СЕРВИСНЫЙ МАРШРУТИЗАТОР СЕРИИ ISN505
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СЕРВИСНОГО МАРШРУТИЗАТОРА CS
РУКОВОДСТВО СИСТЕМНОГО ПРОГРАММИСТА
ВЕРСИЯ ПО 3.25.00

2025

СОДЕРЖАНИЕ

История изменений документа **4**
Аннотация **5**
1 Общие сведения о программе **6**
2 Требования к техническим и программным средствам **11**
3 Структура программы **12**
4 Управление пользователями **14**
4.1 Создание и корректировка группы **14**
4.2 Создание пользователя **15**
4.3 Корректировка пользователя **16**
4.4 Удаление группы **17**
4.5 Удаление пользователя **18**
5 Работа с профилями программы **19**
5.1 Сохранение настроек профиля **19**
5.2 Создание нового профиля **19**
5.3 Загрузка профиля **19**
5.4 Удаление профиля **20**
5.5 Сохранение профиля на USB-носитель **20**
5.6 Сохранение профиля на сетевом хранилище **20**
5.7 Копирование профиля с USB-носителя **21**
5.8 Копирование профиля из сетевого хранилища **21**
5.9 Выбор автоматически загружаемого профиля **21**
5.10 Просмотр профилей **22**
6 Настройка параметров программы **23**
6.1 Настройка параметров времени и даты **23**
6.2 Настройка тайм-аутов **24**
6.3 Наименование хоста ip-адреса **26**
6.4 Указание хоста и доменного имени **27**
6.5 Настройка SSH **27**
6.6 Настройка SSH VRF **29**
6.7 Настройка Telnet **31**
6.8 Настройка Telnet VRF **33**

6.9 Подключение Telnet-клиента 35
6.10Настройка TFTP сервера 36
7 Дополнительные возможности 38
8 Обновление программы 39
8.1 Обновление ПО СМ с помощью USB-носителя 39
8.2 Обновление программного обеспечения TIANOCORE и BMC 40
Перечень условных обозначений и сокращений 42
Приложение 1. Подготовка автоматизированного рабочего места 45
1. Аппаратные средства 45
2. Подключение устройств 45

История изменений документа

Версия документа	Дата выпуска	Внесены изменения	Версия ПО
Версия 3.0	01.11.2025		3.25.00
Версия 2.0	24.07.2025		3.24.13
Версия 1.0	17.04.2025		3.24.10

Аннотация

Данный документ является руководством системного программиста программного обеспечения сервисного маршрутизатора CS, предназначенного для организации и предоставления функций коммутации и маршрутизации трафика.

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

Данный документ разработан под версию программного обеспечения сервисного маршрутизатора 3.25.00 от 01.11.2025, работа программного обеспечения сервисного маршрутизатора 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 в операционной системе Linux, Windows и знающий основы сетевого администрирования.

Для наглядности в тексте настоящего руководства используются различные стили оформления (таблица 1).

Таблица 1 – Стили оформления в документе

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

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 RIPv2, RIPng, OSPFv2, OSPFv3, IS-IS, BGPv4.

ПО СМ поддерживает возможность добавления описания к статическим маршрутам.

ПО СМ поддерживает добавление Loopback интерфейсов.

ПО СМ поддерживает статические маршруты в качестве next-hop - физический порт, Loopback, Tunnel.

ПО СМ поддерживает фильтрацию маршрутов (prefix list).

ПО СМ обеспечивает фильтрацию маршрутов по:

- длине префикса и префикса сети;
- номеру автономной системы.

ПО СМ поддерживает изменение административной дистанции к статическим маршрутам.

ПО СМ поддерживает коммутацию пакетов (bridging).

ПО СМ поддерживает агрегацию интерфейсов LAG/LACP (802.3ad).

ПО СМ обеспечивает поддержку VLAN (802.1Q) с количеством номеров 4096.

