СЕРВИСНЫЙ МАРШРУТИЗАТОР СЕРИИ ISN415
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СЕРВИСНЫЙ МАРШРУТИЗАТОР CS
РУКОВОДСТВО СИСТЕМНОГО ПРОГРАММИСТА
ВЕРСИЯ ПО 3.24.05

Содержание

Аннотация **5**

История изменений документа **6**

1. Общие сведения о программе **7**

2. Требования к техническим и программным средствам **10**

3. Структура программы **11**

4. Установка программ **13**

5. Управление пользователями **14**

5.1. Создание группы **14**

5.2. Создание пользователя **15**

5.3. Корректировка группы **16**

5.4. Корректировка пользователя **16**

5.5. Удаление группы **17**

5.6. Удаление пользователя **18**

6. Работа с профилями программы **19**

6.1. Загрузка профиля **19**

6.2. Сброс настроек **19**

6.3. Сохранение профиля **20**

6.4. Создание нового профиля **20**

6.5. Удаление профиля **20**

6.6. Сохранение профиля 20

6.7. Сохранение профиля на USB-носитель 21

6.8. Сохранение профиля на сетевом хранилище 21

6.9. Копирование профиля на СМ 22

6.10. Копирование профиля из сетевого хранилища 22

6.11. Выбор автоматически загружаемого профиля 22

6.12. Просмотр профилей 23

7. Настройка параметров программы 24

7.1. Настройка параметров времени и даты 24

7.2. Настройка тайм-аутов 25

7.3. Наименование хоста ip-адреса 27

7.4. Указания хоста и доменного имени 28

7.5. Настройка SSH 28

7.6. Настройки SSH VRF 31

7.7. Настройка Telnet-сервера 37

7.8. Настройка Telnet-сервера на VRF 40

7.9. Настройки Telnet-клиента 43

7.10. Настройка TFTP сервера 44

8. Дополнительные возможности 46

9. Обновление программы 47

9.1. Обновление ПО СМ с помощью USB-носителя 47

9.2. Обновление ПО СМ с помощью FTP сервера 50

9.3. Обновление программного обеспечения U-boot и BMC 52

9.4. Сброс к заводским настройкам 53

Перечень условных обозначений и сокращений 55

Приложение 1 Подготовка автоматизированного рабочего места 57

Приложение 2 Удаленное подключение к сервисному маршрутизатору 59

Техническая поддержка 65

Аннотация

Данный документ является руководством системного программиста программного обеспечения сервисного маршрутизатора CS (далее по тексту – ПО СМ), предназначенного для организации и предоставления функций коммутации и маршрутизации трафика.

Данный документ описывает общие сведения, структуру, настройки, проверки, дополнительные возможности и сообщения системному программисту ПО СМ.

Данный документ разработан под версию ПО СМ 3.24.05 от 20.09.2024, работа ПО СМ в более ранних версиях может отличаться от текущей.

Настоящий документ входит в состав программной документации на изделие и рассчитан на пользователя, имеющего навыки работы на персональной электронной вычислительной машине (ПЭВМ) в операционной системе (ОС) Linux, Windows и знающий основы сетевого администрирования.

Для наглядности в тексте настоящего руководства используются различные стили оформления.

Области применения стилей указаны в таблице 1.

Таблица 1 – Стили оформления в документе

Стиль оформления	Область применения	Пример
Полужирный шрифт Arial	Выделяет примеры синтаксиса команд	**configure terminal**
Шрифт Consolas	Выделяет вывод CLI	`Name  #  Rule` `100   1   src: 192.168.1.1/32`

История изменений документа

Версия документа	Дата выпуска	Внесены изменения	Версия ПО
Версия 10.0	01.10.2024		3.24.05
Версия 9.0	20.09.2024		3.24.04
Версия 8.0	03.07.2024		3.24.00
Версия 7.0	04.04.2024		3.23.00
Версия 6.0	31.01.2024		3.22.02
Версия 5.0	05.10.2023		3.21.68-09
Версия 4.0	30.06.2022		3.21.68-09
Версия 3.0	30.12.2021		3.21.68-08
Версия 2.0	20.12.2021		
Версия 1.0	17.06.2021		

1. Общие сведения о программе

ПО СМ предназначено для обеспечения функций коммутации и маршрутизации трафика.

ПО СМ обеспечивает функционирование по протоколу IPv4 (RFC 791).

ПО СМ обеспечивает функционирование по протоколу IPv6 (RFC 2460).

ПО СМ обеспечивает обработку Jumbo Frames (кадров размером до 1900 байт) на всех интерфейсах Ethernet.

ПО СМ обеспечивает назначение статических IP-адресов своим интерфейсам.

ПО СМ обеспечивает одноадресную статическую маршрутизацию IP-пакетов.

ПО СМ поддерживает одноадресную динамическую маршрутизацию по протоколам RIP, RIPng, OSPF, IS-IS, BGP.

ПО СМ поддерживает агрегацию портов с помощью LACP.

ПО СМ обеспечивает перераспределение маршрутной информации:

- между протоколами динамической маршрутизации;
- статических маршрутов в протоколы динамической маршрутизации.

ПО СМ поддерживает маршрутизацию на основе политик (Policy routing):

- на основе IP адреса источника;
- на основе номера порта источника и назначения.

ПО СМ поддерживает балансировку нагрузки при наличии нескольких маршрутов с одинаковой метрикой.

ПО СМ поддерживает протоколы увеличения доступности шлюза VRRP и CARP.

ПО СМ поддерживает протокол обнаружения проблем связности BFD.

ПО СМ обеспечивает быструю сходимость протоколов динамической маршрутизации с помощью протокола BFD.

ПО СМ обеспечивает обнаружение доступности следующего транзитного участка для статических маршрутов с помощью протокола BFD.

ПО СМ поддерживает динамическое конфигурирование сетевых настроек на узлах в качестве DHCP-сервера.

ПО СМ поддерживает работу в качестве DNS-сервера, DNS-клиента, DNS-proxy.

ПО СМ поддерживает протокол синхронизации времени NTP.

ПО СМ поддерживает многоадресную динамическую маршрутизацию по протоколам IGMP, PIM.

ПО СМ поддерживает протокол учета сетевого трафика Netflow.

ПО СМ поддерживает протокол сетевого управления SNMP.

ПО СМ поддерживает механизм IP SLA.

ПО СМ поддерживает сетевую систему обнаружения и предотвращения вторжений SNORT, способную выполнять регистрацию пакетов и осуществлять глубокий анализ трафика.

ПО СМ поддерживает многопротокольную коммутацию по MPLS меткам (Multiprotocol label switching) RFC 3031.

ПО СМ поддерживает технологию виртуальной маршрутизации и переадресации (Virtual Routing and Forwarding (VRF)).

ПО СМ поддерживает преобразование сетевых адресов NAT.

ПО СМ обеспечивает базовые концепции трансляции сетевых адресов:

- статическая (Static Network Address Translation);
- динамическая (Dynamic Address Translation);
- маскарадная (NAPT, NAT Overload, PAT).

ПО СМ поддерживает следующие методы обеспечения качества обслуживания в сетях: FIFO, PQ, CBQ, WFQ, HFSC, RED, GRED, HTB, RIO, SFQ, TBF, WRR, INPUT, WRED.

ПО СМ поддерживает использование иерархических дисциплин QoS.

ПО СМ поддерживает технологию создания виртуальных частных сетей DMVPN.

ПО СМ поддерживает протоколы OpenVPN и IPSec.

ПО СМ поддерживает функцию туннелирования по протоколам: PPPoE, PPTP, IPIP, GRE, L2TP.

ПО СМ обеспечивает фильтрацию трафика по следующим полям:

- порт (TCP/UDP) отправителя;
- порт (TCP/UDP) получателя;
- IP-адрес отправителя;
- IP-адрес получателя;
- MAC-адрес отправителя;
- флаги заголовка сегмента TCP;
- значение поля «Протокол» заголовка IP;
- значение поля «ToS» (TOS/DSCP) заголовка IP.

ПО СМ поддерживает журналирование Syslog.

ПО СМ поддерживает следующие виды управления:

- локальное через интерфейс командной строки (CLI);
- удаленное по протоколу ssh;
- удаленное по протоколу Telnet.

ПО СМ обеспечивает корректность задаваемых параметров функционирования.

ПО СМ обеспечивает механизмы идентификации и аутентификации, использующиеся при входе в систему управления изделием.

ПО СМ поддерживает удаленную аутентификацию/авторизацию по протоколу RADIUS и обеспечивает функционирование в качестве клиента.

ПО СМ поддерживает аутентификацию/авторизацию/учет по протоколу TACACS+.

ПО СМ поддерживает задание учетных записей администратора/оператора и их паролей.

ПО СМ поддерживает следующие виды обновления:

- локальное (с внутреннего/внешнего накопителя);
- удаленное (по протоколам TFTP, FTP).

ПО СМ обеспечивает сохранение сконфигурированных профилей.

ПО СМ обеспечивает вывод перечня имеющихся в системе профилей, их просмотр, а также их копирование на внешний носитель.

ПО СМ обеспечивает сброс к заводским настройкам.

ПО СМ поддерживает взаимодействие с коммутационным чипом Marvell Link Street 88E6390X (далее – модуль коммутации).

ПО СМ поддерживает конфигурирование следующих параметров модуля коммутации:

- включение/выключение портов модуля;

- скорость портов и режим передачи;
- автосогласование;
- параметры тегирования кадров (VLAN-трафик);
- STP-состояние портов;
- параметры режима обучения и заполнения таблиц коммутации;
- создание/изменение/удаление записей в таблицах коммутации.

ПО СМ обеспечивает получение информации о текущем состоянии модуля коммутации:

- конфигурация и статус портов модуля коммутации;
- STP-состояние интерфейсов;
- состояние таблиц коммутации;
- значения счетчиков кадров на портах.

