

УТВЕРЖДЕН
ИСКП.30346-01 34 01-ЛУ

ZENATOR NS RT
Руководство оператора
ИСКП.30346-01 34 01
Листов 55

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

2024

Литера О1

АННОТАЦИЯ

Данный документ является руководством оператора для Zenator NS Rt (программное обеспечение (ПО) сервера удаленного доступа к виртуальной частной сети с функцией двухфакторной аутентификации сетевых клиентских устройств), далее по тексту – Zenator NS Rt или программа.

Документ описывает назначение, условия и порядок функционирования Zenator NS Rt, а также действия оператора при запуске и во время выполнения программы.

Настоящее руководство входит в состав эксплуатационной документации и рассчитано на пользователя, имеющего навыки работы в операционной системе (ОС) Linux.

СОДЕРЖАНИЕ

	Лист
1. Назначение программы	5
2. Условия выполнения программы.....	10
2.1. Требования к техническим средствам	10
2.2. Требования к пользователю	11
3. Выполнение программы	13
4. Работа в Web-интерфейсе администратора сервера регистрации	14
4.1. Вход в программу через Web-интерфейс	14
4.2. Основное окно Web-интерфеса	15
4.3. Регистрация клиента	15
4.4. Активация и деактивация устройства	17
5. Настройка фильтрации, коммутации и маршрутизации	19
5.1. Авторизация и аутентификация в CLI-интерфейсе.....	19
5.2. Работа в командной строке.....	19
5.2.1. Общие сведения	19
5.2.3. Настройка аутентификации	23
5.2.4. Система разграничения доступа	25
5.2.5. Управление пользователями и группами.....	29
5.2.6. Управление профилями конфигурации.....	31
5.2.7. Управление интерфейсами.....	34
5.2.8. Команды просмотра и управления журналами	37
5.2.9. Настройка возможностей удаленного конфигурирования.....	39
5.2.10. Обновление программного обеспечения	40
5.2.11. Системные команды	41
5.2.12. Настройка сервера регистрации.....	44
5.2.13. Контроль целостности	46
5.2.14. Управление сессиями.....	48
5.2.15. Тестирование	48
5.2.16. Доступ с помощью REST API	49
5.2.17. Технологический доступ.....	49
6. Сообщения оператору.....	50
Приложение 1. ИСКП.30346-01 34 01-1 Руководство по настройке	

Примечание. Документ ИСКП.30346-01 34 01-1 выполнен в электронном виде и находится на компакт-диске ИСКП.30346-01 96 01 с эксплуатационной документацией.

Приложение 2. Настройка сеанса связи между ПЭВМ и АП через последовательный СОМ-порт.....	51
Приложение 3. Настройка доступа к Web-интерфейсу.....	52
Перечень принятых сокращений	53

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Zenator NS Rt предназначен для предоставления защищенного доступа в корпоративную сеть с удаленных рабочих станций и персональных компьютеров мобильных сотрудников.

1.2. Zenator NS Rt выполняет функции ПО сервера удаленного доступа к виртуальной частной сети с поддержкой двухфакторной аутентификации сетевых клиентских устройств.

1.3. В части сервера регистрации Zenator NS Rt обеспечивает:

- запись и хранение данных о зарегистрированных (лицензированных) устройствах;

- запись и хранение данных о пользователях устройств, которые могут быть как организациями, так и физическими лицами;

- запись и хранение данных пользователей сети, разграничение их прав для различных операций с объектами системы (права доступа);

- выпуск, запись и отзыв записей регистрации устройств.

Лицензии на использование устройства в корпоративной инфраструктуре могут выпускаться онлайн, непосредственно через соединение клиента с сервером.

1.4. Zenator NS Rt дополнительно обеспечивает функции фильтрации сетевого взаимодействия, коммутации и маршрутизации пакетов информации сетей передачи данных по протоколам IPv4, IPv6 и предоставляет следующие телекоммуникационные услуги:

- маршрутизация/коммутация сетевого трафика;

- балансировка трафика;

- туннелирование трафика;

- динамическое конфигурирование настроек сетевых узлов;

- синхронизация часов сетевых узлов;

- перенаправление (зеркалирование) трафика;

- фильтрацию входящего, исходящего и пересылаемого трафика;

- локальное и удаленное управление.

1.5. Zenator NS Rt обеспечивает пропускную способность в режиме межсетевого экранирования не менее 400 Мбит/с при минимально допустимой заполненной таблице маршрутизации, заполненной таблице фильтрации (1000 записей), отсутствующих настройках приоритизации и длине пакета 1500 байт.

1.6. Zenator NS Rt поддерживает следующие интерфейсы:

- Ethernet 10BASE-T/100BASE-T/1000BASE-T;
- Ethernet 1000Base-X;
- RS-232.

1.7. В части работы сетевых интерфейсов Zenator NS Rt обеспечивает:

- явное задание скорости интерфейса для Ethernet (10/100/1000), режим работы (half duplex, full duplex), автосогласование;
- явную настройку максимального размера полезного блока данных (MTU) на сетевых интерфейсах, в том числе и туннельных;
- поддержку loopback-интерфейсов;
- возможность назначения нескольких IP-адресов на своих интерфейсах и подынтерфейсах;
- программное определение позиций интерфейсов;
- возможность агрегации сетевых интерфейсов в группу согласно стандарту Института Инженеров Электротехники и Электроники (IEEE) 802.3ad.

1.8. В части маршрутизации (коммутации) сетевого трафика Zenator NS Rt обеспечивает:

- маршрутизацию IP-трафика;
- статическую маршрутизацию;
- динамическую маршрутизацию;
- маршрутизацию на основе задаваемых политик (policy-routing).

1.9. Динамическая маршрутизация осуществляется по следующим протоколам:

- протокол маршрутизации (RIPv2);
- протокол динамической маршрутизации (OSPFv2).

1.10. Zenator NS Rt обеспечивает балансировку нагрузки при наличии нескольких маршрутов с одинаковой метрикой.

1.11. Zenator NS Rt обеспечивает функционирование VLAN IEEE 802.1Q.

1.12. В части туннелирования трафика Zenator NS Rt обеспечивает:

- туннелирование по протоколу туннелирования сетевых пакетов (GRE);
- туннелирование по протоколу «IP over IP» (IPIP);
- поддержку протокола туннелирования второго уровня L2TP.

1.13. В части предоставления функций посредничества Zenator NS Rt обеспечивает:

- возможность переадресации DNS-запросов от клиента к удаленному DNS-серверу (DNS-проху);

- возможность назначения и (или) изменения MAC-адреса на своих интерфейсах и подынтерфейсах;

- статическое и динамическое заполнение таблицы MAC-адресов с помощью протокола разрешения адресов (ARP);

- возможность функционирования как ARP-проху.

1.14. В части динамического конфигурирования настроек сетевых узлов Zenator NS Rt обеспечивает запрашивающие хосты IP-адресами и другими конфигурационными параметрами с помощью протокола динамической конфигурации хоста (DHCPv4).

1.15. В части реализации функций адресации Zenator NS Rt обеспечивает:

- настройка интерфейса автоконфигурированием средствами DHCPv4;

- распределение IP-адресов на определенный срок.

1.16. Zenator NS Rt обеспечивает функционирование протокола передачи точного времени (NTPv4) клиента/сервера с возможностью явно задать часовой пояс.

1.17. Zenator NS Rt обеспечивает фильтрацию IP-пакетов в соответствии с заданными правилами фильтрации на основе:

- IP-адресов отправителя и получателя;

- сетевых интерфейсов;

- протоколов;

- номеров портов UDP/TCP;

- флагов TCP/IP-пакетов;

- состояния соединений;

- прикладных протоколов и приложений.

1.18. Zenator NS Rt обеспечивает три базовые концепции трансляции адресов:

- статическая (SNAT);

- динамическая (DAT);

- маскарадная – трансляция сетевого адреса в зависимости от TCP/UDP-порта получателя (PAT).

1.19. В части защищенной передачи трафика Zenator NS Rt обеспечивает функционирование защищенной виртуальной частной сети (VPN) на основе OpenVPN.

1.20. В части локального и удаленного управления Zenator NS Rt обеспечивает возможность конфигурирования себя с помощью интерфейса командной строки (CLI) локально (путем ввода с клавиатуры текстовых команд), через выделенный порт управления и удаленно (при подключении по сетевому протоколу прикладного уровня (SSH) или Telnet).

1.21. В части предоставления функций мониторинга Zenator NS Rt обеспечивает:

- возможность вывода информации о текущей загрузке центрального процессора и оперативного запоминающего устройства;
- передачу данных о событиях на удаленный сервер (syslog);
- возможность удаленного мониторинга по протоколу SNMPv2;
- поддержку протокола оповещения канального уровня (LLDP).

1.22. В части администрирования Zenator NS Rt обеспечивает:

- проверку корректности основных задаваемых параметров функционирования;
- вывод текстового предупреждения в CLI при некорректно задаваемом параметре;
- сохранение сконфигурированных профилей;
- возможность вывода в текстовом виде имеющихся в системе профилей через интерфейс управления, а также их копирование на внешний носитель информации;
- применение сохраненных профилей;
- получение обновлений с локальных серверов с последующей полной переустановкой ПО силами администратора сети.

1.23. В части предоставления функций отказоустойчивости Zenator NS Rt обеспечивает:

- автоматическое переключение на резервный канал по сетевому протоколу, объединяющему группу маршрутизаторов в один виртуальный маршрутизатор (VRRP);
- автоматический контроль целостности программного обеспечения;

– возможность поддерживать работу сервиса сторожевого таймера («watchdog») для выполнения автоматической перезагрузки устройства в случае прекращения нормального функционирования демона (зависания).

1.24. Zenator NS Rt обеспечивает ведение журналов, в которых регистрирует следующие события:

- загрузка, инициализация системы и её остановка;
- вход (выход) пользователей в систему (из системы), с фиксацией ошибок авторизации;
- результат фильтрации входящих (исходящих) пакетов.

1.25. Zenator NS Rt позволяет сортировать, архивировать и просматривать журналы регистрации.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Требования к техническим средствам

2.1.1. Zenator NS Rt должен устанавливаться на аппаратную платформу (АП) «Сервер MS-3040» ЦРМП.466219.001 или на АП со следующими характеристиками:

- 1) процессор с архитектурой x86;
- 2) оперативная память – не менее 16 Гбайт;
- 3) постоянное запоминающее устройство – не менее 128 Гбайт;
- 4) интерфейс USB – не менее одного;
- 5) интерфейс стандарта RS-232 – не менее одного;
- 6) интерфейс Ethernet 10/100/1000BaseT, соответствующий требованиям IEEE 802.3u, 802.3ab – не менее двух;
- 7) интерфейс Ethernet 1000Base-X – не менее двух;
- 8) интерфейсный модуль SFP – не менее двух с характеристиками:
 - стандарт Ethernet – 1000Base-LX;
 - тип разъема – LC;
 - тип волокна – одномодовое;
 - длина волны – не менее 1310 нанометра;
 - скорость передачи данных – до 1,25 Гбайт/с;
 - рабочая дистанция – не менее 2000 м;
 - количество волокон – не менее двух.

Примечания:

1. Порт RS-232 необходим для технологического управления изделием в отсутствие подключаемых клавиатуры и монитора. На некоторых АП он может отсутствовать.

2. Аппаратная платформа должна быть произведена предприятием включенным в перечень производителей промышленной продукции, произведенной на территории Российской Федерации, размещенный на официальном сайте Минпромторг России.

3. Количество интерфейсов Ethernet и SFP определяется договором поставки. Допускается применение интерфейсов SFP+.

2.1.2. В зависимости от версии ПО и комплектации оборудования функциональные возможности программы могут отличаться.

2.1.3. Для эксплуатации программы необходимо наличие не менее двух штатных единиц – администратора безопасности и администратора сети.

2.2. Требования к пользователю

2.2.1. Zenator NS Rt используется в сетях связи, обрабатывающих информацию разной степени конфиденциальности.

При использовании Zenator NS Rt применяются следующие требования:

– для обработки сведений, содержащих государственную тайну, люди, допущенные к работе с программой, должны действовать в соответствии с законом РФ «О государственной тайне» от 21.07.1993 № 5485-1, а также политикой безопасности и правилами обработки сведений, содержащих государственную тайну, утвержденными на предприятии;

– для обработки сведений, содержащих коммерческую тайну, люди, допущенные к работе с программой, должны действовать в соответствии с законом РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ, а также политикой безопасности и правилами обработки сведений, содержащих коммерческую тайну, утвержденными на предприятии.

2.2.2. Для работы с Zenator NS Rt пользователю необходимо обладать следующими профессионально-техническими навыками:

– знать принципы функционирования и обладать опытом администрирования локальных вычислительных сетей;

– знать правила передачи информации, содержащей государственную или коммерческую тайну, по открытым каналам связи;

– знать средства и механизмы защиты информации, которые могут использоваться для передачи информации, содержащей государственную или коммерческую тайну, по открытым каналам связи и обладать опытом их использования;

– обладать навыками работы с ОС Linux на уровне опытного пользователя.

2.2.3. Для обслуживания программы необходимо не менее двух штатных единиц – администратор безопасности и администратор сети (пользователь программы).

Администратор безопасности должен иметь профильное образование в области информационной безопасности и обладать навыками в области администрирования средств защиты информации, а также иметь опыт администрирования локальных вычислительных сетей связи.

Администратор сети должен иметь опыт администрирования локальных вычислительных сетей связи.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. При включении блока питания АП Zenator NS Rt запускается автоматически.

3.2. Типовая первоначальная настройка и конфигурирование изделия в части фильтрации, коммутации и маршрутизации пакетов информации выполняется на предприятии-изготовителе.

3.3. Для настройки ПО сервера удаленного доступа Zenator NS Rt необходимо к АП подключить технологический монитор и клавиатуру. Если АП не имеет возможности подключения монитора и клавиатуры, то необходимо соединить ее с персональной электронно-вычислительной машиной (ПЭВМ) через USB-COM и COM-RJ 45.

Примечание. Настройка сеанса связи между ПЭВМ и АП через последовательный COM-порт приведена в приложении 2 настоящего руководства.

3.4. Управление защищенным доступом в корпоративную сеть осуществляется с помощью Web-интерфейса администратора сервера регистрации. Работа в Web-интерфейсе приведена в разделе 4 настоящего руководства.

Управление защищенным доступом с помощью интерфейса командной строки приведено в 5.2.12 настоящего руководства.

3.5. Настройка фильтрации сетевого взаимодействия, коммутации и маршрутизации пакетов информации сетей передачи данных осуществляется с помощью интерфейса командной строки. Работа в командной строке приведена в разделе 5 настоящего руководства.

4. РАБОТА В WEB-ИНТЕРФЕЙСЕ АДМИНИСТРАТОРА СЕРВЕРА РЕГИСТРАЦИИ

4.1. Вход в программу через Web-интерфейс

4.1.1. Для начала работы в Web-интерфейсе пользователю необходимо выполнить следующие действия:

1) проверить следующие возможности браузера, установленного на рабочем месте, для корректного функционирования Web-интерфейса:

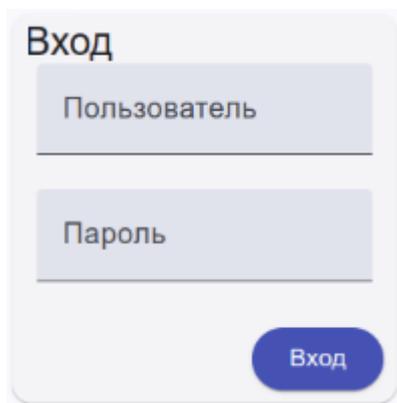
- браузер поддерживает протоколы HTTP/HTTPS;
- браузер поддерживает исполнение HTML5, Java Script и ECMA Script 5;

2) настроить сетевой интерфейс, через который будет осуществляться доступ к Web-интерфейсу.

Примечание. Настройка доступа к Web-интерфейсу приведена в приложении 3 настоящего руководства;

3) Ввести в адресной строке браузера IP-адрес и порт, через который будет осуществляться доступ к Web-интерфейсу.

Далее происходит запуск Web-интерфейса и на экране открывается окно авторизации (рис. 1).



The image shows a web form for login. At the top, the word 'Вход' is written in a dark font. Below it are two light blue input boxes. The first box is labeled 'Пользователь' and the second is labeled 'Пароль'. At the bottom right of the form is a blue button with the text 'Вход' in white.

Рис. 1

4.1.2. Для перехода к настройке защищенного доступа сетевых клиентских устройств к виртуальной частной сети необходимо ввести логин, пароль и нажать на кнопку «Вход».

Примечание. «По умолчанию» логин – «admsec», пароль – «12345678i.».

4.2. Основное окно Web-интерфеса

4.2.1. После успешного прохождения аутентификации администратор переходит в окно, примерный вид которого представлен на рис. 2.

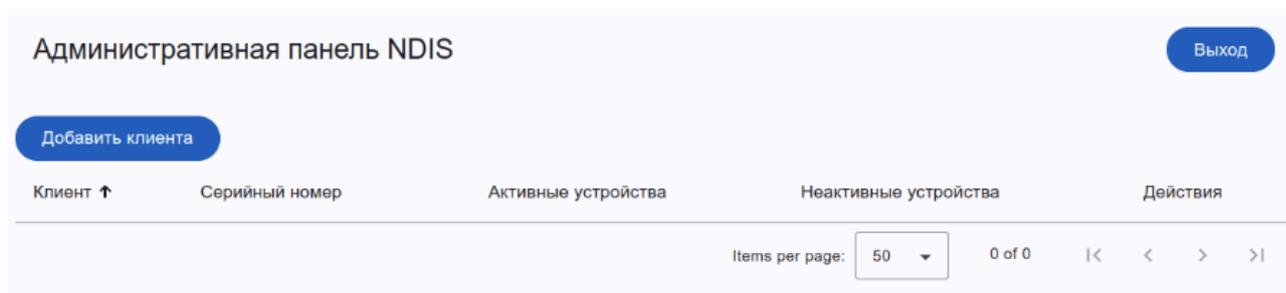


Рис. 2

4.2.2. Основное окно Web-интерфейса администратора содержит таблицу со списком клиентов NDIS и кнопки «Добавить клиента» и «Выход».

4.2.3. Список клиентов NDIS и соответствующие им устройства представлен в виде таблицы, каждая строка которой содержит следующие поля и объекты:

- «Клиент» – имя пользователя;
- «Серийный номер» – серийный номер NDIS-клиента. Поле автоматически генерируется сервером регистрации при добавлении нового клиента;
- «Активные устройства» – список UID активных устройств NDIS-клиента;
- «Неактивные устройства» – список UID неактивных устройств NDIS-клиента;
- «Действия» – кнопки «Журнал» и «Удалить».

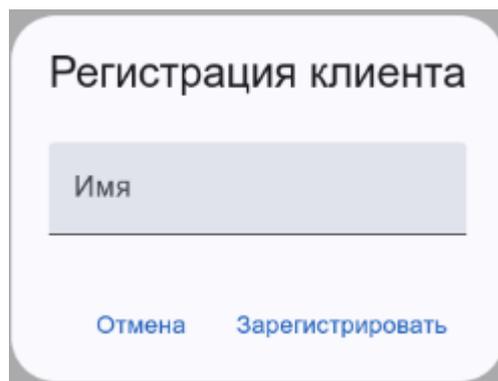
При нажатии на пункт меню «Выход» происходит выход из Web-интерфейса.

4.2.4. Для удаления клиента необходимо выбрать его в списке и нажать кнопку «Удалить». Удаление клиента приводит к удалению клиента из NDIS и OpenVPN (с отзывом сертификата).

4.2.5. Для просмотра журнала клиента необходимо выбрать его имя в списке и нажать кнопку «Журнал». При отсутствии данных в журнале, появится диалоговое окно с сообщением «Нет данных», в котором необходимо нажать кнопку «Закрыть».

4.3. Регистрация клиента

4.3.1. При нажатии на кнопку «Добавить клиента» отображается окно «Регистрация клиента», внешний вид которого представлен на рис. 3.



Регистрация клиента

Имя

Отмена Зарегистрировать

Рис. 3

4.3.2. Окно «Регистрация клиента» содержит поле для ввода имени пользователя NDIS-сервера, кнопки «Отмена» и «Зарегистрировать».

Примечание. Для регистрации клиента должен быть настроен VPN-сервер для NDIS-службы с помощью интерфейса командной строки. Пример настройки приведен в 5.2.12.2.1 данного руководства.

4.3.3. Для регистрации клиента необходимо ввести имя пользователя и нажать кнопку «Зарегистрировать», либо выйти без сохранения изменений, нажав кнопку «Отмена».

4.3.4. После регистрации клиента, имя клиента и серийный номер клиента, которое назначил ему NDIS-сервер, появятся в списке клиентов NDIS (рис. 4).



Административная панель NDIS

Выход

Добавить клиента

Клиент ↑	Серийный номер	Активные устройства	Неактивные устройства	Действия
client_name	2a31-bc1f-1fb3-236b-40f2			Журнал Удалить

Items per page: 50 1 – 1 of 1

Рис. 4

Внешний вид окна представленного на рис 4 описывает состояние службы NDIS после регистрации клиента с именем «client_name». Клиент получает свой уникальный серийный номер и использует его в дальнейшем для создания заявок на активацию устройств с помощью программы-клиента NDIS, которая вычисляет уникальный идентификатор оборудования (UID), на котором она выполняется. После получения UID оборудования от клиента сервер NDIS отмечает данное устройство как неактивное (рис. 5).

4.4. Активация и деактивация устройства

4.4.1. Для активации устройства необходимо выбрать его имя в списке клиентов NDIS (рис. 5) и нажать номер неактивного устройства.

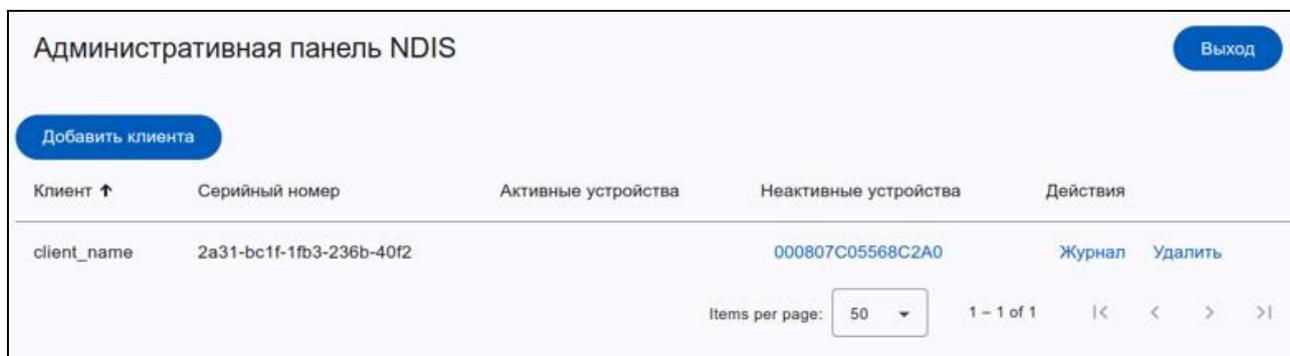


Рис. 5

Появится диалоговое окно для подтверждения активации устройства, в котором необходимо нажать кнопку «ОК», либо выйти без сохранения изменений, нажав кнопку «Отмена» (рис.6).

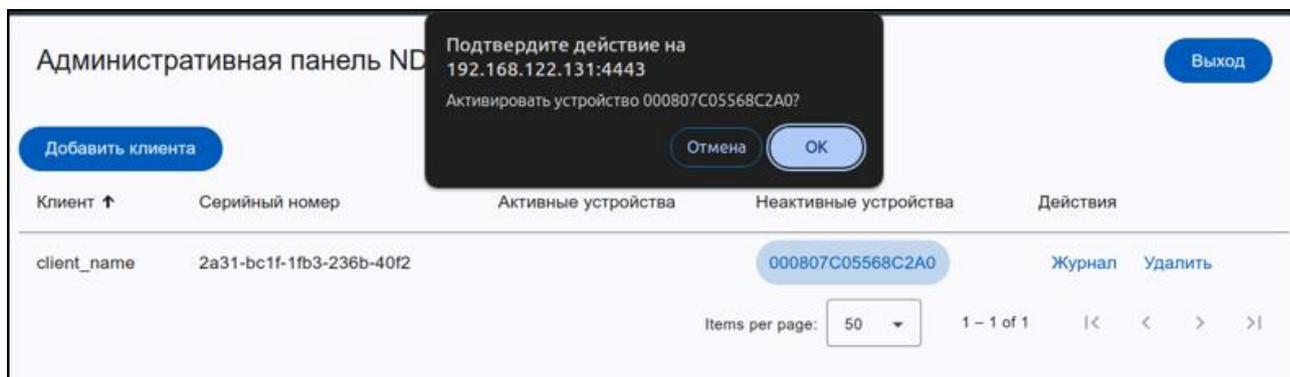


Рис. 6

4.4.2. После активации клиентского устройства окно примет вид, представленный на рис. 7.

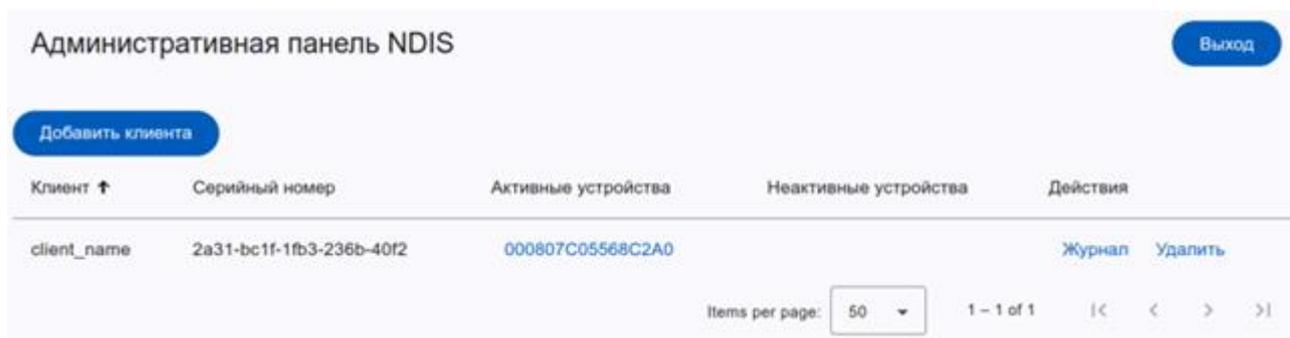


Рис. 7

4.4.3. Для отзыва лицензии необходимо выбрать его имя в списке клиентов NDIS и нажать на номер активного устройства (рис.8).

Появится диалоговое окно для подтверждения деактивации устройства, в котором необходимо нажать кнопку «ОК», либо выйти без сохранения изменений, нажав кнопку «Отмена».

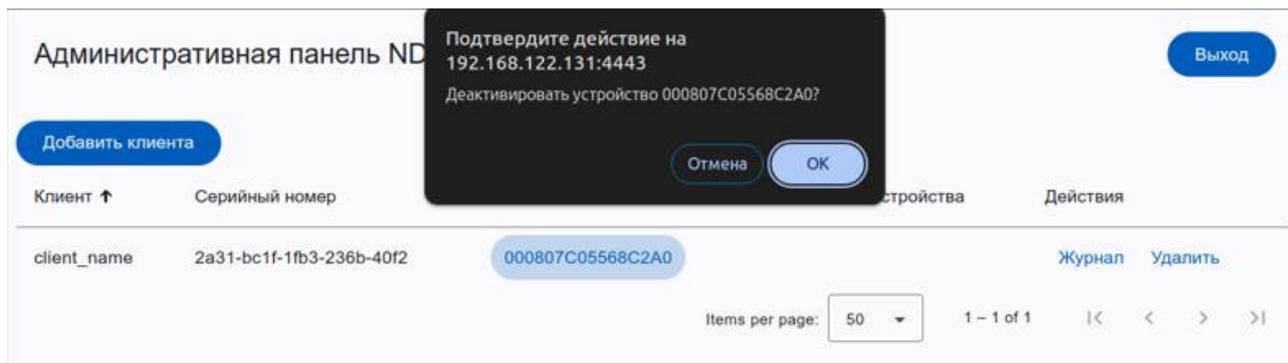


Рис. 8

5. НАСТРОЙКА ФИЛЬТРАЦИИ, КОММУТАЦИИ И МАРШРУТИЗАЦИИ

5.1. Авторизация и аутентификация в CLI-интерфейсе

5.1.1. При включении АП автоматически запускается Zenator NS Rt и начинается процедура самотестирования, при этом осуществляются следующие проверки целостности:

- файловой системы;
- ПО;
- аппаратной конфигурации.

5.1.2. После запуска программы на АП в консоли технологической ПЭВМ необходимо авторизоваться.

В поле «zenator login: » ввести имя пользователя «admsec» и нажать клавишу «Enter».

В поле «Password: » ввести пароль «12345678i.» и нажать клавишу «Enter».

Примечания:

1. Пароль на экране не отображается. Данный пароль устанавливается «по умолчанию» в процессе инсталляции программы.

2. При первом запуске рекомендуется сменить пароль на более безопасный.

3. Длина задаваемого пароля не должна превышать 32 символа.

5.1.3. После входа в систему в консоли ПЭВМ появятся следующие сообщения:

1) «Welcome <name>!» – приглашение входа в систему с учетной записью «name» («name» – имя пользователя);

2) «zenator>» – строка приглашения к вводу команд.

5.2. Работа в командной строке

5.2.1. Общие сведения

5.2.1.1. Настройку программы следует производить с использованием созданной учетной записи из консоли ПЭВМ с помощью команд CLI.

5.2.1.2. Подробное описание команд CLI и их параметров для настройки фильтрации, коммутации и маршрутизации приведено в приложении 1 к данному руководству ИСКП.30346-01 34 01-1.

5.2.1.3. При описании формата вызова команды используются символы: квадратные скобки ([]), фигурные скобки ({}), угловые скобки (< >) и вертикальная черта (|). При записи формата действуют следующие соглашения:

– параметры, указанные в квадратных скобках ([]), считаются необязательными;

– параметры, указанные в фигурных скобках ({}), считаются обязательными;

– параметры, не заключенные ни в квадратные, ни в круглые скобки, считаются обязательными;

– параметры, указанные в угловых скобках (< >) являются значением параметра;

– вертикальная черта (|) указывает, что следует выбрать только один из перечисленных параметров. Например, запись вида «[a | b]» означает, что можно выбрать либо параметр «a», либо параметр «b», либо ни один из параметров. Аналогично, запись вида «{ a | b }» означает, что нужно выбрать либо параметр «a», либо параметр «b».

5.2.1.4. При описании команд используются одни и те же параметры. Назначение этих параметров приводится при первом упоминании в команде. Далее, в последующих командах, их описание может отсутствовать.

Примечание. Приведенные правила описания команд действуют в рамках каждого подраздела руководства.

5.2.1.5. Действия оператора должны осуществляться в соответствии с подсказками, выдаваемыми в процессе настройки программы. Для вызова подсказки к команде необходимо нажать сочетание клавиш «Shift+?».

5.2.1.6. Программа обеспечивает автодополнение команд по нажатию клавиши «Tab».

В случае, если команда состоит из одного слова, то при нажатии на клавишу «Enter» происходит автодополнение и последующее выполнение команды. В случае, если команда состоит из двух слов, то при вводе первого слова и нажатии на клавишу «Enter» происходит автодополнение первого слова, при вводе второго слова и нажатии на клавишу «Enter» происходит автодополнение второго слова и выполнение команды. В случае, если команда состоит из трех и более слов, автодополнение по клавише «Enter» не выполняется.

Автодополнение команд по клавише «Пробел» выполняется только при введении команд. При вводе значений параметров автодополнение не выполняется.

5.2.1.7. Получение справочной информации по конкретной команде выполняется командой

help <command_name>

где <command_name> – имя команды.

При нажатии клавиш «Tab» или «Пробел» на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

Примечания:

1. Для перехода в конец файла справочной информации необходимо нажать сочетание клавиш «Shift + G».

2. Для выхода из файла, содержащего справочную информацию, необходимо нажать сочетание клавиш «Shift + Q».

5.2.1.8. Команды «commit», «rollback», «discard», «diff» и «! *[<comments>]*» выполняются в тех режимах конфигурации, в которых они доступны.

5.2.1.9. Применение последних изменений выполняется командой

commit [complete | confirmed] {delay}{comment}

где *complete* – гарантированное завершение отложенного коммита;

confirmed – запуск процедуры отложенного коммита. В случае невыполнения завершения отложенного коммита за время задержки выполняется откат конфигурации (*rollback*);

delay – значение задержки в секундах перед выполнением команды «*rollback*». Может принимать значения от «30» до «3600».

comment – описание для коммита, задается в двойных кавычках.

Примечания:

1. Если изменения конфигурации не применены, то в строке приглашения к вводу команд присутствует «!». После выполнения команд «*discard*» или «*commit*» знак «!» пропадает.

2. Команда «*commit*» не выполняется, если после выполнения любой команды в строке приглашения к вводу команд отсутствует «!».

5.2.1.10. Вывод статуса применения конфигурации выполняется с помощью команды

show commit status

5.2.2. Команда «*show*» позволяет посмотреть текущие настройки интерфейсов и получить полную информацию об их конфигурации.

При выводе конфигурации могут встречаться имена интерфейсов в шестнадцатеричном формате, которые соответствуют именам интерфейсов изделия в десятичном формате. Например, GigabitEthernet0/a/0 (в шестнадцатеричном формате) соответствует Ethernet 0/10/0 (в десятичном формате).

5.2.2.1. Отмена последних изменений, примененных командой «commit», выполняется с помощью команды

rollback

5.2.2.2. Проверка конфигурации системы или отдельного модуля, выполняется с помощью команды

check commit [<module>]

где <module> – модуль, для которого необходимо проверить конфигурацию.

5.2.2.3. Отмена последних изменений, не примененных командой «commit», выполняется с помощью команды

discard [<mod-name>]

где <mod-name> – модуль, для которого необходимо отменить последние изменения.

При нажатии клавиш «Tab» или «Пробел» на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

Примечание. Если параметр «mod-name» не указывать, то отмена последних изменений, не примененных командой «commit», будет выполнена для всех модулей.

5.2.2.4. Вывод всех последних изменений, еще не примененных командой «commit», выполняется с помощью команды

diff

Примечание. Если после выполнения команды «commit» никаких изменений выполнено не было, то на экран ничего выведено не будет.

5.2.2.5. Если после выполнения команды «commit» были выполнены изменения, то на экране будет отображен модуль, где будут указаны предыдущая конфигурация системы и текущая конфигурация системы. Знаком «-» и красным цветом обозначена предыдущая конфигурация системы, знаком «+» и зеленым цветом обозначена текущая конфигурация системы (команда «commit» еще не выполнялась). Для отмены выполнения команды, а также для удаления заданных параметров к команде добавляется префикс «no».

Примечание. Префикс «no» используется только для тех команд, в которых он доступен.

5.2.2.6. Программа обеспечивает возможность настройки системы с помощью команд основной конфигурации, а также выполнением команд доступных в режиме конфигурации.

После входа в режим конфигурации обеспечивается возможность выполнения команд конфигурации с помощью префикса «do» добавленного к команде

```
do <command>
```

где <command> – команда из режима основной конфигурации.

Примечание. С префиксом «do» могут выполняться все команды основной конфигурации, кроме «discard», «load» и «commit».

5.2.2.7. Для активации/деактивации системного почтовика используется команда

```
system mailer {integrity | login | alert | failure} {on | off}
```

где on – включение системного менеджера;

off – выключение системного менеджера.

5.2.2.8. Добавление комментария в историю пользовательского ввода выполняется при помощи специального символа «!» следующим образом

```
! [<comments>]
```

где <comments> – комментарий.

5.2.2.9. При работе с системой рекомендуется использование USB-накопителей с архитектурой файловой системы Ext2, Ext3, Ext4 и VFAT. Для обмена данными с ОС Windows необходимо использовать файловую систему VFAT.

5.2.3. Настройка аутентификации

5.2.3.1. Для задания режима аутентификации используется команда

```
system authentication mode {session | command}
```

где command – аутентификация требуется на каждую команду;

session – аутентификация требуется на каждую сессию. Используется «по умолчанию».

При задании режима сессии пользователь проходит верификацию один раз, когда заходит в систему, в дальнейшем система доверяет пользователю.

При задании режима команды, от пользователя требуется подтверждение в виде пароля на каждую команду (принцип «нулевого доверия»).

5.2.3.2. Для задания минимальной длины пароля используется команда

```
system authentication password min-length <min_len>
```

где `<min_len>` – значение минимальной длины пароля в символах. Может принимать значения от «1» до «256». Значение «по умолчанию» равно «1».

5.2.3.3. Для установки требуемого уровня сложности пароля используется команда

```
system authentication password complexity <complexity>
```

где `<complexity>` – уровень сложности пароля, может принимать значения от «0» до «3». Значение «по умолчанию» равно «0».

Для уровня сложности равного:

- «0» – требования к паролю не предъявляются;
- «1» – пароль должен содержать прописные и строчные буквенные символы;
- «2» – пароль должен содержать прописные и строчные буквенные символы, цифры;
- «3» – пароль должен содержать прописные и строчные буквенные символы, цифры и специальные символы.

5.2.3.4. Сброс настроек аутентификации для пользователя выполняется командой

```
system authentication reset <user>
```

где `<user>` – имя пользователя.

5.2.3.5. Для установки количества попыток авторизации и времени блокировки/разблокировки пользователя используется команда

```
system authentication password attempts {<attempts>} [lock-time <lock_val>]  
[unlock-time <unlock_val>]
```

где `<attempts>` – максимальное количество попыток авторизации. Значение «по умолчанию» равно «3»;

`<lock_val>` – интервал между неудачными попытками ввода пароля, задается в секундах. Может принимать значения от «0» до «365», «по умолчанию» равно «0»;

`<unlock_val>` – продолжительность блокировки пользователя при превышении попыток авторизации, задается в секундах. Может принимать значения от «0» до «365», «по умолчанию» равно «60».

5.2.3.6. Включение/выключение аутентификации пользователей через radius-сервер выполняется командой

```
system authentication radius {on | off | server}
```

5.2.3.7. Включение/выключение аутентификации пользователей через ldap-сервер выполняется командой

```
system authentication ldap {on | off}
```

5.2.3.8. Отображение конфигурации аутентификации пользователя для пользователя или для всех пользователей выполняется командой

show system authentication local [<user>]

5.2.4. Система разграничения доступа

5.2.4.1. Система дискреционного доступа, входящая в состав агента управления, вводит дополнительный функционал по обеспечению разграничения доступа на основе дискреционной модели.

5.2.4.2. Для реализации данного функционала вводится понятие объекта (ресурса) доступа. В Zenator NS Rt определен следующий перечень защищаемых информационных ресурсов:

- команды;
- журналы;
- внешние носители информации (USB-накопители);
- профили (текущая конфигурация устройства или сохранённая в файле).

Для каждой команды CLI вводится запись, сопоставляющая имя команды и список ресурсов, к которым команде необходим доступ для успешного выполнения.

5.2.4.3. Для взаимодействия с Zenator NS Rt предусмотрено три группы пользователей:

- администраторы сети (АС) (группа «admin»);
- администраторы безопасности (АБ) (группа «admsec»);
- администраторы аудита (АА) (группа «admaud»).

Матрица доступа определяет и разграничивает права АС, АБ и АА, которые представлены в таблице 1.

Таблица 1

Пользователь/функция	АБ	АС	АА	Примечание
Создание, сохранение, применение профиля конфигурации изделия	+	-	-	Согласно ролевой модели в части профилей конфигурации (таблица 2)
Импорт профиля конфигурации с внешнего носителя	+	-	-	
Экспорт профиля конфигурации на внешний носитель	+	-	-	Строго владелец профиля конфигурации
Управление учетными записями пользователей	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
Изменение качества паролей, настройка пароля временного действия	+	-	-	
Настройка политики блокировки пользователей при неуспешном использовании механизма аутентификации/идентификации: – время блокировки; – количество неуспешных попыток, после которых пользователь блокируется	+	-	-	
Модификация прав на функционал согласно ролевой модели	+	-	-	Включение/выключение прав «по разрешению»
Настройка физических интерфейсов	+	-	-	
Настройка loopback-интерфейсов	+	-	-	
Настройка работы в режиме сетевого моста	+	-	-	
Настройка конфигурации VLAN в рамках сетевого моста	+	-	-	
Настройка маршрутизации, основанной на политиках маршрутизации	+	-	-	
Настройка трансляции портов и адресов средствами NAT	+	-	-	
Настройка агрегации физических интерфейсов	+	-	-	
Настройка статической, динамической маршрутизации (RIPv2, RIPv2, OSPFv2)	+	-	-	
Настройка протоколов VRRP, BFD, LLDP	+	-	-	
Настройка режима работы изделия в кластере вида «Активный» / «Пассивный»	+	-	-	
Настройка DHCP-сервера	+	-	-	
Настройка DNS-клиента, DNS-проxy	+	-	-	
Настройка конфигурации туннелей IPsec, L2TP, IPsec/GRE, OpenVPN	+	-	-	
Настройка доступа по протоколам SSHv2, Telnet и SNMP	+	-	-	
Настройка зеркалирования трафика на физические интерфейсы	+	-	-	
Настройка конфигурации доступа с помощью REST API- сервера	+	-	-	
Добавление/удаление доверенных узлов и сетей в части управления изделием	+	-	-	
Настройка скорости физического интерфейса, режима работы (half duplex, full duplex)	+	-	-	
Настройка времени по сетевому протоколу NTP	+	-	-	
Настройка ARP-проxy	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
Разделение трафика в соответствии с классом трафика между физическими каналами	+	-	-	
Применение правил фильтрации на основе ACL	+	-	-	
Включение/выключение учета событий, подвергающихся аудиту в: – журнал «auth» (журнал информации о фактах идентификации, аутентификации); – журнал «ipfilter» (журнал событий срабатывания правил межсетевого экранирования); – журнал «commands» (журнал команд администратора, вводимых с консоли управления); – журнал «daemon» (внутренний журнал агента управления); – журнал «testing» (информация о самотестировании системы); – журнал «syslog» (информация от ядра ОС и системных утилит); – журнал «router» (информация о работе протоколов динамической маршрутизации)	+	-	-	
Включение/выключение выдачи предупреждающих сообщений на консоль управления изделия	+	-	-	
Настройка параметров архивации журналов	+	-	-	
Включение/выключение записи событий, подвергающихся аудиту, на внешний узел по протоколу Syslog, SNMP trap	+	-	-	
Тестирование целостности по запросу, конфигурация расписания самотестирования целостности	+	-	-	
Проведение ручного тестирования: – правил фильтрации; – прохождения сетевых пакетов	+	-	-	
Настройка внутреннего представления времени	+	-	-	
Предоставление технологического доступа к изделию	+	-	-	
Задание политики фильтрации «по умолчанию»	+	-	-	
Выключение/перезагрузка изделия	+	-	-	
Возврат до заводских настроек	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
Задание серверов, с которых будет осуществляться загрузка обновлений изделия с последующей их установкой	+	-	-	
Создание шаблонов (списков) правил фильтрации трафика	+	-	-	
Управление Zenator NS Rt с помощью: – локального управления; – протоколов Telnet, SSHv2 и REST API	+	-	-	
Мониторинг состояния каналов средствами ICMP	+	-	-	
Настройка числа одновременных подключений с одного IP-адреса	+	-	-	
Выгрузка журналов событий, подвергаемых аудиту, на внешний носитель	+	-	-	
Программное отключение внешнего носителя	+	-	-	
Просмотр информации о текущей загрузке центрального процессора и ОЗУ	+	-	-	
Просмотр настроек в части: – интерфейсов; – статической маршрутизации; – динамической маршрутизации (RIPv2, RIPv6, OSPFv2); – приоритизации трафика; – протоколов LLDP, IKE	+	-	-	
Просмотр журналов событий: – журнала «auth»; – журнала «ipfilter»; – журнала «commands»; – журнала «daemon»; – журнала «testing»; – журнала «syslog»; – журнала «router»	+	-	-	Просмотр позволяет осуществлять выборку и сортировку данных из журнала
Просмотр настроек изделия в части: – маршрутизации, основанной на политиках; – трансляции адресов; – списков классификации трафика	+	-	-	
Просмотр настроек изделия в части: – туннелирования; – фильтрации трафика; – управления изделием; – журналирования; – самотестирования (контроля целостности); – протокола NTP	+	-	-	

5.2.4.4. В таблице 2 представлена ролевая модель доступа к профилям конфигурации.

