Консольный сервер SCS

SCS-32

Руководство по эксплуатации

Версия ПО 1.1.0

Содержание

1 Введение

1.1 Аннотация

Консольный сервер SCS-32 — это решение для централизованного управления сетевой инфраструктурой. Устройство позволяет администрировать коммутаторы, маршрутизаторы и другое оборудование через консольные порты, обеспечивает стабильный доступ даже при сбоях основной сети. Благодаря поддержке защищенных протоколов, встроенным механизмам аутентификации и журналирования, администраторы получают полный контроль над оборудованием и быстрый доступ к диагностике и восстановлению систем.

В данном руководстве по эксплуатации изложены назначение, технические характеристики, конструктивное исполнение, порядок установки, рекомендации по начальной настройке и обновлению программного обеспечения консольного сервера SCS-32 (далее консольный сервер или устройство).

1.2 Целевая аудитория

Данное руководство пользователя предназначено для технического персонала, выполняющего установку, настройку и мониторинг устройств посредством интерфейса командной строки (CLI), а также процедуры по обслуживанию системы и обновлению ПО. Квалификация технического персонала предполагает знание основ работы стеков протоколов TCP/IP, принципов построения Ethernet-сетей.

1.3 Условные обозначения

Обозначение	Описание
[ ]	В квадратных скобках в командной строке указываются необязательные параметры, но их ввод предоставляет определенные дополнительные опции.
{ }	В фигурных скобках в командной строке указываются возможные обязательные параметры. Необходимо выбрать один из параметров.
«,» **«-»**	Данные знаки в описании команды используются для указания диапазонов.
«|»	Данный знак в описании команды обозначает «или».
<Полужирный курсив>	Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре.
`Текст в рамке`	В рамках с текстом указаны примеры и результаты выполнения команд.

1.4 Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

Информация содержит справочные данные об использовании устройства.

2 Описание изделия

2.1 Назначение

Консольный сервер SCS-32 предназначен для администрирования коммутаторов, маршрутизаторов и другого оборудования через консольные порты, обеспечивая стабильный доступ даже при сбоях основной сети.

Устройства поддерживают защищенные протоколы и обладают встроенными механизмами аутентификации и журналирования, что позволяет получить полный контроль над оборудованием и быстрый доступ к диагностике и восстановлению систем.

2.2 Функции

2.2.1 Функции интерфейсов

В таблице 1 приведен список функций интерфейсов устройства.

Таблица 1 — Функции интерфейсов устройства

Определение полярности подключения кабеля (Auto MDI/MDIX)	Автоматическое определение типа кабеля — перекрестный кабель или кабель прямого подключения. • MDI (Medium Dependent Interface — прямой) — стандарт кабелей для подключения оконечных устройств; • MDIX (Medium Dependent Interface with Crossover — перекрестный) — стандарт кабелей для подключения концентраторов и коммутаторов.
Поддержка обратного давления (Back pressure)	Метод обратного давления используется на полудуплексных соединениях для регулирования потока данных от встречного устройства путем создания коллизий. Метод позволяет избежать переполнения буферной памяти устройства и потери данных.
Агрегирование каналов (LAG, Link aggregation)	Агрегирование (объединение) каналов позволяет увеличить пропускную способность канала связи и повысить его надежность. Консольный сервер поддерживает статическое и динамическое агрегирование каналов. При динамическом агрегировании используется протокол LACP для управления группой каналов.

2.2.2 Функции при работе с MAC-адресами

В таблице 2 приведены функции устройства при работе с MAC-адресами.

Таблица 2 — Функции работы с MAC-адресами

Таблица MAC-адресов	Таблица MAC-адресов устанавливает соответствие между MAC-адресами и интерфейсами устройства и используется для коммутации пакетов данных. Терминальный сервер имеет таблицу емкостью до 128k MAC-адресов и резервируют определенные MAC-адреса для использования системой.
Режим обучения	MAC-таблица может содержать либо статические адреса, либо адреса, изученные при прохождении пакетов данных через устройство. Изучение происходит за счет регистрации MAC-адресов отправителей пакетов с привязкой их к портам и VLAN. Впоследствии эти данные используются для коммутации встречных пакетов. Время хранения зарегистрированных MAC-адресов ограничено, его продолжительность может настраиваться администратором. Если MAC-адрес получателя, указанный в принятом устройством пакете, отсутствует в таблице, то такой пакет отправляется далее как широковещательный в пределах L2-сегмента сети.

2.2.3 Функции второго уровня сетевой модели OSI

В таблице 3 приведены функции и особенности второго уровня (уровень 2 OSI).

Таблица 3 — Описание функций второго уровня (уровень 2 OSI)

Поддержка VLAN	VLAN (Virtual Local Area Network) — это средство разделения сети на изолированные сегменты на уровне L2. Использование VLAN позволяет повысить устойчивость работы крупных сетей за счет деления их на более мелкие сети, изолировать разнородный трафик данных между собой и решить многие другие задачи. Сервер поддерживают различные способы терминации VLAN: • VLAN на базе меток пакетов данных, в соответствии с IEEE 802.1Q; • Терминация Q-in-Q (802.1ad)

2.2.4 Функции третьего уровня сетевой модели OSI

В таблице 4 приведены функции третьего уровня (уровень 3 OSI).

Таблица 4 — Описание функций третьего уровня (Layer 3)

Статические IP-маршруты	Администратор устройства имеет возможность добавлять и удалять статические записи в таблицу маршрутизации.
Таблица ARP	ARP (Address Resolution Protocol) — протокол для выяснения соответствия адресов сетевого и канального уровней. Таблица ARP содержит информацию об изученном соответствии. Соответствие устанавливается на основе анализа ответов от сетевых устройств, адреса устройств запрашиваются с помощью широковещательных пакетов.
Клиент DHCP	Протокол DHCP (Dynamic Host Configuration Protocol) дает возможность автоматизировать управление сетевыми устройствами. Клиент DHCP позволяет серверу получать сетевой адрес и дополнительные параметры от внешнего DHCP-сервера.

2.2.5 Функции управления и конфигурирования

Таблица 5 — Основные функции управления и конфигурирования

Загрузка и выгрузка файла настройки	Параметры устройства сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства. Для передачи файлов могут использоваться протоколы TFTP, FTP, SCP.
Интерфейс командной строки (CLI)	Управление посредством CLI осуществляется локально через последовательный порт RS-232 либо удаленно через Telnet, SSH. Интерфейс командной строки консоли (CLI) является промышленным стандартом. Интерпретатор CLI предоставляет список команд и ключевых слов для помощи пользователю и сокращению объема вводимых данных.
Syslog	Протокол Syslog обеспечивает передачу информационных сообщений о происходящих в системе событиях и ведение журнала событий.
Сетевые утилиты ping, traceroute	Утилиты ping и traceroute — предназначены для проверки доступности сетевых устройств и для определения маршрутов передачи данных в IP-сетях.
Управление контролируемым доступом — уровни привилегий	Консольный сервер поддерживает управление уровнем доступа пользователей к системе. Уровни доступа позволяют управлять зонами ответственности администраторов устройств. Уровни доступа нумеруются от 1 до 15, уровень 15 соответствует полному доступу к управлению устройством.
Аутентификация	Аутентификация — это процедура проверки подлинности пользователя. Консольный сервер поддерживает следующие методы аутентификации: • локальная — для аутентификации используется локальная база данных пользователей, хранящаяся на самом устройстве; • групповая — база данных пользователей хранится на сервере аутентификации. Для взаимодействия с сервером используются протоколы RADIUS и TACACS.
Сервер SSH/ сервер Telnet	Функции сервера SSH и Telnet позволяют установить соединение с устройством для управления им.
Reverse SSH/Telnet	Функции позволяют управлять устройствами, непосредственно подключенными к консольным портам сервера.
Автоматическое восстановление конфигурации	Устройство поддерживает автоматическую систему восстановления конфигурации, которая предотвращает ситуации потери удаленного доступа к устройству после смены конфигурации. Если в течение заданного времени после изменения конфигурации не было введено подтверждение — произойдет автоматический откат конфигурации до предыдущего использовавшегося состояния.

2.2.6 Функции сетевой защиты

В таблице 6 приведены функции сетевой защиты, выполняемые устройством.

Таблица 6 — Функции сетевой защиты

Access Control List (ACL)	Механизм фильтрации трафика на терминальном сервере. Он позволяет разрешать или запрещать пакеты по заданным правилам. Возможна настройка гибкой фильтрации трафика по L2-L4 заголовкам.

2.3 Основные технические характеристики

Основные технические параметры консольного сервера приведены в таблице 7.

Таблица 7 — Основные технические характеристики

Общие параметры	
Интерфейсы	32 × Последовательный порт RS-232 (RJ-45) 2 × 10GBASE-R/1000BASE-X (SFP+/ SFP) 2 ×10/100/1000BASE-T (RJ-45) 2 × USB 3.0 1 × Консольный порт RS-232 (RJ-45) 1 × Modem (Dial-up) 1 × Слот для micro-SD карт
Типы оптических трансиверов	1000BASE-X SFP 10GBASE-R SFP+
Дуплексный и полудуплексный режимы интерфейсов	• дуплексный и полудуплексный режимы для электрических портов • дуплексный режим для оптических портов
Скорость передачи данных	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10 Гбит/с
Количество статических маршрутов	100
Размер базы FIB	300
Количество L3-интерфейсов	sub – 5 Q-in-Q – 5

Соответствие стандартам	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3ae 10GBASE Ethernet ANSI/IEEE 802.3 автоопределение скорости IEEE 802.3x контроль потоков данных IEEE 802.3ad объединение каналов LACP IEEE 802.1Q виртуальные локальные сети VLAN IEEE 802.1v, IEEE 802.3ac
Управление	
Локальное управление	CLI
Удаленное управление	Telnet, SSH
Физические характеристики и условия окружающей среды	
Источники питания	Сеть переменного тока: 100—240 В, 50—60 Гц Сеть постоянного тока: 36—72 В Варианты питания: • один источник питания постоянного или переменного тока; • два источника питания постоянного или переменного тока с возможностью горячей замены.
Максимальная потребляемая мощность	32 Вт
Масса	3,854 кг
Габаритные размеры (Ш × В × Г)	440 × 44 × 308 мм
Интервал рабочих температур	от -10 до +45 °C
Интервал температуры хранения	от -40 до +70 °C
Относительная влажность при эксплуатации (без образования конденсата)	не более 80 %
Относительная влажность при хранении (без образования конденсата)	от 10 до 95 %
Срок службы	не менее 15 лет

2.4 Конструктивное исполнение

В данном разделе описано конструктивное исполнение устройства. Представлены изображения передней, задней и боковых панелей устройства. Описаны разъемы, светодиодные индикаторы и органы управления.

2.4.1 Конструктивное исполнение SCS-32

Устройство выполнено в металлическом корпусе с возможностью установки в 19” конструктив, высота корпуса 1U.

Передняя панель устройства SCS-32

Внешний вид передней панели SCS-32 показан на рисунке 1.

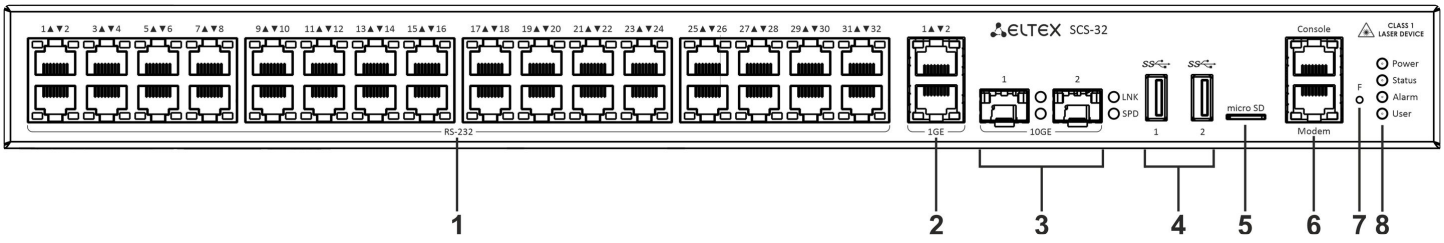


Рисунок 1 — Передняя панель SCS-32

В таблице 8 приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели SCS-32.

Таблица 8 — Описание разъемов, индикаторов и органов управления передней панели SCS-32

№	Элемент передней панели	Описание
1	RS-232	32 последовательных порта для подключения устройств к консольному серверу.
2	1GE	2 порта Gigabit Ethernet 10/100/1000BASE-T (RJ-45).
3	10GE	2 порта 10GBASE-R/1000BASE-X (SFP+/ SFP).
4	USB	2 порта USB 3.0 для подключения USB-устройств.
5	microSD	Разъем для установки microSD-карты памяти.
6	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
	Modem (Dial-up)	Последовательный порт RS-232 (RJ-45) для подключения внешнего модема.
7	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.

№	Элемент передней панели	Описание
8	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.

Задняя панель устройств SCS-32

Внешний вид задней панели SCS-32 показан на рисунке 2.

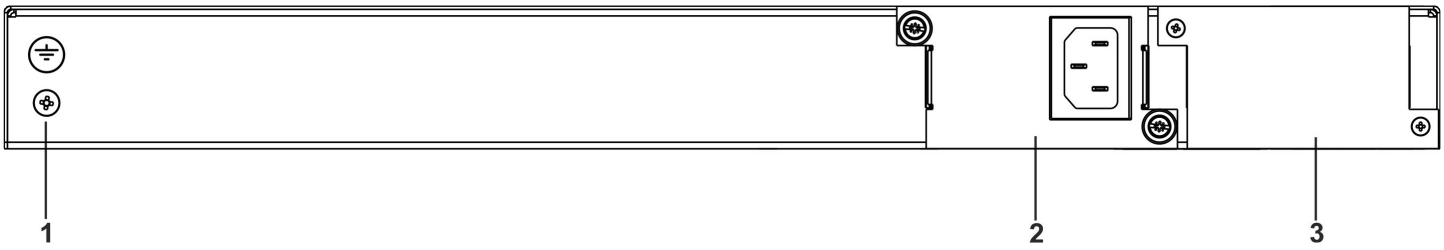


Рисунок 2 — Задняя панель SCS-32

В таблице 9 приведен перечень разъемов, расположенных на задней панели SCS-32.

Таблица 9 — Описание разъемов задней панели SCS-32

№	Описание
1	Клемма для заземления устройства.
2	Основной источник питания
3	Место для установки резервного источника питания.

Боковые панели устройства SCS-32

Внешний вид боковых панелей SCS-32 приведен на рисунках ниже.

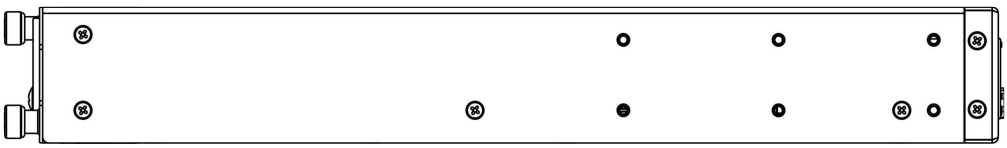


Рисунок 3 — Левая панель SCS-32

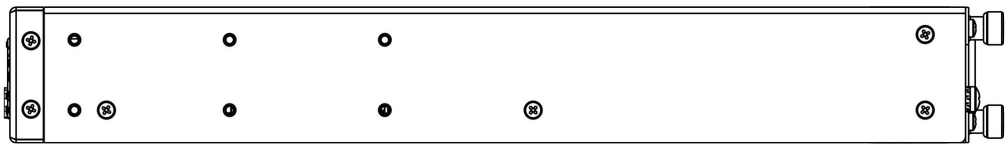


Рисунок 4 — Правая панель SCS-32

2.4.2 Световая индикация

Световая индикация SCS-32

Состояние интерфейсов Ethernet отображается двумя светодиодными индикаторами — LINK/ACT зеленого цвета и SPEED янтарного цвета.

Таблица 10 — Световая индикация состояния интерфейсов Ethernet

Свечение индикатора SPEED	Свечение индикатора LINK/ ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Выключен	Горит постоянно зеленым	Установлено соединение на скорости 10 или 100 Мбит/с.
Горит постоянно янтарным	Горит постоянно зеленым	Установлено соединение на скорости 1000 Мбит/с.
X	Мигает	Идет передача данных.

1

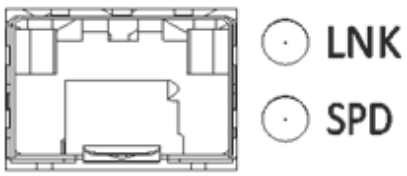


Рисунок 5 — Расположение индикаторов состояния SFP/SFP+-интерфейсов

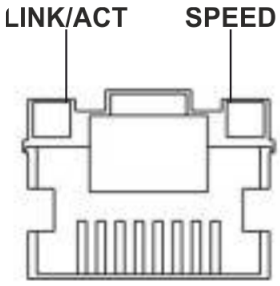


Рисунок 6 — Расположение индикаторов разъема RJ-45

В следующей таблице приведено описание состояний системных индикаторов устройства и их значений.

Таблица 11 — Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		Красный	Отказ внутренних источников питания устройства.
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Мигает зеленым	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.	-	-

2.5 Комплект поставки

В базовый комплект поставки SCS-32 входят:

- консольный сервер SCS-32;
- комплект для крепления устройства в стойку 19”;
- декларация соответствия;
- паспорт;
- памятка о документации.

⚠ По заказу покупателя в комплект поставки могут быть включены SFP/SFP+-трансиверы.

3 Установка и подключение

В данном разделе описаны процедуры установки устройства в стойку и подключения к питающей сети.

3.1 Установка устройства в стойку

Для установки устройства в стойку:

1. Выберите необходимое положение кронштейна (рисунок 7). Совместите четыре отверстия кронштейна с четырьмя отверстиями на боковой панели устройства. С помощью отвертки прикрепите кронштейн винтами к корпусу.
2. Повторите шаг 1 для другой боковой панели устройства.
3. Совместите отверстия кронштейнов с отверстиями на передних вертикальных направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки, для того чтобы устройство располагалось горизонтально.
4. С помощью отвертки прикрепите консольный сервер к стойке винтами.

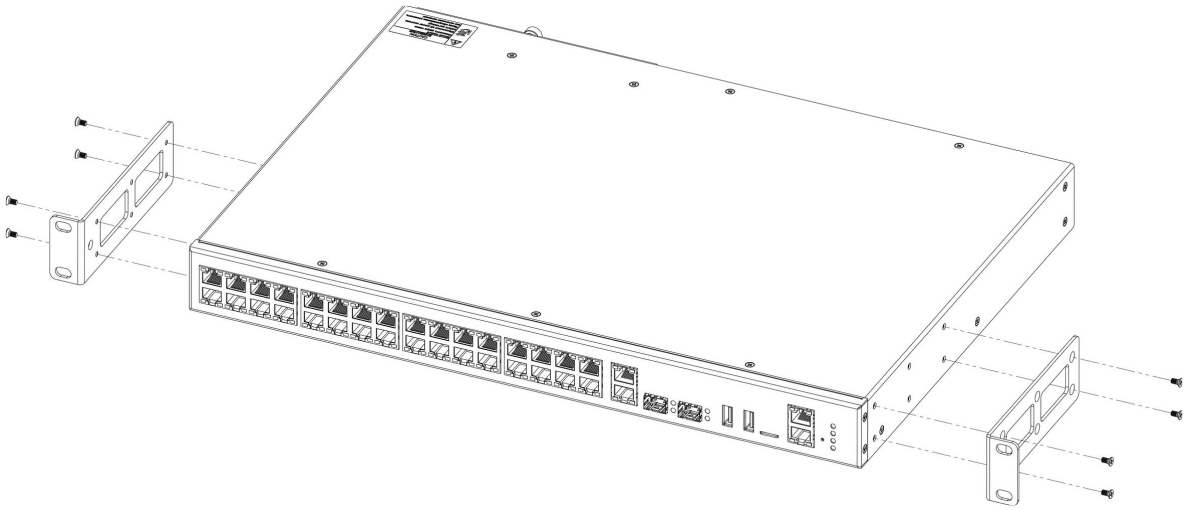


Рисунок 7 – Крепление кронштейнов к устройству

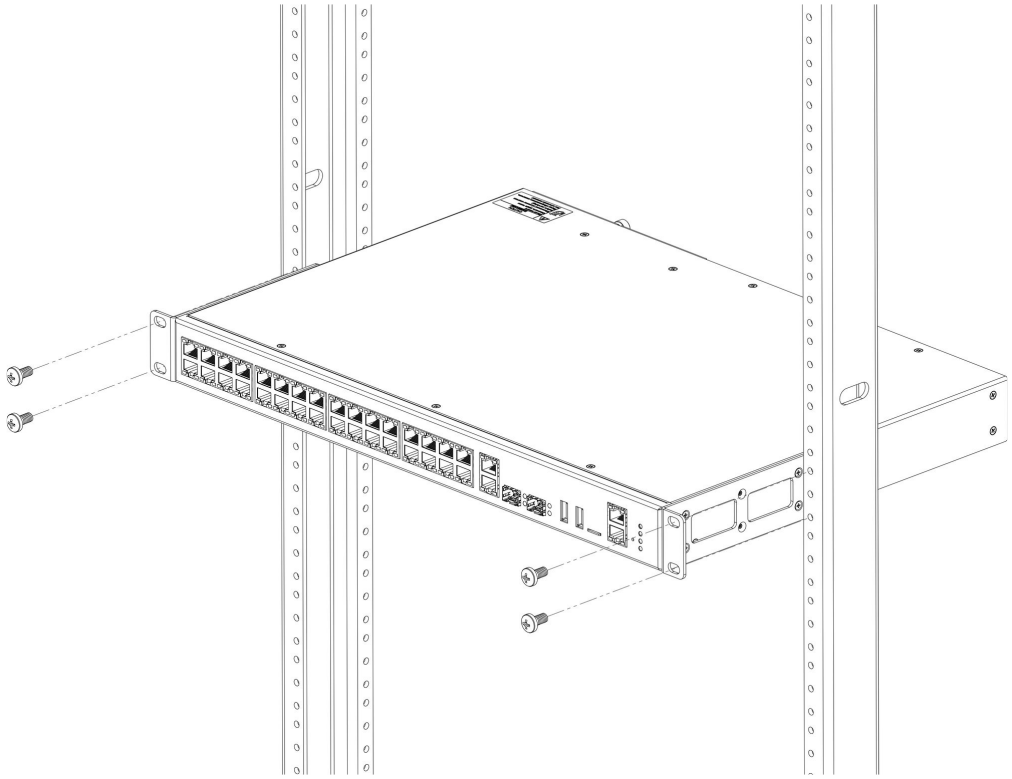


Рисунок 8 − Установка устройства в стойку

3.2 Установка модулей питания

Консольный сервер может работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

Места для установки модулей питания с электрической точки зрения равноценны. С точки зрения использования устройства, модуль питания может находиться в основном и резервном разъемах, информация о приоритетности находится в таблице "Описание разъемов задней панели консольного сервера". Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания консольный сервер продолжает работу без перезапуска.