ПО СМ поддерживает следующие служебные протоколы второго уровня:

- STP;
- RSTP;
- MSTP;
- LLDP.

ПО СМ поддерживает встроенные утилиты - iperf, tcpdump, ping, traceroute.

ПО СМ поддерживает зеркалирование передаваемого трафика.

ПО СМ поддерживает мониторинг: процессора, памяти, температуры, системы охлаждения, состояния SSD диска.

ПО СМ поддерживает режим файлового сервера.

ПО СМ поддерживает работу 3G/4G/LTE модемов.

2. Требования к техническим и программным средствам

Минимальные условия, выдвигаемые к аппаратной платформе, необходимые для выполнения ПО СМ:

- аппаратная платформа на базе процессора Baikal-T1;
- оперативная память: 2 ГБ;
- постоянное запоминающее устройство: 16 ГБ.

3. Структура программы

Структурная схема ПО СМ представлена на рисунке 1.

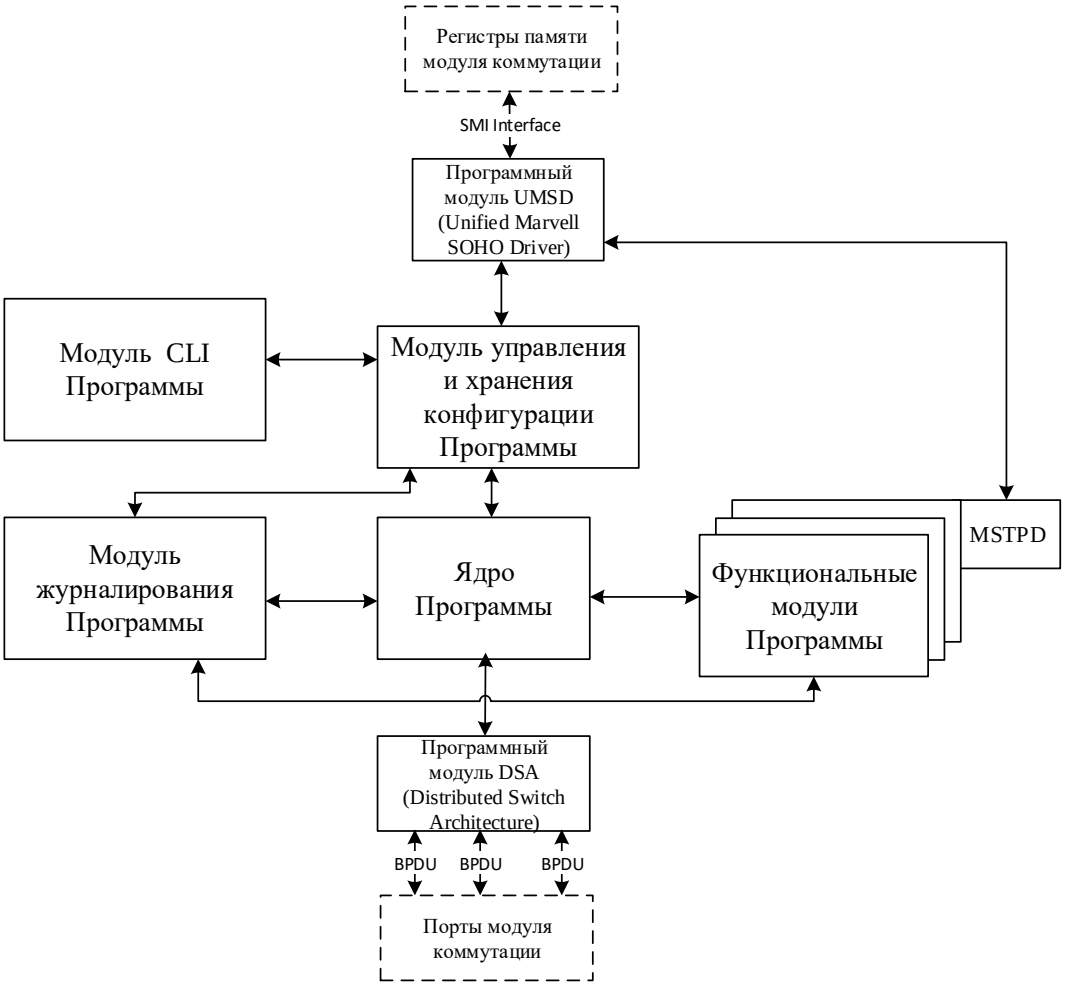

Рисунок 1 – Структурная схема ПО СМ

ПО СМ функционально подразделяется на следующие составные части:

- ядро ПО СМ, отвечающее за взаимодействие с драйверами устройства, обработку сетевых пакетов;
- функциональные модули ПО СМ, отвечающие за функциональные возможности программы (протоколы, технологии);
- модуль управления и хранения конфигураций ПО СМ, отвечающий за настройку функциональных модулей по поступившим в модуль командам и синхронизацию функционирования разных модулей;
- модуль журналирования ПО СМ, отвечающий за протоколирование различных действий/событий составных частей ПО СМ;
- модуль ПО СМ CLI (Command Line Interface), отвечающий за интерфейс «человек-программа»;
- модуль DSA – отвечает за проецирование физических интерфейсов модуля коммутации в ядро. Отвечает за передачу служебных пакетов BPDU для поддержки работы механизмов предотвращения петель внутри одной подсети

(семейство протоколов распределенного связующего дерева xSTP) и служебных сообщений протокола LLDP;

- программный модуль UMSD (Unified Marvell SOHO Driver) – отвечает за чтение и запись данных в регистры памяти модуля коммутации.

Взаимодействия ПО СМ с другими программами не предусмотрено.

4. Установка программ

Установка ПО СМ осуществляется в соответствии с указаниями инструкции по установке RU.07622667.00004-01 91 01.

5. Управление пользователями

> ⚠ Внимание!
>
> По умолчанию на маршрутизаторе создан пользователь с правами администратора и логином «admin», паролем «admin». В целях безопасности пароль необходимо заменить!

Создание, корректировку и удаление пользователей может производить пользователь с уровнем привилегий 14 и более.

5.1. Создание группы

Для создания группы осуществите вход в настройки конфигурации ПО СМ (см. рисунок 2), выполнив команду:

configure terminal

```
admin@sr-be# configure terminal
admin@sr-be(config)#
```

Рисунок 2 – Настройки конфигурации

Для создания новой группы (см. рисунок 3), выполните команду:

group <groupname> privilege <privilegelevel>

```
admin@sr-be(config)# group other privilege 5
admin@sr-be(config)#
```

Рисунок 3 – Создание новой группы

где:

- <groupname> – наименование группы;
- <privilegelevel> – уровень привилегий группы.

Убедитесь в создании новой группы вызвав просмотр существующих групп (см. рисунок 4), выполнив команду:

show groups

```
admin@sr-be# show groups
  Group   | Privilege
----------------------
 admin    | 15
 service  | 1
 other    | 5
admin@sr-be#
```

Рисунок 4 – Просмотр групп

5.2. Создание пользователя

Для создания пользователя осуществите вход в настройки конфигурации ПО СМ (см. рисунок 2), выполнив команду:

configure terminal

Для создания нового пользователя (см. рисунок 5), выполните команду:

username add <username> group <usergroup>

```
admin@sr-be(config)# username add manager_one group other
```

Рисунок 5 – Создание нового пользователя

где:

- <username> – наименование пользователя;
- <usergroup> – наименование существующей группы, куда будет добавлен пользователь.

Задайте пароль для нового пользователя, придумайте последовательность символов и дважды введите ее (см. рисунок 6).

```
admin@sr-be(config)# username add manager_one group other
Enter password:
Repeat password:
admin@sr-be(config)#
```

Рисунок 6 – Установка пароля

> **Примечание**
>
> При вводе пароля символы на экране не отображаются

Убедитесь в создании нового пользователя, вызвав просмотр существующих пользователей (см. рисунок 7), выполнив команду:

show users

```
admin@sr-be(config)# show users
     User    |   Group  |  Type   | Privilege
-----------------------------------------------
 admin       |   admin  |  local  | 15
 manager_one |   other  |  local  | 5
admin@sr-be(config)#
```

Рисунок 7 – Просмотр пользователей

5.3. Корректировка группы

Для корректировки группы осуществите вход в настройки конфигурации ПО СМ (см. рисунок 2), выполнив команду:

configure terminal

Для корректировки уровня привилегий группы (см. рисунок 3), выполните команду:

group <groupname> privilege <privilegelevel>

где:

- <groupname> – наименование группы;
- <privilegelevel> – уровень привилегий группы.

5.4. Корректировка пользователя

Для корректировки пользователя осуществите вход в настройки конфигурации ПО СМ (см. рисунок 2), выполнив команду:

configure terminal

Корректировка пользователя выполняется с помощью ключевого слова «edit» и предоставляет следующие вариации:

- изменение группы вхождения пользователя (см. рисунок 8), выполнив команду:

username edit <username> group <groupname>

```
admin@sr-be(config)# username edit manager_one group admin
```

Рисунок 8 – Изменение группы пользователя

где:

- <username> – наименование пользователя;
- <groupname> – наименование существующей группы, куда будет перенесен пользователь.

○ изменение пароля пользователя (см. рисунок 9), выполнив команду:

username edit <username> password

```
admin@sr-be(config)# username edit manager_one password
```

Рисунок 9 – Изменение пароля пользователя

где <username> – наименование пользователя.

Задайте новый пароль для пользователя, придумайте последовательность символов и дважды введите ее (см. рисунок 6).

> Примечание
>
> При вводе пароля символы на экране не отображаются

5.5. Удаление группы

Для удаления группы осуществите вход в настройки конфигурации ПО СМ (см. рисунок 2), выполнив команду:

configure terminal

Предварительно удалите из группы всех участников согласно 5.6 настоящего руководства.

Для удаления группы (см. рисунок 10), выполните команду:

no group <groupname>

```
admin@sr-be(config)# no group other
```

Рисунок 10 – Удаление группы

где <groupname> – наименование группы.