ПО СМ поддерживает QinQ на WAN портах.

ПО СМ поддерживает логические интерфейсы (sub interface) на WAN портах.

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 VRRPv2/v3, CARP и управление их параметрами.

ПО СМ поддерживает Tracking на основании VRRP- или SLA-теста.

ПО СМ поддерживает управление административным статусом интерфейса.

ПО СМ поддерживает управление атрибутом AS-PATH и preference в route-map.

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 DHCP-клиент.

ПО СМ поддерживает DHCP Relay Option 82

ПО СМ поддерживает динамическое конфигурирование сетевых настроек на узлах в качестве DHCP-сервера с поддержкой опций 1,2,3,4,6,9,12,15,19,20,21,22,23,26,33,42,43,51,53,60,61,66,67,68,150,176,242.

ПО СМ поддерживает работу в качестве DNS-сервера (master/slave), DNS-клиента, DNS-proxy.

ПО СМ поддерживает протокол синхронизации времени NTP.

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

ПО СМ поддерживает балансировки нагрузки ECMP.

ПО СМ поддерживает ARP, Proxy ARP.

ПО СМ поддерживает протокол учета сетевого трафика Netflow v5/v9/v10.

ПО СМ поддерживает протокол сетевого управления SNMPv1/v2/v3.

ПО СМ поддерживает SNMP trap.

ПО СМ поддерживает стандартные и расширенные SNMP MIB.

ПО СМ поддерживает защиту от ошибок конфигурирования, восстановление конфигурации с помощья rollback.

ПО СМ поддерживает проверку целостности системных файлов ПО.

ПО СМ обеспечивает вывод информации по сервисам/процессам.

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 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 до 8 приоритетных очередей на порт.

ПО СМ поддерживает приоритизацию трафика с поддержкой - 801.2p, DSCP, IP Precedence.

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 перемаркировку приоритетов.

ПО СМ поддерживает применение политик (policy-map).

ПО СМ поддерживает управление полосой пропускания (shaping).

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 режимы IPsec: «policy-based» и «route-based».

ПО СМ поддерживает алгоритмы шифрования DES, 3DES, CAST AES, Blowfish, Camellia.

ПО СМ поддерживает алгоритмы шифрования аутентификация сообщений IKE MD5, SHA-1, SHA-2.

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 Time-Based ACL, DPI, защиту от DoS-атак, логирование событий срабатывания правил функций сетевой защиты.

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 программного обеспечения:

- локальное (с внутреннего/внешнего накопителя);
- удаленное (по протоколам HTTP, SFTP, 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 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 программного обеспечения сервисного маршрутизатора:

- аппаратная платформа на базе процессора Baikal-M;
- оперативная память: 8 ГБ;
- постоянное запоминающее устройство: 60 ГБ.

3 Структура программы

Структурная схема программы (рисунок 1).