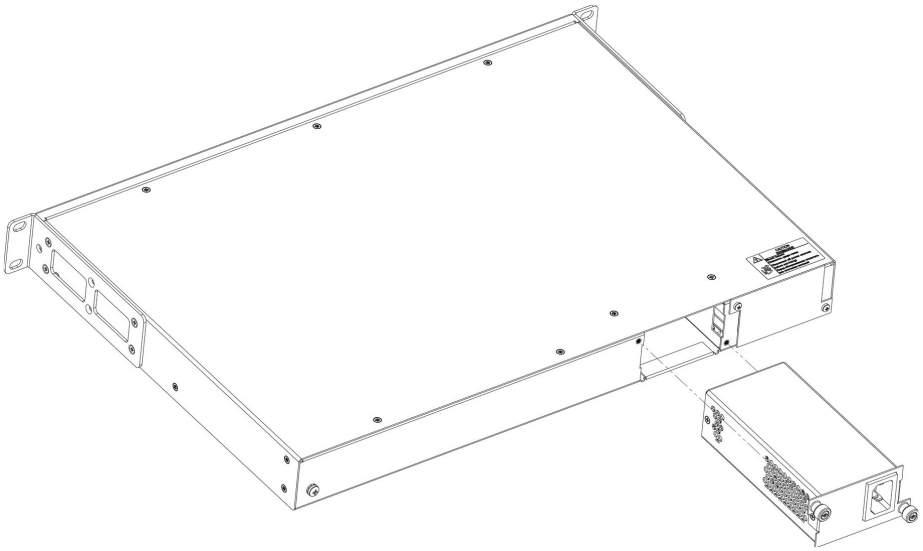


Рисунок 9 − Установка модулей питания

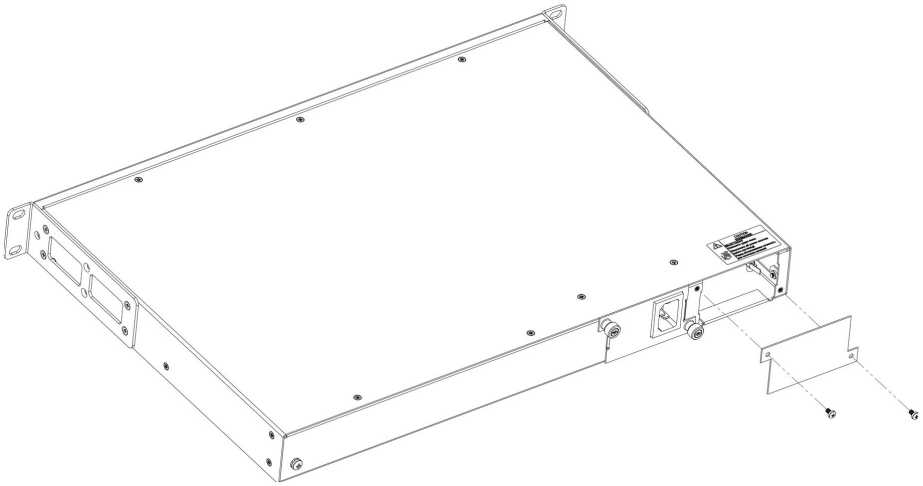


Рисунок 10 – Установка заглушки

Индикация аварии модуля питания может быть вызвана не только отказом модуля, но и отсутствием первичного питания.

Состояние модулей питания может быть проверено по индикации на передней панели консольного сервера (см. раздел Световая индикация) или по диагностике, доступной через интерфейсы управления устройства.

3.3 Подключение питающей сети

1. Прежде чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства через заземляющий винт М4. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиями Правил устройства электроустановок (ПУЭ).
2. Оборудование, подключаемое к последовательному порту консольного сервера, также должно быть надежно заземлено.
3. Подключите к устройству кабель питания. В зависимости от комплектации устройства, питание может осуществляться от сети переменного тока либо от сети постоянного тока. При подключении сети переменного тока следует использовать кабель, входящий в комплект устройства. Для подключения к сети постоянного тока используйте провод сечением не менее 1 мм^2.
4. Включите питание устройства и убедитесь в отсутствии аварий по состоянию индикаторов на передней панели.

3.4 Установка и удаление SFP-трансиверов

⚠ Установка оптических модулей может производиться как при выключенном, так и при включенном устройстве.

3.4.1 Установка трансивера

1. Вставьте верхний SFP-модуль в слот открытой частью разъема вниз, а нижний SFP-модуль – открытой частью разъема вверх.

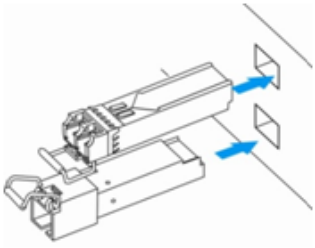


Рисунок 11 – Установка SFP-трансиверов

2. Надавите на модуль по направлению внутрь корпуса устройства до появления характерного щелчка фиксации модуля.

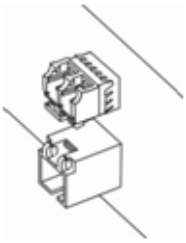


Рисунок 12 – Установленные SFP-трансиверы

3.4.2 Удаление трансивера

1. Откиньте рукоятку модуля, это приведет к разблокированию удерживающей защелки.

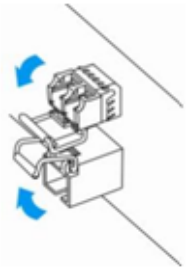


Рисунок 13 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

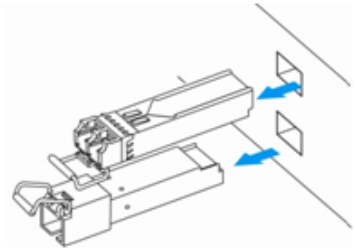


Рисунок 14 – Извлечение SFP-трансиверов

4 Интерфейсы управления

Настройка и мониторинг устройства могут осуществляться через различные интерфейсы управления.

Для доступа к устройству может использоваться сетевое подключение по протоколам Telnet и SSH или прямое подключение через консольный порт, соответствующий спецификации RS-232. При доступе по протоколам Telnet, SSH и при подключении через консольный порт для управления устройством используется интерфейс командной строки.

> ⚠ Заводская конфигурация включает в себя преднастроенный интерфейс gigabitethernet 1/0/1 с адресом 192.168.1.1/24 для доступа к устройству по протоколу SSH.
> В заводской конфигурации по умолчанию создан пользователь «admin» с паролем «password».

При использовании любого из перечисленных интерфейсов управления действуют единые принципы работы с конфигурацией. Должна соблюдаться определенная, описанная здесь, последовательность изменения и применения конфигурации, позволяющая защитить устройство от некорректного конфигурирования.

4.1 Интерфейс командной строки (CLI)

Интерфейс командной строки (Command Line Interface, CLI) – интерфейс, предназначенный для управления, просмотра состояния и мониторинга устройства. Для работы потребуется любая установленная на ПК программа, поддерживающая работу по протоколам Telnet, SSH или прямое подключение через консольный порт (например, HyperTerminal).

Интерфейс командной строки обеспечивает авторизацию пользователей и ограничивает их доступ к командам на основании уровня доступа, заданного администратором.

В системе может быть создано необходимое количество пользователей, права доступа задаются индивидуально для каждого из них.

Для обеспечения безопасности командного интерфейса все команды разделены на две категории – привилегированные и непривилегированные. К привилегированным в основном относятся команды конфигурирования. К непривилегированным – команды мониторинга.

Система позволяет нескольким пользователям одновременно подключаться к устройству.

4.2 Типы и порядок именования интерфейсов консольного сервера

При работе консольного сервера используются сетевые интерфейсы различного типа и назначения. Система именования позволяет однозначно адресовать интерфейсы по их функциональному назначению и местоположению в системе. Далее в таблице приведен перечень типов интерфейсов.

Таблица 12 – Типы и порядок именования интерфейсов сервера

Тип интерфейса	Обозначение
Физические интерфейсы	Обозначение физического интерфейса включает в себя его тип и идентификатор. Идентификатор физических интерфейсов имеет вид **<ID>/<SLOT>/<PORT>**, где: • **<ID>** – идентификатор устройства, • **<SLOT>** – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • **<PORT>** – порядковый номер порта.
Порты 1 Гбит/с	**gigabitethernet <ID>/<SLOT>/<PORT>** Пример обозначения: **gigabitethernet 1/0/1** ⚠ Допускается использовать сокращенное наименование, например gi1/0/1.
Порты 10 Гбит/с	**tengigabitethernet <ID>/<SLOT>/<PORT>** Пример обозначения: **tengigabitethernet 1/0/2** ⚠ Допускается использовать сокращенное наименование, например te1/0/2.
Группы агрегации каналов	Обозначение группы агрегации каналов включает в себя его тип и идентификатор. Идентификатор имеет порядковый номер группы агрегации каналов в диапазоне [1..2]. Примеры обозначений: **port-channel 1** ⚠ Допускается использовать сокращенное наименование, например, po1.
Саб-интерфейсы	Обозначение саб-интерфейса образуется из обозначения базового интерфейса и идентификатора (VLAN) саб-интерфейса, разделенных точкой. Примеры обозначений: • **gigabitethernet 1/0/1.100** • **tengigabitethernet 1/0/2.123** • **port-channel 1.6** ⚠ Идентификатор саб-интерфейса может принимать значения [2..4094].

Тип интерфейса	Обозначение
Q-in-Q интерфейсы	Обозначение Q-in-Q интерфейса образуется из обозначения базового интерфейса, идентификатора сервисного VLAN и идентификатора пользовательского VLAN, разделенных точкой. Примеры обозначений: • **gigabitethernet 1/0/1.100.10** • **tengigabitethernet 1/0/2.45.12** • **port-channel 1.6.34** ⚠ Идентификатор сервисного и пользовательского VLAN может принимать значения [1..4094].
Логические интерфейсы	Обозначение логического интерфейса является порядковым номером интерфейса: Примеры обозначений: • **loopback 4**
Последовательные интерфейсы	Обозначение последовательного интерфейса включает в себя его тип и идентификатор. Идентификатор последовательного интерфейса имеет вид **<ID>/<SLOT>/<PORT>**, где • **<ID>** – идентификатор устройства, • **<SLOT>** – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • **<PORT>** – порядковый номер порта. Пример обозначения: **serial 1/0/1, aux 1/0/1**
USB-модемы	Обозначение USB-модема включает в себя его тип и порядковый номер: **cellular modem <MODEM-NUM>** Пример обозначения: **cellular modem 1**

⚠ Некоторые команды поддерживают одновременную работу с группой интерфейсов. Для указания группы интерфейсов может быть использовано перечисление через запятую или указание диапазона идентификаторов через дефис «-».
Примеры указания групп интерфейсов:

```
interface gigabitethernet 1/0/1, gigabitethernet 1/0/2
interface tengigabitethernet 1/0/1-2
interface gi1/0/1-2,te1/0/1
```

5 Начальная настройка консольного сервера

5.1 Заводская конфигурация консольного сервера

При отгрузке устройства потребителю на нем загружена заводская конфигурация, которая включает минимально необходимые базовые настройки, позволяющие получить сетевой доступ к устройству для выполнения расширенного конфигурирования.

5.1.1 Описание заводской конфигурации

```
syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit

interface gigabitethernet 1/0/1
  ip address 192.168.1.1/24
exit
interface gigabitethernet 1/0/2
  shutdown
exit
interface tengigabitethernet 1/0/1
  shutdown
exit
interface tengigabitethernet 1/0/2
  shutdown
exit

security passwords default-expired

ip ssh server

ntp enable
ntp broadcast-client enable
```

Для подключения к локальной сети настроен интерфейс Gigabitethernet 1/0/1 с адресом 192.168.1.1/24. Остальные интерфейсы находятся в выключенном состоянии. Для сетевого доступа к серверу включен протокол SSH. Также для синхронизации времени преднастроен NTP-клиент в широковещательном режиме. Активировано логирование со следующими параметрами: максимальное количество файлов для логирования — 3, размер каждого — 512 КБ, уровень логирования — info.

Для обеспечения возможности конфигурирования устройства при первом включении в конфигурации сервера создана учетная запись администратора "admin" с паролем "password". Пользователю будет предложено изменить пароль администратора при начальном конфигурировании устройства.

5.2 Подключение и конфигурирование консольного сервера

Консольный сервер предназначен для обеспечения централизованного удаленного доступа к консольным портам сетевого и серверного оборудования. Он используется для управления устройствами через последовательные (console) интерфейсы, независимо от состояния их основной сети. Основной функцией консольного сервера является предоставление администраторам возможности подключаться к оборудованию (маршрутизаторам, коммутаторам, серверам) через консольные порты, что важно при первичной настройке, диагностике и восстановлении после сбоев. Даже при недоступности устройства по IP-сети доступ через консоль остается возможным.

5.2.1 Подключение к консольному серверу

Предусмотрены следующие способы подключения к устройству:

Подключение по локальной сети Ethernet

При первоначальном старте устройство загружается с заводской конфигурацией. Описание заводской конфигурации приведено в разделе Заводская конфигурация консольного сервера данного руководства.

Для работы достаточно подключить сетевой кабель передачи данных (патч-корд) к порту Gigabitethernet 1/0/1.

Подключение через консольный порт RS-232

При помощи кабеля RJ-45/DBF9, который входит в комплект поставки устройства, соедините порт **«Console»** консольного сервера с портом RS-232 компьютера.

Запустите терминальную программу (например, HyperTerminal или Minicom) и создайте новое подключение. Должен быть использован режим эмуляции терминала VT100.

Выполните следующие настройки интерфейса RS-232:

Скорость: 115200 бит/с
Биты данных: 8 бит
Четность: нет
Стоповые биты: 1
Управление потоком: нет

5.2.2 Применение изменения конфигурации

Любые изменения, внесенные в конфигурацию, вступят в действие только после применения команды:

```
scs# commit
Configuration has been successfully committed
```

После применения данной команды запускается таймер "отката" конфигурации. Для остановки таймера и механизма "отката" используется команда:

```
scs# confirm
Configuration has been successfully confirmed
```

Значение таймера "отката" по умолчанию — 600 секунд. Для изменения данного таймера используется команда:

```
scs(config)# system config-confirm timeout <TIME>
```

- <TIME> — интервал времени ожидания подтверждения конфигурации, принимает значение в секундах [120..86400].

5.2.3 Базовая настройка сервера

Процедура настройки SCS-32 при первом включении состоит из следующих этапов:

- Изменение пароля пользователя «admin» при первой авторизации.
- Создание новых пользователей.
- Назначение имени устройства (Hostname).
- Применение базовых настроек.

Изменение пароля пользователя «admin» при первой авторизации

При первом входе в систему необходимо сменить пароль по умолчанию привилегированного пользователя «admin». До смены пароля пользовательская настройка устройства недоступна.

После указания нового пароля необходимо применить изменения в конфигурации командой **commit** и подтвердить изменения командой **confirm**:

```
scs(change-expired-password)# password <new password>
scs(change-expired-password)# commit
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
scs(change-expired-password)# confirm
Configuration has been confirmed. Commit timer canceled.
scs#
```

Создание новых пользователей

Для управления устройством SCS существует возможность создавать пользовательские учетные записи, у которых администратор может индивидуально задать:

- пароль;
- уровень привилегий;

- режим работы учетной записи.

Для создания нового пользователя системы или настройки любого из параметров: имени пользователя, пароля, уровня привилегий и режима работы используются команды:

```
scs(config)# username <name>
scs(config-user)# password <password>
scs(config-user)# privilege <privilege>
scs(config-user)# mode <mode>
scs(config-user)# exit
```

⚠ Уровни привилегий 1-9 разрешают доступ к устройству и просмотр его оперативного состояния, но запрещают настройку. Уровни привилегий 10-14 разрешают как доступ, так и настройку большей части функций устройства. Уровень привилегий 15 разрешает как доступ, так и настройку всех функций устройства.

⚠ У учетных записей есть несколько режимов работы:

- cli — режим работы по умолчанию, пользователь получает доступ к интерфейсу командной строки, предназначенному для управления, просмотра состояния и мониторинга устройства;
- techsupport — пользователь получает доступ к командной оболочке, в которой выполняется процедура отладки устройства совместно с специалистами технической поддержки;
- sftp — пользователь используется для организации доступа к встроенному SFTP-серверу, возможность работы в какой-либо командой оболочке при этом у пользователя отсутствует.

⛔ Пользователь «admin» является единственным предустановленным пользователем в конфигурации устройства. Это приводит к определенным особенностям работы с ним:
1) Применение команды no username admin не удаляет пользователя «admin» из конфигурации, а приводит его к настройкам по умолчанию — паролю «password» и 15 уровню привилегий.
2) Отключить возможность авторизации пользователя «admin» можно командой **no admin login enable**.
3) Пользователь «admin» с настройками по умолчанию (пароль «password», уровень привилегий 15) не отображается в выводах команд **show running-config** и **show candidate-config**.

Пример команд для создания нескольких учетных записей — пользователя «**netmaster**» с уровнем привилегий **15** для управления оборудованием, пользователя «**watcher**» с уровнем привилегий **1** для ограниченного просмотра оперативной информации, а также пользователя «**techsup**» для отладки устройства совместно с сотрудниками технической поддержки:

```
scs# configure
scs(config)# username netmaster
scs(config-user)# password P@ssW0rd
scs(config-user)# privilege 15
scs(config-user)# exit
scs(config)# username watcher
scs(config-user)# password password
scs(config-user)# privilege 1
scs(config-user)# exit
scs(config)# username techsup
scs(config-user)# password PsWdTs
scs(config-user)# mode techsupport
scs(config-user)# exit
scs(config)#
```

Назначение имени устройства

Для назначения имени устройства используются следующие команды:

```
scs# configure
scs(config)# hostname <new-name>
```

После применения конфигурации приглашение командной строки изменится на значение, заданное параметром <**new-name**>.

6 Рекомендации по безопасной настройке

Рекомендации по безопасной настройке носят общий характер и подходят для большинства инсталляций. Настоящие рекомендации в значительной степени повышают безопасность эксплуатации устройства, но не являются исчерпывающими. В зависимости от схемы применения устройства необходимо настраивать и другие параметры безопасности. В некоторых специфических случаях выполнение данных рекомендаций может привести к неработоспособности сети. При настройке устройства стоит в первую очередь следовать техническим требованиям и регламентам сетей, в которых будет эксплуатироваться данное устройство.

6.1 Общие рекомендации

- Рекомендуется всегда отключать неиспользуемые физические интерфейсы с помощью команды shutdown. Команда подробно описана в разделе Конфигурирование и мониторинг интерфейсов справочника команд CLI.
- Рекомендуется всегда настраивать синхронизацию системных часов с доверенными источниками сетевого времени (NTP). Алгоритм настройки NTP приведен в разделе Настройка NTP настоящего руководства. Подробная информация о командах для настройки NTP приведена в разделе Управление системными часами справочника команд CLI.
- Рекомендуется отключать NTP broadcast client, включенный по умолчанию в заводской конфигурации.
- Рекомендуется использовать ACL для ограничения доступа к консольному серверу и устройствам, непосредственно подключенным к устройству. Алгоритм настройки списков доступа приведён в разделе Управление безопасностью настоящего руководства.

6.2 Настройка системы логирования событий

Алгоритмы настройки системы логирования событий приведены в подразделе «Настройка Syslog» раздела Мониторинг настоящего руководства.

Подробная информация о командах для настройки системы логирования событий приведена в разделе Управление SYSLOG справочника команд CLI.

6.2.1 Рекомендации

- Рекомендуется настроить хранение сообщений о событиях в файл syslog на устройстве и передачу этих событий на внешний syslog-сервер.
- Рекомендуется ограничивать размер syslog-файла на устройстве.
- Рекомендуется настраивать ротацию syslog-файлов на устройстве.
- Рекомендуется включать нумерацию сообщений syslog.

6.2.2 Предупреждения

- Данные, хранящиеся в файловой системе **tmpsys:syslog**, не сохраняются при перезагрузке устройства. Этот тип файловой системы рекомендуется использовать для хранения оперативных логов.
- Не рекомендуется использовать файловую систему **flash:syslog** для хранения логов, так как это может привести к преждевременному выходу из строя устройства.

6.2.3 Пример настройки

Задача:

Настроить хранение сообщений о событиях уровня info и выше в файл syslog на устройстве и настроить передачу этих событий на внешний syslog-сервер. Ограничить файл размером 512 кБ. Включить ротацию 3 файлов. Включить нумерацию сообщений syslog.

Решение:

Настраиваем хранение syslog-сообщений в файле:

```
scs(config)# syslog file tmpsys:syslog/default
scs((config-syslog-file)# severity info
scs((config-syslog-file)# exit
```

Настраиваем ограничение размера и ротацию файлов:

```
scs(config)# syslog max-files 3
scs(config)# syslog file-size 512
```

Настраиваем передачу сообщений на внешний сервер:

```
scs(config)# syslog host mylog
scs(config-syslog-host)# remote-address 192.0.2.2
scs(config-syslog-host)# transport udp
scs(config-syslog-host)# port 514
scs(config-syslog-host)# severity info
scs(config-syslog-host)# exit
```

Включаем нумерацию сообщений syslog:

```
scs(config)# syslog sequence-numbers
```

6.3 Настройка политики использования паролей

Алгоритмы настройки политики использования паролей приведены в разделе Настройка AAA настоящего руководства.

Подробная информация о командах для настройки политики использования паролей приведена в разделе Настройка AAA справочника команд CLI.

6.3.1 Рекомендации

- Рекомендуется всегда включать требования на смену пароля по умолчанию пользователя admin.
- Рекомендуется ограничивать время жизни паролей и запрещать повторно использовать как минимум предыдущий пароль.
- Рекомендуется выставлять требования минимальной длины пароля больше 8 символов.
- Рекомендуется выставлять требования на использование строчных и прописных букв, цифр и спецсимволов.