Убедитесь в удалении группы вызвав просмотр существующих групп (см. рисунок 4), выполнив команду:

show groups

5.6. Удаление пользователя

Для удаления пользователя осуществите вход в настройки конфигурации ПО СМ (см. рисунок 2), выполнив команду:

configure terminal

Для удаления пользователя (см. рисунок 11), выполните команду:

no username <username>

```
admin@sr-be(config)# no username manager_one
```

Рисунок 11 – Удаление пользователя

где <username> – наименование пользователя.

Убедитесь в удалении пользователя вызвав просмотр существующих пользователей (см. рисунок 7), выполнив команду:

show users

6. Работа с профилями программы

Для хранения настроек подключения, маршрутизации и интерфейсов в ПО СМ используются профили. Описание их создания, изменения, удаления, а также загрузки и выгрузки приведено в этом разделе.

> **Примечание**
>
> При загрузке нового профиля все изменения, которые были проведены без последующего сохранения профиля теряются.

Создание, корректировку и удаление, а также загрузка и выгрузка профилей может производить пользователь с уровнем привилегий 14 и более.

6.1. Загрузка профиля

Для загрузки профиля (см. рисунок 12), выполните команду:

load <profilename>

```
admin@sr-be# load startup
```

Рисунок 12 – Загрузка профиля

где <profilename> – наименование профиля.

6.2. Сброс настроек

Для сброса настроек профиля (см. рисунок 13), выполните команду:

load null

```
admin@sr-be# load null
```

Рисунок 13 – Сброс настроек

Подтвердите свое решение о сбросе настроек (см. рисунок 14), введя в консоль:

yes

```
admin@sr-be# load null
Do you really want to load null config? (yes/no)
Yes
```

Рисунок 14 – Подтверждение сброса настроек

6.3. Сохранение профиля

Для сохранения настроек профиля (см. рисунок 15), выполните команду:

write <profilename> comment “<profilecomment>”

```
admin@sr-be# write second-profile comment “add new settings from ftp”
```

Рисунок 15 – Сохранение профиля

где:

- <profilename> – наименование профиля;
- <profilecomment> – небольшое словесное описание профиля, оставляемое пользователем по желанию.

6.4. Создание нового профиля

Создание нового профиля происходит аналогично 6.3, в команде <profilename> необходимо ввести новое наименование.

6.5. Удаление профиля

Для удаления профиля (см. рисунок 16), выполните команду:

no profile <profilename>

```
admin@sr-be# no profile second-profile
```

Рисунок 16 – Удаление профиля

где <profilename> – наименование профиля.

6.6. Сохранение профиля

Для сохранения копии профиля на сервисном маршрутизаторе CS (далее по тексту – СМ) (см. рисунок 17), выполните команду:

copy profile <profilename> path <path>

```
admin@sr-be# copy profile other path home/service/tftp
```

Рисунок 17 – Сохранение профиля на СМ

где:

- <profilename> – наименование профиля;
- <path> – путь, куда будет записан профиль.

6.7. Сохранение профиля на USB-носитель

Подключите USB-носитель к разъему USB1 на лицевой панели СМ.
Для сохранения профиля на USB-носитель (см. рисунок 18), выполните команду:

copy profile <configname> to flash <devname> <dirname>

```
admin@sr-be# copy profile other to flash /media/usb0 /media/usb0/2
```

Рисунок 18 – Сохранение профиля на USB-носителе

где:

- <configname> – наименование профиля;
- <devname> – имя устройства;
- <dirname> – путь, куда будет записан профиль.

6.8. Сохранение профиля на сетевом хранилище

Для сохранения профиля на сетевом хранилище (см. рисунок 19), выполните команду:

copy profile <configname> to url <type> <client_ip> remotedir <remote_dir>

```
admin@sr-be# copy profile other to url ftp 2.2.2.2 remotedir ftp
```

Рисунок 19 – Сохранение профиля на сетевом хранилище

где:

- <configname> – наименование профиля;
- <url> – универсальный указатель ресурса;
- <type> – тип сетевого хранилища, возможные варианты: ftp, sftp, tftp;
- <client_ip> – IP адрес сетевого хранилища;
- <remote_dir> – каталог на сетевом хранилище.

6.9. Копирование профиля на СМ

Для копирования профиля на СМ (см. рисунок 20), выполните команду:

copy profile <configname> from flash <devname> <dirname>

```
copy profile other from flash /media/usb0 /media/usb0/2
```

Рисунок 20 – Копирование профиля на СМ

где:

- <configname> – наименование профиля;
- <devname> – имя устройства;
- <dirname> – путь, куда будет записан профиль.

6.10. Копирование профиля из сетевого хранилища

Для копирования профиля из сетевого хранилища (см. рисунок 21), выполните команду:

copy profile <configname> from url <type> <client_ip> remotedir <remote_dir>

```
copy profile other from url ftp 1.1.1.1 remotedir ftp
```

Рисунок 21 – Копирование профиля из сетевого хранилища

где:

- <configname> – наименование профиля;
- <url> – универсальный указатель ресурса;
- <type> – тип сетевого хранилища, возможные варианты: ftp, sftp, tftp;
- <client_ip> – IP адрес сетевого хранилища;
- <remote_dir> – каталог на сетевом хранилище.

6.11. Выбор автоматически загружаемого профиля

Для выбора загрузочного профиля (см. рисунок 22), выполните команду:

startup-profile <profilename>

```
admin@sr-be# startup-profile newstartup
```

Рисунок 22 – Выбор автоматически загружаемого профиля

где <profilename> – наименование профиля.

Для сохранения настроек текущего профиля в загрузочный (см. рисунок 23), выполните команду:

write startup comment “<profilecomment>”

```
admin@sr-be# write startup comment “new start profile”
```

Рисунок 23 – Настройки автоматически загружаемого профиля

где <profilecomment> – небольшое словесное описание профиля, оставляемое пользователем по желанию.

6.12. Просмотр профилей

Для просмотра профилей установленных на устройстве (см. рисунок 24), выполните команду:

show profiles

```
admin@sr-be# show profiles
Flags: b – boot profile, l – last loaded profile, m – profile was modifiled was
modified or corrupted
| Flags | Profile Name | Comment     |
-------------------------------------
|       | other        | new profile |
| blm   | startup      |             |

admin@sr-be#
```

Рисунок 24 – Просмотр профилей

7. Настройка параметров программы

Настройки параметров SSH, SSH VRF, Telnet, Telnet VRF, TFTP, времени и даты, тайм-аутов, хостов и домена может производить пользователь с уровнем привилегий 14 и более.

7.1. Настройка параметров времени и даты

Для настройки параметров времени и даты осуществите вход в настройки конфигурации ПО СМ (см. рисунок 25), выполнив команду:

configure terminal

```
admin@sr-be# configure terminal
admin@sr-be(config)#
```

Рисунок 25 – Настройки конфигурации

Для настройки текущей даты (см. рисунок 26), выполните команду:

system clock date <currentdate>

```
admin@sr-be(config)# system clock date 08.08.2023
```

Рисунок 26 – Настройки текущей даты

где <currentdate> – текущая дата в формате ДД.ММ.ГГГГ.

Для настройки текущего времени (см. рисунок 27), выполните команду:

system clock time <currenttime>

```
admin@sr-be(config)# system clock time 14:46:37
```

Рисунок 27 – Настройки текущего времени

где <currenttime> – текущее время в формате ЧЧ:ММ:СС.

Для настройки часового пояса (см. рисунок 28), выполните команду:

system clock timezone <currenttimezone>

```
admin@sr-be(config)# system clock timezone Europe
```

Рисунок 28 – Настройка часового пояса

где <currenttimezone> – наименование страны или континента с текущим часовым поясом.

> Примечание
>
> Для получения списка возможных наименований:
> - введите команду system clock timezone и нажмите клавишу «?»;
> - нажмите клавишу «Tab», на экране отобразится список возможных наименований.

Для синхронизации параметров времени и даты с сервером (см. рисунок 29), выполните команду:

system clock synchronize <server>

```
admin@sr-be(config)# system clock synchronize time-server
```

Рисунок 29 – Синхронизация времени и даты

где <server> – IPv4 адрес, либо имя сервера.

Для просмотра установленной на СМ даты и времени (см. рисунок 30), выполните команду:

show clock

```
admin@sr-be(config)# show clock
Sun 12 Apr 2015 12:09:25 PM MSK
admin@sr-be(config)#
```

Рисунок 30 – Просмотр текущей даты и времени

7.2. Настройка тайм-аутов

Тайм-аут – время, которое пользователь может оставаться неактивным, после чего он будет отключен фоновой службой.

Для изменения времени тайм-аутов осуществите вход в настройки конфигурации ПО СМ (см. рисунок 25), выполнив команду:

configure terminal

Для изменения тайм-аута неактивности пользователя при работе в консоли, подключенной по SSH (см. рисунок 31), выполните команду:

system ssh timeout <timeoutseconds>

```
admin@sr-be(config)# system ssh timeout 3000
```

Рисунок 31 – Изменения тайм-аута при подключении по SSH

где <timeoutseconds> – значение времени в секундах.

Для установки тайм-аута неактивности пользователя при работе в консоли, подключенной по Telnet (см. рисунок 32), выполните команду:

system telnet timeout <timeoutseconds>

```
admin@sr-be(config)# system telnet timeout 3000
```

Рисунок 32 – Изменения тайм-аута при подключении по Telnet

где <timeoutseconds> – значение времени в секундах.

Для установки тайм-аута неактивности пользователя при работе в консоли, подключенной по COM-порту (см. рисунок 33), выполните команду:

system tty timeout <timeoutseconds>

```
admin@sr-be(config)# system tty timeout 3000
```

Рисунок 33 – Изменения тайм-аута при подключении по COM-порту

где <timeoutseconds> – значение времени в секундах.

