

СЕРВИСНЫЙ МАРШРУТИЗАТОР СЕРИИ ISN505 ИНСТРУКЦИЯ ПО УСТАНОВКЕ И БЫСТРОМУ ЗАПУСКУ ВЕРСИЯ ПО 3.24.10



СОДЕРЖАНИЕ

7.2 Проверка настроек	33
8 Настройка удаленного доступа	35
8.1 Настройка удаленного доступа по протоколу SSH	35
8.2 Настройка удаленного доступа по протоколу Telnet	37
9 Настройка сервера доменного имени	
9.1 Проверка настроек	40
10Настройка DHCP-сервера на устройстве	42
11 Настройка журналирования событий на удаленный Syslog-сервер	44
12Установка даты, времени и часового пояса	46
12.1Настройка времени	46
12.2Настройка даты	46
12.3Смена часового пояса	47
12.4Настройка синхронизации времени с NTP-сервера	47
13Команды диагностики	48
13.1Ping 48	
13.2Traceroute	48
14Дополнительные руководства по работе с устройством	49
15Техническая поддержка	50

История изменений документа

Версия документа	Дата выпуска	Внесены изменения	Версия ПО
Версия 2.0	17.04.2024		3.24.10
Версия 1.0	21.02.2024		3.24.09

Настоящая инструкция содержит рекомендации по начальной настройке сервисных маршрутизаторов (далее по тексту – устройство).

Исполнения и условные обозначения устройства – Таблица 1.

Таблица 1 – Исполнения и у	исповные обозначения	устройства
таолица т – исполнения и	условные осозначения	устроиства

Исполнение	Условное обозначение
КРПГ.465614.001-18	ISN50502T5-M10A
КРПГ.465614.001-19	ISN50502T5-M11A
КРПГ.465614.001-20	ISN50502T5-M12A
КРПГ.465614.001-21	ISN50502T5-M13A
КРПГ.465614.001-22	ISN50502T5-M14A
КРПГ.465614.001-23	ISN50502T5-M15A
КРПГ.465614.001-24	ISN50502T5-M16A
КРПГ.465614.001-25	ISN50502T5-MA
КРПГ.465614.001-33	ISN50502T5-M17A

В документе описаны способы подключения к интерфейсу CLI, работа с паролями пользователей, создание и настройка VLAN, базовая настройка устройства, работа с конфигурациями, смена даты, времени и часового пояса, команды сетевой диагностики.

Инструкция предназначена для технического персонала, выполняющего установку и настройку устройства посредством интерфейса командной строки (CLI), а также процедуры по обслуживанию системы.

Перед началом настройки необходимо также внимательно ознакомиться с руководством по эксплуатации КРПГ.465614.001РЭ.

1 Условные обозначения

Для наглядности в тексте документа использованы различные стили оформления. Области применения стилей – <u>Таблица 2</u>.

Таблица 2 – Стили оформления в документе

Стиль оформления	Область применения	Пример
Полужирный текст	Выделение команд	команды пате

Устройство имеет несколько режимов конфигурации – Таблица 3.

Таблица 3 – Режимы конфигурации

Режимы конфигурации	Способ доступа	Приглашение в командной строке	Способ выхода из режима
Привилегированный режим	Авторизуйтесь	admin@sr-be#	-
Режим глобальной конфигурации	Выполните команду configure terminal	admin@sr-be(config)#	С помощью команды exit, end

2 Подключение к интерфейсу командной строки (CLI)

2.1 Подключение по локальной сети Ethernet с помощью SSH

Шаг 1. Подключите сетевой кабель передачи данных (патч-корд) к WAN порту «eth 3» и к устройству, предназначенному для управления.

Шаг 2. Откорректируйте IP-адрес интерфейса управляющего 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

Шаг 3. Для проверки связности выполните команду ping 192.168.0.1 с помощью командной строки.

C:\User\admin>ping 192.168.0.1

Результат выполнения команды:

Pinging 192.168.0.1 with 32 bytes of data: Reply from 192.168.0.1: bytes=32 time<1ms TTL=64 Reply from 192.168.0.1: bytes=32 time<1ms TTL=64 Reply from 192.168.0.1: bytes=32 time<1ms TTL=64 Reply from 192.168.0.1: bytes=32 time=1ms TTL=64 Ping statistics for 192.168.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0msyes

Шаг 4. С помощью командной строки осуществите удаленное подключение, выполнив команду

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

I	📫 Приме	чание			
:	ssh	<username>@<ipaddress> где:</ipaddress></username>	<username></username>	_	имя
пользователя; <ipaddress> – ip-адрес сервисного маршрутизатора.</ipaddress>					

Шаг 5. Подтвердите удаленное подключение, введя в консоль команду уез

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**

Шаг 6. Введите пароль для осуществления входа пользователя

Warning: Permanently added '192.168.0.1' (RSA) to the list of known hosts. admin@192.168.0.1's password:

📔 Примечание

Пароль по умолчанию admin, при вводе пароля символы на экране не отображаются

Удаленный вход в систему выполнен.

Выполните команду **show interfaces brief** чтобы узнать IP-адреса интерфейсов на сервисном маршрутизаторе.

Interface	HW Address	IPv4 Address	Admin/Link	DHCPv4 Description
eth1	94:3f:bb:00:2d:e3	unassigned	DOWN/DOWN	OFF
eth2	94:3f:bb:00:2d:fe	unassigned	DOWN/DOWN	OFF
eth3	94:3f:bb:00:2d:fe	unassigned	UP/UP	OFF
eth4	94:3f:bb:00:2d:fe	unassigned	UP/DOWN	ON
vlan1	94:3f:bb:00:2d:ff	192.168.0.1/24	UP/UP	OFF

📫 Примечание

При отсутствии подключения к сервисному маршрутизатору обратитесь в службу поддержки https://istokmw.ru/support/

2.2 Подключение по локальной сети Ethernet с помощью Telnet

📙 Примечание

Убедитесь, что на сервисном маршрутизаторе настроен удаленный доступ по протоколу Telnet. По умолчанию функция отключена.