6.3.2 Пример настройки

Задача:

- Настроить парольную политику с обязательным требованием смены пароля по умолчанию, временем действия пароля 1 месяц и запретом на использование 12 последних паролей.
- Задать минимальную длину пароля 16 символов, максимальную — 64 символа.
- Пароль должен содержать не менее 3 прописных букв, не менее 5 строчных букв, не менее 4 цифр и не менее 2 спецсимволов. Пароль в обязательном порядке должен содержать все 4 типа символов.

Решение:

Включаем запрос на смену пароля по умолчанию для пользователя admin:

```
scs(config)# security passwords default-expired
```

Устанавливаем время жизни пароля 30 дней и запрет на использование предыдущих 12 паролей:

```
scs(config)# security passwords lifetime 30
scs(config)# security passwords history 12
```

Устанавливаем ограничения на длину пароля:

```
scs(config)# security passwords min-length 16
scs(config)# security passwords max-length 24
```

Устанавливаем ограничения по минимальному количеству символов соответствующих типов:

```
scs(config)# security passwords upper-case 3
scs(config)# security passwords lower-case 5
scs(config)# security passwords special-case 2
scs(config)# security passwords numeric-count 4
scs(config)# security passwords symbol-types 4
```

6.4 Настройка политики AAA

Алгоритмы настройки политики AAA приведены в разделе Настройка AAA настоящего руководства.

Подробная информация о командах для настройки политики AAA приведена в разделе Настройка AAA справочника команд CLI.

6.4.1 Рекомендации

- Рекомендуется использовать ролевую модель доступа на устройство.
- Рекомендуется использовать персональные учетные записи для аутентификации на устройстве.
- Рекомендуется включать логирование вводимых пользователем команд.
- Рекомендуется использовать несколько методов аутентификации для входа на устройства через консоль, удалённого входа на устройства и повышения привилегий. Оптимальной считается комбинация из аутентификации по одному из протоколов RADIUS/TACACS/LDAP и локальной аутентификации.
- Рекомендуется отключить встроенную учётную запись **admin**.
- Рекомендуется настроить логирование изменений локальных учётных записей.
- Рекомендуется настроить логирование изменений политики AAA.

6.4.2 Предупреждения

- Встроенную учётную запись **admin** удалить нельзя, только отключить авторизацию для неё командой **no admin login enable**.
- Команда **no username admin** не удаляет пользователя **admin**, сбрасывает его конфигурацию в значения по умолчанию. После применения этой команды пользователь **admin** не будет отображаться в конфигурации.
- Команда **no password** для пользователя **admin** также не удаляет пароль пользователя **admin**, а сбрасывает его в значение по умолчанию. После применения этой команды пароль пользователя admin перестает отображаться в конфигурации и становится ‘password'.
- Перед отключением авторизации для пользователя **admin** в конфигурацию устройства необходимо настроить пользователя с уровнем привилегий 15 или задать ENABLE-пароль для уровня привилегий 15.

6.4.3 Пример настройки

Задача:

Настроить политику AAA:

- Для удаленного входа по протоколу SSH использовать аутентификации через RADIUS.
- Для входа через локальную консоль использовать аутентификации через RADIUS, в случае отсутствия связи с RADIUS-серверами использовать локальную аутентификацию.
- Использовать ENABLE-пароль, заданный через RADIUS, в случае отсутствия связи с RADIUS-серверами использовать локальный ENABLE-пароль.
- Установить пользователю admin пониженный уровень привилегий.
- Настроить логирование изменений локальных учетных записей.
- Настроить логирование изменений политик AAA.
- Настроить логирование вводимых команд.

Решение:

Создаем локального пользователя local-operator с уровнем привилегий 8:

```
scs(config)# username local-operator
scs(config-user)# password Pa$$w0rd1
scs(config-user)# privilege 8
scs(config-user)# exit
```

Задаём локальный ENABLE-пароль:

```
scs(config)# enable password $6e5c4r3e2t!
```

Далее необходимо отключить авторизацию у пользователя admin:

```
scs(config)# no admin login enable
```

Настраиваем связь с двумя RADIUS-серверами, основным 192.168.1.11 и резервным 192.168.2.12:

```
scs(config)# radius-server host 192.168.1.11
scs(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
scs(config-radius-server)# priority 100 scs(config-radius-server)# exit
scs(config)# radius-server host 192.168.2.12
scs(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
scs(config-radius-server)# priority 150
scs(config-radius-server)# exit
```

Настраиваем политику AAA:

```
scs(config)# aaa authentication login CONSOLE radius local
scs(config)# aaa authentication login SSH radius
scs(config)# aaa authentication enable default radius enable
scs(config)# aaa authentication mode break
scs(config)# line console
scs(config-line-console)# login authentication CONSOLE
scs(config-line-console)# exit scs(config)# line ssh
scs(config-line-ssh)# login authentication SSH
scs(config-line-ssh)# exit
```

Настраиваем логирование:

```
scs(config)# logging userinfo
scs(config)# logging aaa
scs(config)# syslog cli-commands
```

6.5 Настройка удаленного управления

Подробная информация о командах настройки удаленного доступа приведена в разделе Настройка доступа SSH, Telnet справочника команд CLI.

6.5.1 Рекомендации

- Не рекомендуется включать удаленное управление по протоколу Telnet.
- Рекомендуется использовать криптостойкие алгоритмы аутентификации sha2-512 и отключить все остальные.
- Рекомендуется использовать криптостойкие алгоритмы шифрования aes256ctr и отключить все остальные.
- Рекомендуется использовать криптостойкий алгоритм обмена ключами шифрования dh-group-exchange-sha256 и отключить все остальные.
- Рекомендуется использовать криптостойкий алгоритм верификации Host-Key для SSH rsa и отключить все остальные.
- Рекомендуется разрешить доступ к удаленному управлению устройством только с определенных IP-адресов.
- Перед началом эксплуатации рекомендуется перегенерировать ключи шифрования.

6.5.2 Пример настройки

Задача:

Сгенерировать новые ключи шифрования. Использовать криптостойкие алгоритмы.

Решение:

Отключаем устаревшие и не криптостойкие алгоритмы:

```
scs(config)# ip ssh server
scs(config)# ip ssh authentication algorithm md5 disable
scs(config)# ip ssh authentication algorithm md5-96 disable
scs(config)# ip ssh authentication algorithm ripemd160 disable
scs(config)# ip ssh authentication algorithm sha1 disable
scs(config)# ip ssh authentication algorithm sha1-96 disable
scs(config)# ip ssh authentication algorithm sha2-256 disable
scs(config)# ip ssh encryption algorithm 3des disable
scs(config)# ip ssh encryption algorithm aes128 disable
scs(config)# ip ssh encryption algorithm aes128ctr disable
scs(config)# ip ssh encryption algorithm aes192 disable
scs(config)# ip ssh encryption algorithm aes192ctr disable
scs(config)# ip ssh encryption algorithm aes256 disable
scs(config)# ip ssh encryption algorithm arcfour disable
scs(config)# ip ssh encryption algorithm arcfour128 disable
scs(config)# ip ssh encryption algorithm arcfour256 disable
scs(config)# ip ssh encryption algorithm blowfish disable
scs(config)# ip ssh encryption algorithm cast128 disable
scs(config)# ip ssh key-exchange algorithm dh-group-exchange-sha1 disable
scs(config)# ip ssh key-exchange algorithm dh-group1-sha1 disable
scs(config)# ip ssh key-exchange algorithm dh-group14-sha1 disable
scs(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp256 disable
scs(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp384 disable
scs(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp521 disable
scs(config)# ip ssh host-key algorithm dsa disable
scs(config)# ip ssh host-key algorithm ecdsa256 disable
scs(config)# ip ssh host-key algorithm ecdsa384 disable
scs(config)# ip ssh host-key algorithm ecdsa521 disable
scs(config)# ip ssh host-key algorithm ed25519 disable
```

Генерируем новые ключи шифрования:

```
scs# update ssh-host-key rsa 2048
```

7 Управление интерфейсами

7.1 Настройка физического интерфейса

7.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Переход в режим конфигурирования функционала.	**scs(config)# interface gigabitethernet** **scs(config)# interface tengigabitethernet** **scs(config)# interface port-channel <ID>**	<ID> — порядковый номер группы агрегации каналов, принимает значения [1..2].
2	Включить/отключить интерфейс.	**scs(config-if-gi)# shutdown/no shutdown**	
3	Задать описание (необязательно).	**scs(config-if-gi)# description <text>**	<text> — до 255 символов.
4	Задать MTU (необязательно).	**scs(config-if-gi)# mtu <count>**	<count> — 552-10000. Значение по умолчанию: 1500.
5	Задать скорость (необязательно).	**scs(config-if-gi)# speed 1000M/100M/10M/10G/auto**	Значение по умолчанию: auto.

Шаг	Описание	Команда	Ключи
6	Задать MAC-адрес (необязательно).	**scs(config-if-gi)# mac-address <ADDR>**	<ADDR> — MAC-адрес сетевого моста, задается в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

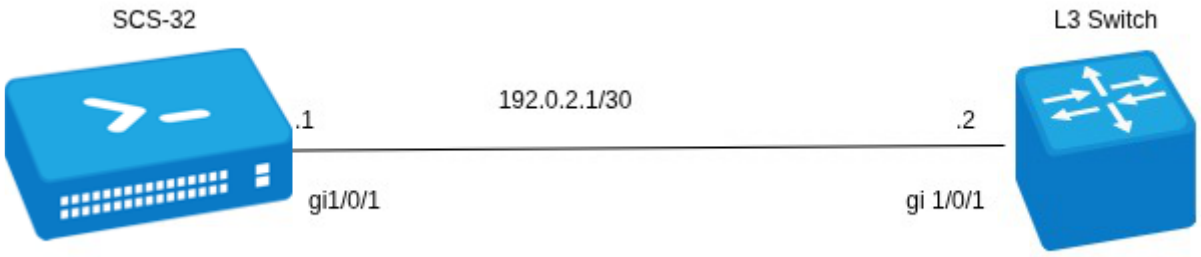
7.1.2 Алгоритм настройки режима L3

Шаг	Описание	Команда	Ключи
1.1	Задать IP-адрес. Получить IP-адрес от DHCP-сервера.	**scs(config-if-gi)# ip address <ADDR/LEN>** или **scs(config-if-gi)# ip address <ADDR/LEN> secondary**	<ADDR/LEN> — IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA — DDD принимает значения [0..255] и EE принимает значения [1..32]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом.
1.2		**scs(config-if-gi)# ip address dhcp**	
2.1	Задать IPv6-адрес. Получить IPv6-адрес от DHCP-сервера.	**scs(config-if-gi)# ipv6 address <ADDR/P>**	<ADDR/P> — IP-адрес и длина маски подсети, задаётся в виде <X:X:X:X::X/N>, где каждая буква X — это шестнадцатеричные значения шести 16-битных элементов адреса и N — длина префикса, принимает значения [1..128].
2.2		**scs(config-if-gi)# ipv6 address dhcp**	

7.1.3 Пример настройки в режиме L3

Задача:

Настроить интерфейс для терминации трафика в соответствии со схемой.



Решение:

Перейдите в режим конфигурирования, включите интерфейс и задайте IPv4-адрес из диапазона 192.0.2.0/30:

```
scs# configure
scs(config)# interface gigabitethernet 1/0/1
scs(config-if-gi)# no shutdown
scs(config-if-gi)# ip firewall disable
scs(config-if-gi)# ip address 192.0.2.1/30
```

Сохраните изменения:

```
scs(config)# commit
scs(config)# confirm
```

Для просмотра настроенного адреса можно воспользоваться следующей командой:

```
scs-32# sh ip interfaces
IP address        Interface       Admin     Link    Type      Precedence    Description
--------------   -------------   -------   -----   -------   -----------   -------------
192.0.2.1/30      gi1/0/1         Up        Up      static    primary       --
```

7.2 Настройка терминации на саб-интерфейсе

Для терминирования Ethernet-фреймов конкретного VLAN на определенном физическом интерфейсе необходимо создать саб-интерфейс с указанием номера VLAN, фреймы которого будут терминироваться. При создании двух саб-интерфейсов с одинаковыми VLAN, но на разных физических/агрегированных интерфейсах, коммутация Ethernet-фреймов между данными саб-интерфейсами будет невозможна, т. к. сегменты за пределами саб-интерфейсов будут являться отдельными широковещательными доменами. Для обмена данными между абонентами разных саб-интерфейсов (даже с одинаковым VLAN ID) будет использоваться маршрутизация, т. е. обмен данными будет происходить на третьем уровне модели OSI.

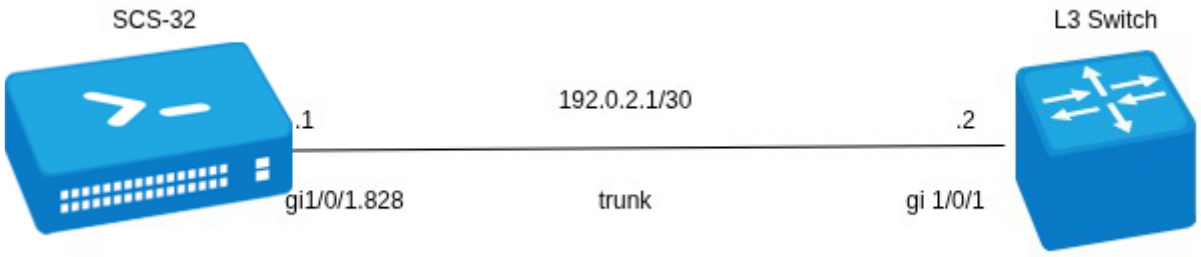
7.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса.	**scs(config)# interface gigabitethernet <PORT>.<S-VLAN>** или **interface tengigabitethernet <PORT>.<S-VLAN>** или **interface port-channel <CH> .<S-VLAN>**	<PORT> — номер физического интерфейса. <CH> — номер агрегированного интерфейса. <S-VLAN> — идентификатор создаваемого S-VLAN.
2	Задать описание саб-интерфейса (необязательно).	**scs(config-if-sub)# description <DESCRIPTION>**	<DESCRIPTION> — описание интерфейса, задается строкой до 255 символов.
3	Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически.	**scs(config-if-sub)# ip address <ADDR/LEN>** или **scs(config-if-sub)# ip address <ADDR/LEN> secondary**	<ADDR/LEN> — IP-адрес и длина маски подсети, задается в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA — DDD принимает значения [0..255] и EE принимает значения [1..32]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом.
		scs(config-if-sub)# ipv6 address <IPV6-ADDR/LEN>	<IPV6-ADDR/LEN> — IP-адрес и префикс подсети, задается в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].
		scs(config-if-sub)# ip address dhcp	Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом справочника команд CLI.

7.2.2 Пример настройки саб-интерфейса

Задача:

Настроить терминацию подсети 192.0.2.1/30 в VLAN: 828 на физическом интерфейсе gigabitethernet 1/0/1.



Решение:

Создадим саб-интерфейс для VLAN: 828:

```
scs(config)# interface gigabitethernet 1/0/1.828
```

Настроим IP-адрес из необходимой подсети:

```
scs(config)# interface gigabitethernet 1/0/1.828
scs(config-if-sub)# ip address 192.0.2.1/30
scs(config-if-sub)# exit
```

Сохраните изменения:

```
scs(config)# commit
scs(config)# confirm
```

Для просмотра настроенного адреса можно воспользоваться следующей командой:

```
scs-32# sh ip interfaces
IP address        Interface       Admin     Link    Type      Precedence    Description
--------------   -------------   -------   -----   -------   -----------   -------------
192.168.0.2/30    gi1/0/1.828      Up        Up      static    primary        --
```

7.3 Настройка терминации на Q-in-Q интерфейсе

Q-in-Q — технология передачи пакетов с двумя 802.1q-тегами. Данная технология используется для расширения количества используемых VLAN в сети передачи данных. Внутренним тегом (InnerTag) называется 802.1q-заголовок ближе к payload. Также внутренний тег называют C-VLAN (Customer VLAN). Внешний тег (OuterTag) — это 802.1q-заголовок, добавленный к изначальному 802.1q-пакетом, также называется S-VLAN (Service VLAN). Использование двойных меток в Ethernet-фреймах описывается протоколом 802.1ad.

7.3.1 Алгоритм настройки

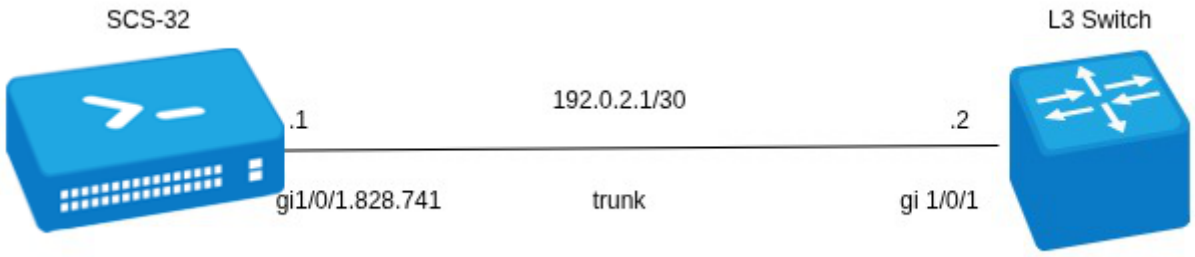
Шаг	Описание	Команда	Ключи
1	Создать саб-интерфейс физического интерфейса.	**scs(config)# interface gigabitethernet <PORT>.<S-VLAN>** или **interface tengigabitethernet <PORT>.<S-VLAN>** или **interface port-channel <CH>.<S-VLAN>**	<PORT> — номер физического интерфейса. <CH> — номер агрегированного интерфейса. <S-VLAN> — идентификатор создаваемого S-VLAN.
2	Создать Q-in-Q интерфейс.	**scs(config)# interface gigabitethernet <PORT>.<S-VLAN>.<C-VLAN>** или **scs(config)# interface tengigabitethernet <PORT>.<S-VLAN>.<C-VLAN>** или **scs(config)# interface port-channel <CH>.<S-VLAN>.<C-VLAN>**	<PORT> — номер физического интерфейса. <CH> — номер агрегированного интерфейса. <S-VLAN> — идентификатор создаваемого S-VLAN. <C-VLAN> — идентификатор создаваемого C-VLAN.
3	Задать описание Q-in-Q интерфейс (необязательно).	**scs(config-if-qinq)# description <DESCRIPTION>**	<DESCRIPTION> — описание интерфейса, задается строкой до 255 символов.
5	Указать IPv4/IPv6-адрес и маску подсети для конфигурируемого интерфейса или включить получение IP-адреса динамически.	**scs(config-if-qinq)# ip address <ADDR/LEN>** или **scs(config-if-qinq)# ip address <ADDR/LEN> secondary**	<ADDR/LEN> — IP-адрес и длина маски подсети, задается в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA — DDD принимает значения [0..255] и EE принимает значения [1..32]. Ключ secondary указывает, что настроенный адрес является дополнительным IP-адресом. Если это ключевое слово отсутствует, настроенный адрес является основным IP-адресом. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации справочника команд CLI.

Шаг	Описание	Команда	Ключи
		scs(config-if-qinq)# ipv6 address <IPV6-ADDR/LEN>	<IPV6-ADDR/LEN> — IP-адрес и префикс подсети, задается в виде X:X:X:X::X/EE, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128]. Дополнительные функции IPv6-адресации см. в разделе Настройка IPv6-адресации справочника команд CLI.
		scs(config-if-qinq)# ip address dhcp	Дополнительные функции при работе DHCP-клиента см. в разделе Управление DHCP-клиентом справочника команд CLI.
6	Установить интервал времени, в течение которого собирается статистика о нагрузке на саб-интерфейс (необязательно).	**scs(config-if-sub)# load-average <TIME>**	<TIME> — интервал в секундах, принимает значения [5..150].
7	Изменить размер MTU (MaximumTransmitionUnit). MTU более 1500 будет активно только если применена команда "system jumbo-frames" (необязательно).	**scs(config-if-sub)# mtu <MTU>**	<MTU> — значение MTU в байтах. Значение по умолчанию: 1500.
8	Включить запись статистики использования текущего интерфейса (необязательно).	**scs(config-if-sub)# history statistics**	

7.3.2 Пример настройки Q-in-Q интерфейса

Задача:

Настроить терминацию подсети 192.0.2.1/24 комбинации C-VLAN: 741, S-VLAN: 828 на физическом интерфейсе gigabitethernet 1/0/1.



Решение:

Создадим саб-интерфейс для S-VLAN: 828:

```
scs(config)# interface gigabitethernet 1/0/1.828
scs(config-if-sub)# exit
```

Создадим Q-in-Q-интерфейс для S-VLAN: 741 и настроим IP-адрес из необходимой подсети:

```
scs(config)# interface gigabitethernet 1/0/1.828.741
scs(config-if-qinq)# ip address 192.0.2.1/30
scs(config-if-qinq)# exit
```

Для просмотра настроенного адреса можно воспользоваться следующей командой:

```
scs-32# sh ip interfaces
IP address        Interface         Admin    Link    Type      Precedence    Description
--------------    -------------     -----    -----   -------   -----------   -------------
192.168.0.2/30    gi1/0/1.828.741    Up       Up      static    primary        --
```

7.4 Настройка USB-модемов

Использование USB-модемов позволяет организовать дополнительный канал связи для работы с оборудованием, подключенным к консольному серверу. При подключении USB-модемов возможно использовать USB-концентраторы. Одновременно в системе может быть сконфигурировано до 2 USB-модемов.