Таблица 2

Право	Пояснение	Примечание
г	Применение/чтение профиля конфигурации	
w	Модификация сохраненного профиля конфигурации	
с	Разрешение смены активного профиля на другой и/или создание нового профиля на основе активного	
о	Владелец профиля может модифицировать права доступа на данный профиль. Право владения профилем конфигурации подразумевает возможность его удаления, а также его сохранения на внешний носитель	Единовременно может существовать только один владелец профиля конфигурации

5.2.4.5. В части конфигурации заводских настроек для АБ разрешен полный доступ ко всем функциям изделия.

5.2.5. Управление пользователями и группами

5.2.5.1. Для взаимодействия с программой предусмотрено три группы пользователей:

- «admin» – администраторы сети;
- «admsec» – администраторы безопасности;
- «admaud» – администраторы аудита.

5.2.5.2. После первоначальной установки существуют следующие учётные записи:

- «admin» – в группе admin;
- «admsec» – в группе admsec;
- «admaud» – в группе admaud.

Для учетных записей «admsec», «admin» и «admaud» изначально установлен пароль «12345678i.» без кавычек.

Указанные выше учетные записи не могут быть удалены.

5.2.5.3. Создание нового пользователя выполняется командой

```
system user add {admin | admsec | admaud} <name> password <pass> [aging  
<age_val>]
```

где <name> – имя нового пользователя. Может принимать значения от «2» до «32»;
<pass> – пароль для нового пользователя. Длина пароля должна быть не меньше минимальной длины пароля, заданной с помощью команды приведенной в 5.2.3.2;

<age_val> – количество дней жизни пароля.

5.2.5.4. Блокировка/разблокировка пользователя выполняется командой

```
system user {lock | unlock} <name>
```

где <name> – имя пользователя;

lock – блокировать пользователя;

unlock – разблокировать пользователя.

Примечание. Возможности блокировки пользователя «admsec» не существует.

5.2.5.5. Изменение пароля существующего пользователя выполняется командой

```
system user edit <name> password <pass> [aging <age_val>]
```

где <pass> – новый пароль для пользователя. Длина пароля должна быть не меньше минимальной длины пароля, заданной с помощью команды, приведенной в 5.2.3.2.

5.2.5.6. Добавление/удаление почты пользователя выполняется командой

```
[no] system user mail <name> <email>
```

где <email> – почта пользователя. Почтовое имя пользователя задается в формате «abc@def.mail».

5.2.5.7. Удаление пользователя выполняется командой

```
system user del <name>
```

5.2.5.8. Установка/удаление лимита подключений к системе для пользователя выполняется командой

```
[no] system user limit <name> <limit>
```

где <limit> – ограничение одновременного входа пользователей в систему.

5.2.5.9. Просмотр списка пользователей системы, их группы и статус выполняется командой

```
show system users
```

5.2.5.10. Примечание. При выводе списка пользователей системы около имени заблокированного пользователя отображается восклицательный знак (например, «(!) user»).

5.2.6. Управление профилями конфигурации

5.2.6.1. Установка доступа/запрета на выполнение команды выполняется командой

```
grant command access {admin | admsec | admaud} {p | d} <module_name>  
“<command_name>”
```

где <module_name> – имя модуля;

<command_name> – имя команды. Необходимо указывать в двойных кавычках.

p – разрешить выполнение команды (permit);

d – запретить выполнение команды (deny).

Примечание. Команда выполняется для групп «admin» и «admaud» при наличии прав на выполнение для конкретной группы пользователей.

5.2.6.2. Регистрация нового пустого профиля выполняется командой

```
register profile <profile_name>
```

где <profile_name> – имя профиля.

Примечание. Для регистрации профиля команда «commit» не требуется.

5.2.6.3. Назначение права доступа к профилю для группы пользователей выполняется командой

```
grant profile access {admin | admsec | admaud} [rwco] <profile_name>
```

где параметры <r>, <w>, <c>, <o>:

– <r> – применение/чтение профиля конфигурации;

– <w> – модификация сохраненного профиля конфигурации;

– <c> – смена активного профиля и/или создание нового профиля на основе активного;

– <o> – владелец профиля может модифицировать права доступа на данный профиль;

<profile-name> – имя профиля.

Право владения профилем конфигурации подразумевает возможность его удаления, а также его сохранения на внешний носитель. Возможно присвоение прав владельца нескольким группам пользователей.

5.2.6.4. Удаление из списка ранее зарегистрированного профиля выполняется командой

```
unregister profile <profile_name>
```

5.2.6.5. Назначение прав доступа на произведение действий над журналами для группы пользователей выполняется командой

```
grant log access {admin | admsec | admaud} [rw] {syslog | auth | commands | daemon | ipfilter | testing | router}
```

где параметры <r>, <w>:

- <r> – чтение;
- <w> – запись на внешний носитель.

5.2.6.6. Регистрация внешнего носителя системы выполняется командой

```
register flash
```

5.2.6.7. Удаление внешнего носителя из списка зарегистрированных в системе устройств выполняется командой

```
unregister flash <num>
```

где <num> – номер внешнего носителя.

5.2.6.8. Монтирование USB-накопителя в систему выполняется командой

```
system mount flash
```

5.2.6.9. Отмонтирование USB-накопителя от устройства выполняется командой

```
system umount flash
```

Примечание: Последовательность работы с flash-накопителем выглядит следующим образом:

```
register flash
```

```
system mount flash
```

```
system umount flash
```

```
unregister flash <number>
```

5.2.6.10. Сохранение профиля с конфигурацией в системе выполняется командой

```
save profile <profile_name>
```

Примечания:

1. Для сохранения профиля его следует сначала зарегистрировать.
2. При сохранении профиля команда «commit» не требуется.

5.2.6.11. Сохранение профиля конфигурации на первый примонтированный USB-накопитель выполняется командой

save profile <profile_name> flash

5.2.6.12. Загрузка профиля с базовой конфигурацией выполняется командой

load profile <profile_name>

Примечания:

1. Перед загрузкой нового профиля удаляются все настройки текущего профиля.

2. Загрузка профиля группы пользователей с разрешением доступа только на чтение и модификацию (параметры «gw» заданные в соответствии с 5.2.6.3) делает недоступным загрузку других профилей.

5.2.6.13. Загрузка профиля конфигурации в систему с первого примонтированного USB-накопителя выполняется командой

load profile <profile_name> flash

Примечание. Для применения профиля необходимо его зарегистрировать в системе в соответствии с 5.2.6.2 и загрузить в соответствии с 5.2.6.12.

5.2.6.14. Сброс настроек конфигурации программного обеспечения к заводской базовой конфигурации выполняется командой

load profile null

Примечания:

1. При выполнении этой команды будут удалены все несохраненные настройки.

2. После выполнения команды сохраненные ранее профили остаются в системе.

3. После выполнения команды происходит автоматический вход под пользователем, выполнившим команду.

5.2.6.15. Установка профиля как загружаемого при старте системы выполняется командой

set running-profile <config_name>

где <config_name> – имя профиля.

5.2.6.16. Вывод текущих настроек прав доступа к команде выполняется командой

show command access <module_name> “<command_name>”

где <module_name> – имя модуля;

<command_name> – имя команды. Необходимо указывать в двойных кавычках.

5.2.6.17. Вывод текущих настроек прав доступа к журналам выполняется командой

show log access {syslog | auth | commands | daemon | ipfilter | testing | router}

5.2.6.18. Вывод списка команд, которые доступны данной группе пользователей, выполняется командой

show group access {admin | admsec | admaud}

Примечания:

1. Для перехода в конец списка команд необходимо нажать сочетание клавиш «Shift+G».

2. Для выхода из списка команд необходимо нажать сочетание клавиш «Shift+Q».

5.2.6.19. Вывод текущих настроек прав доступа для профиля выполняется командой

show profile access <profile_name>

5.2.6.20. Вывод списка всех зарегистрированных профилей конфигурации, а также информации, какой профиль активный, а какой загружается при старте системы, выполняется командой

show profiles

5.2.6.21. Вывод конфигурации профиля выполняется командой

show profiles [<profiles_name>]

5.2.6.22. Вывод списка зарегистрированных в системе внешних носителей выполняется командой

show flash

5.2.6.23. Вывод текущей конфигурации системы или конкретного модуля выполняется командой

show running-profile [<module_name>]

1. Для выхода из файла текущей конфигурации необходимо нажать комбинации клавиш «Shift+Q».

2. При нажатии комбинации клавиш «Shift+?», после ввода команды «show running-profile», на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

5.2.7. Управление интерфейсами

5.2.7.1. Вход в режим конфигурации интерфейса выполняется командой

interface <iface_name>

где <iface_name> – имя интерфейса.

5.2.7.2. Включение/выключение визуальной индикации на интерфейсе выполняется командой

```
blink <iface_name> {on | off}
```

Приведенные ниже в 5.2.7.3 – 5.2.7.13 команды выполняются в режиме конфигурации физического интерфейса и при выключенном интерфейсе.

5.2.7.3. Выключение/включение интерфейса выполняется командой

```
[no] shutdown
```

5.2.7.4. Установка/удаление IP-адреса интерфейса выполняется командой

```
[no] (ip4-address | ip6-address } <ip_addr/mask>
```

где <ip_addr/mask> – IP-адрес/маска подсети интерфейса.

Примечание. Одному интерфейсу можно назначить больше одного IP-адреса.

5.2.7.5. Включение/выключение DHCP-клиента на интерфейсе выполняется командой

```
[no] (ip4-address | ip6-address } dhcp [nodns] [nodefault]
```

где nodns – включить режим без dns;

nodefault – включить режим без маршрутов «по умолчанию».

Ответ от DHCP-сервера передается в течение 180 секунд.

Примечание. Перед включением DHCP-клиента необходимо включить интерфейс.

5.2.7.6. Установка/удаление значения MTU на интерфейсе выполняется командой

```
[no] mtu <mtu>
```

где <mtu> – параметр MTU, задается в октетах. Может принимать значения от «68» до «9216».

При удалении текущего значения MTU на интерфейсе происходит установка значения «по умолчанию».

5.2.7.7. Включение/выключение неразборчивого режима приема пакетов на интерфейсе выполняется командой

```
[no] promiscuous
```

5.2.7.8. Установка/удаление текущего MAC-адреса интерфейса выполняется командой

```
[no] mac-address <mac>
```

где <mac> – значение MAC-адреса в формате «hh:hh:hh:hh:hh:hh».

При удалении текущего значения MAC-адреса на интерфейсе происходит установка значения «по умолчанию».

5.2.7.9. Установка/удаление описания интерфейса выполняется командой
[no] description <comment>

где <comment> – описание интерфейса.

Примечание. Описание интерфейса указывается без кавычек в случае содержания в описании одного слова и в двойных кавычках при двух и более словах. Текст в описании может содержать пробелы, не может содержать символы «'» и «-» и превышать 255 символов.

5.2.7.10. Включение/выключение режима автосогласования связи интерфейса выполняется командой

autonegotiation {on | off}

Примечание. В случае включенного автосогласования режима связи интерфейса, происходит автоматическое согласование скорости интерфейсов. При этом устанавливается наименьшая из указанных в канале скоростей.

5.2.7.11. Установка скорости интерфейса выполняется командой

speed <speed_value>

где <speed_value> – скорость, может принимать значения «10», «100», «1000», «10000».

Примечание. В случае включенного автосогласования скорости, происходит автоматическое согласование режимов связи интерфейсов.

5.2.7.12. Установка дуплексного/полудуплексного режима связи интерфейса выполняется командой

duplex <duplex_value>

где <duplex_value> – режим связи интерфейса, может принимать значения «full», «half».

5.2.7.13. Выход из режима конфигурации физического интерфейса выполняется командой

exit

5.2.7.14. Вывод конфигурации всех интерфейсов или определенного интерфейса выполняется командой

show interfaces [detail] [serial | <iface_name>] [statistics]

где serial – отображение информации о последовательных интерфейсах;

detail – отображение расширенных настроек конкретного интерфейса или всех интерфейсов;

statistics – отображение статистики. Применение опции возможно при задании имени определенного интерфейса.

5.2.7.15. Вывод информации о DHCP-клиентах выполняется командой

```
show dhcp-client [<iface_name>]
```

5.2.8. Команды просмотра и управления журналами

5.2.8.1. Задание максимального размера журнала перед архивацией выполняется командой

```
log rotate max-size <log_size>
```

где **<log_size>** – предельный объем архивов для журнала в Мбайт. Может принимать значения от «1» до «3600». Значение «по умолчанию» равно «10».

Сброс текущего значения размера журнала и установка значения «по умолчанию» выполняется командой

```
no log rotate max-size
```

5.2.8.2. Задание максимального количества архивных файлов выполняется командой

```
log rotate count <log_num>
```

где **<val>** – максимальное количество архивных файлов. Может принимать значения от «1» до «100». Значение «по умолчанию» равно «5».

Сброс текущего значения и установка значения «по умолчанию» выполняется командой

```
no log rotate count
```

5.2.8.3. Установка/удаление временного интервала фоновой проверки размера журналов выполняется командой

```
[no] log rotate interval <log_time>
```

где **<log_time>** – временной интервал, задается в секундах. Может принимать значения от «1» до «65535». Значение «по умолчанию» равно «60».

5.2.8.4. Включение/отключение локального хранения журнала выполняется командой

```
[no] log <facility> local {on | off}
```

где **<facility>** – выбор журнала. Параметр может принимать следующие значения:

– **syslog** – журнал системных команд;

- auth – журнал событий аутентификации;
- commands – журнал команд пользователя;
- daemon – журнал выполненных функций;
- ipfilter – журнал событий срабатывания правил межсетевого экранирования;
- testing – журнал тестирования и самотестирования системы;
- router – журнал, содержащий информацию о работе протоколов динамической маршрутизации.

5.2.8.5. Включение/отключение удаленного хранения журнала выполняется командой

```
[no] log <facility> remote {on | off}
```

5.2.8.6. Указание/удаление IP-адреса удаленного сервера хранения журналов выполняется командой

```
[no] log <facility> remote <ip_addr> [port <port>]
```

где <ip_addr> – IP-адрес удаленного сервера хранения журналов;

<port> – номер порта удаленного сервера хранения журналов. «По умолчанию» используется порт «514».

5.2.8.7. Включение/отключение вывода на экран терминала выполняется командой

```
[no] log <facility> terminal {on | off}
```

Вывод происходит в тот терминал, из которого была вызвана команда.

5.2.8.8. Выгрузка журнала на внешний носитель выполняется командой

```
save log <facility> flash [clear]
```

где flash – первый примонтированный внешний носитель;

clear – очистить журнал после копирования на внешний носитель.

5.2.8.9. Для установки/изменения уровня журналирования сообщений используется команда

```
log level <facility> <level>
```

где <level> – уровень записи в журнал.

Параметр может принимать следующие значения:

- debug – отладочная информация;
- info – информационные сообщения;
- warning – предупреждения;
- error – сообщения об ошибках;
- critical – критические ошибки в программе.

5.2.8.10. Вывод журнала выполняется командой

```
show log <facility> [search [after <start_date> <start_time>] | [before <end_date>
<end_time>]] | [sender <name_sender>] | [success {OK | FAIL}] | [action <action>] |
[level <level>] | [module <name_module>] | [text <text>] [limit <limit>] [tail <count_tail>]
```

где <start_date> – начальная дата интервала поиска в формате «yyyy-mm-dd»;

<end_date> –конечная дата интервала поиска в формате «yyyy-mm-dd»;

<start_time> – начальное время интервала поиска в формате «hh:mm:ss» или «hh:mm»;

<end_time> – конечное время интервала поиска в формате «hh:mm:ss» или «hh:mm»;

<name_sender> – имя отправителя;

success – сортировка по успешности действия. Параметр может принимать значения «OK» или «FAIL»;

<action> – действие. Поиск вхождения указанной подстроки;

<name_module> – имя модуля поиска, на основании действий которого была создана запись в журнале;

<text> – текстовая строка;

<limit> – максимальное число записей, которое необходимо вывести;

<count_tail> – количество строк с конца файла.

Примечания:

1. Параметр «start_date» должен быть меньше или равен «end_date». Параметр «start_time» должен быть меньше или равен «end_time».

2. Для перехода в конец файла журналирования необходимо нажать сочетание клавиш «Shift + G».

3. Для выхода из файла, необходимо нажать сочетание клавиш «Shift + Q».

5.2.8.11. Просмотр уровня логирования выполняется командой

```
show log <level> <facility>
```

5.2.9. Настройка возможностей удаленного конфигурирования

5.2.9.1. Включение/выключение возможности удаленного конфигурирования Zenator NS Rt с помощью протокола SSH выполняется командой

```
system ssh {on | off}
```

«По умолчанию» протокол SSH включен.

5.2.9.2. Задание порта подключения для протокола SSH выполняется командой

ssh port <number>

где <number> – номер порта для подключения. Может принимать значения от «0» до «65535». Значение «по умолчанию» равно «22».

5.2.9.3. Установка/удаление режима разрешения доступа по SSH-протоколу определенным хостам или пользователям выполняется командой

[no] ssh {allow | deny} [user <user_name>] [host <ip_pattern>]

где <user_name> – имя пользователя;

<ip_pattern> – IP-адрес хоста;

allow – установка режима разрешения указанным пользователям доступ по SSH;

deny – установка режима запрета указанным пользователям доступ по SSH.

5.2.9.4. Вывод состояния протокола SSH выполняется командой

show ssh

5.2.9.5. Включение/выключение возможности удаленного конфигурирования Zenator NS Rt с помощью протокола Telnet выполняется командой

system telnet {on | off}

«По умолчанию» протокол Telnet включен.

5.2.9.6. Задание порта подключения для протокола Telnet выполняется командой

telnet port <number>

где <number> – номер порта для подключения. Может принимать значения от «0» до «65535». Значение «по умолчанию» равно «23».

5.2.9.7. Вывод состояния протокола Telnet выполняется командой

show telnet

5.2.10. Обновление программного обеспечения

5.2.10.1. Задание/удаление доверенного сервера обновлений выполняется командой

system update-server {main | flash} [certificate <cert_file> key <key_file>] [interval <interval>]

где main – главный сервер;

flash – обновления с флеш-носителя;

<cert_file> – имя файла, содержащего сертификат клиента;

<key_file> – имя файла, содержащего ключ сертификата;

– <interval> – промежуток времени для автоматической проверки обновлений.

При обновлении с флеш-носителя, он должен быть примонтирован и зарегистрирован в системе в соответствии с 5.2.6.9.

5.2.10.2. Вывод адреса сервера обновлений выполняется командой
show system update-server

5.2.10.3. Получение списка обновлений Zenator NS Rt выполняется командой
system update

5.2.10.4. Обновление общесистемного ПО выполняется командой
system upgrade

5.2.10.5. Откат ПО до предыдущей версии выполняется командой
system rollback

5.2.11. Системные команды

5.2.11.1. Системные команды управления пользователями и группами приведены в 5.2.5.

5.2.11.2. Администрирование системных модулей выполняется командой
system modules <name> {on | off | reload}

где <name> – название модуля;

on – включение модуля;

off – выключение модуля;

reload – перезагрузка модуля.

5.2.11.3. Просмотр списка модулей, находящихся в системе, выполняется командой

show system modules

5.2.11.4. Создание/удаление учетной записи пользователя службы поддержки выполняется командой

[no] system maintenance-access

5.2.11.5. Редактирование имени хоста системы выполняется командой

set system hostname <system_name>

где <system_name> – имя хоста системы.

5.2.11.6. Задание/удаление почтового имени «по умолчанию» выполняется командой

[no] set system mailname <mailname>

где <mailname> – почтовое имя. Почтовое имя задается в формате «abc@<имя домена>».

5.2.11.7. Перезагрузка системы без сохранения конфигурации (загружается профиль «null») выполняется командой

```
system reboot
```

5.2.11.8. Выключение системы выполняется командой

```
system shutdown
```

5.2.11.9. Включение/отключение программного интерфейса приложения (API) выполняется командой

```
system api {on | off | certificate <file_name>}
```

где <file_name> – имя файла сертификата.

5.2.11.10. Включение/выключение LLDP выполняется командой

```
system lldp {on | off}
```

5.2.11.11. Проверка доступности удаленного узла с помощью ICMP-запросов выполняется командой

```
ping <addr> [source {iface <iface_name> | addr <ip_addr>}] [size <size>] [interval <interval>] [count <count>] [timeout <timeout>] [tos <tos>],
```

где <addr> – IP-адрес удаленного узла;

<iface_name> – имя интерфейса;

<size> – размер пакета. Значение задается в байтах;

<interval> – временной интервал работы команды, задается в секундах.

Значение «по умолчанию» равно «1»;

<count> – количество генерируемых ICMP-запросов;

<timeout> – значение интервала в секундах;

<tos> – значение ToS.

Примечание. Прервать выполнение команды можно с помощью клавиши «Enter».

5.2.11.12. Захват и проверка сетевого трафика на интерфейсе выполняется командой

```
tcpdump <iface_name>
```

где <iface_name> – имя интерфейса.

5.2.11.13. Сканирование сети выполняется командой

```
nmap <host_port>
```

где <host_port> – адрес хоста и порт.

5.2.11.14. Загрузка/сохранение сертификата SSL выполняется командой

```
{load | save} certificate flash <file_name>
```

где <file_name> – имя файла сертификата.

5.2.11.15. Удаление сертификата SSL выполняется командой

delete certificate {all | <file_name>}

5.2.11.16. Сохранение системных неизменяемых файлов на флеш-носитель выполняется командой

save backup flash

5.2.11.17. Разрешение доменного имени выполняется командой

domain lookup <name>

где <name> – имя сервера.

5.2.11.18. Вывод информации сертификатов SSL выполняется командой

show certificate <file_name>

где <file_name> – имя файла CA-сертификата.

5.2.11.19. Вывод информации о загруженности центрального процессора выполняется командой

show system cpu [interval <interv>]

где <interv> – время, задается в секундах.

5.2.11.20. Вывод почтового имени, заданного «по умолчанию», выполняется командой

show system mailname

5.2.11.21. Вывод имени системы выполняется командой

show system hostname

5.2.11.22. Вывод информации о загруженности оперативного запоминающего устройства выполняется командой

show system memory

5.2.11.23. Вывод названия программного обеспечения Zenator NS Rt и его версии выполняется командой

show version

5.2.11.24. Вывод номера сборки программного обеспечения Zenator NS Rt выполняется командой

show version build

5.2.11.25. Вывод состояния сервиса API выполняется командой

show system api

5.2.12. Настройка сервера регистрации

5.2.12.1. Основные команды сервера регистрации

5.2.12.1.1. Добавление пользователя клиентского устройства выполняется с помощью команды

```
ndis add user <name>
```

где <name> – имя пользователя.

5.2.12.1.2. Удаление пользователя клиентского устройства выполняется с помощью команды

```
ndis delete user <name>
```

5.2.12.1.3. Активация клиентского устройства пользователя выполняется с помощью команды

```
ndis add user <name> uid <UID>
```

где <UID> – уникальный идентификатор клиентского устройства (серийный номер клиентского устройства). При вводе значения используется автодополнение из списка неактивных устройств.

Примечание. Серийный номер появляется в списке неактивных устройств после того, как клиент NDIS присылает этот номер серверу NDIS.

5.2.12.1.4. Деактивация клиентского устройства пользователя выполняется с помощью команды

```
ndis add user <name> uid <UID>
```

Примечание. Устройство удаляется из секции [devices] конфигурационного файла.

5.2.12.1.5. Задание/удаление сервера VPN для клиентов NDIS выполняется командой

```
[no] ndis vpn <тип сервера> <имя сервера>
```

где <тип сервера> – тип сервера. Может принимать значение «openvpn»;

<имя сервера> – имя NDIS-сервера.

5.2.12.1.6. Включение/выключение NDIS-сервера выполняется командой

```
system ndis {on | off}
```

5.2.12.1.7. Вывод состояния сервера регистрации выполняется командой

```
show system ndis
```

5.2.12.1.8. Вывод списка пользователей клиентских устройств выполняется командой

```
show ndis users
```

5.2.12.1.9. Вывод списка клиентских устройств пользователя выполняется командой

```
show ndis user <name>
```

5.2.12.2. Пример настройки службы NDIS

5.2.12.2.1. Задаем сервер VPN для клиентов NDIS с помощью команд:

```
ndis vpn openvpn ovpn1  
commit
```

Примечание. OpenVPN-сервер с именем «ovpn1» должен быть настроен. Пример настройки OpenVPN-сервера приведен в приложении 1 к данному руководству ИСКП.30346-01 34 01-1 в разделе 1.34.2.

5.2.12.2.2. Генерируем серийный номер для клиента с помощью команд:

```
ndis add user client1  
commit
```

5.2.12.2.3. Вывод списка клиентских устройств пользователя выполняется командой

```
show ndis user client1
```

5.2.12.2.4. Список клиентских устройств пользователя будет иметь следующий вид (для примера):

```
Serial: <серийный номер>
```

```
Active devices:
```

```
<UID>
```

```
...
```

```
Inactive devices:
```

```
<UID>
```

```
...
```

5.2.12.2.5. Запускаем для работы службу NDIS с помощью команд:

```
system ndis on  
commit
```

5.2.12.3. Активируем пока еще неактивный UID с помощью команд:

```
ndis add user client1 uid <UID>
```

commit

Примечание. <UID> – уникальный идентификатор клиентского устройства (серийный номер клиентского устройства), которое NDIS-клиент отправил NDIS– серверу.

5.2.13. Контроль целостности

5.2.13.1. Программа имеет систему контроля целостности, обеспечивающую обслуживание двух типов объектов:

- постоянно неизменяемые;
- транзакционно-изменяемые.

К первому типу относятся системные файлы, исполняемые файлы сервисов, предоставляемых изделию.

Транзакционно-изменяемыми являются журналы и файлы конфигурации изделия.

5.2.13.2. При установке программы создаются таблицы контрольных сумм для каждого из типов объектов. Сами таблицы также подлежат контролю целостности.

Программа производит автоматическую проверку целостности транзакционно-изменяемых объектов.

Программа производит проверку целостности неизменяемых объектов при старте системы.

5.2.13.3. Принудительная проверка целостности всех журналов выполняется командой

check integrity logs

5.2.13.4. Принудительная проверка целостности журнала выполняется командой

check integrity log {syslog | auth | commands | daemon | ipfilter | testing | router}

5.2.13.5. Задание принудительной проверки всех изменяемых конфигурационных файлов изделия выполняется командой

check integrity configs

5.2.13.6. Задание принудительной проверки всех неизменяемых конфигурационных файлов изделия выполняется командой

check integrity system

5.2.13.7. Задание принудительной проверки всех неизменяемых файлов изделия выполняется командой

check integrity files

5.2.13.8. Задание интервала проверки контроля целостности выполняется командой

check integrity interval <interval_val>

где <interval_val> – значение интервала проверки, задается в секундах. Может принимать значения от «180» до «7200». «По умолчанию» проверка целостности выполняется каждые 30 мин.

5.2.13.9. Задание интервала проверки загрузки критически важных сервисов выполняется командой

check services interval <interval_val>

5.2.13.10. Задание интервала проверки диска выполняется командой

check disk interval <interval_val>

5.2.13.11. Задание интервала проверки памяти выполняется командой

check memory interval <interval_val>

5.2.13.12. Задание интервала проверки центрального процессора выполняется командой

check cpu interval <interval_val>

5.2.13.13. Отображение значения временного интервала проверки контроля целостности выполняется командой

show integrity interval

5.2.13.14. Отображение значения временного интервала проверки загрузки критически важных сервисов выполняется командой

show services interval

5.2.13.15. Отображение значения временного интервала проверки памяти выполняется командой

show memory interval

5.2.13.16. Отображение значения временного интервала проверки диска выполняется командой

show disk interval

5.2.13.17. Отображение значения временного интервала проверки центрального процессора выполняется командой

show cpu interval

5.2.14. Управление сессиями

5.2.14.1. Zenator NS Rt обеспечивает возможность одновременного подключения нескольких пользователей к системе. При входе пользователя в систему автоматически создается сессия, которая хранит параметры взаимодействия с системой. Сессия завершается при выходе пользователя из системы или по тайм-ауту (равен 10 мин).

Если пользователь не выполнял ни одной команды в течение 10 мин, автоматически происходит завершение сессии, при этом, если пользователь выполнял какие-либо другие действия, то переход к окну авторизации не происходит. При выполнении любой команды по истечении тайм-аута на экране отобразится сообщение об ошибке «Error: No session (expired, invalid...)» и будет выполнен переход к окну авторизации. При выполнении команды тайм-аут обновляется. Начало сессий и их завершение отображается в журнале «auth».

Примечание. Для пользователей, выполнивших вход в программу с помощью CLI и выполнивших вход в программу с помощью Web-интерфейса, создаются отдельные сессии.

5.2.14.2. Для вывода на экран информации о всех текущих сессиях используется команда

show sessions

Примечание. Номер текущей сессии отмечен знаком «*».

5.2.14.3. Для принудительного завершения сессии используется команда

session drop <number>

где <number> – номер сессии, которую необходимо завершить. Может принимать значения от «1» до «100».

Примечание. Данная команда обеспечивает возможность принудительного завершения как своей сессии, так и сессии, созданной другим пользователем.

5.2.15. Тестирование

5.2.15.1. Тестирование выполняется с помощью команды

test [<test_name>]

где <test_name> – имя теста.

Параметр может принимать следующие значения:

– «acl» – тест функций фильтрации и логирования;

- «static_routes» – тест функций создания статистических маршрутов;
- «bridge» – тест функций создания сетевых мостов;
- «loopback» – тест функций loopback.

5.2.15.2. Вывод списка тестов или содержание теста выполняется командой *show tests [<test_name>]*

5.2.16. Доступ с помощью REST API

5.2.16.1. В Zenator NS Rt реализован REST API - прикладной программный интерфейс, который использует HTTP-запросы для получения, извлечения, размещения и удаления данных.

Аббревиатура REST в контексте API расшифровывается как «передача состояния представления».

5.2.16.2. Подробное описание применения и настройки доступа к интерфейсу REST API приведено в приложении 3 к данному руководству ИСКП.30346-01 34 01-1.

5.2.17. Технологический доступ

5.2.17.1. Технологический доступ предназначен для прямого доступа к средствам ПО и используется службой технической поддержки для решения задач, недоступных штатными средствами.

5.2.17.2. Технологический доступ осуществляется локально или через сетевое подключение по протоколам SSH или Telnet при помощи двойной авторизации. На первом этапе сотрудником технической поддержки осуществляется ввод имени пользователя и пароля одноразовой учетной записи. На втором этапе производится авторизованное технологическое подключение.

Примечание. Для протоколов SSH и Telnet требуется предварительное включение с помощью команд «system ssh on» или «system telnet on».

5.2.17.3. Для создания одноразовой учетной записи служит команда «maintenance_access», выполняемая АБ изделия. В результате ее выполнения будет получено имя пользователя и пароль, которые необходимо сообщить при обращении в службу технической поддержки.

6. СООБЩЕНИЯ ОПЕРАТОРУ

6.1. Действия оператора должны осуществляться в соответствии с подсказками, выдаваемыми на экран монитора в процессе функционирования Zenator NS Rt.

6.2. Сообщения, выдаваемые программой оператору, могут быть двух типов:

- сообщения, отображаемые после применения изменений командой «commit»;
- сообщения, отображаемые после выполнения команды.

6.3. Все сообщения приведены в приложении 1 к данному руководству ИСКП.30346-01 34 01-1.

НАСТРОЙКА СЕАНСА СВЯЗИ МЕЖДУ ПЭВМ И АП ЧЕРЕЗ ПОСЛЕДОВАТЕЛЬНЫЙ СОМ-ПОРТ

1.1. Запустить технологическую ПЭВМ и авторизоваться в ОС.

Примечание. Установленная на технологическую ПЭВМ ОС должна быть сертифицирована.

1.2. Для установки сеанса связи между ПЭВМ и АП через последовательный СОМ-порт установить эмулятор терминала для ОС, установленной на ПЭВМ, аналогичный «minicom» для ОС на базе ядра Linux.

1.3. В данном приложении в качестве примера описан вариант установки и настройки эмулятора терминала «minicom» на ПЭВМ с предустановленной ОС «Astra Linux Special Edition» версии 1.6. Перед началом работы необходимо:

1) открыть окно терминала, нажав сочетание клавиш «Alt + T»;

2) установить «minicom» с помощью команды

```
apt-get install minicom
```

Примечание. При установке «minicom» будет запрошен инсталляционный диск ОС;

3) запустить «minicom» с помощью команды

```
minicom -s
```

4) в открывшемся окне настройки конфигурации выполнить следующие действия:

– выбрать пункт «Настройка последовательного порта» и нажать «Enter»;

– убедиться (при необходимости выставить) в том, что для параметра «Скорость/Четность/Биты» выставлено значение «115200 8N1»;

– для параметров «Аппаратное управление потоком» и «Программное управление потоком» выставить значение «нет» и нажать «Enter»;

– выбрать пункт «Сохранить настройки как df1» и нажать «Enter»;

– выбрать пункт «Выход из Minicom» и нажать «Enter»;

5) в консоли включить «minicom» с помощью команды

```
minicom -D /dev/ttyUSB0
```

где ttyUSB0 – имя и номер последовательного порта, к которому подключена АП.

НАСТРОЙКА ДОСТУПА К WEB-ИНТЕРФЕЙСУ

1.1 Запустить технологическую ПЭВМ и авторизоваться в ОС.

1.2 После запуска программы на АП в консоли технологической ПЭВМ необходимо авторизоваться.

В поле «zenator login: » ввести имя пользователя «admsec» и нажать клавишу «Enter».

В поле «Password: » ввести пароль «12345678i.» и нажать клавишу «Enter».

1.3 Настроить сетевой интерфейс, через который будет осуществляться доступ к Web-интерфейсу командами:

```
interface <iface_name>
```

```
no shutdown
```

```
ip-address dhcp
```

```
exit
```

```
commit
```

1.4 Настроить брандмауэр, разрешая входящий и исходящий трафик командами:

```
set ip4 input policy accept
```

```
set ip4 output policy accept
```

```
commit
```

1.5. Вывести конфигурацию сетевого интерфейса с помощью команды

```
show interfaces <iface_name>
```

Примечание. Зафиксировать значение IP-адреса интерфейса.

Перечень принятых сокращений

АА	– администратор аудита
АБ	– администратор безопасности
АП	– аппаратная платформа
АС	– администратор сети
ОС	– операционная система
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
API	– Application Programming Interface (программный интерфейс приложения)
ARP	– Address Resolution Protocol (протокол разрешения адресов)
CLI	– Command Line Interface (интерфейс командной строки)
DAT	– Dynamic Address Translation (динамическое преобразование адресов)
DHCP	– Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)
DNS	– Domain Name System (система доменных имен)
GRE	– Generic Routing Encapsulation («общая инкапсуляция маршрутов» – протокол туннелирования сетевых пакетов)
IEEE	– Institute of Electrical and Electronics Engineers (Институт Инженеров Электротехники и Электроники)
ICMP	– Internet Control Message Protocol (протокол межсетевых управляющих сообщений)
IPIP	– IP over IP («IP поверх IP» – протокол туннелирования)
LLDP	– Link Layer Discovery Protocol (протокол оповещения канального уровня)
MTU	– Maximum Transmission Unit (максимальный размер полезного блока данных)
NAT	– Network Address Translation (преобразование сетевых адресов)
NTP	– Network Time Protocol (протокол передачи точного времени)
OSPF	– Open Shortest Path First (протокол динамической маршрутизации)
PAT	– Port Address Translation (технология трансляции сетевого адреса в

	зависимости от TCP/UDP-порта получателя)
RADIUS	– Remote Authentication in Dial-In User Service (протокол аутентификации, авторизации, сбора сведений об использованных ресурсах)
REST API	– прикладной программный интерфейс передачи состояния представления
RIP	– Routing Information Protocol (протокол маршрутизации)
RIPng	– Routing Information Protocol Next Generation (протокол маршрутизации для IPv6)
SNAT	– Static Network Address Translation (статический NAT)
SNMP	– Simple Network Management Protocol (простой протокол сетевого управления)
SSH	– Secure Shell (сетевой протокол прикладного уровня)
VLAN	– Virtual Local Area Network (виртуальная локальная сеть)
VPN	– Virtual Private Network (виртуальная частная сеть)
VRRP	– Virtual Router Redundancy Protocol (сетевой протокол, объединяющий группу маршрутизаторов в один виртуальный маршрутизатор)

УТВЕРЖДЕН

ИСКП.30346-01 34 01-ЛУ

ZENATOR NS RT

Руководство оператора

Приложение 1

Руководство по настройке

ИСКП.30346-01 34 01-1

Листов 184

Инва. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

2024

Литера О₁

СОДЕРЖАНИЕ

	Лист
1. Настройка программы	4
1.1. Общие сведения	4
1.2. Аутентификация пользователей.....	7
1.3. Система разграничения доступа	9
1.4. Управление пользователями и группами.....	14
1.5. Управление профилями конфигурации	15
1.6. LDAP	19
1.7. RADIUS	21
1.8. Управление интерфейсами.....	21
1.9. Loopback-интерфейс.....	23
1.10. Сетевой мост.....	24
1.11. Агрегирование каналов	25
1.12. ARP	27
1.13. Статическая маршрутизация	28
1.14. Динамическая маршрутизация	29
1.14.1. OSPF	29
1.14.2. RIP.....	34
1.14.3. RIPNG	36
1.15. Route-maps	37
1.16. Правила контроля доступа.....	38
1.17. Списки контроля доступа	43
1.18. Фильтрация в соответствии с правилами доступа	44
1.19. NAT	45
1.20. Policy Basic Routing	46
1.21. Команды просмотра и управления журналами	49
1.22. DHCP–сервер.....	52
1.23. NTP	54
1.24. Установка локального времени и даты	55
1.25. Настройка возможностей удаленного конфигурирования	55
1.26. SNMP	56
1.27. Зеркалирование портов	57

1.28. Туннельный интерфейс.....	58
1.28.1. GRE.....	58
1.28.2. IPsec.....	58
1.29. VPN.....	59
1.29.1. VPN-сервер.....	59
1.29.2. VPN-клиент.....	61
1.30. OpenVPN.....	64
1.30.1. OpenVPN-сервер.....	64
1.30.2. Пример настройки OpenVPN-сервера.....	67
1.31. L2TP.....	68
1.31.1. L2TP-сервер.....	68
1.31.2. L2TP-клиент.....	71
1.32. IPSec.....	74
1.33. VRRP.....	77
1.34. LLDP.....	79
1.35. Вывод статистики.....	80
1.36. Обновление программного обеспечения.....	80
1.37. Системные команды.....	81
1.38. Команды администратора сервера регистрации.....	84
1.39. Контроль целостности.....	85
1.40. Управление сессиями.....	87
1.41. Технологический доступ.....	87
1.42. API.....	88
1.42.1. Вход в API.....	88
1.42.2. Структура REST API.....	89
1.42.3. Примеры вызова методов отображения системной информации.....	91
1.42.4. Примеры настройки системных модулей с помощью REST API.....	93
2. Сообщения, выдаваемые программой после применения изменений командой «commit».....	100
3. Сообщения, отображаемые после выполнения команд.....	125
Перечень принятых сокращений.....	183

1. НАСТРОЙКА ПРОГРАММЫ

1.1. Общие сведения

1.1.1. Настройку программы следует производить с использованием созданной учетной записи из интерфейса командной строки (CLI).

1.1.2. В данном руководстве при описании формата вызова команды используются символы: квадратные скобки ([]), фигурные скобки ({ }), угловые скобки (< >) и вертикальная черта (|). При записи формата действуют следующие соглашения:

- параметры, указанные в квадратных скобках ([]), считаются необязательными;

- параметры, указанные в фигурных скобках ({ }), считаются обязательными;

- параметры, не заключенные ни в квадратные, ни в круглые скобки, считаются обязательными;

- параметры, указанные в угловых скобках (< >) являются значением параметра;

- вертикальная черта (|) указывает, что следует выбрать только один из перечисленных параметров. Например, запись вида «[a | b]» означает, что можно выбрать либо параметр «a», либо параметр «b», либо ни один из параметров. Аналогично, запись вида «{ a | b }» означает, что надо выбрать либо параметр «a», либо параметр «b».

1.1.3. При описании команд используются одни и те же параметры. Назначения этих параметров приводятся при первом упоминании в команде. Далее, в последующих командах, их описание может отсутствовать.

Примечание. Такое правило описания команд действует в рамках каждого подраздела данного руководства.

1.1.4. Действия оператора должны осуществляться в соответствии с подсказками, выдаваемыми в процессе настройки программы. Для вызова подсказки к команде необходимо нажать сочетание клавиш «Shift+?».

1.1.5. Программа обеспечивает автодополнение команд по нажатию клавиши «Tab».

В случае, если команда состоит из одного слова, то при нажатии на клавишу «Enter» происходит автодополнение и последующее выполнение команды. В случае, если команда состоит из двух слов, то при вводе первого слова и нажатии на клавишу «Enter» происходит автодополнение первого слова, при вводе второго слова и нажатии на клавишу «Enter» происходит автодополнение второго слова и выполнение команды. В случае, если команда состоит из трех и более слов, автодополнение по клавише «Enter» не выполняется.

Автодополнение команд по клавише «Пробел» выполняется только при введении команд. При вводе значений параметров автодополнение не выполняется.

1.1.6. Получение справочной информации по конкретному модулю, выполняется командой

```
help <module_name>
```

где *<module_name>* – имя модуля.

При нажатии клавиш «Tab» или «Пробел» на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

Примечания:

1. Для перехода в конец файла справочной информации необходимо нажать сочетание клавиш «Shift + G».

2. Для выхода из файла, содержащего справочную информацию, необходимо нажать сочетание клавиш «Shift + Q».

1.1.7. Команды «commit», «rollback», «discard», «diff» и «! *[<comments>]*» выполняются в тех режимах конфигурации, в которых они доступны.

1.1.8. Применение последних изменений выполняется командой

```
commit [complete | confirmed] {delay}{comment}
```

где *complete* – гарантированное завершение отложенного коммита;

confirmed – запуск процедуры отложенного коммита. В случае невыполнения завершения отложенного коммита за время задержки выполняется откат конфигурации (*rollback*);

delay – значение задержки в секундах перед выполнением команды «*rollback*». Может принимать значения от «30» до «3600».

comment – описание для коммита, задается в двойных кавычках.

Примечания:

1. Если изменения конфигурации не применены, то в строке-приглашении к вводу команд присутствует «!». После выполнения команд «*discard*» или «*commit*» знак «!» пропадает.

2. Команда «commit» не выполняется, если после выполнения любой команды в строке-приглашении к вводу команд отсутствует «!».

1.1.9. Вывод статуса применения конфигурации выполняется с помощью команды

show commit status

1.1.10. Команда «show» позволяет посмотреть текущие настройки интерфейсов и получить полную информацию об их конфигурации.