Шаг 1. Подключите сетевой кабель передачи данных (патч-корд) к WAN порту «eth1» и к устройству, предназначенному для управления.

Шаг 2. Откорректируйте IP-адрес интерфейса управляющего устройства, его маску и адрес шлюза.

📙 Примечание

По умолчанию IP-адрес – 198.18.1.100, маска подсети – 255.255.255.0, адрес шлюза – 198.18.1.1

Шаг 3. Для проверки связности выполните команду ping 198.18.1.1 с помощью командной строки.

C:\User\admin>ping 198.18.1.1

Результат выполнения команды:

Pinging 198.18.1.1 with 32 bytes of data: Reply from 198.18.1.1: bytes=32 time<1ms TTL=64 Reply from 198.18.1.1: bytes=32 time<1ms TTL=64 Reply from 198.18.1.1: bytes=32 time<1ms TTL=64 Reply from 198.18.1.1: bytes=32 time=1ms TTL=64 Ping statistics for 198.18.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0msyes

Шаг 4. С помощью командной строки осуществите удаленное подключение, выполнив команду

C:\User\admin>telnet 198.18.1.1

Шаг 5. Введите логин и пароль для осуществления входа пользователя

SR-BE sr-be login:

📙 Примечание

По умолчанию логин admin, пароль admin, при вводе пароля символы на экране не отображаются

Удаленный вход в систему выполнен.

Выполните команду **show interfaces brief** чтобы узнать IP-адреса интерфейсов на сервисном маршрутизаторе.

Interface	HW Address	IPv4 Address	Admin/Link	DHCPv4 Description
eth1	94:3f:bb:00:2d:e3	unassigned	DOWN/DOWN	OFF
eth2	94:3f:bb:00:2d:fe	unassigned	DOWN/DOWN	OFF
eth3	94:3f:bb:00:2d:fe	unassigned	UP/UP	OFF
eth4	94:3f:bb:00:2d:fe	unassigned	UP/DOWN	ON
vlan1	94:3f:bb:00:2d:ff	192.168.0.1/24	UP/UP	OFF

📙 Примечание

При отсутствии подключения к сервисному маршрутизатору обратитесь в службу поддержки https://istokmw.ru/support/

2.3 Подключение через консольный порт RS-232

Устройство имеет консольный порт на корпусе.

Для соединения через консоль необходимо наличие следующего оборудования:

- терминал или компьютер с последовательным портом и возможностью эмулировать терминал;
- о кабель консольный RJ45-DB9.

📙 Примечание

Кабель консольный RJ45-DB9 не входит в комплект поставки и приобретается отдельно. Если ноутбук или компьютер пользователя не оснащен интерфейсом RS-232, необходимо приобрести кабель-адаптер USB-RS232. Кабель-адаптер USB-RS232 не входит в комплект поставки и приобретается отдельно. Установить используемые адаптером драйвера по необходимости.

Для установки соединения через консоль выполните следующие действия:

Шаг 1. Включите АРМ и войдите в ОС с использованием учетной записи администратора.

Шаг 2. Соедините порт «Console» устройства с портом RS-232 компьютера с помощью кабеля консольного (рисунок 1).



Рисунок 1 – Распределение контактов разъемов кабеля

Шаг 3. Подключите кабель к терминалу или последовательному порту компьютера с установленным программным обеспечением эмуляции терминала.

Шаг 4. Запустите терминальную программу (например, PuTTY или Microsoft Windows HyperTerminal) и установите параметры программного обеспечения эмуляции терминала.

Выполните следующие настройки интерфейса RS-232:

- о скорость: 115200 бит/с;
- о биты данных: 8 бит;
- о четность: нет;
- о стоповые биты: 1;
- о управление потоком: нет.

Шаг 5. Подключите питание к устройству. На терминале появится загрузочная последовательность.

После выполнения загрузочной последовательности появится командная строка с приглашением устройства:

SR-BE sr-be ttySO Sr-be login: Password:

Шаг 6. Введите имя пользователя и пароль.

По умолчанию для входа в систему с правами администратора используйте:

- о имя пользователя: admin;
- о пароль: admin.

Устройство готово к настройке.

2.4 Настройки по умолчанию

На устройство загружена начальная конфигурация, которая включает минимально необходимые базовые настройки:

- все порты устройства предназначены для подключения к внешней сети (WANпорты, их подробное описание представлено в подразделе <u>Описание WAN-</u> <u>портов</u> настоящей инструкции);
- все интерфейсы устройства открыты для удаленного доступа с помощью протоколов Telnet, SSH.

 на устройстве задано имя пользователя и пароль (см. <u>Таблица 4</u>). Для настройки устройства при первом включении в конфигурации устройства используется учетная запись администратора admin;

Таблица 4 – Имя пользователя и пароль

Имя пользователя	Пароль
admin	admin
Примечание - имя пользователя и пароль вводят с учетом регистра.	

- устройство использует заданное на заводе имя устройства «sr-be» и доменное имя «sr-be». При конфигурировании имя устройства меняют.
 Подробнее об этом можно прочитать в разделе <u>Настройка имени устройства</u> и доменного имени системы настоящей инструкции;
- функция SSH для удаленного управления устройством по умолчанию включена:

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

Для просмотра начальной конфигурации выполните команду:

admin@sr-be# show running-config

Результат выполнения команды:

interface eth1	
exit	
interface eth2	
exit	
interface eth3	
no shutdown	
exit	
interface eth4	
ip address dhcp	

exit
log deamon level WARNING
ipv6 dhcp relay dhcp6-relay vrf default exit
log netflow maxsize 1G
radius accounting off
samba server off exit
system tty timeout 600 system ssh timeout 600 system telnet timeout 600 system ssh on
system integrity alert led
system memory-cache policy aggressive
interface vlan1 vid 1 ethertype 0x8100 no shutdown ip address 192.168.0.1/24 exit
logging monitor 7
router ldp exit
router rsvp exit
end

Для просмотра более подробных настроек по умолчанию выполните команды:

admin@sr-be# show profile name boot

3 Изменение паролей пользователей

Имя пользователя и пароль вводится при входе в систему во время сеансов администрирования устройства.