7.4.1 Алгоритм настройки USB-модемов

Шаг	Описание	Команда	Ключи
1	После подключения USB-модема дождаться, когда система обнаружит подключенное устройство.		
2	Определить, какой номер устройства назначен на подключенный USB-модем.	**scs# show cellular status modem**	В поле "USB port" будет указан идентификатор подключенного устройства.
3	Создать профиль настроек для USB-модема и перейти в режим конфигурирования профиля.	**scs(config)# cellular profile <ID>**	<ID> — идентификатор профиля настроек для USB-модема в системе [1..10].
4	Задать описание профиля настроек (необязательно).	**scs(config-cellular-profile)# description <DESCRIPTION>**	<DESCRIPTION> — описание профиля, задается строкой до 255 символов.
5	Задать точку доступа мобильной сети.	**scs(config-cellular-profile)# apn <NAME>**	<NAME> — точка доступа мобильной сети, задается строкой до 31 символа.
6	Задать имя пользователя мобильной сети (если мобильный оператор требует аутентификации по логину/паролю).	**scs(config-cellular-profile)# user <NAME>**	<NAME> — имя пользователя, задается строкой до 31 символа.
7	Установить пароль для пользователя мобильной сети (если мобильный оператор требует аутентификации по логину/паролю).	**scs(config-user)# password ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> — пароль в открытой форме, задается строкой [1 .. 64] символов, может включать символы [0-9a-fA-F]; <ENCRYPTED-TEXT> — пароль в зашифрованной форме, задаётся строкой [2..128] символов.
8	Активировать пользователя (если мобильный оператор требует аутентификации по логину/паролю).	**scs(config-user)# enable**	

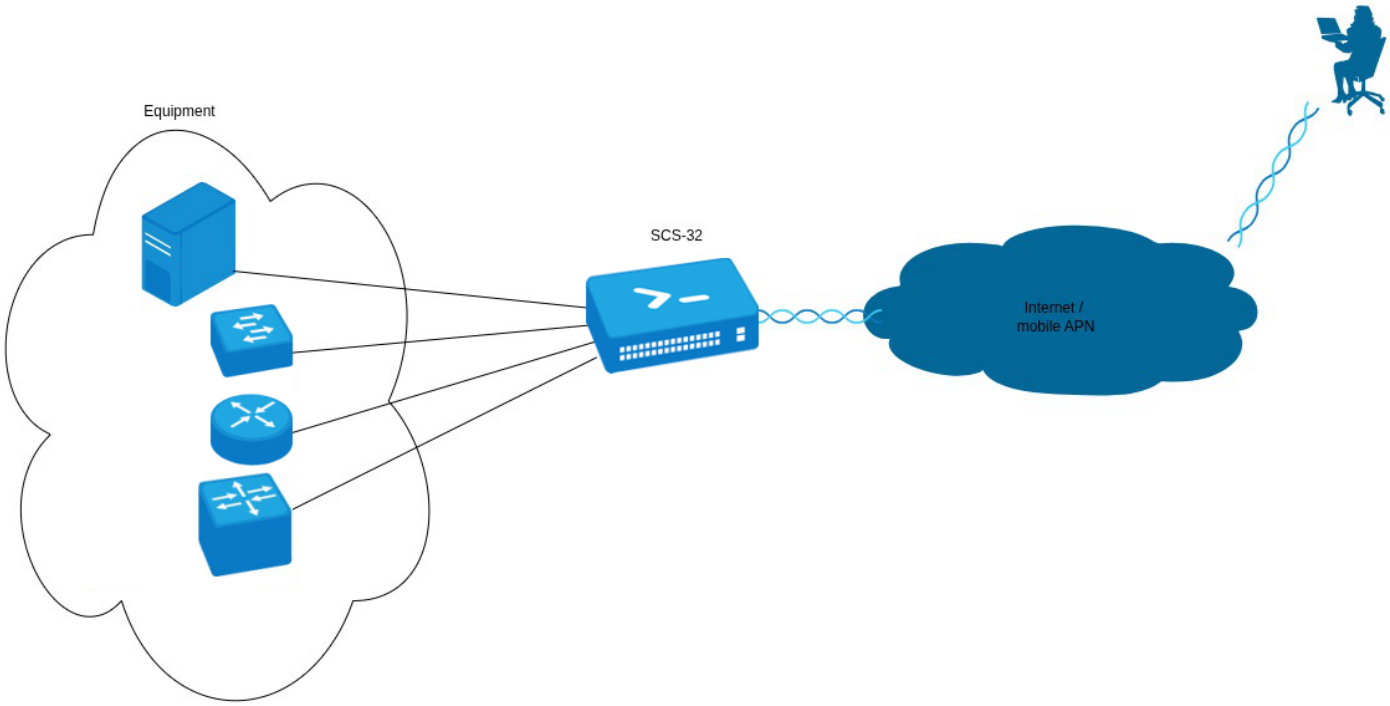
Шаг	Описание	Команда	Ключи
9	Установить номер дозвона для подключения к мобильной сети.	**scs(config-cellular-profile)# number <WORD>**	<WORD> — номер дозвона для подключения к мобильной сети, задаётся строкой до 15 символов.
10	Задать метод аутентификации пользователя в мобильной сети (необязательно).	**scs(config-cellular-profile)# allowed-auth <TYPE>**	<TYPE> — метод аутентификации пользователя в мобильной сети [none, PAP, CHAP, MSCHAP, MSCHAPv2, EAP]. Значение по умолчанию: PAP.
11	Ограничить возможность использования семейств IP-адресов в мобильной сети.	**scs(config-cellular-profile)# ip-version { ipv4 | ipv6 }**	ipv4 — семейство IPv4; ipv6 — семейство IPv6.
12	Создать USB-модем в конфигурации сервера и перейти в режим конфигурирования модема.	**scs(config)# cellular modem <ID>**	<ID> — идентификатор USB-модема в системе [1..10].
13	Установить режим работы беспроводного модема.	**scs(config)# mode <MODE>**	<MODE> — режим работы USB-модема [stick, hilink].
14	Задать описание модема (необязательно).	**scs(config-cellular-modem)# description <DESCRIPTION>**	<DESCRIPTION> — описание модема, задается строкой до 255 символов.
15	Задать идентификатор USB-модема, назначенного системой (определен в пункте 2).	**scs(config-cellular-modem)# device <WORD>**	<WORD> — идентификатор USB-порта подключенного модема, задаётся строкой до 12 символов.
16	Назначить ранее созданный профиль настроек для USB-модема.	**scs(config-cellular-modem)# profile <ID>**	<ID> — идентификатор профиля настроек для USB-модема в системе [1..10].
17	Задать код разблокировки SIM-карты (в случае необходимости).	**scs(config-cellular-modem)# pin <WORD>**	<WORD> — код разблокировки SIM-карты [4..8]. Возможно использование только цифр.
18	Разрешить использование того или иного режима работы сети USB-модема (необязательно).	**scs(config-cellular-modem)# allowed-mode <MODE>**	<MODE> — допустимый режим работы сети USB-модема [2g, 3g, 4g]. По умолчанию: разрешены все режимы, поддерживаемые модемом.

Шаг	Описание	Команда	Ключи
19	Задать размер максимального принимаемого пакета (необязательно).	**scs(config-cellular-modem)# mru { <MRU> }**	<MRU> — значение MRU, принимает значения в диапазоне [128..16383]. Значение по умолчанию: 1500.
20	Изменить максимальный размер обрабатываемых пакетов MTU (MaximumTransmitionUnit). MTU более 1500 будет активно, только если применена команда "system jumbo-frames" (необязательно).	**scs(config-cellular-modem)# mtu <MTU>**	<MTU> — значение MTU в байтах. Значение по умолчанию: 1500.
21	Задать предпочтительный режим работы USB-модема в мобильной сети (необязательно).	**scs(config-cellular-modem)# preferred-mode { <MODE> }**	<MODE> — предпочтительный режим работы USB-модема [2g, 3g, 4g].
22	Активировать USB-модем.	**scs(config-cellular-modem)# enable**	
Список поддерживаемых устройств, предоставленный производителем интегрированного драйвера, см. по ссылке.			

7.4.2 Пример настройки

Задача:

Настроить подключение к сети Интернет, используя USB-модем.



Решение:

Для примера разберём подключение к сотовому оператору МТС.

После подключения модема необходимо дождаться, когда система обнаружит устройство. Определим порт устройства, который был назначен на подключённый USB-модем:

```
scs# show cellular status modem
Number
device  USB port    Manufacturer    Model   Current state   Interface   Link    state
1       1-2         huawei          E3372   Disabled        --          Down
```

Создадим профиль настроек для USB-модема:

```
scs(config)# cellular profile 1
```

Зададим APN, который требует провайдер, или иной необходимый адрес. Ниже показан пример подключения к APN МТС:

```
scs(config-cellular-profile)# apn internet.mts.ru
```

При необходимости задаем имя пользователя, пароль, номер дозвона и метод аутентификации:

```
scs(config-cellular-profile)# user mts
scs(config-ppp-user)# password ascii-text mts
scs(config-cellular-profile)# number *99#
scs(config-cellular-profile)# allowed-auth PAP
```

Перейдём к конфигурированию USB-модема и зададим идентификатор, соответствующий порту устройства, который был определён в начале:

```
scs(config)# cellular modem 1
scs(config-cellular-modem)# device 1-2
```

Назначим соответствующий профиль настроек и активируем модем:

```
scs(config-cellular-modem)# profile 1
scs(config-cellular-modem)# enable
```

Настройка завершена.

7.5 Настройка AUX

Настройка AUX используется для указания параметров взаимодействия с внешними устройствами, подключенными через последовательные интерфейсы к SCS.

7.5.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования последовательного интерфейса.	**scs(config)# line aux [<ID>/ <SLOT>/<PORT>]**	<ID> — идентификатор устройства; <SLOT> — номер модуля в составе устройства или 0 при отсутствии деления устройства на модули; <PORT> — порядковый номер порта.

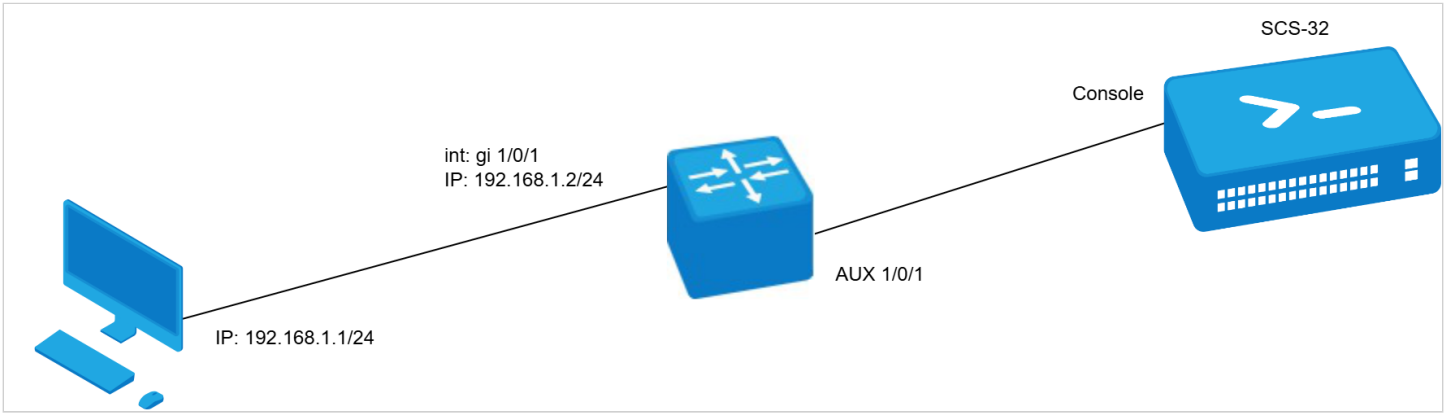
Шаг	Описание	Команда	Ключи
2	Установить необходимые параметры последовательного интерфейса для взаимодействия с подключенным устройством (необязательно). Данные параметры, как правило, указаны в инструкции подключаемого устройства. По умолчанию будут использованы стандартные значения.	**scs(config-line-aux) databits <BITS>** **scs(config-line-aux) flowcontrol <FMODE>** **scs(config-line-aux) parity <PMODE>** **scs(config-line-aux) speed <SPEED>** **scs(config-line-aux) stopbits <STOP-BITS>**	<BITS> — количество бит данных в посылке [7..8]; Значение по умолчанию: 8. <FMODE> — режим управления потоком. Принимает значения: • software — программное управление потоком; • hardware — аппаратное управление потоком; • disabled — управление потоком отключено; Значение по умолчанию: disabled. <PMODE> — режим установки бита четности. Принимает значения: • odd — проверка на нечетность; • even — проверка на четность; • none — бит четности не выставляется; Значение по умолчанию: none. <SPEED> — скорость работы последовательного интерфейса в бит/с. Принимает значения: 300; 1200; 2400; 4800; 9600; 19200; 38400; 57600; 115200; Значение по умолчанию: 115200. <STOP-BITS> — количество стоповых битов в посылке [1..2]; Значение по умолчанию: 1.
3	Задать описание последовательного интерфейса (необязательно).	**scs(config-line-aux)# description <DESCRIPTION>**	<DESCRIPTION> — описание интерфейса, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
4	При использовании подключаемого устройства в качестве модема перевести последовательный интерфейс в режим работы с модемом (необязательно). Примечание: невозможно использовать совместно с командой "transport telnet port".	**scs(config-line-aux)# modem inout**	
5	Установить протокол, по которому будет осуществляться подключение.	**scs(config-line-aux)# transport input <AUX_TRANSPORT>**	<AUX_TRANSPORT> - транспорт с помощью которого будет осуществляться подключение к AUX порту: • SSH • telnet
6	Установить TCP-порт для режима подключения reverse telnet. Примечание: невозможно использовать совместно с командой "modem inout".	**scs(config-line-aux)# transport telnet port <PORT>**	<PORT> — номер TCP-порта. Принимает значения [1..65535].

7.5.2 Примеры настроек

Задача 1:

Настроить подключение к консольному порту scs, используя консольный сервер SCS-32.



Решение:

Сконфигурировать SCS-32

Настроим параметры согласования:

```
scs(config)# line aux 1/0/1
scs(config-line-aux)# transport telnet port 3001
scs(config-line-aux)# exit
```

Сконфигурируем IP-адрес на SCS-32:

```
scs(config)# interface gigabitethernet 1/0/1
scs(config-if-gi)# ip address 192.168.1.2/24
scs(config-if-gi)# exit
```

Включим telnet-сервер:

```
scs-32(config)# ip telnet server
```

7.5.3 Схемы распайки переходников

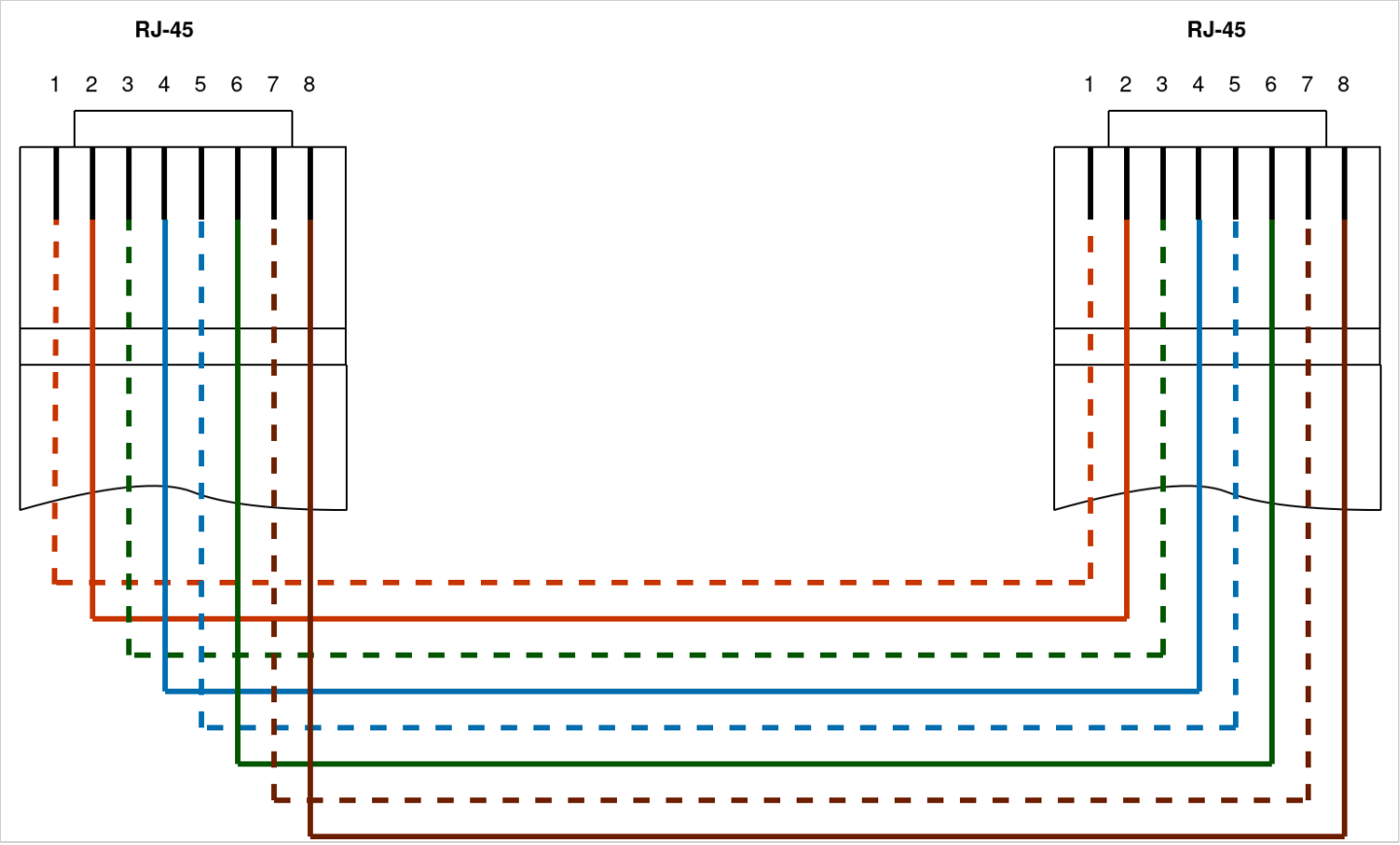
Порты RS-232 на устройстве SCS-32 распинованы по схеме DCE.

Распиновка RS-232 портов по схеме DCE	
Pin	**Сигнал**
1	RTS
2	DTR
3	TXD
4	GND (Земля)
5	GND (Земля)
6	RXD
7	DSR
8	CTS

Далее будут приведены схемы распайки переходников для подключения устройствам с распиновкой консольного порта по схемам DTE, т.к. на большинстве устройств используется распиновка типа DTE, в том числе на устройствах SCS, MES и т.д.

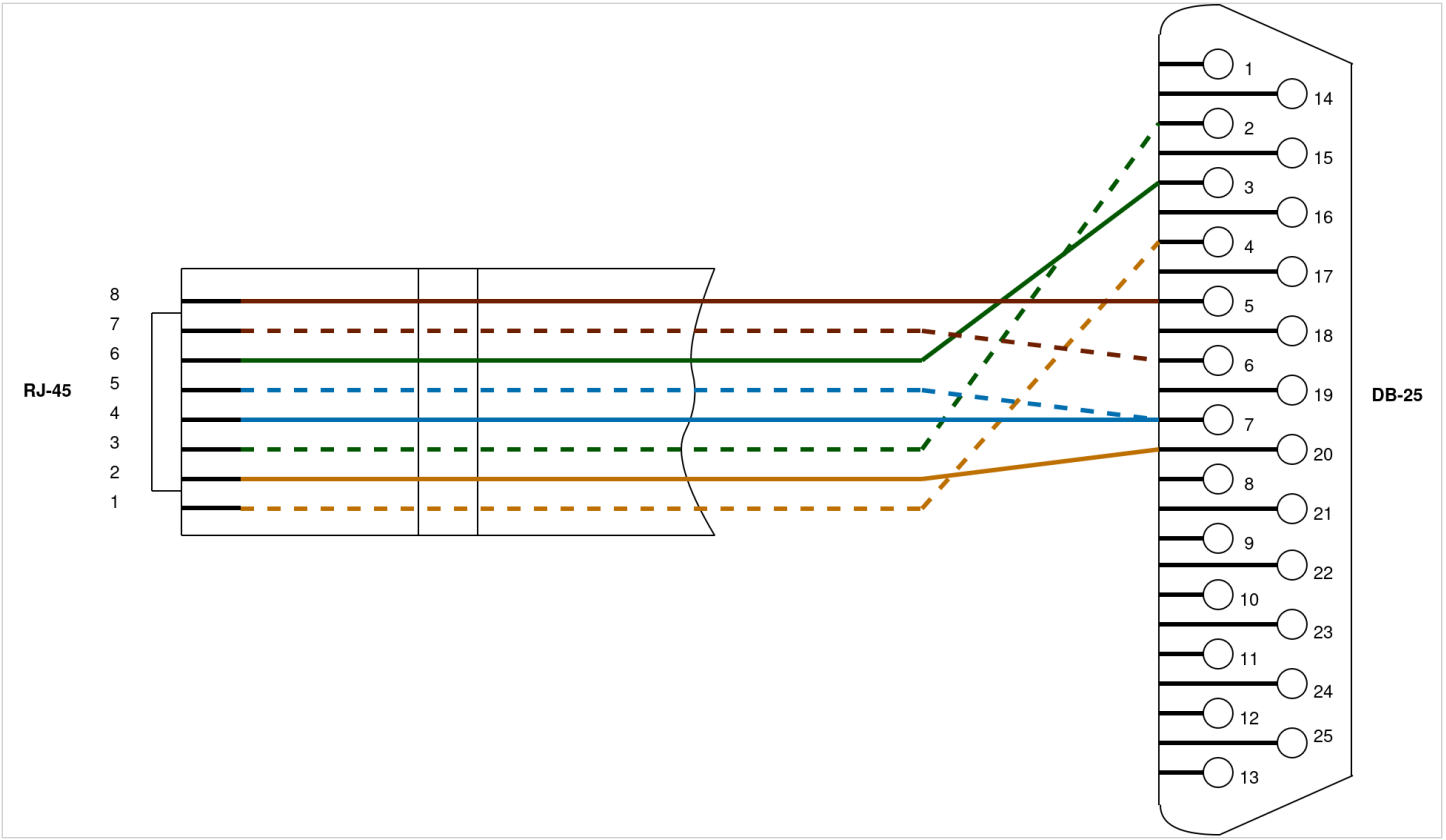
RJ-45 <--> RJ-45 pinout

Типовая распиновка прямого кабеля (RJ45 <-> RJ45)				
RJ45 Pin (8P8C)	**Цвет провода (T568B)**	**Сигнал**	**RJ45 Pin (8P8C)**	**Сигнал**
1	Бело-оранжевый	CTS	1	RTS
2	Оранжевый	DSR	2	DTR
3	Бело-зеленый	RXD	3	TXD
4	Синий	GND (Земля)	4	GND (Земля)
5	Бело-синий	GND (Земля)	5	GND (Земля)
6	Зеленый	TXD	6	RXD
7	Бело-коричневый	DTR	7	DSR
8	Коричневый	RTS	8	CTS