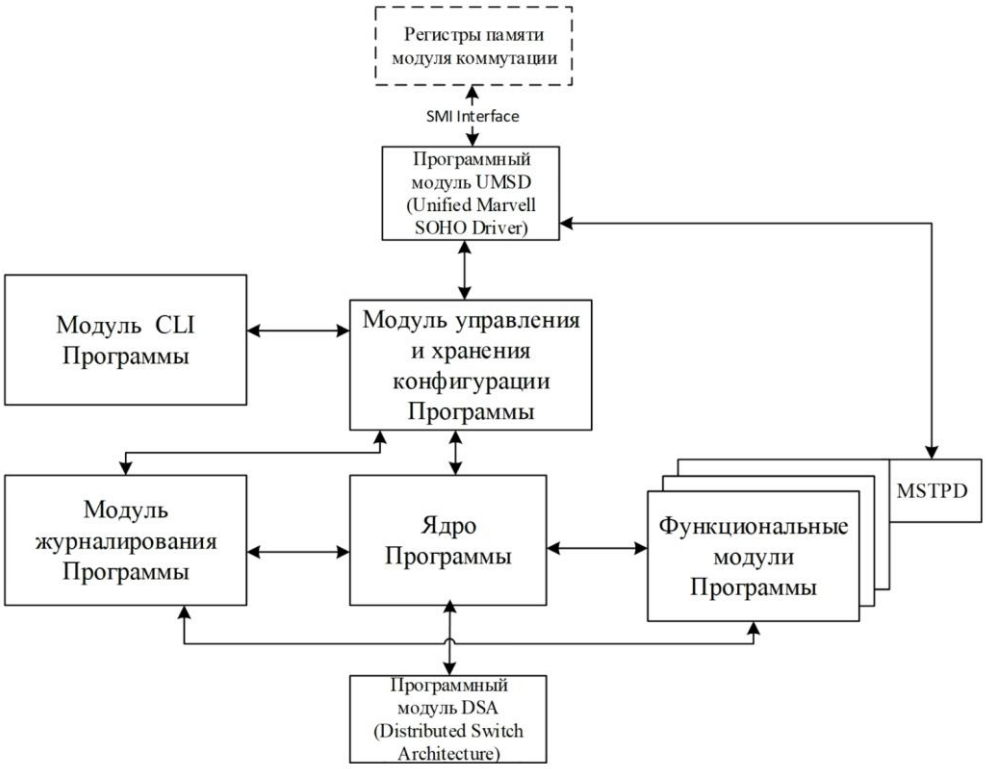

Рисунок 1 – Структурная схема программы

Программа функционально подразделяется на следующие части:

- ядро ПО отвечает за взаимодействие с драйверами устройства, обработку сетевых пакетов;
- функциональные модули ПО отвечают за функциональные возможности программы (протоколы, технологии);
- модуль управления и хранения конфигураций ПО отвечает за настройку функциональных модулей по поступившим в модуль командам и синхронизацию функционирования разных модулей;
- модуль журналирования ПО отвечает за протоколирование различных действий/событий составных частей программы;
- модуль ПО – CLI (Command Line Interface) отвечает за интерфейс «человек-программа»;

- модуль DSA – отвечает за проецирование физических интерфейсов модуля коммутации в ядро. Отвечает за передачу служебных сообщений протокола LLDP;
- 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 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.

4.1 Создание и корректировка группы

Для создания или корректировки группы осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

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

Для создания новой группы, выполните команду:

group <groupname> privilege <privilegelevel>

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

где: – <groupname> – наименование группы;

– <privilegelevel> – уровень привилегий группы.

Убедитесь в создании новой группы вызвав просмотр существующих групп, выполнив команду:

show groups

```
admin@sr-be# show groups
Group | Privilege
```

```
--------------------
admin  | 15
service | 1
other   | 5
admin@sr-be#
```

При корректировке уровня привилегий группы используйте наименование существующей группы пользователей.

Примечание

Данная настройка управляет только базой локальных групп пользователей; она не позволяет корректировать группы пользователей, авторизованных через RADIUS/TACACS+.

Настройки этой команды сохраняются в общих настройках системы, но не профилях, поэтому они не меняются при загрузке нового профиля.

4.2 Создание пользователя

Для создания пользователя осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

Для создания нового пользователя, выполните команду:

username add <username> group <usergroup>

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

где: – <username> – наименование пользователя;

– <usergroup> – наименование существующей группы, куда будет добавлен пользователь.

Задайте пароль для нового пользователя, придумайте последовательность символов и дважды введите ее.

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

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

Примечание

При вводе пароля символы на экране не отображаются.

Данная настройка управляет только базой локальных пользователей; она не позволяет добавить пользователей уже авторизованных через RADIUS/TACACS+.

Настройки этой команды сохраняются в общих настройках системы, но не профилях, поэтому они не меняются при загрузке нового профилях.