А Внимание!

Для защиты входа в систему необходимо сменить пароль пользователя «admin».

3.1 Пользователь «admin»

Для изменения пароля пользователя «admin» выполните следующие команды:

admin@sr-be#configure terminal admin@sr-be(config)#username edit admin password Enter password: <new-password> Repeat password: <new-password> admin@sr-be(config)# exit

где <new-password> - новый пароль для пользователя «admin».

📫 Примечание

При вводе пароля символы на экране не отображаются

3.2 Создание групп

Создайте новую группу с указанием уровня привилегий от 1 до 14 с помощью следующих команду group <group_name> privilege <privilege_level>.

где: - <group_name> - имя новой группы;

- <privilege_level> - уровень привилегий у группы.

Пример создания группы «operators» с уровнем привилегий 1:

admin@sr-be#**configure terminal** admin@sr-be(config)#**group operators privilege 1** Для проверки результата выполните команду: admin@sr-be(config)#**show groups**

Group | Privilege -----admin | 15 service | 1 operators | 1

3.3 Создание новых пользователей

Для создания пользователя укажите имя пользователя и имя группы с необходимым уровнем привилегий, используя команду **username add <username> group <usergroup>**. где: - <username> - имя нового пользователя;

- <usergroup> - группа к которой добавляется новый пользователь.

Пример создания пользователя «boris» с паролем «b0ris_istok» группы «operators»:

admin@sr-be#**configure terminal** admin@sr-be(config)#**username add boris group operators** Enter password: Repeat password:

Для проверки результата выполните команду show users.

admin@sr-be#configure terminal admin@sr-be(config)#show users

Результат выполнения команд:

User | Group | Type | Privilege -----admin | admin | local | 15 boris | operators | local | 1

4 Настройка имени устройства и доменного имени системы

Имя устройства используется в запросах интерфейса командной строки и именах файлов конфигурации по умолчанию. Для смены имени устройства и доменного имени системы используйте команду system host-name <hostname> domain-name <domain_name>.

где: - <hostname> - имя устройства;

- <domain_name> - доменное имя.

Например, для смены имени устройства «RouterA» и доменного имени «istok.ab» выполните команды:

admin@sr-be#**configure terminal** admin@sr-be(config)# **system host-name RouterA domain-name istok.ab**

После применения конфигурации приглашение командной строки изменится на значение, заданное параметром <hostname>.

Для проверки настроек имени устройства выполните команду:

admin@RouterA(config)#show host-name

Результат выполнения команды:

RouterA

Для проверки настроек доменного имени выполните команду:

admin@RouterA(config)#show domain-name

Результат выполнения команды:

RouterA.istok.ab

5 Работа с конфигурацией

5.1 Применение настроек

5.1.1 Применение локальных профилей

Для загрузки существующего файла конфигурации, расположенного на устройстве, используйте команду **load**. Например, для загрузки конфигурационного файла «TEST»:

admin@sr-be# load TEST

Результат выполнения команды:

Clearing configuration for module debug Loading configuration for module debug Clearing configuration for module system_configs Clearing configuration for module dhcp_client Clearing configuration for module routing

📁 Примечание

Перед загрузкой нового профиля удаляются все текущие настройки.

5.1.2 Применение профилей, скаченных через TFTP

Шаг 1. Убедитесь в наличии TFTP-сервера в сети.

Шаг 2. Загрузите файл с TFTP-сервера. Для этого выполните команду с указанием IP-адреса TFTP-сервера и имени профиля:

admin@sr-be# copy profile TEST2 from url tftp 192.168.1.14 remotedir /wew/

Шаг 3. Для проверки загрузки файла выполните команду:

admin@sr-be#**show profiles**

Шаг 4. Загрузите скаченный файл конфигурации, выполнив команду:

admin@sr-be# load TEST2

Результат выполнения команды:

Clearing configuration for module debug Loading configuration for module debug Clearing configuration for module system_configs Clearing configuration for module dhcp_client Clearing configuration for module routing

5.2 Сброс настроек

Для выполнения загрузки файла начальной конфигурации выполните команду:

admin@sr-be#load default

Результат выполнения команды:

Clearing configuration for module debug Loading configuration for module debug Clearing configuration for module system_configs Clearing configuration for module dhcp_client Clearing configuration for module l2tp_server Clearing configuration for module l2tp_client

5.3 Сохранение настроек

5.3.1 Сохранение профилей локально

Для сохранения сконфигурированного профиля, например, «TEST», выполните команду:

admin@sr-be#**write TEST**

Если указан параметр comment, то к профилю добавляется комментарий, который будет показан при выводе доступных профилей:

admin@sr-be#write TEST comment keep

Для вывода на экран сохраненного профиля конфигурации выполните команду:

admin@sr-be#show profile name TEST

Результат выполнения команды:

Profile Name Loaded by Created by Loaded at											
	TEST	I	l	admin		I					

Для вывода на экран содержимого профиля конфигурации TEST выполните команду:

admin@sr-be#show profile name TEST detail

Результат выполнения команды:

```
{
    "comment": "",
    "watchdog": {
        "watchdog_interval": 60,
        "watchdog_enabled": false
},
    "dynamic_routing_imi": {
        "commands": [
            "!",
        "no service password-encryption",
            "!",
        "logging monitor 7"
```

Для вывода на экран имен всех профилей конфигурации выполните команду:

admin@sr-be#show profiles

Результат выполнения команды:

Flags:	b - boot profile	e, I - last loac	ded profile, m - profile was modified or corrupted
Flags	Profile Name	e Comment	t
	TEST	keep	1

Работа	С	конф	игу	заци	1ей
	_				

T

| bl | startup

Для удаления сконфигурированного профиля используйте команду:

admin@sr-be# no profile TEST

Для проверки удаления профиля выполните команду:

I

admin@sr-be#show profiles

Результат выполнения команды:

Flags:	Flags: b - boot profile, I - last loaded profile, m - profile was modified or corrupted								
Flag	Flags Profile Name Comment								
	· · · · · · · · · · · · · · · · · · ·								
bl	startup		I						

5.3.2 Сохранение профилей удаленно по протоколу TFTP

Схема подключения сети - Рисунок 2.