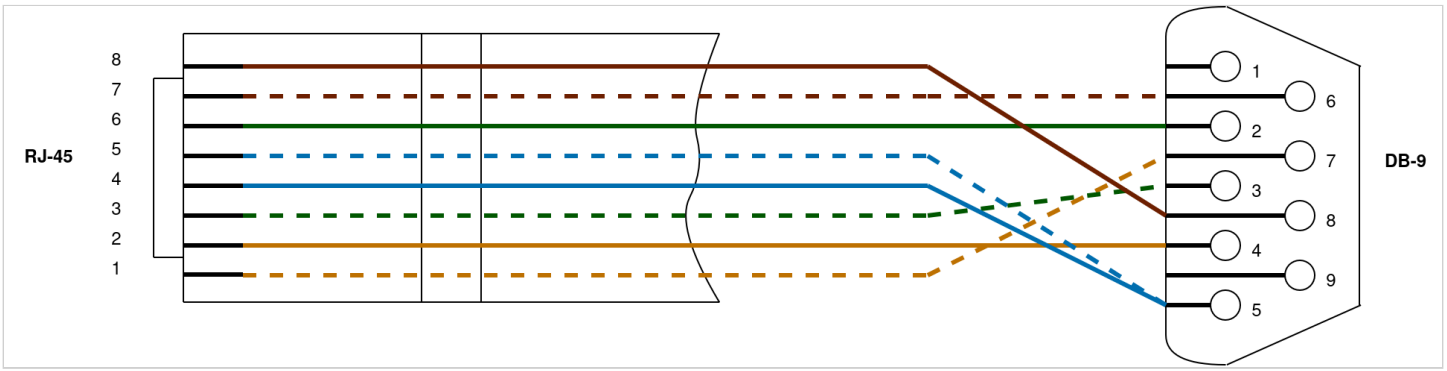
RJ-45 <--> DB-25 pinout

Типовая распиновка прямого кабеля (RJ45 <-> DB25 Male/Female)				
RJ45 Pin (8P8C)	**Цвет провода (T568B)**	**Сигнал**	**DB25 Pin (RS-232)**	**Сигнал**
1	Бело-оранжевый	CTS	4	RTS
2	Оранжевый	DSR	20	DTR
3	Бело-зеленый	RXD	2	TXD
4	Синий	GND (Земля)	7	GND (Земля)
5	Бело-синий	GND (Земля)	7	GND (Земля)
6	Зеленый	TXD	3	RXD
7	Бело-коричневый	DTR	6	DSR
8	Коричневый	RTS	5	CTS



RJ-45 <--> DB-9 pinout

Типовая распиновка прямого кабеля (RJ45 <-> DB9 Male/Female)				
RJ45 Pin (8P8C)	**Цвет провода (T568B)**	**Сигнал**	**DB9 Pin (RS-232)**	**Сигнал**
1	Бело-оранжевый	CTS	7	RTS
2	Оранжевый	DSR	4	DTR
3	Бело-зеленый	RXD	3	TXD
4	Синий	GND (Земля)	5	GND (Земля)
5	Бело-синий	GND (Земля)	5	GND (Земля)
6	Зеленый	TXD	2	RXD
7	Бело-коричневый	DTR	6	DSR
8	Коричневый	RTS	8	CTS



8 Управление функциями второго уровня (L2)

8.1 Настройка физического интерфейса

8.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Переход в режим конфигурирования функционала.	**scs(config)# interface gigabitethernet** **scs(config)# interface tengigabitethernet** **scs(config)# interface port-channel <ID>**	<ID> — порядковый номер группы агрегации каналов, принимает значения [1..2] .
2	Выключить интерфейс.	**scs(config-if-gi)# shutdown**	
3	Задать описание (необязательно).	**scs(config-if-gi)# description <text>**	<text> — до 255 символов.
4	Задать MTU (необязательно).	**scs(config-if-gi)# mtu <count>**	<count> — 552-10000. Значение по умолчанию: 1500.
5	Задать скорость и режим работы приемопередатчика (необязательно).	**scs(config-if-gi)# speed <SPEED> <DUPLEX>**	<SPEED> значение скорости: • 10M — значение скорости 10 Мбит/с; • 100M — значение скорости 100 Мбит/с; • 1000M — значение скорости 1000 Мбит/с; • 10G — значение скорости 10 Гбит/с; • auto — автоматический выбор режима (недоступно для 10G-интерфейсов). Значение по умолчанию: auto. <DUPLEX> — режим работы приемопередатчика, принимает значения: • full-duplex — дуплекс; • half-duplex — полудуплекс.
6	Задать MAC-адрес (необязательно).	**scs(config-if-gi)# mac-address <ADDR>**	<ADDR> — MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].

8.1.2 Пример настройки режима L2

Задача:

Настроить интерфейс gigabitethernet 1/0/1 на прохождение трафика следующим образом:

- Задать MAC-address 68:13:e2:7e:e4:9a;
- Перевести интерфейс в режим Routerport;
- Установить значение MTU=1400;
- Перевести интерфейс в режим работы Full-duplex на скорости 100M.

Решение:

Перейдём в режим конфигурирования интерфейса gigabitethernet 1/0/1 и зададим на нем MAC-address 68:13:e2:7e:e4:9a:

```
scs# configure
scs(config)# interface gigabitethernet 1/0/1
scs(config-if-gi)# mac-address 68:13:e2:7e:e4:9a
```

Установим значение MTU на интерфейсе, равное 1400:

```
scs(config-if-gi)# mtu 1400
```

Установим на интерфейсе скорость 100M и согласуем режим работы приемопередатчика в полном дуплексе. Выйдем из режима конфигурирования, применим и сохраним настройки:

```
scs(config-if-gi)# speed 100m full-duplex
scs(config-if-gi)# end
scs# commit
scs# confirm
```

Проверим настроенные параметры на интерфейсе:

```
scs# show interfaces switch-port status gigabitethernet 1/0/1
Interface       gigabitethernet 1/0/1
  Status:       Up
  Media:        copper
  Speed:        100M
  Duplex:       full
  Flow Control: Disabled
  MDI Mode:     MDI
```

8.2 Настройка LLDP

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.

8.2.1 Алгоритм настройки

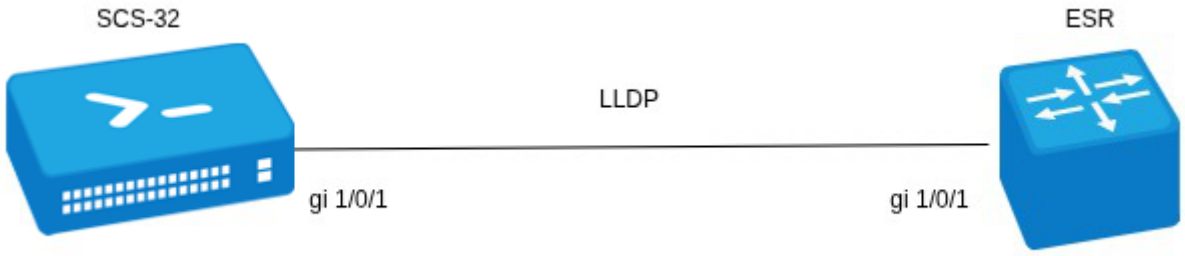
Шаг	Описание	Команда	Ключи
1	Активировать LLDP на консольном сервере.	**scs(config)# lldp enable**	
2	Включить прием и обработку LLDPDU на физическом интерфейсе.	**scs(config-if-gi)# lldp receive**	
3	Включить отправку LLDPDU на физическом интерфейсе.	**scs(config-if-gi)# lldp transmit**	
4	Установить период отправки LLDPDU (необязательно).	**scs(config)# lldp timer <SEC>**	<SEC> — период времени в секундах, принимает значение [1..32768]. Значение по умолчанию: 30.
5	Установить период, в течение которого консольный сервер хранит информацию, полученную по LLDP (необязательно).	**scs(config)# lldp hold-multiplier <SEC>**	<SEC> — период времени в секундах, принимает значение [1..10]. Значение по умолчанию: 4.
6	Установить IP-адрес, который будет передаваться в LLDP TLV в качестве management-address (необязательно).	**scs(config)# lldp management-address <ADDR>**	<ADDR> — IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. По умолчанию задается один из существующих.

Шаг	Описание	Команда	Ключи
7	Установить поле system-description, которое будет передаваться в LLDP TLV в качестве system-description (необязательно).	**scs(config)# lldp system-description <DESCRIPTION>**	<DESCRIPION> — описание системы, задается строкой до 255 символов. По умолчанию содержит информацию о модели и версии ПО сервера.
8	Установить поле system-name, которое будет передаваться в LLDP TLV в качестве system-name (необязательно).	**scs(config)# lldp system-name <NAME>**	<NAME> — имя системы, задается строкой до 255 символов. По умолчанию совпадает с заданным hostname.

8.2.2 Пример настройки

Задача:

Организовать обмен и обработку LLDPDU между маршрутизатором ESR и консольным сервером.



Решение:

1. Конфигурирование SCS.
   Включим LLDP глобально на устройстве:

```
scs(config)# lldp enable
```

   Включим прием и отправку LLDPDU на интерфейсе gi 1/0/1:

```
scs(config)# interface gigabitethernet 1/0/1
scs(config-if-gi)# lldp receive
scs(config-if-gi)# lldp transmit
```

2. Конфигурирование ESR.
   Включим LLDP глобально на маршрутизаторе:

```
esr(config)# lldp enable
```

   Включим прием и отправку LLDPDU на интерфейсе gi 1/0/1:

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# lldp receive
esr(config-if-gi)# lldp transmit
```

   Общую информацию по LLDP-соседям можно посмотреть командой:

```
scs# show lldp neighbors
```

   Подробную информацию по соседу конкретного интерфейса можно посмотреть командой:

```
scs# show lldp neighbors gigabitethernet 1/0/1
```

   Общую статистику по LLDP можно посмотреть командой:

```
scs# show lldp statistics
```

8.3 Настройка LACP

LACP — протокол для агрегирования каналов, позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала.

8.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Установить приоритет системы для протокола LACP.	**scs(config)# lacp system-priority <PRIORITY>**	**<PRIORITY>** — приоритет, указывается в диапазоне [1..65535]. Значение по умолчанию: 1.

Шаг	Описание	Команда	Ключи
2	Установить механизм балансировки нагрузки для групп агрегации каналов.	**scs(config)# port-channel load-balance { src-dst-mac-ip | src-dst-mac | src-dst-ip | src-dst-mac-ip-port }**	• **src - dst - mac - ip** — механизм балансировки основывается на MAC-адресе и IP-адресе отправителя и получателя; • **src - dst - mac** — механизм балансировки основывается на MAC-адресе отправителя и получателя; • **src - dst - ip** — механизм балансировки основывается на IP-адресе отправителя и получателя; • **src - dst - mac - ip - port** — механизм балансировки основывается на MAC-адресе, IP-адресе и порте отправителя и получателя.
3	Установить административный таймаут протокола LACP.	**scs(config)# lacp timeout {short | long }**	• **long** — длительное время таймаута; • **short** — короткое время таймаута. Значение по умолчанию: long.
4	Создать и перейти в режим конфигурирования агрегированного интерфейса.	**scs(config)# interface port-channel <CH>**	**<CH>** — порядковый номер группы агрегации каналов, принимает значения [1..2].
		scs(config)# interface port-channel <CH> .<S-VLAN>	**<CH>** — порядковый номер группы агрегации каналов, принимает значения [1..2]. **<S-VLAN>** — идентификатор создаваемого S-VLAN.
		scs(config)# interface port-channel <CH> .<S-VLAN>.<C-VLAN>	**<CH>** — порядковый номер группы агрегации каналов, принимает значения [1..2] . **<S-VLAN>** — идентификатор создаваемого S-VLAN. **<C-VLAN>** — идентификатор создаваемого C-VLAN.

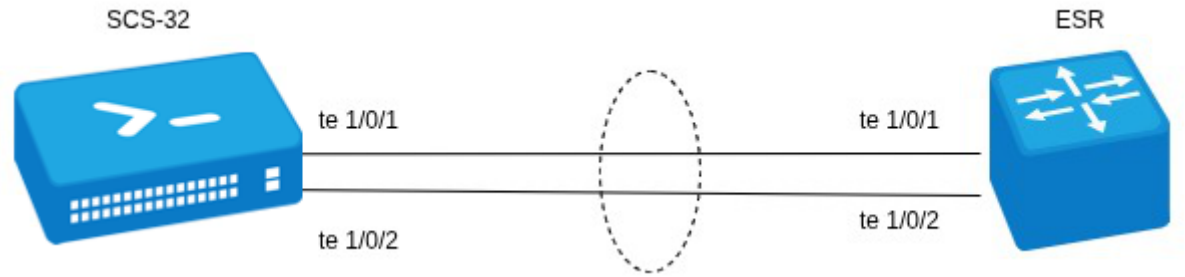
Шаг	Описание	Команда	Ключи
5	Задать скорость (необязательно).	**scs(config-if-port-channel)# speed <SPEED>**	**<SPEED>** — значение скорости: • 10M — значение скорости 10 Мбит/с; • 100M — значение скорости 100 Мбит/с; • 1000M — значение скорости 1000 Мбит/с; • 10G — значение скорости 10 Гбит/с; **Параметр наследуют все физические интерфейсы, принадлежащие данной группе агрегации каналов.** Значение по умолчанию: 1000M
6	Изменить размер MTU (MaximumTransmitionUnit). MTU более 1500 будет активно, только если применена команда system jumbo-frames (необязательно).	**scs(config-if-port-channel)# mtu <MTU>**	**<MTU>** — значение MTU в байтах. **Параметр наследуют все физические интерфейсы, принадлежащие данной группе агрегации каналов.** Значение по умолчанию: 1500.
7	Перейти в режим конфигурирования физического интерфейса.	**scs(config)# interface <IF-TYPE><IF-NUM>**	**<IF-TYPE>** — тип интерфейса (gigabitethernet или tengigabitethernet). **<IF-NUM>** — U/S/P — U-устройство (1), S — слот (0), P — порт.
8	Включить физический интерфейс в группу агрегации каналов с указанием режима формирования группы агрегации каналов.	**scs(config-if-gi)# channel-group <ID> mode <MODE>**	**<ID>** — порядковый номер группы агрегации каналов, принимает значения [1..2] . **<MODE>** — режим формирование группы агрегации каналов: • **auto** — добавить интерфейс в динамическую группу агрегации с поддержкой протокола LACP; • **on** — добавить интерфейс в статическую группу агрегации.

Шаг	Описание	Команда	Ключи
9	Установить LACP-приоритет интерфейса Ethernet.	**scs(config-if-gi)# lacp port-priority <PRIORITY>**	**<PRIORITY>** — приоритет, указывается в диапазоне [1..65535]. Значение по умолчанию: 1.
10	Установить интервал времени, в течение которого собирается статистика о нагрузке на интерфейс (необязательно).	**scs(config-if-gi)# load-average <TIME>**	**<TIME>** — интервал в секундах, принимает значения [5..150].
11	Включить запись статистики использования текущего интерфейса (необязательно).	**scs(config-if-gi)# history statistics**	
Также для агрегированного интерфейса возможно настроить: • IPv4/IPv6-адресацию (см. в разделах Настройка IP-адресации, Настройка IPv6-адресации и Управление DHCP-клиентом справочника команд CLI).			

8.3.2 Пример настройки

Задача:

Настроить агрегированный канал между консольным сервером и коммутатором с помощью tengigabitethernet-интерфейсов со значением MTU 9000.



Решение:

1. Предварительная конфигурация:
   Предварительно на устройствах необходимо включить поддержку Jumbo-фреймов. Для вступления изменений в силу требуется перезагрузка устройства:

   ```
   scs (config)# system jumbo-frames
   ```

2. Основной этап конфигурирования:
   Создадим интерфейс port-channel 1:

   ```
   scs(config)# interface port-channel 1
   ```

Зададим размер MTU = 9000:

```
scs(config-if-port-channel)# mtu 9000
```

Установим значение скорости физических интерфейсов, на которых будет работать агрегированный интерфейс:

```
scs(config-if-port-channel)# speed 10G
```

Включим интерфейсы в созданную группу агрегации каналов с ID 3 в режиме auto с поддержкой протокола LACP:

```
scs(config-if-te)# channel-group 1 mode auto
```

Дальнейшая конфигурация port-channel проводится как на обычном физическом интерфейсе.

9 Управление маршрутизацией

9.1 Конфигурирование статических маршрутов

Статическая маршрутизация — вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации консольного сервера без использования протоколов динамической маршрутизации.

9.1.1 Алгоритм настройки

Добавить статический маршрут возможно командой в режиме глобальной конфигурации:

```
scs(config)# ip route  <SUBNET>  <NEXTHOP> { [ resolve ] | interface <IF> | blackhole |
unreachable | prohibit }[ name <NAME>] | [ <METRIC> ]
no ip route  <SUBNET> [ <METRIC> ]
```

- <SUBNET> — адрес назначения, может быть задан в следующих видах:
  - AAA.BBB.CCC.DDD — IP-адрес хоста, где каждая часть принимает значения [0..255];
  - AAA.BBB.CCC.DDD/NN — IP-адрес подсети с маской в виде префикса, где AAA-DDD принимают значения [0..255] и NN принимает значения [1..32].
- <NEXTHOP> — IP-адрес шлюза, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255];
- resolve — при указании данного параметра IP-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;
- <IF> — имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов консольного сервера;
- blackhole — при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;
- unreachable — при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);
- prohibit — при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);
- <METRIC> — метрика маршрута, принимает значения [0..255];
- <NAME> — имя (описание) маршрута, текстовая переменная длиной до 31 символа;

Для добавления статического IPv6-маршрута к указанной подсети используется команда:

```
scs(config)# ipv6 route  <SUBNET>  <NEXTHOP> { [ resolve ] | interface <IF> | blackhole |
unreachable | prohibit } [ <METRIC> ] | [ name <NAME>]
no ipv6 route <SUBNET> [ <METRIC> ]
```

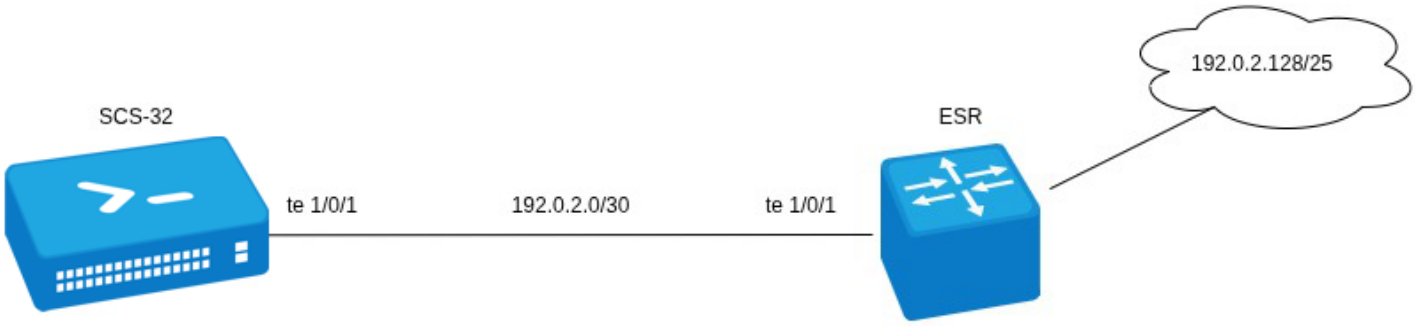
- <SUBNET> — адрес назначения, может быть задан в следующих видах:
  - X:X:X:X::X — IPv6-адрес хоста, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
  - X:X:X:X::X/EE — IPv6-адрес подсети с маской в виде префикса, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF] и EE принимает значения [1..128].

- <NEXTHOP> — IPv6-адрес шлюза, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
- resolve — при указании данного параметра IPv6-адрес шлюза будет рекурсивно вычислен через таблицу маршрутизации. Если при рекурсивном вычислении не удастся найти шлюз из напрямую подключенной подсети, то данный маршрут не будет установлен в систему;
- <IF> — имя IP-интерфейса, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов консольного сервера;
- blackhole — при указании команды пакеты до данной подсети будут удаляться устройством без отправки уведомлений отправителю;
- unreachable — при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Host unreachable, code 1);
- prohibit — при указании команды пакеты до данной подсети будут удаляться устройством, отправитель получит в ответ ICMP Destination unreachable (Communication administratively prohibited, code 13);
- [METRIC] — метрика маршрута, принимает значения [0..255];
- <NAME> — имя (описание) маршрута, текстовая переменная длиной до 31 символа.

9.1.2 Пример настройки

Задача:

Настроить статический маршрут до подсети 192.0.2.128/25, находящейся за маршрутизатором ESR.



Решение:

Для интерфейса te1/0/1 настроим адрес 192.0.2.1/30. Через данный интерфейс будет организовано подключение к маршрутизатору ESR.

