE способна вести логирование DNS-запросов следующих типов ресурсных записей: A, AAAA, CNAME, DNSKEY, DS, HTTPS (Type 65), MX, NS, PTR, RRSIG, TXT. Эта функциональная возможность доступна при наличии лицензии DNS_LOG.

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

Таблица 59

Параметр	Описание
enable | disable	Включение/выключение логирования DNS-запросов
log_interface	Интерфейс для отправки log-сообщений. Возможные значения: • **dedicated** – интерфейс LOG; с данным параметром связаны параметры **ip_address**, **gateway**, **source_port**, **mtu**; • **mng** – интерфейс MNG (используется по умолчанию)
server_ip_and_port	**<IP-адрес>:<порт>** log-сервера
ip_address	**<IP-адрес>/<маска подсети>** источника, которые будут передаваться в log-пакетах. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
gateway	Адрес шлюза, который будет передаваться в log-пакетах. Требуется в том случае, если log-сервер, указанный в параметре **server_ip_and_port**, не находится в подсети, указанной в параметре **ip_address**. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
source_port	Номер порта источника для отправки сообщений на log-сервер. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**. По умолчанию 1088. Если для логирования выбран интерфейс MNG (**log_interface mng**), то используется случайный порт
mtu	Значение MTU для пакетов, отправляемых на log-сервер. Данный параметр действует только при **log_interface dedicated** и скрыт в

Параметр	Описание
	выводе конфигурации при **log_interface mng**. По умолчанию 1500
log_format	Формат логов. На данный момент поддерживается только двоичный формат (**binary**)
include_redirection_info { on | off }	Добавляет в логи IPv4/IPv6-адрес DNS-сервера, на который был перенаправлен DNS-запрос. Должна быть настроена и включена функция перенаправления DNS-запросов.

ВНИМАНИЕ! Для правильной работы функции логирования DNS-запросов обязательно должно быть включено логирование абонентских соединений (ветка конфигурации **system.connection_log**).

Предусмотрены счётчики DNS-запросов каждого типа ресурсной записи и общего количества DNS-запросов по TCP, UDP, IPv4 и IPv6. Для вывода этих счётчиков необходимо отправить команду **show counters all | include dns** (см. пример ниже).

```
EcoSGE:# show counters all | include dns
cr_dns_udp: 15
cr_dns_tcp: 5
cr_dns_ipv4: 10
cr_dns_ipv6: 10
cr_dns_a: 2
cr_dns_aaaa: 1
cr_dns_cname: 1
cr_dns_dnskey: 2
cr_dns_ds: 2
cr_dns_https: 3
cr_dns_mx: 1
cr_dns_ns: 1
cr_dns_ptr: 2
cr_dns_rsig: 3
cr_dns_txt: 2
```

OID счётчиков для опроса по SNMP имеет вид **1.3.6.1.4.1.45555.1.2.<номер счётчика>**. Номера счётчиков указаны в таблице ниже.

Таблица 60

Счётчик	Номер в OID
cr_dns_udp	851
cr_dns_tcp	852
cr_dns_ipv4	853
cr_dns_ipv6	854
cr_dns_a	855
cr_dns_aaaa	856
cr_dns_ns	857
cr_dns_mx	858
cr_dns_ptr	859
cr_dns_txt	860
cr_dns_dnskey	861
cr_dns_rsig	862
cr_dns_ds	863
cr_dns_cname	864

Счётчик	Номер в OID
cr_dns_https	865

13.6 QoE

QoE (Quality of Experience) – интегральный параметр, представляющий собой общую приемлемость качества услуги, субъективно воспринимаемую конечным пользователем. В концепции 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 и могут 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 модуль логирования;
- модуль аккаунтинга сессий (логирование количества переданных байт/пакетов);
- модуль анализа OTT (Over-the-Top), позволяющий анализировать параметры предоставления видеосервисов: подсчёт байтов подсессии OTT, время последнего PSH пакета в подсессии от сервера, дельта времени между GET пакетом от клиента и PSH пакетом от сервера в подсессии.

Логирование производится как для IPv4, так и для IPv6-соединений. Для обработки IPv6 требуется отдельная лицензия.

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

Настройки логирования QoE находятся в ветке конфигурации **system.qoe_log**.

Параметры настройки QoE описаны в таблице ниже.

Таблица 61

Параметр	Описание
{ enable | disable }	Включение/выключение логирования QoE
interim_threshold	Количество килобайт от 1 до 65535, при накоплении которого будет отправлен лог. Учитывается и исходящий, и входящий трафик. После отправки лога подсчёт начинается заново. По умолчанию задано значение 0, при котором лог будет отправлен только при закрытии сессии. В случае закрытия сессии до накопления заданного количества килобайт будет отправлен лог с указанием фактического количества килобайт. Если вместе с этим параметром задан параметр **interim_interval** (значение отлично от 0), и отправка лога по условию **interim_interval** произойдёт до накопления заданного количества килобайт, то при отправке данного лога счётчик килобайтов

Параметр	Описание
	будет сброшен, и подсчёт начнётся заново. Данный параметр доступен при наличии лицензии Accounting Log
interim_interval	Периодичность логирования от 1 до 65535 секунд с момента создания сессии. Если в течение заданного периода трафик равен нулю, то лог не будет отправлен. По умолчанию задано значение 0, при котором лог будет отправлен только при закрытии сессии. В случае закрытия сессии до истечения заданного времени будет отправлен лог с указанием фактического количества килобайт. Если вместе с этим параметром задан параметр **interim_threshold** (значение отлично от 0), и отправка лога по условию **interim_threshold** произойдёт до истечения заданного периода, то при отправке данного лога счётчик времени будет сброшен, и отсчёт начнётся заново. Данный параметр доступен при наличии лицензии Accounting Log
interim_mode	Данный параметр определяет, какие значения будут передаваться в логах: изменения за определённый период или суммарные значения с момента открытия сессии. Периодичность логирования зависит от параметров **interim_interval** и **interim_threshold**. Возможные значения параметра: • **delta** – передавать изменения за определённый период (значение по умолчанию); • **accumulated** – передавать суммарные значения с момента открытия сессии. Примеры логов для обоих значений параметра даны после таблицы. Данный параметр доступен при наличии лицензии Accounting Log
log_interface	Интерфейс для отправки log-сообщений. Возможные значения: • **dedicated** – интерфейс LOG; с данным параметром связаны параметры **ip_address**, **gateway**, **source_port**, **mtu**; • **mng** – интерфейс MNG (используется по умолчанию)
syn_log	Опция для лицензии QoE, которая добавляет возможность логирования пакетов SYN. Для получения данной опции следует обратиться в службу технической поддержки. Возможные значения: on, off При значении **on** каждый 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-сервера
ip_address	**<IP-адрес>/<маска подсети>** источника, которые будут передаваться в log-пакетах. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
gateway	Адрес шлюза, который будет передаваться в log-пакетах. Требуется в том случае,

Параметр	Описание
	если log-сервер, указанный в параметре **server_ip_and_port**, не находится в подсети, указанной в параметре **ip_address**. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**
source_port	Номер порта источника для отправки сообщений на log-сервер. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**. По умолчанию 1089. Если для логирования выбран интерфейс MNG (**log_interface mng**), то используется случайный порт
mtu	Значение MTU для пакетов, отправляемых на log-сервер. Данный параметр действует только при **log_interface dedicated** и скрыт в выводе конфигурации при **log_interface mng**. По умолчанию 1500

Пример настройки:

```
EcoSGE:system.qoe_log# ls
enable
interim_threshold 1
interim_interval 60
interim_mode delta
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
```

Ниже рассмотрены примеры логов в зависимости от значения параметра **interim_mode**. Формат логов зависит от парсера, используемого для их обработки, и может отличаться от приведённых примеров.