Рисунок 2 – Применение профилей, скачанных через TFTP-сервер



Для копирования файла текущей конфигурации на TFTP-сервер в указанную директорию выполните команду: admin@sr-be# copy profile TEST to url tftp 192.168.1.14 remotedir /wew/

6 Настройка WAN-портов

6.1 Описание WAN-портов

Порты WAN используются для подключения устройства к внешней сети, в частности для подключения к сети провайдера с целью получения доступа в интернет. Устройство имеет два WAN-порта SFP (1000BASE-X), что позволяет использовать подключение сразу к нескольким операторам связи (рисунок 3).



Рисунок 3 – WAN-порты. Передняя панель ISN50502T5-MA

Имена интерфейсов начинаются с префикса eth (Ethernet), далее указывается порядковый номер порта: eth1 - eth4. Нумерация портов соответствует маркировке на передней панели устройства. Названия портов чувствительны к регистру и указываются только с маленькой буквы.

📙 Примечание

В модулях расширения нумерация WAN-портов может меняться, начиная с третьего порядкового номера.

6.2 Назначение ІР-адреса

6.2.1 Назначение статического IP-адреса

Для настройки статического IP-адреса WAN-интерфейсу выполните следующие команды

admin@sr-be#configure terminal admin@sr-be(config)#interface eth1 admin@sr-be(config-if-[eth1])#no shutdown admin@sr-be(config-if-[eth1])#ip address 172.16.0.2 255.255.0.0 admin@sr-be(config-if-[eth1])#exit где: - 172.16.0.2 - статический ІР-адрес;

- 255.255.0.0 - маска подсети.

📙 Примечание

Для присвоения статического IP-адреса отключите динамическое получение IPадреса командой no ip address dhcp

Вместо маски подсети вида «255.255.0.0» можно ввести длину префикса «/16», например:

admin@sr-be(config-if-[eth1])#ip address 172.16.0.2/16

Убедитесь, что адрес назначен интерфейсу после применения конфигурации.

Выполните следующую команду:

admin@sr-be(config)#show interfaces eth1

Результат выполнения команды:

eth1: Administrative status: UP Link: DOWN IPv4 Address: 172.16.0.2/16 RX: 0 bytes / 0 packets TX: 728 bytes / 6 packets MTU: 1500 HW Address: 94:3f:bb:ff:ff:03 IPv6 Address: fe80::963f:bbff:fe00:2de3/64 Autonegotiation: on Duplex: unknown Speed: unknown Supported speeds (Mb/s): 10, 100, 1000 ALLMULTI mode ON RPS: disabled

Также проверить IP-адрес интерфейса можно с помощью команды:

admin@sr-be(config)#show interfaces brief

Результат выполнения команды:

Interface	HW Address	IPv4 Address	Admin/Link	DHCPv4	Description
eth1	94:3f:bb:00:2d:e3	172.16.0.2/16	UP/DOWN	OFF	
eth2	94:3f:bb:00:2d:fa	unassigned	DOWN/DOWN	OFF	
eth3	94:3f:bb:00:2d:fc	unassigned	DOWN/DOWN	OFF	
eth4	94:3f:bb:00:2d:fe	unassigned	DOWN/DOWN	OFF	
vlan1	94:3f:bb:00:2d:ff	192.168.0.1/24	UP/UP	OFF	

Для отмены статического IP-адреса выполните команды:

admin@sr-be#configure terminal admin@sr-be(config)#interface eth1 admin@sr-be(config-if-[eth1])# no ip address admin@sr-be(config-if-[eth1])# exit

6.2.2 Получение динамического IP-адреса

Схема подключения сети - Рисунок 4.



Рисунок 4 – Получение динамического IP-адреса



Перед настройкой DHCP на устройстве убедитесь, что DHCP-сервер готов.

Пример настройки получения IP-адреса от DHCP-сервера на WAN-интерфейсе eth1:

admin@sr-be**#configure terminal** admin@sr-be(config)**#interface eth1** admin@sr-be(config-if-[eth1])**#ip address dhcp** admin@sr-be(config-if-[eth1])**#no shutdown** admin@sr-be(config-if-[eth1])**#exit**

Убедитесь, что адрес назначен интерфейсу после применения конфигурации.