```
scs(config)# interface te1/0/1
scs(config-if-te)# ip address 192.0.2.1/30
scs(config-if-te)# exit
```

Создадим маршрут для взаимодействия с сетью 192.0.2.128/25, используя в качестве шлюза устройство ESR (192.0.2.2):

```
scs(config)# ip route 192.0.2.128/25 192.0.2.2
```

Просмотреть таблицу маршрутизации можно командой:

```
scs# sh ip route
Codes: C - connected, S - static,
       D - DHCP derived, K - kernel route,
       * - FIB route
C     * 192.0.2.0/30    [0/0]             dev te1/0/1                      [direct 09:17:25]
S     * 192.0.2.128/25  [1/0]             via 192.0.2.2    on te1/0/1      [static 12:05:13]
```

Настройка завершена.

10 Управление безопасностью

10.1 Настройка AAA

AAA (Authentication, Authorization, Accounting) — используется для описания процесса предоставления доступа и контроля над ним.

- Authentication (аутентификация) — сопоставление персоны (запроса) существующей учетной записи в системе безопасности. Осуществляется по логину, паролю.
- Authorization (авторизация, проверка полномочий, проверка уровня доступа) — сопоставление учетной записи в системе и определенных полномочий.
- Accounting (учет) — слежение за подключением пользователя или внесенным им изменениям.

10.1.1 Алгоритм настройки локальной аутентификации

Шаг	Описание	Команда	Ключи
1	Задать список методов аутентификации по умолчанию (default)/с именем <NAME> и указать local.	**scs(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>]**	<NAME> — имя списка, задается строкой до 31 символа. Способы аутентификации: • local — аутентификация с помощью локальной базы пользователей; • tacacs — аутентификация по списку TACACS-серверов; • radius — аутентификация по списку RADIUS-серверов.

Шаг	Описание	Команда	Ключи
2	Задать список методов аутентификации повышения привилегий пользователей по умолчанию (default)/с именем <NAME> и указать enable.	**scs(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>]**	<NAME> — имя списка, задается строкой до 31 символа. Способы аутентификации: • local — аутентификация с помощью локальной базы пользователей; • tacacs — аутентификация по списку TACACS-серверов; • radius — аутентификация по списку RADIUS-серверов.
3	Указать способ перебора методов аутентификации в случае отказа (необязательно).	**scs(config)# aaa authentication mode <MODE>**	<MODE> — способы перебора методов: • chain — если сервер вернул FAIL, перейти к следующему в цепочке методу аутентификации; • break — если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
4	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (необязательно).	**scs(config)# aaa authentication attempts max-fail <COUNT> <TIME>**	<COUNT> — количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> — интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> — 5; <TIME> — 300.
5	Включить запрос на смену пароля по умолчанию для пользователя admin (необязательно).	**scs(config)# security passwords default-expired**	

Шаг	Описание	Команда	Ключи
6	Включить режим запрета на использование ранее установленных паролей локальных пользователей (необязательно).	**scs(config)# security passwords history <COUNT>**	<COUNT> — количество паролей, сохраняемых в памяти сервера. Принимает значение в диапазоне [1..15]. Значение по умолчанию: 0.
7	Установить время действия пароля локального пользователя (необязательно).	**scs(config)# security passwords lifetime <TIME>**	<TIME> — интервал времени действия пароля в днях. Принимает значение в диапазоне [1..365]. По умолчанию: время действия пароля локального пользователя не ограничено.
8	Установить ограничение на минимальную длину пароля локального пользователя и ENABLE-пароля (необязательно).	**scs(config)# security passwords min-length <NUM>**	<NUM> — минимальное количество символов в пароле. Принимает значение в диапазоне [8..128]. Значение по умолчанию: 0.
9	Установить ограничение на максимальную длину пароля локального пользователя и ENABLE-пароля (необязательно).	**scs(config)# security passwords max-length <NUM>**	<NUM> — максимальное количество символов в пароле. Принимает значение в диапазоне [8..128]. Значение по умолчанию: не ограничено.
10	Установить минимальное количество типов символов, которые должны присутствовать в пароле локального пользователя и ENABLE-пароле (необязательно).	**scs(config)# security passwords symbol-types <COUNT>**	<COUNT> — минимальное количество типов символов в пароле. Принимает значение в диапазоне [1..4]. Значение по умолчанию: 1.
11	Установить минимальное количество строчных букв в пароле локального пользователя и ENABLE-пароле (необязательно).	**scs(config)# security passwords lower-case <COUNT>**	<COUNT> — минимальное количество строчных букв в пароле локального пользователя и ENABLE-пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.
12	Установить минимальное количество прописных (заглавных) букв в пароле локального пользователя и ENABLE-пароле (необязательно).	**scs(config)# security passwords upper-case <COUNT>**	<COUNT> — минимальное количество прописных (заглавных) букв в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.

Шаг	Описание	Команда	Ключи
13	Установить минимальное количество цифр в пароле локального пользователя и ENABLE-пароле (необязательно).	**scs(config)# security passwords numeric-count <COUNT>**	<COUNT> — минимальное количество цифр в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.
14	Установить минимальное количество специальных символов в пароле локального пользователя и ENABLE-пароле (необязательно).	**scs(config)# security passwords special-case <COUNT>**	<COUNT> — минимальное количество специальных символов в пароле. Принимает значение в диапазоне [0..128]. Значение по умолчанию: 0.
15	Добавить пользователя в локальную базу и перейти в режим настройки параметров пользователя.	**scs(config)# username <NAME>**	<NAME> — имя пользователя, задается строкой до 31 символа.
16	Установить пароль пользователя.	**scs(config-user)# password { <CLEAR-TEXT> | encrypted <HASH_SHA512> }**	<CLEAR-TEXT> — пароль, задается строкой [8 .. 32] символов, принимает значения [0-9a-fA-F]; <HASH_SHA512> — хеш пароля по алгоритму sha512, задаётся строкой из 110 символов.
17	Установить уровень привилегий пользователя.	**scs(config-user)# privilege <PRIV>**	<PRIV> — необходимый уровень привилегий. Принимает значение [1..15].

Шаг	Описание	Команда	Ключи
18	Установить режим работы учетной записи пользователя (необязательно).	**scs(config-user)# mode <MODE>**	<MODE> — режим работы учетной записи пользователя. Может принимать значения: • cli — режим работы по умолчанию, пользователь получает доступ к интерфейсу командной строки, предназначенному для управления, просмотра состояния и мониторинга устройства; • techsupport — пользователь получает доступ к командной оболочке, в которой выполняется процедура отладки устройства совместно с специалистами технической поддержки; • sftp — пользователь используется для организации доступа к встроенному SFTP-серверу, возможность работы в какой-либо командой оболочке при этом у пользователя отсутствует.

Шаг	Описание	Команда	Ключи
19	Указать метод аутентификации SSH-сессий для пользователя (необязательно).	**scs(config-user)# ssh authentication method <METHOD>**	<METHOD> — метод аутентификации SSH-сессий. Может принимать значения: • password — аутентификация пользователя при открытии SSH-сессий может быть произведена только по паролю; • pubkey — аутентификация пользователя при открытии SSH-сессий может быть произведена только по публичному ключу; • both — аутентификация пользователя при открытии SSH-сессий может быть произведена как по паролю, так и по публичному ключу.
20	Указать имя файла публичного ключа, который будет использован при аутентификации SSH-сессии пользователя (необязательно).	**scs(config-user)# ssh pubkey <NAME>**	<NAME> — имя файла публичного ключа, расположенного в разделе crypto:public-key, задаётся строкой до 31 символа.
21	Отключить авторизацию для предустановленного пользователя admin (необязательно).	**scs(config)# no admin login enable**	
22	Перейти в режим конфигурирования соответствующего терминала.	**scs(config)# line <TYPE>**	<TYPE> — тип консоли: • console — локальная консоль; • telnet — удаленная консоль; • ssh — защищенная удаленная консоль; • консольный (последовательный) порт.
23	Активировать список аутентификации входа пользователей в систему.	**scs(config-line-console)# login authentication <NAME>**	<NAME> — имя списка, задается строкой до 31 символа. Создан на шаге 1.
24	Активировать список аутентификации повышения привилегий пользователей.	**scs(config-line-console)# enable authentication <NAME>**	<NAME> — имя списка, задается строкой до 31 символа. Создан на шаге 2.

Шаг	Описание	Команда	Ключи
25	Задать интервал, по истечении которого будет разрываться бездействующая сессия.	**scs(config-line-console)# exec-timeout <SEC>**	<SEC> — период времени в минутах, принимает значения [1..65535].

10.1.2 Алгоритм настройки AAA по протоколу RADIUS

Шаг	Описание	Команда	Ключи
1	Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов RADIUS-сервера (необязательно).	**scs(config)# radius-server dscp <DSCP>**	<DSCP> — значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
2	Задать глобальное значение количества перезапросов к последнему активному RADIUS-серверу (необязательно).	**scs(config)# radius-server retransmit <COUNT>**	<COUNT> — количество перезапросов к RADIUS-серверу, принимает значения [1..10]. Значение по умолчанию: 1.
3	Задать глобальное значение интервала, по истечении которого консольный сервер считает, что RADIUS-сервер недоступен (необязательно).	**scs(config)# radius-server timeout <SEC>**	<SEC> — период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.
4	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**scs(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> }**	<IP-ADDR> — IP-адрес RADIUS-сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> — IPv6-адрес RADIUS-сервера, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]
5	Задать описание конфигурируемого RADIUS-сервера (необязательно).	**scs(config-radius-server)# description <description>**	<description> — описание RADIUS-сервера, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
6	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и времени блокировки (необязательно).	**scs(config-radius-server)# aaa authentication attempts max-fail <COUNT> <TIME>**	<COUNT> — количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> — интервал времени в секундах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> — 5; <TIME> — 300.
7	Задать пароль для аутентификации на удаленном RADIUS-сервере.	**scs(config-radius-server)# key ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }**	<TEXT> — строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> — зашифрованный пароль, размером [8..16] байт, задается строкой [16..32] символов.
8	Задать приоритет использования удаленного RADIUS-сервера (необязательно).	**scs(config-radius-server)# priority <PRIORITY>**	<PRIORITY> — приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
9	Задать интервал, по истечении которого консольный сервер считает, что данный RADIUS-сервер недоступен (необязательно).	**scs(config-radius-server)# timeout <SEC>**	<SEC> — период времени в секундах, принимает значения [1..30]. Значение по умолчанию: используется значение глобального таймера.
10	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых RADIUS-пакетах.	**scs(config-radius-server)# source-address { <ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> — IP-адрес источника, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> — список адресов, которые будут использоваться в качестве source address.

Шаг	Описание	Команда	Ключи
11	Задать интерфейс консольного сервера, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых RADIUS-пакетах.	**scs(config-radius-server)# source-interface <IF>**	<IF> — имя интерфейса устройства, задается в виде, описанном в разделе Типы и порядок именования интерфейсов консольного сервера.
12	Задать список методов аутентификации по умолчанию (default)/с именем <NAME> и указать radius.	**scs(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>]**	<NAME> — имя списка, задается строкой до 31 символа. Способы аутентификации: • local — аутентификация с помощью локальной базы пользователей; • tacacs — аутентификация по списку TACACS-серверов; • radius — аутентификация по списку RADIUS-серверов.
13	Задать список методов аутентификации повышения привилегий пользователей по умолчанию (default)/с именем <NAME> и указать radius.	**scs(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>]**	<NAME> — имя списка строка до 31 символа; • default — имя списка по умолчанию. <METHOD> — способы аутентификации: • enable — аутентификация с помощью enable-паролей; • tacacs — аутентификация по протоколу TACACS; • radius — аутентификация по протоколу RADIUS.

Шаг	Описание	Команда	Ключи
14	Указать способ перебора методов аутентификации в случае отказа (необязательно).	**scs(config)# aaa authentication mode <MODE>**	<MODE> — способы перебора методов: • chain — если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break — если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
15	Сконфигурировать RADIUS в списке способов учета сессий пользователей (необязательно).	**scs(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]**	<METHOD> — способы учета: • tacacs — учет сессий по протоколу TACACS; • radius — учет сессий по протоколу RADIUS.
16	Перейти в режим конфигурирования соответствующего терминала.	**scs(config)# line <TYPE>**	<TYPE> — тип консоли: • console — локальная консоль; • telnet — удаленная консоль; • ssh — защищенная удаленная консоль; • aux — консольный (последовательный) порт.
			<NAME> — имя списка, задается строкой до 31 символа. Создан на шаге 12.
18	Активировать список аутентификации повышения привилегий пользователей.	**scs(config-line-console)# enable authentication <NAME>**	<NAME> — имя списка, задается строкой до 31 символа. Создан на шаге 13.

10.1.3 Алгоритм настройки AAA по протоколу TACACS

Шаг	Описание	Команда	Ключи
1	Задать глобальное значение кода DSCP для использования в IP-заголовках исходящих пакетов TACACS-сервера (необязательно).	**scs(config)# tacacs-server dscp <DSCP>**	<DSCP> — значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
2	Задать глобальное значение интервала, по истечении которого консольный сервер считает, что TACACS-сервер недоступен (необязательно).	**scs(config)# tacacs-server timeout <SEC>**	<SEC> — период времени в секундах, принимает значения [1..30]. Значение по умолчанию: 3 секунды.
3	Добавить TACACS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**scs(config)# tacacs -server host { <IP-ADDR> | <IPV6-ADDR> }**	<IP-ADDR> — IP-адрес TACACS-сервера, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] <IPV6-ADDR> — IPv6-адрес TACACS-сервера, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]
4	Задать описание конфигурируемого TACACS-сервера (необязательно).	**scs(config-tacacs-server)# description <description>**	<description> — описание TACACS-сервера, задается строкой до 255 символов.
5	Указать количество неудачных попыток аутентификации для блокировки логина пользователя и время блокировки (необязательно)	**scs(config-tacacs-server)# aaa authentication attempts max-fail <COUNT> <TIME>**	<COUNT> — количество неудачных попыток аутентификации, после которых произойдет блокировка пользователя, принимает значения [1..65535]; <TIME> — интервал времени в минутах, на который будет заблокирован пользователь, принимает значения [1..65535]. Значение по умолчанию: <COUNT> — 5; <TIME> — 300.

Шаг	Описание	Команда	Ключи
6	Задать пароль для аутентификации на удаленном TACACS-сервере	**scs(config-tacacs-server)# key ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }**	<TEXT> — строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> — зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.
7	Задать номер порта для обмена данными с удаленным TACACS-сервером (необязательно).	**scs(config-tacacs-server)# port <PORT>**	<PORT> — номер TCP-порта для обмена данными с удаленным сервером, принимает значения [1..65535]. Значение по умолчанию: 49 для TACACS-сервера.
8	Задать приоритет использования удаленного TACACS сервера (необязательно).	**scs(config-tacacs-server)# priority <PRIORITY>**	<PRIORITY> — приоритет использования удаленного сервера, принимает значения [1..65535]. Чем ниже значение, тем приоритетнее сервер. Значение по умолчанию: 1.
9	Задать IPv4/IPv6-адрес, который будет использоваться в качестве IP/IPv6-адреса источника в отправляемых TACACS-пакетах.	**scs(config-tacacs-server)# source-address { <ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> — IP-адрес источника, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <NETWORK_OBJ_GROUP_NAME> — список адресов, которые будут использоваться в качестве source address.
10	Задать интерфейс консольного сервера, IPv4/IPv6-адрес которого будет использоваться в качестве IPv4/IPv6-адреса источника в отправляемых TACACS-пакетах.	**scs(config-tacacs-server)# source-interface <IF>**	<IF> — имя интерфейса устройства, задаётся в виде, описанном в разделе Типы и порядок именования интерфейсов консольного сервера.

Шаг	Описание	Команда	Ключи
11	Задать список методов аутентификации по умолчанию (default)/с именем <NAME> и указать tacacs.	**scs(config)# aaa authentication login { default | <NAME> } <METHOD 1> [<METHOD 2>] [<METHOD 3>]**	<NAME> — имя списка, задается строкой до 31 символа. Способы аутентификации: • local — аутентификация с помощью локальной базы пользователей; • tacacs — аутентификация по списку TACACS-серверов; • radius — аутентификация по списку RADIUS-серверов.
12	Задать список методов аутентификации повышения привилегий пользователей по умолчанию (default)/с именем <NAME> и указать tacacs.	**scs(config)# aaa authentication enable <NAME><METHOD 1> [<METHOD 2>] [<METHOD 3>]**	<NAME> — имя списка строка до 31 символа; • default — имя списка по умолчанию. <METHOD> — способы аутентификации: • enable — аутентификация с помощью enable-паролей; • tacacs — аутентификация по протоколу TACACS; • radius — аутентификация по протоколу RADIUS.
13	Задать список методов авторизации команд, вводимых пользователем в систему по умолчанию (default)/с именем <NAME> и указать tacacs.	**scs(config)# aaa authorization commands { default | <NAME> } <METHOD 1>[<METHOD 2>]**	<NAME> — имя списка, задается строкой до 31 символа. Способы аутентификации: local — авторизация с помощью локальной базы пользователей; tacacs — авторизация по списку TACACS-серверов.

Шаг	Описание	Команда	Ключи
14	Указать способ перебора методов аутентификации в случае отказа (необязательно).	**scs(config)# aaa authentication mode <MODE>**	<MODE> — способы перебора методов: • chain — если сервер вернул FAIL, переход к следующему в цепочке методу аутентификации; • break — если сервер вернул FAIL, прекратить попытки аутентификации. Если сервер недоступен, продолжить попытки аутентификации следующими в цепочке методами. Значение по умолчанию: chain.
15	Сконфигурировать список способов учета команд, введенных в CLI (необязательно).	**scs(config)# aaa accounting commands stop-only <METHOD>**	<METHOD> — способы учета: tacacs — учет введенных команд по протоколу TACACS.
16	Сконфигурировать tacacs в списке способов учета сессий пользователей (необязательно).	**scs(config)# aaa accounting login start-stop <METHOD 1> [<METHOD 2>]**	<METHOD> — способы учета: • tacacs — учет сессий по протоколу TACACS; • radius — учет сессий по протоколу RADIUS.
17	Перейти в режим конфигурирования соответствующего терминала.	**scs(config)# line <TYPE>**	<TYPE> — тип консоли: • console — локальная консоль; • telnet — удаленная консоль; • ssh — защищенная удаленная консоль; • aux — консольный (последовательный) порт.
18	Активировать список аутентификации входа пользователей в систему.	**scs(config-line-console)# login authentication <NAME>**	<NAME> — имя списка, задается строкой до 31 символа. Создан на шаге 11.
19	Активировать список аутентификации повышения привилегий пользователей.	**scs(config-line-console)# enable authentication <NAME>**	<NAME> — имя списка, задается строкой до 31 символа. Создан на шаге 12.
20	Активировать список авторизации команд вводимых пользователем в систему.	**scs(config-line-console)# commands authorization <NAME>**	<NAME> — имя списка, задается строкой до 31 символа. Создан на шаге 13.

10.1.4 Пример настройки аутентификации по Telnet через RADIUS-сервер

Задача:

Настроить аутентификацию пользователей, подключающихся по Telnet, через RADIUS (192.0.2.12/24).

Решение:

Настроим подключение к RADIUS-серверу и укажем ключ (password):

```
scs# configure
scs(config)# radius-server host 192.0.2.12
scs(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
scs(config-radius-server)# exit
```

Создадим профиль аутентификации:

```
scs(config)# aaa authentication login log radius
```

Укажем режим аутентификации, используемый при подключении по Telnet-протоколу:

```
scs(config)# line telnet
scs(config-line-telnet)# login authentication log
scs(config-line-telnet)# exit
scs(config)# exit
```

Просмотреть информацию по настройкам подключения к RADIUS-серверу можно командой:

```
scs# show aaa radius-servers
```

Посмотреть профили аутентификации можно командой:

```
scs# show aaa authentication
```

10.2 Настройка привилегий команд

Настройка привилегий команд является гибким инструментом, который позволяет назначить набору команд минимально необходимый уровень пользовательских привилегий (1-15). В дальнейшем при создании пользователя можно задать уровень привилегий, определяя доступный ему набор команд.

- *1-9 уровни* — позволяют использовать все команды мониторинга (show …);
- *10-14 уровни* — позволяют использовать все команды кроме команд перезагрузки устройства, управления пользователями и ряда других;
- *15 уровень* — позволяет использовать все команды.

10.2.1 Алгоритм настройки

Для изменения минимального уровня привилегий необходимого для выполнения команды CLI используется команда:

```
scs(config)# privilege <COMMAND-MODE> level <PRIV><COMMAND>
```

<COMMAND-MODE> — командный режим;

<PRIV> — необходимый уровень привилегий поддерева команд, принимает значение [1..15];

<COMMAND> — поддерево команд, задается строкой до 255 символов.

10.2.2 Пример настройки привилегий команд

Задача:

Перевести все команды просмотра информации об интерфейсах на уровень привилегий 10, кроме команды «show interfaces port-channel». Команду «show interfaces bridges» перевести на уровень привилегий 3.

Решение:

В режиме конфигурирования определим команды, разрешенные на использование с уровнем привилегий 10 и уровнем привилегий 3:

```
scs(config)# privilege root level 3 "show interfaces port-channel"
scs(config)# privilege root level 10 "show interfaces"
```

10.3 Настройка списков доступа (IP ACL)

IP Access Control List или IP ACL — список контроля доступа, содержит правила, определяющие прохождение трафика через интерфейс.

10.3.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать список контроля доступа и перейти в режим его конфигурирования.	**scs(config)# ip access-list extended <NAME>**	<NAME> — имя создаваемого списка контроля доступа, задается строкой до 31 символа.
2	Указать описание конфигурируемого списка контроля доступа (необязательно).	**scs(config-acl-ip)# description <DESCRIPTION>**	<DESCRIPTION> — описание списка контроля доступа, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
3	Создать правило и перейти в режим его конфигурирования. Правила обрабатываются сервером в порядке возрастания их номеров.	**scs(config-acl-ip)# rule <ORDER>**	<ORDER> — номер правила, принимает значения [1...4094].
4	Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям.	**scs(config-acl-ip-rule)# action <ACT>**	<ACT> — назначаемое действие: • permit — прохождение трафика разрешается; • deny — прохождение трафика запрещается.
5	Установить имя/номер протокола, для которого должно срабатывать правило (необязательно).	**scs(config-acl-ip-rule)# match protocol <TYPE>**	<TYPE> — тип протокола, принимает значения: esp, icmp, icmp6, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rsvp, l2tp, gre. При указании значения «any» правило будет срабатывать для любых протоколов.
		scs(config-acl-ip-rule)# match protocol-id <ID>	<ID> — идентификационный номер IP-протокола, принимает значения [0x00-0xFF].
6	Установить IP-адреса отправителя, для которых должно срабатывать правило (необязательно).	**scs(config-acl-ip-rule)# match source-address { <ADDR> <MASK> | any }**	<ADDR> — IP-адрес отправителя, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <MASK> — маска IP-адреса, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. Биты маски, установленные в 0, задают биты IP-адреса, исключаемые из сравнения при поиске. При указании значения «any» правило будет срабатывать для любого IP-адреса отправителя/получателя.
7	Установить IP-адреса получателя, для которых должно срабатывать правило (необязательно).	**scs(config-acl-ip-rule)# match destination-address { <ADDR> <MASK> | any }**	

Шаг	Описание	Команда	Ключи
8	Установить MAC-адреса отправителя, для которых должно срабатывать правило (необязательно).	**scs(config-acl-ip-rule)# match source-mac <ADDR><WILDCARD>**	<ADDR> — MAC-адрес отправителя, задается в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]; <WILDCARD> — маска MAC-адреса, задается в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске.
9	Установить MAC-адреса получателя, для которых должно срабатывать правило (необязательно).	**scs(config-acl-ip-rule)# match destination-mac <ADDR><WILDCARD>**	
10	Установить номер TCP/UDP-порта отправителя, для которого должно срабатывать правило (если указан протокол).	**scs(config-acl-ip-rule)# match source-port <TYPE> {<FROM-PORT> - <TO-PORT> | <PORT>}**	<TYPE> — тип аргумента, устанавливаемый в качестве порта: • **port-range** — указать диапазон портов; • **any** — установить в качестве порта любой порт. <FROM-PORT> — начальный порт диапазона; <TO-PORT> — конечный порт диапазона; <PORT> — указание единичного порта.
11	Установить номер TCP/UDP-порта получателя, для которого должно срабатывать правило (если указан протокол).	**scs(config-acl-ip-rule)# match destination-port <TYPE> {<FROM-PORT> - <TO-PORT> | <PORT>}**	
12	Установить значение 802.1p приоритета, для которого должно срабатывать правило (необязательно).	**scs(config-acl-ip-rule)# match cos <COS>**	<COS> — значение 802.1p приоритета, принимает значения [0..7].
13	Установить значение кода DSCP, для которого должно срабатывать правило (необязательно). Невозможно использовать совместно с IP Precedence.	**scs(config-acl-ip-rule)# match dscp <DSCP>**	<DSCP> — значение кода DSCP, принимает значения [0..63].
14	Установить значение кода IP Precedence, для которого должно срабатывать правило (необязательно). Невозможно использовать совместно с DSCP.	**scs(config-acl-ip-rule)# match ip-precedence <IPP>**	<IPP> — значение кода IP Precedence, принимает значения [0..7].

Шаг	Описание	Команда	Ключи
15	Установить значение идентификационного номера VLAN, для которого должно срабатывать правило (необязательно).	**scs(config-acl-ip-rule)# match vlan <VID>**	<VID> — идентификационный номер VLAN, принимает значения [1..4094].
16	Активировать правило.	**scs(config-acl-ip-rule)# enable**	
17	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика.	**scs(config-if-gi)# service-acl ip input <NAME>**	<NAME> — имя списка контроля доступа, задается строкой до 31 символа.
18	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации исходящего трафика.	**scs(config-if-gi)# service-acl ip output <NAME>**	<NAME> — имя списка контроля доступа, задается строкой до 31 символа.

10.3.2 Пример настройки списка доступа

Задача:

Разрешить прохождения трафика только из подсети 192.168.20.0/24.

Решение:

Настроим список доступа для фильтрации по подсетям:

```
scs# configure
scs(config)# ip access-list extended white
scs(config-acl-ip)# rule 1
scs(config-acl-ip-rule)# action permit
scs(config-acl-ip-rule)# match source-address 192.168.20.0 255.255.255.0
scs(config-acl-ip-rule)# enable
scs(config-acl-ip-rule)# exit
scs(config-acl-ip)# exit
```

Применим список доступа на интерфейс Gi1/0/1 для входящего трафика:

```
scs(config)# interface gigabitethernet 1/0/1
scs(config-if-gi)# service-acl ip input white
```

Просмотреть детальную информацию о списке доступа возможно через команду:

```
scs# show ip access-list white
```

10.4 Настройка списков доступа (MAC ACL)

MAC Access Control List или MAC ACL — список контроля доступа, содержит правила на основе L2 заголовка, определяющие прохождение трафика через интерфейс.

10.4.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Создать список контроля доступа и перейти в режим его конфигурирования.	**scs(config)# mac access-list extended <NAME>**	<NAME> — имя создаваемого списка контроля доступа, задаётся строкой до 31 символа.
2	Указать описание конфигурируемого списка контроля доступа (необязательно).	**scs(config-acl-mac)# description <DESCRIPTION>**	<DESCRIPTION> — описание списка контроля доступа, задаётся строкой до 255 символов.
3	Создать правило и перейти в режим его конфигурирования. Правила обрабатываются сервером в порядке возрастания их номеров.	**scs(config-acl-mac)# rule <ORDER>**	<ORDER> — номер правила, принимает значения [1...4094].
4	Указать действие, которое должно быть применено для трафика, удовлетворяющего заданным критериям.	**scs(config-acl-mac-rule)# action <ACT>**	<ACT> — назначаемое действие: • permit — прохождение трафика разрешается; • deny — прохождение трафика запрещается.
5	Установить имя/номер протокола, для которого должно срабатывать правило (необязательно).	**scs(config-acl-mac-rule)# match protocol <TYPE>**	<TYPE> — тип протокола, принимает значения: arp, ip, ipv6, lacp, lldp, cdp, stp, vtp. При указании значения «any» правило будет срабатывать для любых протоколов.
		scs(config-acl-mac-rule)# match ethertype <ID>	<ID> — идентификационный номер инкапсулированного протокола, принимает значения [0x0600-0xFFFF].

Шаг	Описание	Команда	Ключи
8	Установить MAC-адреса отправителя, для которых должно срабатывать правило (необязательно).	**scs(config-acl-mac-rule)# match source-mac <ADDR><WILDCARD>**	<ADDR> — MAC-адрес отправителя, задается в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]; <WILDCARD> — маска MAC-адреса, задается в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF]. Биты маски, установленные в 0, задают биты MAC-адреса, исключаемые из сравнения при поиске.
9	Установить MAC-адреса получателя, для которых должно срабатывать правило (необязательно).	**scs(config-acl-mac-rule)# match destination-mac <ADDR><WILDCARD>**	
12	Установить значение 802.1p приоритета, для которого должно срабатывать правило (необязательно).	**scs(config-acl-mac-rule)# match cos <COS>**	<COS> — значение 802.1p приоритета, принимает значения [0..7].
15	Установить значение идентификационного номера VLAN, для которого должно срабатывать правило (необязательно).	**scs(config-acl-mac-rule)# match vlan <VID>**	<VID> — идентификационный номер VLAN, принимает значения [1..4094].
16	Активировать правило.	**scs(config-acl-mac-rule)# enable**	
17	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации входящего трафика.	**scs(config-if-gi)# service-acl mac input <NAME>**	<NAME> — имя списка контроля доступа, задается строкой до 31 символа.
18	Указать список контроля доступа к конфигурируемому интерфейсу для фильтрации исходящего трафика.	**scs(config-if-gi)# service-acl mac output <NAME>**	<NAME> — имя списка контроля доступа, задается строкой до 31 символа.

10.4.2 Пример настройки списка доступа

Задача:

Запретить сетевую активность с клиентом, имеющим mac-address 18:d6:c7:01:31:4d.

Решение:

Настроим список доступа для фильтрации по заданному критерию:

```
scs# configure
scs(config)# mac access-list extended white
scs(config-acl-mac)# rule 1
scs(config-acl-mac-rule)# action deny
scs(config-acl-mac-rule)# match source-mac 18:d6:c7:01:31:4d
scs(config-acl-mac-rule)# enable
scs(config-acl-mac-rule)# exit
scs(config-acl)# exit
```

Применим список доступа на интерфейс Gi1/0/1 для входящего трафика:

```
scs(config)# interface gigabitethernet 1/0/1
scs(config-if-gi)# service-acl mac input white
```

Просмотреть детальную информацию о списке доступа возможно через команду:

```
scs# show mac access-list white
```

11 Управление сервисами

11.1 Настройка NTP

NTP (англ. *Network Time Protocol* — протокол сетевого времени) — сетевой протокол для синхронизации внутренних часов оборудования с использованием IP-сетей, использует для своей работы протокол UDP, учитывает время передачи и использует алгоритмы для достижения высокой точности синхронизации времени.

11.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить NTP.	**scs(config)# ntp enable**	
2	Задать IP-адрес NTP-сервера, либо участника NTP-синхронизации.	**scs(config)# ntp { pool | server | peer } { <IPV4> | IPV6}**	<IPV4> — IP-адрес назначения (шлюз), задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <IPV6> — IP-адрес назначения (шлюз), задается в виде X:X:X:X::X, где каждая часть X принимает значения в шестнадцатеричном формате [0..FFFF].
3	Включить отправку нескольких пакетов вместо одного при установке соединения.	**scs(config-ntp)# burst**	
4	Включить отправку нескольких пакетов вместо одного в случае разрыва соединения.	**scs(config-ntp)# iburst**	
6	Установить максимальное значение интервала времени между отправкой сообщений NTP-серверу (не обязательно).	**scs(config-ntp)# maxpoll <INTERVAL>**	<INTERVAL> — максимальное значение интервала опроса. Параметр команды используется как показатель степени двойки при вычислении длительности интервала в секундах, вычисляется путем возведения двойки в степень, заданную параметром команды, принимает значение [10..17]. Значение по умолчанию: 10 (210= 1024 секунды или 17 минут 4 секунды).

Шаг	Описание	Команда	Ключи
7	Установить минимальное значение интервала времени между отправкой сообщений NTP-серверу (не обязательно).	**scs(config-ntp)# minpoll <INTERVAL>**	<INTERVAL> — минимальное значение интервала опроса в секундах вычисляется путем возведения двойки в степень, заданную параметром команды, принимает значение [4..6]. Значение по умолчанию: 6 (26= 64 секунды или 1 минута 4 секунды).
8	Отметить данный NTP-сервер как предпочтительный (не обязательно).	**scs(config-ntp)# prefer**	
9	Определить список доверенных IP-адресов, с которыми может происходить обмен ntp-пакетами (не обязательно).	**scs(config)# ntp access-addresses <NAME>**	<NAME> — имя профиля IP-адресов, задается строкой до 31 символа.
10	Указать идентификатор ключа из профиля связки ключей (не обязательно).	**scs(config)# ntp authentication trusted-key <ID>**	<ID> — идентификатор ключа из профиля связки ключей.
11	Указать имя профиля связки ключей (не обязательно).	**scs(config)# ntp authentication key-chain <WORD>**	<WORD> — имя профиля связки ключей.
12	Активировать аутентификацию для NTP по ключу (не обязательно).	**scs(config)# ntp authentication enable**	
13	Включить режим приема широковещательных сообщений NTP-серверов для глобальной конфигурации (не обязательно).	**scs(config)# ntp broadcast-client enable**	
14	Задать значение кода DSCP для использования в IP-заголовке исходящих пакетов NTP-сервера (не обязательно).	**scs(config)# ntp dscp <DSCP>**	<DSCP> — значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 46.
17	Указать source-IP-адреса для NTP-пакетов для всех peer (не обязательно).	**scs(config)# ntp source address <ADDR>**	<ADDR> — IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].

Шаг	Описание	Команда	Ключи
18	Задать текущие время и дату в ручном режиме (не обязательно).	**scs# set date <TIME> [<DAY> <MONTH> [<YEAR>]]**	<TIME> — устанавливаемое системное время, задается в виде HH:MM:SS, где: • HH — часы, принимает значение [0..23]; • MM — минуты, принимает значение [0 .. 59]; • SS — секунды, принимает значение [0 .. 59]. • <DAY> — день месяца, принимает значения [1..31]; <MONTH> — месяц, принимает значения [January/February/March/April/May/June/July/August/September/October/November/December]; <YEAR> — год, принимает значения [2001..2037].

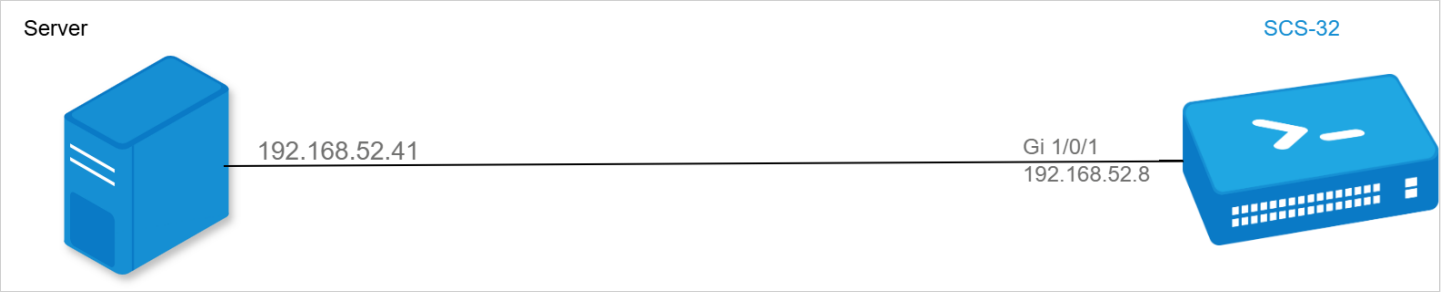
11.1.2 Пример настройки

Задача:

Настроить синхронизацию времени от NTP-сервера.

IP-адрес SCS — 192.168.52.8,

IP-адрес NTP-сервера — 192.168.52.41.



Решение:

⚠ Предварительно нужно настроить IP-адрес для интерфейса gi1/0/1, чтобы обеспечить IP-связность с NTP-сервером.
Пример:

```
interface gigabitethernet 1/0/1
  ip address 192.168.52.8/24
exit
```

Основной этап конфигурирования:

Включение синхронизации системных часов с удаленными серверами:

```
scs(config)# ntp enable
```

Настройка NTP-сервера:

```
scs-(config)# ntp server 192.168.52.41
```

Указать предпочтительность данного NTP-сервера (необязательно):

```
scs-1000(config-ntp)# prefer
```

Указать интервал времени между отправкой сообщений NTP-серверу:

```
scs(config-ntp)# minpoll 4
scs(config-ntp)# end
scs# commit
scs# confirm
```

Команда для просмотра текущей конфигурации протокола NTP:

```
scs# show ntp configuration
```

Команда для просмотра текущего состояния NTP-серверов (пиров):

```
scs# show ntp peers
```

11.2 Настройка Reverse Telnet/SSH

Reverse Telnet/SSH — это технология удаленного управления физическими консольными портами (RS-232, AUX) оборудования (маршрутизаторы, серверы) через сеть.

11.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования последовательного интерфейса.	**scs(config)# line aux [<ID>/ <SLOT>/<PORT>]**	<ID> — номер устройства; <SLOT> — номер модуля в составе устройства или 0 при отсутствии деления устройства на модули; <PORT> — порядковый номер порта.

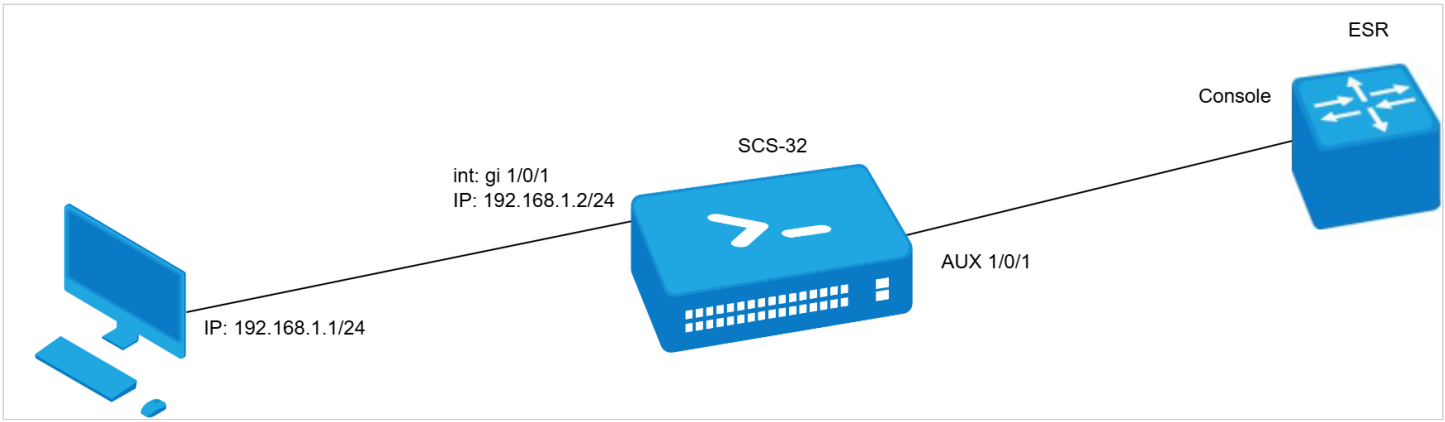
Шаг	Описание	Команда	Ключи
2	Установить необходимые параметры последовательного интерфейса для взаимодействия с подключенным устройством (необязательно). Данные параметры, как правило, указаны в инструкции подключаемого устройства. По умолчанию будут использованы стандартные значения.	**scs(config-line-aux) databits <BITS>** **scs(config-line-aux) flowcontrol <FMODE>** **scs(config-line-aux) parity <PMODE>** **scs(config-line-aux) speed <SPEED>** **scs(config-line-aux) stopbits <STOP-BITS>**	<BITS> — количество бит данных в посылке [7..8]; Значение по умолчанию: 8. <FMODE> — режим управления потоком. Принимает значения: • software — программное управление потоком; • hardware — аппаратное управление потоком; • disabled — управление потоком отключено; Значение по умолчанию: disabled. <PMODE> — режим установки бита четности. Принимает значения: • odd — проверка на нечетность; • even — проверка на четность; • none — бит четности не выставляется; Значение по умолчанию: none. <SPEED> — скорость работы последовательного интерфейса в бит/с. Принимает значения: 300; 1200; 2400; 4800; 9600; 19200; 38400; 57600; 115200; Значение по умолчанию: 115200. <STOP-BITS> — количество стоповых битов в посылке [1..2]; Значение по умолчанию: 1.
3	Задать описание последовательного интерфейса (необязательно).	**scs(config-line-aux)# description <DESCRIPTION>**	<DESCRIPTION> — описание интерфейса, задаётся строкой до 255 символов.

Шаг	Описание	Команда	Ключи
4	Установить протокол по которому будет осуществляться подключение.	**scs(config-line-aux)# transport input <AUX_TRANSPORT>**	<AUX_TRANSPORT> — протокол с помощью которого будет осуществляться подключение к AUX-порту: • SSH • Telnet
5	Установить TCP-порт для режима подключения reverse telnet.	**scs(config-line-aux)# transport telnet port <PORT>**	<PORT> — номер TCP-порта. Принимает значения [1..65535].

11.2.2 Пример настройки

Задача 1:

Настроить подключение к маршрутизатору ESR с помощью Reverse Telnet.



Решение:

Сконфигурировать SCS-32

Настроим параметры согласования:

```
scs-32(config)# line aux 1/0/1
scs-32(config-line-aux)# transport telnet port 3001
scs-32(config-line-aux)# exit
scs-21-1(config)#
```

Сконфигурируем IP-адрес на SCS-32:

```
scs-32(config)# interface gigabitethernet 1/0/1
scs-32(config-if-gi)# ip address 192.168.1.2/24
scs-32(config-if-gi)# exit
scs-32(config)#
```

Включим Telnet-сервер:

```
scs-32(config)# ip telnet server
```

Подключение выполняется в формате:

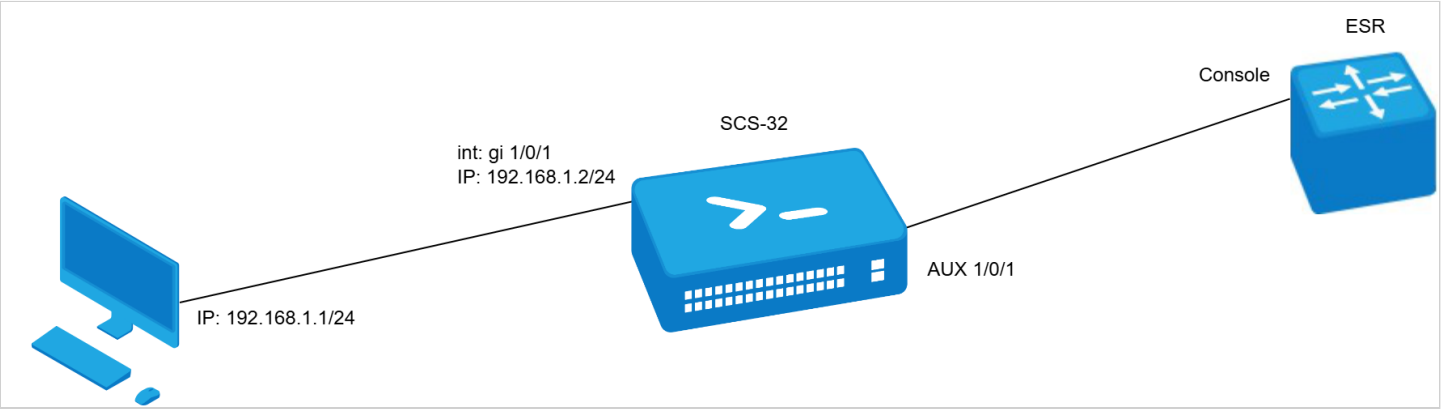
`telnet <ip> <port>`

Пример:

```
PC@PC:~$ telnet 192.168.1.2 3001
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.

scs-32 login: admin
Password:

*****************************************
*            Welcome to SCS-32          *
*****************************************

scs-30 login:
```

Задача 2:

Настроить подключение к маршрутизатору ESR с помощью Reverse SSH.



Решение:

Сконфигурировать SCS-32

Настроим параметры согласования:

```
scs-32(config)# line aux 1/0/1
scs-32(config-line-aux)# transport input ssh
scs-32(config-line-aux)# exit
scs-21-1(config)#
```

Сконфигурируем IP-адрес на SCS-32:

```
scs-32(config)# interface gigabitethernet 1/0/1
scs-32(config-if-gi)# ip address 192.168.1.2/24
scs-32(config-if-gi)# exit
scs-32(config)#
```

Включим SSH-сервер:

```
scs-32(config)# ip SSH server
```

Подключение выполняется в формате:

`ssh <user>:<console>@<ip>`

Пример