Пример 1. Логирование при interim_mode delta

Настройки:

- interim_mode **delta**
- interim_threshold **1** (т. е. 1024 байт)
- interim_interval **5**

Исходящий пакет: payload 2500 байт, IPv6, UDP

По данному пакету будут сформированы и отправлены следующие логи:

1. Egress UDP bytes in/out=0/1024 pkts in/out=0/1 – выполнено условие **interim_threshold 1**; счётчик bytes out зарегистрировал отправку первых 1024 байт пакета; счётчик pkts out зарегистрировал один исходящий пакет.

2. Egress UDP bytes in/out=0/1024 pkts in/out=0/0 – выполнено условие **interim_threshold 1**; счётчик bytes out зарегистрировал отправку следующих 1024 байт пакета; счётчик pkts out показывает 0, так как количество пакетов не изменилось; всего отправлено 2048 байт; осталось отправить 514 байт (452 – payload, 62 – заголовки Ethernet (14), IPv6 (40) и UDP (8)), при этом условие **interim_threshold 1** уже не может быть выполнено; ожидается выполнение условия **interim_interval 5**.

3. Egress UDP bytes in/out=0/514 pkts in/out=0/0 – выполнено условие **interim_interval 5**; счётчик bytes out зарегистрировал отправку последних 514 байт пакета; счётчик pkts out показывает 0, так как количество пакетов не изменилось.

4. Egress UDP bytes in/out=0/0 pkts in/out=0/0 – данный лог отправлен при закрытии сессии. Трафика после отправки лога 3 не было, поэтому при **interim_mode delta** переданы нулевые значения.

Пример 2. Логирование при interim_mode accumulated

Настройки:

- interim_mode **accumulated**
- interim_threshold **1** (т. е. 1024 байт)
- interim_interval **5**

Исходящий пакет: payload 2500 байт, IPv6, UDP

По данному пакету будут сформированы и отправлены следующие логи:

1. Egress UDP bytes in/out=0/1024 pkts in/out=0/1 – выполнено условие **interim_threshold 1**, счётчик bytes out зарегистрировал отправку первых 1024 байт пакета, счётчик pkts out зарегистрировал один исходящий пакет.

2. Egress UDP bytes in/out=0/2048 pkts in/out=0/1 – выполнено условие **interim_threshold 1**, счётчик bytes out зарегистрировал отправку следующих 1024 байт пакета и показывает суммарное значение 2048; счётчик pkts out показывает 1, так как количество пакетов не изменилось; осталось отправить 514 байт (452 – payload, 62 – заголовки Ethernet (14), IPv6 (40) и UDP (8)), при этом условие **interim_threshold 1** уже не может быть выполнено; ожидается выполнение условия **interim_interval 5**.

3. Egress UDP bytes in/out=0/2562 pkts in/out=0/1 – выполнено условие **interim_interval 5**, счётчик bytes out зарегистрировал отправку последних 514 байт пакета и показывает суммарное значение 2562; счётчик pkts out показывает 1, так как количество пакетов не изменилось.

4. Egress UDP bytes in/out=0/2562 pkts in/out=0/1 – данный лог отправлен при закрытии сессии. Трафика после отправки лога 3 не было, поэтому при **interim_mode accumulated** переданы те же суммарные значения, что и в логе 3.

14 Перенаправление DNS-запросов

Данная функциональность позволяет провайдеру перенаправлять DNS-запросы абонентов на свой DNS-сервер, независимо от того, какой IP-адрес DNS-сервера указан в исходном запросе. Перенаправление выполняется на основании заданных правил. Можно задать до 8 правил (например, отдельные правила для разных подсетей).

Настройка перенаправления DNS-запросов производится в ветке **system.dns_redirects**. В первую очередь необходимо создать правило командой **create dns_redirect <имя правила>**. Затем следует задать параметры правила и применить настройки. В таблице ниже дано описание параметров правила.

Таблица 62

Параметр	Описание
enable | disable	Включение / выключение правила
priority	Приоритет правила. Чем меньше значение, тем выше приоритет. По умолчанию 100
dns_redirect_timeout	Время ожидания ответа DNS-сервера в секундах. По умолчанию 5
dns_redirect_no_response_count	Максимально допустимое количество последовательных DNS-запросов, на которые в течение **dns_redirect_timeout** от DNS-сервера не поступило ответа. По умолчанию 3. При достижении данного количества DNS-серверу присваивается статус "недоступен"
dns_redirect_deadtime	Время в секундах, в течение которого на DNS-сервер в статусе "недоступен" не будут перенаправляться DNS-запросы. По умолчанию 120
dns_redirect_ipv4_servers ( )	IPv4-адреса DNS-серверов, на которые должны перенаправляться DNS-запросы в пакетах IPv4. Можно задать до 32 адресов. Если указано несколько адресов, то для выбора DNS-сервера применяется алгоритм Round-robin. Адреса можно указывать как по отдельности через пробел, так и диапазоном через дефис или длину префикса (не меньше 27)
dns_redirect_ipv6_servers ( )	IPv6-адреса DNS-серверов, на которые должны перенаправляться DNS-запросы в пакетах IPv6. Можно задать до 32 адресов. Если указано несколько адресов, то для выбора DNS-сервера применяется алгоритм Round-robin. Адреса можно указывать в полной и сокращённой форме как по отдельности через пробел, так и диапазоном через дефис или длину префикса (не меньше 123)
acl ( )	Предварительно созданный ACL для трафика IPv4, которому должны соответствовать пакеты для того, чтобы к ним было применено правило перенаправления. Можно указать несколько ACL через пробел. Порядок указания определяет последовательность проверки трафика на соответствие правилам ACL
aclv6 ( )	Предварительно созданный ACL для трафика IPv6, которому должны соответствовать пакеты для того, чтобы к ним было применено правило перенаправления. Можно указать несколько ACL через пробел. Порядок указания определяет последовательность проверки трафика на соответствие правилам ACL

Пример настройки:

```
configure
goto dns_redirects
create dns_redirect A
goto dns_redirectA
enable
```

```
priority 100
dns_redirect_timeout 5
dns_redirect_no_response_count 3
dns_redirect_deadtime 120
dns_redirect_ipv4_servers ( 10.10.0.100 10.10.0.111-10.10.0.115 )
dns_redirect_ipv6_servers ( fc00::2 fc00::3 )
acl ( aclv4_dns_redirect )
aclv6 ( aclv6_dns_redirect )
apply
```

Примечание. Настройки не будут применены, если при установленном параметре **enable** выполняется хотя бы одно из следующих условий:

- задан **acl**, но не задан **dns_redirect_ipv4_servers**;
- задан **aclv6**, но не задан **dns_redirect_ipv6_servers**;
- не задан ни **acl**, ни **aclv6**;
- не создан ACL, указанный в параметре **acl** или **aclv6**.