Для этого выполните следующую команду:

admin@sr-be(config)#show interfaces eth1

Результат выполнения команды:

eth1: Administrative status: UP Link: UP IPv4 Address: 172.16.0.2/16 RX: 31332 bytes / 486 packets TX: 2138 bytes / 25 packets MTU: 1500 HW Address: 94:3f:bb:ff:ff:03 IPv6 Address: fe80::963f:bbff:fe00:2de3/64 Autonegotiation: on Duplex: unknown Speed: unknown Supported speeds (Mb/s): 10, 100, 1000 ALLMULTI mode ON RPS: disabled

Также проверить IP-адрес интерфейса можно с помощью команды:

admin@sr-be(config)#show interfaces brief

Результат выполнения команды:

InterfaceHW AddressIPv4 AddressAdmin/LinkDHCPv4 Descriptioneth194:3f:bb:00:2d:e3172.16.0.2/16UP/UPONeth294:3f:bb:00:2d:fa unassignedDOWN/DOWNOFF

eth3	94:3f:bb:00:2d:fc	unassigned	DOWN/DOWN	OFF
eth4	94:3f:bb:00:2d:fe	unassigned	DOWN/DOWN	OFF
vlan1	94:3f:bb:00:2d:ff	192.168.0.1/24	I UP/UP	OFF

Для удаления полученного IP-адреса по протоколу DHCP выполните команды:

admin@sr-be#**configure terminal** admin@sr-be(config)#**interface eth1** admin@sr-be(config-if-[eth1])#**no ip address dhcp**

6.3 Настройка маршрута по умолчанию

6.3.1 Добавление статического маршрута по умолчанию

Статические маршруты обеспечивают фиксированные пути маршрутизации по сети. Они настраиваются вручную на маршрутизаторе. Если топология сети изменяется, статический маршрут должен быть обновлен.

Статический маршрут по умолчанию добавляется в режиме конфигурации с помощью команды **ip route**. Пример схемы сети - <u>Рисунок 5</u>.



Рисунок 5 – Схема настройки маршрута по умолчанию

Для настройки на сервисном маршрутизаторе маршрута по умолчанию выполните команду:

admin@sr-be#**configure terminal** admin@sr-be(config)#**ip route default 172.16.0.1**

Эта запись будет аналогична записи следующего вида:

admin@sr-be#configure terminal

admin@sr-be(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.1

Чтобы убедиться, что вы правильно настроили статическую маршрутизацию по умолчанию, выполните команду **show ip route** и найдите статические маршруты, обозначенные буквой «S»:

admin@sr-be(config)#show ip route

Результат выполнения команды:

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
IP Route Table for VRF "default"
Gateway of last resort is 172.16.0.1 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 172.16.0.1, eth1
```

- C 127.0.0.0/8 is directly connected, lo
- C 172.168.0.0/24 is directly connected, vlan1

6.3.2 Изменение маршрута по умолчанию

Удалите старый маршрут по умолчанию с помощью команд:

admin@sr-be#**configure terminal** admin@sr-be(config)#**no ip route default 172.16.0.1**

Эта запись будет аналогична записи следующего вида:

admin@sr-be#**configure terminal** admin@sr-be(config)#**no ip route 0.0.0.0 0.0.0.0 172.16.0.1**

Введите новый маршрут по умолчанию, например:

admin@sr-be(config)#ip route default 172.20.0.1

6.4 Настройка правил фильтрации

Ниже приведен пример настройки удаленного доступа к устройству по SSH от хоста с IP-адресом 192.168.3.16/24. Пример схемы сети - <u>Рисунок 6</u>.



Рисунок 6 – Схема настройки правил фильтрации

Шаг 1. Создайте access-list «100» с IP-адресом 192.168.3.16/24, порт назначения 22, выполнив команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#ip access-list 100 sourceip 192.168.3.16/24 destinationports 22 protocol tcp
```

Шаг 2. Создайте access-list «500» с IP-адресом сети 0.0.0.0/0, порт назначения 22, выполнив команды:

admin@sr-be(config)#ip access-list 500 sourceip 0.0.0.0/0 destinationports 22 protocol tcp

Шаг 3. Для проверки создания access-list (ов) выполните команду:

admin@sr-be(config)#show ip access-list

Команда выведет все списки доступа, прописанные на устройстве:

Name # Rule 100 1 src: 192.168.3.16/24 dp: 22 prot: 6 500 1 src: 0.0.0.0/0 dp: 22 prot: 6

Шаг 4. Настройте ограничения удаленного доступа к устройству, выполнив команду:

admin@sr-be(config)#ip filter input position 10 permit access-list 100

Команда разрешает входящий ТСР-трафик от хоста 192.168.3.16/24, порт назначения 22.

admin@sr-be(config)#ip filter input position 20 deny access-list 500

Команда запрещает весь входящий ТСР-трафик от других хостов, порт назначения

22.

Шаг 5. Проверьте настройки, выполнив команду:

admin@sr-be(config)#show ip filter

Результат выполнения команды:

Cha	Chain INPUT (policy ACCEPT 0 packets, 0 bytes)									
#	Pkts	Bytes	Action	Rule config						
0	0	0	permit	src: 192.168.3.16/24 dp: 22 prot: 6						
1 0 0			deny	src: 0.0.0.0/0 dp: 22 prot: 6						

Для отмены настройки правил фильтрации выполните команды в режиме конфигурации:

admin@sr-be(config)#**no ip filter input access-list 100** admin@sr-be(config)#**no ip filter input access-list 500**

Для удаления access-list выполните команды в режиме конфигурации:

admin@sr-be(config)#**no ip access-list 100** admin@sr-be(config)#**no ip access-list 500**

7 Настройка VLAN

VLAN – коммутируемая сеть, которая логически сегментирована по функциям, проектной группе или приложению, независимо от физического местоположения пользователей. VLAN имеют те же атрибуты, что и физические локальные сети, но вы можете группировать конечные станции, даже если они физически не расположены в одном сегменте локальной сети. Любой LAN-порт устройства может принадлежать VLAN, а одноадресные, широковещательные и многоадресные пакеты пересылаются и заполняются только конечными станциями в VLAN.

Пример схемы сети - Рисунок 7.



