



Сервисные маршрутизаторы

**ISN41508T3, ISN41508T3-M/ISES1004,
ISN41508T3-M, ISN41508T4, ISN41508T3-M-AC,
ISN41508T3-M/ISES1004, ISN41508T3-M/ISES0108,
ISN41508T3-M/ISES0114, ISN41508T3-M/ISES0116,
ISN41508T3-M/ISES1009, ISN41508T3-M-
AC/ISES1004, ISN41508T3-M-AC/ISES0108,
ISN41508T3-M-AC/ISES0114, ISN41508T3-M-
AC/ISES0116, ISN41508T3-M-AC/ISES1009**

Руководство по установке и быстрому запуску

КРПГ.465614.001Д26

Версия ПО 3.21

Версия документа	Дата выпуска	Содержание изменений
Версия 1.0	30.09.2021	Первая публикация
Версия программного обеспечения	3.21.21	

СОДЕРЖАНИЕ

Список рисунков	5
Список таблиц	7
Введение.....	8
Условные обозначения	9
1 Подключение к интерфейсу командной строки (CLI).....	10
1.1 Подключение через консольный порт RS-232	10
1.2 Настройки по умолчанию	11
2 Изменение паролей для пользователей	14
2.1 Пользователь «admin».....	14
2.2 Пользователь «serviceuser».....	14
2.3 Создание групп	14
2.4 Создание новых пользователей.....	15
3 Настройка сервера доменного имени	16
4 Настройка имени устройства и доменного имени системы.....	17
5 Настройка WAN-портов	18
5.1 Описание WAN-портов.....	18
5.2 Назначение IP-адреса	21
5.2.1 Назначение статического IP-адреса	21
5.2.2 Получение динамического IP-адреса	22
5.3 Настройка DHCP-сервера на устройстве	23
5.4 Настройка маршрута по умолчанию	25
5.4.1 Добавление статического маршрута по умолчанию	25
5.4.2 Изменение маршрута по умолчанию	26
5.5 Настройка удаленного доступа	26
5.5.1 Настройка удаленного доступа по протоколу SSH	26
5.5.2 Протокол SSH включен по умолчанию. Для отключения SSH на устройстве введите команду: 28	
5.5.3 Настройка удаленного доступа по протоколу TELNET	28
5.6 Настройка журналирования событий на удаленный Syslog-сервер.....	28
5.7 Настройка централизованной аутентификации пользователей через RADIUS- сервер	30
5.8 Настройка правил фильтрации	31
6 Настройка VLAN.....	33

6.1	Описание LAN-портов	33
6.2	Создание VLAN	36
6.3	Назначение Access-порта в VLAN	37
6.4	Назначение IP-адреса на VLAN-интерфейс	38
6.5	Настройка интерфейса в режиме Trunk	38
6.6	Назначение trunk-порту списка разрешенных VLAN	39
7	Работа с конфигурацией	40
7.1	Сохранение настроек	40
7.1.1	Сохранение профилей локально	40
7.1.2	Сохранение профилей удаленно по протоколу TFTP	41
7.2	Применение настроек	41
7.2.1	Применение локальных профилей	41
7.2.2	Применение профилей, скаченных через TFTP	41
7.3	Сброс настроек	42
7.3.1	Для выполнения загрузки файла начальной конфигурации введите команду:	42
7.3.2	Для удаления всех несохраненных настроек:	42
8	Установка даты, времени и часового пояса	43
8.1	Настройка времени	43
8.2	Настройка даты	43
8.3	Смена часового пояса	43
8.4	Настройка синхронизации времени с NTP-сервера	43
9	Команды диагностики	45
9.1	Ping	45
9.2	Traceroute	45
10	Дополнительные руководства по работе с устройством	46
11	Техническая поддержка	47

СПИСОК РИСУНКОВ

Рисунок 1 – Настройка сервера доменного имени в локальной сети	16
Рисунок 2 – Передняя панель ISN41508T3	18
Рисунок 3 – Передняя панель ISN41508T3-M	18
Рисунок 4 – Передняя панель ISN41508T4	18
Рисунок 5 – Передняя панель ISN41508T3-M-AC	19
Рисунок 6 – Передняя панель ISN41508T3-M/ISES1004	19
Рисунок 7 – Передняя панель ISN41508T3-M/ISES0108	19
Рисунок 8 – Передняя панель ISN41508T3-M/ISES0114	19
Рисунок 9 – Передняя панель ISN41508T3-M/ISES0116	19
Рисунок 10 – Передняя панель ISN41508T3-M/ISES1009	20
Рисунок 11 – Передняя панель ISN41508T3-M-AC/ISES1004	20
Рисунок 12 – Передняя панель ISN41508T3-M-AC/ISES0108	20
Рисунок 13 – Передняя панель ISN41508T3-M-AC/ISES0114	20
Рисунок 14 – Передняя панель ISN41508T3-M-AC/ISES0116	20
Рисунок 15 – Передняя панель ISN41508T3-M-AC/ISES1009	21
Рисунок 24 – Получение динамического IP-адреса	22
Рисунок 25 – Настройка DHCP-сервера на устройстве	24
Рисунок 26 – Настройка маршрута по умолчанию	25
Рисунок 27 – Настройка удаленного доступа по протоколу SSH	26
Рисунок 28 – Настройка журналирования событий на удаленный Syslog-сервер	28
Рисунок 29 – Настройка централизованной аутентификации пользователей через RADIUS-сервер	30
Рисунок 30 – Настройка правил фильтрации	32
Рисунок 31 – Передняя панель ISN41508T3	33
Рисунок 32 – Передняя панель ISN41508T3-M	33
Рисунок 33 – Передняя панель ISN41508T4	33
Рисунок 34 – Передняя панель ISN41508T3-M-AC	33
Рисунок 35 – Передняя панель ISN41508T3-M/ISES1004	34
Рисунок 36 – Передняя панель ISN41508T3-M/ISES0108	34
Рисунок 37 – Передняя панель ISN41508T3-M/ISES0114	34
Рисунок 38 – Передняя панель ISN41508T3-M/ISES0116	34
Рисунок 39 – Передняя панель ISN41508T3-M/ISES1009	34
Рисунок 40 – Передняя панель ISN41508T3-M-AC/ISES1004	35

Рисунок 41 – Передняя панель ISN41508T3-M-AC/ISES0108.....	35
Рисунок 42 – Передняя панель ISN41508T3-M-AC/ISES0114.....	35
Рисунок 43 – Передняя панель ISN41508T3-M-AC/ISES0116.....	35
Рисунок 44 – Передняя панель ISN41508T3-M-AC/ISES1009.....	35
Рисунок 45 – Создание VLAN	36
Рисунок 46 – Применение профилей, скаченных через TFTP-сервер	41
Рисунок 47 – Настройка синхронизации времени с NTP-сервера.....	43

СПИСОК ТАБЛИЦ

Таблица 1 – Стили оформления в документе	9
Таблица 2 – Режимы конфигурации	9

ВВЕДЕНИЕ

Настоящее руководство содержит рекомендации по начальной настройке сервисных маршрутизаторов ISN41508T3, ISN41508T3-M, ISN41508T4, ISN41508T3-M-AC, ISN41508T3-M/ISES1004, ISN41508T3-M/ISES0108, ISN41508T3-M/ISES0114, ISN41508T3-M/ISES0116, ISN41508T3-M/ISES1009, ISN41508T3-M-AC/ISES1004, ISN41508T3-M-AC/ISES0108, ISN41508T3-M-AC/ISES0114, ISN41508T3-M-AC/ISES0116, ISN41508T3-M-AC/ISES1009 (далее по тексту – устройство). 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.

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

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

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Для наглядности в тексте документации используются различные стили оформления.

Области применения стилей указаны в таблице 1.

Таблица 1 – Стили оформления в документе

Стиль оформления	Область применения	Пример
Полужирный текст	Выделяет имена команд	команды name
Курсивный (полужирный) текст	Выделяет предупреждения и примечания	« <i>Примечание</i> »; « <i>Внимание!</i> »
Шрифт Courier New	Выделяет примеры синтаксиса команд	admin@sr-be#configure terminal
Полужирный шрифт Courier New	Выделяет вывод CLI	Name # Rule 100 1 src: 192.168.1.1/32 500 1 src: 0.0.0.0/0

Устройство имеет несколько режимов конфигурации. Режимы представлены в таблице 2.

Таблица 2 – Режимы конфигурации

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

1 ПОДКЛЮЧЕНИЕ К ИНТЕРФЕЙСУ КОМАНДНОЙ СТРОКИ (CLI)

1.1 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;
- 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.

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.

Внимание! На компьютер предварительно должно быть установлено программное обеспечение эмуляции терминала.

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:

- скорость: 115200 бит/с;
- биты данных: 8 бит;
- четность: нет;
- стоповые биты: 1;
- 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 ttyS0
Sr-be login:
Password:
```

Шаг 6. Введите имя пользователя и пароль.

По умолчанию для входа в систему с правами администратора используйте:

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

Устройство готово к настройке.

1.2 Настройки по умолчанию

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

1) все порты устройства разделены на две группы: WAN- и LAN-порты. Их подробное описание представлено в подразд. 5.1 «Описание WAN-портов» и 6.1 «Описание LAN-портов» настоящей Инструкции;

2) все интерфейсы устройства открыты для удаленного доступа с помощью протоколов Telnet, SSH;

3) все LAN-порты устройства по умолчанию относятся к VLAN 1 с именем «Default».

VLAN id	Name	Member ports (t-tagged, u-untagged)
1	default	swp1 (u) , swp2 (u) , swp3 (u) , swp4 (u) , swp5 (u) , swp6 (u) , swp7 (u) , swp8 (u)

4) на устройстве заданы имена пользователей и пароли для разных уровней привилегий: режим администрирования, пользовательский, безопасный режим.

Имя пользователя – Пароль:

admin – admin;

serviceuser – serviceuser;

master – предоставляется по требованию.

Примечание. Имена пользователей и паролей вводятся с учетом регистра.

5) 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 4 «Настройка имени устройства».

Для настройки устройства при первом включении в конфигурации устройства используется учетная запись администратора **admin**;

б) функция SSH для удаленного управления устройством по умолчанию включена.