При выводе конфигурации могут встречаться имена интерфейсов в шестнадцатеричном формате, которые соответствуют именам интерфейсов изделия в десятичном формате. Например, GigabitEthernet0/a/0 (в шестнадцатеричном формате) соответствует Ethernet 0/10/0 (в десятичном формате).

1.1.11. Отмена последних изменений, примененных командой «commit», выполняется с помощью команды

rollback

1.1.12. Проверка конфигурации системы или отдельного модуля, выполняется с помощью команды

check commit [<module>]

где <module> – модуль, для которого необходимо проверить конфигурацию.

1.1.13. Отмена последних изменений, не примененных командой «commit», выполняется с помощью команды

discard [<mod-name>]

где <mod-name> – модуль, для которого необходимо отменить последние изменения.

При нажатии клавиш «Tab» или «Пробел» на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

Примечание. Если параметр «mod-name» не указывать, то отмена последних изменений, не примененных командой «commit», будет выполнена для всех модулей.

1.1.14. Вывод всех последних изменений, еще не примененных командой «commit», выполняется с помощью команды

diff

Примечание. Если после выполнения команды «commit» никаких изменений выполнено не было, то на экран ничего выведено не будет.

1.1.15. Если после выполнения команды «commit» были выполнены изменения, то на экране будет отображен модуль, где будут указаны предыдущая конфигурация системы и текущая конфигурация системы. Знаком «-» и красным цветом обозначена предыдущая конфигурация системы, знаком «+» и зеленым цветом обозначена текущая конфигурация системы (команда «commit» еще не выполнялась). Для отмены выполнения команды, а также для удаления заданных параметров к команде добавляется префикс «no».

Примечание. Префикс «no» используется только для тех команд, в которых он доступен.

1.1.16. Программа обеспечивает возможность настройки системы с помощью команд основной конфигурации, а также выполнением команд доступных в режиме конфигурации.

После входа в режим конфигурации обеспечивается возможность выполнения команд конфигурации с помощью добавления префикса «do» к команде

do <command>

где <command> – команда из режима основной конфигурации.

Примечание. С префиксом «do» могут выполняться все команды основной конфигурации, кроме «discard», «load» и «commit».

1.1.17. Для активации/деактивации системного почтовика используется команда *system mailer {integrity | login | alert | failure} {on | off}*

где on – включение системного менеджера;

off – выключение системного менеджера.

1.1.18. Добавление комментария в историю пользовательского ввода выполняется при помощи специального символа «!»;

! [<comments>]

где <comments> – комментарий.

1.1.19. При работе с системой рекомендуется использование USB-накопителей с архитектурой файловой системы Ext2, Ext3, Ext4 и VFAT. Для обмена данными с ОС Windows необходимо использовать файловую систему VFAT.

1.2. Аутентификация пользователей

1.2.1. Задание режима аутентификации выполняется командой

system authentication mode {session | command}

где command – аутентификация требуется на каждую команду;

session – аутентификация требуется на каждую сессию. Используется «по умолчанию».

При задании режима сессии пользователь проходит верификацию один раз, когда заходит в систему, в дальнейшем система доверяет пользователю.

При задании режима команды, от пользователя требуется подтверждение в виде пароля на каждую команду (принцип «нулевого доверия»).

1.2.2. Задание минимальной длины пароля выполняется командой

system authentication password min-length <min_len>

где <min_len> – минимальная длина пароля в символах, может принимать значения от «1» до «256». Значение «по умолчанию» равно «1».

1.2.3. Установка требуемого уровня сложности пароля выполняется командой

system authentication password complexity <complexity>

где <complexity> – уровень сложности пароля, может принимать значения от «0» до «3». Значение «по умолчанию» равно «0».

Для уровня сложности равного:

- «0» – требования к паролю не предъявляются;
- «1» – пароль должен содержать прописные и строчные буквенные символы;
- «2» – пароль должен содержать прописные и строчные буквенные символы, цифры;

- «3» – пароль должен содержать прописные и строчные буквенные символы, цифры и специальные символы.

1.2.4. Установка количества попыток авторизации и времени блокировки/разблокировки пользователя выполняется командой

system authentication password attempts <attempts> [lock-time <lock_val>] [unlock-time <unlock_val>]

где <attempts> – максимальное количество попыток авторизации, может принимать значения от «1» до «256». Значение «по умолчанию» равно «3»;

<lock_val> – интервал между неудачными попытками ввода пароля, задается в секундах. Может принимать значения от «0» до «365». Значение «по умолчанию» равно «0»;

<unlock_val> – продолжительность блокировки пользователя при превышении попыток авторизации, задается в секундах. Может принимать значения от «0» до «365». Значение «по умолчанию» равно «60».

1.2.5. Сброс настроек аутентификации для пользователя выполняется командой

```
system authentication reset <user>
```

где <user> – имя пользователя.

1.2.6. Включение/выключение аутентификации пользователей через radius-сервер выполняется командой

```
system authentication radius {on | off | server}
```

1.2.7. Включение/выключение аутентификации пользователей через ldap-сервер выполняется командой

```
system authentication ldap {on | off}
```

1.2.8. Отображение конфигурации аутентификации пользователя для пользователя или для всех пользователей выполняется командой

```
show system authentication local [<user>]
```

1.3. Система разграничения доступа

1.3.1. Система дискреционного доступа, входящая в состав агента управления, вводит дополнительный функционал по обеспечению разграничения доступа на основе дискреционной модели.

1.3.2. Для реализации данного функционала вводится понятие объекта (ресурса) доступа. В Zenator NS Rt определен следующий перечень защищаемых информационных ресурсов:

- команды;
- журналы;
- внешние носители информации (USB-накопители);
- профили (текущая конфигурация устройства или сохранённая в файле).

Для каждой команды CLI вводится запись, сопоставляющая имя команды и список ресурсов, к которым команде необходим доступ для успешного выполнения.

1.3.3. Для взаимодействия с Zenator NS Rt предусмотрено три группы пользователей:

- администраторы сети (АС) (группа «admin»);
- администраторы безопасности (АБ) (группа «admsec»);
- администраторы аудита (АА) (группа «admaud»).

1.3.4. Матрица доступа определяет и разграничивает права АС, АБ и АА, которые представлены в таблице 1.

Таблица 1

Пользователь/функция	АБ	АС	АА	Примечание
Создание, сохранение, применение профиля конфигурации изделия	+	-	-	Согласно ролевой модели в части профилей конфигурации (таблица 2)
Импорт профиля конфигурации с внешнего носителя	+	-	-	
Экспорт профиля конфигурации на внешний носитель	+	-	-	Строго владелец профиля конфигурации
Управление учетными записями пользователей	+	-	-	
Изменение качества паролей, настройка пароля временного действия	+	-	-	
Настройка политики блокировки пользователей при неуспешном использовании механизма аутентификации/идентификации: – время блокировки; – количество неуспешных попыток, после которых пользователь блокируется	+	-	-	
Модификация прав на функционал согласно ролевой модели	+	-	-	Включение/выключение прав «по разрешению»
Настройка физических интерфейсов	+	-	-	
Настройка loopback-интерфейсов	+	-	-	
Настройка работы в режиме сетевого моста	+	-	-	
Настройка групп VLAN в рамках сетевого моста	+	-	-	
Настройка маршрутизации, основанной на политиках маршрутизации	+	-	-	
Настройка трансляции портов и средствами NAT	+	-	-	
Настройка агрегации физических интерфейсов	+	-	-	
Настройка статической, динамической (RIPv2, OSPFv2, RIPv2)	+	-	-	
Настройка протоколов VRRP, BFD, LLDP	+	-	-	
Настройка режима работы изделия в кластере вида «Активный» / «Пассивный»	+	-	-	
Настройка DHCP-сервера	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
Настройка DNS-клиента, DNS-проxy	+	-	-	
Настройка конфигурации туннелей IPSec, L2TP, IPIP/GRE, OpenVPN	+	-	-	
Настройка доступа по протоколам SSHv2, Telnet и SNMP	+	-	-	
Настройка зеркалирования трафика на физические интерфейсы	+	-	-	
Настройка конфигурации доступа с помощью REST API- сервера	+	-	-	
Добавление/удаление доверенных узлов и сетей в части управления изделием	+	-	-	
Настройка скорости физического интерфейса, режима работы (half duplex, full duplex)	+	-	-	
Настройка времени по сетевому протоколу NTP	+	-	-	
Настройка ARP-проxy	+	-	-	
Разделение трафика в соответствии с классом трафика между физическими каналами	+	-	-	
Применение правил фильтрации на основе ACL	+	-	-	
Включение/выключение учета событий, подвергающихся аудиту в: – журнал «auth» (журнал информации о фактах идентификации, аутентификации); – журнал «ipfilter» (журнал событий срабатывания правил межсетевого экранирования); – журнал «commands» (журнал команд администратора, вводимых с консоли управления); – журнал «daemon» (внутренний журнал агента управления); – журнал «testing» (информация о самотестировании системы); – журнал «syslog» (информация от ядра ОС и системных утилит); – журнал «router» (информация о работе протоколов динамической маршрутизации)	+	-	-	
Включение/выключение выдачи предупреждающих сообщений на консоль управления изделия	+	-	-	
Настройка параметров архивации журналов	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
Включение/выключение записи событий, подвергающихся аудиту, на внешний узел по протоколу Syslog, SNMP trap	+	-	-	
Тестирование целостности по запросу, конфигурация расписания самотестирования целостности	+	-	-	
Проведение ручного тестирования: – правил фильтрации; – прохождения сетевых пакетов	+	-	-	
Настройка внутреннего представления времени	+	-	-	
Предоставление технологического доступа к изделию	+	-	-	
Задание политики фильтрации «по умолчанию»	+	-	-	
Выключение/перезагрузка изделия	+	-	-	
Возврат до заводских настроек	+	-	-	
Задание серверов, с которых будет осуществляться загрузка обновлений изделия с последующей их установкой	+	-	-	
Создание шаблонов (списков) правил фильтрации трафика	+	-	-	
Управление Zenator NS Rt с помощью: – локального управления; – протоколов Telnet, SSH и REST API	+	-	-	
Мониторинг состояния каналов средствами ICMP	+	-	-	
Настройка числа одновременных подключений с одного IP-адреса	+	-	-	
Выгрузка журналов событий, подвергаемых аудиту, на внешний носитель	+	-	-	
Программное отключение внешнего носителя	+	-	-	
Просмотр информации о текущей загрузке центрального процессора и ОЗУ	+	-	-	
Просмотр настроек в части: – интерфейсов; – статической маршрутизации; – динамической маршрутизации (RIPv2, RIPvng, OSPFv2); – приоритизации трафика; – протоколов LLDP, IKE	+	-	-	

Пользователь/функция	АБ	АС	АА	Примечание
Просмотр журналов событий: – журнала «auth»; – журнала «ipfilter»; – журнала «commands»; – журнала «daemon»; – журнала «testing»; – журнала «syslog»; – журнала «router»	+	+	+	Просмотр позволяет осуществлять выборку и сортировку данных из журнала
Просмотр настроек изделия в части: – маршрутизации, основанной на политиках; – трансляции адресов; – списков классификации трафика	+	-	-	
Просмотр настроек изделия в части: – туннелирования; – фильтрации трафика; – управления изделием; – журналирования; – самотестирования (контроля целостности); – протокола NTP	+	-	-	

1.3.5. В таблице 2 представлена ролевая модель доступа к профилям конфигурации.

Таблица 2

Право	Пояснение	Примечание
r	Применение/чтение профиля конфигурации.	
w	Модификация сохраненного профиля конфигурации	
s	Разрешение смены активного профиля на другой и/или создание нового профиля на основе активного	
o	Владелец профиля может модифицировать права доступа на данный профиль. Право владения профилем конфигурации подразумевает возможность его удаления, а также его сохранения на внешний носитель	Единовременно может существовать только один владелец профиля конфигурации

1.3.6. В части конфигурации заводских настроек для АБ разрешен полный доступ ко всем функциям изделия.

1.4. Управление пользователями и группами

1.4.1. Для взаимодействия с программой предусмотрено три группы пользователей:

- «admin» – администраторы сети;
- «admsec» – администраторы безопасности;
- «admaud» – администраторы аудита.

1.4.2. После первоначальной установки существуют следующие учётные записи:

- «admin» – в группе «admin»;
- «admsec» – в группе «admsec»;
- «admaud» – в группе «admaud».

Для учетных записей «admsec», «admin» и «admaud» изначально установлен пароль «12345678i.» без кавычек.

Указанные выше учетные записи не могут быть удалены.

1.4.3. Создание нового пользователя выполняется командой
system user add {admin | admsec | admaud} <name> password <pass> [aging <age_val>]

где <name> – имя нового пользователя;

<pass> – пароль для нового пользователя. Длина пароля должна быть не меньше минимальной длины пароля, заданной с помощью команды, приведенной в 1.2.2;

<age_val> – количество дней жизни пароля.

1.4.4. Блокировка/разблокировка пользователя выполняется командой
system user {lock | unlock} <name>

где <name> – имя пользователя;

lock – заблокировать пользователя;

unlock – разблокировать пользователя.

Примечание. Возможности блокировки пользователя «admsec» не существует.

1.4.5. Изменение пароля существующего пользователя выполняется командой
system user edit <name> password <pass> [aging <age_val>]

где <pass> – новый пароль для пользователя. Длина пароля должна быть не меньше минимальной длины пароля, заданной с помощью команды, приведенной в 1.2.2.

1.4.6. Добавление/удаление почты пользователя выполняется командой

```
[no] system user mail <name> <email>
```

где <email> – почта пользователя. Почтовое имя пользователя задается в формате «abc@<имя домена>».

1.4.7. Удаление пользователя выполняется командой

```
system user del <name>
```

1.4.8. Установка/удаление лимита подключений к системе для пользователя выполняется командой

```
[no] system user limit <name> <limit>
```

где <limit> – ограничение одновременного входа пользователей в систему.

1.4.9. Просмотр списка пользователей системы, их группы и статус выполняется командой

```
show system users
```

Примечание. При выводе списка пользователей системы около имени заблокированного пользователя отображается восклицательный знак (например, «(!) user»).

1.5. Управление профилями конфигурации

1.5.1. Установка доступа/запрета на выполнение команды выполняется командой

```
grant command access {admin | admsec | admaud} {p | d} <module_name>  
“<command_name>”
```

где <module_name> – имя модуля;

<command_name> – имя команды. Необходимо указывать в двойных кавычках.

p – разрешить выполнение команды (permit);

d – запретить выполнение команды (deny).

Примечание. Команда выполняется для групп «admin» и «admaud» при наличии прав на выполнение для конкретной группы пользователей.

1.5.2. Регистрация нового пустого профиля выполняется командой

```
register profile <profile_name>
```

где <profile_name> – имя профиля.

Примечание. Для регистрации профиля команда «commit» не требуется.

1.5.3. Назначение права доступа к профилю для группы пользователей выполняется командой

grant profile access {admin | admsec | admaud} [rwco] <profile_name>

где параметры <r>, <w>, <c>, <o>:

- <r> – применение/чтение профиля конфигурации;
- <w> – модификация сохраненного профиля конфигурации;
- <c> – смена активного профиля и/или создание нового профиля на основе активного;
- <o> – владелец профиля может модифицировать права доступа на данный профиль;
- <profile-name> – имя профиля.

Право владения профилем конфигурации подразумевает возможность его удаления, а также его сохранения на внешний носитель. Возможно присвоение прав владельца нескольким группам пользователей.

1.5.4. Удаление из списка ранее зарегистрированного профиля выполняется командой

unregister profile <profile_name>

1.5.5. Назначение прав доступа на произведение действий над журналами для группы пользователей выполняется командой

grant log access {admin | admsec | admaud} [rw] {syslog | auth | commands | daemon | ipfilter | testing | router}

где параметры <r>, <w>:

- <r> – чтение;
- <w> – запись на внешний носитель.

1.5.6. Регистрация внешнего носителя системы выполняется командой

register flash

1.5.7. Удаление внешнего носителя из списка зарегистрированных в системе устройств выполняется командой

unregister flash <num>

где <num> – номер внешнего носителя.

1.5.8. Монтирование USB-накопителя в систему выполняется командой

system mount flash

1.5.9. Отмонтирование USB-накопителя из системы выполняется командой

system umount flash

Примечание: Последовательность работы с flash-накопителем выглядит следующим образом:

register flash

system mount flash

system umount flash

unregister flash <number>

1.5.10. Сохранение профиля с конфигурацией в системе выполняется командой

save profile <profile_name>

Примечания:

1. Для сохранения профиля его следует сначала зарегистрировать.

2. При сохранении профиля команда «commit» не требуется.

1.5.11. Сохранение профиля конфигурации на первый примонтированный USB-накопитель выполняется командой

save profile <profile_name> flash

1.5.12. Загрузка профиля с базовой конфигурацией выполняется командой

load profile <profile_name>

Примечания:

1. Перед загрузкой нового профиля удаляются все настройки текущего профиля.

2. Загрузка профиля группы пользователей с разрешением доступа только на чтение и модификацию (параметры «gw» заданные в соответствии с 1.5.2) делает недоступным загрузку других профилей.

1.5.13. Загрузка профиля конфигурации в систему с первого примонтированного USB-накопителя выполняется командой

load profile <profile_name> flash

Примечание. Для применения профиля необходимо его зарегистрировать в системе в соответствии с 1.5.2 и загрузить в соответствии с 1.5.12.

1.5.14. Сброс настроек конфигурации программного обеспечения к заводской базовой конфигурации выполняется командой

load profile null

Примечания:

1. При выполнении команды будут удалены все несохраненные настройки.

2. После выполнения команды, сохраненные ранее профили остаются в системе.

3. После выполнения команды происходит автоматический вход под пользователем, выполнившим команду.

1.5.15. Установка профиля как загружаемого при старте системы выполняется командой

```
set running-profile <config_name>
```

где *<config_name>* – имя профиля.

1.5.16. Вывод текущих настроек прав доступа к команде выполняется командой

```
show command access <module_name> “<command_name>”
```

где *<module_name>* – имя модуля;

<command_name> – имя команды. Необходимо указывать в двойных кавычках.

1.5.17. Вывод текущих настроек прав доступа к журналам выполняется командой

```
show log access {syslog | auth | commands | daemon | ipfilter | testing | router}
```

1.5.18. Вывод списка команд, которые доступны данной группе пользователей выполняется командой

```
show group access {admin | admsec | admaud}
```

Примечания:

1. Для перехода в конец списка команд необходимо нажать сочетание клавиш «Shift+G».

2. Для выхода из списка команд необходимо нажать сочетание клавиш «Shift+Q».

1.5.19. Вывод текущих настроек прав доступа для профиля выполняется командой

```
show profile access <profile_name>
```

1.5.20. Вывод списка всех зарегистрированных профилей конфигурации, а также информации, какой профиль активный, а какой загружается при старте системы, выполняется командой

```
show profiles
```

1.5.21. Вывод конфигурации профиля выполняется командой

```
show profiles [<profiles_name>]
```

1.5.22. Вывод списка зарегистрированных в системе внешних носителей выполняется командой

```
show flash
```

1.5.23. Вывод текущей конфигурации системы или конкретного модуля выполняется командой

```
show running-profile [<module_name>]
```

Примечания:

1. Для выхода из файла текущей конфигурации необходимо нажать комбинации клавиш «Shift+Q» или «Q».

2. При нажатии комбинации клавиш «Shift+?», после ввода команды «show running-profile», на экран будет выведен список всех модулей системы, для которых выполняется данная команда.

1.6. LDAP

1.6.1. Создание/удаление LDAP-клиента, а также вход в режим его конфигурации выполняется командой

```
create | delete ldap client
```

1.6.2. Загрузка сертификата с первого примонтированного USB-накопителя выполняется командой

```
load certificate flash
```

1.6.3. Сохранение сертификата на первый примонтированный USB-накопитель выполняется командой

```
save certificate flash
```

Примечание: Последовательность работы описана в 1.5.9.

Приведенные ниже в 1.6.4 – 1.6.15 команды выполняются в режиме конфигурации LDAP-клиента.

1.6.4. Установка IP-адреса хоста LDAP-сервера выполняется командой

```
host <ipaddr>
```

где <ipaddr> – IP-адрес LDAP-сервера.

1.6.5. Удаление всех LDAP-серверов или LDAP-сервера с указанным IP-адресом выполняется командой

```
no host {all | <ipaddr>}
```

1.6.6. Установка порта LDAP-сервера выполняется командой

```
port <auth_port>
```

где <auth_port> – порт LDAP-сервера.

1.6.7. Установка версии протокола LDAP выполняется командой

```
protocol {ldap_v_2 | ldap_v_3}
```

1.6.8. Установка общего имени пользователя LDAP выполняется командой
user <user_name>

где <user_name> – общее имя пользователя.

1.6.9. Установка административного пароля LDAP-сервера выполняется командой

password <pswd_string>

где <pswd_string> – пароль LDAP-сервера.

1.6.10. Установка домена выполняется командой

domain <dmn_name>

где <dmn_name> – имя домена.

1.6.11. Установка временных опций соединения выполняется командой

timelimit <time_limit> [bind <bind_val>] [idle <idle_val>]

где <time_limit> – время ожидания соединения, может принимать значения от «0» до «600000»;

<bind_val> – значение bind;

<idle_val> – значение idle.

1.6.12. Установка области поиска LDAP выполняется командой

scope {subtree | one_level | base_object}

1.6.13. Установка режима LDAP SSL выполняется командой

ssl {on | off} [reqcert <reqcert_val>]

где <reqcert_val> – уровень требования к сертификату SSL. Может принимать значения «never», «allow», «try», «demand», «hard».

1.6.14. Установка LDAP SSL-сертификата выполняется командой

ca-certificate <cert_path>

где <cert_path> – путь к сертификату.

1.6.15. Выход из режима конфигурации LDAP выполняется командой

exit

1.6.16. Включение/выключение аутентификации пользователей через LDAP-сервер выполняется командой

system authentication ldap {on | off}

1.6.17. Вывод конфигурации клиента LDAP выполняется командой

show ldap

1.7. RADIUS

1.7.1. Конфигурирование RADIUS-сервера выполняется командой

```
system authentication radius server <host> <secret> [port <port>] [src <src_addr>]  
[timeout <timeout>]
```

где <host> – IP-адрес RADIUS-сервера;

<secret> – пароль для клиента Пароль для клиента должен совпадать с паролем для RADIUS-сервера;

<src_addr> – IP-адрес, с которого будут выполняться запросы к RADIUS-серверу;

<port> – номер порта RADIUS-сервера, может принимать значения от «1024» до «65535»;

<timeout> – время ожидания ответа от RADIUS-сервера, задается в секундах. Может принимать значения от «1» до «100».

1.7.2. Удаление всех RADIUS-серверов или RADIUS-сервера с указанным IP-адресом выполняется командой

```
no system authentication radius server [<host>]
```

1.7.3. Включение/выключение RADIUS-сервера выполняется командой

```
system authentication radius {on | off}
```

1.7.4. Вывод конфигурации RADIUS -клиента выполняется командой

```
show radius client
```

1.8. Управление интерфейсами

1.8.1. Вход в режим конфигурации интерфейса выполняется командой

```
interface <iface_name>
```

где <iface_name> – имя интерфейса.

1.8.2. Включение/выключение визуальной индикации на интерфейсе выполняется командой

```
blink <iface_name> {on | off}
```

Приведенные ниже в 1.8.3 – 1.8.13 команды выполняются в режиме конфигурации физического интерфейса и при выключенном интерфейсе.

1.8.3. Выключение/включение интерфейса выполняется командой

```
[no] shutdown
```

1.8.4. Установка/удаление IP-адреса интерфейса выполняется командой
[no] (ip4-address | ip6-address) <ip_addr/mask>

где <ip_addr/mask> – IP-адрес/маска подсети интерфейса.

Примечание. Одному интерфейсу можно назначить больше одного IP-адреса.

1.8.5. Включение/выключение DHCP-клиента на интерфейсе выполняется командой

[no] (ip4-address | ip6-address) dhcp [nodns] [nodefault]

где nodns – включить режим без dns;

nodefault – включить режим без маршрутов «по умолчанию».

Ответ от DHCP-сервера передается в течение 180 секунд.

Примечание. Перед включением DHCP-клиента необходимо включить интерфейс.

1.8.6. Установка/удаление значения MTU на интерфейсе выполняется командой
[no] mtu <mtu>

где <mtu> – параметр MTU, задается в октетах. Может принимать значения от «68» до «9216».

При удалении текущего значения MTU на интерфейсе происходит установка значения «по умолчанию».

1.8.7. Включение/выключение неразборчивого режима приема пакетов на интерфейсе выполняется командой

[no] promiscuous

1.8.8. Установка/удаление текущего MAC-адреса интерфейса выполняется командой

[no] mac-address <ip-addr>

где <ip-addr> – значение MAC-адреса в формате «hh:hh:hh:hh:hh:hh».

При удалении текущего значения MAC-адреса на интерфейсе происходит установка значения «по умолчанию».

1.8.9. Установка/удаление описания интерфейса выполняется командой

[no] description <comment>

где <comment> – описание интерфейса.

Примечание. Описание интерфейса указывается без кавычек в случае содержания в описании одного слова и в двойных кавычках при двух и более словах. Текст в описании может содержать пробелы, не может содержать символы «'» и «-» и превышать 255 символов.

1.8.10. Включение/выключение режима автосогласования связи интерфейса выполняется командой

autonegotiation {on | off}

Примечание. В случае включенного автосогласования режима связи интерфейса, происходит автоматическое согласование скорости интерфейсов. При этом устанавливается наименьшая из указанных в канале скоростей.

1.8.11. Установка скорости интерфейса выполняется командой

speed <speed_value>

где *<speed_value>* – скорость, может принимать значения «10», «100», «1000», «10000».

Примечание. В случае включенного автосогласования скорости, происходит автоматическое согласование режимов связи интерфейсов.

1.8.12. Установка дуплексного/полудуплексного режима связи интерфейса выполняется командой

duplex <duplex_value>

где *<duplex_value>* – режим связи интерфейса, может принимать значения «full», «half».

1.8.13. Выход из режима конфигурации физического интерфейса выполняется командой

exit

1.8.14. Вывод конфигурации всех интерфейсов или определенного интерфейса выполняется командой

show interfaces [detail] [serial | <iface_name>] [statistics]

где *serial* – отображение информации о последовательных интерфейсах;

detail – отображение расширенных настроек конкретного интерфейса или всех интерфейсов;

statistics – отображение статистики. Применение опции возможно при задании имени определенного интерфейса.

1.8.15. Вывод информации о DHCP-клиентах выполняется командой

show dhcp-client [<iface_name>]

1.9. Loopback-интерфейс

1.9.1. Добавление/удаление loopback-интерфейса выполняется командой

create | delete loopback <iface_num>

где *<iface_num>* – номер интерфейса. Может принимать значения от «1» до «16777214».

1.10. Сетевой мост

1.10.1. Создание/удаление сетевого моста (bridge-интерфейса), а также вход в режим его конфигурации выполняется командой

```
create | delete bridge-domain <number>
```

где *<number>* – номер bridge-интерфейса. Может принимать значения от «1» до «16777214».

Приведенные ниже в 1.10.2 – 1.10.9 команды выполняются в режиме конфигурации bridge-интерфейса.

1.10.2. Задание/удаление описания интерфейса выполняется командой

```
[no] description <description>
```

где *<description>* – текст для описания bridge-интерфейса.

Примечание. Описание интерфейса указывается без кавычек в случае содержания в описании одного слова и в двойных кавычках при двух и более словах. Текст в описании может содержать пробелы, не может содержать символы «'» и «-» и превышать 255 символов.

1.10.3. Установка максимального возраста MAC-адреса в секундах выполняется командой

```
ageing <value>
```

где *<value>* – значение максимального возраста MAC-адреса, задается в секундах. Может принимать значения от «0» до «1000000».

1.10.4. Включение/выключение STP выполняется командой

```
[no] stp
```

1.10.5. Установка приоритета STP выполняется командой

```
stp-priority <value>
```

где *<value>* –приоритет STP. Может принимать значения от «0» до «255».

1.10.6. Включение/выключение режима VLAN-фильтрации выполняется командой

```
[no] vlan-filtering
```

1.10.7. Установка протокола VLAN выполняется командой

```
vlan-protocol {dot1q | dot1ad}
```

1.10.8. Установка идентификатора VLAN выполняется командой

```
vlan-id <value>
```

где *<value>* – значение идентификатора VLAN.

1.10.9. Выход из режима конфигурации сетевого моста

exit

1.10.10. Добавление/удаление интерфейса в сетевой мост выполняется командой

```
[no] bridge <number> interface <iface> [mode dot1q <dot1q_vid> | dot1ad  
<dot1ad_vid> inner_dot1q <inner_dot1q_vid>] [untagged] [pvid] [self] [master]
```

где <iface> – имя интерфейса;

untagged – режим, при котором интерфейс будет рассматриваться на выходе, как немаркированный;

pvid – режим, при котором указанные кадры будут объединены в немаркированный vlan;

self – режим, при котором vlan настроен на физическом устройстве. Этот режим требуется, если устройство является мостом;

master — режим, при котором vlan настроен на программном устройстве типа сетевой мост;

<dot1q_vid> – значение интерфейса при выборе режима 802.1q;

<dot1ad_vid> – значение интерфейса при выборе режима 802.1ad;

<inner_dot1q_vid> – значение внутреннего интерфейса при выборе режима 802.1q.

Примечания:

1. При добавлении интерфейса в сетевой мост, интерфейс должен быть в состоянии «down».

2. При задании номера bridge-интерфейса равным «0» конфигурируются только параметры интерфейса (снятие, установка метки). Используется, например, при создании на интерфейсе устройства VLAN.

1.10.11. Вывод конфигурации всех bridge-интерфейсов или определенного интерфейса выполняется командой

```
show bridge-domain [<number>] [detail]
```

где detail – подробный вывод конфигурации.

1.11. Агрегирование каналов

1.11.1. Создание/удаление bond-интерфейса, а также вход в режим его конфигурации выполняется командой

```
create | delete bond <interface_num>
```

где <interface_num> – номер bond-интерфейса.

Приведенные ниже в 1.11.2 – 1.11.5 команды выполняются в режиме конфигурации bond-интерфейса.

1.11.2. Добавление/удаление физического интерфейса в bond-интерфейс выполняется командой

```
[no] enslave <iface_name>
```

где <iface_name> – имя интерфейса.

Примечания:

1. MTU bond-интерфейса считается равным наименьшему MTU среди добавленных в него физических интерфейсов. Bond-интерфейс имеет единый IP-адрес на все добавленные в него физические интерфейсы.

2. Перед добавлением/удалением физического интерфейса в bond-интерфейс, его необходимо выключить.

1.11.3. Задание режима работы bond-интерфейсов выполняется командой

```
mode {round-robin | active-backup | xor | broadcast | lacp} [miimon <miimon_value>]
```

где <miimon_value> – значение частоты наблюдения, измеряется в миллисекундах. Может принимать значения от «0» до «16777214».

Режимы работы:

– «round-robin» – пакеты по очереди передаются через все интерфейсы. Данный режим работы обеспечивает балансировку нагрузки и отказоустойчивость. Режим используется «по умолчанию»;

– «active-backup» – активен только один интерфейс, остальные интерфейсы используются для горячей замены;

– «xor» – для каждого получателя определяется интерфейс в соответствии с MAC-адресом, режим обеспечивает балансировку нагрузки и отказоустойчивость;

– «broadcast» – все пакеты передаются на все интерфейсы в группе; режим обеспечивает отказоустойчивость;

– «lacp» – режим работы с поддержкой спецификации 802.3ad.

Режим изменяется для всех bond-интерфейсов. Во время смены режима работы происходит перезагрузка модуля ядра, поэтому все bond-интерфейсы удаляются и создаются заново.

1.11.4. Задание политики выбора (балансировки), на какой физический интерфейс bond-интерфейса посылать пакет выполняется командой

```
load-balance {12 | 123 | 134}
```

Режимы работы:

– «l2» – используется только хэш MAC-адресов отправителя и получателя (политика «по умолчанию»);

– «l23» – используется хэш MAC-адресов и IP-адресов;

– «l34» – используется хэш IP-адресов и номеров портов.

Во время смены политики происходит перезагрузка модуля ядра, поэтому все bond-интерфейсы удаляются и создаются заново.

Примечание. Задание политики выбора (балансировки) возможно только при выборе режима работы bond-интерфейсов – «larc» или «hog».

1.11.5. Выход из режима конфигурации интерфейса выполняется командой *exit*

1.11.6. Просмотр конфигурации bond-интерфейса выполняется командой *show bond [<config>]*

где <config> – номер конфигурации.

1.12. ARP

1.12.1. Добавление/удаление статической записи в ARP-таблицу выполняется командой

```
[no] ip arp <ip_addr> <mac_addr> <iface_name>
```

где <ip_addr> – IP-адрес стороннего узла;

<mac_addr> – MAC-адрес стороннего узла;

<iface_name> – имя интерфейса.

«По умолчанию» используется динамическое заполнение таблицы MAC-адресов.

1.12.2. Добавление/удаление ARP-прокси выполняется командой

```
[no] ip arp проху <iface_name>
```

1.12.3. Добавление/удаление приватного VLAN выполняется командой

```
[no] ip arp проху pvlan <iface_name>
```

1.12.4. Удаление ARP-таблицы выполняется командой

```
ip arp flush <iface_name>
```

1.12.5. Вывод ARP-таблицы на экран выполняется командой

```
show ip arp
```

1.12.6. Вывод интерфейсов ARP-прокси на экран выполняется командой
show ip arp proxy

1.13. Статическая маршрутизация

1.13.1. Задание/удаление статистического маршрута выполняется командой
[no] ip route <dest_ip/mask> [blackhole] [via <gateway>] [interface <iface>] [distance <distance>] [table <table>]

где <dest_ip/mask> – сеть назначения;

blackhole – возможность «отбрасывания» пакетов без уведомления;

<gateway> – IP-адрес шлюза;

<iface> – имя интерфейса;

<distance> – административная дистанция, может принимать значения от «1» до «255»;

<table> – номер таблицы маршрутизации, может принимать значения от «0» до «65535».

Примечание. При удалении статистического маршрута допускается частичный ввод команды без параметров. Например, команда «no ip route 10.0.0.0/24» удалит все заданные в конфигурации маршруты на сеть «10.0.0.0/24».

1.13.2. Добавление/удаление маршрута «по умолчанию» выполняется командой

[no] ip route default [blackhole] [via <gateway>] [interface <iface>] [distance <distance>] [table <table>]

1.13.3. Добавление/удаление маршрута с несколькими IP-адресами «по умолчанию» (для балансировки нагрузки) выполняется командой

*[no] ip route balance <dest_ip/mask> [distance <distance>]
[nexthop [<gateway1_ip>] [interface <interface_1>] [table <table_1>]
[nexthop [<gateway2_ip>] [interface <interface_2>] [table <table_2>]
[nexthop [<gateway3_ip>] [interface <interface_3>] [table <table_3>]]]]*

где <dest_ip/mask> – сеть назначения;

<interface_1>, <interface_2>, <interface_3> – имена интерфейсов;

<table_1>, <table_2>, <table_3> – номера таблиц маршрутизации.

1.13.4. Добавление/удаление IP-таблицы выполняется командой

[no] ip table id <table_id> name <table_name>

где <table_id> – номер таблицы маршрутизации;

<table_name> – имя таблицы.

1.13.5. Вывод списка IP-таблиц выполняется командой

show ip tables

1.13.6. Вывод сообщений из журнала выполняется командой

show ip route logs [last <count>]

где last – вывод последней части журнала;

<count> – количество строк.

1.13.7. Вывод таблицы маршрутизации выполняется командой

*show {ip | ip6} route [<dest_ip/mask> | all | connected | static | kernel | summary |
ospf | rip | table <table_id>]*

где <dest_ip/mask> – адрес назначения маршрута;

all – все маршруты;

connected – маршруты, определенные при подключении к определенной сети;

static – заданные вручную статические маршруты;

kernel – маршруты, полученные по DHCP;

rip – маршруты, полученные по данным протокола динамической маршрутизации RIP;

ospf – маршруты, полученные по данным протокола динамической маршрутизации OSPF.

1.14. Динамическая маршрутизация

1.14.1. OSPF

1.14.1.1. Включение/отключение протокола OSPF, а также вход в режим конфигурации протокола выполняется командой

[no] router ospf

Приведенные ниже в 1.14.1.2 – 1.14.1.23 команды выполняются в режиме конфигурации OSPF.

1.14.1.2. Включение/выключение перераспределения маршрутов выполняется командой

*[no] redistribute {rip | connected | static} [metric <metric>] [metric-type
<metric-type>] [route-map <route_map_name>]*

где <metric> – значение метрики OSPF;

<metric-type> – тип метрики, может принимать значения «1» или «2»;

<route_map_name> – имя карты маршрутов;

rip – маршруты, полученные по данным протокола динамической маршрутизации RIP;

static – заданные вручную статические маршруты;

connected – маршруты, определенные при подключении к определенной сети.

1.14.1.3. Задание/удаление интерфейса, через который осуществляется только прием обновлений OSPF выполняется командой

```
[no] passive-interface <interface>
```

где <interface> – имя интерфейса.

1.14.1.4. Задание/удаление явным образом соседа OSPF выполняется командой

```
[no] neighbor <ip_address> [poll-interval <poll_interval>] [priority <priority>]
```

где <ip_address> – IP-адрес соседа;

<poll_interval> – интервал опроса. Может принимать значения от «1» до «65535»;

<priority> – приоритет маршрутизатора, посылаемый данному соседу. Может принимать значения от «0» до «255».

1.14.1.5. Задание интервала пересылки hello-пакетов выполняется командой

```
interface <interface> hello-interval <val>
```

где <interface> – имя интерфейса;

<val> – интервал, задается в секундах. Может принимать значения от «1» до «65535». Значение «по умолчанию» равно «10».

1.14.1.6. Задание интервала, после которого сосед считается «мертвым», выполняется командой

```
interface <interface> dead-interval <val>
```

где <val> – интервал, задается в секундах. Может принимать значения от «1» до «65535». Значение «по умолчанию» равно «40».

1.14.1.7. Задание интервала, после которого производится повторная пересылка неподтвержденного служебного пакета выполняется командой

```
interface <interface> retransmit-interval <val>
```

где <val> – интервал, задается в секундах. Значение «по умолчанию» равно «5».

1.14.1.8. Задание пароля для аутентификации соседа OSPF выполняется командой

```
interface <interface> authentication {md5 <md5_key> | text <password>}
```

где <md5_key> значение идентификатора MD5-ключа.

Может принимать значения от «1» до «255»;

<password> – пароль, длина которого не должна превышать 8 символов. Могут быть использованы любые символы, кроме пробела и «'».

1.14.1.9. Выключение аутентификации соседа OSPF выполняется командой
interface <interface> no authentication

1.14.1.10. Задание/удаление BFD на интерфейсе выполняется командой
interface <interface> [no] bfd

1.14.1.11. Выключение обнаружения несоответствия MTU на интерфейсе выполняется командой

interface <interface> mtu-ignore

«По умолчанию» параметр «mtu-ignore» не указан.

1.14.1.12. Включение обнаружения несоответствия MTU на интерфейсе выполняется командой

interface <interface> no mtu-ignore

1.14.1.13. Задание/удаление метрики участка на интерфейсе выполняется командой

interface <interface> [no] cost <val>

где <val> – метрика участка. Может принимать значения от «0» до «65535».

1.14.1.14. Добавление/удаление прикрепленной к данной зоне сети выполняется командой

[no] network <address/mask> area <area>

где <address/mask> – IP-адрес и маска сети OSPF;

<area> – номер зоны. Может принимать значения от «0» до «2147483647».

1.14.1.15. Установка аутентификации выполняется командой

[no] area <number> authentication [message-digest]

где <number> – номер зоны. Может принимать значения от «0» до «2147483647»;
message-digest – дайджест сообщения.

Примечание. При задании номера зоны равным «0» можно ввести только параметр «authentication [message-digest]».

1.14.1.16. Задание/удаление типа зоны с опциональным запретом на пересылку межзональных маршрутов выполняется командой

[no] area <number> {stub [no-summary] | nssa [no-summary]}

Типы зон:

– «nssa» – не совсем тупиковая зона, обладает всеми свойствами тупиковых зон, однако в не совсем тупиковых зонах могут находиться ASBR (пограничные маршрутизаторы автономной системы OSPF, находящиеся на границе с другой автономной системой OSPF, из которой транслируются маршруты в сеть OSPF);

– «stub» – тупиковая зона, не принимает информацию о внешних маршрутах для автономной системы OSPF, но принимает маршруты из других зон, не может содержать ASBR.

При указании «no-summary» для параметров «stub» и «nssa», соответствующие зоны становятся полностью тупиковыми (не принимает рассылки не только внешних, но и межзональных сообщений LSA. Все внешние и межзональные маршруты заменяются пограничным маршрутизатором зоны на маршрут «по умолчанию»).

1.14.1.17. Задание/удаление настроек механизма объединения межзональных маршрутов выполняется командой

```
[no] area <number> range <address/mask> [advertise | not-advertise] [cost <cost_value>]
```

где <number> – номер зоны OSPF, частные маршруты которой будут агрегированы в суммарный маршрут. Может принимать значения от «0» до «2147483647»;

<address/mask> – IP-адрес и маска подсети объявляемого суммарного маршрута;

<cost_value> – значение стоимости, назначенной суммарному маршруту, значение задается в Мбит/с;

advertise – разрешение анонсирования суммарного маршрута. Параметр установлен «по умолчанию»;

not-advertise – запрет объявления суммарного маршрута для описанного диапазона. После применения данного параметра описанный диапазон становится скрытым для всех остальных зон OSPF.

Примечания:

1. Задание параметра «cost» применимо только к пограничным маршрутизаторам (ABR-маршрутизаторам). Метрика вычисляется по формуле «cost» = «reference bandwidth» / «link bandwidth», где «reference bandwidth» – пропускная способность «по умолчанию», относительно которой рассчитывается стоимость интерфейса, а «link bandwidth» значение пропускной способности на интерфейсе.

2. Данная команда выполняется только при указании типов зон «nssa» и «stub».

1.14.1.18. Задание сводной стоимости тупиковой области «по умолчанию» для маршрутов зоны выполняется командой

```
area <number> default-cost <default-cost>
```

где <default-cost> – стоимость «по умолчанию». Может принимать значения от «0» до «16777214».

Примечания:

1. Данная команда выполняется только при указании типов зон «nssa» и «stub».

2. Для того чтобы обозначить недоступную сеть, OSPF использует метрику, равную «16777215», которая считается недостижимой метрикой для OSPF.

1.14.1.19. Включение/выключение распространения информации об IP-адресе «по умолчанию» (шлюзе) выполняется командой

```
[no] default-information originate [always] [metric <metric_val>] [metric-type <metric_type>] [route-map <route_map_name>]
```

где <metric_val> – метрика для заимствованных маршрутов. Может принимать значения от «0» до «16777214»;

<metric_type> – тип метрики для заимствованных маршрутов. Может принимать значения «1» или «2»;

<route_map_name> – имя карты для заимствованных маршрутов.

Параметр «always» включает распространение информации об IP-адресе «по умолчанию» (если распространения информации выключено). «По умолчанию» параметр установлен.

1.14.1.20. Задание/удаление значения для корректировки справочного значения пропускной способности OSPF выполняется командой

```
[no] auto-cost reference-bandwidth <cost>
```

где <cost> – значение для корректировки справочного значения пропускной способности OSPF, задается в Мбит/с. Значение «по умолчанию» равно 100 Мбит/с.

1.14.1.21. Задание/удаление интервала времени ожидания уведомления о состоянии соединения с соседом выполняется командой

```
[no] timers lsa arrival <timer_value>
```

где <timer_value> – интервал времени, через который происходит уведомление о состоянии соседа, измеряется в секундах. Может принимать значения от «0» до «600000».