Рисунок 7 – Схема настройки локальной сети

7.1 Настройка сети

Для создания VLAN введите идентификационный номер VLAN-ID (vid) с помощью команд:

admin@sr-be#configure terminal admin@sr-be(config)#vlan20

📙 Примечание

- 1. VLAN-ID может принимать значения от 2 до 4094.
- 2. При необходимости задайте имя VLAN с помощью команды name.
- 3. Для создания списка VLAN перечислите VLAN-ID через «,» или «-» в режиме

глобальной конфигурации: vlan 2,3,5-8

Назначьте VLAN20 саб-интерфейсу eth1.2

admin@sr-be#configure terminal admin@sr-be(config)#interface eth1 admin@sr-be(config-if-[eth1])#no shutdown admin@sr-be(config-if-[eth1])#exit admin@sr-be(config)#interface eth1.2 admin@sr-be(config-if-[eth1.2])#vid 20 ethertype 0x8100 admin@sr-be(config-if-[eth1.2])#no shutdown admin@sr-be(config-if-[eth1.2])#no shutdown

Настройте статический IP-адрес на VLAN-интерфейсе

admin@sr-be(config)#interface vlan20 admin@sr-be(config-if-[vlan20])#vid 20 admin@sr-be(config-if-[vlan20])#ip address 192.168.3.1/24 admin@sr-be(config-if-[vlan20])#no shutdown admin@sr-be(config-if-[vlan20])#exit

Также возможно назначение динамического IP-адреса:

admin@sr-be(config)#interface vlan20

admin@sr-be(config-if-[vlan20])#vid 20 admin@sr-be(config-if-[vlan20])#ip address dhcp admin@sr-be(config-if-[vlan20])#no shutdown admin@sr-be(config-if-[vlan20])#exit

Для удаления VLAN используйте команды:

admin@sr-be#configure terminal admin@sr-be(config)#no vlan20

А Внимание!

Прежде чем удалить VLAN, убедитесь, что всем интерфейсам с данным VLAN назначен другой VLAN.

7.2 Проверка настроек

Выполните команду show vian all для проверки созданных VLAN

VLAN idNameMember ports (t-tagged, u-untagged)20Vlan0020--

Выполните команду show interfaces eth1.2 для проверки состояния eth1.2

eth1.20 vid20: Administrative status: UP Link: DOWN RX: 0 bytes / 0 packets TX: 0 bytes / 0 packets MTU: 1500 Tx buffer: 1000 HW Address: 94:3f:bb:00:30:4a IPv6 Address: fe80:963f:bbff:fe00:304a/64 EtherType: 0x8100 Encapsulation: dot1q

Выполните команду show interfaces vlan20 для проверки настройки vlan20

vlan20 vid 20: Administrative status: UP Link: DOWN IPv4 Address: 192.168.3.1/24 RX: 0 bytes / 0 packets TX: 0 bytes / 0 packets MTU: 1500 Tx buffer: 1000 HW Address: 94:3f:bb:00:30:4c IPv6 Address: fe80:963f:bbff:fe00:304c/64 EtherType: 0x8100 Encapsulation: dot1q

8 Настройка удаленного доступа

8.1 Настройка удаленного доступа по протоколу SSH

Пример схемы настройка удаленного доступа по протоколу SSH через WAN-порт - <u>Рисунок 8</u>.



Рисунок 8 – Схема настройки удаленного доступа по протоколу SSH



Настройте WAN-порт eth1

admin@sr-be**#configure terminal** admin@sr-be(config)**#interface eth1** admin@sr-be(config-if-[eth1])**#no shutdown** admin@sr-be(config-if-[eth1])**#no ip address dhcp** admin@sr-be(config-if-[eth1])**#ip address 192.168.1.1/24** admin@sr-be(config-if-[eth1])**#exit**

Для настройки удаленного доступа необходимо указать IP-адрес интерфейса, который будет принимать SSH-соединение:

admin@sr-be(config)#system ssh listen-address 192.168.1.1

Для вывода на экран настроек SSH-сервера выполните команду:

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

Результат выполнения команды:

SSH server enabled Version: 2 Port: 22 Listen addresses: 192.168.1.1 all-ipv6 Whitelist: all all-ipv6 SSH timeout: 600

Выполните команду **ssh admin@192.168.1.1** на устройстве, через которое осуществляться подключение и дождитесь приглашения ввода учётных данных (password)

The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established. RSA key fingerprint is SHA256:5DGX/BWLmyFK1cBZLAJGvwrZNQVCMFP65HZdLJEjttU. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.1.1' (RSA) to the list of known hosts. admin@192.168.1.1's password:

Для удаления настроенных параметров SSH выполните команды:

admin@sr-be#**configure terminal** admin@sr-be(config)# **no system ssh listen-address 192.168.1.1**

Протокол SSH включен по умолчанию. Для отключения SSH на устройстве выполните команды:

admin@sr-be#configure terminal admin@sr-be(config)# system ssh off

8.2 Настройка удаленного доступа по протоколу Telnet

Пример схемы настройки удаленного доступа по протоколу Telnet через WAN-порт - <u>Рисунок 9</u>.



Рисунок 9 – Схема настройки протокола Telnet

А Внимание!

Для подключения через Telnet должен быть настроен IP-адрес на интерфейсе устройства, через который будет осуществляться подключение.

Настройте WAN-порт eth1

admin@sr-be**#configure terminal** admin@sr-be(config)**#interface eth1** admin@sr-be(config-if-[eth1])**#no shutdown** admin@sr-be(config-if-[eth1])**#no ip address dhcp** admin@sr-be(config-if-[eth1])**#ip address 198.18.1.1/24** admin@sr-be(config-if-[eth1])**#exit**

Включите протокол Telnet

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

Для вывода на экран статуса Telnet-сервера выполните команду:

admin@sr-be(config)#show system telnet

Результат выполнения команды:

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

Для отключения Telnet на устройстве выполните команды:

admin@sr-be#configure terminal admin@sr-be(config)# system telnet off

9 Настройка сервера доменного имени

DNS-серверы поддерживают каталог доменных имен и сопоставлений IP-адресов. Служба доменных имен используется для преобразования доменных имен в IP-адреса и наоборот.

Это позволяет использовать как преобразование имени в IP-адрес, так и преобразование IP-адреса в имя внутри сети.