```
SSH configuration
Root login: permitted
```

```
SSH server enabled
```

```
Version: 2
Port: 22
Listen addresses:
  all
Whitelist:
  all
```

Для просмотра начальной конфигурации введите команду:

```
admin@sr-be# show running-config
```

```
interface eth1
  exit
interface eth2
  exit

system console authentication-list default
system ssh authentication-list default

ipv6 dhcp relay dhcp6-relay
  vrf default

ip dhcp relay dhcp-relay
  vrf default

interface switchport1
  shutdown
  exit
interface switchport2
  shutdown
  exit
interface switchport3
  shutdown
  exit
interface switchport4
  shutdown
  exit
interface switchport5
  shutdown
  exit
interface switchport6
  shutdown
  exit
interface switchport7
  shutdown
  exit
interface switchport8
  shutdown
  exit

ntp restrict 127.0.0.1/32
ntp restrict default ignore
ntp restrict ::1/128
ntp restrict default-ipv6 ignore

radius accounting off

logging monitor 7

router ldp
  exit

router rsvp
  exit

end
```

Для просмотра более подробных настроек по умолчанию введите команду:

```
admin@sr-be# save startup  
admin@sr-be# show profile startup detail
```

***Примечание.** Настройки по умолчанию возможно посмотреть только при первой загрузке изделия. Далее, чтобы посмотреть все произведенные настройки на изделии необходимо воспользоваться командой **show profile name profile name**.*

2 ИЗМЕНЕНИЕ ПАРОЛЕЙ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

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

Для защищенного входа в систему необходимо сменить пароли пользователей «admin», «serviceuser».

2.1 Пользователь «admin»

Для изменения пароля пользователя «admin» введите 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
```

2.2 Пользователь «serviceuser»

Пользователь «serviceuser» предназначен для сбора диагностических данных в случаях, когда требуется техническая поддержка.

Для изменения пароля пользователя «serviceuser» введите следующие команды:

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

2.3 Создание групп

Создайте новую группу с указанием уровня привилегий от 1 до 14 с помощью следующих команд:

```
admin@sr-be# configure terminal
admin@sr-be(config)#group <group_name> privilege <privilege_level>
```

Пример создания группы «operators» с уровнем привилегий 1:

```
admin@sr-be#configure terminal
admin@sr-be(config)#group operators privilege 1
```

Для проверки результата введите команду:

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

Group		Privilege
admin		15
service		1
operators		1

Для удаления группы пользователей введите команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#no group operators
```

2.4 Создание новых пользователей

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

Пример создания пользователя «boris» с паролем «12345678» группы «operators»:

```
admin@sr-be#configure terminal
admin@sr-be(config)#username add boris group operators
Enter password: 12345678
Repeat password: 12345678
```

Для проверки результата введите команду:

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

User	Type	Type
admin	admin	local
serviceuser	service	local
boris	operators	local

Для удаления пользователя введите команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#no username boris
```

3 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 представлен на рисунке 1.

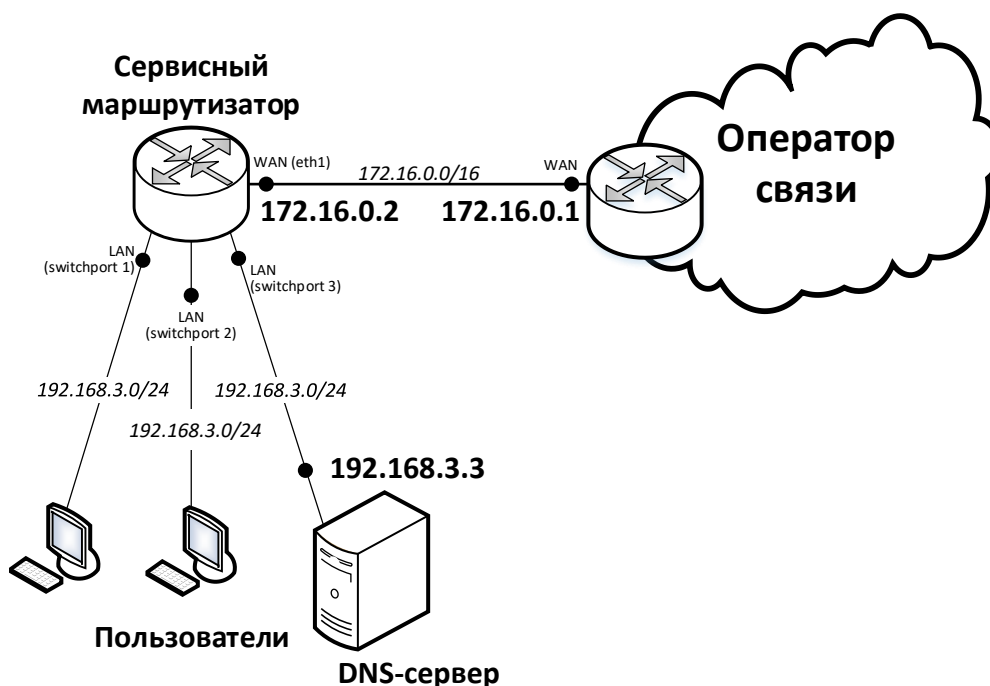


Рисунок 1 – Настройка сервера доменного имени в локальной сети

Шаг 1. Добавьте адрес сервера разрешения доменных имен с помощью команд:

```
admin@sr-be#configure terminal
admin@sr-be(config)#name-server 192.168.3.3
```

Шаг 2. Для вывода на экран адреса DNS-сервера введите команду:

```
admin@sr-be(config)#show name-servers
```

Результат выполнения команды:

```
nameserver 192.168.3.3
```

Для удаления адреса DNS-сервера введите команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#no name-server 192.168.3.3
```


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 команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#system host-name <hostname> domain-name <domain_name>
```

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

Например, для смены имени устройства «service-router» и доменного имени «istok.ab» введите команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#system host-name service-router domain-name istok.ab
```

Для проверки настроек имени устройства введите команду:

```
admin@service-router(config)#show host-name
```

Результат выполнения команды:

service-router

Для проверки настроек доменного имени введите команду:

```
admin@service-router(config)#show domain-name
```

Результат выполнения команды:

service-router.istok.ab

5 НАСТРОЙКА WAN-ПОРТОВ

5.1 Описание WAN-портов

Порты WAN используются для подключения устройства ко внешней сети, в частности для подключения к сети провайдера с целью получения доступа в интернет. Устройство имеет два WAN-порта RJ-45 (10/100/1000BASE-T) (для устройств ISN41508T4 – два порта SFP (1000BASE-X) (см. рис. 2 – 15), что позволяет использовать подключение сразу к нескольким операторам связи.

В устройствах ISN41508T3-M/ISES1004, ISN41508T3-M/ISES0108, ISN41508T3-M/ISES0114, ISN41508T3-M/ISES0116, ISN41508T3-M/ISES1009, ISN41508T3-M-AC/ISES1004, ISN41508T3-M-AC/ISES0108, ISN41508T3-M-AC/ISES0114, ISN41508T3-M-AC/ISES0116, ISN41508T3-M-AC/ISES1009 установлен один модуль расширения с WAN-портами.

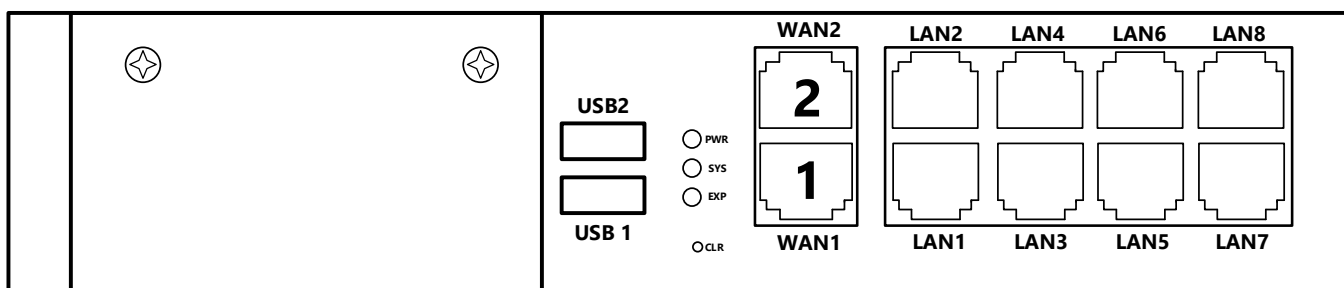


Рисунок 2 – WAN-порты. Передняя панель ISN41508T3

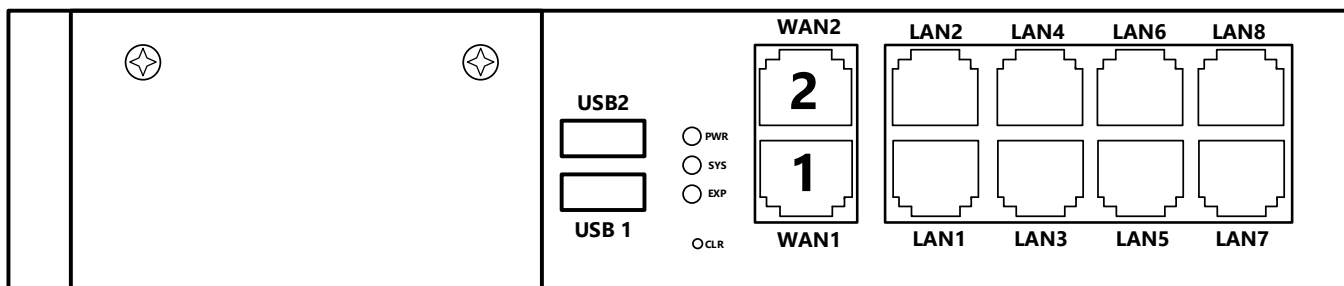


Рисунок 3 – WAN-порты. Передняя панель ISN41508T3-M

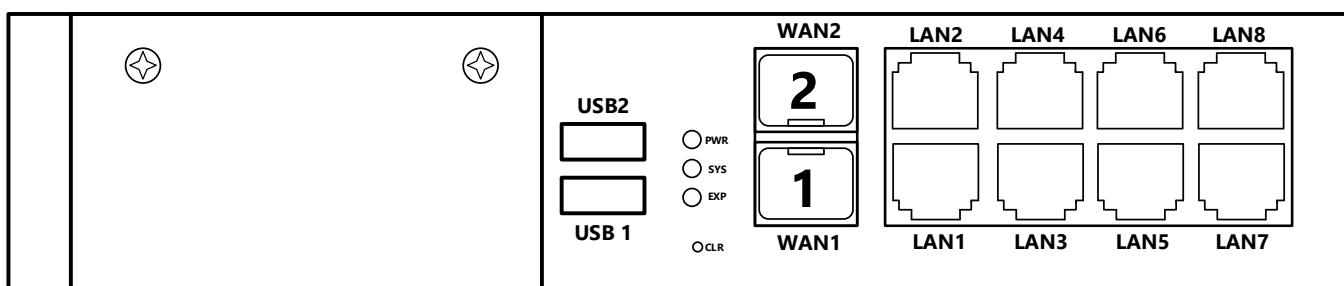


Рисунок 4 – WAN-порты. Передняя панель ISN41508T4

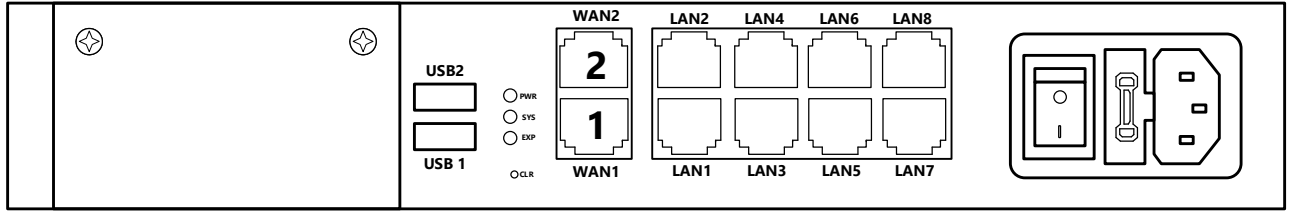


Рисунок 5 – WAN-порты. Передняя панель ISN41508T3-M-AC

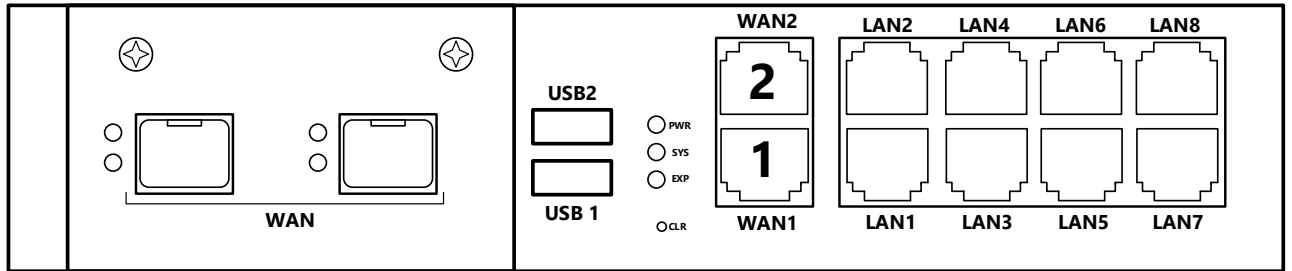


Рисунок 6 – WAN-порты. Передняя панель ISN41508T3-M/ISES1004

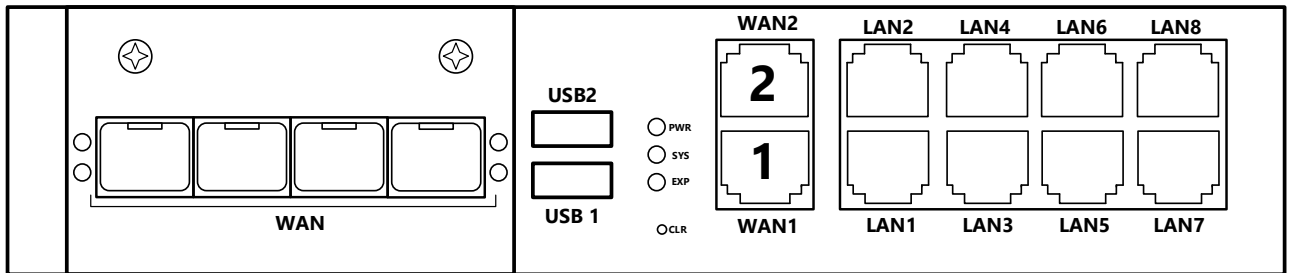


Рисунок 7 – WAN-порты. Передняя панель ISN41508T3-M/ISES0108

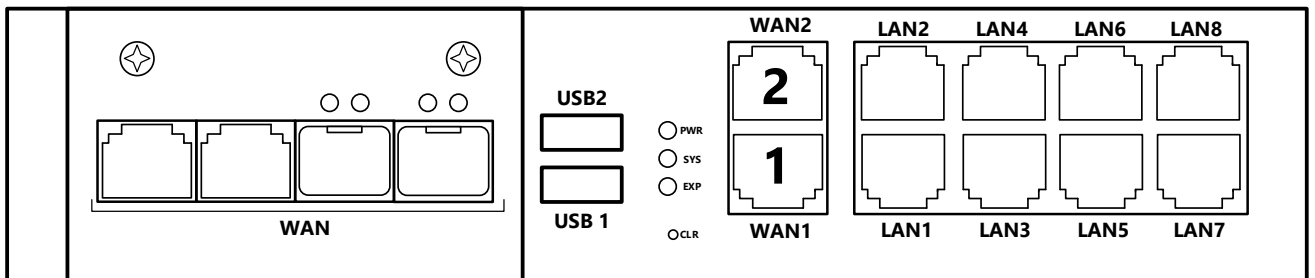


Рисунок 8 – WAN-порты. Передняя панель ISN41508T3-M/ISES0114

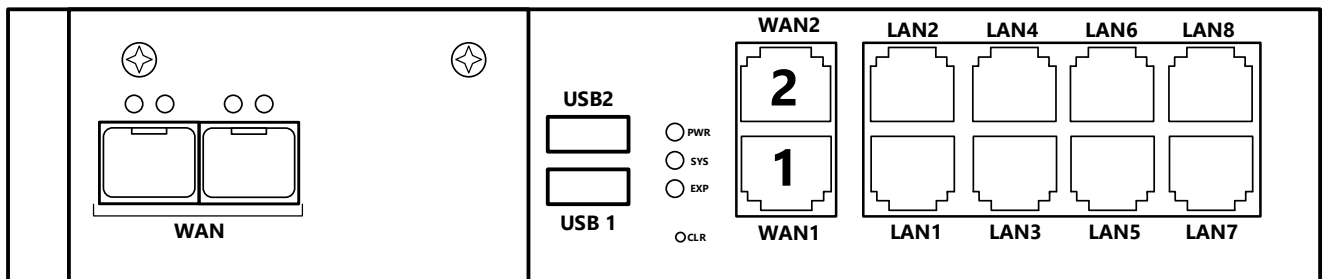


Рисунок 9 – WAN-порты. Передняя панель ISN41508T3-M/ISES0116. WAN-порты

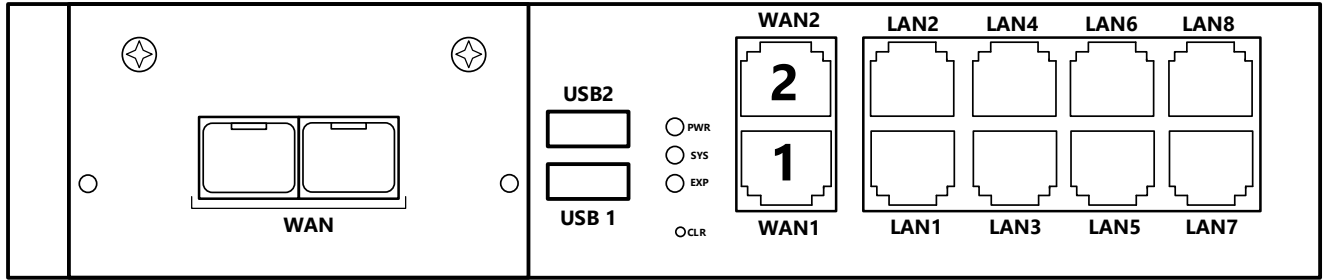


Рисунок 10 – WAN-порты. Передняя панель ISN41508T3-M/ISES1009

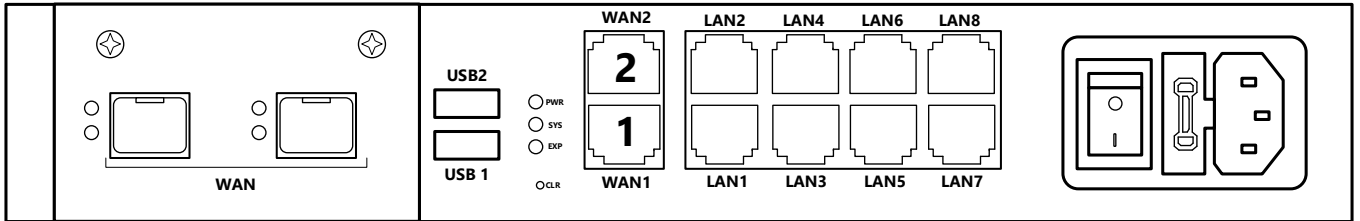


Рисунок 11 – WAN-порты. Передняя панель ISN41508T3-M-AC/ISES1004

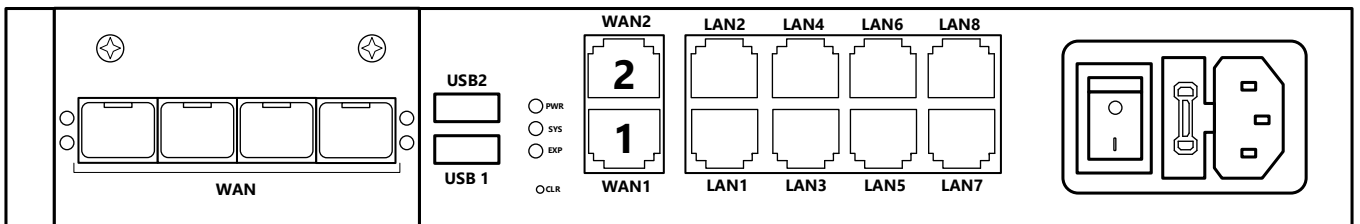


Рисунок 12 – WAN-порты. Передняя панель ISN41508T3-M-AC/ISES0108

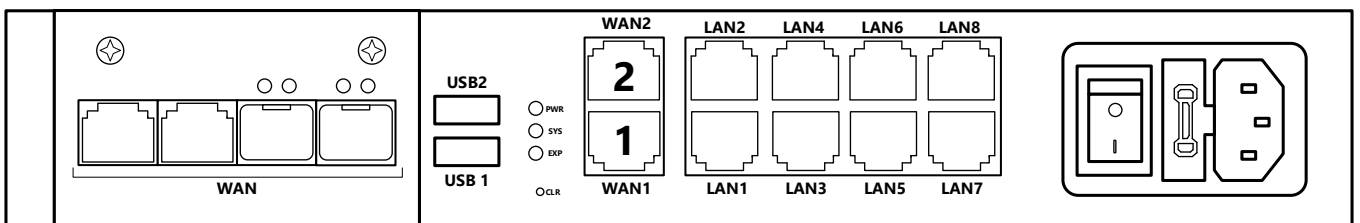


Рисунок 13 – WAN-порты. Передняя панель ISN41508T3-M-AC/ISES0114

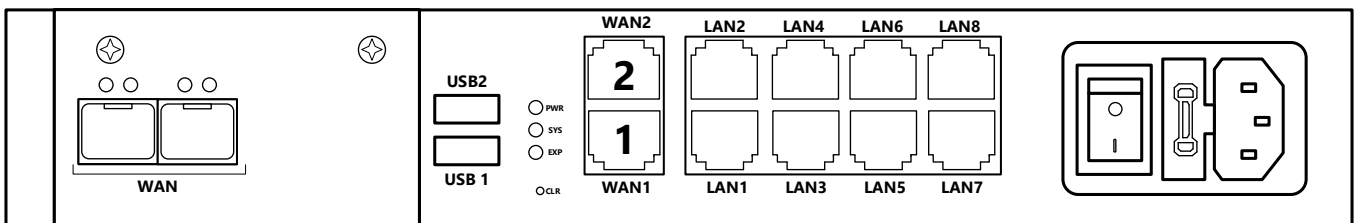


Рисунок 14 – WAN-порты. Передняя панель ISN41508T3-M-AC/ISES0116

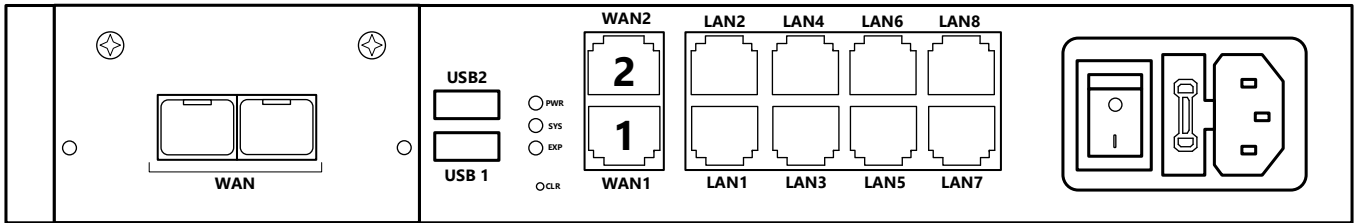


Рисунок 15 – WAN-порты. Передняя панель ISN41508T3-M-AC/ISES1009

Имена интерфейсов начинается с префикса **eth** (Ethernet), далее указывается порядковый номер порта: **eth1** и **eth2**. Нумерация портов соответствует маркировке на передней панели устройства (WAN1, WAN2). Названия портов чувствительны к регистру и указываются только с маленькой буквы.

Примечание. В модулях расширения нумерация WAN-портов может меняться, начиная с 3 порядкового номера, например, в модуле ISES0108 нумерация портов: **eth3 – eth6**, в ISES1009: **eth3 – eth4**.

5.2 Назначение IP-адреса

5.2.1 Назначение статического IP-адреса

Для настройки статического IP-адреса введите следующие команды:

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

Пример настройки статического IP-адреса 172.16.0.2 с маской подсети 255.255.0.0 для WAN-интерфейса **eth1**:

```
admin@sr-be#configure terminal
admin@sr-be(config)#interface eth1
admin@sr-be(config-if-[eth1])#ip address 172.16.0.2 255.255.0.0
admin@sr-be(config-if-[eth1])#no shutdown
admin@sr-be(config-if-[eth1])#exit
```

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. Введите следующую команду:

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

```
eth1:
  Link: UP
  IPv4 Address: 172.16.0.2/16
  RX: 0 bytes / 0 packets
  TX: 968 bytes / 8 packets
  MTU: 1500
  HW Address: 94:3f:bb:ff:ff:03
```

```
IPv6 Address: fe80::963f:bbff:feff:ff03/64
Autonegotiation: on
Duplex: Full
Speed: 1000
Supported speeds (Mb/s): 10, 100, 1000
```

Также проверить IP-адрес интерфейса можно с помощью команды:

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

Interface	HW Address	IPv4 Address	Admin/Link	DHCPv4	Description
eth1	7a:72:6c:4b:7a:36	172.16.0.2/16	UP/UP	OFF	
eth2	7a:72:6c:4b:7b:b8	unassigned	DOWN/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	

Для отмены статического IP-адреса введите 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
```

5.2.2 Получение динамического IP-адреса

Пример схемы подключения представлен на рисунке 16.

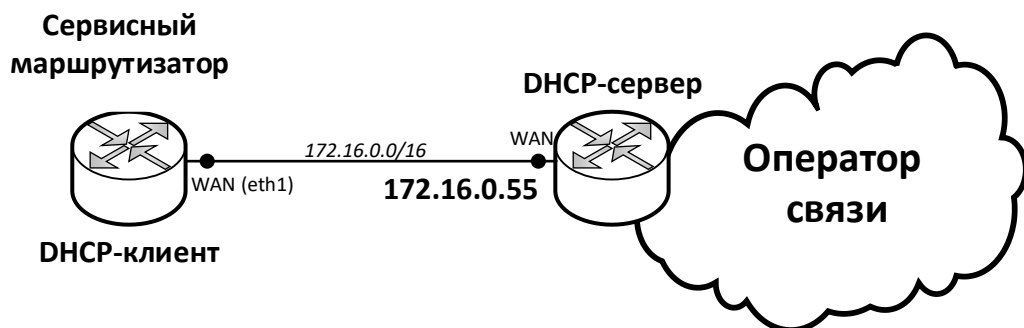


Рисунок 16 – Получение динамического IP-адреса

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 введите следующую команду:

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

```
eth1:
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:feff:ff03/64
Autonegotiation: on
Duplex: Full
Speed: 1000
Supported speeds (Mb/s): 10, 100, 1000
```

Также проверить IP-адрес интерфейса можно с помощью команды:

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

Interface	HW Address	IPv4 Address	Admin/Link	DHCPv4	Description
eth1	94:3f:bb:ff:ff:03	172.16.0.2/16	UP/UP	ON	
eth2	94:3f:bb:ff:ff:01	unassigned	DOWN/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	

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

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

```
admin@sr-be#configure terminal
admin@sr-be(config)#no ip address dhcp
```

5.3 Настройка 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 представлен на рисунке 17.

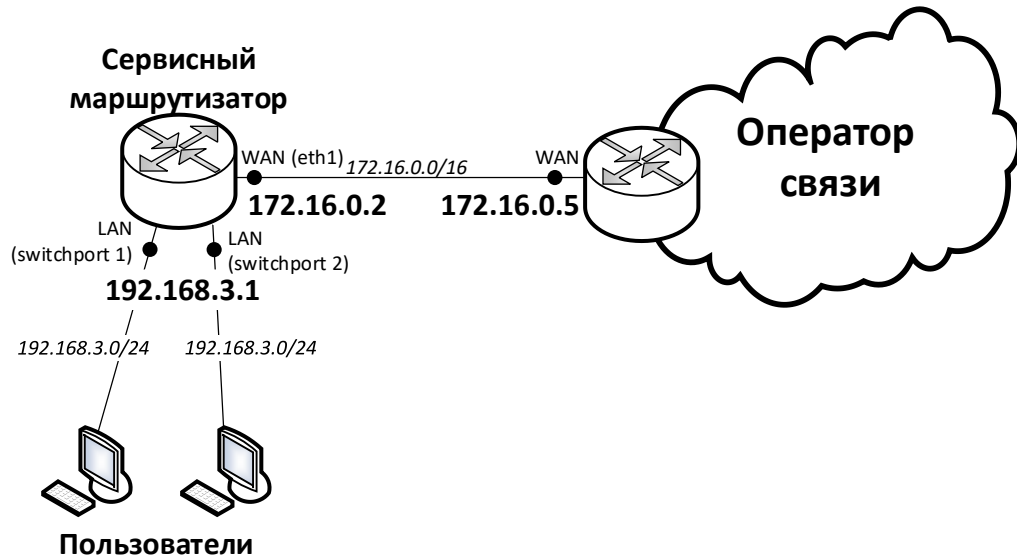


Рисунок 17 – Настройка DHCP-сервера на устройстве

Для настройки DHCP-сервера на устройстве введите 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
```

Примечания:

- 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) Выполнение команды **range** возможно только, если ранее была введена команда **network**.

Проверьте настройки DHCP-сервера с помощью команды:

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

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 – 192.168.3.35 введите команду:

```
admin@sr-be#configure terminal
admin@sr-be(config)#ip dhcp pool 10
admin@sr-be(config-dhcp)#no range 192.168.3.3 192.168.3.35
admin@sr-be(config-dhcp)#exit
```


Для удаления всего набора локальных адресов введите команды:

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

Для отключения службы DHCP-сервера введите команды:

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

5.4 Настройка маршрута по умолчанию

5.4.1 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 представлен на рисунке 18.



Рисунок 18 – Настройка маршрута по умолчанию

Для настройки на сервисном маршрутизаторе маршрута по умолчанию введите 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, введите команду **show ip route** и найдите статические маршруты, обозначенные буквой «S»:

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

```
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    172.16.0.0/16 is directly connected, eth1
```

5.4.2 Изменение маршрута по умолчанию

Шаг 1. 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
```

или команд:

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

Шаг 2. Введите новый маршрут по умолчанию, например:

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

5.5 Настройка удаленного доступа

5.5.1 Настройка удаленного доступа по протоколу SSH

5.5.1.1 Настройка удаленного доступа по протоколу SSH через WAN-порт

Пример схемы сети представлен на рисунке 19.

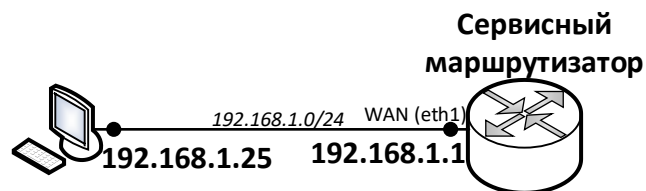


Рисунок 19 – Настройка удаленного доступа по протоколу SSH

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

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

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

Для вывода на экран настроек SSH-сервера введите команду:

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

```
SSH configuration
Root login: permitted
SSH server enabled
Version: 2
Port: 22
Listen addresses:
 192.168.1.1
Whitelist:
All
```

Для удаления настроенных параметров SSH введите команды:

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

5.5.1.2 Настройка удаленного доступа по протоколу SSH через LAN-порт

Пример схемы сети представлен на рисунке 20.