Для диагностики и просмотра статистики перенаправления DNS-запросов предусмотрены следующие команды:

show dns_redirect brief – вывод сводной информации по всем правилам. Пример выводимых данных:

```
# show dns_redirect brief
      Name          Priority       Status
  dns_redirectA       100          enable
  dns_redirectB       200          enable
```

show dns_redirect <имя правила> counters – вывод подробной информации по отдельному правилу. Пример выводимых данных:

```
# show dns_redirect dns_redirectA counters
     DNS IP         TOTAL SENT      NO ANSWER    STATUS   DEADTIME
-------------------------------------------------------------------------
-----------
   10.10.0.100          456098         310      DEAD    90
   10.10.0.111       25698345783          0     ALIVE     -
        fc00::2                  34747123               23         ALIVE
-
        fc00::3                      1435             132          DEAD
50
```

где

TOTAL SENT – общее количество DNS-запросов, перенаправленных на данный DNS-сервер (64-битный счётчик)

NO ANSWER – количество событий, когда от данного DNS-сервера не было получено ответа (32-битный счётчик)

STATUS – DEAD: серверу присвоен статус "недоступен", и он не используется для перенаправления; ALIVE – сервер используется для перенаправления

DEADTIME – оставшееся время **dns_redirect_deadtime** (только для серверов в статусе DEAD)

clear dns_redirect <имя правила> { all | <IP-адрес> } – сброс счётчиков TOTAL SENT и NO ANSWER для всех DNS-серверов (**all**) или для определённого DNS-сервера (**IP-адрес**). Данная команда выполняется только в конфигурационном режиме. Пример выводимых данных:

```
# clear dns_redirect dns_redirectA 10.10.0.100
Ok
# show dns_redirect dns_redirectA counters
     DNS IP         TOTAL SENT      NO ANSWER    STATUS   DEADTIME
-------------------------------------------------------------------------
-----------
   10.10.0.100            0        0       DEAD    90
     10.10.0.111       25698345783        0      ALIVE     -
        fc00::2                  34747123            23          ALIVE
-
        fc00::3                    1435            132           DEAD
50
```

reset dns_redirect <имя правила> { all | <IP-адрес> } – сброс таймера **dns_redirect_deadtime** и возврат определённого сервера (**IP-адрес**) или всех серверов (**all**) в группу DNS-серверов, используемых для перенаправления. Данная команда выполняется только в конфигурационном режиме. Пример выводимых данных:

```
# reset dns_redirect dns_redirectA fc00::3
Ok
# show dns_redirect dns_redirectA counters
         DNS IP         TOTAL SENT      NO ANSWER    STATUS   DEADTIME
-------------------------------------------------------------------------
-----------
      10.10.0.100            0        0       DEAD    90
      10.10.0.111       25698345783        0      ALIVE     -
        fc00::2                  34747123            23          ALIVE
-
        fc00::3                    1435            132          ALIVE
50
```

15 Подмена IP-адресов в DNS-ответах

По отдельной лицензии для системы EcoSGE доступна функция DNS Substitution, которая выполняет подмену IP-адресов в незашифрованных DNS-ответах на запросы ресурсных записей типа A (для IPv4) и AAAA (для IPv6). Параметры настройки данной функции содержатся в ветке конфигурации **system.dns_substitution**:

```
EcoSGE:system.dns_substitution# show
disable
acl none
aclv6 none
domains ( )
```

В таблице ниже дано описание параметров функции DNS Substitution.

Таблица 63

Параметр	Описание
enable | disable	Включение / выключение функции (по умолчанию **disable**)
acl	ACL для трафика IPv4, к которому необходимо применять функцию. По умолчанию **none** (не применять к трафику IPv4)
aclv6	ACL для трафика IPv6, к которому необходимо применять функцию. По умолчанию **none** (не применять к трафику IPv6). Параметр доступен при наличии лицензии на работу с трафиком IPv6
domains ( )	Список пар "доменное_имя IP_адрес_для_подмены". Можно указывать как IPv4-, так и IPv6-адреса. При несоответствии типа запрошенной ресурсной записи (A или AAAA) и версии IP-адреса в ответе DNS-сервера подмена не производится. Максимальное количество пар – 8192

При задании списка **domains ( )** одной строкой количество пар "доменное_имя IP_адрес_для_подмены" ограничено максимальной длиной строки CLI (1000 символов). Поэтому для большого количества таких пар следует указывать их по одной в отдельных строках или использовать оператор +=. Пример параметра **domains ( )**, содержащего три пары:

```
domains (
  "host1.domain1 198.51.100.1"
  "host2.domain2 198.51.100.2"
  "host3.domain3 198.51.100.3"
)
```

Для удаления пары "доменное_имя IP_адрес" из списка **domains ( )** необходимо использовать оператор **-=**.

Подсчёт количества пакетов с подменёнными IPv4- и IPv6-адресами ведётся счетчиками **cr_dns_spoof_ipv4** и **cr_dns_spoof_ipv6**.

16 Защита от TCP SYN Flooding

В систему EcoSGE по отдельной лицензии может быть добавлен механизм SYN Cookie + SYN Proxy (далее – SYN Proxy) для противодействия DoS-атакам типа TCP SYN Flooding (RFC 4987).

Для использования данного механизма не требуется производить какие-либо сложные настройки. Достаточно создать ACL для IPv4 и/или IPv6, к которому необходимо применять механизм SYN Proxy, указать ACL в ветке конфигурации **system.tcp_protection** и включить защиту.

```
EcoSGE:system.tcp_protection# ls
enable
acl aclflood
aclv6 aclv6flood
```

Внимание! Механизм SYN Proxy не поддерживает Hairpin NAT.

Работа механизма SYN Proxy подробно описана в разделе III этого документа (англ.). Отдельно следует указать на две важные особенности работы данного механизма:

- после получения ACK клиента начинается согласование между SYN Proxy и целевым сервером. До успешного завершения согласования SYN Proxy отбрасывает все GET-запросы клиента;
- при прохождении через SYN Proxy сбрасываются все опции исходного TCP-сегмента.