Для установки тайм-аута неактивности пользователя при работе в веб-приложении (см. рисунок 34), выполните команду:

system web timeout <timeoutseconds>

```
admin@sr-be(config)# system web timeout 3000
```

Рисунок 34 – Изменения тайм-аута при работе в веб-приложении

где <timeoutseconds> – значение времени в секундах.

Для просмотра установленного времени различных тайм-аутов (см. рисунок 35), выполните команду:

show timeout

```
admin@sr-be(config)# show timeout
CLI inactivity timeout (sec):
 Console: 3000
 SSH:     3000
 Telnet:  3000
 web:     3000

admin@sr-be(config)#
```

Рисунок 35 – Просмотра тайм-аутов

7.3. Наименование хоста ip-адреса

Для добавления или удаления наименований хостов осуществите вход в настройки конфигурации ПО СМ (см. рисунок 25), выполнив команду:

configure terminal

Для добавления имени хосту определенного ip-адреса (см. рисунок 36), выполните команду:

ip host <hostname> <ip>

```
admin@sr-be(config)# ip host myhost 255.255.255.1
```

Рисунок 36 – Добавление имени хоста

где:

- <hostname> – устанавливаемое имя хоста;
- <ip> – ip-адрес в формате X.X.X.X – для IPv4; X:X::X:X – для IPv6.

Для удаления имени хоста определенного ip-адреса (см. рисунок 37), выполните команду:

no ip host <hostname>

```
admin@sr-be(config)# no ip host ip4-host
```

Рисунок 37 – Удаление имени хоста

где <hostname> – устанавливаемое имя хоста.

Для просмотра наименований хостов (см. рисунок 38), выполните команду:

show hosts

```
admin@sr-be(config)# show hosts
127.0.0.1     localhost
127.0.0.1             sr-be
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


admin@sr-be(config)#
```

Рисунок 38 – Просмотр наименований хостов

7.4. Указания хоста и доменного имени

Для создания или изменения хоста и доменного имени (см. рисунок 39), выполните команду:

system host-name <hostname> domain-name <domainname>

```
admin@sr-be(config)# system host-name myhost domain-name wk
admin@myhost(config)#
```

Рисунок 39 – Указания имени хоста и доменного имени

где:

- <hostname> – устанавливаемое имя хоста;
- <domainname> – устанавливаемое имя домена.

7.5. Настройка SSH

Для настройки SSH осуществите вход в настройки конфигурации ПО СМ (см. рисунок 25), выполнив команду:

configure terminal

Для изменения активности SSH (см. рисунок 40), выполните команду:

system ssh <changestatus>

```
admin@sr-be(config)# system ssh on
```

Рисунок 40 – Изменение активности SSH сервера

где <changestatus> – указание состояния SSH, может быть on или off.

Для установки номера SSH порта (см. рисунок 41), выполните команду:

system ssh port <sshport>

```
admin@sr-be(config)# system ssh port 2649
```

Рисунок 41 – Установки номера SSH порта

где <sshport> – номер SSH порта, обозначается числом от 1 до 65535.

Для установки адреса SSH порта (см. рисунок 42), выполните команду:

system ssh listen-address <sshaddresses>

```
admin@sr-be(config)# system ssh listen-address 255.255.255.1
```

Рисунок 42 – Установки адреса SSH порта

где <sshaddresses> – адрес SSH порта, вводится в виде X.X.X.X.

Для управления списком доступа (см. рисунок 43), выполните команду:

system ssh whitelist <networks>

```
admin@sr-be(config)# system ssh whitelist 255.255.255.1/20
```

Рисунок 43 – Указания списка доступа SSH

где <networks> – список сетей X.X.X.X/X.

Для настройки повторного подключение при разрыве соединения (см. рисунок 44), выполните команду:

system ssh limit period-time <periodvalue> count <countvalue>

```
admin@sr-be(config)# system ssh limit period-time 60 count 100
```

Рисунок 44 – Ограничения периода времени

где:

- <periodvalue> – значение периода в секундах;
- <countvalue> – устанавливает количество попыток подключения.

Для настройки генерации нового сервисного ключа (см. рисунок 45), выполните команду:

system ssh key generate <keytype> modulus <keylength>

```
admin@sr-be(config)# system ssh key generate rsa modulus 256
```

Рисунок 45 – Настройки генерации нового сервисного ключа

где:

- <keytype> – тип генерируемого ключа, возможные варианты: rsa, dsa, ecdsa, ed25519;
- <keylength> – длина ключа в битах, возможные варианты: 256, 384, 512, 768, 1024, 2048, 4069, 8192.

Для добавления публичного ключа (см. рисунок 46), выполните команду:

system ssh public-key username <username> key-string <stringvalue>

```
admin@sr-be(config)# system ssh public-key username user01 key-string ssh01
```

Рисунок 46 – Добавление публичного ключа

где:

- <username> – имя пользователя;
- <stringvalue> – строка с публичным ключом.

Для просмотра настроек SSH (см. рисунок 47), выполните команду:

show system ssh

```
admin@sr-be(config)# show system ssh

SSH server enabled
 Version: 2
 Port: 2649
 Listen addresses:
  255.255.255.1
 Whitelist:
  255.255.255.1/20
admin@sr-be(config)#
```

Рисунок 47 – Просмотр настроек SSH

7.6. Настройки SSH VRF

Для настройки SSH VRF осуществите вход в настройки конфигурации ПО СМ (см. рисунок 25), выполнив команду:

configure terminal

Для изменения активности SSH VRF (см. рисунок 48), выполните команду:

system ssh vrf <vrfname> <changestatus>

```
admin@sr-be(config)# system ssh vrf vrf1 on
```

Рисунок 48 – Изменение активности SSH VRF сервера

где:

- <vrfname> – наименование VRF;
- <changestatus> – указание состояния SSH VRF, может быть on, off или restart.

При первичном и повторнов запуске Server SSH на несуществующем VRF выдаются предупреждения (см. рисунок 49):

system ssh vrf <vrfname> whitelist <networks>

```
admin@sr-be(config)# system ssh vrf vrf1 on
Warning: SSH server is configured for a non-existent VRF vrf1.
admin@sr-be(config)# system ssh vrf vrf1 on
Warning: VRF vrf1 does not exist.
```

Рисунок 49 – Предупреждения SSH VRF

где:

- <vrfname> – наименование VRF;
- <networks> – список сетей X.X.X.X/X.

Server SSH будет создан, но не запустится если не создать VRF. Если VRF будет создан, тогда SSH сразу запустится (см. рисунок 50):

```
admin@sr-be(config)# show system ssh
SSH configuration

SSH server enabled
 Version: 2
 Port: 22
 Listen addresses:
  all
  all-ipv6
 Whitelist:
  all
  all-ipv6

SSH server in vrf vrf1 enabled but not running
 Version: 2
 Port: 22
 Listen addresses:
  all
  all-ipv6
 Whitelist:
  all
  all-ipv6
 SSH timeout:     600

admin@sr-be(config)# ip vrf vrf1
admin@sr-be(config-vrf)#show system ssh
SSH configuration

SSH server enabled
 Version: 2
 Port: 22
 Listen addresses:
  all
  all-ipv6
 Whitelist:
  all
  all-ipv6

SSH server in vrf vrf1 enabled
 Version: 2
 Port: 22
 Listen addresses:
  all
  all-ipv6
 Whitelist:
  all
  all-ipv6
 SSH timeout:     600
```

Рисунок 50 – Устранения ошибки SSH VRF

Для установки номера SSH VRF порта (см. рисунок 51), выполните команду:

system ssh vrf <vrfname> port <sshport>

```
admin@sr-be(config)# system ssh vrf1 port 22
```

Рисунок 51 – Установки номера SSH VRF порта

где:

- <vrfname> – наименование VRF;
- <sshport> – номер SSH VRF порта, обозначается числом от 1 до 65535.

Для установки адреса SSH VRF порта (см. рисунок 52), выполните команду:

system ssh vrf <vrfname> listen-address <sshaddresses>

```
admin@sr-be(config)# system ssh vrf vrf1 listen-address 122.255.255.1
```

Рисунок 52 – Установки адреса SSH VRF порта

где:

- <vrfname> – наименование VRF;
- <sshaddresses> – адрес SSH VRF порта, вводится в виде X.X.X.X.

Для управления списком доступа SSH VRF сервера (см. рисунок 53), выполните команду:

system ssh vrf <vrfname> whitelist <networks>

```
admin@sr-be(config)# system ssh vrf vrf1 whitelist 122.255.255.1/20
```

Рисунок 53 – Указания списка доступа SSH VRF

где:

- <vrfname> – наименование VRF;
- <networks> – список сетей X.X.X.X/X.

Для настройки повторного подключения при разрыве соединения (см. рисунок 54), выполните команду:

system ssh vrf <vrfname> limit period-time <periodvalue> count <countvalue>

```
admin@sr-be(config)# system ssh vrf vrf1 limit period-time 60 count 100
```

Рисунок 54 – Ограничения периода времени

где:

- <vrfname> – наименование VRF;
- <periodvalue> – значение периода в секундах;
- <countvalue> – устанавливает количество попыток подключения.

Для настройки генерации нового сервисного ключа (см. рисунок 55), выполните команду:

system ssh vrf <vrfname> key generate <keytype> modulus <keylength>

```
admin@sr-be(config)# system ssh vrf vrf1 key generate rsa modulus 256
```

Рисунок 55 – Настройки генерации нового сервисного ключа

где:

- <vrfname> – наименование VRF;
- <keytype> – тип генерируемого ключа, возможные варианты: rsa, dsa, ecdsa, ed25519;
- <keylength> – длина ключа в битах, возможные варианты: 256, 384, 512, 768, 1024, 2048, 4069, 8192.

Для добавления публичного ключа (см. рисунок 56), выполните команду:

system ssh vrf <vrfname> public-key username <username> key-string <stringvalue>

```
admin@sr-be(config)# system ssh vrf vrf1 public-key username admin key-string ssh01
```

Рисунок 56 – Добавление публичного ключа

где:

- <vrfname> – наименование VRF;
- <username> – имя пользователя;
- <stringvalue> – строка с публичным ключом.