Убедитесь в создании нового пользователя вызвав просмотр существующих пользователей, 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)#
```

4.3 Корректировка пользователя

Для корректировки пользователя осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

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

1) изменение группы вхождения пользователя, выполнив команду:

username edit <username> group <groupname>

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

где: – <username> – наименование пользователя;

– <groupname> – наименование существующей группы, куда будет перенесен пользователь.

2) изменение пароля пользователя, выполнив команду:

username edit <username> password

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

где <username> – наименование пользователя.

Задайте новый пароль для пользователя, придумайте последовательность символов и дважды введите ее.

Примечание

При вводе пароля символы на экране не отображаются.

Данная настройка управляет только базой локальных пользователей; она не позволяет изменить настройки пользователей, авторизованных через RADIUS/TACACS+.

Настройки этой команды сохраняются в общих настройках системы, но не профилях, поэтому они не меняются при загрузке нового профиля.

4.4 Удаление группы

Для удаления группы осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

Предварительно удалите из группы всех участников согласно подразделу удаление пользователя настоящего руководства.

Для удаления группы, выполните команду:

no group <groupname>

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

где <groupname> – наименование группы.

Убедитесь в удалении группы вызвав просмотр существующих групп, выполнив команду:

show groups

Примечание

Данная настройка управляет только базой локальных групп пользователей; она не удаляет группы пользователей, авторизованных через RADIUS/TACACS+.

Настройки этой команды сохраняются в общих настройках системы, но не профиля, поэтому они не меняются при загрузке нового профиля.

4.5 Удаление пользователя

Для удаления пользователя осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

Для удаления пользователя, выполните команду:

no username <username>

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

где <username> – наименование пользователя.

Убедитесь в удалении пользователя вызвав просмотр существующих пользователей, выполнив команду:

show users

5 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.

5.1 Сохранение настроек профиля

Для сохранения настроек профиля, выполните команду:

write <profilename> comment <profilecomment>

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

где: – <profilename> – наименование профиля;

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

5.2 Создание нового профиля

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

5.3 Загрузка профиля

Для загрузки профиля, выполните команду:

load <profilename>

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

где <profilename> – наименование профиля.

5.4 Удаление профиля

Для удаления профиля, выполните команду:

no profile <profilename>

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

где <profilename> – наименование профиля.

5.5 Сохранение профиля на USB-носитель

Подключите USB-носитель к разъему USB1 на лицевой панели сервисного маршрутизатора.

Для сохранения профиля на USB-носитель, выполните команду:

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

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

где: – <configname> – наименование профиля;

– <devname> – имя устройства;

– <dirname> – путь, куда будет записан профиль.

5.6 Сохранение профиля на сетевом хранилище

Для сохранения профиля на сетевом хранилище, выполните команду:

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

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

где: –<profilename> – 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.

5.7 Копирование профиля с USB-носителя

Для копирования профиля с USB-носителя, выполните команду:

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

```
admin@sr-be# copy profile secondprofile from flash /media/usb0 /media/usb0/2
```

где: – <profilename> – наименование профиля;
– <devname> – имя устройства;
– <dirname> – путь, куда будет записан профиль.

5.8 Копирование профиля из сетевого хранилища

Для копирования профиля из сетевого хранилища, выполните команду:

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

```
admin@sr-be# copy profile secondprofile from url ftp 1.1.1.1 remotedir ftp
```

где: – <profilename> – 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.

5.9 Выбор автоматически загружаемого профиля

Для выбора загрузочного профиля, выполните команду:

boot-profile <profilename>

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

где <profilename> – наименование профиля.

Для сохранения настроек текущего профиля в загрузочный, выполните команду:

write <profilename> comment “<profilecomment>”

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

где: – <profilename> – наименование профиля;

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

Примечание

Запрещено изменение или удаление профилей с именами boot, last-loaded, current, default.

5.10 Просмотр профилей

Для просмотра профилей, имеющихся в системе профилей, выполните команду:

show profiles