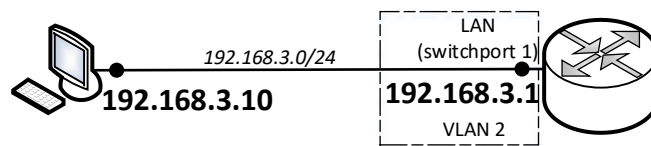


Рисунок 20 – Настройка удаленного доступа по протоколу SSH

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

Шаг 1. Создайте VLAN 2:

```
admin@sr-be#configure terminal
admin@sr-be(config)#vlan 2
```

Шаг 2. Назначьте VLAN 2 интерфейсу switchport 1:

```
admin@sr-be#configure terminal
admin@sr-be(config)#interface switchport 1
admin@sr-be(config-switchport1)#switchport mode access
admin@sr-be(config-switchport1)#switchport access vlan 2
admin@sr-be(config-switchport1)#no shutdown
admin@sr-be(config-switchport1)#exit
```

Шаг 3. Назначьте статический IP-адрес на VLAN 2:

```
admin@sr-be#configure terminal
admin@sr-be(config)#interface vlan 2
admin@sr-be(config-if-[vlan2])#vid 2
admin@sr-be(config-if-[vlan2])#ip address 192.168.3.1/24
admin@sr-be(config-if-[vlan2])#no shutdown
admin@sr-be(config-if-[vlan2])#exit
```

Шаг 4. Для настройки удаленного доступа укажите IP-адрес интерфейса, который будет принимать SSH-соединение:

```
admin@sr-be#configure terminal
admin@sr-be(config)#system ssh listen-address 192.168.3.1
```

Для вывода на экран настроек SSH-сервера введите команду:

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

SSH configuration

```
Root login: permitted
SSH server enabled
Version: 2
Port: 22
Listen addresses:
192.168.3.1
Whitelist:
All
```

Для удаления настроенных параметров SSH введите команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#no system ssh listen-address 192.168.3.1
```

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

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

5.5.2 Настройка удаленного доступа по протоколу TELNET

Для включения Telnet на устройстве введите команды:

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

Для вывода на экран статуса Telnet-сервера введите команду:

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

Telnet server enabled

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

Для отключения Telnet на устройстве введите команды:

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

Для вывода на экран статуса Telnet-сервера введите команду:

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

Telnet server disabled

5.6 Настройка журналирования событий на удаленный Syslog-сервер

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

Пример схемы сети представлен на рисунке 21.

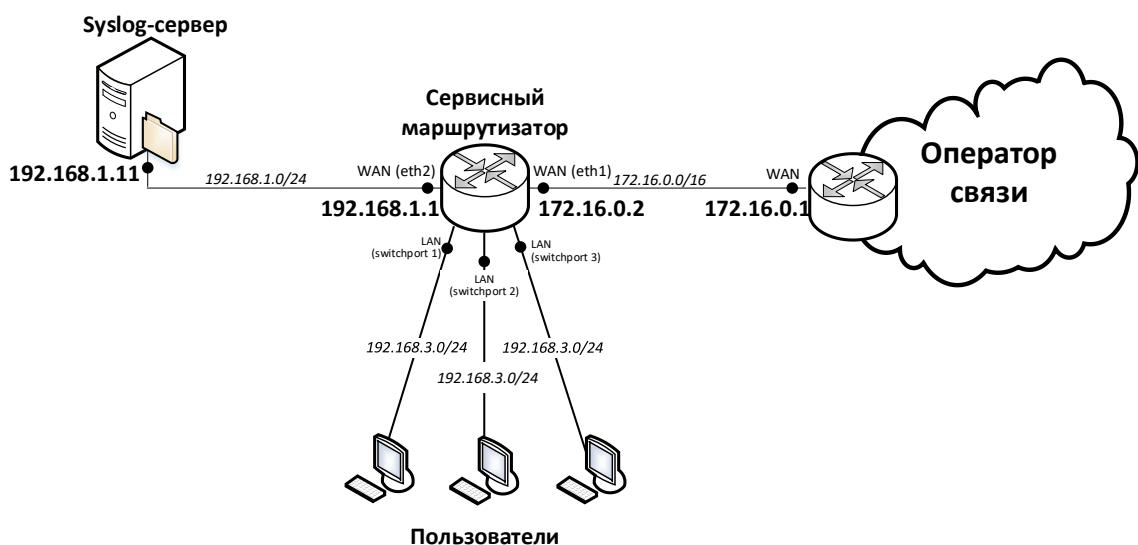


Рисунок 21 – Настройка журналирования событий на удаленный Syslog-сервер
Сервисные маршрутизаторы. Руководство по установке и быстрому запуску КРПГ.465614.001Д26

Введите команды для проверки статуса логгирования:

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

```
access_violation : on
access_list : off
pim ipv4 : off
pim ipv6 : off
syslog : on
kern : on
daemon : on
command-history : on
```

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

- **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);
- **command-history** – лог истории ввода команд.

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

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

Для проверки настроек введите команду:

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

Часть вывода пропущена для краткости

...

```
log syslog remote 192.168.1.11
```

```
system host-name sr-be domain-name sr-be
logging monitor 7
```

```
router ldp
exit
```

```
router rsvp
exit
end
```

Для отмены настроек введите команды:

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

5.7 Настройка централизованной аутентификации пользователей через RADIUS-сервер

Протокол удаленной аутентификации RADIUS служит для связи с сервером аутентификации.

В технологии RADIUS используется модель взаимодействия «клиент-сервер»: RADIUS-сервер получает запрос на подключение пользователя, осуществляет аутентификацию пользователя и возвращает клиенту всю конфигурационную информацию, необходимую для предоставления сервиса пользователю.

При аутентификации по методу RADIUS пароль зашифровывается перед отправкой по сети.

Пример схемы сети представлен на рисунке 22.

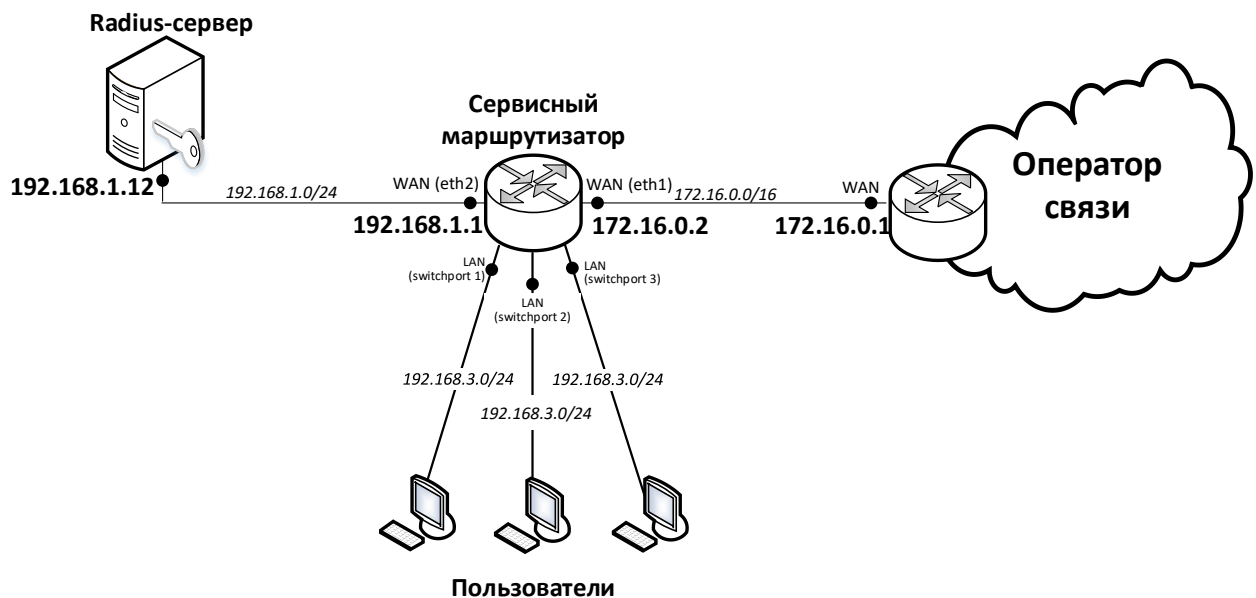


Рисунок 22 – Настройка централизованной аутентификации пользователей через RADIUS-сервер

Шаг 5. Настройте соединение с RADIUS-сервером. Для этого введите IP-адрес RADIUS-сервера и пароль для доступа с помощью команд:

```
admin@sr-be#configure terminal
admin@sr-be(config)#radius server 192.168.1.12 password 12345
```

Для проверки настройки RADIUS-сервера введите команду:

```
admin@sr-be(config)#show radius servers
```

```
192.168.1.12 passwd: qehRopxWSvWL10AxpBU00wA= auth-port: 1812 acct-port: 1813
timeout: 3
```

Шаг 6. Настройте список последовательностей аутентификации с именем RADIUS. Для этого введите команду:

```
admin@sr-be(config)#aaa authentication list RADIUS methods radius local
```

```
admin@sr-be(config)#radius accounting on
```

Для проверки настроек AAA введите команду:

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

Methods lists:

```
list name | auth methods
-----
RADIUS    | radius, local
default   | local
```

Service list:

```
console: default
ssh: default
```

Шаг 7. Настройте метод авторизации для SSH. Для этого введите команду:

```
admin@sr-be(config)#system ssh authentication-list RADIUS
```

Для проверки настроек введите команду:

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

Methods lists:

```
list name | auth methods
-----
RADIUS    | radius, local
default   | local
```

Service list:

```
console: default
ssh: RADIUS
```

Шаг 8. Для смены порта аутентификации необходимо ввести новый порт для аутентификации <1-65535>:

```
admin@sr-be(config)#radius server 192.168.1.12 password 12345 authentication-
port 1920
```

Для проверки смены порта для аутентификации введите команду:

```
admin@sr-be(config)#show radius servers
```

```
192.168.1.12 passwd: qehRopxWSvWLl0AxpB00wA= auth-port: 1920 acct-port: 1813
timeout: 3
```

Для удаления настроек соединения с Radius-сервером введите команду:

```
admin@sr-be(config)#no radius server 192.168.1.12
```

5.8 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 представлен на рисунке 23.

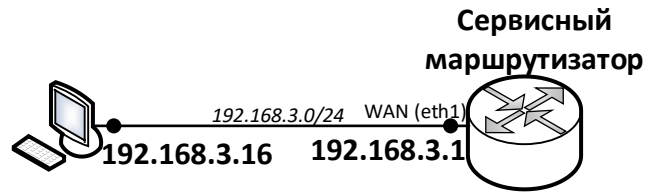


Рисунок 23 – Настройка правил фильтрации

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

```
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:

```
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) введите 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:

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

Команда разрешает входящий TCP-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 TCP-трафик от других хостов, порт назначения 22.

Шаг 5. Проверьте настройки:

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

```
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 введите 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-ов введите команды в режиме конфигурации:

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


6 НАСТРОЙКА VLAN

6.1 Описание LAN-портов

LAN-порты (см. рис. 24 – 37) используются для организации локальной сети. Через них с помощью сетевых кабелей к устройству можно подключить несколько периферийных устройств (компьютеры, принтеры, ксероксы и т.д.) и создать единое сетевое окружение. Устройство имеет восемь LAN-портов RJ-45 (10/100/1000BASE-T).