1.14.1.22. Задание/удаление интервала времени ожидания, через который происходит рассылка анонсов LSA выполняется командой

```
[no] timers throttle lsa all <timer_value>
```

где <timer_value> – интервал времени, через который происходит рассылка анонсов LSA, измеряется в миллисекундах. Может принимать значения от «0» до «5000». Значение «по умолчанию» равно «30».

1.14.1.23. Выход из режима конфигурации OSPF выполняется командой

```
exit
```

1.14.1.24. Установка/удаление IP-адрес для использования его в качестве идентификатора ID-маршрутизатора выполняется командой

```
[no] router id <ip_address>
```

где <ip_address> – значение IP-адрес.

1.14.1.25. Вывод конфигурации и правил маршрутизации OSPF выполняется командой

```
show ospf configuration
```

1.14.1.26. Вывод конфигурации интерфейсов, участвующих в маршрутизации OSPF, выполняется командой

```
show ospf interfaces
```

1.14.1.27. Вывод идентификатора маршрутизатора выполняется командой

```
show router id
```

1.14.2. RIP

1.14.2.1. Включение/отключение протокола RIP, а также вход в режим конфигурации протокола выполняется командой

```
[no] router rip
```

Приведенные ниже в 1.14.2.2 – 1.14.2.9 команды выполняются в режиме конфигурации RIP.

1.14.2.2. Включение/выключение перераспределения маршрутов выполняется командой

```
[no] redistribute { ospf | static | connected } [metric <metric>] [route-map  
<route_map>]
```

где <metric> – метрики RIP, могут принимать значения от «1» до «16»;

<route_map> – имя route-map;

ospf – маршруты, полученные по данным протокола динамической маршрутизации OSPF;

static – заданные вручную статические маршруты;

connected – маршруты, определенные при подключении к определенной сети.

1.14.2.3. Задание/удаление сети, в которой будет работать протокол RIP, выполняется командой

```
[no] network {<ip_with_mask> | <interface_name>}
```

где <ip_with_mask> – IP-адрес и маска подсети;

<interface_name> – имя интерфейса.

1.14.2.4. Задание/удаление пароля для аутентификации соседа RIP выполняется командой

```
[no] interface <interface_name> authentication {md5 <md5_key> | text <password>}
```

где <md5_key> значение идентификатора MD5-ключа. Может принимать значения от «1» до «255»;

<password> – пароль, длина которого не должна превышать 16 символов. Могут быть использованы любые символы, кроме пробела и «'».

1.14.2.5. Добавление/удаление соседа выполняется командой

```
[no] neighbor <ip_address>
```

где <ip_address> – IP-адрес соседа.

1.14.2.6. Установка значений таймеров выполняется командой

```
timers basic <routing_table_update> <routing_information_timeout>
```

```
<garbage_collection>
```

где <routing_table_update> – время обновления таблицы маршрутов, задается в секундах. Может принимать значения от «5» до «2147483647». Значение «по умолчанию» равно «30»;

<routing_information_timeout> – время ожидания маршрутной информации, задается в секундах. Может принимать значения от «5» до «2147483647». Значение «по умолчанию» равно «180»;

<garbage_collection> – значение таймера «сборки мусора». Может принимать значения от «5» до «2147483647». Значение «по умолчанию» равно «120».

1.14.2.7. Задание/удаление интерфейса, через который производится только прием обновлений RIP, выполняется командой

```
[no] passive-interface <interface_name>
```

1.14.2.8. Задание/удаление списка для изменения метрики маршрута выполняется командой

```
[no] offset-list <prefix_list_name> {in | out} <metric>
```

где <prefix_list_name> – имя списка изменения;
<metric> – значение метрики. Может принимать значения от «0» до «16»;
in – изменения входящей метрики маршрута;
out – изменения исходящей метрики маршрута.

1.14.2.9. Выход из режима конфигурации RIP выполняется командой
exit

1.14.2.10. Просмотр конфигурации RIP выполняется командой
show rip

1.14.2.11. Вывод состояния протокола выполняется командой
show rip status

1.14.3. RIPNG

1.14.3.1. Включение/отключение протокола RIPNG, а также вход в режим конфигурации протокола выполняется командой

[no] router ripng

Приведенные ниже в 1.14.3.2 – 1.14.3.7 команды выполняются в режиме конфигурации RIP.

1.14.3.2. Включение/выключение перераспределения маршрутов, полученных по протоколам BGP, статически заданных или в подключенные сети выполняется командой

[no] redistribute {bgp | static | connected} [metric <metric>] [route-map <route_map>]

где <metric> – значение метрики RIP, может принимать значения от «1» до «16»;

<route_map> – имя route-map;

bgp – маршруты, полученные по данным протокола динамической маршрутизации BGP;

static – заданные вручную статические маршруты;

connected – маршруты, определенные при подключении к определенной сети.

1.14.3.3. Задание/удаление сети, в которой будет работать протокол RIPNG, выполняется командой

[no] network {<ip_with_mask> | <interface_name>}

где <ip_with_mask> – IP-адрес интерфейса с бит-маской;

<interface_name> – имя интерфейса.

1.14.3.4. Установка значений таймеров выполняется командой

*timers basic <routing_table_update> <routing_information_timeout>
<garbage_collection>*

где *<routing_table_update>* – время обновления таблицы маршрутов, задается в секундах. Может принимать значения от «5» до «2147483647». Значение «по умолчанию» равно «30»;

<routing_information_timeout> – время ожидания маршрутной информации, задается в секундах. Может принимать значения от «5» до «2147483647». Значение «по умолчанию» равно «180»;

<garbage_collection> – значение таймера «сборки мусора». Может принимать значения от «5» до «2147483647». Значение «по умолчанию» равно «120».

1.14.3.5. Задание/удаление интерфейса, через который производится только прием обновлений RIP, выполняется командой

[no] passive-interface <interface_name>

1.14.3.6. Задание/удаление списка для изменения метрики маршрута выполняется командой

[no] offset-list <prefix_list_name> {in | out} <metric>

где *<prefix_list_name>* – имя списка изменения;

<metric> – метрика. Может принимать значения от «0» до «16»;

in – изменения входящей метрики маршрута;

out – изменения исходящей метрики маршрута.

1.14.3.7. Выход из режима конфигурации RIP выполняется командой

exit

1.14.3.8. Просмотр конфигурации RIP выполняется командой

show ripng

1.14.3.9. Вывод состояния протокола выполняется командой

show ripng status

1.15. Route-maps

1.15.1. Создание/удаление списка префиксов или добавление новых записей выполняется командой

*[no] ip prefix-list <prelist_name> [seq <seq_number>] {deny | permit}
<ip-addr/mask> [le <le_value>] [ge <ge_value>]*

где *<prelist_name>* – имя префикс-листа;

<seq_number> – порядковый номер в списке;

deny – установка пакетов для отклонения;

permit – установка пакетов для пересылки;

<ip-addr/mask> – IP-адрес и маска подсети для записи префикс-листа;

<ge_value> – минимальная длина префикса, может принимать значения от «0» до «32»;

<le_value> – максимальная длина префикса, может принимать значения от «0» до «32».

1.15.2. Создание/удаление записи списка маршрутов, а также вход в режим создания новых записей выполняется командой

```
[no] ip route map <prelist_name> {deny | permit} <seq>
```

где <prelist_name> – имя списка маршрутов;

<seq> – номер строки списка маршрутов.

Приведенные ниже в 1.15.3 – 1.15.4 команды выполняются в режиме конфигурации route-map.

1.15.3. Подключение/отключение префикс-листа к записи списка маршрутов выполняется командой

```
[no] match <prelist_name>
```

1.15.4. Выход из режима конфигурирования записей выполняется командой
exit

1.15.5. Вывод конфигурации списка маршрутов выполняется командой
show ip route map [<name>]

1.16. Правила контроля доступа

1.16.1. Вход в режим конфигурирования правила контроля доступа выполняется командой

```
[no] ip access-rule <acr_name>
```

где <acr_name> – идентификатор правила контроля доступа.

Приведенные ниже в 1.16.2 – 1.16.27 команды выполняются в режиме конфигурации ACL.

1.16.2. Добавление IP-адреса источника выполняется командой
source {<ip_src> | not <ip_src> | any}

где <ip_src> – IP-адрес и маска источника;

any – любой IP-адрес.

1.16.3. Добавление IP-адреса приемника выполняется командой
destination {<ip_dsc> | not <ip_dsc> | any}

где <ip_dst> – IP-адрес и маска приемника.

1.16.4. Задание входного интерфейса выполняется командой

```
interface input {<in_iface> | not <in_iface>}
```

где <in_iface> – имя интерфейса.

1.16.5. Задание выходного интерфейса выполняется командой

```
interface output {<out_iface> | not <out_iface>}
```

где <out_iface> – имя интерфейса.

1.16.6. Задание используемого протокола выполняется командой

```
protocol {proto | not proto}
```

где proto – имя протокола. Могут задаваться следующие протоколы «tcp», «icmp», «udp» и «ip».

1.16.7. Задание используемого типа IP-протокола выполняется командой

```
type {ip4 | ip6}
```

1.16.8. Добавление/удаление правила типа «udp» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type udp [sport <src_port> | not <src_port>] [dport <dst_port> | not <dst_port>]
```

где <seq_num> – номер последовательности ACL, может принимать значения от «1» до «20000»;

<src_port> – номер порта отправителя, может принимать значения от «0» до «65535»;

<dst_port> – номер порта получателя, может принимать значения от «0» до «65535».

1.16.9. Добавление/удаление правила типа «multiport» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type multiport [sport <src_port> | not <src_port>] [dport <dst_port> | not <dst_port>]
```

1.16.10. Добавление/удаление правила типа «modbus» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type modbus [transaction <tr_id> | not <tr_id>] [protocol <proto_id> | not <proto_id>] [length <header_len> | not <header_len>] [unit <unit_id> | not <unit_id>] [function <function_id> | not <function_id>] [register <register_id> | not <register_id>]
```

где <tr_id> – значение идентификатора транзакции;

<proto_id> – значение идентификатора протокола;

<header_len> – значение длины заголовка;

<unit_id> – значение идентификатора узла;

<function_id> – код функции;

<register_id> – значение идентификатора регистра.

1.16.11. Добавление/удаление правила типа «tcp» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type tcp [sport <src_port> | not <src_port>] [mss {single
<mss_single_val> | not <mss_single_val> | range <mss_range_val> | not
<mss_range_val>}] [dport <dst_port> | not <dst_port>] [mask <flag> | not <flag> | all]
```

где <mss_single_val> – максимальный размер сегмента tcp-пакета;

<mss_range_val> – диапазон размера сегмента tcp-пакета;

<flag> – флаги TCP-пакетов. Могут принимать значения «fin», «syn», «rst», «psh», «ack», «urg». Можно указывать от одного до шести флагов.

1.16.12. Добавление/удаление правила типа «dscp» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type dscp {<dscp_val> | not <dscp_val>}
```

где <dscp_val> – значение dscp.

1.16.13. Добавление/удаление правила типа «mac» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type mac source {<mac_src> | not <mac_src>}
```

где <mac_src> – MAC-адрес источника.

1.16.14. Добавление/удаление правила типа «icmp» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type icmp type {<type_icmp> | not <type_icmp>}
```

где <type_icmp> – тип сообщения ICMP.

1.16.15. Добавление/удаление правила типа «state» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type state {<conn_state> | not <conn_state>}
```

где <conn_state> – состояние TCP-соединения.

1.16.16. Добавление/удаление правила типа «length» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type length {<packet_len> | not <packet_len>}
```

где <packet_len> – длина IP-пакета, задается в байтах. Может принимать значения от «20» до «65535».

1.16.17. Добавление/удаление правила типа «so» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type so [class {less <lt_value> | not<lt_value>} | {equal
<eq_value> | not <eq_value>} | {greater <gt_value> | not <eq_value>} | {mask
<mask_value> | not <mask_value>}] [protection-flag {<so_prot_flag_value> | not
<eq_value>}]
```

где <lt_value> – значение класса метки безопасности «меньше»;

<eq_value> – значение класса метки безопасности «равно»;

<gt_value> – значение класса метки безопасности «больше»;

<mask_value> – маска класса метки безопасности;

<so_prot_flag_value> – значение защитного флага метки безопасности.

1.16.18. Добавление/удаление правила типа «eso» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type eso [format {<format_value> | not <format_value>}
format_position {<format_position_value> | not <format_position_value>}] [security-info
{<secinfo_value> | not <secinfo_value>} secinfo_position {<secinfo_position_value> | not
<secinfo_position_value>}]
```

где <format_value> – значение поля «формат» расширенных опций метки безопасности;

<format_position_value> – позиция опции в метке;

<secinfo_value> – значение поля «информация безопасности» расширенных опций метки безопасности;

<secinfo_position_value> – позиция расширенной опции в метке.

1.16.19. Добавление/удаление правила типа «limit» в правило контроля доступа выполняется командой

```
[no] match <seq_num> type limit {<conn_limit> | not <conn_limit>}
```

где <conn_limit> – граничное значение количества TCP-соединения, может принимать значения от «0» до «65535».

Количество TCP-соединений может принимать значения от «0» до «65535».

1.16.20. Добавление/удаление правила типа «algorithm» в правило контроля доступа выполняется командой

[no] match <seq_num> type string algorithm {bm | kpm | regex} [normal <normal_string> | hex <hex_string>] [upper_offset <offset_up>] [lower_offset <offset_down>]

где <normal_string> – строка;

<hex_string> – hex-строка;

<offset_up> – значение верхнего битового отступа;

<offset_down> – значение нижнего битового отступа.

1.16.21. Добавление/удаление правила типа «u32» в правило контроля доступа выполняется командой

[no] match <seq_num> type u32 <u32>

где <u32> – u32-правило.

1.16.22. Добавление/удаление правила типа «set» в правило контроля доступа выполняется командой

[no] match <seq_num> type set <acs_name>

где <acs_name> – имя списка доступа.

1.16.23. Добавление/удаление правила типа «packet» в правило контроля доступа выполняется командой

[no] match <seq_num> type packet {unicast | broadcast | multicast}

где unicast – режим передачи пакета от одного хоста к другому хосту;

broadcast – режим передачи пакета от одного хоста ко всем хостам в сети;

multicast – режим передачи пакета от одного хоста некоторой ограниченной группе хостов.

1.16.24. Установка опций логирования выполняется командой

log {enable | disable}

где enable – включение журналирования;

disable – выключение журналирования.

1.16.25. Установка фильтрации для фрагментированных пакетов выполняется командой

fragment

1.16.26. Установка фильтрации для нефрагментированных пакетов выполняется командой

no fragment

1.16.27. Выход из режима конфигурации списка контроля доступа выполняется командой

exit

1.16.28. Вывод конфигураций всех существующих списков контроля доступа или списка контроля доступа с именем <acl_name> выполняется командой

```
show ip access-rule [<acr_name>]
```

1.17. Списки контроля доступа

1.17.1. Создание/удаление, а также вход в режим конфигурирования списка контроля доступа выполняется командой

```
[no] ip access-set <acs_name> type <acs_type>
```

где <acs_name> – идентификатор списка доступа;

<acs_type> – тип доступа. Используются следующие типы доступа «ip», «net», «mac», «ip:port», «ip:mac», «net:iface».

Приведенные ниже в 1.17.2 – 1.17.5 команды выполняются в режиме конфигурации ACL.

1.17.2. Добавление записи в список контроля доступа выполняется командой

```
add {ip <ip_addr> | net <net_addr> | port <port_value> | mac <mac_addr> |  
interface <iface>}
```

где <ip_addr> – IP-адрес;

<net_addr> – IP-адрес и маска сети;

<port_value> – номер порта;

<mac_addr> – MAC-адрес;

<iface> – имя интерфейса.

1.17.3. Удаление записи из списка контроля доступа выполняется командой

```
delete {ip <ip_addr> | net <net_addr> | port <port_value> | mac <mac_addr> |  
interface <iface>}
```

1.17.4. Задание направления выполняется командой

```
direction {source | destination}
```

где source – источник;

destination – назначение.

1.17.5. Выход из режима конфигурации списка доступа выполняется командой

exit

1.17.6. Вывод конфигурации всех существующих списков контроля доступа или списка контроля доступа с именем «acs_name» выполняется командой

```
show ip access-set [<acs_name>]
```

1.18. Фильтрация в соответствии с правилами доступа

1.18.1. Установка политики фильтрации выполняется командой

```
set {ip4 | ip6} {input | output | forward} [policy {accept | drop}] [log {enable | disable}]
```

где ip4 – фильтрация по протоколу IPv4;

ip6 – фильтрация по протоколу IPv6;

input – фильтрация по входящему направлению;

output – фильтрация по исходящему направлению;

forward – фильтрация по направлению проброса;

accept – политика принятия;

drop – политика отбрасывания;

enable – включение журналирования;

disable – выключение журналирования.

1.18.2. Добавление правила фильтрации в соответствии с правилом контроля доступа выполняется командой

```
ip access-list {input | output | forward} [idx] match-rule <rule_name> {accept | drop | reject [reject-with <reject_msg>] | nfqueue [queue-num <queue_num_val>]}
```

где <rule_name> – идентификатор правила контроля доступа;

idx – желаемая позиция правила в таблице фильтрации;

accept – возможность принимать пакеты;

drop – возможность отбрасывать пакеты;

reject – возможность отмены пакетов;

<reject_msg> – сообщение события;

nfqueue – возможность поместить пакеты для обработки в очередь;

<queue_num_val> – номер очереди.

1.18.3. Удаление правила фильтрации в соответствии с правилом контроля доступа выполняется командой

```
no ip access-list {input | output | forward} [idx] match-rule <rule_name>
```

1.18.4. Вывод статистики правил фильтрации выполняется командой

```
show {ip4 | ip6} filter {input | output | forward}
```

1.18.5. Вывод правил фильтрации, примененных к цепочкам, выполняется командой

```
show ip access-list {input | output | forward}
```

1.18.6. Вывод глобальных настроек политик фильтрации выполняется командой

show {ip4 | ip6} filter policy

1.19. NAT

1.19.1. Создание/удаление, а также вход в режим конфигурирования правила NAT выполняется командой

[no] nat rule <nat_rule_name>

где <nat_rule_name> – имя правила NAT.

Приведенные ниже в 1.19.2 – 1.19.10 команды выполняются в режиме конфигурации соответствующего правила NAT.

1.19.2. Задание/удаление интерфейса выполняется командой

[no] interface <iface_name> direction {input | output}

где <iface_name> – имя интерфейса;

input – цепочка фильтрации по входящему направлению;

output – цепочка фильтрации по исходящему направлению.

1.19.3. Включение маскардинга на NAT выполняется командой

action masquerade {ip4 | ip6} port {<port_val> | range <port_range_val>}

где <port_val> – номер порта, может принимать значения от «0» до «65535»;

<port_range_val> – диапазон значений портов.

1.19.4. Добавление внутренней переадресации для источника выполняется командой

action forward inner source [<in_src_addr> | not <in_src_addr>] port [<in_src_port> | not <in_src_port>]

где <in_src_addr> – внутренний IP-адрес источника;

<in_src_port> – значение порта источника.

1.19.5. Добавление внутренней переадресации для получателя выполняется командой

action forward inner destination [<in_dst_addr> | not <in_dst_addr>] port [<in_dst_port> | not <in_dst_port>]

где <in_dst_addr> – внутренний IP-адрес получателя;

<in_dst_port> – значение порта получателя.

1.19.6. Добавление внешней переадресации для источника выполняется командой

action forward outer source [*<out_src_addr>* | *out_src_range <out_src_addr_range>*]
[*<out_src_port>* | *out_src_range <out_src_port_range>*]

где *<out_src_addr>* – внешний IP-адрес источника;

<out_src_addr_range> – диапазон внешних IP-адресов источника;

<out_src_port> – номер порта источника. Может принимать значения от «0» до «65535»;

<out_src_port_range> – диапазон значений портов источников.

1.19.7. Добавление внешней переадресации для получателя выполняется командой

action forward outer destination [*<out_dst_addr>* | *out_dst_range <out_dst_addr_range>*]
[*<out_dst_port>* | *out_dst_range <out_dst_port_range>*]

где *<out_dst_addr>* – внешний IP-адрес получателя;

<out_dst_addr_range> – диапазон внешних IP-адресов получателя;

<out_dst_port> – номер порта получателя. Может принимать значения от «0» до «65535»;

<out_dst_port_range> – диапазон значений портов получателя.

1.19.8. Задание протокола правил NAT выполняется командой

protocol {tcp | udp | icmp | ip}

1.19.9. Задание желаемой позиции правила в таблице *nat* выполняется командой

index <idx>

где *<idx>* – значение позиции.

1.19.10. Выход из режима конфигурации соответствующего интерфейса выполняется командой

exit

1.19.11. Вывод конфигурации правил для NAT выполняется командой

show {ip4 | ip6} nat [snat | dnat | masquerade]

где *ip4* – вывод конфигурации по протоколу IPv4;

ip6 – вывод конфигурации по протоколу IPv6;

snat – вывод конфигурации SNAT;

dnat – вывод конфигурации DNAT;

masquerade – вывод конфигурации MASQUERADE.

1.20. Policy Basic Routing

1.20.1. Создание/удаление правила, а также вход в режим конфигурирования выполняется командой

```
[no] ip route rule <rule_num>
```

где <rule_num> – номер правила.

Приведенные ниже в 1.20.2 – 1.20.18 команды выполняются в режиме конфигурации правила.

1.20.2. Задание/удаление префикса источника для поиска соответствия выполняется командой

```
[no] from {default | all | any | ip <ip_value>}
```

где default – префикс «по умолчанию»;

all – префикс «все»;

any – префикс «любой»;

<ip_value> – IP-адрес источника.

1.20.3. Задание/удаление префикса приемника для поиска соответствия выполняется командой

```
[no] to {default | all | any | ip <ip_value>}
```

где <ip_value> – IP-адрес приемника.

1.20.4. Задание/удаление значения метки пакетов для поиска соответствия выполняется командой

```
[no] fwmark <fwmark_value>
```

где <fwmark_value> – значение метки пакетов.

1.20.5. Задание/удаление входящего интерфейса для поиска соответствия выполняется командой

```
[no] input <iface_name>
```

где <iface_name> – имя входящего интерфейса.

1.20.6. Задание/удаление исходящего интерфейса для поиска соответствия выполняется командой

```
[no] output <iface_name>
```

где <iface_name> – имя исходящего интерфейса.

1.20.7. Задание/удаление значения IP-протокола для поиска соответствия выполняется командой

```
[no] ipproto <proto_value>
```

где <proto_value> – значение IP-протокола.

1.20.8. Задание значения nat выполняется командой

```
nat <nat_value>
```

где <nat_value> – значение IP-адреса для NAT.

1.20.9. Задание приоритета правила выполняется командой
priority <priority_value>

где <priority_value> – значение приоритета.

1.20.10. Задание протокола маршрутизации выполняется командой
protocol {redirect | kernel | boot | static | zebra}

где redirect – тип протокола «redirect»;

kernel – тип протокола «kernel»;

boot – тип протокола «boot»;

static – тип протокола «static»;

zebra – тип протокола «zebra».

1.20.11. Задание значения realms выполняется командой
realms <realms_value>

где <realms_value> – значение realms.

1.20.12. Задание/удаление порта источника для поиска соответствия выполняется командой

[no] sport <sport_value>

где <sport_value> – порт источника.

1.20.13. Задание/удаление порта назначения для поиска соответствия выполняется командой

[no] dport <dport_value>

где <dport_value> – порт назначения.

1.20.14. Задание/удаление значения TOS для поиска соответствия выполняется командой

[no] tos <tos_value>

где <tos_value> – значение TOS. Значение задается в шестнадцатиричном формате в диапазоне от «0x00» до «0x1E».

1.20.15. Задание идентификатора таблицы маршрутизации выполняется командой

table {local | main | default | num <num_value>}

где local – локальная таблица маршрутизации;

main – главная таблица маршрутизации;

default – таблица маршрутизации «по умолчанию»;

<num_value>– числовой идентификатор таблицы маршрутизации.

1.20.16. Задание/удаление диапазона значений UID для поиска соответствия выполняется командой

```
[no] uidrange <uidrange_value>
```

где <uidrange_value> – диапазон значений UID.

1.20.17. Установка/отмена инвертирования правила для поиска несоответствия выполняется командой

```
[no] invert
```

1.20.18. Выход из режима конфигурации соответствующего интерфейса выполняется командой

```
exit
```

1.20.19. Вывод всех правил или отдельного правила выполняется командой

```
show ip route rules [<rule_num>]
```

1.21. Команды просмотра и управления журналами

1.21.1. Задание максимального размера журнала перед архивацией выполняется командой

```
log rotate max-size <log_size>
```

где <log_size> – предельный объем архивов для журнала в Мбайт. Может принимать значения от «1» до «3600». Значение «по умолчанию» равно «10».

Сброс текущего значения размера журнала и установка значения «по умолчанию» выполняется командой

```
no log rotate max-size
```

1.21.2. Задание максимального количества архивных файлов выполняется командой

```
log rotate count <log_num>
```

где <val> – максимальное количество архивных файлов. Может принимать значения от «1» до «100». Значение «по умолчанию» равно «5».

Сброс текущего значения и установка значения «по умолчанию» выполняется командой

```
no log rotate count
```

1.21.3. Установка/удаление временного интервала фоновой проверки размера журналов выполняется командой

```
[no] log rotate interval <log_time>
```

где `<log_time>` – временной интервал, задается в секундах. Может принимать значения от «1» до «65535». Значение «по умолчанию» равно «60».

1.21.4. Включение/отключение локального хранения журнала выполняется командой

```
[no] log <facility> local {on | off}
```

где `<facility>` – выбор журнала. Параметр может принимать следующие значения:

- `syslog` – журнал системных команд;
- `auth` – журнал событий аутентификации;
- `commands` – журнал команд пользователя;
- `daemon` – журнал выполненных функций;
- `ipfilter` – журнал событий срабатывания правил межсетевого экранирования;
- `testing` – журнал тестирования и самотестирования системы;
- `router` – журнал, содержащий информацию о работе протоколов динамической маршрутизации.

1.21.5. Включение/отключение удаленного хранения журнала выполняется командой

```
[no] log <facility> remote {on | off}
```

1.21.6. Указание/удаление IP-адреса удаленного сервера хранения журналов выполняется командой

```
[no] log <facility> remote <ip_addr> [port <port>]
```

где `<ip_addr>` – IP-адрес удаленного сервера хранения журналов;

`<port>` – номер порта удаленного сервера хранения журналов. «По умолчанию» используется порт «514».

1.21.7. Включение/отключение вывода на экран терминала выполняется командой

```
[no] log <facility> terminal {on | off}
```

Вывод происходит в тот терминал, из которого была вызвана команда.

1.21.8. Выгрузка журнала на внешний носитель выполняется командой

```
save log <facility> flash [clear]
```

где `flash` – первый примонтированный внешний носитель;

`clear` – очистить журнал после копирования на внешний носитель.

1.21.9. Для установки/изменения уровня журналирования сообщений используется команда

```
log level <facility> <level>
```

где `<level>` – уровень записи в журнал. Параметр может принимать следующие значения:

- `debug` – отладочная информация;
- `info` – информационные сообщения;
- `warning` – предупреждения;
- `error` – сообщения об ошибках;
- `critical` – критические ошибки в программе.

1.21.10. Вывод журнала выполняется командой

```
show log <facility> [search [after <start_date> <start_time>] | [before <end_date>
<end_time>]] | [sender <name_sender>] | [success {OK | FAIL}] | [action <action>] |
[level <level>] | [module <name_module>] | [text <text>] [limit <limit>] [tail <count_tail>]
```

где `<start_date>` – начальная дата интервала поиска в формате «yyyy-mm-dd»;

`<end_date>` – конечная дата интервала поиска в формате «yyyy-mm-dd»;

`<start_time>` – начальное время интервала поиска в формате «hh:mm:ss» или «hh:mm»;

`<end_time>` – конечное время интервала поиска в формате «hh:mm:ss» или «hh:mm»;

`<name_sender>` – имя отправителя;

`success` – сортировка по успешности действия. Параметр может принимать значения «OK» или «FAIL»;

`<action>` – действие. Поиск вхождения указанной подстроки;

`<name_module>` – имя модуля поиска, на основании действий которого была создана запись в журнале;

`<text>` – текстовая строка;

`<limit>` – максимальное число записей, которое необходимо вывести;

`<count_tail>` – количество строк с конца файла.

Примечания:

1. Параметр «`start_date`» должен быть меньше или равен «`end_date`». Параметр «`start_time`» должен быть меньше или равен «`end_time`».

2. Для перехода в конец файла журналирования необходимо нажать сочетание клавиш «Shift + G».

3. Для выхода из файла, необходимо нажать сочетание клавиш «Shift + Q».

1.21.11. Просмотр уровня логирования выполняется командой

```
show log <level> <facility>
```

1.22. DHCP–сервер

1.22.1. Создание/удаление DHCP/DHCP6-сервера выполняется командой
create | delete {dhcp-server | dhcp6-server}

Приведенные ниже в 1.22.2 – 1.22.6 команды выполняются в режиме конфигурации DHCP/DHCP6-сервера.

Примечание. Перед запуском DHCP/DHCP6-сервера необходимо указать интерфейс и диапазон IP-адресов, на котором будет работать DHCP/DHCP6-сервер.

1.22.2. Установка/удаление в заводское значение времени аренды адресов «по умолчанию» выполняется командой

[no] default-lease-time <sec>

где <sec> – время, задается в секундах. Может принимать значения от «0» до «3600». Значение «по умолчанию» равно «3600».

1.22.3. Добавление/удаление интерфейса, на котором будет работать DHCP-сервер, выполняется командой

[no] interface <iface_name>

где <iface_name> – имя интерфейса.

Примечания:

1. Перед добавлением интерфейса, на котором будет работать DHCP-сервер, интерфейс необходимо сначала включить и настроить на нем IP-адрес.

2. При указании на интерфейсе двух и более IP-адресов, необходимо, чтобы IP-адреса принадлежали одной подсети.

1.22.4. Задание/удаление локального IP-адреса DHCP-сервера выполняется командой

[no] local-address <ip_addr>

где <ip_addr> – локальный IP-адрес DHCP-сервера.

1.22.5. Добавление/удаление DHCP-пула выполняется командой

[no] pool <name>

где <name> – имя пула DHCP.

1.22.6. Выход из режима конфигурации DHCP-сервера выполняется командой
exit

1.22.7. Включение/выключение/перезагрузка DHCP/DHCP6-сервера выполняется командой

system {dhcp-server | dhcp6-server} {on | off | restart}

1.22.8. Создание/удаление DHCP-пула, а также вход в режим его конфигурации выполняется командой

[no] ip dhcp-pool <name_pool>

где <name_pool> – имя DHCP-пула.

Приведенные ниже в 1.22.9 – 1.22.18 команды выполняются в режиме конфигурации DHCP-пула.

1.22.9. Назначение/удаление IP-адреса сети выполняется командой

[no] network <network_value>

где <network_value> – MAC-адрес сети;

1.22.10. Назначение/удаление конкретного IP-адреса DHCP-клиенту выполняется командой

[no] host mac-address <hwaddr> ip-address <ipaddr>

где <hwaddr> – MAC-адрес DHCP-клиента;

<ipaddr> – IP-адрес, назначаемый DHCP-клиенту.

1.22.11. Задание/удаление диапазона выдаваемых IP-адресов выполняется командой

[no] range <ipstart> <ipend>

где <ipstart> – первый IP-адрес из диапазона;

<ipend> – последний IP-адрес из диапазона.

1.22.12. Установка/удаление предельного времени аренды IP-адреса для данного пула адресов выполняется командой

[no] max-lease-time <sec>

где <sec> – значение максимального времени аренды, задается в секундах. Значение «по умолчанию» равно «3600».

1.22.13. Добавление/удаление принт-сервера для DHCP-клиентов выполняется командой

[no] option lpr-server <ipaddr>

где <ipaddr> – IP-адрес принт-сервера, выдаваемый DHCP-клиентам.

1.22.14. Добавление/удаление NTP-сервера для DHCP-клиентов выполняется командой

[no] option ntp-server <ipaddr> [first]

где <ipaddr> – IP-адрес NTP-сервера, выдаваемый DHCP-клиентам.

Опция «first» указывает, что IP-адрес NTP-сервера добавится в начало списка и будет иметь приоритет «1» при обработке.

1.22.15. Добавление/удаление шлюза «по умолчанию» для DHCP-клиентов выполняется командой

```
[no] option router <ipaddr> [first]
```

где <ipaddr> – IP-адрес, назначаемый шлюзом «по умолчанию» DHCP-клиенту.

Опция «first» указывает, что шлюз «по умолчанию» добавится в начало списка и будет иметь приоритет «1» при обработке.

1.22.16. Добавление/удаление локального доменного имени для DHCP-клиентов выполняется командой

```
[no] option domain-name <name>
```

где <name> – доменное имя, выдаваемое DHCP-клиентам.

1.22.17. Добавление/удаление DNS-сервера для DHCP-клиентов выполняется командой

```
[no] option domain-name-server <ip_addr>
```

где <ip_addr> – IP-адрес DNS-сервера, выдаваемый DHCP-клиентам.

1.22.18. Выход из режима конфигурации DHCP-пула выполняется командой
exit

1.22.19. Вывод конфигурации DHCP-пула выполняется командой
show ip dhcp-pool

1.22.20. Вывод состояния DHCP/DHCP6-сервера выполняется командой
show {dhcp-server | dhcp6-server} status

1.22.21. Просмотр статистики DHCP/DHCP6-сервера выполняется командой
show {dhcp-server | dhcp6-server} clients

1.22.22. Просмотр конфигурации DHCP/DHCP6-сервера выполняется командой
show {dhcp-server | dhcp6-server} config

1.23. NTP

1.23.1. Добавление/удаление NTP-сервера выполняется командой

```
[no] ntp server <ip_addr> [iburst]
```

где <ip_addr> – IP-адрес NTP-сервера;

iburst – установка режима отправки пачки пакетов синхронизации вместо одного пакета.

1.23.2. Добавление/удаление сетевого интерфейса, сеть которого разрешена для подключения NTP-клиентов, выполняется командой

```
[no] ntp interface <iface_name>
```

где <iface_name> – имя интерфейса.

1.23.3. Включение/выключение NTP-сервиса выполняется командой

```
system ntp {on | off}
```

1.23.4. Вывод состояния NTP-сервера выполняется командой

```
show ntp
```

1.24. Установка локального времени и даты

1.24.1. Для установки даты и времени используется команда

```
system clock <date_time>
```

где <date_time> – дата и время. Дата и время задается в формате <YYYYMMDDhhmmss>, где <YYYYMMDD> – год, месяц, день, а <hhmmss> – часы, минуты, секунды.

1.24.2. Установка часовой зоны выполняется командой

```
system clock timezone <timezone>
```

где <timezone> – регион и город, задается в формате <Region/City>.

1.24.3. Для вывода текущих даты и времени используется команда

```
show system clock
```

1.24.4. Просмотр списка всех доступных часовых поясов в формате <Region/City> выполняется командой

```
show system clock timezones [region]
```

1.25. Настройка возможностей удаленного конфигурирования

1.25.1. Задание порта подключения для SSH-протокола выполняется командой

```
ssh port <number>
```

где <number> – номер порта для подключения. Может принимать значения от «0» до «65535». Значение «по умолчанию» равно «22».

1.25.2. Включение/выключение возможности удаленного конфигурирования Zenator NS Rt с помощью протокола SSH выполняется командой

```
system ssh {on | off}
```

«По умолчанию» протокол SSH включен.

1.25.3. Вывод состояния SSH-протокола выполняется командой

show ssh

1.25.4. Установка/удаление режима разрешения доступа по SSH-протоколу определенным хостам или пользователям выполняется командой

[no] ssh {allow | deny} [user <user_name>] [host <ip_pattern>]

где <user_name> – имя пользователя;

<ip_pattern> – IP-адрес хоста;

allow –режима разрешения указанным пользователям доступ по SSH;

deny –режима запрета указанным пользователям доступ по SSH.

1.25.5. Включение/выключение возможности удаленного конфигурирования Zenator NS Rt с помощью протокола Telnet выполняется командой

system telnet {on | off}

«По умолчанию» протокол Telnet включен.

1.25.6. Вывод состояния протокола Telnet выполняется командой

show telnet

1.25.7. Задание порта подключения для протокола Telnet выполняется командой

telnet port <number>

где <number> – номер порта для подключения. Может принимать значения от «0» до «65535». Значение «по умолчанию» равно «23».

1.26. SNMP

1.26.1. Включение/выключение службы SNMP выполняется командой

system snmp {on | off}

1.26.2. Включение протокола SNMP и установка параметров доступа выполняется командой

snmp community <comm> {ro | rw} [<ip_addr>]

где <comm> – пароль для SNMP-сервера. Пароль для SNMP-клиента должен совпадать с паролем SNMP-сервера;

<ip_addr> – IP-адрес подсети, с которого разрешено получение запросов;

ro – доступ для SNMP-сервера только на чтение;

rw – доступ для SNMP-сервера на чтение и редактирование.

1.26.3. Выключение протокола SNMP выполняется командой

no snmp community [<comm>]

1.26.4. Включение/выключение опции trap выполняется командой

snmp trap {on | off}

1.26.5. Установка/удаление местонахождения SNMP-сервера выполняется командой

[no] snmp location <location>

где <location> – местонахождение SNMP-сервера.

Местонахождение SNMP-сервера указывается без кавычек. Текст не может содержать пробелы и символ «'».

1.26.6. Установка/удаление параметра контактного имени SNMP-сервера выполняется командой

[no] snmp contact <contact>

где <contact> – контактные данные администратора SNMP-сервера. Контактные данные администратора SNMP-сервера указываются без кавычек. Текст не может содержать пробелы и символ «'».

1.26.7. Установка/удаление IP-адреса SNMP-сервера выполняется командой

[no] snmp src-address <ip_addr>

где <ip-addr> – IP-адрес SNMP-сервера, на котором принимается SNMP-запрос.

1.26.8. Установка/удаление параметра «host» выполняется командой

[no] snmp host <ip_addr> [version {v1 | v2c}] <comm>

где <ip_addr> – IP-адрес, на который будут отправлены SNMP traps.

1.26.9. Отображение текущего статуса протокола SNMP выполняется командой

show snmp status

1.26.10. Отображение настроек SNMP trap выполняется командой

show snmp traps

1.27. Зеркалирование портов

1.27.1. Создание/удаление зеркалирования портов выполняется командой

mirror [idx] source <src_iface_name> destination <dst_ip_addr> [interface <dst_iface_name>] [port <dst_port_value> <proto_value>] [tcp | udp]

где idx – желаемая позиция правила в таблице зеркалирования;

<src_iface_name> – имя транслирующего интерфейса;

<dst_ip_addr> – транслируемый IP-адрес;

<dst_iface_name> – имя транслируемого интерфейса;

<dst_port_value> – значение транслируемого порта;

<proto_value> – тип протокола.

1.27.2. Вывод конфигурации правил для таблицы правил mangle выполняется командой

```
show {ip4 | ip6} mangle
```

1.27.3. Вывод конфигурации правил зеркалирования для таблицы правил mangle выполняется командой

```
show {ip4 | ip6} mangle mirror
```

1.28. Туннельный интерфейс

1.28.1. GRE

1.28.1.1. Создание/удаление gre-интерфейса, вход в режим конфигурации интерфейса выполняется командой

```
create | delete gre <iface_num>
```

где <iface_num> – номер туннельного интерфейса.

Приведенные ниже в 1.28.1.2 – 1.28.1.4 команды выполняются в режиме конфигурации интерфейса.

1.28.1.2. Задание IP-адреса локального узла начала туннеля выполняется командой

```
source <src_ip>
```

где <src_ip> – IP-адрес локального узла конца туннеля.

1.28.1.3. Задание IP-адреса удаленного узла конца туннеля выполняется командой

```
destination <dst_ip>
```

где <dst_ip> – IP-адрес удаленного узла конца туннеля.

1.28.1.4. Выход из режима конфигурации туннельного интерфейса

```
exit
```

1.28.1.5. Просмотр конфигурации gre-интерфейса выполняется командой

```
show gre [<interface_num>]
```

1.28.2. IPIP

1.28.2.1. Создание/удаление ipip-интерфейса, вход в режим конфигурации интерфейса выполняется командой

```
create | delete ipip <iface_num>
```

где <iface_num> – номер туннельного интерфейса.

Приведенные ниже в 1.28.2.2 – 1.28.2.4 команды выполняются в режиме конфигурации интерфейса.

1.28.2.2. Задание IP-адреса локального узла *ipip*-интерфейса выполняется командой

```
source <src_ip>
```

где *<src_ip>* – IP-адрес локального узла туннеля.

1.28.2.3. Задание IP-адреса удаленного узла *ipip*-интерфейса выполняется командой

```
destination <dst_ip>
```

где *<dst_ip>* – IP-адрес удаленного узла туннеля.

1.28.2.4. Выход из режима конфигурации туннельного интерфейса

```
exit
```

1.28.2.5. Просмотр конфигурации *ipip*-интерфейса выполняется командой

```
show ipip[<interface_num>]
```

1.29. VPN

1.29.1. VPN-сервер

1.29.1.1. Создание/удаление VPN-сервера, а также вход в режим его конфигурации выполняется командой

```
create | delete vpn server
```

Приведенные ниже в 1.29.1.2 – 1.29.1.18 команды выполняются в режиме конфигурации интерфейса VPN-сервера.

1.29.1.2. Задание типа аутентификации с использованием секретного ключа выполняется командой

```
auth secret static_key <static_key_name>
```

где *<static_key_name>* – имя файла, содержащего секретный ключ.

1.29.1.3. Задание типа аутентификации с использованием TLS выполняется командой

```
auth tls [ca-authority <ca_cert_name>] [server-certificate <server_cert_name>]  
[server-key <server_key_name>] [dh-key <dh_key_name>]
```

где *<ca_cert_name>* – имя файла, содержащего CA-сертификат;

<server_cert_name> – имя файла, содержащего сертификат;

<server_key_name> – имя файла, содержащего ключ;

<dh_key_name> – имя файла, содержащего dh-ключ.

1.29.1.4. Задание типа туннеля выполняется командой

```
device {tap | tun}
```

где tap и tun – типы туннеля.

1.29.1.5. Задание используемого протокола выполняется командой

```
protocol {tcp4 | tcp6 | udp4 | udp6}
```

1.29.1.6. Задание порта VPN-сервера выполняется командой

```
port <port_number>
```

где <port_number> – номер порта. Значения номера порта могут принимать значения от «1» до «65535».

1.29.1.7. Задание/удаление IP-адреса на туннельном интерфейсе выполняется командой

```
[no] {ifconfig | ifconfig-ipv6} <local_address>
```

где <local_address> – IP-адрес подсети туннельного интерфейса.

Примечание. Команда выполняется при установке режима «tap».

1.29.1.8. Задание/удаление IP-адреса сервера выполняется командой

```
[no] {server-address | server-address-ipv6} <server_address>
```

где <server_address> – IP-адрес сервера.

Примечание. Команда выполняется при установке режима tun.

1.29.1.9. Задание/удаление маршрута после установления соединения для VPN-клиента выполняется с помощью команд

```
[no] ip {route | route-ipv6} {<addr> | <addr/mask>}
```

где <addr> – IP-адрес сети;

<addr/mask> – IP-адрес сети с битовой маской.

1.29.1.10. Задание/удаление маршрута на сеть клиента выполняется с помощью команд