```
admin@sr-be(config)#show profiles
Flags: b – boot profile, l – last loaded profile, m – profile was modifiled was
modified or corrupted
|  Flags  |  Profile Name  |     Comment     |
-----------------------------------------------
|         | base_config    |                 |
|    l    | default        |                 |
| b       | startup        | new start profile  |
admin@sr-be(config)#
```

6 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.

6.1 Настройка параметров времени и даты

Для настройки параметров времени и даты осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

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

Для настройки текущей даты, выполните команду:

system clock date <currentdate>

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

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

Для настройки текущего времени, выполните команду:

system clock time <currenttime>

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

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

Для настройки часового пояса, выполните команду:

system clock timezone <currenttimezone>

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

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

Примечание

Для получения списка доступных наименований часовых поясов:

введите команду system clock timezone и нажмите клавишу «?», для получения подсказки о функционале введенной команды;

нажмите клавишу «Tab», на экране отобразится список доступных часовых поясов.

Для синхронизации параметров времени и даты с сервером, выполните команду:

system clock synchronize <server>

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

где <server> – IPv4/IPv6 адрес, либо имя сервера.

Для просмотра установленной на СМ даты и времени, выполните команду:

show clock

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

6.2 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, выполнив команду:

configure terminal

Для изменения тайм-аута неактивности пользователя при работе в консоли выполните команду:

system <protocol> timeout <timeoutseconds>

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

где: – <timeoutseconds> – значение времени в секундах;

– <protocol> - протоколы подключения к консоли, возможные варианты: ssh, tty, telnet.

Для изменения тайм-аута неактивности пользователя при работе в консоли, подключенной по SSH VRF, выполните команду:

system ssh vrf <vrfname> timeout <timeoutseconds>

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

где: – <vrfname> – наименование VRF;

– <timeoutseconds> – значение времени в секундах.

Для изменения тайм-аута неактивности пользователя при работе в консоли, подключенной по Telnet VRF, выполните команду:

system telnet vrf <vrfname> timeout <timeoutseconds>

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

где: – <vrfname> – наименование VRF;

– <timeoutseconds> – значение времени в секундах.

Для просмотра установленного времени различных тайм-аутов, выполните команду:

show timeout

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

Для сброса тайм-аута неактивности пользователя к значениям по умолчанию, подключенного по SSH , выполните команду:

no system ssh timeout

```
admin@sr-be(config)# no system ssh timeout
```

Для сброса тайм-аута неактивности пользователя к значениям по умолчанию, подключенного по Telnet, выполните команду:

no system telnet timeout

```
admin@sr-be(config)# no system telnet timeout
```

Примечание

Если тайм-ауты стоят в дефолтных значениях, то они не показываются в `show running-config system-config`.

Значение тайм-аута 0 отменяет ограничение.

6.3 Наименование хоста ip-адреса

Для добавления или удаления наименований хостов осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

Для добавления имени хосту определенного ip-адреса, выполните команду:

ip host <hostname> <ip>

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

где: – <hostname> – устанавливаемое имя хоста;

– <ip> – ip-адрес (X.X.X.X – для IPv4; X:X::X:X – для IPv6).

Для удаления имени хоста определенного ip-адреса, выполните команду:

no ip host <hostname>

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

где <hostname> – устанавливаемое имя хоста.

Для просмотра наименований хостов, 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
```

6.4 Указание хоста и доменного имени

Для создания или изменения хоста и доменного имени, выполните команду:

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

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

где: – <hostname> – устанавливаемое имя хоста;

– <domainname> – устанавливаемое имя домена.

6.5 Настройка SSH

Для настройки SSH осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

Для изменения активности SSH, выполните команду:

system ssh <changestatus>

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

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

Для установки номера SSH порта, выполните команду:

system ssh port <sshport>

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

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

Для установки прослушиваемого адреса на SSH сервере, выполните команду:

system ssh listen-address <sshaddresses>

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

где <sshaddresses> – IPv4/IPv6 адрес прослушивания (X.X.X.X – для IPv4; X:X::X:X – для IPv6).