Для настройки времени неактивности подключения (см. рисунок 57), выполните команду:

system ssh vrf <vrfname> timeout <timeoutseconds>

```
admin@sr-be(config)# system ssh vrf vrf1 timeout 600
```

Рисунок 57 – Настройка времени неактивности подключения

где:

- <vrfname> – наименование VRF;
- <timeoutseconds> – значение времени в секундах.

Для просмотра настроек SSH VRF (см. рисунок 58), выполните команду:

show system ssh

```
admin@sr-be(config)# show system ssh

SSH server enabled
 Version: 2
 Port: 2649
 Listen addresses:
  255.255.255.1
 Whitelist:
  255.255.255.1/20
SSH server in vrf vrf1 enable
 Version: 2
 Port: 22
 Listen address:
  122.255.255.1
 Whitelist:
  122.255.255.1/20
admin@sr-be(config)#
```

Рисунок 58 – Просмотр настроек SSH VRF

Для выполнения перезапуска SSH VRF (см. рисунок 59), выполните команду:

system ssh vrf <vrfname> restart

```
admin@sr-be(config)#system ssh vrf vrf1 restart
Warning: SSH server is configured for a non-existent VRF vrf1.
admin@sr-be(config)#show system ssh
SSH configuration
SSH server enabled
 Version: 2
 Port: 22
 Listen addresses:
  all
  all-ipv6
 Whitelist:
  all
  all-ipv6
SSH server in vrf vrf1 enabled but not running
 Version: 2
 Port: 22
 Listen addresses:
  all
  all-ipv6
 Whitelist:
  all
  all-ipv6
```

```
SSH timeout:     600
```

Рисунок 59 – Перезапуск SSH VRF

где:

- <vrfname> – наименование VRF.

Для удаления настроек whitelist SSH VRF (см. рисунок 60), выполните команду:

no system ssh vrf <vrfname> whitelist <networks>

```
admin@sr-be(config)# no system ssh vrf vrf1 whitelist 198.18.0.0/24
```

Рисунок 60 – Удаление настроек whitelist SSH VRF

где:

- – <vrfname> – наименование VRF;
- – <networks> – список сетей X.X.X.X/X.

7.7. Настройка Telnet-сервера

Для настройки Telnet осуществите вход в настройки конфигурации ПО СМ (см. рисунок 25), выполнив команду:

configure terminal

Для изменения активности Telnet (см. рисунок 61), выполните команду:

system telnet <changestatus>

```
admin@sr-be(config)# system telnet on
```

Рисунок 61 – Изменение активности Telnet

где <changestatus> указание состояния Telnet, может быть on, off или restart.

Для просмотра настроек Telnet (см. рисунок 62), выполните команду:

show system telnet

```
admin@sr-be(config)# show system telnet
Telnet server enable
```

Рисунок 62 – Просмотр настроек Telnet

Для перезапуска Telnet-сервера (см. рисунок 63), выполните команду:

system telnet restart

```
admin@sr-be(config)# #system telnet restart
admin@sr-be(config)# show system telnet
Telnet configuration

Telnet server enabled
 Port: 23
 Listen address: all IPv4
 Whitelist:
  all-ipv4
  all-ipv6
 Telnet timeout:     600
admin@sr-be(config)#
```

Рисунок 63 – Перезапуск Telnet сервера

В случае если Telnet-сервер находится в выключенном состоянии (Telnet server disable), при выполнении команды restart произойдет включение (Telnet server enabled).

Для настройки whitelist, которая разрешает соединения хостам только из определенной сети (см. рисунок 64), выполните команду:

system telnet whitelist <networks>

```
admin@sr-be(config)#system telnet whitelist 10.65.5.104/32
admin@sr-be(config)#show system telnet
Telnet configuration

Telnet server disabled
 Port: 23
 Listen address: all IPv4
 Whitelist:
  10.65.5.104/32
  all-ipv6
 Telnet timeout:     600
```

Рисунок 64 – Настройка whitelist

где <networks> – список сетей X.X.X.X/X.

Для настройки listen-address, которая позволяет прослушивать адреса (см. рисунок 65), выполните команду:

system telnet listen-address <ipaddr>

```
admin@sr-be(config)# system telnet listen-address 10.65.5.99
admin@sr-be(config)# show system telnet
Telnet configuration

Telnet server enabled
 Port: 23
 Listen address: 10.65.5.99
 Whitelist:
  all-ipv4
  all-ipv6
 Telnet timeout:     600

admin@sr-be(config)# show tcp
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0:22            0.0.0.0:*              LISTEN
tcp        0      0 10.65.5.99:23         0.0.0.0:*              LISTEN
```

Рисунок 65 – Настройка listen-address

где <ipadress> –IPv4/IPv6 адресса для прослушивания.

Для удаления настроек whitelist (см. рисунок 66), выполните команду:

no system telnet whitelist <networks>

```
admin@sr-be(config)# no system telnet whitelist 10.65.5.104/32
admin@sr-be(config)# show system telnet
Telnet configuration

Telnet server disabled
 Port: 23
 Listen address: all IPv4
 Whitelist:
  all-ipv4
  all-ipv6
 Telnet timeout:     600
```

Рисунок 66 – Удаление настроек whitelist

где:

- <networks> – список сетей X.X.X.X/X.

7.8. Настройка Telnet-сервера на VRF

Для подключения Telnet-сервера на VRF, (см. рисунок 67), выполните команду:

system telnet vrf <vrfname> <changestatus>

```
admin@sr-be(config)# system telnet vrf vrf1 on
```

Рисунок 67 – Изменение активности Telnet-сервера на VRF

где:

- <vrfname> – наименование VRF;
- <changestatus> – указание состояния Telnet-сервера, может быть on, off или restart.

Если заданного VRF не существует, то при выполнении будет выдано предупреждение (см. Рисунок 68):

```
admin@sr-be(config)# system telnet vrf vrf1 port 200
Warning: Telnet server is configured for a non-existent VRF vrf1.
```

Рисунок 68 – Предупреждение об отсутствии VRF

Telnet-сервер будет создан, но не запустится, если не будет задан VRF. Для устранения ошибки требуется создать VRF и Telnet , будет запущен (см. рисунок 69)

```
admin@sr-be(config)# ip vrf vrf1
admin@sr-be(config)# show system telnet
Telnet configuration

Telnet server disabled
 Port: 23
 Listen address: all IPv4
 Whitelist:
  all-ipv4
  all-ipv6

Telnet server in vrf vrf1 disabled
 Port: 200
 Listen address: all IPv4
 Whitelist:
  all-ipv4
  all-ipv6
 Telnet timeout:     600
```

Рисунок 69 – Устранение ошибки Telnet-сервера на VRF

Для настройки listen-address на VRF, которая позволяет прослушивать адреса (см. рисунок 70), выполните команду:

system telnet vrf <vrfname> listen-address <ipaddr>

```
admin@sr-be(config)# system telnet vrf vrf1 listen-address 198.18.0.1
Warning: Telnet server is configured for a non-existent VRF vrf1.
admin@sr-be(config)# show system telnet
Telnet configuration

Telnet server disabled
 Port: 23
 Listen address: all IPv4
 Whitelist:
  all-ipv4
  all-ipv6

Telnet server in vrf vrf1 disabled
 Port: 23
 Listen address: 198.18.0.1
 Whitelist:
  all-ipv4
  all-ipv6
 Telnet timeout:     600
```

Рисунок 70 – Настройка listen-address на VRF

где:

- <vrfname> – наименование VRF;

- <ipadress> –IPv4/IPv6 адресса для прослушивания.

Для настройки whitelist на VRF, которая разрешает соединения хостам только из определенной сети (см. рисунок 71), выполните команду:

system telnet vrf <vrfname> whitelist <networks>

```
admin@sr-be(config)# system telnet vrf vrf1 whitelist 10.10.10.0/24
admin@sr-be(config)# system telnet restart
admin@sr-be(config)# show system telnet
Telnet configuration
Telnet server enabled
 Port: 23
 Listen address: all IPv4
 Whitelist:
  all-ipv4
  all-ipv6
Telnet server in vrf vrf1 enabled
 Port: 100
 Listen address: 192.168.0.2
 Whitelist:
  10.10.10.0/24
  all-ipv6
 Telnet timeout:     600
```

Рисунок 71 – Настройка whitelist на VRF

где:

- – <vrfname> – наименование VRF;
- – <networks> – список сетей X.X.X.X/X.

Для удаления настроек port на VRF (см. рисунок 72), выполните команду:

no system telnet vrf <vrfname> port <portnumber>

```
admin@sr-be(config)# no system telnet vrf vrf1 port
```

Рисунок 72 – Удаление настроек port на VRF

где:

- <vrfname> – наименование VRF;
- <portnumber> – номер порта.

Для удаления настроек whitelist на VRF (см. рисунок 73), выполните команду:

no system telnet vrf <vrfname> whitelist <networks>

```
admin@sr-be(config)# no system telnet vrf vrf1 whitelist 10.65.5.104/32
admin@sr-be(config)# show system telnet
Telnet configuration

Telnet server disabled
 Port: 23
 Listen address: all IPv4
 Whitelist:
  all-ipv4
  all-ipv6

Telnet server in vrf vrf1 disabled
 Port: 23
 Listen address: all IPv4
 Whitelist:
  all-ipv4
  all-ipv6
 Telnet timeout:     600
```

Рисунок 73 – Удаление настроек whitelist на VRF

где:

- <vrfname> – наименование VRF;
- <networks> – список сетей X.X.X.X/X.