```
[no] ip {route | route-ipv6} client <client_name> {<addr> | <addr/mask>}
```

где <client_name> – имя VPN-клиента;

<addr> – IP/IPv6-адрес сети;

<addr/mask> – IP/IPv6-адрес сети с битовой маской.

1.29.1.11. Включение/отключение передачи конфигурации интерфейса после установления соединения VPN-клиенту выполняется командой

```
[no] push client <client_name> [ignore-global-push]
```

При указании параметра «ignore-global-push» общие маршруты будут игнорироваться.

1.29.1.12. Разрешение/запрет обмена трафиком между клиентами выполняется командой

[no] client-to-client

1.29.1.13. Включение/выключение передачи конфигурации всем VPN-клиентам выполняется командой

[no] push client all

1.29.1.14. Включение/выключение сжатия трафика выполняется командой

[no] compression

1.29.1.15. Задание/удаление времени проверки соединения и времени переподключения выполняется с помощью команды

[no] keepalive <ping_timeout> <dead_timeout>

где <ping_timeout> – время проверки соединения;

<dead_timeout> – время переподключения. Должно принимать значение не менее «2 × <ping_timeout>».

1.29.1.16. Задание/удаление максимального числа VPN-клиентов выполняется командой

[no] client-max-number <client_max_number>

где <client_max_number> – максимальное число VPN-клиентов.

1.29.1.17. Проверка конфигурации сервера выполняется командой

check

1.29.1.18. Выход из режима конфигурации VPN-сервера с помощью команды

exit

1.29.1.19. Включение/выключение/перезагрузка VPN-сервера выполняется командой

vpn server {on | off | restart}

1.29.1.20. Генерация статического ключа выполняется командой

vpn create static-key <file_name>

где <file_name> – имя файла.

1.29.1.21. Просмотр конфигурации VPN-сервера выполняется командой

show vpn server

1.29.2. VPN-клиент

1.29.2.1. Создание/удаление VPN-клиента, а также вход в режим его конфигурации выполняется командой

```
create | delete vpn client <client_name>
```

где *<client_name>* – номер клиента. Может принимать значения от «1» до «3600».

Приведенные ниже в 1.29.2.2 – 1.29.2.16 команды выполняются в режиме конфигурации интерфейса VPN-клиента.

1.29.2.2. Задание типа аутентификации с использованием секретного ключа выполняется командой

```
auth secret static_key <static_key_name>
```

где *<static_key_name>* – имя файла, содержащего секретный ключ.

1.29.2.3. Задание типа туннеля выполняется командой

```
device {tap | tun}
```

где *tap* и *tun* – типы туннеля.

1.29.2.4. Задание типа аутентификации с использованием TLS выполняется командой

```
auth tls ca-authority <ca_cert_name> client-certificate <client_cert_name> client-key  
<client_key_name> dh-key <dh_key_name>
```

где *<ca_cert_name>* – имя файла, содержащего CA-сертификат;

<client_cert_name> – имя файла, содержащего сертификат клиента;

<client_key_name> – имя файла, содержащего ключ клиента;

<dh_key_name> – имя файла, содержащего dh-ключ.

1.29.2.5. Включение/отключение вывода предупреждений о попытках повторного воспроизведения выполняется командой

```
[no] mute-replay warnings
```

«По умолчанию» опция выключена.

1.29.2.6. Включение/выключение использования режима TLS выполняется командой

```
[no] dynamic port number
```

Опция актуальна только для UDP, так как при использовании TCP всегда используется случайный порт. «По умолчанию» опция выключена.

1.29.2.7. Задание используемого протокола выполняется командой

```
protocol {tcp4 | tcp6 | udp4 | udp6}
```

1.29.2.8. Задание/удаление IP-адреса на туннельном интерфейсе выполняется командой

[no] {ifconfig | ifconfig-ipv6} <local_address>

где <local_address> – IP-адрес подсети туннельного интерфейса.

Примечание. Команда выполняется при установке режима «tap».

1.29.2.9. Задание/удаление IP-адреса сервера выполняется командой

[no] {server-address | server-address-ipv6} <server_address>

где <server_address> – IP-адрес сервера.

Примечание. Команда выполняется при установке режима «tun».

1.29.2.10. Задание порта сервера выполняется командой

port <port_number>

где <port_number> – номер порта сервера. Может принимать значения от «1» до «65535». Значение порта «по умолчанию» равно «1194».

1.29.2.11. Разрешение/запрет использования случайного IP-адреса сервера выполняется командой

[no] server-address random

«По умолчанию» опция выключена.

1.29.2.12. Включение/отключение бесконечного времени разрешения использования IP-адреса сервера выполняется командой

[no] server-address infinite

«По умолчанию» опция выключена.

1.29.2.13. Установка/удаление опций DHCP выполняется командой

[no] dhcp option {dns | wins} <ip_addr>

где <ip_addr> – IP-адрес интерфейса.

Параметр «dns» обозначает использование удаленного DNS-сервера.

Параметр «wins» обозначает использование удаленного WINS-сервера.

1.29.2.14. Включение/отключение сжатия трафика выполняется командой

[no] compression

1.29.2.15. Проверка минимальной конфигурации клиента выполняется командой

check

1.29.2.16. Выход из режима конфигурации VPN-клиента с помощью команды

exit

1.29.2.17. Включение/выключение/перезагрузка VPN-клиента выполняется командой

vpn client {on | off | restart} <client_name>

1.29.2.18. Просмотр конфигурации VPN-клиента выполняется командой
show vpn client

1.30. OpenVPN

1.30.1. OpenVPN-сервер

1.30.1.1. Создание/удаление OpenVPN-сервер, а также вход в режим его конфигурации выполняется командой

```
create | delete openvpn-server <server_name>
```

где *<server_name>* – имя OpenVPN-сервера.

1.30.1.2. Включение/выключение OpenVPN-сервера выполняется командой
system openvpn-server <server_name> {on | off}

1.30.1.3. Обновление ключа шифрования OpenVPN-сервера выполняется командой

```
refresh openvpn-server key <server_name>
```

1.30.1.4. Создание/удаление клиента для сервера выполняется командой

```
create | delete openvpn-server client <server_name> name <client_name>
```

```
[country <country_name>] [organization <org_name>]
```

где *<client_name>* – имя OpenVPN-клиента;

<country_name> – название страны;

<org_name> – название организации.

Вместе с клиентом создается или отзывается его сертификат. Сертификаты клиентов подписываются сертификатом конкретного сервера (не корневым сертификатом).

1.30.1.5. Сохранение сертификата на USB-накопитель выполняется командой
save openvpn-certificate server <server_name> client <client_name>

Примечания:

1. Предварительно созданный сертификат сохраняется на USB-накопитель в формате OVPN.

2. USB-накопитель должен быть примонтирован и зарегистрирован в системе в соответствии с 1.5.9.

Приведенные ниже в 1.30.1.6 – 1.30.1.25 команды выполняются в режиме конфигурации OpenVPN-сервера.

1.30.1.6. Задание типа аутентификации клиентов по статическому ключу выполняется командой

```
auth-method static
```

1.30.1.7. Задание типа аутентификации с использованием TLS выполняется командой

```
auth-method tls [no_dh]
```

где *no_dh* – отключение обмена ключами Диффи-Хеллмана.

1.30.1.8. Задание типа туннеля *tun* выполняется командой

```
tunnel tun
```

1.30.1.9. Задание типа туннеля *tap* выполняется командой

```
tunnel tap [bridged [gateway {<ip_addr> | domain | dhcp}]]
```

где *bridged* – указывается при наличии сетевого моста.

gateway – параметр определяет сетевые настройки, которые сервер будет сообщать клиентам.

1.30.1.10. Задание используемого протокола выполняется командой

```
protocol {tcp | tcp4 | tcp6 | udp | udp4 | udp6}
```

1.30.1.11. Задание/удаление *ip*-адреса для подключения к серверу выполняется командой

```
[no] bind address {<public_addr> | domain}
```

где *<public_addr>* – *ip*-адрес для подключения к серверу.

Примечание. Команда выполняется при установке режима *tun*.

1.30.1.12. Задание/удаление порта для подключения к серверу выполняется командой

```
[no] bind port <port_number>
```

где *<port_number>* – номер порта. Значения номера порта могут принимать значения от «1» до «65535».

1.30.1.13. Задание виртуальной подсети, откуда клиентам будут назначены адреса, выполняется командой

```
[no] network <ip_with_mask>
```

где *<ip_with_mask>* – *IP*-адрес и маска подсети.

Маска подсети «/31» используется для соединения типа «точка-точка», которое доступно для метода аутентификации *static*.

1.30.1.14. Задание/удаление диапазона *IP*-адресов, из которого выдаются *IP*-адреса клиентам, выполняется командой

[no] ip-pool start <start_pool_address> end <stop_pool_address> [linear]

где <start_pool_address> – стартовый IP-адрес;

<stop_pool_address> – конечный IP-адрес;

linear – последовательная выдача IP-адресов из диапазона.

1.30.1.15. Задание диапазона IP-адресов из всех доступных адресов в виртуальной подсети выполняется командой

ip-pool full [linear]

1.30.1.16. Задание/удаление маршрута после установления соединения для VPN-клиента выполняется с помощью команд

[no] route <net_addr/mask> [gateway {<ip_addr> | domain}] [metric <value>]

1.30.1.17. Задание/удаление маршрута на сеть клиента выполняется с помощью команд

[no] client network <client_name> <net_addr/mask>

где <client_name> – имя VPN-клиента;

<net_addr/mask> – IP-адрес сети с битовой маской.

1.30.1.18. Включение/отключение передачи конфигурации интерфейса после установления соединения VPN-клиенту выполняется командой

[no] client ignore-common-push <client_name>

1.30.1.19. Разрешение/запрет обмена трафиком между клиентами выполняется командой

[no] client-to-client

1.30.1.20. Включение/выключение передачи маршрута VPN-клиенту выполняется командой

[no] push route [client <client_name>] <net_addr/mask> [gateway {<ip_addr> | domain}] [metric <value>]

1.30.1.21. Включение/выключение передачи IP-адреса тунеля VPN-клиенту выполняется командой

[no] push address client <client_name> local {<ip_addr> | domain} remote {<ip_addr> | domain}

1.30.1.22. Включение/выключение сжатия трафика выполняется командой

[no] compression

1.30.1.23. Задание/удаление времени проверки соединения и времени переподключения выполняется с помощью команды

[no] keepalive <ping_timeout> <dead_timeout>

где `<ping_timeout>` – время проверки соединения;
`<dead_timeout>` – время переподключения. Должно принимать значение не менее «2 × `<ping_timeout>`».

1.30.1.24. Задание/удаление максимального числа VPN-клиентов выполняется командой

```
[no] client-max-number <client_max_number>
```

где `<client_max_number>` – максимальное число VPN-клиентов.

1.30.1.25. Выход из режима конфигурации VPN-сервера с помощью команды
`exit`

1.30.1.26. Просмотр конфигурации OpenVPN-сервера выполняется командой
`show openvpn-server <server_name>`

1.30.1.27. Вывод клиентов OpenVPN-сервера выполняется командой
`show openvpn-server <server_name> clients`

1.30.2. Пример настройки OpenVPN-сервера

1.30.2.1. Создаем сервер, привяжем его к адресу `bind_addr` с помощью команд:
Интерфейс с адресом `<bind_addr>` должен быть поднят.

```
create openvpn-server 1
  auth-method tls
  bind address <bind_addr>
  network 172.16.0.0/24
  ip-pool start 172.16.0.2 end 172.16.0.20
  exit
commit
```

Примечание. Интерфейс с адресом `<bind_addr>` должен быть поднят.

1.30.2.2. Создаем клиента с помощью команд:

```
create openvpn-server client 1 name 11
commit
```

1.30.2.3. Запускаем сервер с помощью команд:

```
system openvpn-server 1 on
commit
```

1.30.2.4. На машине клиента по SSH-протоколу обращаемся к OpenVPN-серверу и копируем в текущую директорию конфигурацию клиента с помощью команды

```
scp <bind_addr>:/etc/openvpn/server/1/clients/11/11.ovpn .
```

1.30.2.5. На машине клиента запускаем openvpn с помощью команды

```
sudo openvpn --config 11.ovpn
```

1.31. L2TP

1.31.1. L2TP-сервер

1.31.1.1. Создание/удаление L2TP-сервера, а также вход в режим его конфигурации выполняется командой

```
create | delete l2tp server <interface_num>
```

где <interface_num> – номер интерфейса.

Приведенные ниже в 1.31.1.2 – 1.31.1.25 команды выполняются в режиме конфигурации L2TP-сервера.

1.31.1.2. Задание/удаление локального IP-адреса интерфейса L2TP-сервера выполняется командой

```
[no] ip local <ip_addr>
```

где <ip_addr> – локальный IP-адрес интерфейса.

1.31.1.3. Задание MTU на интерфейсе L2TP-сервера выполняется командой

```
ip mtu <mtu>
```

где <mtu> – параметр MTU, задается в октетах. Может принимать значения от «128» до «16384».

1.31.1.4. Установка значения MRU на интерфейсе L2TP-сервера выполняется командой

```
ip mru <mru>
```

где <mru> – параметр MRU в октетах. Может принимать значения от «128» до «16384».

1.31.1.5. Задание/удаление IP-адреса интерфейса L2TP-клиента (задание/удаление маршрута «по умолчанию») выполняется командой

```
[no] ip route <ip_addr/mask>
```

где <ip_addr/mask> – IP-адрес интерфейса и маска интерфейса L2TP -клиента.

1.31.1.6. Добавление/удаление IP-адресов DNS-серверов, передаваемых клиентам выполняется командой

```
[no] dns-servers <ip_addr1> [<ip_addr2>]
```

где <ip-addr1> и <ip-addr2> – IP-адреса DNS-серверов.

1.31.1.7. Установка/удаление текущего значения временного интервала посылки эхо-запросов выполняется командой

```
[no] lcp-echo-interval <val>
```

где <val> – временной интервал посылки эхо-запросов, задается в секундах.

При удалении текущего значения временного интервала посылки эхо-запросов на интерфейсе происходит установка значения «по умолчанию».

1.31.1.8. Установка/удаление числа неуспешных эхо-запросов, после которых соединение считается разорванным выполняется командой

```
[no] lcp-echo-failure <val>
```

где <val> – число неуспешных эхо-запросов.

При удалении текущего значения неуспешных эхо-запросов на интерфейсе происходит установка значения «по умолчанию».

1.31.1.9. Задание/удаление параметров авторизации клиентов на L2TP-сервере выполняется командой

```
[no] auth-clients username <name> password <pass>
```

где <name> – имя клиента;

<pass> – пароль клиента.

1.31.1.10. Задание/удаление IP-адреса RADIUS-сервера для авторизации клиентов выполняется командой

```
[no] auth-clients radius <addr>
```

где <addr> – IP-адреса radius-сервера.

1.31.1.11. Задание/удаление диапазона IP-адресов, из которого выдаются IP-адреса клиентам, выполняется командой

```
[no] ip pool <start_pool_address> <stop_pool_address>
```

где <start_pool_address> – стартовый IP-адрес;

<stop_pool_address> – конечный IP-адрес.

1.31.1.12. Задание/удаление диапазона разрешенных IP-адресов L2TP-клиентов выполняется командой

```
[no] ip lacpool <start_pool_address> <stop_pool_address>
```

1.31.1.13. Задание/удаление диапазона запрещенных IP-адресов L2TP-клиентов выполняется командой

```
[no] ip deny pool <start_pool_address> <stop_pool_address>
```

1.31.1.14. Задание/удаление имени хоста сервера выполняется командой

```
[no] hostname <name>
```

где <name> – имя хоста сервера.

1.31.1.15. Задание/удаление предварительного общего ключа PSK для авторизации с IPsec выполняется командой

```
[no] pre-shared-key <key>
```

где <key> – ключ.

1.31.1.16. Установка требования/отказа клиенту в PPP-аутентификации выполняется командой

```
[no] authentication {require | refuse}
```

где require – требование PPP-аутентификации;

refuse – отказ PPP-аутентификации.

1.31.1.17. Установка требования/отказа PPP-аутентификации по протоколу PAP выполняется командой

```
[no] pap {require | refuse}
```

1.31.1.18. Установка требования/отказа PPP-аутентификации по протоколу CHAP выполняется командой

```
[no] chap {require | refuse}
```

1.31.1.19. Установка требования/отказа PPP-аутентификации по протоколу MSCHAPv1 выполняется командой

```
[no] mschap {require | refuse}
```

1.31.1.20. Установка требования/отказа клиенту в unix-аутентификации (логин и пароль берется из локального «etc/passwd») выполняется командой

```
[no] unix-authentication {yes | no}
```

где yes – требование unix-аутентификации;

no – отказ unix-аутентификации.

1.31.1.21. Установка/отмена разрешения создания только одного туннеля между клиентом и сервером выполняется командой

```
[no] exclusive {yes | no}
```

1.31.1.22. Установка/отмена использования сокрытия полей AVP выполняется командой

```
[no] hidden-bit {yes | no}
```

1.31.1.23. Установка/отмена использования бита длины, указывающего полезную нагрузку l2tp-пакета выполняется командой

```
[no] length-bit {yes | no}
```

1.31.1.24. Установка/отмена использования запрета назначения адреса из пула (например, использование rppd с поддержкой RADIUS) выполняется командой

```
[no] ip assign {yes | no}
```

1.31.1.25. Выход из режима конфигурации интерфейса L2TP-сервера выполняется командой

```
exit
```

1.31.1.26. Включение/выключение L2TP-клиента выполняется командой

```
system l2tp server <interface_num> {on | off}
```

1.31.1.27. Вывод конфигурации L2TP-сервера выполняется командой

```
show l2tp server [<interface_num>]
```

1.31.2. L2TP-клиент

1.31.2.1. Создание/удаление L2TP-клиента, а также вход в режим его конфигурации выполняется командой

```
create | delete l2tp client <interface_num>
```

где <interface_num> – номер интерфейса.

Приведенные ниже в 1.31.2.2 – 1.31.2.22 команды выполняются в режиме конфигурации L2TP-клиента.

1.31.2.2. Задание/удаление IP-адреса L2TP-сервера выполняется командой

```
[no] server ip <addr>
```

где <iaddr> – IP-адрес L2TP-сервера.

1.31.2.3. Задание/удаление имени DNS-сервера выполняется командой

```
[no] server dns <dns>
```

где <dns> – имя DNS-сервера.

1.31.2.4. Задание MTU на интерфейсе L2TP-клиента выполняется командой

```
ip mtu <mtu>
```

где <mtu> – параметр MTU, задается в октетах. Может принимать значения от «128» до «16384».

1.31.2.5. Установка значения MRU на интерфейсе L2TP-клиента выполняется командой

```
ip mru <mru>
```

где <mru> – параметр MRU в октетах. Может принимать значения от «128» до «16384».

1.31.2.6. Установка/удаление текущего значения временного интервала посылки эхо-запросов выполняется командой

[no] lcp-echo-interval <val>

где <val> – временной интервал посылки эхо-запросов, задается в секундах.

При удалении текущего значения временного интервала посылки эхо-запросов на интерфейсе происходит установка значения «по умолчанию».

1.31.2.7. Установка/удаление числа неуспешных эхо-запросов, после которых соединение считается разорванным выполняется командой

[no] lcp-echo-failure <val>

где <val> – число неуспешных эхо-запросов.

При удалении текущего значения неуспешных эхо-запросов на интерфейсе происходит установка значения «по умолчанию».

1.31.2.8. Установка/удаление текущего значения числа попыток соединения, после которого соединение перестает устанавливаться, выполняется командой

[no] maxfall <num>

где <num> – число попыток соединения, после которого соединение перестает устанавливаться.

1.31.2.9. Включение/выключение постоянного возобновления соединения при ошибках выполняется командой

[no] persistent

При удалении текущего значения числа попыток соединения, после которого соединение перестает устанавливаться, происходит установка значения «по умолчанию».

1.31.2.10. Установка/удаление текущего значения временного интервала между повторными подключениями выполняется командой

[no] holdoff <sec>

где <sec> – значение интервала, задается в секундах.

При удалении текущего значения временного интервала между повторными подключениями происходит установка значения «по умолчанию».

1.31.2.11. Задание/удаление параметров авторизации клиентов на L2TP-сервере выполняется командой

[no] auth-clients username <name> password <pass>

где <name> – имя клиента;

<pass> – пароль клиента.

1.31.2.12. Включение/выключение использования маршрута до PPTP-сервера в качестве маршрута «по умолчанию» выполняется командой

```
[no] use-default-route
```

1.31.2.13. Включение/выключение использования dns-серверов, IP-адреса которых получены от PPTP-сервера, выполняется командой

```
[no] use-dns
```

1.31.2.14. Задание/удаление предварительного общего ключа PSK для авторизации с IPsec выполняется командой

```
[no] pre-shared-key <key>
```

где <key> – ключ.

1.31.2.15. Установка требования/отказа клиенту в PPP-аутентификации выполняется командой

```
[no] authentication {require | refuse}
```

где require – требование PPP-аутентификации;

refuse – отказ PPP-аутентификации.

1.31.2.16. Установка требования/отказа PPP-аутентификации по протоколу PAP выполняется командой

```
[no] pap {require | refuse}
```

1.31.2.17. Установка требования/отказа PPP-аутентификации по протоколу CHAP выполняется командой

```
[no] chap {require | refuse}
```

1.31.2.18. Установка требования/отказа PPP-аутентификации по протоколу MSCHAPv1 выполняется командой

```
[no] mschap {require | refuse}
```

1.31.2.19. Задание/удаление описания интерфейса выполняется командой

```
[no] description <comment>
```

где <comment> – текст для описания интерфейса.

Примечание. Описание интерфейса указывается без кавычек в случае содержания в описании одного слова и в двойных кавычках при двух и более словах. Текст в описании может содержать пробелы, не может содержать символы «'» и «-» и превышать 255 символов.

1.31.2.20. Установка/удаление максимального количества попыток повторной установки L2TP-соединения с сервером выполняется командой

```
redial max <maxr>
```

где *<maxt>* – максимальное количество попыток соединения.

1.31.2.21. Установка/удаление временного интервала между повторными попытками установления L2TP-соединения выполняется командой

```
redial timeout <timeout>
```

где *<timeout>* – временной интервал.

1.31.2.22. Выход из режима конфигурации интерфейса L2TP-клиента выполняется командой

```
exit
```

1.31.2.23. Включение/выключение L2TP-клиента выполняется командой

```
system l2tp client <interface_num> {on | off}
```

1.31.2.24. Вывод конфигурации L2TP-клиента выполняется командой

```
show l2tp client [<interface_num>]
```

1.32. IPSec

1.32.1. Создание/удаление интерфейса IPSec, а также вход в режим его конфигурации выполняется командой

```
create | delete ipsec <number>
```

где *<number>* – номер туннеля IPSec, может принимать значения от «1» до «100».

Приведенные ниже в 1.32.2 – 1.32.23 команды выполняются в режиме конфигурации IPSec.

1.32.2. Задание/удаление локального IP-адреса туннеля выполняется командой

```
[no] local addr {<ip_address> | <ip_address_with_mask> | <range> | fqdn | any}
```

где *<ip_address>* – локальный IPv4/IPv6-адрес туннеля;

<ip_address_with_mask> – IPv4/IPv6-адрес туннеля с битовой маской;

<range> – диапазон IPv4/IPv6-адресов;

fqdn – имя домена;

any – специальное значение IPv4/IPv6-адреса.

1.32.3. Задание/удаление IP-адреса удаленной стороны туннеля выполняется командой

```
[no] remote addr {<ip_address> | <ip_address_with_mask> | <range> | fqdn | any}
```

где *<ip_address>* – удаленный IPv4/IPv6-адрес туннеля.

1.32.4. Задание/удаление IP-адреса хоста источника выполняется командой

```
[no] local sourceip {<ip_address> | <ip_address_with_mask> | <range> | <virtual_addr>}
```

где <ip_address> – IPv4/IPv6-адрес хоста источника;
 <ip_address_with_mask> – IPv4/IPv6-адрес хоста источника с битовой маской;
 <virtual_addr> – запрос виртуального адреса для использования в качестве внутреннего туннельного адреса. Может принимать значения «config», «config4», «config6».

1.32.5. Задание/удаление IP-адреса хоста приемника выполняется командой

[no] remote sourceip {<ip_address> | <ip_address_with_mask> | <range> | <virtual_addr>}

где <ip_address> – IPv4/IPv6-адрес хоста приемника;

<ip_address_with_mask> – IPv4/IPv6-адрес хоста приемника с битовой маской;

1.32.6. Задание IP-адреса локальной сети выполняется командой

local network ip <ip_address_with_mask> [proto <proto_value>] [port <port_value>]

где <ip_address_with_mask> – IP-адрес локальной сети с битовой маской;

<proto_value> – тип протокола источника;

<port_value> – значение порта источника.

1.32.7. Задание специального IP-адреса локальной сети выполняется командой

local network dynamic [proto <proto_value>] [port <port_value>]

1.32.8. Удаление IP-адреса локальной сети выполняется командой

no local network

1.32.9. Задание IP-адреса удаленной сети выполняется командой

remote network ip <ip_address_with_mask> [proto <proto_value>] [port

<port_value>]

где <ip_address> – IP-адрес удаленной сети с битовой маской;

<proto_value> – тип протокола приемника;

<port_value> – значение порта приемника.

1.32.10. Задание специального IP-адреса удаленной сети выполняется командой

remote network dynamic [proto <proto_value>] [port <port_value>]

1.32.11. Удаление IP-адреса удаленной сети выполняется командой

no remote network

1.32.12. Задание/удаление идентификатора источника выполняется командой

[no] local id <id>

где <id> – идентификатор источника.

1.32.13. Задание/удаление идентификатора приемника выполняется командой

[no] remote id <id>

где <id> – идентификатор приемника.

1.32.14. Задание/удаление параметров сертификата источника выполняется командой

```
[no] local certificate name <cert_name>
```

где <cert_name> – имя файла сертификата.

1.32.15. Задание/удаление параметров сертификата приемника выполняется командой

```
[no] remote certificate name <cert_name>
```

1.32.16. Установка режима аутентификации выполняется командой
authentication {pubkey | secret | rsasig | never}

1.32.17. Установка/удаление алгоритмов IKE выполняется командой

```
[no] ike-alg <encrypted> <integrity> <dh_group> <pfr>
```

где <encrypted> – алгоритм шифрования. Параметр может принимать значения из следующего перечня алгоритмов (3des | aes128 | aes192 | aes256 | aes128ctr | aes192ctr | aes256ctr | aes128ccm | aes256ccm16 | camellia256);

<integrity> – алгоритм проверки целостности данных и аутентификации. Параметр может принимать значения из следующего перечня алгоритмов (sha1 | md5_128 | sha1_160 | aesxcbc | aes256gmac | sha256 | sha384 | sha512 | sha256_96);

<dh_group> – группа Diffie-Hellman для установления ключей. Параметр может принимать значения из следующего перечня групп (modp3072 | modp4096 | modp8192 | modp2048 | modp1536 | modp1024 | modp768 | ecp256 | ecp384 | ecp521 | ecp224 | ecp192);

<pfr> – группа псевдослучайных функций. Параметр может принимать значения из следующего перечня групп (pfrmd5 | prfsha1 | prfaesgmac | prfsha384 | prfsha512).

1.32.18. Установка/удаление алгоритма ESP выполняется командой

```
[no] esp-alg <encrypted> <integrity> <dh_group>
```

1.32.19. Установка/удаление PSK выполняется командой

```
[no] pre-shared-key <key>
```

где <key> – крипто-ключ. Длина крипто-ключа может принимать значения от «32» до «64» символов.

1.32.20. Установка/удаление времени жизни безопасной ассоциации выполняется командой

ike-lifetime <lifetime_value> {sec | min | hour | days}

где *<lifetime_value>* – времени жизни безопасной ассоциации.

1.32.21. Установка/удаление времени жизни действия ключей выполняется командой

sa-lifetime <lifetime_value> {sec | min | hour | days}

1.32.22. Установка режима туннеля выполняется командой

type {transport | tunnel}

1.32.23. Выход из режима конфигурации IPSec выполняется командой

exit

1.32.24. Установка/удаление количества повторных передач пакетов перед отказом выполняется командой

[no] set ipsec retransmit-tries <count>

где *<count>* – количество повторных передач пакетов, задается в секундах. Может принимать значения от «1» до «255».

При удалении текущего значения количества повторных передач пакетов перед отказом происходит установка значения «по умолчанию». Значение «по умолчанию» равно «5».

1.32.25. Рестарт модуля выполняется командой

ipsec restart

1.32.26. Включение/отключение интерфейса IPSec выполняется командой

ipsec <number> {on | off}

1.32.27. Вывод состояния IPSec-туннеля с номером *<number>* выполняется командой

show ipsec [<number>]

1.33. VRRP

1.33.1. Вход в режим конфигурации экземпляра VRRP, а также создание/удаление интерфейса VRRP, выполняется командой

create | delete vrrp <vrrp_name>

где *<name>* – имя экземпляра VRRP.

Приведенные ниже в 1.33.2 – 1.33.10 команды выполняются в режиме конфигурации экземпляра VRRP.

Примечания:

1. Перед созданием экземпляра VRRP необходимо войти в режим конфигурации интерфейса, поверх которого будет работать VRRP, включить интерфейс и задать IP-адрес.

2. Для каждого экземпляра должны быть обязательно заданы следующие параметры:

- IP-адрес виртуального маршрутизатора;
- ID виртуального маршрутизатора;
- интерфейс, поверх которого должен работать VRRP.

1.33.2. Задание/удаление интерфейса, поверх которого должен работать VRRP выполняется командой

```
[no] interface <iface_name>
```

где <iface_name> – имя интерфейса.

1.33.3. Включение/отключение режима вытеснения выполняется командой

```
[no] preempt
```

1.33.4. Установка/удаление текущего значения приоритета маршрутизатора выполняется командой

```
[no] priority <prio>
```

где <prio> – значение приоритета от «1» до «255». Наивысший приоритет – «255».

При удалении текущего значения приоритета маршрутизатора происходит установка значения «по умолчанию». Значение приоритета «по умолчанию» равно «100».

1.33.5. Добавление/удаление интерфейса в список мониторинга состояния выполняется командой

```
[no] track <iface_name>
```

1.33.6. Задание/удаление времени между запросами статуса у устройства, участвующего в обмене информации по основному каналу, выполняется командой

```
[no] dead-time <sec>
```

где <sec> – интервал между запросами статуса у устройства, участвующего в обмене информации по основному каналу, задается, задается в секундах. Может принимать значения от «1» до «255». Значение «по умолчанию» равно «4».

1.33.7. Добавление/удаление IP-адреса виртуального маршрутизатора выполняется командой

```
[no] virtual ip <ip_addr>
```

где <ip_addr> – IPv4/IPv6-адрес виртуального маршрутизатора.

1.33.8. Указание/удаление ID виртуального маршрутизатора выполняется командой

```
[no] virtual id <val>
```

где <val> – числовой идентификатор виртуального маршрутизатора.

1.33.9. Задание/удаление интервала между запросами выполняется командой

```
[no] interval <sec>
```

где <sec> – интервал между запросами, задается в секундах. Может принимать значения от «1» до «255». Значение «по умолчанию» равно «1».

1.33.10. Выход из режима конфигурации экземпляра VRRP выполняется командой

```
exit
```

1.33.11. Включение/выключение экземпляра VRRP выполняется командой

```
system vrrp <vrrp_name> {on | off}
```

1.33.12. Просмотр конфигурации экземпляров VRRP выполняется командой

```
show vrrp [key]
```

где <key> – идентификатор клиента.

1.34. LLDP

1.34.1. Создание/удаление транслирующего LLDP-интерфейса выполняется командой

```
create | delete lldp <iface_name> [port-description <port_descr>]
```

где <iface_name> – имя интерфейса;

<port_descr> – описание порта.

1.34.2. Установка интервала времени между рассылками LLDP-сообщений выполняется с помощью команды выполняется командой

```
set lldp tx-interval <tx-interval>
```

где <tx-interval> – значение интервала времени между рассылками LLDP-сообщений. Может принимать значения от «2» до «300».

1.34.3. Установка значения множителя для tx-интервала выполняется с помощью команды

```
set lldp tx-hold <tx-hold>
```

где <tx-hold> – множитель для tx-интервала. Значение «по умолчанию» равно «4».

1.34.4. Установка статуса LLDP-сообщений выполняется с помощью команды

```
set lldp status {disabled | tx-only | rx-only | rx-and-tx}
```

где disabled – отключение отправки и получения LLDP-сообщений;

tx-only – только отправка LLDP-сообщений, входящие сообщения LLDP блокируются;

rx-only – только получение LLDP-сообщений, исходящие сообщения LLDP блокируются;

rx-and-tx – отправка и получение LLDP-сообщений (режим «по умолчанию»).

1.34.5. Задание IPv4/IPv6-адреса управления выполняется командой

set lldp management-ip <ip_addr>

где <ip_addr> – IPv4/IPv6-адрес интерфейса.

1.34.6. Включение/выключение агента SNMP выполняется командой

lldp snmp-subagent {enable | disable}

1.34.7. Включение/выключение LLDP-интерфейса выполняется командой

system lldp {on | off}

1.34.8. Вывод конфигурации LLDP-протокола выполняется командой

show lldp config

1.34.9. Вывод статистики по протоколу LLDP выполняется командой

show lldp statistics

1.35. Вывод статистики

1.35.1. Вывод статистики для протокола TCP выполняется командой

*show {ip | ip4 | ip6} statistics tcp [src-ip <s_ip>] [src-port <s_port>] [dest-ip <d_ip>]
[dst-port <d_port>] [state]*

где ip – вывод статистики по протоколу IP;

ip4 – вывод статистики по протоколу IPv4;

ip6 – вывод статистики по протоколу IPv6;

<s_ip> – IP-адрес источника;

<s_port> – номер порта источника, может принимать значения от «0» до «65535»;

<d_ip> – IP-адрес получателя;

<d_port> – номер порта получателя, может принимать значения от «0» до «65535»;

state – состояние соединения.

1.36. Обновление программного обеспечения

1.36.1. Получение списка обновлений Zenator NS Rt выполняется командой
system update

1.36.2. Задание/удаление доверенного сервера обновлений выполняется командой

```
system update-server {main | flash} [certificate <cert_file> key <key_file>] [interval <interval>]
```

где main – главный сервер;

flash – обновления с флеш-носителя;

<cert_file> – имя файла, содержащего сертификат клиента;

<key_file> – имя файла, содержащего ключ сертификата;

<interval> – промежуток времени для автоматической проверки обновлений.

При обновлении с флеш-носителя, он должен быть примонтирован и зарегистрирован в системе в соответствии с 1.5.9.

1.36.3. Вывод адреса сервера обновлений выполняется командой
show system update-server

1.36.4. Обновление общесистемного программного обеспечения выполняется командой

```
system upgrade
```

1.36.5. Откат программного обеспечения до предыдущей версии выполняется командой

```
system rollback
```

1.37. Системные команды

1.37.1. Системные команды управления пользователями и группами приведены в 1.4.

1.37.2. Администрирование системных модулей выполняется командой
system modules <name> {on | off | reload}

где <name> – название модуля;

on – включение модуля;

off – выключение модуля;

reload – перезагрузка модуля.

1.37.3. Просмотр списка модулей, находящихся в системе, выполняется командой

```
show system modules
```

1.37.4. Создание/удаление учетной записи пользователя службы поддержки выполняется командой

[no] system maintenance-access

1.37.5. Редактирование имени хоста системы выполняется командой

set system hostname <system_name>

где <system_name> – имя хоста системы.

1.37.6. Задание/удаление почтового имени «по умолчанию» выполняется командой

[no] set system mailname <mailname>

где <mailname> – почтовое имя. Почтовое имя задается в формате «abc@<имя домена>».

1.37.7. Перезагрузка системы без сохранения конфигурации (загружается профиль «null») выполняется командой

system reboot

1.37.8. Выключение системы выполняется командой

system shutdown

1.37.9. Включение/отключение сервиса API выполняется командой

system api {on | off | certificate <file_name>}

где <file_name> – имя файла сертификата.

1.37.10. Включение/выключение LLDP выполняется командой

system lldp {on | off}

1.37.11. Проверка доступности удаленного узла с помощью ICMP-запросов выполняется командой

ping <addr> [source {iface <iface_name> | addr <ip_addr>}] [size <size>] [interval <interval>] [count <count>] [timeout <timeout>] [tos <tos>],

где <addr> – IP-адрес удаленного узла;

<iface_name> – имя интерфейса;

<size> – размер пакета. Значение задается в байтах;

<interval> – временной интервал работы команды, задается в секундах.

Значение «по умолчанию» равно «1»;

<count> – количество генерируемых ICMP-запросов;

<timeout> – значение интервала в секундах;

<tos> – значение «ToS». Значение задается в шестнадцатичном формате в диапазоне от «0x00» до «0x1E».

Примечание. Прервать выполнение команды можно с помощью клавиши «Enter».

1.37.12. Захват и проверка сетевого трафика на интерфейсе выполняется командой

```
tcpdump <iface_name>
```

где <iface_name> – имя интерфейса.

1.37.13. Сканирование сети выполняется командой

```
nmap <host_port>
```

где <host_port> – адрес хоста и порт.

1.37.14. Загрузка/сохранение сертификата SSL выполняется командой

```
{load | save} certificate flash <file_name>
```

где <file_name> – имя файла сертификата.

1.37.15. Удаление сертификата SSL выполняется командой

```
delete certificate {all | <file_name>}
```

1.37.16. Сохранение системных неизменяемых файлов на флеш-носитель выполняется командой

```
save backup flash
```

1.37.17. Разрешение доменного имени выполняется командой

```
domain lookup <name>
```

где <name> – имя сервера.

1.37.18. Вывод информации сертификатов SSL выполняется командой

```
show certificate <file_name>
```

где <file_name> – имя файла CA-сертификата.

1.37.19. Вывод информации о загрузенности центрального процессора выполняется командой

```
show system cpu [interval <interv>]
```

где <interv> – время, задается в секундах.

1.37.20. Вывод почтового имени, заданного «по умолчанию», выполняется командой

```
show system mailname
```

1.37.21. Вывод имени системы выполняется командой

```
show system hostname
```

1.37.22. Вывод информации о загрузенности оперативного запоминающего устройства выполняется командой

```
show system memory
```

1.37.23. Вывод названия программного обеспечения и его десятичного номера выполняется командой

```
show version
```

1.37.24. Вывод версии программного обеспечения выполняется командой

```
show version build
```

1.37.25. Вывод состояния сервиса API выполняется командой

```
show system api
```

1.38. Команды администратора сервера регистрации

1.38.1. Добавление пользователя клиентского устройства выполняется с помощью команды

```
ndis add user <name>
```

где <name> – имя пользователя.

1.38.2. Удаление пользователя клиентского устройства выполняется с помощью команды

```
ndis delete user <name>
```

1.38.3. Активация клиентского устройства пользователя выполняется с помощью команды

```
ndis add user <name> uid <UID>
```

где <UID> – уникальный идентификатор клиентского устройства (серийный номер клиентского устройства). При вводе значения используется автодополнение из списка неактивных устройств.

Примечание. Серийный номер появляется в списке неактивных устройств после того, как клиент NDIS присылает этот номер серверу NDIS.

1.38.4. Деактивация клиентского устройства пользователя выполняется с помощью команды

```
ndis add user <name> uid <UID>
```

Примечание. Устройство удаляется из секции [devices] конфигурационного файла.

1.38.5. Задание/удаление сервера VPN для клиентов NDIS выполняется с помощью команды

```
[no] ndis vpn <тип сервера> <имя сервера>
```

где <тип сервера> – тип сервера. Может принимать значение «openvpn»;

<имя сервера> – имя NDIS-сервера.

1.38.6. Включение/выключение NDIS-сервера выполняется с помощью команды
system ndis {on | off}

1.38.7. Вывод состояния сервера регистрации выполняется с помощью команды

show system ndis

1.38.8. Вывод списка пользователей клиентских устройств выполняется с помощью команды

ndis show ndis users

1.38.9. Вывод списка клиентских устройств пользователя с помощью команды командой

show ndis show user <name>

1.39. Контроль целостности

1.39.1. Программа имеет систему контроля целостности, обеспечивающую обслуживание двух типов объектов:

– постоянно неизменяемые (системные файлы, исполняемые файлы сервисов, предоставляемых изделию);

– транзакционно-изменяемые (журналы и файлы конфигурации изделия).

1.39.2. При установке программы создаются таблицы контрольных сумм для каждого из типов объектов. Сами таблицы также подлежат контролю целостности.

Программа производит автоматическую проверку целостности транзакционно-изменяемых объектов. Программа производит проверку целостности неизменяемых объектов при старте системы.

1.39.3. Принудительная проверка целостности всех журналов выполняется командой

check integrity logs

1.39.4. Принудительная проверка целостности журнала выполняется командой
check integrity log {syslog | auth | commands | daemon | ipfilter | testing | router}

1.39.5. Задание принудительной проверки всех изменяемых конфигурационных файлов изделия выполняется командой

check integrity configs

1.39.6. Задание принудительной проверки всех системных файлов изделия выполняется командой

check integrity system

1.39.7. Задание принудительной проверки всех неизменяемых файлов изделия выполняется командой

check integrity files

1.39.8. Задание интервала проверки контроля целостности выполняется командой

check integrity interval <interval_val>

где <interval_val> – значение интервала проверки, задается в секундах. Может принимать значения от «180» до «7200». «По умолчанию» проверка целостности выполняется каждые 30 мин.

1.39.9. Задание интервала проверки загрузки критически важных сервисов выполняется командой

check services interval <interval_val>

1.39.10. Задание интервала проверки диска выполняется командой

check disk interval <interval_val>

1.39.11. Задание интервала проверки памяти выполняется командой

check memory interval <interval_val>

1.39.12. Задание интервала проверки центрального процессора выполняется командой

check cpu interval <interval_val>

1.39.13. Отображение значения временного интервала проверки контроля целостности выполняется командой

show integrity interval

1.39.14. Отображение значения временного интервала проверки загрузки критически важных сервисов выполняется командой

show services interval

1.39.15. Отображение значения временного интервала проверки памяти выполняется командой

show memory interval

1.39.16. Отображение значения временного интервала проверки диска выполняется командой

show disk interval

1.39.17. Отображение значения временного интервала проверки центрального процессора выполняется командой

show cpu interval

1.40. Управление сессиями

1.40.1. Zenator NS Rt обеспечивает возможность одновременного подключения нескольких пользователей к системе. При входе пользователя в систему автоматически создается сессия, которая хранит параметры взаимодействия с системой. Сессия завершается при выходе пользователя из системы или по тайм-ауту (равен 10 мин).

Если пользователь не выполнял ни одной команды в течение 10 мин, автоматически происходит завершение сессии, при этом, если пользователь выполнял какие-либо другие действия, то переход к окну авторизации не происходит. При выполнении любой команды по истечении тайм-аута на экране отобразится сообщение об ошибке «Error: No session (expired, invalid...)» и будет выполнен переход к окну авторизации. При выполнении команды тайм-аут обновляется. Начало сессий и их завершение отображается в журнале «auth».

Примечание. Для пользователей, выполнивших вход в программу с помощью CLI и выполнивших вход в программу с помощью Web-интерфейса, создаются отдельные сессии.

1.40.2. Для вывода на экран информации о всех текущих сессиях используется команда

show sessions

Примечание. Номер текущей сессии отмечен знаком «*».

1.40.3. Для принудительного завершения сессии используется команда

session drop <number>

где <number> – номер сессии, которую необходимо завершить. Может принимать значения от «1» до «100».

Примечание. Данная команда обеспечивает возможность принудительного завершения как своей сессии, так и сессии, созданной другим пользователем.

1.41. Технологический доступ

1.41.1. Технологический доступ предназначен для прямого доступа к средствам программного обеспечения и используется службой технической поддержки для решения задач, недоступных штатными средствами.

1.41.2. Технологический доступ осуществляется локально или через сетевое подключение по протоколам SSH или Telnet при помощи двойной авторизации. На

первом этапе сотрудником технической поддержки осуществляется ввод имени пользователя и пароля одноразовой учетной записи. На втором этапе производится авторизованное технологическое подключение.

Примечание. Для протоколов SSH и Telnet требуется предварительное включение с помощью команд «system ssh on» или «system telnet on».

1.41.3. Для создания одноразовой учетной записи служит команда «maintenance_access», выполняемая АБ изделия. В результате ее выполнения будет получено имя пользователя и пароль, которые необходимо сообщить при обращении в службу технической поддержки.

1.42. API

1.42.1. Вход в API

1.42.1.1. API предназначен для разработчиков ПО в части интеграции с внешними системами конфигурирования и мониторинга.

1.42.1.2. Для начала работы в API-интерфейсе пользователю необходимо выполнить следующие действия:

1) настроить сетевой интерфейс, через который будет осуществляться доступ к API-интерфейсу в соответствии с 1.8;

2) включить сервис API командой «system api on».

Примечание. Доступ к сервису API осуществляется с персональной электронно-вычислительной машины, которая находится в одной подсети с Zenator NS Rt.

1.42.1.3. Клиентам для работы с REST API необходимо получить токен авторизации. Для этого требуется выполнить следующие действия:

1) Отправить запрос типа «POST» по адресу «http:// <ip_address>:8080/api/token», где <ip_address> – IP-адрес интерфейса.

Запрос должен содержать следующую последовательность данных
grant_type=password&client_id=<id клиента>&username=<имя пользователя>&password = <пароль>

Например, для получения токена авторизации для пользователя «admsec» с паролем «12345678i.» необходимо с помощью утилиты командной строки curl ввести (без пробелов) следующий запрос