Когда клиент отправляет доменное имя на DNS-сервер для разрешения, сервер либо преобразует имя в IP-адрес в своем локальном кэше, либо обращается к другому DNS-серверу, чтобы получить IP-адрес для клиента.

Локальный DNS-сервер потребуется, если рабочие станции обмениваются данными по имени рабочей станции, а не по IP.

Пример схемы сети - Рисунок 10.



Рисунок 10 – Настройка сервера доменного имени в локальной сети

Шаг 1. Настройте интерфейс eth1 на сервисном маршрутизаторе.

RouterA#configure terminal RouterA(config)#interface eth1 RouterA(config-if-[eth1])#no shutdown RouterA(config-if-[eth1])#no ip address dhcp RouterA(config-if-[eth1])#ip address 100.10.10.10/24 RouterA(config-if-[eth1])#exit

Шаг 2. Настройте loopback интерфейс

RouterA(config)#interface lo1 RouterA(config-if-[lo1])#no shutdown RouterA(config-if-[lo1])#ip address 1.1.1.1/24 RouterA(config-if-[lo1])#exit

Шаг 3. Настройте DNS сервер

RouterA(config)**#ip route 0.0.0/0 100.10.10.20** RouterA(config)**#dns-server** RouterA(dns-server)**#zone master test.do** RouterA(config-dnszone-[test.do])**#set ns ns1** RouterA(config-dnszone-[test.do])**#set refresh 300 sec** RouterA(config-dnszone-[test.do])**#entry a 192.168.0.1 pc** RouterA(config-dnszone-[test.do])**#entry a 100.10.10.10 ns1** RouterA(config-dnszone-[test.do])**#entry a 1.1.1.1 lo1** RouterA(config-dnszone-[test.do])**#entry ns ns1** RouterA(config-dnszone-[test.do])**#entry ns ns1** RouterA(config-dnszone-[test.do])**#entry ns ns1** RouterA(config-dnszone-[test.do])**#exit** RouterA(dns-server)**#dns-server on** RouterA(dns-server)**#end**

Для отключения службы DNS-сервера выполните команды:

RouterA(config)#dns-server RouterA(dns-server)#dns-server off

9.1 Проверка настроек

Шаг 1. Проверьте настройки DNS-сервера выполнив команду show dns-server:

DNS Server
Status: running
Listen address:
any
Listen port: 53
Allow query address:
any
Allow transfer address:
any
Recursion: False
Master zone: test.do
\$TTL 38400
@ IN SOA ns1 admin@test.do (
1438828620

300 3600 604800 86400) lo1 A 1.1.1.1 pc A 192.168.0.1 ns1 A 100.10.10.10 @ NS ns1

Шаг 2. Выйдите из учетной записи пользователя выполнив команду exit:

C:\Users\Conference>

Шаг 3. Проверьте записи DNS-сервера выполнив на PC команды: nslookup pc.test.do 100.10.10.10

Server: UnKnown Address: 100.10.10.10 Name: pc.test.do Address: 192.168.0.1

nslookup ns1.test.do 100.10.10.10

Server: UnKnown Address: 100.10.10.10 Name: ns1.test.do Address: 100.10.10.10

10Настройка DHCP-сервера на устройстве

Устройство поддерживает клиентов в VLAN, объединяя их в виртуальную локальную сеть, независимо от ее физической топологии. Устройство может использовать протокол динамической конфигурации хоста (DHCP), чтобы включить автоматическое назначение конфигураций IP для узлов в этих сетях.

Пример схемы подключения - Рисунок 11.



Рисунок 11 – Настройка DHCP-сервера на устройстве

Для настройки DHCP-сервера на устройстве выполните команды:

admin@sr-be#configure terminal admin@sr-be(config)#ip dhcp pool 10 admin@sr-be(config-dhcp[10])#network 192.168.3.0/24 admin@sr-be(config-dhcp[10])#range 192.168.3.3 192.168.3.50 admin@sr-be(config-dhcp[10])#exit admin@sr-be(config)#ip dhcp server on

📙 Примечание

1. Номер пула должен быть назначен в диапазоне от 1 до 65535.

2. network 192.168.3.0/24 – подсеть, для которой будут выдаваться адреса DHCP-сервером. 3. range 192.168.3.3 192.168.3.50 – начальный и конечный IP-адрес диапазона адресов.

4. Вывод команды range возможен только, если ранее была выполнена команда network

Проверьте настройки DHCP-сервера с помощью команды:

admin@sr-be#**show ip dhcp**

Результат выполнения команды:

VRF: default default-lease-time 600; Pool: 10 subnet 192.168.3.0 netmask 255.255.255.0 { range 192.168.3.3 192.168.3.50; }

Для удаления пула IP-адресов 192.168.3.3 – 192.168.3.50 выполните команды:

admin@sr-be#configure terminal admin@sr-be(config)#ip dhcp pool 10 admin@sr-be(config-dhcp)#no range 192.168.3.3 192.168.3.50 admin@sr-be(config-dhcp)#exit

Для удаления всего набора локальных адресов выполните команды:

admin@sr-be#configure terminal admin@sr-be(config)#no ip dhcp pool 10

Для отключения службы DHCP-сервера выполните команды:

admin@sr-be#configure terminal admin@sr-be(config)#ip dhcp server off

11 Настройка журналирования событий на удаленный Syslog-сервер

Данные из системного журнала устройства можно пересылать по протоколу Syslog на удаленный сервер. Сбор лог-сообщений позволит иметь полную статистику происходящих с устройством событий, проводить анализ и заранее выявлять возможные проблемы.