Для мониторинга работы механизма SYN Proxy предусмотрено несколько счётчиков, описание которых дано таблице ниже.

Таблица 64

Имя счётчика	Описание
cr_tcp_syn_cookie_sent_ipv4 cr_tcp_syn_cookie_sent_ipv6	Количество SYN, в ответ на которые был отправлен SYN Cookie (SYN/ACK, сгенерированный механизмом SYN Proxy)
cr_tcp_syn_cookie_established_ipv4 cr_tcp_syn_cookie_established_ipv6	Количество SYN Cookie, в ответ на которые получен ACK
cr_tcp_syn_proxy_established_ipv4 cr_tcp_syn_proxy_established_ipv6	Количество TCP-сессий, установленных с использованием механизма SYN Proxy
cr_tcp_syn_sent_ipv4 cr_tcp_syn_sent_ipv6	Количество всех установленных и полуоткрытых (был только SYN) TCP-сессий
cr_tcp_established_ipv4 cr_tcp_established_ipv6	Общее количество установленных TCP-сессий
cr_tcp_syn_cookie_invalid_ipv4 cr_tcp_syn_cookie_invalid_ipv6	Количество SYN Cookie, у которых не совпал хеш

В таблице ниже указаны OID счётчиков в MIB.

Таблица 65

OID	Имя счётчика
1.3.6.1.4.1.45555.1.2.696	cr_tcp_established_ipv6
1.3.6.1.4.1.45555.1.2.697	cr_tcp_syn_sent_ipv6
1.3.6.1.4.1.45555.1.2.698	cr_tcp_established_ipv4
1.3.6.1.4.1.45555.1.2.699	cr_tcp_syn_sent_ipv4
1.3.6.1.4.1.45555.1.2.770	cr_tcp_syn_cookie_sent_ipv4
1.3.6.1.4.1.45555.1.2.771	cr_tcp_syn_cookie_established_ipv4
1.3.6.1.4.1.45555.1.2.772	cr_tcp_syn_cookie_invalid_ipv4
1.3.6.1.4.1.45555.1.2.773	cr_tcp_syn_proxy_established_ipv4
1.3.6.1.4.1.45555.1.2.774	cr_tcp_syn_cookie_sent_ipv6
1.3.6.1.4.1.45555.1.2.775	cr_tcp_syn_cookie_established_ipv6
1.3.6.1.4.1.45555.1.2.776	cr_tcp_syn_cookie_invalid_ipv6
1.3.6.1.4.1.45555.1.2.777	cr_tcp_syn_proxy_established_ipv6

Для мониторинга SYN Proxy можно также использовать команду **show cps**, которая выводит в отдельной графе "TCP protection" следующие данные для IPv4 и IPv6:

- количество SYN в секунду, в ответ на которые был отправлен SYN Cookie (syn per second);
- количество SYN Cookie в секунду, в ответ на которые получен ACK (resv cookie per second);
- количество TCP-сессий в секунду, установленных с использованием механизма SYN Proxy (proxy session per second).

```
EcoSGE:# show cps
ipv4 tcp total/cps/tps: 0/0/0
ipv4 udp total/cps/tps: 0/0/0
total ipv4 cps+tps: 0
-------------------------------------
ipv6 tcp cps: 0
ipv6 udp cps: 0
total ipv6 cps: 0
=====================================
total ipv6+ipv4 cps+tps: 0
tcp fps total/v4/v6: 0/0/0
udp fps total/v4/v6: 0/0/0
total fps: 0
TCP protection
-------------------------------------
syn per second ipv4: 0
resv cookie per second ipv4: 0
proxy session per second ipv4: 0
syn per second ipv6: 0
resv cookie per second ipv6: 0
proxy session per second ipv6: 0
```

В выводе команды **show sessions local any** все сессии, созданные с использованием механизма SYN Proxy, обозначаются меткой |SC|:

ingress TCP 185.61.79.70:3775-185.61.79.70:3775 213.24.130.100:40088 ; Last packet 29.14 seconds ago; To be deleted right now. |SC|

17 Функция Sniffer

В систему EcoSGE по отдельному запросу может быть добавлена функция Sniffer (сниффер) для передачи копии определённого трафика во внешнюю систему мониторинга и анализа. Данная функция использует протокол инкапсуляции TZSP.

Настройка функции Sniffer производится в ветке конфигурации **system.sniffer**, которая по умолчанию имеет следующий вид:

```
EcoSGE:system.sniffer# ls
disable
log_interface default
server_ip_and_port 0.0.0.0:0
ip_address 0.0.0.0/0
gateway 0.0.0.0
source_port 1088
permanent_sniffer off
hookpoint lan
snaplen 0
strip_eb_header on
per_session_pkt_count 0
acl none
aclv6 none
```

В таблице ниже дано описание параметров функции Sniffer.

Таблица 66

Параметр	Описание
enable | disable	Включение/выключение функции
log_interface	Интерфейс для отправки копии трафика во внешнюю систему: • **default** – интерфейс LOG (используется по умолчанию); с данным параметром связаны параметры **ip_address**, **gateway**, **source_port**; • **mng** – интерфейс MNG. **Внимание!** Следует учитывать, что MTU для интерфейса MNG всегда равен 1500, в отличие от интерфейса LOG, для которого MTU задаётся параметром **l2mtu** в ветке конфигурации **system.nat_defaults**. Поэтому копии пакетов на выходе из интерфейса MNG могут быть фрагментированными.
server_ip_and_port	**<IP-адрес>:<порт>** внешнего сервера, принимающего копию трафика. **Внимание!** Для передачи копии трафика EcoSGE использует протокол TZSP. Стандартный порт назначения для данного протокола – 37008
ip_address	**<IP-адрес>/<маска подсети>** для интерфейса LOG. Данный параметр доступен только при **log_interface default**
gateway	Адрес шлюза для интерфейса LOG. Данный параметр доступен только при **log_interface default**. Требуется в том случае, если сервер, указанный в параметре **server_ip_and_port**, не находится в подсети, указанной в параметре **ip_address**
source_port	Номер порта источника для интерфейса LOG. По умолчанию 1088. Данный параметр доступен только при **log_interface default**. Если выбран интерфейс MNG (**log_interface mng**), то используется случайный порт.