```
igor@igor-H610M-S2H-DDR4:~$ ssh admin:aux1@192.168.1.2
admin:aux1@192.168.1.2's password:

scs-30 login:
```

где:

admin — имя пользователя SSH;
aux1 — имя консоли;
192.168.1.2 — адрес устройства.

12 Мониторинг

12.1 Настройка SNMP

SNMP (англ. Simple Network Management Protocol — простой протокол сетевого управления) — протокол, предназначенный для управления устройствами в IP-сетях на основе архитектур TCP/UDP. SNMP предоставляет данные для управления в виде переменных, описывающих конфигурацию управляемой системы.

12.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить SNMP-сервер.	**scs(config)# snmp-server**	

Шаг	Описание	Команда	Ключи
2	Определить community для доступа по протоколу SNMPv2c.	**scs(config)# snmp-server [encrypted] community <COMMUNITY> [<TYPE>] [{ <IP-ADDR> | <IPV6-ADDR> }] [client-list <OBJ-GROUP-NETWORK-NAME>] [<VERSION>] [view <VIEW-NAME>] [encrypt]**	encrypted — при добавлении данного параметра, ввод названия сообщества <COMMUNITY> требуется производить в зашифрованном виде. <COMMUNITY> — сообщество для доступа по протоколу SNMP; <TYPE> — уровень доступа: • **ro** — доступ только для чтения; • **rw** — доступ для чтения и записи. <IP-ADDR> — IP-адрес клиента, которому предоставлен доступ, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> — IPv6-адрес клиента, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <OBJ-GROUP-NETWORK-NAME> — имя профиля IP-адресов, от которых обрабатываются snmp-запросы, задается строкой до 31 символа; <VERSION> — версия SNMP, поддерживаемая данным community, принимает значения v1 или v2c; <VIEW-NAME> — имя профиля SNMP view, задаётся строкой до 31 символа; encrypt — при добавлении данного параметра, название сообщества <COMMUNITY> будет отображаться в конфигурации устройства в зашифрованном виде.
3	Устанавливает значение переменной SNMP, содержащей контактную информацию.	**scs(config)# snmp-server contact <CONTACT>**	<CONTACT> — контактная информация, задается строкой до 255 символов.
4	Установить значение кода DSCP для использования в IP-заголовке исходящих пакетов SNMP-сервера (не обязательно).	**scs(config)# snmp-server dscp <DSCP>**	<DSCP> — значение кода DSCP, принимает значения в диапазоне [0..63]. Значение по умолчанию: 63.
5	Создать SNMPv3-пользователя.	**scs(config)# snmp-server user <NAME>**	<NAME> — имя пользователя, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
6	Устанавливает значение переменной SNMP, содержащей информацию о расположении оборудования.	**scs(config)# snmp-server location <LOCATION>**	<LOCATION> — информация о расположении оборудования, задается строкой до 255 символов.
7	Определить уровень доступа пользователя по протоколу SNMPv3.	**scs(config-snmp-user)# access <TYPE>**	<TYPE> — уровень доступа: • **ro** — доступ только для чтения; • **rw** — доступ для чтения и записи.
8	Определить режим безопасности пользователя по протоколу SNMPv3.	**scs(config-snmp-user)# authentication access <TYPE>**	<TYPE> — режим безопасности: • **auth** — используется только аутентификация; • **priv** — используется аутентификация и шифрование данных.
9	Определить алгоритм аутентификации SNMPv3-запросов.	**scs(config-snmp-user)# authentication algorithm <ALGORITHM>**	<ALGORITHM> — алгоритм шифрования: • **md 5** — пароль шифруется по алгоритму md5; • **sha 1** — пароль шифруется по алгоритму sha1.
10	Установить пароль для аутентификации SNMPv3-запросов.	**scs(config-snmp-user)# authentication key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> — пароль, задается строкой от 8 до 16 символов; • **encrypted** — при указании команды задается зашифрованный пароль: <ENCRYPTED-TEXT> — зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
11	Активировать фильтрацию и установить профиль IP-адресов, с которых могут приниматься SNMPv3-пакеты с данным именем SNMPv3-пользователя.	**scs(config-snmp-user)# client-list <NAME>**	<NAME> — имя ранее сознанной object-group, задается строкой до 31 символа.

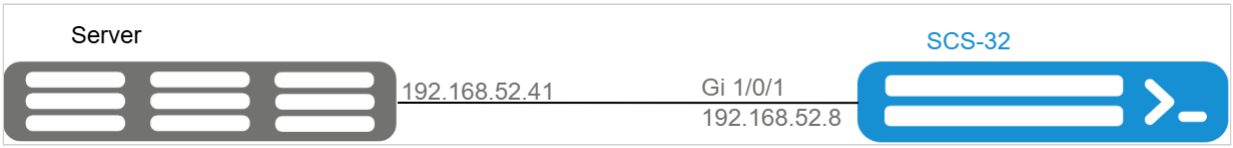
Шаг	Описание	Команда	Ключи
13	Активировать фильтрацию и установить IPv4/IPv6-адрес, которому предоставлен доступ к консольному серверу под данным SNMPv3-пользователем.	**scs(config-snmp-user)# ip address <ADDR>**	<ADDR> — IP-адрес клиента, которому предоставлен доступ, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
		scs(config-snmp-user)# ipv6 address <ADDR>	<IPV6-ADDR> — IPv6-адрес клиента, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
14	Активировать SNMPv3-пользователя.	**scs(config-snmp-user)# enable**	Значение по умолчанию: процесс выключен.
15	Определить алгоритм шифрования передаваемых данных.	**scs(config-snmp-user)# privacy algorithm <ALGORITHM>**	<ALGORITHM> — алгоритм шифрования: • **aes 128** — использовать алгоритм шифрования AES-128; • **des** — использовать алгоритм шифрования DES.
16	Установить пароль для шифрования передаваемых данных.	**scs(config-snmp-user)# privacy key ascii-text { <CLEAR-TEXT> | encrypted <ENCRYPTED-TEXT> }**	<CLEAR-TEXT> — пароль, задается строкой от 8 до 16 символов; <ENCRYPTED-TEXT> — зашифрованный пароль размером от 8 байт до 16 байт (от 16 до 32 символов) в шестнадцатеричном формате (0xYYYY...) или (YYYY...).
17	Установить профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для user.	**scs(config-snmp-user)# view <VIEW-NAME>**	<VIEW-NAME> — имя SNMP view профиля, на основании которого обеспечивается доступ к OID, задается строкой до 31 символа.
18	Включить передачу SNMP-уведомлений на указанный IP-адрес и перейти в режим настройки SNMP-уведомлений.	**scs(config)# snmp-server host { <IP-ADDR> | <IPV6-ADDR> }**	<IP-ADDR> — IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]. <IPV6-ADDR> — IPv6-адрес, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF];
19	Определить порт коллектора SNMP-уведомлений на удаленном сервере (не обязательно).	**scs(config-snmp-host)# port <PORT>**	<PORT> — номер UDP-порта, указывается в диапазоне [1..65535]. Значение по умолчанию: 162.

Шаг	Описание	Команда	Ключи
20	Установить IP-адрес для отправки уведомлений на удаленный сервер.	**scs(config-snmp-host)# source-address { <ADDR> | <IPV6-ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> — IP-адрес, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> — IPv6-адрес, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> — список адресов, которые будут использоваться в качестве source address. Значение по умолчанию: IPv4/IPv6 — адрес интерфейса, ближайшего к удаленному SNMP-серверу.
21	Установить интерфейс консольного сервера, IPv4/IPv6-адрес которого будет использоваться для отправки уведомлений на удаленный сервер.	**scs(config-snmp-host)# source-interface <IF>**	<IF> — имя интерфейса устройства, задается в виде, описанном в разделе Типы и порядок именования интерфейсов консольного сервера;
22	Разрешить отправку SNMP-уведомлений различных типов.	**scs(config)# snmp-server enable traps <TYPE>**	<TYPE> — тип фильтруемых сообщений. Может принимать значения: config, entry, entry-sensor, environment, envmon, files-operations, flash, flash-operations, interfaces, links, ports, screens, snmp, syslog. Дополнительные параметры зависят от типа фильтра. См. справочник команд CLI.
23	Создать профиль snmp view, позволяющий разрешать или запрещать доступ к тем или иным OID для community (SNMPv2) и user (SNMPv3).	**scs(config)# snmp-server view <VIEW-NAME>**	<VIEW-NAME> — имя профиля SNMP view, задается строкой до 31 символа.

12.1.2 Пример настройки

Задача:

Настроить SNMPv3-сервер с аутентификацией и шифрованием данных для пользователя admin. IP-адрес консольного сервера — 192.168.52.8, IP-адрес сервера — 192.168.52.41.



Решение:

Предварительно нужно выполнить следующие действия:

- указать зону для интерфейса gi1/0/1;
- настроить IP-адрес для интерфейсов gi1/0/1.

Основной этап конфигурирования:

Включаем SNMP-сервер:

```
scs(config)# snmp-server
```

Создаем пользователя SNMPv3:

```
scs(config)# snmp-server user admin
```

Определим режим безопасности:

```
scs(snmp-user)# authentication access priv
```

Определим алгоритм аутентификации для SNMPv3-запросов:

```
scs(snmp-user)# authentication algorithm md5
```

Установим пароль для аутентификации SNMPv3-запросов:

```
scs(snmp-user)# authentication key ascii-text 123456789
```

Определим алгоритм шифрования передаваемых данных:

```
scs(snmp-user)# privacy algorithm aes128
```

Установим пароль для шифрования передаваемых данных:

```
scs(snmp-user)# privacy key ascii-text 123456789
```

Активируем SNMPv3-пользователя:

```
scs(snmp-user)# enable
```

Определяем сервер-приемник Trap-PDU-сообщений:

```
scs(config)# snmp-server host 192.168.52.41
```

12.2 Настройка Syslog

Syslog (англ. *System Log* — системный журнал) — стандарт отправки и регистрации сообщений о происходящих в системе событиях, используется в сетях, работающих по протоколу IP.

12.2.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Включить отправку syslog-сообщений на snmp-сервер в виде snmp-trap.	**scs(config)# syslog snmp**	
2	Активировать или деактивировать отправку на snmp-сервер событий работы отдельных процессов консольного сервера (не обязательно).	**scs(config-syslog-snmp)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> — см. в справочнике команд CLI. Если описаны разрешающие критерии (match process-name) — логируются только сообщения указанных процессов. Если указаны запрещающие критерии (match not process-name) — логируются сообщения всех не запрещенных процессов. По умолчанию разрешено логирование сообщений всех процессов.

Шаг	Описание	Команда	Ключи
3	Указать уровень важности сообщений, которые будут отправляться на snmp-сервер.	**scs(config-syslog-snmp)# severity <SEVERITY>**	<SEVERITY> — уровень важности сообщения, принимает значения (в порядке убывания важности): • **emerg** — в системе произошла критическая ошибка, система неработоспособна; • **alert** — сигналы тревоги, необходимо немедленное вмешательство персонала; • **crit** — критическое состояние системы, сообщение о событии; • **error** — сообщения об ошибках; • **warning** — предупреждения, неаварийные сообщения; • **notice** — сообщения о важных системных событиях; • **info** — информационные сообщения системы; • **debug** — отладочные сообщения, предоставляют пользователю информацию для корректной настройки системы; • **none** — отключает вывод syslog-сообщений.
4	Включить отображение syslog-сообщений при удаленных подключениях (Telnet, SSH) (не обязательно).	**scs(config)# syslog monitor**	
5	Активировать или деактивировать отображение при удаленных подключениях событий работы отдельных процессов консольного сервера (не обязательно).	**scs(config-syslog-monitor)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> — описано во 2 пункте.
6	Указать уровень важности сообщений, которые будут отображаться при удаленных подключениях.	**scs(config-syslog-monitor)# severity <SEVERITY>**	<SEVERITY> — описано в 3 пункте.
7	Включить отображение syslog-сообщений при консольном подключении (не обязательно).	**scs(config)# syslog console**	

Шаг	Описание	Команда	Ключи
8	Активировать или деактивировать отображение при консольном подключении событий работы отдельных процессов консольного сервера (не обязательно).	**scs(config-syslog-console)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> — описано во 2 пункте.
9	Указать уровень важности сообщений, которые будут отображаться при консольном подключении.	**scs(config-syslog-console)# severity <SEVERITY>**	<SEVERITY> — описано в 3 пункте.
10	Указать категорию сообщений, которые будут сохраняться в локальный syslog-файл или отправляться на удаленный syslog-сервер.	**scs(config)# syslog facility <FACILITY>**	<FACILITY> — категория сообщений, принимает значения [local0..local7].
11	Включить сохранение сообщений syslog в указанный файл журнала (при необходимости ведения локального syslog-файла).	**scs(config)# syslog file <NAME>**	<NAME> — имя файла, в который будет производиться запись сообщений заданного уровня, задается строкой до 31 символа.
12	Активировать или деактивировать сохранение в локальный syslog-файл событий работы отдельных процессов консольного сервера (не обязательно).	**scs(config-syslog-file)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> — описано во 2 пункте.
13	Указать уровень важности сообщений, которые будут сохраняться в локальный syslog-файл.	**scs(config-syslog-file)# severity <SEVERITY>**	<SEVERITY> — описано в 3 пункте.
14	Указать максимальный размер файла журнала (не обязательно).	**scs(config)# syslog file-size <SIZE>**	<SIZE> — размер файла, принимает значение [10..10000000] Кбайт.
15	Задать максимальное количество файлов, сохраняемых при ротации (не обязательно).	**scs(config)# syslog max-files <NUM>**	<NUM> — максимальное количество файлов, принимает значения [1.. 1000].
16	Включить передачу сообщений syslog на удаленный syslog-сервер (при необходимости отправки сообщений на удаленный syslog-сервер).	**scs(config)#syslog host <HOSTNAME>**	<HOSTNAME> — наименование syslog-сервера, задается строкой до 31 символа. Используется только для идентификации сервера при конфигурировании. Значение «all» используется в команде no syslog host для удаления всех syslog-серверов;

Шаг	Описание	Команда	Ключи
17	Указать что использовать в качестве значения поля HOSTNAME при передачи сообщений на удаленный syslog-сервер (не обязательно).	**scs(config-syslog-host)# identifier { fqdn | ip | hostname }**	fqdn — использовать в качестве значения полное имя устройства: hostname.domain_name. Используется только вместе с настроенным domain name; ip — использовать в качестве значения IP-адрес интерфейса устройства. Если не указан source-address, то в качестве значения будет использован IP-адрес интерфейса, за которым находится удаленный syslog-сервер; hostname — использовать в качестве значения имя устройства.
18	Указать IPv4/IPv6-адрес удаленного syslog-сервера.	**scs(config-syslog-host)# remote-address { <ADDR> | <IPV6-ADDR> }**	<ADDR> — IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> — IPv6-адрес, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
19	Указать IPv4/IPv6-адрес консольного сервера, от которого будут отправляться пакеты на удаленный syslog-сервер (не обязательно).	**scs(config-syslog-host)# source-address { <ADDR> | <IPV6-ADDR> | object-group <NETWORK_OBJ_GROUP_NAME> }**	<ADDR> — IP-адрес, задается в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> — IPv6-адрес, задается в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <NETWORK_OBJ_GROUP_NAME> — список адресов, которые будут использоваться в качестве source address; Значение по умолчанию: IPv4/IPv6-адрес интерфейса, с которого отправляется пакеты на удаленный syslog-сервер.
20	Указать транспортный протокол для передачи пакетов на удаленный syslog-сервер (не обязательно).	**scs(config-syslog-host)# transport { tcp | udp }**	Значение по умолчанию: отсутствует (глобальная таблица маршрутизации).

Шаг	Описание	Команда	Ключи
21	Указать номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями (не обязательно).	**scs(config-syslog-host)# port <PORT>**	<PORT> — номер TCP/UDP-порта, на который будут отправляться пакеты с syslog-сообщениями. Значение по умолчанию: 514.
22	Активировать или деактивировать отправку на удаленный syslog-сервер событий работы отдельных процессов консольного сервера (не обязательно).	**scs(config-syslog-host)# match [not] process-name <PROCESS-NAME>**	<PROCESS-NAME> — описано во 2 пункте.
23	Указать уровень важности сообщений, которые будут сохраняться в локальный syslog-файл.	**scs(config-syslog-host)# severity <SEVERITY>**	<SEVERITY> — описано в 3 пункте.
24	Включить вывод отладочных сообщений во время загрузки устройства (не обязательно).	**scs(config)#syslog reload debugging**	
25	Включить процесс логирования введенных команд пользователя на локальный syslog-сервер (не обязательно).	**scs(config)# syslog cli-commands**	
26	Включить нумерацию сообщений (не обязательно).	**scs(config)#syslog sequence-numbers**	
27	Включить точность даты сообщений до миллисекунд (не обязательно).	**scs(config)#syslog timestamp msec**	
28	Включить отображение имени процесса, который сформировал сообщение (не обязательно).	**scs(config)#syslog program-name**	
29	Включить регистрацию неудачных аутентификаций (не обязательно).	**scs(config)#logging login on-failure**	
30	Включить регистрацию изменений настроек системы аудита (не обязательно).	**scs(config)#logging syslog configuration**	
31	Включить регистрацию изменений настроек пользователя (не обязательно).	**scs(config)#logging userinfo**	

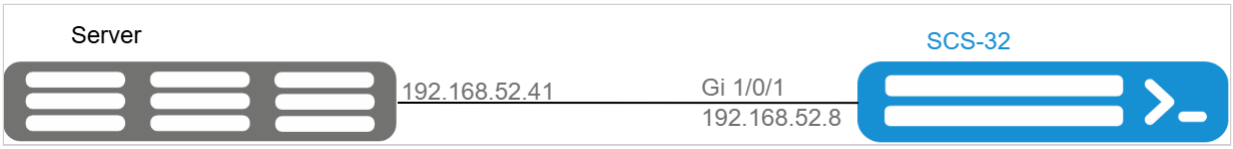
12.2.2 Пример настройки

Задача:

Настроить отправку сообщений для следующих системных событий:

- неудачная аутентификация пользователя;
- внесены изменения в конфигурацию логирования системных событий;
- старт/остановка системного процесса;
- внесены изменения в профиль пользователей.

IP-адрес консольного сервера — 192.168.52.8, IP-адрес Syslog-сервера — 192.168.52.41. Использовать параметры по умолчанию для отправки сообщений — протокол UDP, порт 514.



Решение:

Предварительно нужно выполнить следующие действия:

- указать зону для интерфейса gi1/0/1;
- настроить IP-адрес для интерфейсов gi1/0/1.

Основной этап конфигурирования:

Создаем файл на консольном сервере для системного журнала, уровень сообщений для журналирования — info:

```
scs(config)# syslog file tmpsys:syslog/scs
scs(config-syslog-file)# severity info
scs(config-syslog-file)# exit
```

Указываем IP адрес и параметры удаленного syslog-сервера:

```
scs(config)# syslog host SERVER
scs(config-syslog-host)# remote-address 192.168.52.41
scs(config-syslog-host)# severity info
scs(config-syslog-host)# exit
```

Задаем логирование неудачных попыток аутентификации:

```
scs(config)# logging login on-failure
```

Задаем логирование изменений конфигурации syslog:

```
scs(config)# logging syslog configuration
```

Задаем логирование старта/остановки системных процессов:

```
scs(config)# logging service start-stop
```

Задаем логирование внесений изменений в профиль пользователей:

```
scs(config)# logging userinfo
```

Изменения конфигурации вступят в действие после применения:

```
scs# commit
Configuration has been successfully committed
scs# confirm
Configuration has been successfully confirmed
```

Посмотреть текущую конфигурацию системного журнала:

```
scs# show syslog configuration
```

Посмотреть записи системного журнала:

```
scs# show syslog scs
```

12.3 Проверка целостности

Проверка целостности подразумевает проверку целостности хранимых исполняемых файлов.

12.3.1 Процесс настройки

Шаг	Описание	Команда	Ключи
1	Запустить проверку целостности системы	**scs# verify filesystem <detailed>**	**detailed** – детальный вывод информации в консоль.

12.3.2 Пример конфигурации

Задача:

Проверить целостность файловой системы.

Решение:

Запускаем проверку целостности:

```
scs# verify filesystem
Filesystem Successfully Verified
```

12.4 Настройка архивации конфигурации консольного сервера

На устройствах SCS предусмотрена функция локального и/или удаленного копирования конфигурации по таймеру или при применении конфигурации.

12.4.1 Процесс настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим настройки параметров резервирования конфигурации.	**scs(config)# archive**	
2	Установить тип сохранения резервных конфигураций консольного сервера (не обязательно).	**scs(config-ahchive)# type <TYPE>**	<TYPE> — тип сохранения резервных конфигураций консольного сервера. Принимает значения: • **local;** • **remote;** • **both.** Значение по умолчанию: remote.
3	Включить режим резервирования конфигурации по таймеру (не обязательно).	**scs(config-ahchive)# auto**	
4	Включить режим резервирования конфигурации после каждого успешного применения конфигурации (не обязательно).	**scs(config-ahchive)# by-commit**	
5	Указать путь для удаленного копирования конфигураций консольного сервера (обязательно для типов remote и both).	**scs(config-ahchive)# path <PATH>**	<PATH> — определяет протокол, адрес сервера, расположение и префикс имени файла на сервере.
6	Задать период времени для автоматического резервирования конфигурации (не обязательно, актуально только для режима auto).	**scs(config-ahchive)# time-period <TIME>**	<TIME> — периодичность автоматического резервирования конфигурации, принимает значение в минутах [1..525600]. Значение по умолчанию: 720 минут.
7	Задать максимальное количество локально сохраняемых резервных копий конфигураций (не обязательно, актуально при типах local и both).	**scs(config-ahchive)# count-backup <NUM>**	<NUM> — максимальное количество локально сохраняемых резервных копий конфигураций. Принимает значения в диапазоне [1..100]. Значение по умолчанию: 1.

12.4.2 Пример конфигурации

Задача:

Настроить локальное и удаленное резервное копирование конфигурации консольного сервера 1 раз в сутки и при успешном изменении конфигурации. Удаленные копии необходимо отправлять на tftp-сервер 172.16.252.77 в подпапку scs-example. Максимальное количество локальных копий — 30.

Решение:

Для успешной работы удаленной архивации конфигураций, между SCS и сервером должна быть организована IP-связность, настроены разрешения на прохождение tftp-трафика по сети и сохранения файлов на сервере.

Основной этап конфигурирования:

Перейти в режим конфигурирования резервного копирования конфигураций:

```
scs# configure
scs(config)# archive
```

Задать режим локального и удаленного резервного копирования конфигурации:

```
scs(config-archive)# type both
```

Настроить путь для удаленного копирования конфигураций и максимальное количество локальных резервных копий:

```
scs(config-archive)# path tftp://172.16.252.77:/scs-example/scs-example.cfg
scs(config-archive)# count-backup 30
```

Задать интервал резервного копирования конфигурации в случае отсутствия изменений:

```
scs(config-archive)# time-period 1440
```

Включить режимы архивации конфигурации консольного сервера по таймеру и при успешном изменении конфигурации:

```
scs(config-archive)# auto
scs(config-archive)# by-commit
```

После применения данной конфигурации 1 раз в сутки и при каждом успешном изменении конфигурации консольного сервера на tftp-сервер будет отправляться конфигурационный файл с именем вида "scs-exampleYYYYMMDD_HHMMSS.cfg". Также на самом сервер в разделе flash:backup/ будет создаваться файл с именем вида "config_YYYYMMDD_HHMMSS". Когда в разделе flash:backup/ накопится 30 таких файлов, при создании нового будет удаляться наиболее старый. Посмотреть можно командой:

```
scs(config)# show archive configuration
```

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: https://eltex.ru/support/

Servicedesk: https://servicedesk.eltex-co.ru

На официальном сайте компании вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку:

Официальный сайт компании: https://eltex.ru

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex.ru/download/