Пример схемы сети - Рисунок 12

Syslog - сервер			Сервисный					\frown
	192.168.1.0/24	маршрутизатор		WAN (eth1) 172.16.0.0/16 W		VAN 📑	Оператор связи	
	192.168.1.11	192.16.0.2	17	72.16.0.2	172.16.	.0.1		

Рисунок 12 – Схема настройки журналирования событий на удаленный Syslog-сервер

Выполните команды для проверки статуса логирования:

admin@sr-be#configure terminal admin@sr-be(config)#show logs status

Результат выполнения команды:

access_violation : on access_list : off pim ipv4 : off pim ipv6 : off netflow : off pppoe-server : off pptp-server : off syslog : on kern : on vpn : off daemon : on command-history : on system_integrity_log : on

По умолчанию, лог сообщений от устройства на Syslog-сервер будут отсылаться в следующих категориях:

- о syslog лог системных изменений;
- kern– лог сообщений от ядра Linux и предупреждения, которые могут быть полезны при устранении ошибок пользовательских модулей, встроенных в ядро;
- daemon лог сообщений о различных процессах, которые запущены в системе (демоны);
- о command-history лог истории ввода команд.

Чтобы настроить отправку логов на устройстве, необходимо указать IP-адрес удаленного Syslog-сервера, выполнив команды:

admin@sr-be#**configure terminal** admin@sr-be(config)#**log syslog remote 192.168.1.11**

Для проверки настроек выполните команду:

admin@sr-be(config)#show running-config

Результат выполнения команды:

Часть вывода пропущена для краткости

log syslog remote 192.168.1.11

system tty timeout 600

•••

...

Для отмены отправки логов на Syslog-сервер выполнив команды:

admin@sr-be#**configure terminal** admin@sr-be(config)#**log syslog remote 0.0.0.0**

12Установка даты, времени и часового пояса

Для вывода на экран текущего времени и даты выполните команду:

admin@sr-be#**show clock**

Результат выполнения команды:

Чт янв 30 08:41:04 MSK 2021

12.1 Настройка времени

Установите текущее время с помощью команды system clock time <HH:MM[:SS]>, например:

admin@sr-be#**configure terminal** admin@sr-be(config)#**system clock time 12:30:16** admin@sr-be(config)#**show clock**

Результат выполнения команды:

Чт янв 30 12:30:22 MSK 2021

12.2 Настройка даты

Установите дату с помощью команды system clock date <DD.MM.YYYY>, например:

admin@sr-be#configure terminal admin@sr-be(config)#system clock date 18.08.2021 admin@sr-be(config)#show clock

Результат выполнения команды:

Ср авг 18 12:31:22 МSK 2021

12.3 Смена часового пояса

Для смены часового пояса используйте команду **system clock timezone**, далее нажмите <Tab> для выбора страны, нажмите <Tab> для выбора города, например:

admin@sr-be#**configure terminal** admin@sr-be(config)#**system clock timezone Europe Moscow**

12.4 Настройка синхронизации времени с NTP-сервера

Схема подключения сети - Рисунок 13.



Рисунок 13 – Настройка синхронизации времени с NTP-сервера

Для настройки синхронизации с NTP-сервером выполните команды:

admin@sr-be#configure terminal admin@sr-be(config)#ntp server 192.168.1.15 admin@sr-be(config)#ntp restrict default kod nomodify notrap noquery nopeer admin@sr-be(config)#ntp on admin@sr-be(config)#exit

📙 Примечание

Чтобы синхронизировать время с помощью протокола NTP, следует предварительно вручную настроить текущее время, дату и часовой пояс (см. подразделы Сохранение настроек, Применение настроек, Сброс настроек). При сильной разнице (более 1000 секунд) синхронизация осуществляться не будет.

13Команды диагностики

13.1 Ping

Используйте команду **ping** для диагностики проблем сетевого соединения между устройствами. С помощью эхо-пакетов ICMP можно определить активно ли удаленное устройство, узнать время задержек при передаче пакетов и наличие их потерь.

Пример команды для проверки доступности хоста 192.168.3.2 в сети:

admin@sr-be#ping 192.168.3.2 repeat 4

Результат выполнения команды:

PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data. 64 bytes from 192.168.3.2: icmp_seq=1 ttl=128 time=1.27 ms 64 bytes from 192.168.3.2: icmp_seq=2 ttl=128 time=1.27 ms 64 bytes from 192.168.3.2: icmp_seq=3 ttl=128 time=1.16 ms 64 bytes from 192.168.3.2: icmp_seq=4 ttl=128 time=1.36 ms

--- 192.168.3.2 ping statistics ---4 packets transmitted, 4trace received, 0% packet loss, time 7ms rtt min/avg/max/mdev = 1.164/1.266/1.362/0.078 ms

Прервать выполнение команды можно сочетанием клавиш <Ctrl + C>.

13.2 Traceroute

Команда traceroute используется для обнаружения путей следования пакета до адресов удаленных устройств, а также точек нарушения маршрутизации.

Пример команды для определения и вывода на экран маршрута следования данных до хоста 192.168.3.2 в сети:

admin@sr-be#traceroute 192.168.3.2

Результат выполнения команды:

```
traceroute to 192.168.3.2 (192.168.3.2), 30 hops max, 60 byte packets 1 192.168.3.2 0.987 ms 0.016 ms 0.016 ms
```

14Дополнительные руководства по работе с устройством

- 1. КРПГ.465614.001РЭ Руководство по эксплуатации.
- 2. RU.07622667.00026-01 34 01-1 Руководство оператора.
- 3. RU.07622667.00026-01 34 01-2 Руководство оператора. Приложение 1. Справочник команд CLI.
- 4. RU.07622667.00026-01 32 01 Руководство системного программиста.

15Техническая поддержка

На официальном сайте компании АО «НПП «Исток» им. Шокина» вы можете найти техническую документацию и обновить программное обеспечение устройства.

Официальный сайт компании: <u>https://istokmw.ru/</u>

Техническая поддержка



Официальный сайт компании: <u>https://istokmw.ru/</u>



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



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: <u>support@istokmw.ru</u> web: <u>https://istokmw.ru/support/</u>



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