Параметр	Описание
permanent_sniffer	Режим работы: • **off** – ручное управление (по умолчанию). Запуск Sniffer производится командой **sniff**, а остановка – нажатием комбинации клавиш **Ctrl+C** (см. пример 1 ниже). Если отправить команду с опцией **local**, то сниффер будет выводить в консоль информацию об обрабатываемых пакетах (см. пример 2 ниже). Более подробно команда ручного запуска сниффера рассмотрена ниже. • **on** – фоновый режим. Sniffer работает постоянно, и для его остановки необходимо задать **permanent_sniffer off** и применить изменение командой **apply**
hookpoint	Точка перехвата трафика для копирования: • **lan** – перед NAT (по умолчанию), • **wan** – после NAT От выбора точки перехвата трафика зависит то, какой IP-адрес – локальный или глобальный – будет адресом источника в копиях исходящих пакетов и адресом назначения в копиях входящих пакетов (см. примеры 3 и 4 ниже)
snaplen	Количество байтов оригинального пакета, которые будут переданы в копии. Диапазон значений: от 0 до 65535. По умолчанию 0 (копировать весь пакет)
strip_eb_header	Когда EcoSGE работает в связке с EcoBalancer, последний добавляет в пакеты дополнительные служебные заголовки. При значении **on** (по умолчанию) сниффер удаляет такие заголовки, а при значении **off** копирует пакеты полностью. Данный параметр доступен при наличии опции Filter Control в программном обеспечении EcoSGE
per_session_pkt_count	Количество копируемых пакетов из каждой сессии. По умолчанию 0 (без ограничения). Данный параметр доступен при наличии опции Accounting Log в программном обеспечении EcoSGE
acl	ACL для трафика IPv4, к которому необходимо применять функцию Sniffer. По умолчанию задано значение **none**, при котором сниффер будет обрабатывать весь трафик IPv4
aclv6	ACL для трафика IPv6, к которому необходимо применять функцию Sniffer. По умолчанию задано значение **none**, при котором сниффер будет обрабатывать весь трафик IPv6
Внимание! Особенности одновременного использования параметров **acl** и **aclv6**: • при значении **none** у обоих параметров сниффер будет обрабатывать весь трафик IPv4 и IPv6; • если в одном из параметров указан ACL, а у другого значение **none**, то сниффер будет обрабатывать только тот трафик, который соответствует указанному ACL.	

Для функции Sniffer предусмотрены следующие счётчики:

- **cr_sniffer_try_send_tzsp** – количество попыток отправки копий пакетов;
- **cr_sniffer_send_tzsp** – количество успешно отправленных копий пакетов;
- **cr_sniffer_copy_mbuf_error** – ошибки копирования пакетов в буфер;

- **cr_sniffer_packet_data_enqueue_error** – ошибки записи данных о пакете в буфер.

Пример 1. Ручное управление функцией Sniffer (**permanent_sniffer off**):

```
EcoSGE:system.sniffer# sniff
Starting sniffer, export to 192.168.5.3:37008
Running...
^C
Interrupted by user
Stopping...
```

Если Sniffer работает в фоновом режиме (**permanent_sniffer on**), то в ответ на команду **sniff** система сообщит, что Sniffer уже запущен:

```
EcoSGE:system.sniffer# sniff
Sniffer already running
```

Пример 2. Выполнение команды **sniff local**:

```
EcoSGE:system.sniffer# sniff local
Starting sniffer, export local
2023-08-30T15:01:27+00:00 UDP 172.16.1.1:53 > 192.168.1.1:53, length 542
2023-08-30T15:01:27+00:00 UDP 172.16.1.1:53 > 192.168.1.1:53, length 542
2023-08-30T15:01:27+00:00 UDP 172.16.1.1:53 > 192.168.1.1:53, length 542
2023-08-30T15:01:29+00:00 UDP [fd00::1]:53 > [aacc::1]:53, length 62
2023-08-30T15:01:29+00:00 UDP [fd00::1]:53 > [aacc::1]:53, length 62
2023-08-30T15:01:29+00:00 UDP [fd00::1]:53 > [aacc::1]:53, length 62
```

В примерах 3 и 4 ниже показана информация о копиях пакетов в зависимости от выбранной точки перехвата трафика. Пакеты передавались между локальным адресом 192.168.0.2 и внешним адресом 192.168.0.3 через устройство EcoSGE, на котором настроена трансляция в глобальный адрес 3.3.3.3.

Пример 3. Информация о копии пакета при **hookpoint lan**:

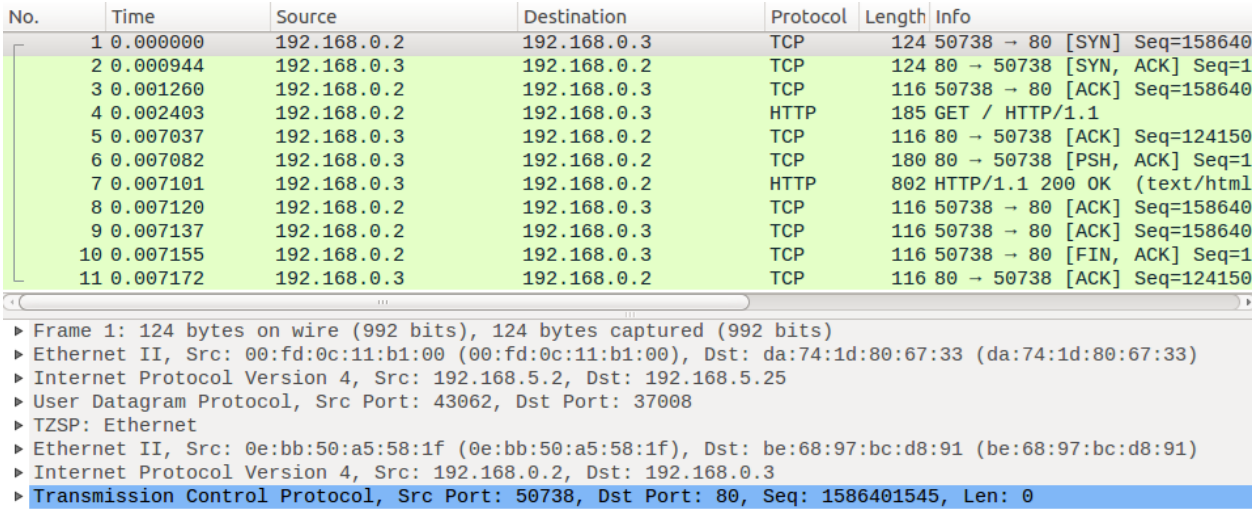

Рисунок 20

В вышеприведённом примере можно видеть, что адресом источника (Source) исходящих пакетов 1, 3, 4, 8, 9, 10 и адресом назначения (Destination) входящих пакетов 2, 5, 6, 7, 11 является локальный адрес 192.168.0.2.