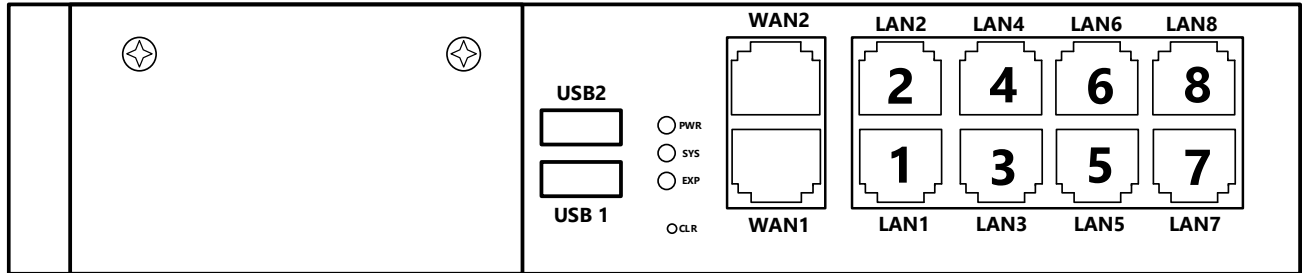


Рисунок 24 – LAN-порты. Передняя панель ISN41508T3

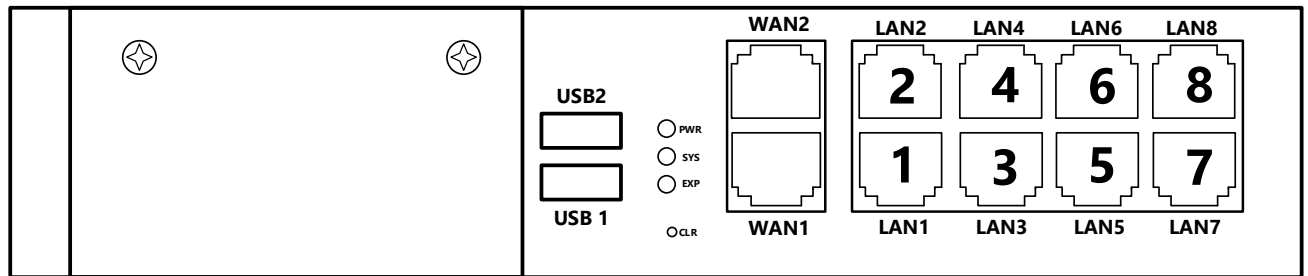


Рисунок 25 – LAN-порты. Передняя панель ISN41508T3-M

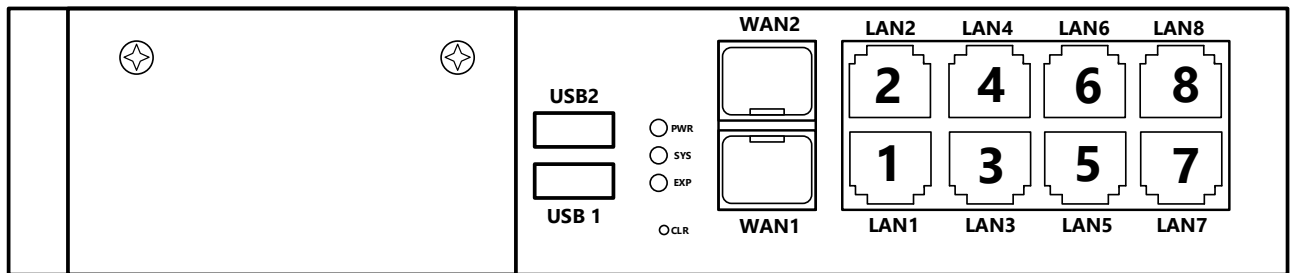


Рисунок 26 – LAN-порты. Передняя панель ISN41508T4

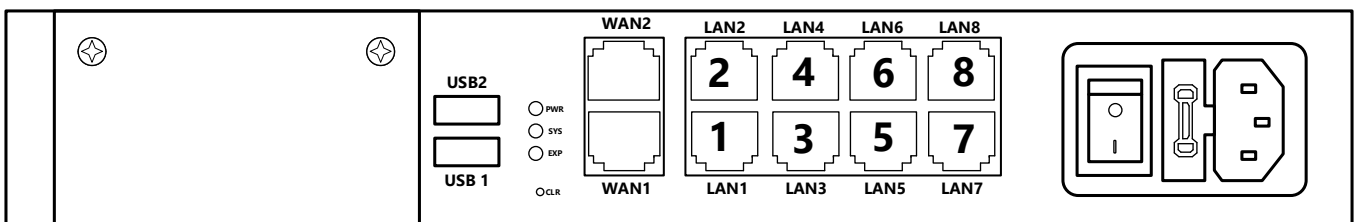


Рисунок 27 – LAN-порты. Передняя панель ISN41508T3-M-AC

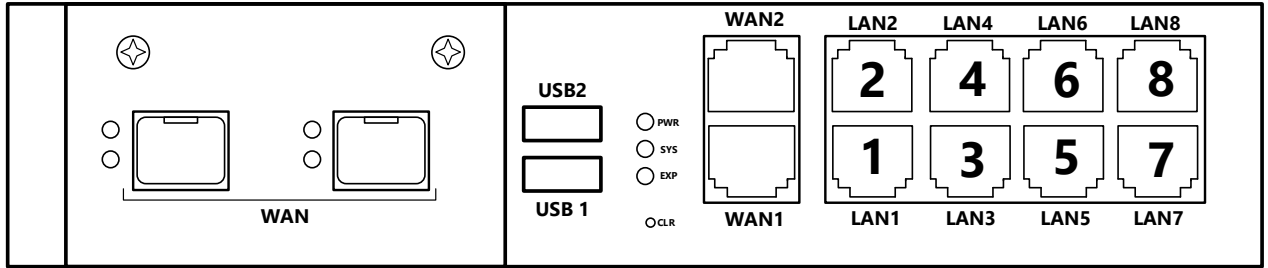


Рисунок 28 – LAN-порты. Передняя панель ISN41508T3-M/ISES1004

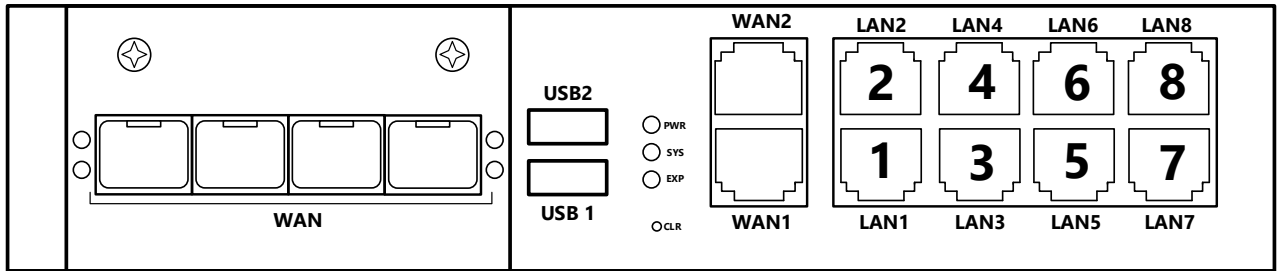


Рисунок 29 – LAN-порты. Передняя панель ISN41508T3-M/ISES0108

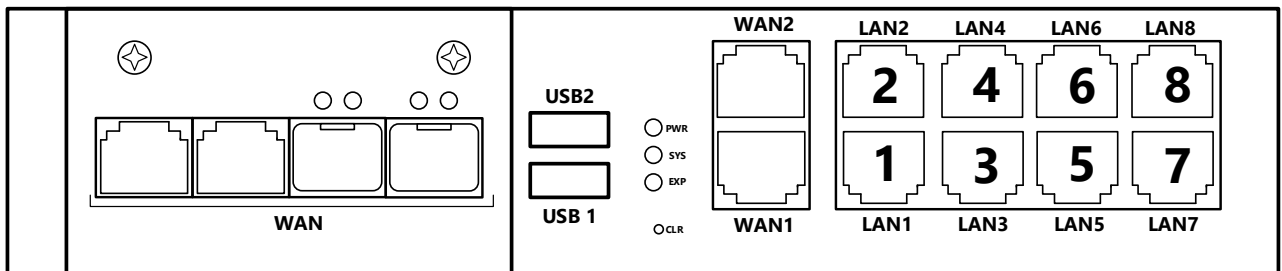


Рисунок 30 – LAN-порты. Передняя панель ISN41508T3-M/ISES0114

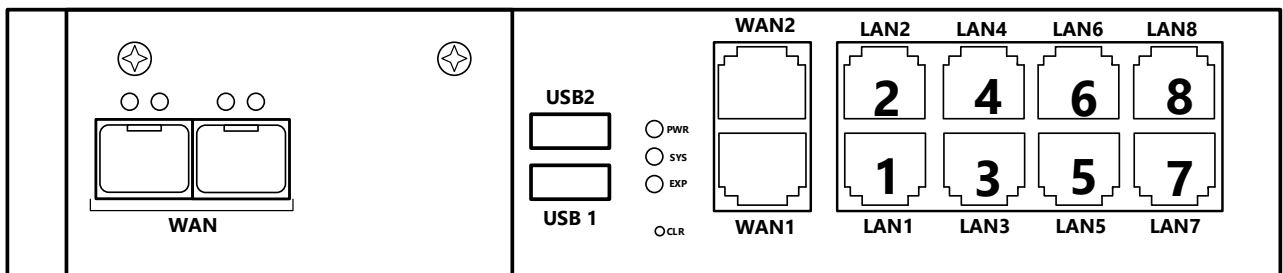


Рисунок 31 – LAN-порты. Передняя панель ISN41508T3-M/ISES0116

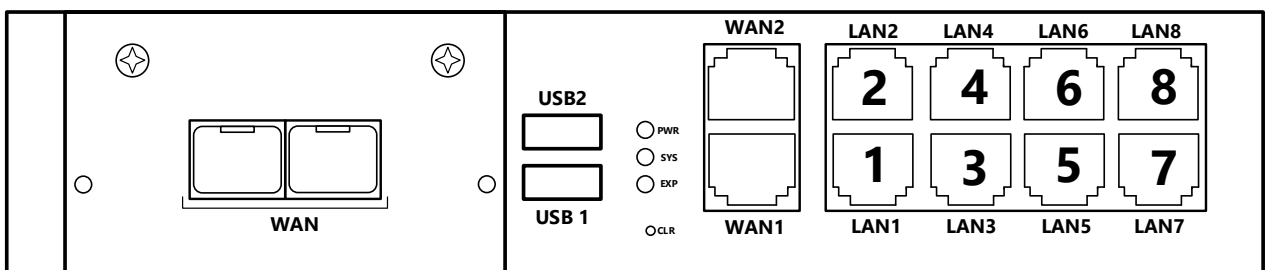


Рисунок 32 – LAN-порты. Передняя панель ISN41508T3-M/ISES1009

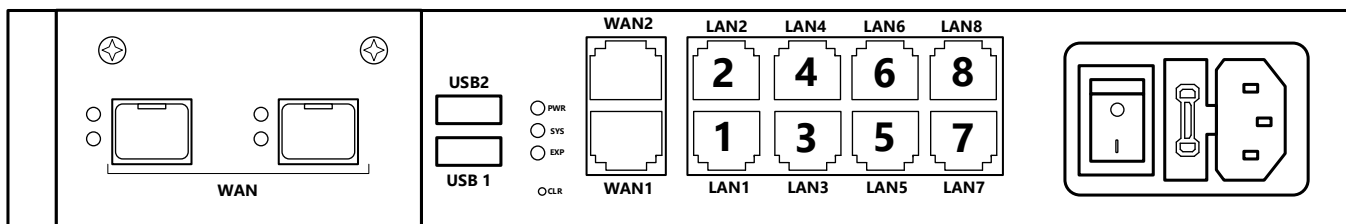


Рисунок 33 – LAN-порты. Передняя панель ISN41508T3-M-AC/ISES1004

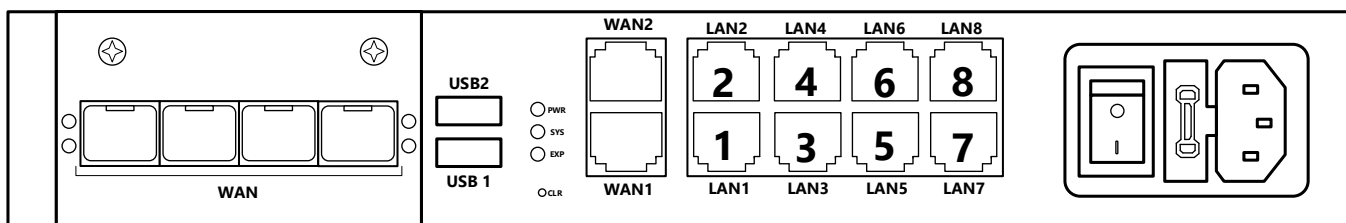


Рисунок 34 – LAN-порты. Передняя панель ISN41508T3-M-AC/ISES0108

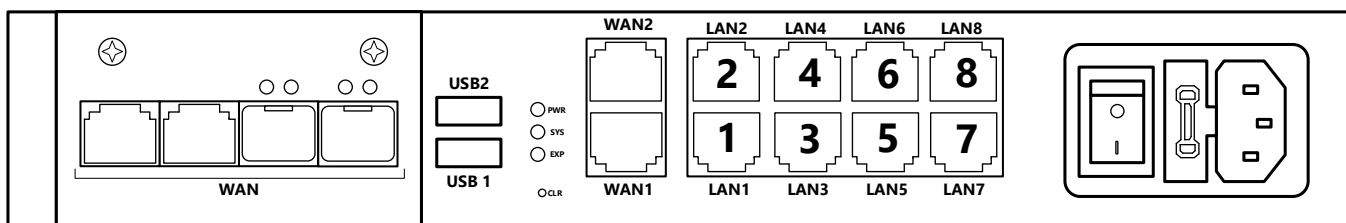


Рисунок 35 – LAN-порты. Передняя панель ISN41508T3-M-AC/ISES0114

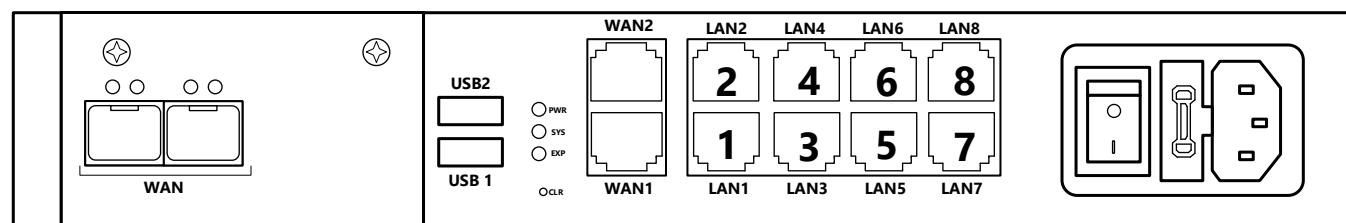


Рисунок 36 – LAN-порты. Передняя панель ISN41508T3-M-AC/ISES0116

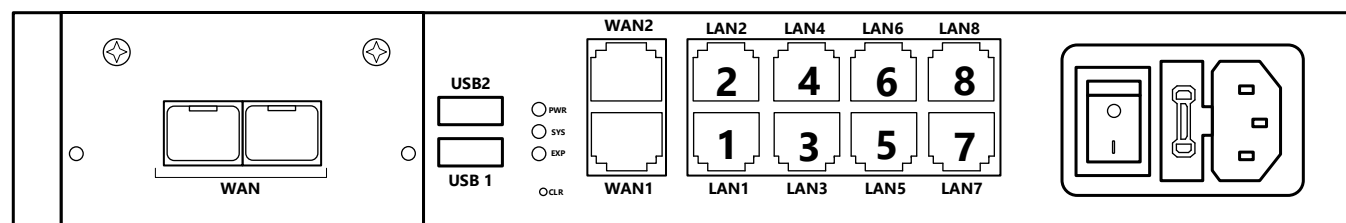


Рисунок 37 – LAN-порты. Передняя панель ISN41508T3-M-AC/ISES1009

Имена интерфейсов начинаются с префикса **switchport**, далее указывается порядковый номер порта: **switchport 1 – switchport 8**. Нумерация портов соответствует маркировке на передней панели устройства (LAN1 – LAN8). Названия портов чувствительны к регистру и указываются только с маленькой буквы.

6.2 Создание 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 представлен на рисунке 38.

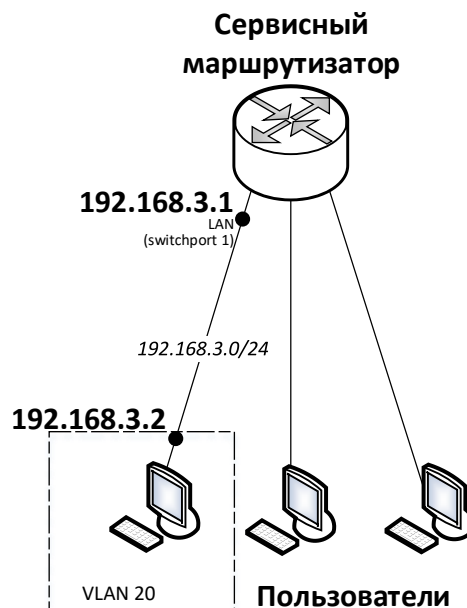


Рисунок 38 – Создание VLAN

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

```
admin@sr-be#configure terminal
admin@sr-be(config)#vlan 20
```

Примечания:

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:

```
admin@sr-be#configure terminal
admin@sr-be(config)#vlan 2,3,5-8
```

Команда **show vlan all** в режиме глобальной конфигурации отображает параметры для всех VLAN, настроенных на устройстве:

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

```
VLAN id  Name      Member ports (t-tagged, u-untagged)
  1      default    swp1 (u) , swp2 (u) , swp3 (u) , swp4 (u) , swp5 (u) , swp6 (u) ,
          swp7 (u) , swp8 (u)
  20     Vlan0020  --
```

Для определенной VLAN используйте ID:

```