```
curl -X POST http://192.168.5.244:8080/api/token -d 'grant_type=password&
username=admsec&password=12345678i.&client_id=cadmin'
```

2) В ответ на запрос получить токен авторизации в формате
access_token=<токен авторизации>&expires_in=<тайм-аут> &
token_type =<тип токена>&scope=<область доступа>&refresh_token=<токен
обновления>

Например, на предыдущий запрос будет получен следующий токен авторизации

```
access_token=wf5wtDfacH00J9Gh9NI0rMHDLDWaUt&expires_in=3600&token_type
=Bearer&scope=zenator&refresh_token=aM9WnnTZFrXhGJhVDPCHHxQhYBlzJz
```

1.42.2. Структура REST API

1.42.2.1. REST API ориентирован на обмен данными в формате JSON.

1.42.2.2. HTTP-запрос к закрытой части REST API должен включать в себя заголовок вида «Authorization: Bearer =<токен авторизации>».

1.42.2.3. REST API предоставляет интерфейс для работы с системными модулями, список которых можно получить, выполнив запрос (без пробелов) типа «GET» к модулю.

Например, запрос к модулю «sys_profile» будет иметь следующий вид

```
curl -H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt'
http://192.168.5.244:8080/api/sys_profile/get_registered_modules?load=1
```

В ответ на запрос будет получен список системных модулей

```
{
  "code": 0,
  "data": [
    [
      "acl",
      12
    ],
    [
      "api_control",
      12
    ],
    [
```

```

"arp",
12
],
...
[
"vxlan",
15
]
],
"description": "",
"template": "show_modules"
}

```

1.42.2.4. Модуль может предоставлять методы доступа к разнообразной информации. Список таких методов можно получить, выполнив запрос типа «GET» к выбранному модулю.

Например, получить список доступных методов модуля «api_control» можно с помощью запроса

```

curl -H 'Authorization: Bearer wf5wtDfachH00J9Gh9NI0rMHDLDWaUt'
http://192.168.5.244:8080/api/api_control/get_module_methods?mod=api_control

```

В ответ на запрос будет получен список доступных методов

```

{
"code": 0,
"data": [
{
"arguments": [
{
"name": "target_module",
"type": "str"
},
{
"name": "config",
"type": "str"
}
]
},
]
}

```

```

"name": "commit"
},
{
  "arguments": [
    {
      "name": "mod",
      "type": "str"
    }
  ],
  "name": "get_module_methods"
},
{
  "arguments": [],
  "name": "show"
}
],
"description": ""
}

```

1.42.3. Примеры вызова методов отображения системной информации

1.42.3.1. Для получения версии программного обеспечения необходимо ввести следующий запрос

```

curl -H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt'
http://192.168.5.244:8080/api/system/show_version

```

В ответ на запрос будет получена версия программного обеспечения в виде

```

{
  "code": 0,
  "data": "VX \u0418\u0421\u0410\u041f.30318-01 build_1.0.40 02/18/22 01:00:02",
  "description": "",
  "template": "show_data"
}

```

1.42.3.2. Для получения данных о загрузке центрального процессора необходимо ввести следующий запрос

```
curl -H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt'
```

```
http://192.168.5.244:8080/api/system/show_cpu
```

В ответ на запрос будет получена версия программного обеспечения в виде

```
{
  "code": 0,
  "data": "cpu: 0.08%\ncpu0: 0.05%\ncpu1: 0.15%\ncpu2: 0.08%\ncpu3: 0.05%",
  "description": "",
  "template": "show_data"
}
```

1.42.3.3. Для получения системного времени необходимо ввести следующий запрос

```
curl -H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt'
```

```
http://192.168.5.244:8080/api/system/show_system_clock
```

В ответ на запрос будет получена версия программного обеспечения в виде

```
{
  "code": 0,
  "data": "Local Time: \u0412\u0442 \u0444\u0435\u0432\u0440\u0435 22 11:29:07 MSK
2022\nTime Zone: Europe/Moscow\n",
  "description": "",
  "template": "show_data"
}
```

1.42.3.4. Для получения информации об использовании памяти необходимо ввести следующий запрос

```
curl -H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt'
```

```
http://192.168.5.244:8080/api/system/show_memory
```

В ответ на запрос будет получена версия программного обеспечения в виде

```
{
  "code": 0,
  "data": {
    "free memory": "6,0G",
    "total memory": "7,9G",
    "used memory": "133M"
  },
  "description": "",
```

```
"template": "show_data"
}
```

1.42.4. Примеры настройки системных модулей с помощью REST API

1.42.4.1. Изменение конфигурации интерфейсов

1.42.4.1.1. Рассмотрим процедуру составления запроса на изменение конфигурации loopback-интерфейса.

1.42.4.1.2. Изменение конфигурации loopback-интерфейса можно выполнить в Zenator NS Rt с помощью команд:

```
create loopback 1
commit
```

Вывод конфигурации loopback-интерфейса в Zenator NS Rt выполняется командой

```
show running-profile loopback
```

В результате в консоле будет выведена следующая конфигурация loopback-интерфейса

```
loopback: {
  "1": "loop1"
}
```

1.42.4.1.3. Данную конфигурацию можно загрузить в модуль «loopback» средствами REST API.

Для настройки модуля необходимо выполнить запрос типа «HTTP POST» к модулю «loopback», который будет иметь следующий вид

```
curl -X POST \
  -H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt' \
  -H 'Content-Type: application/json' \
  'http://192.168.5.244:8080/api/loopback' \
  -d '{
    "1": "loop1"
  }'
```

В ответ на запрос будет получена следующая конфигурация

```
{
  "code": 0,
```

```
"description": "",
"loopback": {
  "1": "loop1"
}
}
```

1.42.4.2. Загрузка конфигурации сетевых маршрутов

1.42.4.2.1. Рассмотрим процедуру составления запроса на изменение конфигурации сетевых маршрутов.

1.42.4.2.2. Загрузку конфигурации сетевых маршрутов можно выполнить в Zenator NS Rt с помощью команды

```
ip route 10.10.10.0/24 via 172.16.0.1
```

1.42.4.2.3. Данную конфигурацию можно загрузить в модуль «static_routes» средствами REST API.

Для настройки модуля необходимо выполнить запрос типа «HTTP POST» к модулю «static_routes», который будет иметь следующий вид

```
curl -X POST \
  -H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt' \
  -H 'Content-Type: application/json' \
  'http://192.168.5.244:8080/api/static_routes'
-d '{
  "ip_tables": {},
  "multiple": {},
  "single": {
    "_10.10.10.0/24_172.16.0.1": {
      "blackhole": "",
      "destination": "10.10.10.0/24",
      "distance": "",
      "gateway": "172.16.0.1",
      "iface": "",
      "proto": "ipv4",
      "table": ""
    }
  }
}
```

```
}'
```

В ответ на запрос будет получена следующая конфигурация

```
{
  "code": 0,
  "description": "",
  "static_routes": {
    "ip_tables": {},
    "multiple": {},
    "single": {
      "_10.10.10.0/24_172.16.0.1": {
        "blackhole": "",
        "destination": "10.10.10.0/24",
        "distance": "",
        "gateway": "172.16.0.1",
        "iface": "",
        "proto": "ipv4",
        "table": ""
      }
    }
  }
}
```

1.42.4.3. Создание сетевого моста

1.42.4.3.1. Рассмотрим процедуру составления запроса на создание сетевого моста.

1.42.4.3.2. Создание сетевого моста можно выполнить в Zenator NS Rt с помощью команд:

```
create bridge-domain 1
commit
```

Вывод конфигурации bridge -интерфейса в Zenator NS Rt выполняется командой

```
show bridge-domain
```

В результате будет выведена следующая конфигурация bridge -интерфейса

```
Bridge-domain: 1
```

```
Description:
```

Ageing: 0

STP: 0

Vlan filtering: 0

Vlan protocol: 802.1Q

Vlan id: None

1.42.4.3.3. Данную конфигурацию можно загрузить в модуль «bridge» средствами REST API.

Для настройки модуля необходимо выполнить запрос типа «HTTP POST» к модулю «bridge», который будет иметь следующий вид

```
curl -X POST \
  -H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt' \
  -H 'Content-Type: application/json' \
  'http://192.168.5.244:8080/api/bridge' \
  -d '{
    "0": {
      "ifaces": {},
      "number": 0
    },
    "1": {
      "ageing_time": 0,
      "description": "",
      "ifaces": {},
      "number": 1,
      "stp_priority": 0,
      "stp_state": 0,
      "vlan_filtering": 0,
      "vlan_id": null,
      "vlan_protocol": "802.1Q"
    }
  }'
```

1.42.4.4. Загрузка конфигурации интерфейсов

1.42.4.4.1. Рассмотрим процедуру конфигурации интерфейса.

1.42.4.4.2. Конфигурацию интерфейса «ens4» можно выполнить в Zenator NS Rt с помощью команд:

```
interface ens4
no shutdown
ip-address 1.1.1.1/24
exit
commit
```

1.42.4.4.3. Данную конфигурацию можно загрузить в модуль «interface» средствами REST API.

Для настройки модуля необходимо выполнить запрос типа «HTTP POST» к модулю «interface», который будет иметь следующий вид

```
curl -X POST \
-H 'Authorization: Bearer wf5wtDfacH00J9Gh9NI0rMHDLDWaUt' \
-H 'Content-Type: application/json' \
'http://192.168.5.244:8080/api/interface' \
-d '{
  "ens3": {
    "admin_state": "up",
    "autoneg": "on",
    "duplex": "full",
    "ip_list": [
      "172.20.0.10/24"
    ],
    "link_state": "up",
    "mac": "00:50:14:09:00:09",
    "mtu": "1500",
    "promisc": "off",
    "speed": 1000
  },
  "ens4": {
    "admin_state": "up",
    "autoneg": "on",
    "duplex": "full",
    "ip_list": [
```

```

    "1.1.1.1/24"
  ],
  "link_state": "down",
  "mac": "00:50:14:19:00:09",
  "mtu": "1500",
  "promisc": "off",
  "speed": 1000
},
"ens5": {
  "admin_state": "down",
  "autoneg": "on",
  "duplex": "full",
  "ip_list": [],
  "link_state": "down",
  "mac": "00:50:14:29:00:09",
  "mtu": "1500",
  "promisc": "off",
  "speed": 1000
}
}'

```

В ответ на запрос будет получена следующая конфигурация «ens4»-интерфейса

```

{
  "code": 0,
  "description": "",
  "interface": {
    "ens3": {
      "admin_state": "up",
      "autoneg": "on",
      "duplex": "full",
      "ip_list": [
        "172.20.0.10/24"
      ],
      "link_state": "up",

```