Пример 4. Информация о копии пакета при **hookpoint wan**:

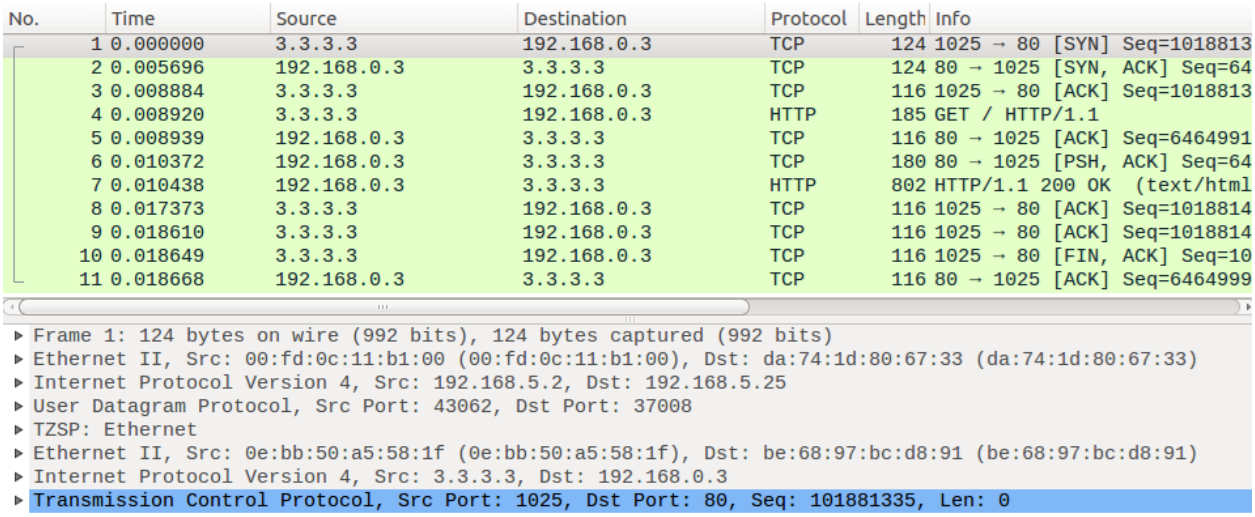

Рисунок 21

В вышеприведённом примере можно видеть, что адресом источника (Source) исходящих пакетов 1, 3, 4, 8, 9, 10 и адресом назначения (Destination) входящих пакетов 2, 5, 6, 7, 11 является глобальный адрес 3.3.3.3.

Предусмотрена возможность запуска дополнительных экземпляров сниффера вручную с параметрами, отличными от заданных в ветке конфигурации **system.sniffer**. Одновременно могут работать не более 8 снифферов, включая фоновый.

Общий синтаксис команды запуска сниффера имеет вид:

sniff [acl <aclname>] [src_ip <ip_address>] [dst_ip <ip_address>] [aclv6 <aclv6name>] [src_ipv6 <ipv6_address>] [dst_ipv6 <ipv6_address>] [runtime <number>] [pkt_count <number>] [hookpoint { wan | lan }] [per_session_pkt_count <number>] [snaplen <number>] [output <pcap_file_name>] [strip_eb_header { on | off }] [local]

Назначение параметров **acl**, **aclv6**, **hookpoint**, **per_session_pkt_count**, **snaplen**, **strip_eb_header** в команде то же, что и у одноимённых параметров в ветке конфигурации **system.sniffer**. **Внимание!** Если не указать эти параметры в команде, то они будут взяты из конфигурации.

Можно видеть, что команда ручного запуска сниффера может содержать ряд дополнительных параметров, которые отсутствуют в конфигурации. Их описание дано в таблице ниже.

Таблица 67

Параметр команды	Описание
src_ip	Фильтр по IPv4-адресу источника для указанного **acl**. Можно указать один адрес, диапазон через дефис или подсеть
dst_ip	Фильтр по IPv4-адресу назначения для указанного **acl**. Можно указать один адрес, диапазон через дефис или подсеть
src_ipv6	Фильтр по IPv6-адресу источника для указанного **aclv6**. Можно указать один адрес,

Параметр команды	Описание
	диапазон через дефис или подсеть
dst_ipv6	Фильтр по IPv6-адресу источника для указанного **aclv6**. Можно указать один адрес, диапазон через дефис или подсеть
runtime	Продолжительность работы в секундах. Если также задан параметр **pkt_count**, то сниффер завершит работу при выполнении любого из двух условий: • по истечении времени **runtime**, даже если не обработано заданное количество пакетов **pkt_count**; • при достижении заданного количества обработанных пакетов **pkt_count**, даже если не истекло время **runtime**
pkt_count	Общее количество пакетов, которое необходимо обработать. Если также задан параметр **runtime**, то сниффер завершит работу при выполнении любого из двух условий: • при достижении заданного количества обработанных пакетов **pkt_count**, даже если не истекло время **runtime** • по истечении времени **runtime**, даже если не обработано заданное количество пакетов **pkt_count**;
output	Позволяет записать информацию о трафике в локальный Pcap-файл в директории /log/. Файл будет содержать информацию об оригинальных пакетах без заголовков TZSP
local	Если указан, то сниффер будет выводить в консоль информацию об обрабатываемых пакетах (см. пример 2 выше), но при этом не будет отправлять копии пакетов на внешний сервер

В команде учитывается порядок указания параметров. Так, например, система не примет команду **sniff local runtime 10 acl aclv4**. В данном случае правильной будет команда **sniff acl aclv4 runtime 60 local**.

18 Общая диагностика системы

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.

18.1 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
```

18.2 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: 0/335544320 (0.0%)
Translation table used/total: 0/335544320 (0.0%)
Ipv6 sess table   used/total: 0/125829120 (0.0%)
Ipv6 translation table used/total: 0/125829120 (0.0%)
Abon table NAT64  used/total: 0/3932160 (0.0%)
Abons table      used/total: 0/3932160 (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 68

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 IPv4 (текущее/максимальное)
Translation table used/total	Счётчик заполнения таблицы трансляций IPv4 (текущее/максимальное)
Ipv6 sess table used/total	Счётчик заполнения таблицы сессий IPv6 (текущее/максимальное)

Параметр	Описание
Ipv6 translation table used/total	Счётчик заполнения таблицы трансляций IPv6 (текущее/максимальное)
Abon table NAT64 used/total	Счётчик заполнения таблицы уникальных пользователей, использующих IPv6 (текущее/максимальное)
Abons table used/total	Счётчик заполнения таблицы уникальных пользователей, использующих IPv4 (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)
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**

18.3 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.

18.4 Сбор и выгрузка диагностической информации

Если по каким-либо причинам специалисту службы технической поддержки компании RDP не может быть предоставлен удалённый доступ к устройству для его диагностики, то можно создать зашифрованный архив с подробной диагностической информацией и выгрузить его на FTP или TFTP-сервер. При передаче по FTP возможно указание логина и пароля на FTP-сервере.

Полный синтаксис команды сбора и выгрузки диагностической информации имеет вид:

tech-support url <url> [number <n>] [interval <i1>] [backtrace <i2>] [verbose] [dryrun] [force]

Аргументы команды:

number <n> – количество циклов опроса всех счётчиков EcoSGE (по умолчанию 300)

interval <i1> – интервал между циклами опроса счётчиков в микросекундах (по умолчанию 2000000)

backtrace <i2> – сбор дополнительной служебной информации; работает только в конфигурационном режиме; требует уровень привилегий 15; сбор выполняется 2 раза с заданным интервалом i2 в секундах

verbose – установить максимальную детализацию журнала системных событий на время выполнения команды; работает только в конфигурационном режиме; требует уровень привилегий 15

dryrun – получить информацию и создать архив, но не отправлять его на сервер.

force – принудительное завершение выполнения команды в другой консоли и запуск в текущей

В ходе выполнения команды в консоль выводится информация о выполняемых действиях:

```
2:2:> tech-support url tftp://192.168.5.1 number 1
Start collecting tech info. It takes few minutes.
Mon Feb 19 18:12:04 UTC 2024 Beginning
Preparing system data...
Preparing econat proc data...
[##################################################] 100%
Preparing econat statistics...
Preparing econat counters...
[##################################################] 100%
Preparing econat exe archive...
[##################################################] 100%
Archiving and encrypting info...
Sending /tmp/tech_support/tech_support.enc and /mnt/DPIDATA content to
tftp://192.168.5.1...
[##################################################] 100%
Mon Feb 19 18:12:32 UTC 2024 Done
```

При успешном выполнении команды на хосте, указанном в команде, появляется файл tech_support.enc размером около 30 МБ, а также файлы из папки /mnt/DPIDATA системного диска EcoSGE. Эти файлы необходимо отправить запросившему их сотруднику технической поддержки.

19 Действия с прошивкой

В EcoSGE предусмотрено несколько разделов жесткого диска для встроенного программного обеспечения (прошивки). Это два основных раздела PRIM1 и PRIM2, в которых может быть установлена какая-либо версия прошивки, и служебный раздел FALLBACK.

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

Например:

```
EcoSGE: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 EcoSGE загрузится при перезапуске.

19.1.1 Обновление прошивки

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

Для того чтобы получить необходимую информацию в CLI EcoSGE 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.

```
EcoSGE: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**.

19.1.2 Изменение параметров перезагрузки

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

Например:

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

```
EcoSGE:9:# firmware revert
Using PRIM1 as boot partition
Next boot from partition PRIM1
EcoSGE:10:# firmware status
```

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

20 Счётчики

В устройстве EcoSGE действуют счётчики сбора системной статистики.

Для просмотра состояния всех счётчиков 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 сброса счётчиков необходимо отправить команду **clear counters**.

```
EcoSGE:# clear counters
Counters has been zeroed
```

Примечание. Команда **clear counters** не применяется к программным интерфейсным счётчикам.

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
```

21 Справочник по командам

Краткое описание команд приведено в таблице ниже.

Обозначения:

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

Режим:

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

VALUE – вводимое значение параметра.

Таблица 69

Команда	Описание	Режим	Приоритет
`( )`	Очистить редактируемый элемент конфигурации – массив	C	4
`VALUE`	Присвоить значение редактируемому элементу конфигурации	C	4
`( VALUE VALUE )`	Присвоить значение редактируемому элементу конфигурации – массиву	C	4
`?`	Контекстная справка	O/C	0
`helpme %`	Вывод описания параметров и веток, доступных на текущем уровне дерева конфигурации	O/C	0
`!`	Вывод веток, доступных на текущем уровне дерева конфигурации	O/C	0
`{`	Вход в редактируемый элемент в конфигурационном дереве	O/C	0
`}`	Выход из редактируемого элемента в конфигурационном дереве	O/C	0
`+= ( VALUE VALUE )`	Добавить несколько значений в редактируемый элемент конфигурации – массив	C	4
`+= VALUE`	Добавить значение в редактируемый элемент конфигурации – массив	C	4
`-= ( VALUE VALUE )`	Удалить несколько значений из редактируемого элемента конфигурации – массива	C	4
`-= VALUE`	Удалить значение из редактируемого элемента конфигурации – массива	C	4
`#ИМЯ?`	Присвоить значение редактируемому элементу конфигурации или массиву	C	4
`add (VALUE VALUE )`	Добавить несколько значений в редактируемый элемент конфигурации – массив	C	4
`add VALUE`	Добавить значение в редактируемый элемент конфигурации – массив	C	4
`apply`	Применение конфигурации (безусловное)	C	8
`clear brasinfo all`	Удаление 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

Команда	Описание	Режим	Приоритет
clear sessions all	Очистка таблицы трансляций	C	4
cloneacl SRCNAME NEWNAME	Создание копии ACL содержащую все правила, но имеющую другое имя	C	4
CONFIGITEMNAME	Выбор текущего конфигурационного элемента	O/C	0
configure	Переход в конфигурационный режим	O	0
copy SRC_PROFILENAME DST_PROFILENAME	Копирование конфигурации в указанную. Неприменимо к factory и effective	C	5
copy hwinfo URL	Копирование информации об устройстве в файл на удаленном сервере	O	
create acl ACLNAME	Создание ACL	C	4
create pool POOLNAME	Создание пула	C	4
create user USERNAME level LEVEL secret SECRETTYPE SECRETSTRING	Создание пользователя	C	15
dir	Просмотр списка конфигураций	C	4
disable	Логическое выключение объекта конфигурации (например, пула)	C	4
dpilist	Просмотр загруженных файлов списков URL-фильтрации	O/C	0
dpirun	Обновление базы сайтов из загруженных и включённых списков URL-фильтрации	C	4
dropacls	Удаление всех ACL сразу	C	4
droppools	Удаление всех пулов сразу	C	4
droppolicies	Удаление всех политик сразу	C	4
dropradius	Удаление настроек RADIUS-сервера	C	4
dropservices	Удаление всех сервисов сразу	C	4
edit acl ACLNAME edit ACLNAME	Переход к указанному ACL в дереве конфигурации	O/C	0
edit date DATE	Установка новой даты на устройстве	C	14
edit datetime DATETIME	Установка новый даты и времени на устройстве	C	14
edit pool POOLNAME edit POOLNAME	Переход в дереве конфигурации к указанному пулу	O/C	0
edit time TIME	Установка времени на устройстве	C	14
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	C	15
firmware install	Установка скачанного обновления прошивки	C	15
firmware revert	Установка перезапуска с неактивной прошивки	C	15

Команда	Описание	Режим	Приоритет
`firmware rollback`	Отмена перезапуска с неактивной прошивки	C	15
`firmware status`	Вывод информации об установленных прошивках и их статусе	C	15
`firmware unlock`	Сброс заблокированного процесса обновления прошивки	C	15
`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
`load effective`	Загрузка эффективной конфигурации для редактирования	C	4
`load factory`	Загрузка заводской конфигурации по умолчанию	C	4
`load PROFILENAME`	Загрузка указанной конфигурации для редактирования	C	4
`load startup`	Загрузка стартовой конфигурации для редактирования	C	4
`no acl ACLNAME`	Удаление ACL	C	4
`no pool POOLNAME`	Удаление пула	C	4
`no RULEPRIOIRTY`	Удаление правила ACL (контекстная команда, допускается только внутри самой ACL)	C*	4
`no use ACLNAME POOLNAME`	Разорвать связь между пулом и ACL	C	4
`no user USERNAME`	Удаление пользователя	C	15
`poweroff`	Завершение работы EcoNAT и выключение питания	C	8
`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`	Ввод правила ACL (контекстная команда,	C*	4