Для удаления настроек listen-address на VRF (см. рисунок 74), выполните команду:

no system telnet vrf <vrfname> listen-address <ipadress>

```
admin@sr-be(config)# no system telnet vrf vrf1 listen-address
```

Рисунок 74 – Удаление настроек listen-address на VRF

где:

- <vrfname> – наименование VRF;
- <ipadress> –IPv4/IPv6 адресса для прослушивания.

7.9. Настройки Telnet-клиента

Для настройки Telnet-клиента (см. рисунок 75), выполните команду:

telnet <ipaddr> port <portnum>

```
admin@sr-be# telnet 10.65.5.104 port 23
Trying 10.65.5.104...
```

```
Connected to 10.65.5.104.
Escape character is '^]'.
SR-BE
sr-be login: admin
Password:
Last login: Thu Nov 12 19:52:56 MSK 1970 on pts/1

19:54:16 up 23:04,  2 users,  load average: 0.06, 0.05, 0.01
Last login: Thu Nov 12 19:54:16 on pts/1
```

Рисунок 75 – Удаленный вход в систему Telnet-клиента

где:

- <ipaddr> – IP-адрес Telnet-клиента;
- <portnum> – номер порта.

Для настройки Telnet-клиента на VRF, (см. рисунок 76), выполните команду:

telnet <ipaddr> port <portnum> vrf <vrfname>

где:

- <ipaddr > – IP-адрес Telnet-клиента;
- <portnum> – номер порта;
- <vrfname> – наименование VRF.

```
admin@sr-be(config)# telnet 198.18.0.1 port 23 vrf vrf1
Trying 198.18.0.1...
Connected to 198.18.0.1.
Escape character is '^]'.
SR-BE
sr-be login: admin
Password:
Last login: Wed Jul 31 17:29:05 MSK 2024 on ttyS0
17:33:14 up 1 day, 47 min,  1 user,  load average: 0.05, 0.01, 0.00

Last login: Wed Jul 31 17:33:14 on pts/0
```

Рисунок 76 – Удаленный вход в систему Telnet-клиента на VRF

7.10. Настройка TFTP сервера

Для настройки TFTP осуществите вход в настройки конфигурации ПО СМ (см. рисунок 25), выполнив команду:

configure terminal

Для изменения активности TFTP сервера (см. рисунок 77), выполните команду:

tftp <changestatus>

```
admin@sr-be(config)# tftp on
```

Рисунок 77 – Изменение активности TFTP сервера

где <changestatus> – указание состояния TFTP сервера, может быть on или off.

Для просмотра настроек TFTP сервера (см. рисунок 78), выполните команду:

show tftp

```
admin@sr-be(config)# show tftp
mult.json
```

Рисунок 78 – Просмотр настроек TFTP сервера

8. Дополнительные возможности

Все функциональные возможности ПО СМ и команды для их выполнения приведены в приложении к руководству оператора RU.07622667.00004-01 34 01-2.

9. Обновление программы

Для проведения работы по обновлению ПО СМ необходимо организовать автоматизированное рабочее место (далее – АРМ). Процесс организации АРМ описан в приложении 1 к настоящему руководству.

Обновление программного обеспечения может производить пользователь с уровнем привилегий 15.

9.1. Обновление ПО СМ с помощью USB-носителя

С помощью АРМ создайте установочный USB-носитель выполняя следующие этапы:

- отформатируйте USB-носитель в формате «FAT32»;
- установите метку тома как «INSTALLER»;
- скопируйте в корневую папку USB-носителя файл обновления для ПО СМ.

> **Примечание**
>
> Файл должен называться «image.fw».
> Файл обновления можно скачать с сайта https://istokmw.ru/service-router/

Подключите установочный USB-носитель к разъему USB1 СМ на лицевой части.
С помощью АРМ проверьте, что СМ включен и загрузка системы завершилась.
Осуществите вход в систему (см. рисунок 79).

> **Примечание**
>
> По умолчанию логин «admin», пароль «admin». При вводе пароля символы на экране не отображаются.

```
sr-be login: admin
Password: _
```

Рисунок 79 – Вход админа в системы

Запустите обновление ПО СМ (см. рисунок 80), выполнив команду:

system upgrade

```
Last login: Tue Jun 9 11:51:45 UTC 2020 on ttyl
12:58:29 up 3 min, 0 users, load average: 0.02, 0.03, 0.01

admin@sr-be# system upgrade
```

Рисунок 80 – Запуск обновление ПО СМ

Подтвердите необходимость обновления ПО СМ (см. рисунок 81), введя в консоль:

yes

```
Last login: Tue Jun 9 11:51:45 UTC 2020 on ttyl
12:58:29 up 3 min, 0 users, load average: 0.02, 0.03, 0.01

admin@sr-be# system upgrade
You are preparing to install software updates. This process may take a lot of time
Are you sure you want to proceed?[yes]: yes
```

Рисунок 81 – Подтверждение необходимости обновления программы

Выберите USB-носитель в качестве места, где расположен файл с обновлением (см. рисунок 82), введя в консоль:

flash

```
  For update installation you have to provide update source files.
  You will have to choose one of the two ways to get them:
  1. Copy from usb device (flash).
     If you select this option required files will be copied from device inserted
in usb port.
  2. Copy from url.
     You will have to provide a url to download source files from.
     You will also be prompted for username/password if they are required for
authentication.
  Please choose your source[flash/url]: flash
```

Рисунок 82 – Выбор места нахождения файла

Введите название файла с данными обновления (см. рисунок 83).

> Примечание
>
> Файл должен называться «image.fw».

```
  For update installation you have to provide update source files.
  You will have to choose one of the two ways to get them:
  1. Copy from usb device (flash).
     If you select this option required files will be copied from device inserted
in usb port.
  2. Copy from url.
     You will have to provide a url to download source files from.
     You will also be prompted for username/password if they are required for
authentication.
  Please choose your source[flash/url]: flash
  Please enter path to installation file: image.fw
```

Рисунок 83 – Ввод названия файла

После чего начнется копирование необходимых для обновления файлов (см. рисунок 84).

```
  Starting to copy installation files from flash
218202112 байт (218 MB, 208 MiB) скопировано, 10 s, 21,8 MB/s
6752+1 записей получено
6752+1 записей отправлено
221265920 байт (221 MB, 211 MiB) скопировано, 10,1631 s, 21,8 MB/s
  Copied files from flash
  Copied files...
```

Рисунок 84 – Процесс копирования файлов

Подтвердите сохранение настроек профилей (см. рисунок 85), введя в консоль:

yes

```
  Starting to copy installation files from flash
218202112 байт (218 MB, 208 MiB) скопировано, 10 s, 21,8 MB/s
6752+1 записей получено
6752+1 записей отправлено
221265920 байт (221 MB, 211 MiB) скопировано, 10,1631 s, 21,8 MB/s
  Copied files from flash
  Copied files...

  To preserve your settings you should backup your profiles.
  If you choose not to backup profiles, some settings may be lost in update
  Do you want to backup your profiles?[yes]: yes
```

Рисунок 85 – Подтверждение сохранения настроек профилей

Извлеките USB-флэш накопитель из СМ.

Подтвердите запуск установки (см. рисунок 86), введя в консоль:

yes

```
  To preserve your settings you should backup your profiles.
  If you choose not to backup profiles, some settings may be lost in update
  Do you want to backup your profiles?[yes]: yes
  backup profiles

  System will now reboot to start installation.
  This process will take a long time and you will not be able to abort it
  Do you want to proceed with installation?[yes/no]: yes
```

Рисунок 86 – Подтверждение запуска установки

После автоматической перезагрузки СМ начнет процесс обновления ПО СМ (см. Рисунок 87)

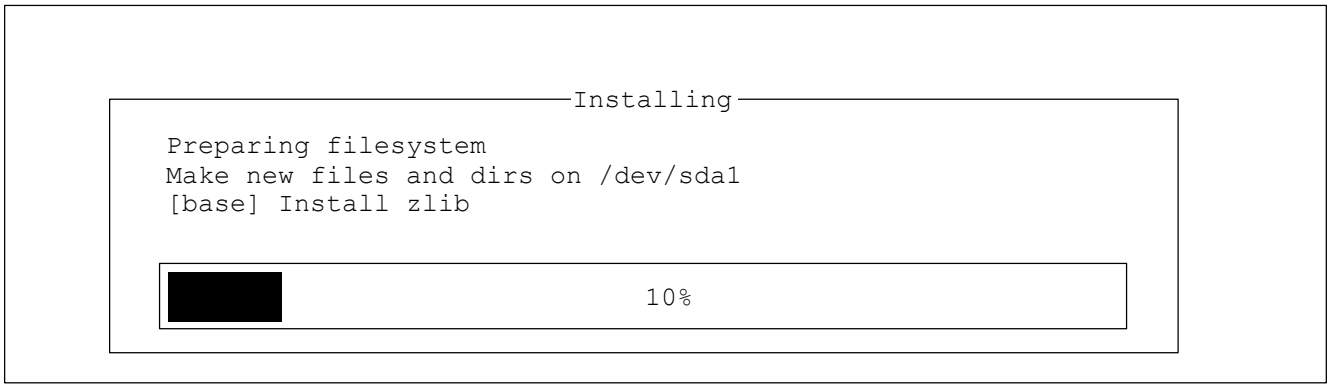

Рисунок 87 – Обновление ПО СМ

По окончанию обновления СМ перезагрузится и вернется в штатный режим работы.

9.2. Обновление ПО СМ с помощью FTP сервера

Подключите СМ к имеющемуся FTP серверу.
Разместите на FTP сервере файл обновления для ПО СМ.

> Примечание
>
> Файл должен называться «image.fw».
> Файл обновления можно скачать с сайта https://istokmw.ru/service-router/

Осуществите вход в систему (см. рисунок 79).

> Примечание
>
> По умолчанию логин «admin», пароль «admin». При вводе пароля символы на экране не отображаются.