```
"mac": "00:50:14:09:00:09",
"mtu": "1500",
"promisc": "off",
"speed": 1000
},
"ens4": {
  "admin_state": "up",
  "autoneg": "on",
  "duplex": "full",
  "ip_list": [
    "1.1.1.1/24"
  ],
  "link_state": "down",
  "mac": "00:50:14:19:00:09",
  "mtu": "1500",
  "promisc": "off",
  "speed": 1000
},
"ens5": {
  "admin_state": "down",
  "autoneg": "on",
  "duplex": "full",
  "ip_list": [],
  "link_state": "down",
  "mac": "00:50:14:29:00:09",
  "mtu": "1500",
  "promisc": "off",
  "speed": 1000
}
}
}
```

2. СООБЩЕНИЯ, ВЫДАВАЕМЫЕ ПРОГРАММОЙ ПОСЛЕ ПРИМЕНЕНИЯ ИЗМЕНЕНИЙ КОМАНДОЙ «COMMIT»

2.1. Сообщения, выдаваемые модулем «access_tools»:

- «Нет такого объекта»;
- «Пользователь не существует»;

2.2. Сообщения, выдаваемые модулем «acl»:

- «Правило доступа не существует: <имя правила>»;
 - «Нет правила <номер правила> в правиле доступа <имя списка>»;
 - «Назначены различные версии протокола IP для источника и приемника»;
 - «IP-адрес источника и(или) приемника не соотносится с установленным типом ACL»;
 - «Правило доступа '<имя правила>' уже определён»;
 - «Сначала установите глобальный протокол ACL»;
 - «Вы пытаетесь установить опции для протокола, отличного от глобального»;
 - «Интерфейс не обнаружен в системе»;
 - «Начальное значение MSS в диапазоне больше, чем конечное»;
 - «Значение MSS должно быть между 512 и 1500»;
 - «Начальное значение номера порта больше, чем конечное»;
 - «MODBUS поддерживается только TCP-протоколом»;
 - «Дублирует правило <имя правила>»;
 - «ACL используется в модулях: <имена модулей>»;
 - «Невозможно изменить версию протокола IP на ACL, которая уже используется модулем: <имя модуля>. Если вы все равно хотите изменить версию протокола, пожалуйста, удалите ACL из конфигурации упоминаемого модуля»;
 - «Невозможно установить опции фрагментации для протокола IPv6»;
 - «Ошибка проверки конфигурации для ACL. Отсутствуют обязательные параметры»;
 - «Ошибка проверки конфигурации ACR. Обнаружены дублирующиеся ACR»;
 - «Список доступа не существует.»;
 - «Тест функций фильтрации и логирования».
- ### 2.3. Сообщения, выдаваемые модулем «api_control»:
- «Модуль '<имя модуля>' не найден»;

– «Невозможно применить конфигурацию: уже существуют непримененные изменения»;

– «Недопустимая конфигурация».

2.4. Сообщения, выдаваемые модулем «agr»:

– «Интерфейс не существует»;

– «Невозможно установить MAC-адрес»;

– «Невозможно удалить MAC-адрес»;

– «Невозможно установить ARP-proxu»;

– «Невозможно удалить ARP-proxu»;

– «Невозможно установить Private VLAN ARP-proxu»;

– «Невозможно удалить Private VLAN ARP-proxu»;

– «Команда "ip arp show" завершилась с ошибкой»;

– «Команда "ip arp flush" завершилась с ошибкой».

2.5. Сообщения, выдаваемые модулем «auth»:

– «Не удалось настроить параметры аутентификации. Внутренняя ошибка»;

– «Ошибка запуска сеанса пользователя: <имя пользователя>»;

– «Ошибка авторизации: не удалось выполнить аутентификацию пользователя <имя пользователя>»;

– «Ошибка авторизации: невозможно получить идентификатор процесса пользователя»;

– «Ошибка авторизации: неверный идентификатор процесса пользователя»;

– «Ошибка авторизации: недопустимый интерпретатор»;

– «Ошибка авторизации: неверный тип соединения»;

– «Ошибка авторизации: недействительный пользователь»;

– «Ошибка авторизации: Сессия уже существует»;

– «Ошибка при старте сеанса пользователя: <имя пользователя>»;

– «Пользователь отсутствует в системе»;

– «Ошибка РАМ авторизации: <имя пользователя>»;

– «Ошибка авторизации: пароль для пользователя <имя пользователя> не установлен»;

– «Ошибка авторизации: пользователь <имя пользователя> заблокирован»;

– «Ошибка авторизации: срок действия пароля пользователя <имя пользователя> истек»;

- «Пароль для пользователя <имя пользователя> принят»;
- «Ошибка авторизации: неправильный пароль для пользователя <имя пользователя>»;
- «Ошибка авторизации: пользователь <имя пользователя> не найден»;
- «Ошибка завершения сессии: <номер сессии>».

2.6. Сообщения, выдаваемые модулем «bond»:

- «Интерфейс <имя интерфейса> не найден»;
- «Bond-интерфейс <имя интерфейса> не существует в системе»;
- «Bond-интерфейс должен быть выключен перед изменением настроек»;
- «Bond-интерфейс должен быть выключен перед изменением настроек. Пожалуйста, подтвердите изменения»;
- «Балансировка нагрузки недоступна для этого режима. Используйте режим lасr или хог»;
- «Интерфейс <имя интерфейса> не является подчиненным bond <имя bond-интерфейса>»;
- «Интерфейс <имя интерфейса> уже является подчиненным bond <имя bond-интерфейса>»;
- «Интерфейс <имя интерфейса> уже является подчиненным bond <имя bond-интерфейса>. Пожалуйста, подтвердите изменения»;
- «Подчиненные интерфейсы не должны быть сконфигурированы: <имя интерфейса>»;
- «Активный интерфейс <имя интерфейса> не является подчиненным bond»;
- «Невозможно создать bond-интерфейс <имя интерфейса>»;
- «Невозможно удалить bond-интерфейс <имя интерфейса>»;
- «Невозможно установить режим bond-интерфейса <имя интерфейса>»;
- «Невозможно установить балансировку нагрузки bond-интерфейса <имя интерфейса>»;
- «Невозможно добавить интерфейс <имя интерфейса> в bond-интерфейс <имя интерфейса>»;
- «Невозможно удалить интерфейс <имя интерфейса> из bond-интерфейса <имя интерфейса>»;
- «Интерфейс <имя интерфейса> уже используется в сетевом мосте <номер bridge-интерфейса>»;

– «Невозможно удалить bond <имя интерфейса>. Интерфейс bond <имя интерфейса> используется в разделах конфигурации:».

2.7. Сообщения, выдаваемые модулем «bridge»:

– «Сетевой мост уже существует – <номер bridge-интерфейса>;»;
– «Сетевой мост не существует – <номер bridge-интерфейса>;»;
– «Интерфейс <имя интерфейса> уже используется в сетевом мосте <номер bridge-интерфейса>;»;

– «Интерфейс <имя интерфейса> используется в сетевом мосте <номер bridge-интерфейса>. Пожалуйста подтвердите изменения»;

– «Сетевой мост с идентификатором <номер bridge-интерфейса> не существует»;

– «Интерфейс <имя интерфейса> не используется в сетевом мосте <номер bridge-интерфейса>;»;

– «Не удалось создать сетевой мост <номер bridge-интерфейса>;»;

– «Не удалось удалить сетевой мост <номер bridge-интерфейса>;»;

– «Не удалось добавить интерфейс к сетевому мосту <номер bridge-интерфейса>;»;

– Не удалось удалить интерфейс из сетевого моста <номер bridge-интерфейса>;»;

– «Номер сетевого моста не может быть равен нулю, если не установлен режим»;

– «Интерфейс <имя интерфейса> не является сетевым мостом»;

– «Интерфейс <имя интерфейса> уже является подчиненным bond {}»;

– «Невозможно удалить сетевой мост <номер bridge-интерфейса>. Интерфейс <имя интерфейса> используется в разделах конфигурации:»;

– «Невозможно добавить интерфейс <имя интерфейса> в сетевой мост <номер bridge-интерфейса>;»;

– «Интерфейс не должен иметь назначенного IP-адреса».

2.8. Сообщения, выдаваемые модулем «config»:

– «Неверный ключ <ключ>;»;

– «Подготовка VPP...»;

– «Сервис core запущен в режиме DEBUG»;

– «Загрузка core...»;

- «выполнено»;
 - «Регистрация модулей в системе:»;
 - «Модули успешно зарегистрированы»;
 - «Ошибка: Сессия не существует (закончена, некорректна...)»;
 - «Эта команда игнорируется в области видимости подменю»;
 - «Доступ запрещен. Профиль не зарегистрирован в системе»;
 - «Доступ запрещен. Нельзя запретить эту команду для группы admsec»;
 - «Доступ запрещен. У вас нет прав на выполнение манипуляций с профилем»;
 - «Доступ запрещен. Вы не являетесь владельцем профиля»;
 - «Доступ запрещен. Вы не можете выполнять операцию чтения на этот профиль»;
 - «Доступ запрещен. У вас нет прав на этот лог-файл»;
 - «Доступ запрещен. У вас нет прав на эту команду»;
 - «Ошибка проверки конфигурации.»;
 - «Взаимоисключающие параметры»;
 - «Отсутствуют обязательные параметры»;
 - «Конфигурация уже существует: <имя конфигурации>»;
 - «Конфигурация не существует: <имя конфигурации>».
- 2.9. Сообщения, выдаваемые модулем «core_log»:
- «Начальная дата должна быть меньше даты окончания»;
 - «Локальное ведение журнала отключено для журнала '<имя журнала>»;
 - «Логирование уже включено»;
 - «Указан неверный уровень журналирования: <значение уровня>»;
 - «Модуль '<имя модуля>' не зарегистрирован»;
 - «Невозможно включить ведение журнала монитора на терминале»;
 - «Ошибка при попытке получить уровень журналирования системы»;
 - «Неверная конфигурация системы журналирования»;
 - «Невозможно открыть файл журнала»;
 - «Нет системных журналов с таким именем»;
 - «Флэш-память не установлена»;
 - «Нет обработчика или неверная категория журнала: <имя журнала>»;
 - «Создан лог-файл '<имя журнала>»;

– «Лог-файл '<имя журнала>' не существует и не может быть создан:
<системное сообщение об ошибке>»;

– «Ошибка при фильтрации данных лога: <имя журнала>».

2.10. Сообщения, выдаваемые модулем «dhcp_relay»:

– «DHCP-сервер уже добавлен»;

– «DHCP-источник уже добавлен»;

– «Невозможно добавить DHCP-relay <IP-адрес>»;

– «Невозможно удалить DHCP-relay <IP-адрес>»;

– «Невозможно добавить опцию DHCP-relay 82»;

– «Невозможно удалить опцию DHCP-relay 82»;

– «Параметры DHCP-сервера или источника не заданы»;

– «Ошибка проверки конфигурации DHCP-relay. Ошибка параметров: <перечень параметров>»;

– «Невозможно добавить DHCP-relay, не указан параметр: <имя параметра>»;

– «Интерфейс <имя интерфейса> не найден».

2.11. Сообщения, выдаваемые модулем «dhcp_server»:

– «DHCP-сервер уже существует:»;

– «DHCP-сервер не обнаружен в системе:»;

– «Пул DHCP-адресов не обнаружен в системе:»;

– «Указанный интерфейс не существует в системе»;

– «Интерфейс должен быть включен и сконфигурирован с использованием IP-адреса»;

– «Интерфейс уже используется в качестве интерфейса DHCP-сервера»;

– «Должен быть указан хотя бы один интерфейс для DHCP-сервера»;

– «Должен быть указан пул IP-адресов»;

– «DHCP-сервер уже запущен»;

– «DHCP-сервер уже выключен»;

– «Слишком большой диапазон адресов»;

– «Указанная сеть недоступна»;

– «Для выбранной сети не настроен ни один пул»;

– «IP-адрес должен принадлежать сети <IP-адрес>»;

– «Указанный адрес хоста уже существует в системе»;

– «Указанный адрес хоста не существует в системе»;

- «Начальный IP-адрес должен быть меньше конечного IP-адреса»;
- «Такой IP-адрес маршрутизатора уже существует в системе»;
- «Превышено предельное количество IP-адресов для маршрутизатора»;
- «Не указан интерфейс для DHCP-сервера»;
- «Указанный IP-адрес недоступен»;
- «Указанный IP-адрес не существует в системе»;
- «Указанный IP-адрес принт-сервера уже существует в системе»;
- «Превышено максимальное количество IP-адресов для списка принт-серверов»;
- «Указанный IP-адрес NTP-сервера не существует в системе»;
- «Превышено максимальное количество IP-адресов для списка NTP-серверов»;
- «Указанный IP-адрес NTP-сервера не существует в системе»;
- «Неверная версия протокола IP»;
- «Установите адрес сети»;
- «Не найден PID файл процесса»;
- «Пул адресов <диапазон IP-адресов> используется и не может быть удален»;
- «Ошибка проверки конфигурации DHCP-сервера. Отсутствуют обязательные параметры: <перечень параметров>».

2.12. Сообщения, выдаваемые модулем «dns»:

- «Не удалось применить параметры DNS-клиента. Внутренняя ошибка»;
- «Не удалось применить настройки DNS-прокси сервера. Внутренняя ошибка»;
- «Пожалуйста, сначала укажите серверы доменных имен»;
- «Сервер имен не существует в системе: <IP-адрес сервера>»;
- «Имя домена не существует в системе»;
- «Перенаправление DNS не включено для интерфейса <имя интерфейса>»;
- «Не удалось проверить статус DNS-сервера».

2.13. Сообщения, выдаваемые модулем «executor»:

- «Не удалось проверить статус сервиса. Внутренняя ошибка».

2.14. Сообщения, выдаваемые модулем «gre»:

- «Интерфейс уже существует в системе: gre <номер gre-интерфейса>»;
- «Интерфейс не существует в системе: gre <номер gre-интерфейса>»;
- «Невозможно создать туннельный интерфейс: gre <номер gre-интерфейса>»;

- «Невозможно удалить туннельный интерфейс: gre <номер gre-интерфейса>;»;
- «Ошибка проверки конфигурации GRE. Отсутствуют обязательные параметры: <перечень параметров>;»;
- «IP-адреса отправителя и получателя не могут совпадать»;
- «Невозможно удалить gre <номер gre-интерфейса>. Интерфейс gre <номер gre-интерфейса> используется в разделах конфигурации:».

2.15. Сообщения, выдаваемые модулем «help»:

- «Модуль <имя модуля> не существует».

2.16. Сообщения, выдаваемые модулем «interface»:

- «Неизвестный тип интерфейса <имя интерфейса>;»;
- «IP-адрес <IP-адрес> перекрывается с <IP-адрес> на интерфейсе <имя интерфейса>;»;
- «IP-адрес <IP-адрес> перекрывается с <IP-адрес>. Пожалуйста, подтвердите изменения»;
- «IP-адрес <IP-адрес> не установлен на интерфейсе <имя интерфейса>;»;
- «Включен режим автосогласования скорости и дуплекса»;
- «Интерфейс не поддерживается данной командой: <имя команды>;»;
- «Интерфейс управляется модулем: <имя модуля>;»;
- «Интерфейс не существует в системе: <имя интерфейса>;»;
- «Неоднозначное имя интерфейса: <имя интерфейса>;»;
- «Не удалось получить индекс для интерфейса <имя интерфейса>;»;
- «Не удалось получить имя интерфейса с индексом <индекс интерфейса>;»;
- «Невозможно получить статус интерфейса <имя интерфейса>;»;
- «Невозможно установить MTU на интерфейсе <имя интерфейса>;»;
- «Невозможно установить MAC-адрес на интерфейсе <имя интерфейса>;»;
- «Невозможно установить IP-адрес на интерфейсе <имя интерфейса>;»;
- «Невозможно удалить IP-адрес на интерфейсе <имя интерфейса>;»;
- «Невозможно включить DHCP-клиент на интерфейсе <имя интерфейса>;»;
- «Невозможно отключить DHCP-клиент на интерфейсе <имя интерфейса>;»;
- «Невозможно установить скорость и дуплекс на интерфейсе <имя интерфейса>;»;
- «Не удастся включить режим индикации на интерфейсе <имя интерфейса>;»;

- «Не удается остановить режим индикации на интерфейсе <имя интерфейса>»;
 - «Режим DHCP уже включен на интерфейсе <имя интерфейса>»;
 - «Выбранная комбинация скорости и дуплекса не поддерживается»;
 - «Режим скорости {} не поддерживается на интерфейсе <имя интерфейса>»;
 - «Режим скорости не поддерживается на интерфейсе <имя интерфейса>»;
 - «Для данного параметра не существует значения по-умолчанию»;
 - «Режим дуплекса не поддерживается на интерфейсе <имя интерфейса>»;
 - «Режим автосогласования не поддерживается на интерфейсе <имя интерфейса>»;
 - «Неразборчивый режим не поддерживается на интерфейсе <имя интерфейса>»;
 - «Установка MTU невозможна на интерфейсе <имя интерфейса>»;
 - «Установка MAC-адреса невозможна на интерфейсе <имя интерфейса>»;
 - «Интерфейс <имя интерфейса> является подчиненным bridge <имя интерфейса>»;
 - «Невозможно включить сабинтерфейс <имя интерфейса> потому что основной интерфейс <имя интерфейса> выключен».
- 2.17. Сообщения, выдаваемые модулем «interface_tools»:
- «Не удалось получить номер слота для интерфейса <имя интерфейса>»;
 - «Не удалось получить имя интерфейса с индексом <индекс интерфейса>»;
 - «Невозможно назначить IP-адрес на интерфейсе с индексом <индекс интерфейса>»;
 - «Невозможно удалить IP-адрес на указанном интерфейсе»;
 - «Невозможно создать подинтерфейс с индексом <индекс подинтерфейса>»;
 - «Невозможно удалить подинтерфейс с индексом <индекс подинтерфейса>»;
 - «Невозможно создать bond-интерфейс»;
 - «Невозможно удалить bond-интерфейс с индексом <номер bond-интерфейса>»;
 - «Невозможно добавить интерфейс с индексом <индекс интерфейса> в конфигурацию bond»;
 - «Невозможно удалить интерфейс с индексом <индекс интерфейса> из конфигурации bond»;

- «Невозможно создать loopback-интерфейс»;
- «Невозможно удалить loopback-интерфейс с индексом <номер loopback-интерфейса>»;
- «Невозможно создать IPIP-интерфейс: <номер ipip-интерфейса>»;
- «Невозможно удалить IPIP-интерфейс с индексом <номер ipip-интерфейса>»;
- «Невозможно создать GRE-интерфейс: <номер gre-интерфейса>»;
- «Невозможно удалить GRE-интерфейс: <номер gre-интерфейса>»;
- «Не удалось сбросить IP-конфигурацию на интерфейсе»;
- «Невозможно установить состояние канала на интерфейсе»;
- «Невозможно установить MTU на интерфейсе»;
- «Невозможно установить MTU для IP-пакета на интерфейсе»;
- «Невозможно установить MAC-адрес на интерфейсе»;
- «Невозможно добавить диапазон адресов '<IP-адрес1>-<IP-адрес2>' в конфигурацию ARP-прокси»;
- «Невозможно удалить диапазон адресов '<IP-адрес1>-<IP-адрес2>' из конфигурации ARP-прокси»;
- «Не удалось включить фильтрацию трафика на системном интерфейсе с индексом <номер интерфейса>»;
- «Не удалось отключить фильтрацию трафика на системном интерфейсе с индексом <номер интерфейса>»;
- «Не удалось включить ARP-прокси на интерфейсе с индексом <номер интерфейса>»;
- «Не удалось отключить ARP-прокси на интерфейсе с индексом <номер интерфейса>»;
- «Не удалось получить системное имя интерфейса <имя интерфейса>».

2.18. Сообщения, выдаваемые модулем «ip_filter»:

- «Схема фильтрации <имя схемы> не обнаружена»;
- «Правило доступа не обнаружено в системе.»;
- «Правило доступа <имя списка> уже используется в цепочке <направление>»;
- «Невозможно установить REJECT сообщение IPv6 для IPv4 ACL»;
- «Невозможно установить REJECT сообщение IPv4 для IPv6 ACL»;
- «Сообщение TCP RESET может быть установлено только для ACL протокола TCP»;

– «IP-адреса источника и получателя ACL имеют различные версии протокола IP»;

– «ACL не обнаружена в конфигурации фильтра: <имя фильтра>»;

– «Ошибка проверки конфигурации Filter. Отсутствуют обязательные параметры: <перечень параметров>».

2.19. Сообщения, выдаваемые модулем «ірір»:

– «Интерфейс уже существует в системе: ірір<номер ірір-интерфейса>»;

– «Интерфейс не существует в системе: ірір<номер ірір-интерфейса>»;

– «Невозможно создать туннельный интерфейс: ірір<номер ірір-интерфейса>»;

– «Невозможно удалить туннельный интерфейс: ірір<номер ірір-интерфейса>»;

– «Ошибка проверки конфигурации IPIP. Отсутствуют обязательные параметры: <перечень параметров>»;

– «Невозможно удалить ірір <номер ірір-интерфейса>. Интерфейс ірір<номер ірір-интерфейса> используется в разделах конфигурации:»;

– «IP-адреса отправителя и получателя не могут совпадать».

2.20. Сообщения, выдаваемые модулем «ірсек»:

– «IPSec уже назначен для: <IP-адрес>»;

– «IPSec-интерфейс не существует в системе:»;

– «Невозможно добавить IPSec-туннель: <IP-адрес>»;

– «Невозможно удалить IPSec-туннель: <IP-адрес>»;

– «IP-адреса отправителя и получателя не должны совпадать»;

– «Ошибка конфигурации модуля. Следующие опции не заданы:»;

– «Размер крипто-ключа для выбранного алгоритма должен быть <количество байт> байт»;

– «CA-сертификат не обнаружен: <имя сертификата>»;

– «Необходимо задать ключ pre-shared-key»;

– «Локальный адрес сети уже назначен

– «Удаленный адрес сети уже назначен»;

– «Локальный адрес уже назначен»;

– «Удаленный адрес уже назначен»;

– «Адрес <IP-адрес> не найден в конфигурации».

2.21. Сообщения, выдаваемые модулем «ірсет»:

– «Нельзя изменить тип созданного списка с <тип списка> на <тип списка>»;

– «Запись не найдена: <номер записи>»;

– «Список доступа не существует: <имя списка>».

2.22. Сообщения, выдаваемые модулем «l2tp_client»:

– «Интерфейс L2TP-клиента уже существует в системе:»;

– «Интерфейс L2TP-клиента не существует в системе:»;

– «Описание не установлено в текущей конфигурации»;

– «Интервал lsr-echo запросов не задан для текущей конфигурации»;

– «Допустимое количество lsr-echo запросов не задано для текущей конфигурации»;

– «Интерфейс уже установлен в режим ожидания»;

– «Удалите параметр максимального количества попыток установки соединения (maxfail) для установки режима ожидания»;

– «На интерфейсе выключен режим ожидания для текущей конфигурации»;

– «Тайм-аут соединения не установлен для текущей конфигурации»;

– «Включите режим переподключения»;

– «Опция получения адресов DNS-серверов уже установлена для текущей конфигурации»;

– «Опция получения адресов DNS-серверов уже отключена для текущей конфигурации»;

– «Опция получения default-маршрута уже установлена для текущей конфигурации»;

– «Удалите параметр режима ожидания (persistent) для задания максимального количества попыток установки соединения»;

– «Невозможно удалить L2TP-клиент <имя клиента>. Интерфейс <имя интерфейса> используется в разделах конфигурации:»;

– «Ошибка проверки конфигурации L2TP-клиента. Отсутствуют обязательные параметры:<перечень параметров>».

2.23. Сообщения, выдаваемые модулем «l2tp_server»:

– «Интерфейс L2TP-сервера уже существует в системе:»;

– «Интерфейс L2TP-сервера не существует в системе:»;

– «Удалите Radius-аутентификацию, чтобы добавить локальные профили аутентификации»;

– «Логин профиля клиента уже добавлен:»;

- «Логин профиля клиента не обнаружен:»;
- «Удалите локальные профили аутентификации, чтобы добавить Radius-аутентификацию»;
- «Radius-сервер не существует в системе:»;
- «Невозможно удалить L2TP-сервер <имя сервера>. Интерфейс <имя интерфейса> используется в разделах конфигурации:»;
- «Ошибка проверки конфигурации L2TP-сервера. Отсутствуют обязательные параметры: <перечень параметров>».

2.24. Сообщения, выдаваемые модулем «ldap»:

- «Адрес уже добавлен в список хостов: <список хостов>»;
- «Адрес не найден в списке хостов: <список хостов>»;
- «Директория сертификатов не обнаружена: <имя директории>»;
- «Сертификаты не обнаружены»;
- «Flash-устройство не подключено»;
- «TAR файл с сертификатами не найден на flash-устройстве: <flash-устройство>»;
- «Отсутствует соединение с LDAP-сервером. Проверьте конфигурацию клиента и соединение с сервером»;
- «Ошибка проверки конфигурации LDAP. Отсутствуют обязательные параметры <перечень параметров>».

2.25. Сообщения, выдаваемые модулем «lldp»:

- «Интерфейс не обнаружен»;
- «Ошибка проверки конфигурации LLDP. Отсутствуют обязательные параметры: <перечень параметров>».

2.26. Сообщение, выдаваемое модулем «logfile»:

- «Не указан параметр 'file_name'».

2.27. Сообщения, выдаваемые модулем «loopback»:

- «Интерфейс <составное имя интерфейса> уже существует»;
- «Интерфейс loop<номер loopback-интерфейса> не найден»;
- «Невозможно создать loopback-интерфейс»;
- «Невозможно удалить loopback-интерфейс <номер loopback-интерфейса>»;
- «Добавлен(ы) интерфейс(ы) loopback: <перечень интерфейсов>»;
- «Удален(ы) интерфейс(ы) loopback: <перечень интерфейсов>»;

– «Невозможно удалить loopback <имя интерфейса>. Интерфейс loop<номер loopback-интерфейса> используется в разделах конфигурации:».

2.28. Сообщения, выдаваемые модулем «mark»:

– «Данный тип маркировки не определен для правила доступа <имя правила> цепочки <имя цепочки>»;

– «Правило доступа не обнаружено <имя правила>»;

– «Маркировку mss можно назначить только для протокола tcp»;

– «Маркировку mss можно назначить только для пакетов SYN»;

– «Ошибка проверки конфигурации для Marked. Отсутствуют обязательные параметры: <перечень параметров>».

2.29. Сообщения, выдаваемые модулем «mirroring»:

– «{} зеркалируется в {}»;

– «{} это зеркало»;

– «Транслирующий интерфейс <имя интерфейса> установлен как зеркало»;

– «Интерфейс <имя интерфейса> не зеркалируется».

2.30. Сообщения, выдаваемые модулем «module_manager»:

– «Непосредственное изменение модуля запрещено»;

– «Модуль <имя модуля> не зарегистрирован».

2.31. Сообщения, выдаваемые модулем «nat»:

– «Версия IP-протокола для указанных адресов не одинакова»;

– «Интерфейс <имя интерфейса> не найден»;

– «Интерфейс должен быть включен и сконфигурирован с использованием IP-адреса»;

– «Установите опции внешней сети»;

– «Установите протокол»;

– «Для установки портов требуется протокол TCP или UDP»;

– «Ошибка проверки конфигурации для NAT. Отсутствуют обязательные параметры: <перечень параметров>».

2.32. Сообщения, выдаваемые модулем «ntp»:

– «NTP-клиент уже активирован»;

– «NTP-клиент уже деактивирован»;

– «Сервер уже добавлен в конфигурацию: <IP-адрес сервера>»;

– «Сервер не обнаружен в конфигурации: <IP-адрес сервера>»;

- «Интерфейс не существует в системе: <имя интерфейса>»;
- «Сеть интерфейса уже разрешена: <IP-адрес сети>»;
- «Сеть интерфейса не разрешена: <IP-адрес сети>»;
- «Следующие опции не заданы: <перечень опций>.

2.33. Сообщения, выдаваемые модулем «ospf»:

- «Пожалуйста, удалите все существующие статические маршруты»;
- «OSPF уже активирован»;
- «OSPF уже деактивирован»;
- «Для перезапуска OSPF требуется предварительная активация»;
- «Сначала запустите OSPF»;
- «Выполните команду commit для перезапуска OSPF»;
- «Интерфейс уже в списке пассивных интерфейсов: <имя интерфейса>»;
- «Интерфейс не обнаружен в списке пассивных интерфейсов: <имя интерфейса>»;
- «Эталонная пропускная способность автоматической стоимости не установлена»;
- «Таймер приема LSA не установлен»;
- «Таймер ускорения LSA не установлен»;
- «Сосед не найден в конфигурации: <IP-адрес соседа>»;
- «Зона 0 может иметь только тип 'normal'»;
- «Сеть <IP-адрес сети> уже добавлена в зону <номер зоны>»;
- «Сеть <IP-адрес сети> уже добавлена в зону <номер зоны>. Пожалуйста, подтвердите изменения»;
- «Зона не сконфигурирована: <номер зоны>»;
- «Сеть <IP-адрес сети> не включена в список сетей зоны <номер зоны>»;
- «Диапазон <диапазон сетей> отсутствует в зоне <номер зоны>»;
- «BFD уже активирован на интерфейсе: <имя интерфейса>»;
- «Режим игнорирования MTU уже активирован на интерфейсе: <имя интерфейса>»;
- «Аутентификация уже активирована на интерфейсе: <имя интерфейса>»;
- «Установите пароль»;
- «BFD уже деактивирован на интерфейсе: <имя интерфейса>»;
- «Аутентификация уже деактивирована на интерфейсе: <имя интерфейса>»;

- «Cost не установлен на интерфейсе: <имя интерфейса>»;
- «Режим игнорирования MTU деактивирован на интерфейсе: <имя интерфейса>».

2.34. Сообщения, выдаваемые модулем «rарі»:

- «Команда не зарегистрирована в VPP API: <имя команды>».

2.35. Сообщения, выдаваемые модулем «rbrg»:

- «Невозможно применить правило - <имя правила>»;
- «Невозможно добавить правило - <имя правила>»;
- «Невозможно удалить правило - <имя правила>»;
- «Правило уже существует - <имя правила>»;
- «Интерфейс '<имя интерфейса>' не существует»;
- «Протокол '<имя протокола>' не существует»;
- «IP-адреса для параметров 'from, to' должны принадлежать одной версии»;
- «Ошибка проверки конфигурации PBR. Обязательные параметры:<перечень параметров>»;
- «Ошибка проверки конфигурации PBR. Взаимоисключающие параметры:<перечень параметров>».

2.36. Сообщения, выдаваемые модулем «rim»:

- «Интерфейс должен быть включен и сконфигурирован с использованием IP-адреса»;
- «Интерфейс <имя интерфейса> уже используется в текущей конфигурации»;
- «Протокол RIM не сконфигурирован для интерфейса: <имя интерфейса>»;
- «Групповой префикс <адрес группы с маской> уже существует в системе»;
- «RP-адрес <RP- адрес> не найден в текущей конфигурации»;
- «Интерфейс с именем <имя интерфейса> не существует».

2.37. Сообщения, выдаваемые модулем «radius»:

- «Невозможно применить конфигурацию Radius»;
- «Указанный адрес хоста не существует в системе: <IP-адрес хоста>».

2.38. Сообщения, выдаваемые модулем «rip»:

- «Протокол RIP должен быть включен»;
- «Выполните команду commit для того, чтобы перезагрузить RIP»;
- «Удалите любые статические маршруты, существующие в системе»;
- «RIP уже активирован»;

- «RIP уже деактивирован»;
- «RIP должен быть активен для того, чтобы выполнить его перезагрузку»;
- «IP-адрес уже добавлен»;
- «Интерфейс уже добавлен»;
- «IP-адрес <IP-адрес> не найден в конфигурации RIP»;
- «Сетевой интерфейс <имя интерфейса> не найден в конфигурации RIP»;
- «Адрес соседа <IP-адрес соседа> уже существует в конфигурации RIP»;
- «Адрес соседа <IP-адрес соседа> не найден в конфигурации RIP»;
- «Пассивный интерфейс уже добавлен»;
- «Пассивный интерфейс <имя интерфейса> не найден в конфигурации RIP»;
- «У интерфейса <имя интерфейса> отсутствует пароль»;
- «Список '<имя списка>' не установлен на входящее направление»;
- «Список '<имя списка>' не установлен на исходящее направление»;
- «Не обнаружена конфигурация RIP».

2.39. Сообщения, выдаваемые модулем «ripng»:

- «Удалите любые статические маршруты, существующие в системе»;
- «RIPNG уже активирован»;
- «RIPNG уже деактивирован»;
- «RIPNG должен быть активен для того, чтобы выполнить его перезагрузку»;
- «IP-адрес уже добавлен»;
- «Интерфейс уже добавлен»;
- «IP-адрес <IP-адрес> не найден в конфигурации RIP»;
- «Сетевой интерфейс <имя интерфейса> не найден в конфигурации RIPNG»;
- «Адрес соседа <IP-адрес соседа> уже существует в конфигурации RIPNG»;
- «Адрес соседа <IP-адрес соседа> не найден в конфигурации RIPNG»;
- «Пассивный интерфейс уже добавлен»;
- «Пассивный интерфейс <имя интерфейса> не найден в конфигурации RIPNG»;
- «У интерфейса <имя интерфейса> отсутствует пароль»;
- «Список '<имя списка>' не установлен на входящее направление»;
- «Список '<имя списка>' не установлен на исходящее направление»;
- «Не обнаружена конфигурация RIPNG».

2.40. Сообщения, выдаваемые модулем «route_maps»:

- «Неправильный формат данных API или веб-интерфейса»;
- «Длина маски подсети (<длина маски>) не может превышать заданную минимальную длину префикса (<длина префикса>)»;
- «Минимальная длина префикса (<длина префикса>) не может превышать заданную максимальную длину префикса (<длина префикса>)»;
- «Длина маски подсети (<длина маски>) не может превышать заданную максимальную длину префикса (<длина префикса>)»;
- «Сеть <IP-адрес сети> уже добавлена в префикс-список <имя списка> под номером <номер записи>»;
- «Префикс-список '<имя списка>' не сконфигурирован»;
- «Идентификатор не существует: <permit/deny> <IP-адрес сети>»;
- «Невозможно сконфигурировать маршрут поверх нового протокола»;
- «Префикс-список '<имя списка>' не существует»;
- «Вес может быть установлен только с активным протоколом BGP»;
- «Локальные приоритеты могут быть выбраны только с активным протоколом BGP»;
- «Префикс-список '<имя списка>' отсутствует в записи <номер записи> маршрута <имя карты маршрутов>».

2.41. Сообщения, выдаваемые модулем «security_access»:

- «Команда отсутствует в агенте управления: <имя команды>»;
- «Невозможно изменить групповую политику для команды: <имя команды>»;
- «Имя профиля "null" зарезервировано системой»;
- «Профиль не найден в системе»;
- «Лог не найден в системе»;
- «Группа не существует в системе или не имеет доступ к командам: <имя группы>»;
- «Профиль уже существует в системе: <имя профиля>»;
- «Невозможно удалить профиль: <имя профиля>. Профиль используется системой»;
- «Flash-устройство или UUID не найдено в системе»;
- «Flash-устройство уже зарегистрировано в системе»;

– «Flash-устройство с таким номером отсутствует в системе: <номер устройства>»;

– «Пользователь не существует в системе или не имеет доступа к командам: <имя пользователя>»;

– «Изменение прав пользователей для данной команды запрещено системой».

2.42. Сообщения, выдаваемые модулем «session_manager»:

– «Достигнут лимит сессий»;

– «Достигнуто максимальное число сессий»;

– «Системная ошибка времени»;

– «Некорректный номер сессии: <номер сессии>»;

– «Ошибка завершения сеанса пользователя»;

– «Ошибка завершения сессии: <номер сессии>»;

– «Завершена сессия для пользователя '<имя пользователя>' с адресом <ip-адрес>».

2.43. Сообщения, выдаваемые модулем «snmp»:

– «Невозможно применить конфигурацию SNMP»;

– «Пароль не существует: <пароль>»;

– «SNMP-хост не существует в системе: {}»;

– «Невозможно получить статус SNMP-сервера»;

– «Для SNMP не заданы параметры хостов».

2.44. Сообщения, выдаваемые модулем «ssh»:

– «Порт используется системой»;

– «Невозможно получить статус SSH-сервера»;

– «SSH-лист доступа '<маска разрешенных адресов>' уже существует в системе»;

– «SSH-лист доступа '<маска разрешенных адресов>' не существует в системе».

2.45. Сообщения, выдаваемые модулем «static_routes»:

– «IP-адрес получателя задан некорректно»;

– «Одиночный маршрут уже существует в системе: <IP-адрес назначения>»;

– «Множественный маршрут уже существует в системе: <IP-адрес назначения>»;

– «Балансный маршрут уже существует в системе: <IP-адрес назначения>»;

- «Неправильно задан IP-адрес шлюза: <IP-адрес шлюза>»;
- «Маршрут уже существует в системе: <IP-адрес назначения>»;
- «Шлюзы должны различаться»;
- «Маршрут не существует в системе: <IP-адрес назначения>»;
- «Балансный маршрут не существует в системе: <IP-адрес назначения>»;
- «Интерфейс <имя интерфейса> отсутствует в интерфейсах '<тип интерфейса>»;
- «Ошибка при выполнении команды: '<имя команды>»;
- «Невозможно добавить маршрут: <IP-адрес назначения>»;
- «Типы адресов destination и gateway должны быть одинаковы»;
- «Таблица <имя таблицы> уже существует»;
- «Таблица <имя таблицы> не может быть модифицирована»;
- «Таблица <имя таблицы> не существует в системе»;
- «Невозможно создать таблицу <имя таблицы>»;
- «Невозможно удалить таблицу <имя таблицы>»;
- «Необходимо установить IP-адрес шлюза или интерфейс источника»;
- «Необходимо установить IP-адрес шлюза и/или административную дистанцию».

2.46. Сообщения, выдаваемые модулем «sys_profile»:

- «Использование модуля заблокировано системой: <имя модуля>»;
- «Имя профиля "null" зарезервировано системой»;
- «Невозможно сохранить профиль, пока не применены или отменены изменения в конфигурации»;
- «Ошибка загрузки конфигурации»;
- «Примените конфигурацию»;
- «Достигнута последняя возможная конфигурация»;
- «Профиль не зарегистрирован в системе или не может быть загружен: <имя модуля>»;
- «Отсутствует конфигурация профиля: <имя профиля>»;
- «Профиль не существует в системе: <имя профиля>»;
- «Нет примонтированных flash-устройств»;
- «Конфигурация отсутствует на flash-устройстве»;

- «Профиль не зарегистрирован в системе: <имя профиля>»;
- «Конфигурация отсутствует: <имя профиля>»;
- «Конфигурация успешно применена для модулей:»;
- «Конфигурация не применена для модулей:»;
- «Выполнение команды commit успешно завершено»;
- «Не найдена конфигурация, требующая применения команды commit»;
- «Модуль <имя модуля> не может быть проверен»;
- «Ошибка проверки конфигурации: <имя профиля>»;
- «Проверка конфигурации: ОК»;
- «Модуль не существует в системе: <имя модуля>».

2.47. Сообщения, выдаваемые модулем «system»:

- «БД контрольной суммы конфигурационных файлов не инициализирована»;
- «Пользователь уже существует в системе: '<имя пользователя>';»;
- «Невозможно удалить пользователя: '<имя пользователя>';»;
- «Пользователь не существует в системе: '<имя пользователя>';»;
- «Запрещено блокировать активного пользователя»;
- «Пользователь уже заблокирован»;
- «Пользователь не заблокирован»;
- «Интерфейс не существует в системе: <имя интерфейса>»;
- «Интерфейс выключен и не имеет назначенного IP-адреса»;
- «Не найдено имя хоста: '<имя хоста>';»;
- «Невозможно создать пользователя поддержки. Внутренняя ошибка '<описание системной ошибки>';»;
- «Невозможно удалить пользователя поддержки. Внутренняя ошибка '<описание системной ошибки>';»;
- «БД хэш-сумм системных файлов не зарегистрирована»;
- «БД хэш-сумм конфигурационных файлов не зарегистрирована»;
- «Нет примонтированных flash-устройств»;
- «Модуль не найден в системе: '<имя модуля>';»;
- «Модуль уже загружен: '<имя модуля>';»;
- «Ошибка загрузки модуля: '<имя модуля>';»;
- «Операция выгрузки запрещена для модуля: '<имя модуля>';»;

- «Модуль не зарегистрирован в системе: '<имя модуля>'»;
- «Процесса с таким PID нет в системе»;
- «Пользователь '<имя пользователя>' уже авторизован в системе. Чтобы его удалить, необходимо выполнить деавторизацию пользователя»;
- «Минимальная длина пароля: <количество символов>»;
- «Пароль должен содержать прописные и строчные буквенные символы»;
- «Пароль должен содержать прописные и строчные буквенные символы, цифры»;
- «Пароль должен содержать прописные и строчные буквенные символы, цифры, специальные символы»;
- «Регион не найден в системе: <значение>»;
- «Временная зона не найдена в системе: <значение>»;
- «Значение года должно быть в интервале (0000, 9999). Текущее значение: <значение>»;
- «Значение месяца должно быть в интервале (01, 12). Текущее значение: <значение>»;
- «Значение дня для февраля високосного года должно быть в интервале (01, 29). Текущее значение: <значение>»;
- «Значение дня для февраля не високосного года должно быть в интервале (01, 28). Текущее значение: <значение>»;
- «Значение дня для выбранного месяца должно быть в интервале (01, 30). Текущее значение: <значение>»;
- «Значение дня для выбранного месяца должно быть в интервале (01, 31). Текущее значение: <значение>»;
- «Значение часа должно быть в интервале (00, 24). Текущее значение: <значение>»;
- «Значение минут должно быть в интервале (00, 59). Текущее значение: <значение>»;
- «Значение секунд должно быть в интервале (00, 59). Текущее значение: <значение>»;
- «Некорректная дата/время: <значение>»;
- «Файл сертификата не обнаружен: <имя файла>»;
- «Директория сертификатов не обнаружена»;

- «Флеш-устройство не подключено»;
- «IP-адрес не обнаружен в системе»;
- «Ошибка выгрузки неизменяемых системных файлов на flash-носитель»;
- «Проверка памяти завершена успешно»;
- «Проверка центрального процессора завершена успешно»;
- «Проверка диска завершена успешно»;
- «Проверка памяти завершилась с ошибкой»;
- «Проверка центрального процессора завершилась с ошибкой»;
- «Проверка диска завершилась с ошибкой».

2.48. Сообщения, выдаваемые модулем «telnet»:

- «Порт используется системой».

2.49. Сообщения, выдаваемые модулем «update»:

- «Сертификат или ключ не найден: <сертификат или ключ>»

2.50. Сообщения, выдаваемые модулем «vpn_client»:

- «VPN-клиент не существует в системе: <номер клиента>»;
- «VPN-клиент уже включен»;
- «VPN-клиент уже выключен»;
- «VPN-клиент не сконфигурирован»;
- «Невозможно добавить устройство при назначенной опции ifconfig»;
- «Невозможно установить IP-адрес при установленном TUN-устройстве»;
- «IP-адрес сервера уже добавлен в конфигурацию»;
- «IP-адрес отсутствует в конфигурации»;
- «Используется другая версия IP-протокола»;
- «Файл не обнаружен: <имя файла>»;
- «Невозможно удалить VPN-клиента <имя интерфейса>. Интерфейс <имя интерфейса> используется в разделах конфигурации:»;
- «Ошибка проверки конфигурации VPN-клиента. Отсутствуют обязательные параметры: <перечень параметров>».

2.51. Сообщения, выдаваемые модулем «vpn_server»:

- «VPN-сервер уже включён»;
- «VPN-сервер выключен»;
- «VPN-сервер не сконфигурирован»;
- «Невозможно добавить устройство при назначенной опции ifconfig»;

- «Невозможно установить IP-адрес при установленном TUN-устройстве»;
 - «Длина маски должна быть меньше {}»;
 - «IP-адрес маршрута уже добавлен в конфигурацию»;
 - «IP-адрес маршрута отсутствует в конфигурации»;
 - «Величина задержки должна быть как минимум вдвое превышать значение пинга»;
 - «Невозможно включить сервер. Отсутствует конфигурация»;
 - «Клиент уже добавлен в черный список»;
 - «Клиент уже добавлен в конфигурацию»;
 - «Клиент отсутствует в черном списке»;
 - «Клиент отсутствует в конфигурации»;
 - «Используется другая версия IP-протокола»;
 - «Невозможно добавить маршрут. Не установлены опции server-address и ifconfig»;
 - «Файл не обнаружен: <имя файла>»;
 - «Невозможно сгенерировать статический ключ»;
 - «Невозможно удалить VPN-сервер. Интерфейс <имя интерфейса> используется в разделах конфигурации:»;
 - «Ошибка проверки конфигурации VPN-сервера. Отсутствуют обязательные параметры: <перечень параметров>».
- 2.52. Сообщения, выдаваемые модулем «vrrp»:
- «Профиль не существует в системе: vrrp <имя экземпляра vrrp>»;
 - «Интерфейс не существует в системе: <имя интерфейса>»;
 - «Интерфейс должен быть включен и сконфигурирован с использованием IP-адреса»;
 - «Профиль с таким интерфейсом и ID уже существует в системе: vrrp <имя экземпляра vrrp>»;
 - «Невозможно активировать: vrrp <имя экземпляра vrrp>»;
 - «Невозможно остановить: vrrp <имя экземпляра vrrp>»;
 - «Невозможно удалить vrrp <имя экземпляра vrrp>. Интерфейс <имя экземпляра vrrp> используется в разделах конфигурации:»;
 - «Ошибка проверки конфигурации VRRP. Отсутствуют обязательные параметры: <перечень параметров>»;

- «Данный интерфейс уже отслеживается»;
- «Данный интерфейс не отслеживается».

3. СООБЩЕНИЯ, ОТОБРАЖАЕМЫЕ ПОСЛЕ ВЫПОЛНЕНИЯ КОМАНД

3.1. Сообщения, выдаваемые модулем «acl»:

- «Конфигурирование ACL»;
- «Идентификатор ACL»;
- «Удаление сконфигурированного ACL»;
- «Команда вывода конфигурации»;
- «Вывод конфигурации ACL»;
- «Отмена команды»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Удаление правила ACL»;
- «Номер последовательности»;
- «Тип правила»;
- «Тип ACL»;
- «Добавление правила ACL»;
- «Подкоманда switch»;
- «MAC-адрес»;
- «MAC-адрес источника»;
- «Любой MAC-адрес приемника»;
- «Имя протокола»;
- «Протокол»;
- «IP-адрес источника»;
- «Подкоманда switch»;
- «Значение 'любой'»;
- «IP-адрес приемника»;
- «Соотношение пакетов по заданному номеру порта источника»;
- «Номер порта»;
- «Соотношение пакетов по заданному номеру порта приемника»;
- «Интерфейс»;
- «Входной интерфейс»;
- «Имя интерфейса»;
- «Выходной интерфейс»;

- «Ограничение кол-ва TCP-соединений»;
- «Граничное значение»;
- «Состояние TCP-соединения»;
- «Состояние соединения»;
- «Максимальный размер сегмента TCP пакета (MSS)»;
- «Единичное значение MSS»;
- «Значение MSS»;
- «Диапазон значений MSS»;
- «Алгоритм кодирования строки»;
- «Обычная строка»;
- «Строка»;
- «Нех-строка»;
- «Верхний битовый отступ»;
- «Нижний битовый отступ»;
- «Значение отступа»;
- «Соотношение пакетов по заданному dscr»;
- «Длина IP-пакета (байт)»;
- «Соотношение по ack-флагу TCP»;
- «Соотношение по fin-флагу TCP»;
- «Соотношение по psh-флагу TCP»;
- «Соотношение по rst-флагу TCP»;
- «Соотношение по urg-флагу TCP»;
- «Идентификатор транзакции»;
- «Значение идентификатора»;
- «Идентификатор протокола»;
- «Длина заголовка MODBUS»;
- «Значение длины заголовка»;
- «Идентификатор узла»;
- «Код функции»;
- «Код»;
- «Идентификатор регистра»;
- «Установка опций логирования»;

- «Включение»;
- «Выключение»;
- «Уровень логирования»;
- «Значение уровня»;
- «U32 значение»;
- «Тип сообщения ICMP»;
- «Значение типа сообщения ICMP»;
- «Тип протокола»;
- «Тип протокола IP»;
- «Установка класса метки безопасности»;
- «Класс метки безопасности меньше»;
- «Класс метки безопасности равен»;
- «Класс метки безопасности больше»;
- «Значение класса»;
- «Маска класса метки безопасности»;
- «Значение маски»;
- «Установка защитного флага метки безопасности»;
- «Значение флага»;
- «Установка поля 'формат' расширенных опций метки безопасности»;
- «Значение формата»;
- «Позиция опции в метке»;
- «Значение позиции»;
- «Установка поля 'информация безопасности' расширенных опций метки безопасности»;
- «Значение информации»;
- «Позиция расширенной опции в метке»;
- «Установка для фрагментированных пакетов»;
- «Установка для нефрагментированных пакетов»;
- «Инверсия значения»;
- «Имя списка доступа»;
- «Флаги списка доступа»;
- «Указать диапазон».

3.2. Сообщения, выдаваемые модулем «api_control»:

- «Управление API»;
- «Включение/выключение API-сервиса»;
- «Показать состояние API-сервиса».

3.3. Сообщения, выдаваемые модулем «agr»:

- «IP-конфигурация»;
- «Отмена IP-конфигурации»;
- «Добавление статического адреса ARP»;
- «IP-адрес»;
- «MAC-адрес»;
- «Имя интерфейса»;
- «Удаление статического адреса ARP»;
- «Вывод ARP-таблицы»;
- «Показать интерфейсы ARP-прокси»;
- «Добавление ARP-прокси»;
- «Удаление ARP-прокси»;
- «Добавление Private VLAN ARP-прокси»;
- «Удаление Private VLAN ARP-прокси»;
- «Удаление ARP-таблицы».

3.4. Сообщения, выдаваемые модулем «auth»:

- «Команда вывода конфигурации»;
- «Команда вывода системной конфигурации»;
- «Вывод конфигурации аутентификации»;
- «Конфигурирование аутентификации»;
- «Подкоманда switch»;
- «Задание режима аутентификации»;
- «Аутентификация требуется на каждую сессию»;
- «Аутентификация требуется на каждую команду»;
- «Конфигурирование пароля аутентификации»;
- «Задание минимальной длины пароля аутентификации»;
- «Минимальная длина пароля (символов)»;
- «Задание сложности пароля аутентификации»;

- «Сложность пароля»;
- «Задание максимального количества попыток входа»;
- «Максимальное число попыток»;
- «Время блокировки»;
- «Время блокировки (с)»;
- «Время разблокировки»;
- «Время разблокировки (с)»;
- «Имя пользователя»;
- «Сброс счетчика ошибок входа»;
- «Включение/выключение системного почтовика»;
- «Статус почтовика»;
- «Тип события».

3.5. Сообщения, выдаваемые модулем «bgr»:

- «Конфигурация маршрутизатора»;
- «Отмена конфигурации маршрутизатора»;
- «Конфигурирование BGP»;
- «Идентификатор AS»;
- «Отключение модуля BGP»;
- «Вывод конфигурации BGP»;
- «Вывод конфигурации соседа BGP»;
- «IP-адрес соседа»;
- «Выбор маршрутов»;
- «Вывод маршрутов, объявленных для соседа»;
- «Вывод маршрутов, полученных от соседа»;
- «Политика выбора пути к AS»;
- «Конфигурация списка префиксов»;
- «Идентификатор списка префиксов»;
- «Разрешить или запретить»;
- «Разрешить»;
- «Запретить»;
- «Регулярное выражение для выбора пути к AS»;
- «Отмена конфигурации фильтра пути к AS»;

- «Выполнение команды из корневой области видимости»;
- «Отмена команды»;
- «Выход в корневую область видимости»;
- «Установка обобщающего IP-адреса»;
- «Установка IP-адреса»;
- «Добавление AS-SET информации в сводку»;
- «Фильтрация специфичных маршрутов в анонсах»;
- «Сброс обобщающего IP-адреса»;
- «Отключение автоматического суммирования»;
- «Специальные опции BGP»;
- «Параметры AS-конфедерации»;
- «Номер AS»;
- «Номера AS-узлов в конфедерации BGP»;
- «Имена узлов в формате 1,3,10,20»;
- «Журналирование изменений состояния BGP-соседей»;
- «Отмена специальных опций BGP»;
- «Отмена журналирования изменений состояния BGP-соседей»;
- «Установка стандартной конфигурации»;
- «Установка значения параметра Local Preference»;
- «Значение опции»;
- «Отмена стандартной конфигурации»;
- «Установка административной дистанции»;
- «Административная дистанция BGP»;
- «Административная дистанция для внешних маршрутов»;
- «Административная дистанция для внутренних маршрутов»;
- «Административная дистанция для локальных маршрутов»;
- «Отмена конфигурации административной дистанции»;
- «Сеть BGP»;
- «Сеть»;
- «Отмена конфигурации BGP-сети»;
- «Передача информации из другого протокола маршрутизации»;
- «Источник передачи»;

- «Метрика для перераспределенных маршрутов»;
- «Стандартная метрика»;
- «Фильтрация route-map для перераспределенных маршрутов»;
- «Идентификатор route-map»;
- «Отмена передачи информации из другого протокола маршрутизации»;
- «Параметры соседа»;
- «IP-адрес»;
- «Описание»;
- «Строка описания (в двойных кавычках)»;
- «Включение мягкой реконфигурации для входящей политики»;
- «Входящие маршруты»;
- «Информирование узла о возможностях BGP»;
- «Установка протокола согласования возможностей»;
- «Установка протокола динамического согласования возможностей»;
- «Установка extended-next-hop протокола согласования возможностей»;
- «Разрешить многоинтервальные сеансы для EBGP-соседей»;
- «Максимальное число интервалов»;
- «Установка пароля»;
- «Пароль»;
- «Установка BGP-соседа»;
- «Номер удаленной AS»;
- «Источник обновления маршрутной информации»;
- «IP-адрес источника»;
- «Идентификатор route-map»;
- «Входящее или исходящее направление»;
- «Входящее направление»;
- «Исходящее направление»;
- «Установка соседа как клиента для рефлектора маршрутов»;
- «Фильтрация входящих BGP-маршрутов»;
- «Идентификатор списка префиксов»;
- «Сброс параметров соседа».

3.6. Сообщения, выдаваемые модулем «bond»:

- «Подкоманда switch»;
 - «Команда вывода конфигурации»;
 - «Вывод конфигурации Bond»;
 - «Номер конфигурации»;
 - «Создание новой или редактирование существующей конфигурации интерфейса bond»;
 - «Номер интерфейса»;
 - «Удаление интерфейса bond»;
 - «Выполнение команды из корневой области видимости»;
 - «Отмена команды»;
 - «В данном режиме сетевые пакеты отправляются 'по кругу', от первого интерфейса к последнему. (используется по умолчанию)»;
 - «Один из интерфейсов работает в активном режиме, остальные в ожидающем»;
 - «Установка активного интерфейса»;
 - «Передача пакетов распределяется на основе хеша заголовка протокола и принимает входящий трафик с любого активного порта»;
 - «Передача во все объединенные интерфейсы»;
 - «Динамическое объединение одинаковых портов»;
 - «Установка MII link частоты наблюдения»;
 - «Значение MII (в миллисекундах)»;
 - «Установка типа балансирования нагрузки Bond»;
 - «Канал для отправки пакета однозначно определяется комбинацией MAC-адресов»;
 - «Канал для отправки пакета определяется по совокупности MAC- и IP-адресов»;
 - «Канал для отправки пакета определяется по совокупности IP-адресов и номеров портов»;
 - «Добавление ethernet-интерфейса в каналную группу»;
 - «Имя интерфейса»;
 - «Удаление ethernet-интерфейса из каналной группы»;
 - «Выход в корневую область видимости»;
- 3.7. Сообщения, выдаваемые модулем «bridge»:

- «Создание сетевого моста»;
- «Номер сетевого моста»;
- «Удалить сетевой мост»;
- «Показать конфигурацию сетевого моста»;
- «Добавить интерфейс в сетевой мост»;
- «Удалить интерфейс из сетевого моста»;
- «Имя интерфейса»;
- «Установить режим интерфейса»;
- «Режим Dot1ad»;
- «Режим Dot1q»;
- «Номер Vlan»;
- «Любой Vlan»;
- «Режим Inner dot1q»;
- «Тип интерфейса»;
- «Тип интерфейса untagged»;
- «Тип интерфейса pvid»;
- «Тип интерфейса self»;
- «Тип интерфейса master»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Отмена команды»;
- «Указать описание сетевого моста»;
- «Описание сетевого моста, в двойных кавычках»;
- «Убрать описание сетевого моста»;
- «Установить устаревание MAC»;
- «Устаревание MAC в секундах»;
- «Включить STP»;
- «Отключить STP»;
- «Установить приоритет STP»;
- «Приоритет STP»;
- «Включить режим фильтрации Vlan»;
- «Отключить режим фильтрации Vlan»;

- «Установить протокол Vlan»;
- «Протокол Vlan»;
- «Установить идентификатор Vlan»;
- «Идентификатор Vlan»;
- «Номер Vlan»;
- «Отмена команды»;
- «Режим»;
- «Указанный Vlan будет рассматриваться как немаркированный на выходе»;
- «Объединяет немаркированные кадры в указанный Vlan»;
- «Vlan настроен на физическом устройстве. (Требуется, если устройство является мостом)»;
- «Vlan настроен на программном устройстве типа сетевой мост»;
- «Показать подробности»;
- «Удалить интерфейс из сетевого моста»;
- «Варианты режима»;
- «Режим 802.1Q»;
- «VLAN Id»;
- «Режим 802.1AD»;
- «Внутренний 802.1Q».

3.8. Сообщения, выдаваемые модулем «core_log»:

- «Отмена команды»;
- «Вывод с начала»;
- «Команда доступа к журналу»;
- «Выбор журнала»;
- «Выбор локальных или удаленных настроек»;
- «Выбор подкоманды»;
- «IP-адрес удаленного rsyslog-сервера»;
- «Установка порта удаленного сервера (по умолчанию - 514)»;
- «Порт удаленного rsyslog-сервера»;
- «Включение/выключение журналирования»;
- «Конфигурирование журналирования»;
- «Отмена конфигурации отображения журнала»;

- «Установка уровня для отображения журнала»;