admin@sr-be#configure terminal
admin@sr-be(config)# show vlan 20
```

```
VLAN id  Name      Member ports (t-tagged, u-untagged)
  20     Vlan0020  --
```

Для удаления VLAN используйте команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#no vlan 20
```

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

6.3 Назначение Access-порта в VLAN

Назначить в VLAN можно LAN-порты устройства switchport 1 – switchort 8.

Пример назначения VLAN 20 интерфейсу switchport 1:

```
admin@sr-be#configure terminal
admin@sr-be(config)#interface switchport 1
admin@sr-be(config-switchport1)#switchport mode access
admin@sr-be(config-switchport1)#switchport access vlan 20
admin@sr-be(config-switchport1)#no shutdown
admin@sr-be(config-switchport1)#exit
```

Для проверки результата настроек введите команду:

```
admin@sr-be(config)#show interfaces switchport1
```

```
switchport1:
Link: DOWN
MTU: 10240
Duplex: full
Autonegotiation: on
Speed: 1000
Supported speeds (Mb/s): 10, 100, 1000
Switchport mode access
Switchport access vlan: 20

Mode: Access
VLAN: 20
```

Для проверки результата настроек введите команду:

```
admin@sr-be(config)#show vlan all
```

```
VLAN id  Name      Member ports (t-tagged, u-untagged)
  1      default    swp2 (u) , swp3 (u) , swp4 (u) , swp5 (u) , swp6 (u) , swp7 (u) ,
          swp8 (u)
  20     Vlan0020  swp1 (u)
```

6.4 Назначение IP-адреса на VLAN-интерфейс

Для настройки внутреннего интерфейса локальной сети следует зайти в режим конфигурирования виртуального интерфейса (например, Vlan 20), задать идентификатор и IP-адрес интерфейса (например, switchport 1).

Для назначения статического IP-адреса введите команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#interface vlan 20
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
```

Для назначения динамического IP-адреса введите команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#interface vlan 20
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 проверки настроек vlan 20 введите команду:

```
admin@sr-be(config)#show interfaces vlan20
```

```
vlan20 vid 20:
Link: UP
IPv4 Address: 192.168.3.1/24
  RX: 13908 bytes / 88 packets
  TX: 1764 bytes / 10 packets
MTU: 1500
HW Address: b4:81:bf:00:00:85
IPv6 Address: fe80::b681:bfff:fe00:85/64
EtherType: 0x8100
  Encapsulation: dot1q
```

6.5 Настройка интерфейса в режиме Trunk

Чтобы настроить порт switchport 5 устройства в качестве магистрального порта, используйте следующие команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#interface switchport 5
admin@sr-be(config-switchport1)#switchport mode trunk
admin@sr-be(config-switchport1)#exit
```