Для управления списком доступа, выполните команду:

system ssh whitelist <networks>

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

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

Для настройки повторного подключение при разрыве соединения, выполните команду:

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

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

где: – <periodvalue> – значение периода в секундах;

– <countvalue> – устанавливает количество попыток подключения.

Для настройки генерации нового сервисного ключа, выполните команду:

system ssh hostkey generate <keytype> modulus <keylength>

```
admin@sr-be(config)# system ssh hostkey generate rsa modulus 1024
```

где: – <keytype> – тип генерируемого ключа, возможные варианты: rsa, dsa, ecdsa, ed25519;

– <keylength> – длина ключа в битах, возможные варианты: 1024, 2048, 4069, 8192.

Для добавления публичного ключа, выполните команду:

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

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

где: – <username> – имя пользователя;

– <stringvalue> – строка с публичным ключом.

Для просмотра настроек SSH, 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
```

6.6 Настройка SSH VRF

Для настройки SSH VRF осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

Для изменения активности SSH VRF, выполните команду:

system ssh vrf <vrfname> <changestatus>

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

где: – <vrfname> – наименование VRF;

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

При запуске Server SSH на несуществующем VRF выдаются предупреждения:

```
Warning: SSH server is configured for a non-existent VRF vrf1.
```

Для установки номера SSH VRF порта, выполните команду:

system ssh vrf <vrfname> port <sshport>

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

где: – <vrfname> – наименование VRF;

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

Для установки прослушиваемого адреса на SSH сервере на VRF, выполните команду:

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

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

где: – <vrfname> – наименование VRF;

– <sshaddresses> – IPv4/IPv6 адрес прослушивания (X.X.X.X – для IPv4; X:X::X:X – для IPv6).

Для управления списком доступа SSH VRF сервера, выполните команду:

system ssh vrf <vrfname> whitelist <networks>

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

где: – <vrfname> – наименование VRF;

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

Для настройки повторного подключение при разрыве соединения, 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
```

где: – <vrfname> – наименование VRF;

– <periodvalue> – значение периода в секундах;

– <countvalue> – устанавливает количество попыток подключения.

Для настройки генерации нового сервисного ключа, выполните команду:

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

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

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 просмотра настроек SSH VRF, 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
```

Для удаления настроек списка доступа SSH VRF сервера, выполните команду:

no system ssh vrf <vrfname> whitelist <networks>

```
admin@sr-be(config)#no system ssh vrf vrf1 whitelist 122.255.255.1/20
```

где: – <vrfname> – наименование VRF;

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

6.7 Настройка Telnet

Для настройки Telnet осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

Для изменения активности Telnet, выполните команду:

system telnet <changestatus>

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

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

Для просмотра настроек Telnet, выполните команду:

show system telnet

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

Для настройки whitelist, которая разрешает соединения хостам только из определенной сети, 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
```

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

Для настройки listen-address, которая позволяет прослушивать адреса, 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
```

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

Для удаления настроек whitelist, 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
```

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

6.8 Настройка Telnet VRF

Для подключения Telnet-сервера на VRF, выполните команду:

system telnet vrf <vrfname> <changestatus>

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

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:

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

Для настройки listen-address на VRF, которая позволяет прослушивать адреса, выполните команду:

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

```
admin@sr-be(config)# system telnet vrf vrf1 listen-address 198.18.0.1
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
```

где: – <vrfname> – наименование VRF;

– <ipadress> –IPv4/IPv6 адреса для прослушивания.