Запустите обновление ПО СМ (см. рисунок 80), выполнив команду:

system upgrade

Подтвердите необходимость обновления ПО СМ (см. рисунок 81), введя в консоль:

yes

Выберите удаленный источник (см. рисунок 88), введя в консоль:

url

```
  For update installation you have to provide update source files.
  You will have to choose one of the two ways to get them:
  1. Copy from usb device (flash).
     If you select this option required files will be copied from device inserted
in usb port.
  2. Copy from url.
     You will have to provide a url to download source files from.
     You will also be prompted for username/password if they are required for
authentication.
  Please choose your source[flash/url]: url
```

Рисунок 88 – Выбор места нахождения файла

Введите в консоль универсальный указатель ресурса до файла обновления (см. рисунок 89).

> **Примечание**
>
> Файл должен называться «image.fw».

```
  For update installation you have to provide update source files.
  You will have to choose one of the two ways to get them:
  1. Copy from usb device (flash).
     If you select this option required files will be copied from device inserted
in usb port.
  2. Copy from url.
     You will have to provide a url to download source files from.
     You will also be prompted for username/password if they are required for
authentication.
  Please choose your source[flash/url]: url
  Currently supported protocols: http, sftp, tftp, ftp
  Please enter url: ftp://192.168.1.2/sr-be/cs/repo/image.fw
```

Рисунок 89 – Ввод пути до файла

После чего начнется копирование необходимых для обновления файлов (см. рисунок 90).

```
  Starting download...
  Download completed: 211.0/211.0M (100%) time spent: 0:00:09
  Download completed!
  Copied files...
```

Рисунок 90 – Процесс копирования файлов

Подтвердите сохранение настроек профилей (см. рисунок 85), введя в консоль:

yes

Подтвердите запуск установки (см. рисунок 86), введя в консоль:

yes

После автоматической перезагрузки СМ начнет процесс обновления ПО СМ.

По окончанию обновления СМ перезагрузится и вернется в штатный режим работы.

9.3. Обновление программного обеспечения U-boot и BMC

С помощью АРМ создайте установочный USB-носитель выполняя следующие этапы:

- отформатируйте USB-носитель в формате «FAT32»;
- установите метку тома как «INSTALLER»;
- скопируйте в корневую папку USB-носителя файл обновления для программы;
- проверьте называния файла соответствию «rt1mb.rom», если название отличается – переименуйте его.

Подключите установочный USB-носитель к разъему USB1 СМ на лицевой части.

Перезагрузите СМ для попадания в boot menu (см. рисунок 91), выполнив команду:

system reboot

```
Last login: Tue Jun 9 11:51:45 UTC 2020 on ttyl
12:58:29 up 3 min, 0 users, load average: 0.02, 0.03, 0.01

admin@sr-be# system reboot
```

Рисунок 91 – Boot menu

> **Примечание**
>
> Также СМ можно перезагрузить, кратковременно обесточив его.

Используя клавиатуру выберите пункт «FW update», после чего начнется процесс обновления (см. рисунок 92).

```
---== RT1MB boot menu ==--

      Normal boot
      FW update
      BMC console
      U-Boot console

Press UP/DOWN to move, ENTER to select menu entry 1
```

Рисунок 92 – Обновление U-boot

По окончанию обновления система вернет возможность ввода команд (см. рисунок 93).

```
SF: Detected MX25U12832F with page size 256 Bytes, erase size 64 KiB, total 16 MiB
(Re)start USB...
USB0: Register 1000140 NbrPorts 1
Starting the controller
USB XHCI 1.00
scaning bus 0 for devices... 3 USB Device(s) found
      scaning usb for storage devices... 1 Storage Device(s) found
      scaning usb for ethernet devices... 0 Ethernet Device(s) found
reading rt1mb.rom
16777216 bytes read in 8761 ms (1.8 MiB/s)
131072 bytes written, 16646144 bytes skipped in 109.488s, speed 158275 B/s
BAIKAL #_
```

Рисунок 93 – Окончание обновление U-boot

Измените настройки запуска СМ (см. рисунок 94), выполнив команды:

setenv ci_instelled1

saveenv

```
SF: Detected MX25U12832F with page size 256 Bytes, erase size 64 KiB, total 16 MiB
(Re)start USB...
USB0: Register 1000140 NbrPorts 1
Starting the controller
USB XHCI 1.00
scaning bus 0 for devices... 3 USB Device(s) found
      scaning usb for storage devices... 1 Storage Device(s) found
      scaning usb for ethernet devices... 0 Ethernet Device(s) found
reading rt1mb.rom
16777216 bytes read in 8761 ms (1.8 MiB/s)
131072 bytes written, 16646144 bytes skipped in 109.488s, speed 158275 B/s
BAIKAL # setenv ci_istalled1
BAIKAL # saveenv
Svaing Environment to Flash...
SF: Detected MX25U12832F with page size 256 Bytes, erase size 64 KiB, total 16 MiB
Erasing SPI flash...done
Writing to SPI flash...done
BAIKAL#
```

Рисунок 94 – Изменение настроек запуска

Для возвращения к штатной работе необходимо перезагрузить СМ, для этого кратковременно обесточьте его.

9.4. Сброс к заводским настройкам

С помощью АРМ проверьте, что СМ включен и загрузка системы завершилась.

Осуществите вход в систему (см. рисунок 79).

> **Примечание**
>
> По умолчанию логин «admin», пароль «admin». При вводе пароля символы на экране не отображаются.

Запустите процесс сброса к заводским настройкам ПО СМ (см. рисунок 95), выполнив команду:

factory-default

```
Last login: Sun Apr 12 13:11:11 MSK 2015 on ttySO
12:10:27 up 3 min, 0 users, load average: 0.25, 0.32, 0.14

admin@sr-be# factory-default
```

Рисунок 95 – Запуск сброса к заводским настройкам ПО СМ

Подтвердите запуск сброса к заводским настройкам ПО СМ (см. рисунок 96), введя в консоль:

deleted all

```
admin@sr-be# factory-default
You are attempting to reset device to factory default state.
This device will be rebooted and will start installation of default software
version.
You will lose all of your data: settings, profiles, users, logs etc.
This process IS NOT REVERSIBLE.
Are you sure you want to proceed? If you are sure enter ‘deleted all’ or enter ‘no’
to cancel: deleted all
```

Рисунок 96 – Подтверждение запуска сброса к заводским настройкам ПО СМ

После автоматической перезагрузки СМ начнется процесс сброса настроек ПО СМ.

По окончанию сброса настроек СМ перезагрузится и вернется в штатный режим работы.

Перечень условных обозначений и сокращений

АРМ	–	**Автоматизированное рабочее место**
ОС	–	Операционная система
ПО СМ	–	Программное обеспечения сервисного маршрутизатора CS
ПЭВМ	–	Персональная электронно-вычислительная машина
СМ	–	Сервисный маршрутизатор CS
CBQ	–	Class-based queueing
DNS	–	Domain Name System
BFD	–	Bidirectional Forwarding Detection
BGP	–	Border Gateway Protocol
BPDU	–	Bridge Protocol Data Unit
CARP	–	Common Address Redundancy Protocol
CLI	–	Command-Line Interface
DHCP	–	Dynamic Host Configuration Protocol
DMVPN	–	Dynamic Multipoint Virtual Private Network
DSCP	–	Differentiated Services Code Point
DSA	–	Distributed Switch Architecture
FIFO	–	First In, First Out
FTP	–	File Transfer Protocol
GRE	–	Generic Routing Encapsulation
GRED	–	Generalized RED
HFSC	–	Hierarchical fair-service curve
HTB	–	Hierarchical Token Bucket
IGMP	–	Internet Group Management Protocol
IP	–	Internet Protocol
IPIP	–	Internet Protocol in IP
IPSec	–	IP Security
IP SLA	–	Internet Protocol Service Level Agreement
IS-IS	–	Intermediate System to Intermediate System
L2TP	–	Layer 2 Tunnelling Protocol
LACP	–	Link Aggregation Control Protocol
LLDP	–	Link Layer Discovery Protocol
MAC	–	Media Access Control
MPLS	–	Multiprotocol Label Switching
MSTP	–	Multiple Spanning Tree Protocol

NAPT	–	Network Address Port Translation
NAT	–	Network Address Translation
NTP	–	Network Time Protocol
OpenVPN	–	Open Virtual Private Network
OSPF	–	Open Shortest Path First
PAT	–	Port address translation
PIM	–	Protocol Independent Multicast
PPTP	–	Point-to-Point Tunneling Protocol
PPPoE	–	Point-to-point protocol over Ethernet
PQ	–	Priority Queuing
RFC	–	Request for Comments
RSTP	–	Rapid spanning tree protocol
QoS	–	Quality of Service
RADIUS	–	Remote Authentication Dial-In User Service
RED	–	Random early detection
RIO	–	RED In/Out
RIP	–	Routing Information Protocol
RIPng	–	RIP next generation
SFQ	–	Stochastic Fairness Queueing
SNMP	–	Simple Network Management Protocol
SSH	–	Secure Shell
STP	–	Spanning Tree Protocol
TACACS+	–	Terminal Access Controller Access Control System plus
TBF	–	Token Bucket Filter
TCP	–	Transmission control protocol
TFTP	–	Trivial File Transfer Protocol
ToS	–	Type of Service
UDP	–	User Datagram Protocol
UMSD	–	Unified Marvell SOHO Driver
VLAN	–	Virtual Local Area Network
VRF	–	Virtual Routing and Forwarding
VRRP	–	Virtual Router Redundancy Protocol
WFQ	–	Weighted Fair Queuing
WRED	–	Weighted Random Early Detection
WRR	–	Weighted Round Robin

Приложение 1
Подготовка автоматизированного рабочего места

1. Аппаратные средства

Для проведения работы с программой необходимо организовать автоматизированное рабочее место.

Перечень оборудования и программного обеспечения, входящего в состав АРМ, приведён в таблице 1.1.