Команда	Описание	Режим	Приоритет
`[ip] [src] SRCADDR [dst] DSTADDR`	допускается только внутри самой ACL)		
`save PROFILENAME`	Сохранение текущей редактируемой конфигурации под указанным именем. Неприменимо к factory и effective	C	5
`save startup`	Сохранение текущей редактируемой конфигурации как стартовой (не рекомендуется использовать, лучше применить конфигурацию командой **apply** и, если её работа будет устраивать, сделать её 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 arp all` `show arp IFNAME`	Вывод информации об ARP	O/C	0
`show bind`	Вывод информации о привязке локальных IP-адресов к глобальным	O/C	0
`show brasinfo IPADDR` `show brasinfo IPADDRRANGE`	Вывод BRAS информации об указанном адресе	O/C	0
`show brasinfo summary`	Просмотр краткой статистики BRAS	O/C	0
`show brasstate`	Вывод информации о состоянии BRAS	O/C	0
`show cairrecords URL`	Вывод категорий ЦАИР по адресу	O/C	0
`show cgnat errors`	Просмотр ошибок выделения портов в CG-NAT пуле	O/C	0
`show config effective`	Просмотр содержимого примененной конфигурации (редактируемая конфигурация остается неизменной)	O/C	0
`show config file PROFILENAME`	Просмотр содержимого указанной конфигурации (редактируемая конфигурация остается неизменной)	O/C	4
`show config startup`	Просмотр стартовой конфигурации (редактируемая	O/C	0

Команда	Описание	Режим	Приоритет
	конфигурация остается неизменной)		
`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 (MiB)	O/C	0
`show memstat detail`	Вывод статистики использования памяти в байтах	O/C	0
`show neighbours IFNAME` `show neighbours all`	Вывод информации, полученной от соседей по протоколу LLDP	O/C	0
`show ntp`	Вывод состояния синхронизации времени по протоколу NTP	O/C	0
`show pool POOLNAME`	Вывод содержимого конфигурации пула на консоль	O/C	0
`show pool usage`	Вывод информации об использовании пулов	O/C	0
`show pools`	Вывод содержимого всех пулов на консоль	O/C	0
`show pool brief`	Вывод краткой информации о редактируемых пулах	O/C	0

Команда	Описание	Режим	Приоритет
show power	Вывод состояния блоков питания	O/C	0
show resources	Вывод статистики ресурсов	O/C	0
show sessions gap ADDR:PORT	Вывод существующих сессий для указанной пары: глобальный адрес + глобальный порт	O/C	0
show sessions global ADDRRANGE	Вывод существующих сессий для указанного глобального адреса	O/C	0
show sessions gport PORT	Вывод существующих сессий для указанного глобального порта	O/C	0
show sessions lap ADDR:PORT	Вывод существующих сессий для указанной пары: локальный адрес + локальный порт	O/C	0
show sessions local ADDRRANGE	Вывод существующих сессий для указанного локального адреса	O/C	0
show sessions lport PORT	Вывод существующих сессий для указанного локального порта	O/C	0
show sessions rap ADDR:PORT	Вывод существующих сессий для указанной пары: внешний адрес + внешний порт	O/C	0
show sessions remote ADDRRANGE	Вывод существующих сессий для указанного внешнего адреса	O/C	0
show sessions rport PORT	Вывод существующих сессий для указанного внешнего порта	O/C	0
show statistics	Вывод статистики занятых/свободных блоков портов	O/C	0
show tacacs	Вывод информации о соединении с TACACS сервером	O/C	0
show temperature	Вывод информации о температуре на ядрах процессоров	O/C	0
show time	Вывод текущего времени устройства (всегда в UTC)	O/C	0
show version	Вывод информации о версии установленного ПО	O/C	0
show version detail	Вывод детальной информации о версии установленного ПО	O/C	0
show xlate gap ADDR:PORT	Вывод всех текущих трансляций для указанной пары: глобальный адрес+ глобальный порт	O/C	0
show xlate gastat ADDRRANGE	Вывод статистики трансляций для указанного глобального адреса	O/C	0
show xlate global ADDRRANGE	Вывод всех текущих трансляций для указанного глобального адреса	O/C	0
show xlate gport PORT	Вывод всех текущих трансляций для указанного глобального порта (независимо от адреса)	O/C	0
show xlate lap ADDR:PORT	Вывод всех текущих трансляций для указанной пары: локальный адрес + локальный порт	O/C	0
show xlate lastat ADDRRANGE	Вывод статистики трансляций для указанного локального адреса	O/C	0
show xlate local ADDRRANGE	Вывод всех текущих трансляций для указанного локального адреса	O/C	0
show xlate lport PORT	Вывод всех текущих трансляций для указанного локального порта (независимо от адреса)	O/C	0
show xlate pool POOLNAME	Вывод трансляций для указанного пула	O/C	0
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

Команда	Описание	Режим	Приоритет
`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

21.1 Фильтрация вывода команд группы Show

Для ряда команд группы **show** предусмотрена возможность фильтрации вывода по одному или нескольким условиям. Фильтрация применима к следующим подгруппам команд:

- show brasinfo
- show cgnat errors
- show config
- show counters
- show dpirecords
- show logs
- show protocols
- show protocounters
- show sessions
- show xlate

В таблице ниже дано описание доступных условий фильтрации.

Таблица 70

Условие	Результат
begin <string> b <string>	Пропуск всех строк от начала до первой строки, содержащей указанную подстроку. Если подстрока содержит пробелы, то её следует указывать в двойных кавычках
count <string> c <string>	Подсчёт количества строк в выводе команды
drop <number> d <number>	Пропуск указанного количества строк от начала вывода
exclude <string> e <string>	Исключение из вывода всех строк, содержащих указанную подстроку. Если подстрока содержит пробелы, то её следует указывать в двойных кавычках
include <string> i <string>	Вывод строк, содержащих указанную подстроку. Если подстрока содержит пробелы, то её следует указывать в двойных кавычках
more	Постраничный вывод

Условие	Результат
m	
regexp <string> r <string>	Вывод строк, удовлетворяющих указанному регулярному выражению. Синтаксис регулярных выражений определён стандартом POSIX
take <number> t <number>	Вывод указанного количества строк

Условия задаются в команде после символа | (вертикальная черта). При указании нескольких условий вертикальная черта ставится перед каждым из них. Пример:

show sessions local any | include "right now" | exclude 192.168.20 | more