```
switchport5:
Link: DOWN
MTU: 10240
Duplex: full
Autonegotiation: on
Speed: 1000
Supported speeds (Mb/s): 10, 100, 1000
Switchport mode trunk
Switchport trunk allowed vlans: 1-4094
Switchport trunk native vlan: 1
```

Внимание! Для порта устройства будут разрешены все VLAN.

6.6 Назначение trunk-порту списка разрешенных VLAN

Чтобы указать перечень разрешенных VLAN (например, VLAN 20, 30) для trunk-порта switchport 5 введите команды:

```
admin@sr-be(config)#configure terminal
admin@sr-be(config)#interface switchport 5
admin@sr-be(config-switchport1)#switchport trunk allowed vlan none
admin@sr-be(config-switchport1)#switchport trunk allowed vlan add 20,30
admin@sr-be(config-switchport1)#no shutdown
admin@sr-be(config-switchport1)#exit
```

Для проверки результата настроек введите команду:

```
admin@sr-be(config)#show interfaces switchport5
```

```
switchport5:
Link: DOWN
MTU: 10240
Duplex: full
Autonegotiation: on
Speed: 1000
Supported speeds (Mb/s): 10, 100, 1000
Switchport mode trunk
Switchport trunk allowed vlans: 20,30
```

7 РАБОТА С КОНФИГУРАЦИЕЙ

7.1 Сохранение настроек

7.1.1 Сохранение профилей локально

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

```
admin@sr-be#save TEST
```

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

```
admin@sr-be#save TEST comment keep
```

Для вывода на экран сохраненного профиля конфигурации введите команду:

```
admin@sr-be#show profile name TEST
```

```
| Profile Name | Loaded by | Created by | Loaded at |
-----|-----|-----|-----|
| TEST        |           | admin      |           |
```

Для вывода на экран содержимого профиля конфигурации TEST введите команду:

```
admin@sr-be#show profile name TEST detail
```

```
{
"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 введите команду:

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

Flags: b - boot profile, l - last loaded profile, m - profile was modified or corrupted

```
| Flags | Profile Name | Comment |
-----|-----|-----|
|       | TEST        | keep   |
| bl    | startup     |        |
```

Для удаления сконфигурированного профиля используйте команду:

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

Для проверки удаления профиля введите команду:

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

Flags: b - boot profile, l - last loaded profile, m - profile was modified or corrupted

```
| Flags | Profile Name | Comment |
-----|-----|-----|
| bl    | startup     |        |
```


7.1.2 Сохранение профилей удаленно по протоколу TFTP

Схема подключения сети представлена на рисунке 39 .

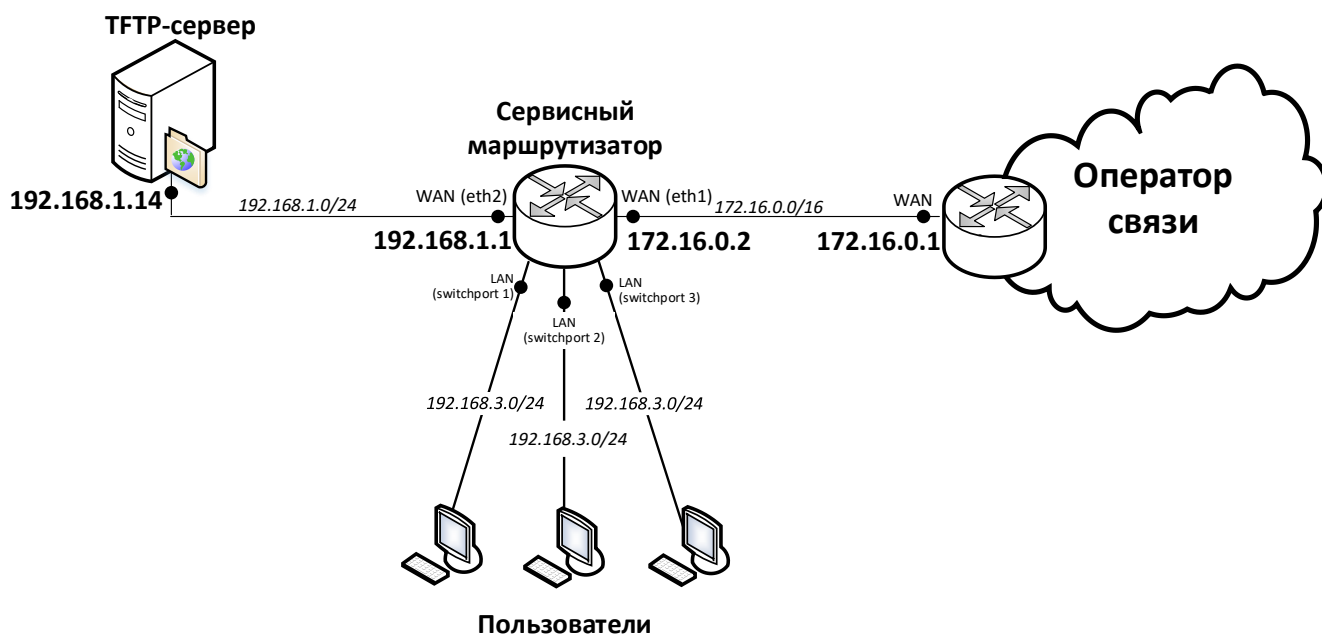


Рисунок 39 – Применение профилей, скаченных через TFTP-сервер

Шаг 1. Убедитесь в наличии сервера TFTP в сети.

Шаг 2. Для копирования файла текущей конфигурации на сервер TFTP в указанную директорию введите команду:

```
admin@sr-be#copy profile TEST tftp 192.168.1.14
```

7.2 Применение настроек

7.2.1 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
```

```
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 настройки текущего профиля.

7.2.2 Применение профилей, скаченных через TFTP

Шаг 1. Убедитесь в наличии сервера TFTP в сети.

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

```
admin@sr-be#copy url tftp://192.168.1.14/ profile TEST2
```

Шаг 3. Для проверки загрузки файла введите команду:

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

Шаг 4. Загрузите скаченный файл конфигурации:

```
admin@sr-be# load TEST2
```

```
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
...
```

7.3 Сброс настроек

7.3.1 Для выполнения загрузки файла начальной конфигурации введите команду:

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

```
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
...
```

7.3.2 Для удаления всех несохраненных настроек:

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

```
Do you really want to load null config? (yes/no)
```

```
admin@sr-be#yes
```

```
Clearing 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
...
```

8 УСТАНОВКА ДАТЫ, ВРЕМЕНИ И ЧАСОВОГО ПОЯСА

Для вывода на экран текущего времени и даты введите команду:

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

```
Чт янв 30 08:41:04 MSK 2021
```

8.1 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
```

```
Чт янв 30 18 12:30:22 MSK 2021
```

8.2 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
```

```
Ср авг 18 12:31:22 MSK 2021
```

8.3 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
```

8.4 Настройка синхронизации времени с NTP-сервера

Схема подключения сети представлена на рисунке 40.

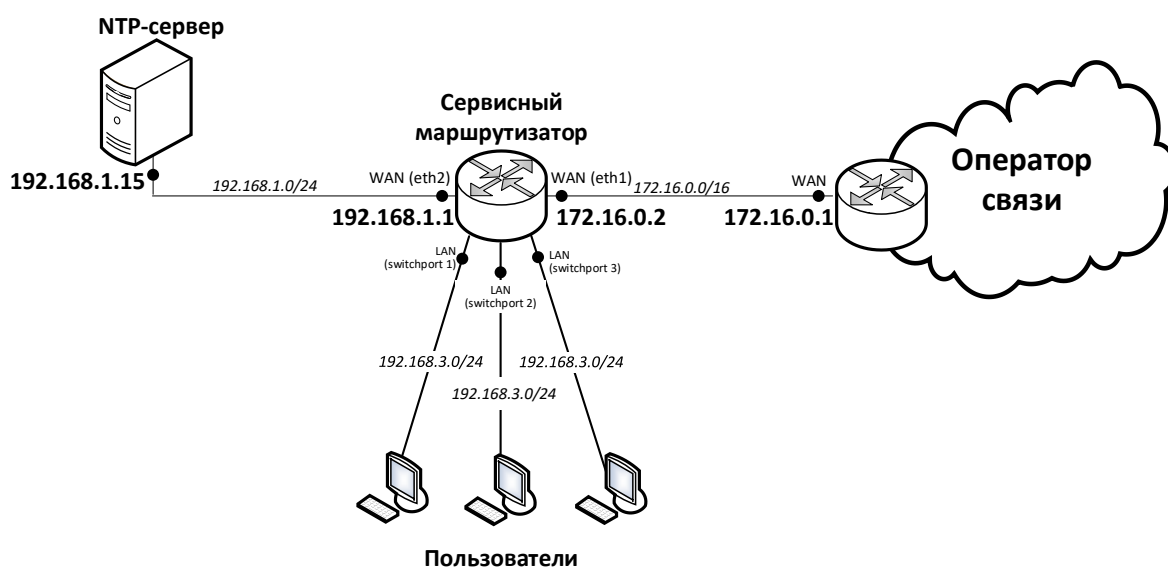


Рисунок 40 – Настройка синхронизации времени с NTP-сервера

Для настройки синхронизации с NTP-сервером введите команды:

```
admin@sr-be#configure terminal
admin@sr-be(config)#ntp server 192.168.1.15
admin@sr-be(config)#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. подразд. 7.1, 7.2, 7.3). При сильной разнице (более 1000 секунд) синхронизация осуществляться не будет.

9 КОМАНДЫ ДИАГНОСТИКИ

9.1 Ping

Схема проверки представлена на рисунке

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

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, 4 trace received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 1.164/1.266/1.362/0.078 ms
```

Можно воспользоваться командой проверки доступности хоста в сети следующего вида:

```
admin@sr-be#ping 192.168.3.2
```

В результате выполнения команды запустится бесконечный **ping**. Он будет продолжаться до тех пор, пока не будет остановлен администратором. Прервать выполнение команды можно сочетанием клавиш **[Ctrl+c]**.

9.2 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

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

10 ДОПОЛНИТЕЛЬНЫЕ РУКОВОДСТВА ПО РАБОТЕ С УСТРОЙСТВОМ

- 1) RU.07622667.00004-01 34 01-1 Руководство оператора.
- 2) RU.07622667.00004-01 34 01-2 Руководство оператора. Приложение 1. Справочник команд CLI.
- 3) RU.07622667.00004-01 32 01-2 Руководство системного программиста.

11 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

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

Официальный сайт компании: http://it.istokmw.ru/service_router/

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					