Для настройки whitelist на VRF, которая разрешает соединения хостам только из определенной сети, 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
```

где: – <vrfname> – наименование VRF;

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

Для удаления настроек port на VRF, выполните команду:

no system telnet vrf <vrfname> port <portnumber>

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

где: – <vrfname> – наименование VRF;

– <portnumber> – номер порта.

Для удаления настроек whitelist на VRF, 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
```

где: – <vrfname> – наименование VRF;

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

Для удаления настроек listen-address на VRF, выполните команду:

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

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

где: – <vrfname> – наименование VRF;

–<ipadress> –IPv4/IPv6 адреса для прослушивания.

6.9 Подключение Telnet-клиента

Для подключения Telnet-клиента, 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
```

где: – <ipaddr> – IP-адрес Telnet-клиента;

– <portnum> – номер порта.

Для подключения Telnet-клиента на VRF, выполните команду:

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

```
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
```

где: – <ipaddr > – IP-адрес Telnet-клиента;

– <portnum> – номер порта;

– <vrfname> – наименование VRF.

6.10 Настройка TFTP сервера

Для настройки TFTP осуществите вход в настройки конфигурации ПО СМ, выполнив команду:

configure terminal

Для изменения активности TFTP сервера, выполните команду:

tftp <changestatus>

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

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

Для просмотра настроек TFTP сервера, выполните команду:

show tftp

```
admin@sr-be(config)# show tftpTFTP server state: on
```

7 Дополнительные возможности

Все функциональные возможности ПО СМ и команды для их выполнения приведены в приложении к руководству оператора RU.07622667.00026-01 34 01-2.

8 Обновление программы

Для проведения работы по обновлению ПО СМ необходимо организовать автоматизированное рабочее место. Процесс организации АРМ описан в приложении 1 подготовка автоматизированного рабочего места.

Обновление программного обеспечения может производить пользователь с уровнем привилегий 15.

8.1 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

Убедитесь в наличии файлов:
rescue.efi
image.fw
install.conf
Файл обновления можно скачать с сайта https://istokmw.ru/service-router/
Если файл с расширением .fw назван отлично от image.fw - переименуйте его в image.fw.

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

Подайте питание на основную плату нажав кнопку PWR на лицевой панели.

Во время запуска платформы нажимайте F2 для входа в Boot Manager.

В Boot Manager выберите USB: ISN505 SW Install после чего начнётся установка ПО СМ (рисунок 2).

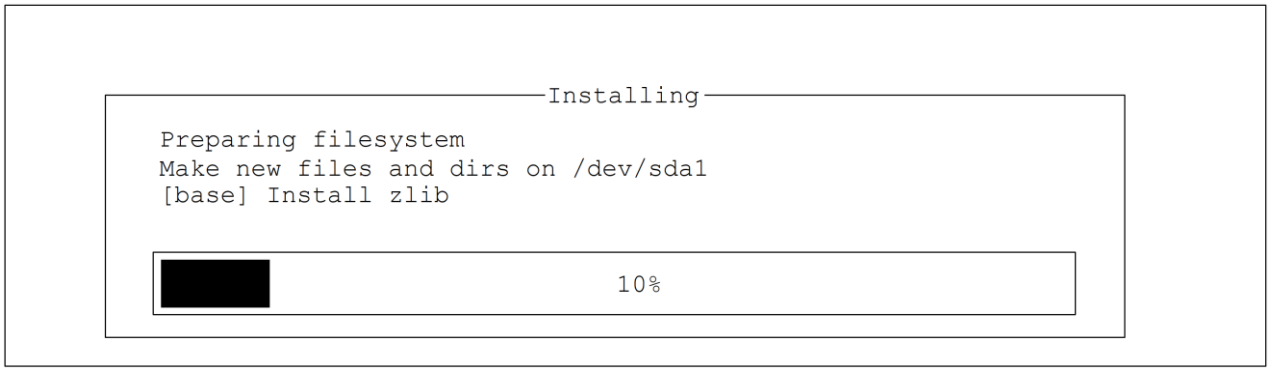

Рисунок 2 – Установка ПО CM CS

По окончанию обновления сервисный маршрутизатор перезагрузится и вернется в штатный режим работы.

8.2 Обновление программного обеспечения TIANOCORE 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 ПО CM.

Примечание

Убедитесь в наличии файлов:

fru.bin

na10.flash.igm

Файл обновления можно скачать с сайта https://istokmw.ru/service-router/

Если наименование файлов отличается - переименуйте их.

Подключите установочный USB-носитель к разъему USB CM на лицевой части.

Подайте питание на основную плату нажав кнопку PWR на лицевой панели.

Во время запуска платформы нажимайте F2 для входа в Boot Manager.

В Boot Manager выберите UEFI Shell.

В появившейся командной строке выполните команду:

fwmanager fw -w -s usb

Дождитесь окончания установки, для возвращения в штатный режим работы перезагрузите СМ.