Таблица 1.1 – Перечень оборудования и программного обеспечения из состава АРМ

Наименование	Кол-во, шт.	Примечание
ПЭВМ с установленной ОС Windows 10, в составе: а) системный блок с характеристиками не хуже: – процессор с частотой 1 ГГц; – объём оперативной памяти — 2 ГБ; – доступный объём жёсткого диска — 32 ГБ; – видеоадаптер — DirectX 9; – интерфейсы — USB 2.0, RJ-45 — 1 шт.; – устройство чтения компакт–дисков. б) монитор; в) клавиатура; г) манипулятор типа «мышь».	1	
Кабель-адаптер USB с разъёмом DB9 (RS-232)	1	
PuTTY	1	

2. Подключение устройств

Для проведения работ с ПО СМ:

- произведите подключение АРМ к аппаратной платформе СМ посредством консольного кабеля RJ-45 – DB9 представленное на рисунках 1.1, 1.2:

Рисунок 1.1 – Распределение контактов разъемов кабеля консольного RJ45-DB9 КРПГ.465965.002

Рисунок 1.2 – Распределение контактов разъемов кабеля для СМ выпуска ранее 05.2024

> **Примечание**
>
> В случае отсутствия порта DB9 на АРМ, необходимо использовать кабель-адаптер USB – DB9 (RS-232). Установить используемые адаптером драйвера по необходимости.

- проверьте корректность подключения изделия к АРМ, в диспетчере устройств;
- запустите программу PuTTY и в её главном окне укажите:
- тип подключения – Serial;
- номер порта из диспетчера устройств ОС;
- скорость – 115200;
- во вкладке «Serial» проверьте настройки источников ввода, для корректной работы выставите на «None»;
- подключитесь к СМ, нажав на кнопку Open.

После этого, интерфейс DB9 (RS-232) станет активным на приём сигналов, АРМ будет считаться подготовленным к работе.

> **Примечание**
>
> В случае отсутствия загрузки ПО СМ необходимо:
> - перезагрузить СМ путем отключения и включения питания;
> - проверить подключение устройств, в частности распайку кабеля DB9 – RJ-45 (см. на рисунках 1.1, 1.2);
> - проверить настройки COM-порта в PuTTY.

Приложение 2
Удаленное подключение к сервисному маршрутизатору

1. Удаленный вход в систему с помощью SSH

Для удаленного доступа к СМ с помощью протокола SSH необходимо выполнить настройку сети устройства, с которого будет осуществляться подключение (TCP/IPv4). Откорректируйте IP-адрес устройства, его маску и адрес шлюза.

> **Примечание**
>
> По умолчанию IP-адрес – 192.168.0.100, маска подсети – 255.255.255.0, адрес шлюза – 192.168.0.1.

Чтобы узнать IP-адреса интерфейсов СМ (см. рисунок 2.1), выполните команду:

show interfaces brief

```
admin@sr-be# show interfaces brief
 Interface    HW Address         IPv4 Address    Admin/Link  DHCPv4  Description

 eth1         00:e6:59:1e:68:01  unassigned      UP/DOWN     ON

 eth2         00:e6:59:1e:68:02  192.168.0.1/24  UP/DOWN     OFF

 switchport1                     n/a             DOWN/DOWN   n/a

 switchport2                     n/a             DOWN/DOWN   n/a

 switchport3                     n/a             DOWN/DOWN   n/a

 switchport4                     n/a             DOWN/DOWN   n/a

 switchport5                     n/a             DOWN/DOWN   n/a

 switchport6                     n/a             DOWN/DOWN   n/a

 switchport7                     n/a             DOWN/DOWN   n/a

 switchport8                     n/a             DOWN/DOWN   n/a

admin@sr-be#
```

Рисунок 2.1 – IP-адреса интерфейсов

С помощью командной строки осуществите удаленное подключение (см. рисунок 2.2), выполнив команду:

ssh <username>@<ipaddress>

```
C:\User\admin>ssh admin@192.168.0.1
```

Рисунок 2.2 – Выбор номера порта

где:

- <username> – наименование пользователя;
- <ipaddress> – ip-адрес СМ.

Подтвердите удаленное подключение (см. рисунок 2.3), введя в консоль:

yes

```
C:\User\admin>ssh admin@192.168.0.1
The authenticity of host ‘192.168.0.1 (192.168.0.1)’ can’t be established.
RSA key fingerprint is SHA256:FzmnRyWGBJFxGjMEEiWLOv87Bim1hH1EmwwxDidEi9o.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Рисунок 2.3 – Подтверждение удаленного подключения

Введите пароль для осуществления входа пользователя (см. рисунок 2.4).

```
C:\User\admin>ssh admin@192.168.0.1
The authenticity of host ‘192.168.0.1 (192.168.0.1)’ can’t be established.
RSA key fingerprint is SHA256:FzmnRyWGBJFxGjMEEiWLOv87Bim1hH1EmwwxDidEi9o.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes
Warning: Permanently added ‘192.168.0.1’ (RSA) to the list of known hosts.
admin@192.168.0.1’s password:
```

Рисунок 2.4 – Вход пользователя

> **Примечание**
>
> При вводе пароля символы на экране не отображаются.

Удаленный вход в систему выполнен.

2. Настройка удаленного входа в систему с помощью SSH

2.1. Для выбора номера порта (см. рисунок 2.5), выполните команду:

ssh <remoteaddress> port <portnumber>

```
admin@sr-be# ssh myhost@sr-be port 22
```

Рисунок 2.5 – Выбор номера порта

где:

- <remoteaddress> – адрес удаленного узла;
- <portnumber> – номер порта.

2.2. Для настройки версии протокола (см. рисунок 2.6), выполните команду:

ssh <remoteaddress> <addressfamily>

```
admin@sr-be# ssh myhost@sr-be ipv4
```

Рисунок 2.6 – Настройка версии протокола

где:

- <remoteaddress> – адрес удаленного узла;
- <addressfamily> – версия протокола, возможные варианты: ipv4, ipv6.

2.3. Для настройки версии SSH (см. рисунок 2.7), выполните команду:

ssh <remoteaddress> protocol <version>

```
admin@sr-be# ssh myhost@sr-be protocol v1
```

Рисунок 2.7 – Настройка версии SSH

где:

- <remoteaddress> – адрес удаленного узла;
- <version> – версия SSH, возможные варианты: v1, v2.

2.4. Для настройки адреса источника (см. рисунок 2.8), выполните команду:

ssh <remoteaddress> source <sourcevalue>

```
admin@sr-be# ssh myhost@sr-be source 122.255.255.1
```

Рисунок 2.8 – Настройка адреса источника

где:

- <remoteaddress> – адрес удаленного узла;
- <sourcevalue> – IP-адрес источника в формате X.X.X.X.

2.5. Для указания VRF (см. рисунок 2.9), выполните команду:

ssh <remoteaddress> vrf <vrfname>

```
admin@sr-be# ssh myhost@sr-be vrf vrf1
```

Рисунок 2.9 – Указание VRF

где:

- <remoteaddress> – адрес удаленного узла;
- <vrfname> – наименование VRF.

2.6. Для настройки алгоритма шифрования (см. рисунок 2.10), выполните команду:

ssh <remoteaddress> cipher <ciphervalue>

```
admin@sr-be# ssh myhost@sr-be cipher 3des-cbc
```

Рисунок 2.10 – Настройка алгоритма шифрования

где:

- <remoteaddress> – адрес удаленного узла;
- <ciphervalue> – алгоритм шифрования, возможные варианты: 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc@lysator.liu.se, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com, chacha20-poly1305@openssh.com.

2.7. Для настройки MAC-алгоритма (см. рисунок 2.11), выполните команду:

ssh <remoteaddress> mac <macvalue>

```
admin@sr-be# ssh myhost@sr-be mac hmac-sha1
```

Рисунок 2.11 – Настройка MAC-алгоритма

где:

- <remoteaddress> – адрес удаленного узла;
- <macvalue> – MAC-алгоритм, возможные варианты: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, hmac-md5, hmac-md5-96, umac-64@openssh.com, umac-128@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-md5-etm@openssh.com, hamc-md5-96-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com.

2.8. Для настройки алгоритма обмена ключами (см. рисунок 2.12), выполните команду:

ssh <remoteaddress> kex <kexvalue>

```
admin@sr-be# ssh myhost@sr-be kex diffie-hellman-group1-sha1
```

Рисунок 2.12 – Настройка алгоритма обмена ключами

где:

- <remoteaddress> – адрес удаленного узла;
- <kexvalue> – алгоритм обмена ключами, возможные варианты: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group-exchange-sha1, diffie-hellman-group-exchange-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, curve25519-sha256, curve25519-shasha256@libssh.org.

2.9. Для настройки алгоритма ключей машины (см. рисунок 2.13), выполните команду:

ssh <remoteaddress> hostkey <hostkeyvalue>

```
admin@sr-be# ssh myhost@sr-be hostkey ssh-ed25519
```

Рисунок 2.13 – Настройка алгоритма ключей машины

где:

- <remoteaddress> – адрес удаленного узла;

- <hostkeyvalue> – алгоритм ключей машины, возможные варианты: ssh-ed25519, ssh-ed25519-cert-v01@openssh.com, ssh-rsa, ssh-dss, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-rsa-cert-v01@openssh.com, ssh-dss-cert-v01@openssh.com, ecdsa-sha2-nistp256-cert-v01@openssh.com, ecdsa-sha2-nistp384-cert-v01@openssh.com, ecdsa-sha2-nistp512-cert-v01@openssh.com.

Техническая поддержка

Официальный сайт компании: https://istokmw.ru/

Документацию и программное обеспечение на изделия можно скачать в разделе «Документация и Программное обеспечение» на странице https://istokmw.ru/service-router/

Базовая техническая поддержка осуществляется
5 дней в неделю по будням с 8:00 до 17:00 (время Московское)
тел: +7 (495) 465-86-48
e-mail: support@istokmw.ru
web: https://istokmw.ru/support/

Личный кабинет технической поддержки по функционированию продуктов
https://helpdesk.istokmw.ru/