- «Уровень записи в журнал»;
- «Фильтрация сообщений журнала по имени модуля»;
- «Имя модуля»;
- «Удаление фильтра по имени модуля для журнала»;
- «Включение вывода журнала в терминал»;
- «Выключение вывода журнала в терминал»;
- «Отмена команды конфигурации журнала»;
- «Установка удаленного IP-адреса по умолчанию»;
- «Вывод конфигурации журналирования»;
- «Поиск»;
- «Дата»;
- «Выбор подкоманды»;
- «Конкретный день»;
- «Начиная с»;
- «Стартовый день»;
- «Конечный день»;
- «Время»;
- «Конкретное время»;
- «Начальное время»;
- «Конечное время»;
- «Отправитель»;
- «Имя отправителя»;
- «Успешно»;
- «Статус журнала»;
- «Действие»;
- «Описание»;
- «Уровень журналирования»;
- «Имя модуля»;
- «Текстовая строка»;
- «ID в журнале»;
- «Значение ID в журнале»;

- «Порядок»;
- «Выбор порядка»;
- «Обратный порядок»;
- «Лимит»;
- «Лимит кол-ва записей»;
- «Вывести (n) строк с конца файла»;
- «Количество строк»;
- «Вывод статуса отображения журнала»;
- «Сохранение журнала на носитель»;
- «Первый примонтированный носитель»;
- «Очистка журналов после копирования»;
- «Установка конфигурации ротации журнала»;
- «Установка максимального размера файла журнала»;
- «Размер в мегабайтах»;
- «Установка максимального кол-ва заархивированных файлов»;
- «Кол-во файлов»;
- «Временной интервал проверки размера файла журнала»;
- «Временной интервал в секундах»;
- «Отмена конфигурации ротации журнала»;
- «Установка отображения журнала политик доступа»;
- «Временной интервал проверки журнала»;
- «Установка уровня журналирования»;
- «Вывод уровня журналирования».

3.9. Сообщения, выдаваемые модулем «dhcp_relay»;

- «Конфигурирование DHCP»;
- «Конфигурирование DHCP-ретранслятора»;
- «Сброс конфигурации DHCP-ретранслятора»;
- «Вывод конфигурации DHCP-ретранслятора»;
- «Выполнение команды из корневой области видимости»;
- «Отмена команды»;
- «Выход в корневую область видимости»;
- «Добавление DHCP-сервера»;

- «IP-адрес сервера»;
- «Установка источника DHCP»;
- «Установка интерфейса»;
- «Имя интерфейса»;
- «Добавление опции 82»;
- «Удаление опции 82».

3.10. Сообщения, выдаваемые модулем «dhcp_server»:

- «Команды DHCP-сервера»;
- «Отмена команды или установка стандартных значений»;
- «Установка связи DHCP-сервера»;
- «Установка статуса DHCP-сервера: on, off»;
- «Установка интерфейса DHCP-сервера»;
- «Имя интерфейса»;
- «Удаление интерфейса DHCP-сервера»;
- «Установка локального IP-адреса»;
- «Локальный IP-адрес»;
- «Удаление локального IP-адреса»;
- «Срок аренды по умолчанию»;
- «Значение срока аренды по умолчанию (секунды, диапазон: [0, max-lease-time]). По умолчанию max-lease-time = 3600»;
- «Вход в подменю для конфигурирования диапазона DHCP»;
- «IP-адрес сети»;
- «Удалить сеть»;
- «Удаление сконфигурированного диапазона DHCP»;
- «Вывод конфигурации DHCP-сервера»;
- «Вывод статуса DHCP-сервера»;
- «Вывод клиентов DHCP-сервера»;
- «Выполнение команды из корневой области видимости»;
- «Отмена команды или установка стандартных значений»;
- «Конфигурирование хоста»;
- «Установка хоста»;
- «MAC-адрес хоста»;

- «IP-адрес»;
- «IP-адрес хоста»;
- «Удаление хоста»;
- «Установка диапазона IP-адресов»;
- «Стартовый IP-адрес диапазона»;
- «Конечный IP-адрес диапазона»;
- «Удаление диапазона IP-адресов»;
- «Максимальное время аренды»;
- «Значение максимального времени аренды»;
- «Установка опций»;
- «Удаление опций»;
- «Установка адреса маршрутизатора для клиента»;
- «Первый в списке»;
- «Удалить адрес маршрутизатора»;
- «Установка принт-сервера»;
- «Удаление принт-сервера»;
- «Установка NTP-сервера»;
- «Удаление NTP-сервера»;
- «Установка доменного имени»;
- «Имя домена (до 2 уровня включительно)»;
- «Удаление доменного имени»;
- «Установка IP-адреса DNS»;
- «Удаление IP-адреса DNS»;
- «Выход в корневую область видимости»;
- «Создать новый DHCP-сервер»;
- «Удалить DHCP-сервер»;
- «Создать новый DHCP6-сервер»;
- «Удалить DHCP6-сервер»;
- «Номер DHCP-сервера»;
- «Имя пула DHCP»;
- «DHCP-сервер уже существует»;
- «DHCP-пул не существует»;

– «DHCP-сервер не существует».

3.11. Сообщения, выдаваемые модулем «dns»:

- «Конфигурация DNS»;
- «Отмена конфигурации DNS»;
- «Конфигурация системных сервисов»;
- «Включение/выключение DNS»;
- «Подкоманда выбора»;
- «Включить DNS»;
- «Выключить DNS»;
- «Конфигурирование DNS»;
- «Отмена конфигурирования DNS»;
- «Команда вывода конфигурации»;
- «Вывод статуса DNS»;
- «Вывод конфигурации DNS»;
- «Конфигурирование DNS-сервера»;
- «IP-адрес DNS»;
- «Удаление конфигурации DNS-сервера»;
- «Конфигурирование домена по умолчанию»;
- «Имя домена»;
- «Удаление домена по умолчанию»;
- «Добавление интерфейса DNS-сервиса»;
- «Имя интерфейса»;
- «Удаление интерфейса DNS-сервиса».

3.12. Сообщения, выдаваемые модулем «gre»:

- «Создание интерфейса»;
- «Удаление интерфейса»;
- «Конфигурация GRE-интерфейса»;
- «Номер интерфейса»;
- «Удаление GRE-интерфейса»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Установить локальный IP-адрес туннеля»;

- «Локальный IP-адрес»;
- «Установить удаленный IP-адрес туннеля»;
- «Удаленный IP-адрес»;
- «Вывод конфигурации туннеля gre».

3.13. Сообщения, выдаваемые модулем «help»:

- «Показать справку для модуля»;
- «Имя модуля для справки».

3.14. Сообщения, выдаваемые модулем «interface»:

- «Конфигурация настроек интерфейса»;
- «Имя интерфейса»;
- «Идентификация интерфейса»;
- «Подкоманда выбора»;
- «Включить индикацию интерфейса»;
- «Отключить индикацию интерфейса»;
- «Показать информацию об интерфейсах»;
- «Показать информацию о последовательных интерфейсах»;
- «Показать интерфейсы по имени»;
- «Показать подробную информацию об интерфейсах»;
- «Показать статистику»;
- «Показать информацию о DHCP-клиентах»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Отмена команды»;
- «Выключение интерфейса»;
- «Включение интерфейса»;
- «Добавление IP-адреса интерфейса»;
- «Выбор подкоманды»;
- «IP-адрес интерфейса с битовой маской»;
- «Запрос IP-адреса у DHCP-сервера»;
- «Отказ от получения адресов DNS-серверов от DHCP-сервера»;
- «Отказ от получения default-маршрута от DHCP-сервера»;
- «Удаление IP-адреса интерфейса»;

- «Установка описания для интерфейса»;
- «Описание интерфейса (в двойных кавычках)»;
- «Удаление описания для интерфейса»;
- «Установка значения MTU»;
- «Значение MTU»;
- «Установка значения MTU по умолчанию»;
- «Установка MAC-адреса интерфейса»;
- «MAC-адрес»;
- «Установка MAC-адреса интерфейса по умолчанию»;
- «Установка скорости на интерфейсе»;
- «Выбор скорости интерфейса»;
- «Установка режима дуплекса на интерфейсе»;
- «Выбор дуплекса на интерфейсе»;
- «Установка неразборчивого режима на интерфейсе»;
- «Выключение неразборчивого режима на интерфейсе»;
- «Установка режима автосогласования»;
- «Режим автосогласования».

3.15. Сообщения, выдаваемые модулем «ip_filter»:

- «Установка списка правил фильтрации»;
- «Удаление настроек списка правил фильтрации»;
- «Отмена команды»;
- «Желаемая позиция правила в таблице фильтрации»;
- «Добавление правила доступа в список правил фильтрации»;
- «Имя правила доступа»;
- «Направление передачи»;
- «Выбор подкоманды»;
- «Входящее направление»;
- «Исходящее направление»;
- «Направление проброса»;
- «Принять пакеты»;
- «Сброс пакетов»;
- «Отмена пакетов»;

- «Отмена соединения с событием»;
- «Сообщение события»;
- «Конфигурация модуля фильтрации»;
- «Установка опций фильтрации»;
- «Политика принятия»;
- «Политика отбрасывания»;
- «IPv4-протокол»;
- «IPv6-протокол»;
- «Фильтрующая цепочка»;
- «Входящий трафик»;
- «Исходящий трафик»;
- «Транзитный трафик»;
- «Политика фильтрации»;
- «Установка опций логирования»;
- «Включение»;
- «Выключение»;
- «Уровень логирования»;
- «Значение уровня»;
- «Вывод параметров фильтрации»;
- «Вывод конфигурации фильтрации»;
- «Вывод политик фильтрации для протокола IPv4»;
- «Вывод политик фильтрации для протокола IPv6»;
- «Вывод статистики правил фильтрации»;
- «Вывод опций IPv4»;
- «Вывод опций IPv6».

3.16. Сообщения, выдаваемые модулем «ірір»:

- «Создание интерфейса»;
- «Удаление интерфейса»;
- «Конфигурация IPIP-интерфейса»;
- «Номер интерфейса»;
- «Удаление IPIP-интерфейса»;
- «Выполнение команды из корневой области видимости»;

- «Выход в корневую область видимости»;
- «Установить локальный IP-адрес туннеля»;
- «Локальный IP-адрес»;
- «Установить удаленный IP-адрес туннеля»;
- «Удаленный IP-адрес»;
- «Вывод конфигурации туннеля ipip».

3.17. Сообщения, выдаваемые модулем «ipsec»:

- «Создание интерфейса ipsec»;
- «Отмена команды»;
- «Удаление интерфейса ipsec»;
- «Создание интерфейса»;
- «Удаление интерфейса»;
- «Добавление интерфейса ipsec»;
- «Вывод состояния туннеля ipsec»;
- «Имя интерфейса»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Установка локальных параметров»;
- «Установка удаленных параметров»;
- «Удаление локальных параметров»;
- «Удаление удаленных параметров»;
- «Установка типа IP-протокола»;
- «Выбор подкоманды»;
- «Установка локального адреса»;
- «Специальное значение адреса»;
- «IP-адрес»;
- «Удаление локального адреса»;
- «Установка удаленного адреса»;
- «Удаление удаленного адреса»;
- «Установка крипто-ключа»;
- «Крипто-ключ»;
- «Установка алгоритма шифрования»;

- «Алгоритм шифрования»;
- «Установка интеграционного ключа»;
- «Установка интеграционного алгоритма»;
- «Целое число»;
- «Значение идентификатора»;
- «Удаление крипто-ключа»;
- «Удаление интеграционного ключа»;
- «Режим туннеля»;
- «Транспортный режим»;
- «Туннельный режим»;
- «Установка адреса удалённой сети»;
- «Установка IP-адреса удалённой сети»;
- «Установка специального адреса удаленной сети»;
- «Удаление адреса удаленной сети»;
- «Установка адреса локальной сети»;
- «Установка IP-адреса локальной сети»;
- «Установка специального адреса локальной сети»;
- «Удаление адреса локальной сети»;
- «Идентификатор интерфейса»;
- «Рестарт модуля ipsec»;
- «Включение»;
- «Выключение»;
- «Установка адреса хоста источника»;
- «Удаление адреса хоста источника»;
- «Установка адреса хоста приемника»;
- «Удаление адреса хоста приемника»;
- «IP-адрес интерфейса с битовой маской»;
- «Установка идентификатора источника»;
- «Идентификатор»;
- «Удаление идентификатора источника»;
- «Установка идентификатора приемника»;
- «Удаление идентификатора приемника»;

- «Установка типа IP-протокола источника»;
- «Установка порта источника»;
- «Значение порта»;
- «Установка типа IP-протокола приемника»;
- «Установка порта приемника»;
- «Параметры сертификата»;
- «Имя файла сертификата»;
- «Удаление файла сертификата»;
- «Установка параметров сертификата источника»;
- «Установка параметров сертификата приемника»;
- «Удаление параметров сертификата источника»;
- «Удаление параметров сертификата приемника»;
- «Удаление файла сертификата источника»;
- «Удаление файла сертификата приемника»;
- «Установка PSK»;
- «Удаление PSK»;
- «Установка IKE DH»;
- «Удаление IKE DH»;
- «Значение»;
- «Установка режима аутентификации»;
- «Тип алгоритма»;
- «Установка алгоритма IKE»;
- «Перечень алгоритмов»;
- «Удаление алгоритма IKE»;
- «Установка алгоритма ESP»;
- «Удаление алгоритма ESP»;
- «Установка алгоритма аутентификации»;
- «Удаление алгоритма аутентификации»;
- «Установка времени жизни безопасной ассоциации»;
- «Тайм-аут»;
- «Значение»;
- «Установка опций»;

- «Установка опций для IPSEC»;
- «Отмена установки опций»;
- «Отмена установки опций для IPSEC»;
- «Установка количества повторных передач пакетов перед отказом (по умолчанию 5) »;
- «Отмена установки количества повторных передач пакетов перед отказом; устанавливается значение по умолчанию (5) »;
- «Значение 1-255»;
- «Имя домена»;
- «Диапазон адресов»;
- «Запрос виртуального адреса для использования в качестве внутреннего туннельного адреса».

3.18. Сообщения, выдаваемые модулем «ipset»:

- «Конфигурирование ACS»;
- «Идентификатор ACS»;
- «Тип ACS»;
- «Значение типа ACS»;
- «Удаление сконфигурированного ACS»;
- «Вывод конфигурации ACS»;
- «Отмена команды»;
- «Выход в корневую область видимости»;
- «Добавить запись»;
- «Код протокола»;
- «IP-адрес»;
- «Сетевой адрес»;
- «Порт»;
- «MAC-адрес»;
- «Интерфейс»;
- «Удалить запись»;
- «Установить направление»;
- «Варианты»;
- «Источник»;
- «Назначение».

3.19. Сообщения, выдаваемые модулем «l2tp_client»:

- «Создание интерфейса»;
- «Удаление интерфейса»;
- «Создание серверного/клиентского L2TP-интерфейса»;
- «Режим конфигурирования клиентского L2TP-интерфейса»;
- «Номер интерфейса»;
- «Идентификатор интерфейса»;
- «Вывод конфигурации L2TP»;
- «Удаление серверного/клиентского L2TP-интерфейса»;
- «Удаление клиентского L2TP-интерфейса»;
- «Вывод конфигурации L2TP-клиента»;
- «Выход в корневую область видимости»;
- «Отмена команды»;
- «Отмена команды IP»;
- «Выбор подкоманды»;
- «Входящие пакеты»;
- «Исходящие пакеты»;
- «Установка параметров IP»;
- «Установка MTU»;
- «Значение MTU»;
- «Установка MRU»;
- «Значение MRU»;
- «Установка маршрута»;
- «IP-маршрут»;
- «Удаление маршрута»;
- «Установка списка аутентификации»;
- «Установка запроса/отказа аутентификации»;
- «Удаление запроса/отказа аутентификации»;
- «Логин»;
- «Установка пароля»;
- «Пароль»;
- «Удаление списка аутентификации»;

- «Установка описания интерфейса»;
- «Описание (в двойных кавычках)»;
- «Удаление описания интерфейса»;
- «Установка транслирующего интерфейса»;
- «Имя интерфейса»;
- «Удаление транслирующего интерфейса»;
- «Установка интервала echo-запросов LCP»;
- «Интервал (с)»;
- «Удаление интервала echo-запросов LCP»;
- «Установка количества неудачных echo-запросов, после которого одноранговый узел считается мертвым»;
- «Кол-во запросов»;
- «Удаление количества неудачных echo-запросов, после которого одноранговый узел считается мертвым»;
- «Активация режима получения адресов dns-серверов от L2TP-сервера»;
- «Отмена режима получения адресов dns-серверов от L2TP-сервера»;
- «Установка использования адреса L2TP-клиента, как маршрута по умолчанию»;
- «Отмена использования адреса L2TP-клиента, как маршрута по умолчанию»;
- «Кол-во попыток»;
- «Установка максимального количества попыток повторной установки L2TP-соединения с сервером»;
- «Удаление максимального количества попыток повторной установки L2TP-соединения с сервером»;
- «Установка режима повторного установления соединения при потере L2TP-соединения с сервером»;
- «Отмена режима повторного установления соединения при потере L2TP-соединения с сервером»;
- «Установка временного интервала между повторными попытками установления L2TP-соединения»;
- «Удаление временного интервала между повторными попытками установления L2TP-соединения»;
- «Установка предварительного общего ключа PSK для авторизации с IPsec»;

- «Пароль»;
- «Удаление предварительного общего ключа PSK»;
- «Установка требование/отказ PPP-аутентификации по протоколу PAP»;
- «Удаление требование/отказ PPP-аутентификации по протоколу PAP»;
- «Установка требование/отказ PPP-аутентификации по протоколу CHAP»;
- «Удаление требование/отказ PPP-аутентификации по протоколу CHAP»;
- «Установка требование/отказ PPP-аутентификации по протоколу MSCHAPv1»;
- «Удаление требование/отказ PPP-аутентификации по протоколу MSCHAPv1»;
- «Установка адреса сервера»;
- «Установка IP-адреса сервера»;
- «IP-адрес»;
- «Установка DNS-сервера»;
- «DNS-имя»;
- «Удаление адреса сервера»;
- «Включение»;
- «Выключение»;
- «L2TP сервер/клиент»;
- «L2TP-клиент».

3.20. Сообщения, выдаваемые модулем «l2tp_server»:

- «Создание сущности»;
- «Удаление сущности»;
- «Создание/редактирование серверного/клиентского L2TP-интерфейса»;
- «Удаление серверного/клиентского L2TP-интерфейса»;
- «Вывод конфигурации серверного/клиентского L2TP-интерфейса»;
- «Создание серверного L2TP-интерфейса»;
- «Номер интерфейса»;
- «Выбор подкоманды»;
- «Удаление серверного L2TP-интерфейса»;
- «Вывод конфигурации L2TP-сервера»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;

- «Отмена команды»;
- «Настройка параметров IPv4»;
- «Отмена параметров IPv4»;
- «Добавление IP-адресов DNS-серверов (максимально - 2)»;
- «IP-адрес»;
- «Удаление IP-адресов DNS-серверов»;
- «Установка интервала echo-запросов LCP»;
- «Интервал (с)»;
- «Удаление интервала echo-запросов LCP»;
- «Установка количества неудачных echo-запросов, после которого одноранговый узел считается мертвым»;
- «Кол-во попыток»;
- «Удаление количества неудачных echo-запросов, после которого одноранговый узел считается мертвым»;
- «Установка MTU»;
- «Значение MTU»;
- «Установка MRU»;
- «Значение MRU»;
- «Установка локального адреса сервера»;
- «Удаление локального адреса сервера»;
- «Установка параметров аутентификации»;
- «Удаление параметров аутентификации»;
- «Аутентификация клиентов»;
- «Логин»;
- «Установка пароля»;
- «Пароль»;
- «Удаление параметров локальной аутентификации»;
- «Установка параметров Radius-аутентификации»;
- «IP-адрес Radius-сервера»;
- «Удаление параметров Radius-аутентификации»;
- «Установка IP-адреса»;
- «IP-адрес»;

- «Удаление IP-адреса»;
- «Установка удаленной аутентификации (radius-сервер)»;
- «Удаление удаленной аутентификации (radius-сервер)»;
- «Установка пула IP-адресов»;
- «Стартовый IP-адрес»;
- «Конечный IP-адрес»;
- «Установка пула разрешенных IP-адресов L2TP-клиентов»;
- «Удаление пула разрешенных IP-адресов L2TP-клиентов»;
- «Установка запрета использования указанного пула IP-адресов»;
- «Удаление пула запрещенных IP-адресов»;
- «Установка предварительного общего ключа PSK для авторизации с IPsec»;
- «Пароль»;
- «удаление предварительного общего ключа PSK»;
- «Установка требование/отказ PPP-аутентификации по протоколу PAP»;
- «Удаление требование/отказ PPP-аутентификации по протоколу PAP»;
- «Установка требование/отказ PPP-аутентификации по протоколу CHAP»;
- «Удаление требование/отказ PPP-аутентификации по протоколу CHAP»;
- «Установка требование/отказ PPP-аутентификации по протоколу MSCHAPv1»;
- «Удаление требование/отказ PPP-аутентификации по протоколу MSCHAPv1»;
- «Установка имени хоста сервера»;
- «Имя хоста»;
- «Удаление имени хоста»;
- «Имя файла»;
- «Установка имени файла с ключом аутентификации ipsec»;
- «Удаление имени файла с ключом аутентификации ipsec»;
- «Требовать/отказывать клиенту в unix-аутентификации (логин и пароль берется из локального etc/passwd)»;
- «Отмена требование/отказ клиенту в unix-аутентификации»;
- «Установка разрешения создания только одного туннеля между клиентом и сервером»;
- «Значение yes/no»;

- «Отмена разрешения создания только одного туннеля между клиентом и сервером»;
- «Использование сокрытия полей AVP»;
- «Отмена использования сокрытия полей AVP»;
- «Использование бита длины, указывающего полезную нагрузку l2tp-пакета»;
- «Отмена использования бита длины, указывающего полезную нагрузку l2tp-пакета»;
- «Установка запрета назначения адреса из пула (например, использование rppd с поддержкой RADIUS)»;
- «Отмена запрета назначения адреса из пула»;
- «Установка маршрута»;
- «IP-маршрут»;
- «Удаление маршрута»;
- «Выбор подкоманды»;
- «Включение»;
- «Выключение»;
- «L2TP-сервер/клиент»;
- «L2TP-сервер».

3.21. Сообщения, выдаваемые модулем «ldap»:

- «Команда вывода конфигурации»;
- «Конфигурирование клиента LDAP»;
- «Отмена конфигурации клиента LDAP»;
- «Вывод конфигурации клиента LDAP»;
- «Сохранение»;
- «Сохранение сертификата»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Отмена команды»;
- «Установка IP-адресов хостов LDAP-сервера»;
- «IP-адрес хоста»;
- «Удаление IP-адресов хостов LDAP-сервера»;
- «Выбор режима»;
- «Все IP-адреса хостов»;

- «Установка порта LDAP-сервера»;
- «Значение порта»;
- «Установка версии протокола LDAP»;
- «Версия протокола»;
- «Установка общего имени пользователя LDAP»;
- «Общее имя пользователя»;
- «Установка административного пароля LDAP-сервера»;
- «Пароль»;
- «Установка домена»;
- «Имя домена»;
- «Установка области поиска LDAP»;
- «Режим поиска»;
- «Установка временных опций соединения»;
- «Значение таймаута»;
- «Установка опции bind»;
- «Значение bind»;
- «Установка опции idle»;
- «Значение idle»;
- «Установка режима LDAP SSL»;
- «Режим работы»;
- «Установка требований к сертификату SSL»;
- «Уровень требований»;
- «Установка сертификата LDAP SSL»;
- «Путь к сертификату»;
- «Подкоманда switch»;
- «Аутентификация LDAP»;
- «Включение»;
- «Выключение».

3.22. Сообщения, выдаваемые модулем «lldp»:

- «Конфигурирование LLDP»;
- «Сброс конфигурации LLDP»;
- «Включение/выключение LLDP»;

- «Установка интервала передачи, сек.»;
- «Интервал передачи (по умолчанию 30)»;
- «Количество tx-интервалов до обновления»;
- «Количество tx-интервалов (по умолчанию 4)»;
- «Установка статуса lldp»;
- «Отключен»;
- «Только TX»;
- «Только RX»;
- «RX и TX»;
- «Установить административный IP-адрес»;
- «ipv4 или ipv6 адрес»;
- «Установка транслирующего интерфейса»;
- «Удаление транслирующего интерфейса»;
- «Вывод информации lldp»;
- «Вывод конфигурации lldp»;
- «Вывод статистики lldp»;
- «Установка описания порта»;
- «Описание порта»;
- «Установка режима агента SNMP»;
- «Выбор подкоманды»;
- «Включение»;
- «Выключение»;
- «Включение LLDP»;
- «Выключение LLDP».

3.23. Сообщения, выдаваемые модулем «loopback»:

- «Создание интерфейса»;
- «Удаление интерфейса»;
- «Номер интерфейса loopback»;
- «Удаление интерфейса loopback».

3.24. Сообщения, выдаваемые модулем «mirroring»:

- «Создать зеркалирование»;
- «Источник»;

- «Транслирующий интерфейс»;
- «Приемник»;
- «Транслируемый IP-адрес»;
- «Транслируемый интерфейс»;
- «Имя интерфейса»;
- «Транслируемый порт»;
- «Номер порта»;
- «Протокол»;
- «Удалить зеркалирование»;
- «Вывод конфигурации»;
- «Вывод опций IPv4»;
- «Вывод опций IPv6»;
- «Вывод конфигурации правил зеркалирования для таблицы правил MANGLE протокола IPv4»;
- «Вывод конфигурации правил для таблицы правил MANGLE протокола IPv4»;
- «Вывод конфигурации правил для таблицы правил MANGLE протокола IPv6»;
- «Вывод конфигурации правил зеркалирования для таблицы правил MANGLE протокола IPv6»;
- «Желаемая позиция правила в таблице зеркалирования».

3.25. Сообщения, выдаваемые модулем «nat»:

- «Конфигурация NAT»;
- «Добавление правила NAT»;
- «Имя правила NAT»
- «Выбор подкоманды»;
- «Интерфейс локальной сети»;
- «Интерфейс внешней сети»;
- «Имя интерфейса»;
- «Использование IP-адресов исходящих интерфейсов как пул адресов»;
- «Удаление IP-nat»;
- «Удаление правила IP-nat»;
- «Выполнение команды корневого уровня»;
- «Отмена команды»;

- «Выход в корневую область видимости»;
- «Добавление интерфейса»;
- «Имя ACL»;
- «Тип интерфейса»;
- «Удаление интерфейса»;
- «Опция 'все'»;
- «Функция NAT»;
- «Включение NAT-маскарадинга»;
- «Единичное значение»;
- «Диапазон портов»;
- «Добавление переадресации»;
- «Опции внутренней сети»;
- «Адрес источника»;
- «IP-адрес»;
- «Порт»;
- «Значение порта»;
- «Адрес получателя»;
- «Опции трансляции адресов NAT»;
- «Диапазон значений»;
- «Диапазон IP-адресов»;
- «Диапазон портов»;
- «Вывод конфигурации»;
- «Вывод опций IPv4»;
- «Вывод опций IPv6»;
- «Вывод конфигурации правил для NAT-протокола IPv4»;
- «Вывод конфигурации правил для NAT-протокола IPv6»;
- «Вывод конфигурации SNAT»;
- «Вывод конфигурации DNAT»;
- «Вывод конфигурации MASQUERADE»;
- «Установка протокола»;
- «Протокол»;
- «Желаемая позиция правила в таблице NAT»;

- «Значение позиции»;
- «Версия IP-протокола»;
- «Инверсия значения».

3.26. Сообщения, выдаваемые модулем «ntp»:

- «NTP-клиент»;
- «NTP-запуск/остановка»;
- «Добавление NTP-сервера»;
- «IP-адрес»;
- «Отправлять пачку пакетов синхронизации, вместо одного»;
- «Удаление параметра NTP»;
- «Удаление NTP-сервера»;
- «Установка разрешенной NTP-сети»;
- «Имя интерфейса»;
- «Удаление разрешенной NTP-сети»;
- «Вывод конфигурации NTP».

3.27. Сообщения, выдаваемые модулем «ospf»:

- «Конфигурирование OSPF»;
- «Вывод конфигурации OSPF»;
- «Вывод конфигурации и правил маршрутизации OSPF»;
- «Вывод конфигурации интерфейсов OSPF»;
- «Вывод ID-маршрутизатора»;
- «IP-адрес для использования в качестве ID-маршрутизатора»;
- «Установка IP-адреса»;
- «Отмена конфигурации ID-маршрутизатора»;
- «Отмена конфигурации маршрутизации»;
- «Отключение модуля OSPF»;
- «Выполнение команды из корневой области видимости»;
- «Отмена команды»;
- «Выход в корневую область видимости»;
- «Установка стоимости OSPF»;
- «Использование метода эталонной полосы пропускания для назначения стоимости OSPF»;

- «Значение эталонной полосы пропускания в Мбит/с»;
- «Отмена использования метода эталонной полосы пропускания для назначения стоимости OSPF»;
- «Заимствование информации из другого протокола маршрутизации»;
- «Источник заимствования»;
- «Метрика для заимствованных маршрутов»;
- «Значение метрики»;
- «Тип метрики для заимствованных маршрутов»;
- «Тип метрики»;
- «Фильтрация картой маршрутов для заимствованных маршрутов»;
- «Имя карты маршрутов»;
- «Отмена заимствования информации из другого протокола маршрутизации»;
- «Выдача маршрута по умолчанию»;
- «Всегда объявлять маршрут по умолчанию»;
- «Не выдавать маршрут по умолчанию»;
- «Параметры узлов-соседей»;
- «IP-адрес»;
- «Интервал опроса»;
- «Интервал опроса 1-65535»;
- «Приоритет»;
- «Значение приоритета 0-255»;
- «Отмена параметров узлов-соседей»;
- «Установка пассивного интерфейса»;
- «Имя интерфейса»;
- «Удаление пассивного интерфейса»;
- «Параметры области OSPF»;
- «Номер области»;
- «Установка аутентификации»;
- «Дайджест сообщения»;
- «Объявленная сводная стоимость тупиковой области по умолчанию»;
- «Значение стоимости»;
- «Задание области OSPF как тупиковой»;

- «Запрет ввода межобластных маршрутов»;
- «Установка области OSPF как nssa»;
- «Запрет ввода межобластных маршрутов»;
- «Объединение соотносящихся маршрутов (только для пограничных маршрутизаторов)»;
- «Префикс диапазона области»;
- «Сообщать данный диапазон (по умолчанию)»;
- «Не сообщать данный диапазон (по умолчанию)»;
- «Отмена параметров области OSPF»;
- «Установка маршрутизации в сети IP»;
- «Префикс сети OSPF»;
- «Установка ID-области OSPF»;
- «Отмена маршрутизации в сети IP»;
- «Установка таймеров»;
- «Удаление таймеров»;
- «Задержка сообщений статуса соединения»;
- «Значение в миллисекундах»;
- «Отмена задержки сообщений статуса соединения»;
- «Адаптивный таймер дросселирования»;
- «Задержка между отсылкой LSA»;
- «Установка для всех»;
- «Отмена установки адаптивного таймера дросселирования»;
- «Установка параметров интерфейса»;
- «Имя интерфейса»;
- «Установка интерфейса»;
- «Установка интервала приветствия»;
- «Значение интервала»;
- «Установка мертвого интервала»;
- «Установка интервала повторной передачи»;
- «Установка Bfd»;
- «Отключение обнаружения несоответствия MTU на этом интерфейсе»;
- «Отмена команд»;

- «Отмена BFD»;
- «Сброс стоимости»;
- «Отмена аутентификации»;
- «Включение обнаружения несоответствия MTU на этом интерфейсе»;
- «Установка пароля аутентификации»;
- «Метод аутентификации»;
- «Установка MD5-аутентификации»;
- «Установка значения идентификатора MD5-ключа»;
- «Установка аутентификации с простым паролем».

3.28. Сообщения, выдаваемые модулем «rbg»:

- «Отмена команды»;
- «Конфигурация PBR»;
- «Добавить правило»;
- «Номер правила»;
- «Отменить конфигурацию PBR»;
- «Удалить правило»;
- «Показать правила»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Установить префикс источника для поиска соответствия»;
- «Префикс»;
- «Префикс 'по умолчанию'»;
- «Префикс 'все'»;
- «Префикс 'любой'»;
- «Префикс 'IP-адрес'»;
- «IP-адрес»;
- «Удалить префикс источника»;
- «Установить префикс назначения для поиска несоответствия»;
- «Удалить префикс назначения»;
- «Установить входящий интерфейс для поиска соответствия»;
- «Имя интерфейса»;
- «Удалить входящий интерфейс»;

- «Установить исходящий интерфейс»;
- «Удалить исходящий интерфейс»;
- «Установить значение TOS»;
- «Значение TOS (16-ричное число, напр. 0x00)»;
- «Удалить значение TOS»;
- «Установить значение fwmark для поиска соответствия»;
- «Значение fwmark»;
- «Удалить значение fwmark»;
- «Установить диапазон значений UID для поиска соответствия»;
- «Диапазон значений UID»;
- «Удалить диапазон значений UID»;
- «Установить значение IP-протокола для поиска соответствия»;
- «Значение IP-протокола (название протокола или число [0-255])»;
- «Удалить значение IP-протокола»;
- «Установить порт источника для поиска соответствия»;
- «Порт источника»;
- «Удалить порт источника»;
- «Установить порт назначения для поиска соответствия»;
- «Порт назначения»;
- «Удалить порт назначения»;
- «Инвертировать правило для поиска несоответствия»;
- «Отменить инвертирование правила»;
- «Установить приоритет правила»;
- «Значение приоритета»;
- «Установить идентификатор таблицы маршрутизации»;
- «Идентификатор таблицы маршрутизации»;
- «Локальная таблица маршрутизации»;
- «Главная таблица маршрутизации»;
- «Таблица маршрутизации по умолчанию»;
- «Числовой идентификатор таблицы маршрутизации»;
- «Значение идентификатора»;
- «Установить значение realms»;

- «Значение realms»;
- «Установить протокол маршрутизации»;
- «Выбрать тип протокола»;
- «Тип redirect»;
- «Тип kernel»;
- «Тип boot»;
- «Тип static»;
- «Тип zebra»;
- «Установить значение nat»;
- «Адрес».

3.29. Сообщения, выдаваемые модулем «pim»:

- «Конфигурирование PIM»;
- «Отмена конфигурации PIM»;
- «Добавление интерфейса»;
- «Имя интерфейса»;
- «Удаление интерфейса»;
- «Добавление RP PIM»;
- «RP IP-адрес»;
- «Групповой префикс»;
- «IP-адрес многоадресной рассылки»;
- «Удаление RP PIM»;
- «Вывод информации»;
- «Вывод информации IPv4»;
- «Вывод конфигурации PIM»;
- «Выбор подкоманды»;
- «Вывод состояния таблицы PIM»;
- «Вывод интерфейсов PIM»;
- «Вывод узлов-соседей PIM»;
- «Вывод PIM RP».

3.30. Сообщения, выдаваемые модулем «radius»:

- «Команда вывода конфигурации»;
- «Конфигурирование клиента radius»;

- «Отмена конфигурации клиента radius»;
- «Отмена конфигурации аутентификации»;
- «Конфигурирование сервера radius»;
- «IP-адрес сервера radius»;
- «Общий секрет клиента radius»;
- «Порт сервера radius»;
- «Порт»;
- «IP-адрес источника»;
- «IP-адрес»;
- «Тайм-аут соединения»;
- «Значение тайм-аута»;
- «Удаление сервера radius»;
- «Подкоманда switch»;
- «Аутентификация Radius»;
- «Включение»;
- «Выключение».

3.31. Сообщения, выдаваемые модулем «rip»:

- «Вход в меню конфигурирования RIP»;
- «Вывод конфигурации RIP»;
- «Вывод статуса RIP»;
- «Отмена конфигурации маршрутизации»;
- «Отключение модуля RIP»;
- «Выполнение команды из корневой области видимости»;
- «Отмена команды»;
- «Заимствование информации из другого протокола маршрутизации»;
- «Тип маршрута»;
- «Метрика»;
- «Значение метрики»;
- «Фильтрация route-map для перераспределенных маршрутов»;
- «Отмена заимствования информации из другого протокола маршрутизации»;
- «Добавление узла-соседа»;
- «IP-адрес»;

- «Удаление узла-соседа»;
 - «Установка сети»;
 - «Выбор подкоманды»;
 - «IP-адрес интерфейса с бит-маской»;
 - «Имя интерфейса»;
 - «Удаление сети»;
 - «Установка пассивного интерфейса»;
 - «Удаление пассивного интерфейса»;
 - «Установка аутентификации на интерфейсе»;
 - «Имя интерфейса»;
 - «Аутентификация»;
 - «Метод аутентификации»;
 - «Пароль»;
 - «Строка пароля»;
 - «Удаление аутентификации на интерфейсе»;
 - «Список для изменения метрики маршрута»;
 - «Имя списка изменения»;
 - «Входящее или исходящее направление»;
 - «Входящее направление»;
 - «Исходящее направление»;
 - «Удаление списка для изменения метрики маршрута»;
 - «Установка таймеров»;
 - «Установка базового таймера»;
 - «Значение таймера обновления таблицы маршрутов в секундах (по умолчанию - 30)»;
 - «Таймер тайм-аута маршрутной информации в секундах (по умолчанию - 180)»;
 - «Таймер сборщика мусора в секундах (по умолчанию - 120)»;
 - «Выход в корневую область видимости».
- 3.32. Сообщения, выдаваемые модулем «ripng»:
- «Вход в меню конфигурирования RIPNG»;
 - «Вывод конфигурации RIPNG»;

- «Вывод статуса RIPNG»;
- «Отмена конфигурации маршрутизации»;
- «Отключение модуля RIPNG»;
- «Выполнение команды из корневой области видимости»;
- «Отмена команды»;
- «Заимствование информации из другого протокола маршрутизации»;
- «Тип маршрута»;
- «Метрика»;
- «Значение метрики»;
- «Фильтрация route-map для перераспределенных маршрутов»;
- «Отмена заимствования информации из другого протокола маршрутизации»;
- «IP-адрес»;
- «Установка сети»;
- «Выбор подкоманды»;
- «IP-адрес интерфейса с бит-маской»;
- «Имя интерфейса»;
- «Удаление сети»;
- «Установка пассивного интерфейса»;
- «Удаление пассивного интерфейса»;
- «Пароль»;
- «Строка пароля»;
- «Список для изменения метрики маршрута»;
- «Имя списка изменения»;
- «Входящее или исходящее направление»;
- «Входящее направление»;
- «Исходящее направление»;
- «Удаление списка для изменения метрики маршрута»;
- «Установка таймеров»;
- «Установка базового таймера»;
- «Значение таймера обновления таблицы маршрутов в секундах (по умолчанию - 30)»;

– «Таймер тайм-аута маршрутной информации в секундах (по умолчанию - 180)»;

– «Таймер сборщика мусора в секундах (по умолчанию - 120)»;

– «Выход в корневую область видимости».

3.33. Сообщения, выдаваемые модулем «root»:

– «Выход и завершение сеанса»;

– «Выход без завершения сеанса».

3.34. Сообщения, выдаваемые модулем «route_maps»:

– «Конфигурирование списка префиксов»;

– «Установка имени списка префиксов»;

– «Порядковый номер в списке»;

– «Порядковый номер»;

– «Выбор подкоманды»;

– «Установка пакетов для отклонения»;

– «Установка пакетов для пересылки»;

– «Сеть для списка префиксов»;

– «Максимальная длина префикса для сопоставления»;

– «Максимальная длина префикса»;

– «Минимальная длина префикса для сопоставления»;

– «Минимальная длина префикса»;

– «Отмена списка префиксов»;

– «Конфигурирование списка маршрутов»;

– «Имя списка маршрутов»;

– «Выбор»;

– «Определение пакетов под блокировку»;

– «Определение пакетов под пересылку»;

– «Порядковый номер»;

– «Отмена конфигурации списка маршрутов»;

– «Вывод списка маршрутов»;

– «Выполнение команды из корневой области видимости»;

– «Конфигурирование списка маршрутов»;

– «Имя списка префиксов»;

- «Отмена команды»;
- «Отмена конфигурации списка маршрутов»;
- «Установка значений в протоколе маршрутизации приемника»;
- «Удаление значений в протоколе маршрутизации приемника»;
- «Установка локального приоритета»;
- «Значение приоритета»;
- «Удаление локального приоритета»;
- «Установка веса маршрута»;
- «Значение веса»;
- «Удаление веса маршрута»;
- «Выход в корневую область видимости».

3.35. Сообщения, выдаваемые модулем «security_access»:

- «Управление доступом»;
- «Управление доступом к команде»;
- «Управление доступом к профилю»;
- «Управление доступом к журналу»;
- «Вывод настроек команды»;
- «Вывод настроек доступа к команде»;
- «Команда в двойных кавычках»;
- «Вывод настроек группы»;
- «Вывод настроек группового доступа к команде»;
- «Идентификатор группы»;
- «Вывод настроек доступа к профилю»;
- «Имя профиля»;
- «Вывод всех зарегистрированных в системе профилей»;
- «Разрешение доступа к команде»;
- «Спецификация доступа»;
- «Разрешение доступа к профилю»;
- «Разрешение доступа к журналу»;
- «Имя журнала»;
- «Вывод настроек журнала»;
- «Вывод настроек доступа к журналу»;

- «Отмена регистрации объекта»;
- «Регистрация объекта»;
- «Регистрация нового пустого профиля»;
- «Отмена регистрации профиля»;
- «Регистрация flash-носителя»;
- «Отмена регистрации flash-носителя»;
- «Номер flash-носителя»;
- «Вывод списка зарегистрированных flash-носителей»;
- «Безопасное отключение внешнего устройства»;
- «Отключение flash-носителя»;
- «Имя модуля»;
- «Имя пользователя».

3.36. Сообщения, выдаваемые модулем «session_manager»:

- «Команда вывода конфигурации»;
- «Управление сессиями»;
- «Вывод информации по сессиям»;
- «Обрыв сессии»;
- «Номер сессии».

3.37. Сообщения, выдаваемые модулем «snmp»:

- «Команда вывода конфигурации»;
- «Конфигурирование SNMP-сервера»;
- «Отмена конфигурации SNMP-сервера»;
- «Вывод информации SNMP»;
- «Вывод статуса сервера SNMP»;
- «Включение SNMP, установка строки сообщества и доступа к привилегиям»;
- «Установка опций SNMP trap»;
- «Установка режима»;
- «Включение»;
- «Выключение»;
- «Вывод настроек SNMP trap»;
- «Строка сообщества»;
- «Выбор подкоманды»;

- «Доступ только на чтение»;
- «Доступ на запись и чтение»;
- «Доступ только из конкретной сети»;
- «Удаление строки сообщества SNMP»;
- «Установка локации SNMP-сервера»;
- «Локация»;
- «Удаление локации SNMP-сервера»;
- «Установка контактного имени SNMP-сервера»;
- «Системное контактное имя»;
- «Удаление контактного имени SNMP-сервера»;
- «Установка IP-адреса источника SNMP-сервера»;
- «IP-адрес источника, который слушает SNMP-сервер»;
- «Удаление IP-адреса источника SNMP-сервера»;
- «Включение отправки SNMP-ловушек на указанный хост»;
- «IP-адрес SNMP-менеджера»;
- «Версия SNMP»;
- «Версия»;
- «Использование SNMPv1»;
- «Использование SNMPv2с»;
- «Строка сообщества»;
- «Удаление IP-адреса хоста сервера SNMP».

3.38. Сообщения, выдаваемые модулем «ssh»:

- «Конфигурация SSH»;
- «Выбор подкоманды»;
- «Разрешить указанным пользователям доступ по SSH»;
- «Запретить указанным пользователям доступ по SSH»;
- «Указать имя пользователя»;
- «Имя пользователя»;
- «Указать шаблон IP-адреса»;
- «Шаблон IP-адреса»;
- «Отмена конфигурации SSH»;
- «Включить сервис SSH»;

- «Выключить сервис SSH»;
- «Установить номер порта для SSH»;
- «Номер порта»;
- «Показать состояние сервиса SSH».

3.39. Сообщения, выдаваемые модулем «static_routes»:

- «IP-конфигурация»;
- «Установить статический маршрут»;
- «Удалить статический маршрут»;
- «Сеть назначения»;
- «Отбрасывать пакеты без уведомления»;
- «IP-адрес шлюза»;
- «Интерфейс источника»;
- «Адрес шлюза»;
- «Имя интерфейса»;
- «Административная дистанция»;
- «Дистанция»;
- «Установить IP-таблицу»;
- «IP-таблица»;
- «Установить маршрут для балансировки нагрузки»;
- «Установить шлюз следующего уровня»;
- «Удалить маршрут для балансировки нагрузки»;
- «Установить маршрут по умолчанию»;
- «Удалить маршрут по умолчанию»;
- «Шлюз»;
- «Отмена IP-конфигурации»;
- «Удалить статический маршрут»;
- «Вывод информации IPv6»;
- «Показать таблицу маршрутов»;
- «Указать адрес назначения маршрута»;
- «Все маршруты»;
- «Связанные маршруты»;
- «Статические маршруты»;

- «Маршруты ядра»;
- «Маршруты BGP»;
- «Маршруты OSPF»;
- «Маршруты RIP»;
- «Показать список IP-таблиц»;
- «Вывод сообщений из журнала»;
- «Вывод последней части журнала»;
- «Количество строк»;
- «Добавление IP-таблицы»;
- «Номер IP-таблицы»;
- «Имя IP-таблицы»;
- «Имя таблицы»;
- «Удаление IP-таблицы».

3.40. Сообщения, выдаваемые модулем «sys_profile»:

- «Изменение конфигурации»;
- «Сохранение конфигурации»;
- «Загрузка конфигурации»;
- «Проверка конфигурации»;
- «Сохранение конфигурации профиля»;
- «Имя профиля»;
- «Первый примонтированный flash-носитель»;
- «Загрузка конфигурации профиля»;
- «Загрузка конфигурации по умолчанию»;
- «Установка профиля как загружаемого при старте системы»;
- «Вывод текущей примененной конфигурации профиля»;
- «Имя модуля»;
- «Вывод текущей примененной конфигурации»;
- «Сохранение текущей примененной конфигурации»;
- «Загрузка конфигурации»;
- «Применение конфигурации»;
- «Выбор подкоманды»;
- «Полностью заверченный коммит»;

– «Полностью завершённый коммит, в противном случае выполняется откат конфигурации»;

- «Задержка (с) перед откатом конфигурации»;
- «Описание для коммита в двойных кавычках»;
- «Откат конфигурации»;
- «Сброс не применённой конфигурации»;
- «Имя модуля»;
- «Вывод изменений в конфигурации профиля»;
- «Конфигурирование системы»;
- «Вывод информации коммита»;
- «Вывод статуса коммита»;
- «Проверка параметров модуля(ей) перед выполнением коммита».

3.41. Сообщения, выдаваемые модулем «system»:

- «Конфигурация системных сервисов»;
- «Изменение конфигурации системы»;
- «Изменение имени хоста системы»;
- «Имя хоста»;
- «Отмена конфигурации системных сервисов»;
- «Перезагрузка системы»;
- «Выключение системы»;
- «Установка даты и времени»;
- «Дата и время в формате: [гггг][мм][дд][чч][мин][сек]»;
- «Изменить дату и время»;
- «Часовой пояс в формате: регион/город»;
- «Показать дату и время»;
- «Показать список доступных часовых поясов»;
- «Регион»;
- «Проверка системы»;
- «Проверка целостности»;
- «Проверка целостности неизменяемых файлов»;
- «Проверка целостности изменяемых файлов»;
- «Показать параметры контроля целостности»;

- «Показать интервал выполнения контроля целостности»;
- «Установки пользователя»;
- «Добавить нового пользователя»;
- «Группа»;
- «Имя пользователя»;
- «Установить пароль»;
- «Пароль»;
- «Установить время действия пароля (в днях)»;
- «Время действия пароля (в днях)»;
- «Редактирование пользователя»;
- «Установить e-mail адрес пользователя»;
- «E-mail адрес»;
- «Отмена установок пользователя»;
- «Удалить e-mail адрес пользователя»;
- «Удалить пользователя»;
- «Заблокировать пользователя»;
- «Разблокировать пользователя»;
- «Показать список системных пользователей»;
- «Создать учетную запись пользователя службы поддержки»;
- «Удалить учетную запись пользователя службы поддержки»;
- «Проверка целостности файла журнала»;
- «Имя файла журнала»;
- «Проверка целостности всех файлов журналов»;
- «Установить интервал выполнения контроля целостности»;
- «Интервал выполнения, с»;
- «Копировать файлы базы данных хэшей»;
- «Копировать файлы на флеш-накопитель»;
- «Администрирование системных модулей»;
- «Выбрать действие: загрузить, выгрузить или перезагрузить системный модуль»;
- «Имя модуля»;
- «Показать зарегистрированные системные модули»;

- «Сортировать модули по приоритету»;
- «Установить системную консоль»;
- «Порт TTY»;
- «Показать системную консоль»;
- «Редактировать лимиты подключений пользователей»;
- «Удалить лимиты подключений для пользователя»;
- «Ограничение одновременного входа пользователей в систему»;
- «Загрузка»;
- «Загрузка атрибутов SSL»;
- «Загрузка сертификатов SSL»;
- «Имя CA-сертификата»;
- «Сохранение»;
- «Сохранение атрибутов SSL»;
- «Сохранение сертификатов SSL»;
- «Удаление»;
- «Удаление атрибутов SSL»;
- «Удаление сертификатов SSL»;
- «Подкоманда выбора»;
- «Опция 'все'»;
- «Вывод конфигурации»;
- «Команда ping»;
- «IP-адрес»;
- «Интерфейс источника»;
- «Имя интерфейса»;
- «IP-адрес»;
- «Размер пакета»;
- «Значение размера пакета (байты)»;
- «Интервал»;
- «Значение интервала (с)»;
- «Количество повторений»;
- «Значение количества повторений»;
- «Количество пакетов ICMP»;

- «Значение количества пакетов ICMP»;
- «Интервал времени ожидания»;
- «Тип обслуживания (ToS)»;
- «Значение ToS»;
- «Конфигурация DNS»;
- «Разрешение доменного имени»;
- «Имя сервера»;
- «Вывод системной информации»;
- «Вывод информации по загрузке процессора»;
- «Вывод информации по использованию ОЗУ»;
- «Вывод версии системы»;
- «Показать имя системы»;
- «Конфигурирование почтового имени по умолчанию»;
- «Имя»;
- «Удаление почтового имени по умолчанию»;
- «Показать почтовое имя по умолчанию»;
- «Время сбора статистики»;
- «Время в секундах»;
- «Сохранение системных неизменяемых файлов»;
- «Сохранение системных неизменяемых файлов на flash-носитель»;
- «Проверка памяти»;
- «Проверка диска»;
- «Проверка ЦПУ»;
- «Интервал проверки»;
- «Отменить проверку по расписанию»;
- «Тип проверки»;
- «Тип проверки»;
- «Команда NMAP»;
- «Адрес хоста и порт».

3.42. Сообщения, выдаваемые модулем «telnet»:

- «Включение/выключение telnet-сервера»;
- «Включение telnet-сервера»;

- «Отключение telnet-сервера»;
- «Конфигурация telnet-сервера»;
- «Установить порт для telnet»;
- «Номер порта»;
- «Показать состояние сервиса telnet».

3.43. Сообщения, выдаваемые модулем «update»:

- «Установить адрес сервера обновлений»;
- «Показать адрес сервера обновлений»;
- «Адрес репозитория»;
- «Обновление базы данных доступных пакетов»;
- «Обновление системы»;
- «Откат системы к предыдущему обновлению».

3.44. Сообщения, выдаваемые модулем «vpn_client»:

- «Создание конфигурации VPN»;
- «Удаление конфигурации VPN»;
- «Конфигурация VPN-клиента»;
- «Идентификатор клиента»;
- «Удаление конфигурации VPN-клиента»;
- «Конфигурация системных сервисов»;
- «Включение/выключение VPN»;
- «Включение/выключение VPN-клиента»;
- «Подкоманда выбора»;
- «Включение VPN-клиента»;
- «Выключение VPN-клиента»;
- «Перезапуск VPN-клиента»;
- «Команда вывода конфигурации»;
- «Показать конфигурацию VPN»;
- «Показать конфигурацию VPN-клиента»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Отмена команды»;
- «Установить номер порта для клиента»;

- «Номер порта»;
- «Установить режим туннеля»;
- «Выбор команды»;
- «Использовать режим L3»;
- «Использовать режим L2»;
- «Использовать случайный номер порта»;
- «Отмена использования случайного номера порта»;
- «Включить предупреждения о попытках повторного воспроизведения»;
- «Отключить предупреждения о попытках повторного воспроизведения»;
- «Использовать случайный номер порта»;
- «Отмена использования случайного номера порта»;
- «Использовать режим TLS»;
- «Отмена использования режима TLS»;
- «Установить протокол»;
- «Установить тип аутентификации»;
- «Использовать секретный ключ»;
- «Использовать TLS»;
- «Использовать TCP»;
- «Использовать UDP»;
- «Использовать TCP (IPv6)»;
- «Использовать UDP (IPv6)»;
- «Установить IP-адрес сервера»;
- «IP-адрес сервера»;
- «Удалить IP-адрес сервера»;
- «Использовать случайный адрес сервера»;
- «Отменить использование случайного адреса сервера»;
- «Установить IP-адреса туннеля»;
- «Установить IPv6-адреса туннеля»;
- «Локальный IP-адрес»;
- «Локальный IPv6-адрес»;
- «Отмена конфигурации IP-адресов туннеля»;
- «Отмена конфигурации IPv6-адресов туннеля»;

- «Установить бесконечное время разрешения адреса сервера»;
- «Отмена конфигурации времени разрешения адреса сервера»;
- «Отключить предупреждения о попытках повторного воспроизведения»;
- «Включить предупреждения о попытках повторного воспроизведения»;
- «Установить параметры DHCP»;
- «Отмена конфигурации параметров DHCP»;
- «Параметры DHCP»;
- «Установить IP-адрес DNS-сервера»;
- «IP-адрес»;
- «Установить IP-адрес WINS-сервера»;
- «Отмена конфигурации параметров DHCP»;
- «Установить режим использования компрессии»;
- «Отменить режим использования компрессии»;
- «Проверить конфигурацию клиента»;
- «Статический ключ аутентификации»;
- «Имя файла»;
- «CA-сертификат»;
- «Сертификат клиента»;
- «Ключ клиента»;
- «DN-ключ».

3.45. Сообщения, выдаваемые модулем «vpn_server»:

- «Создание конфигурации VPN»;
- «Удаление конфигурации VPN»;
- «Конфигурация VPN-сервера»;
- «Конфигурация системных сервисов»;
- «Включение/выключение VPN»;
- «Включение/выключение VPN-сервера»;
- «Подкоманда выбора»;
- «Запуск VPN-сервера»;
- «Остановка VPN-сервера»;
- «Отключение VPN-сервера»;
- «Перезапуск VPN-сервера»;

- «Удаление конфигурации VPN-сервера»;
- «Показать конфигурацию VPN»;
- «Показать конфигурацию VPN-сервера»;
- «Выполнение команды из корневой области видимости»;
- «Выход в корневую область видимости»;
- «Отмена команды»;
- «Установить режим туннеля»;
- «Выбор команды»;
- «Использовать режим L3»;
- «Использовать режим L2»;
- «Установить протокол»;
- «Установить тип аутентификации»;
- «Использовать секретный ключ»;
- «Использовать TLS»;
- «Использовать TCP»;
- «Использовать UDP»;
- «Использовать UDP (IPv6)»;
- «Использовать TCP (IPv6)»;
- «Установить номер порта для сервера»;
- «Номер порта»;
- «Установить IP-адреса туннеля»;
- «Установить IPv6-адреса туннеля»;
- «Локальный IP-адрес»;
- «Локальный IPv6-адрес»;
- «Отмена конфигурации IP-адреса туннеля»;
- «Отмена конфигурации IPv6-адреса туннеля»;
- «Установить пул адресов сервера (режим tun)»;
- «Установить пул адресов сервера (IPv6, tun mode)»;
- «IP-адрес сервера»;
- «Отмена конфигурации пула адресов сервера (режим tun)»;
- «Отмена конфигурации пула адресов сервера (IPv6, tun mode)»;
- «Разрешить соединения между клиентами»;

- «Запретить соединения между клиентами»;
- «IP-конфигурация»;
- «Отмена IP-конфигурации»;
- «Добавить маршрут после установки соединения»;
- «Добавить маршрут после установки соединения (IPv6)»;
- «Адрес сети»;
- «Адрес сети (IPv6)»;
- «Адрес сети с битовой маской»;
- «Отмена добавления маршрута после установки соединения»;
- «Отмена добавления маршрута после установки соединения (IPv6)»;
- «Добавить маршрут на сеть клиента»;
- «Добавить маршрут на сеть клиента (IPv6)»;
- «Имя клиента»;
- «Отмена добавления маршрута на сеть клиента»;
- «Отмена добавления маршрута на сеть клиента (IPv6)»;
- «Отправить настройки клиенту»;
- «Отмена отправки настроек клиенту»;
- «Отправить настройки клиенту»;
- «Игнорировать глобальные настройки для клиентов»;
- «Отправить настройки клиенту»;
- «Отправить настройки всем клиентам»;
- «Отмена отправки настроек всем клиентам»;
- «Установить режим использования компрессии»;
- «Отменить режим использования компрессии»;
- «Установить тайм-ауты поддержки активности»;
- «Время ожидания ответа Ping»;
- «Максимальное время простоя»;
- «Отмена конфигурации тайм-аутов поддержки активности»;
- «Установить максимальное число клиентов»;
- «Максимальное число клиентов»;
- «Отмена конфигурации максимального числа клиентов»;
- «Проверить конфигурацию сервера»;

- «Статический ключ аутентификации»;
- «Имя файла»;
- «СА-сертификат»;
- «Сертификат сервера»;
- «Ключ сервера»;
- «DN-ключ»;
- «Генерация»;
- «Генерация статического ключа»;
- «Имя файла».

3.46. Сообщения, выдаваемые модулем «vrrp»:

- «Создание интерфейса»;
- «Удаление интерфейса»;
- «Создание экземпляра VRRP»;
- «Наименование экземпляра»;
- «Удаление экземпляра VRRP»;
- «Управление службой VRRP»;
- «Подкоманда switch»;
- «Включение VRRP»;
- «Отключение VRRP»;
- «Отображение конфигурации VRRP»;
- «Идентификатор клиента»;
- «Выполнение команды из корневой области видимости»;
- «Отмена команды»;
- «Укажите используемый интерфейс»;
- «Имя интерфейса»;
- «Удалить используемый интерфейс»;
- «Установить режим вытеснения»;
- «Отменить режим вытеснения»;
- «Установить режим приема»;
- «Отменить режим приема»;
- «Установить приоритет»;
- «Значение приоритета»;

- «Установить значение приоритета по умолчанию»;
- «Настроить виртуальный маршрутизатор»;
- «Удалить виртуальный маршрутизатор»;
- «Установить виртуальный IP-адрес»;
- «IP-адрес»;
- «Удалить виртуальный IP-адрес»;
- «Установить идентификатор виртуального маршрутизатора»;
- «Идентификатор виртуального маршрутизатора»;
- «Удалить идентификатор виртуального маршрутизатора»;
- «Установить интервал рассылки извещений»;
- «Интервал в секундах»;
- «Установить интервал рассылки по умолчанию»;
- «Установить интервал простоя»;
- «Установить интервал простоя по умолчанию»;
- «Включить данную конфигурацию»;
- «Выключить данную конфигурацию»;
- «Выход в корневую область видимости»;
- «Добавление интерфейса в список мониторинга состояния»;
- «Удаление интерфейса из списка мониторинга состояния».

Перечень принятых сокращений

АА	– администратор аудита
АБ	– администратор безопасности
АС	– администратор сети
CLI	– Command Line Interface (интерфейс командной строки)