```
Shell> fwmanager fw -w -s usbReading Firmware bin....
FSOpen: Open 'na10.flash.igm' Sucess
Reading File successful.
Erasing SPI Flash...
Erasing successfull.
Writing SPI Flash...
Writing successful.
Verifying SPI Flash...
Verifying successful.
Hard reset of the platform!
```

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
ARM	–	Advanced RISC Machine
BFD	–	Bidirectional Forwarding Detection
BGP	–	Border Gateway Protocol
BMC	–	Baseboard Management Controller
BPDU	–	Bridge Protocol Data Unit
CARP	–	Common Address Redundacy Protocol
CBQ	–	Class-based queueing
CLI	–	Command-Line Interface
DHCP	–	Dynamic Host Configuration Protocol
DMVPN	–	Dynamic Multipoint Virtual Private Network
DNS	–	Domain Name System
DSA	–	Distributed Switch Architecture
DSCP	–	Differentiated Services Code Point
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
LDP	–	Label Distribution Protocol
LLDP	–	Link Layer Discovery Protocol
MAC	–	Media Access Control
MPLS	–	Multiprotocol Label Switching
MSTP	–	Multiple Spanning Tree Protocol
MTU	–	Maximum Transmission Unit
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
QoS	–	Quality of Service
RADIUS	–	Remote Authentication Dial-In User Service
RED	–	Random early detection
RFC	–	Request for Comments
RIO	–	RED In/Out
RIP	–	Routing Information Protocol
RIPng	–	RIP next generation
RSTP	–	Rapid spanning tree protocol
RSVP	–	Resource ReSerVation Protocol
RSVP-TE	–	Resource Reservation Protocol - Traffic Engineering
SFQ	–	Stochastic Fairness Queueing
SNMP	–	Simple Network Management Protocol
SSH	–	Secure Shell

STP	–	Spanning Tree Protocol
TBF	–	Token Bucket Filter
TACACS+	–	Terminal Access Controller Access Control System
TCP	–	Transmission control protocol
TFTP	–	Trivial File Transfer Protocol
ToS	–	Type of Service
TTL	–	Time to Live
UDP	–	User Datagram Protocol
UMSD	–	Unified Marvell SOHO Driver
USB	–	Universal Serial Bus
VLAN	–	Virtual Local Area Network
VPLS	–	Virtual Private LAN Service
VPN	–	Virtual Private Network
VPWS	–	Virtual Private Wire Service
VRF	–	Virtual Routing and Forwarding
VRRP	–	Virtual Router Redundancy Protocol
WAN	–	Wide Area Network
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.

Таблица 1 – Перечень оборудования и программного обеспечения из состава АРМ

Наименование	Кол-во, шт.
ПЭВМ с установленной ОС, в составе: ○ 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. ○ монитор; ○ клавиатура; ○ 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 (рисунок 1, рисунок 2);

Рисунок 1 – Распределение контактов разъемов кабеля консольного RJ45-DB9

Рисунок 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 ОС.

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.

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;

проверить настройки COM-порта в PuTTY.

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

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/