ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон/Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.ru
Сайт: http://www.s-terra.ru

Криптомаршрутизатор Zelax-ST MM-1017

Техническое описание

14.11.2016 г.

Оглавление

1 Введение

Криптомаршрутизатор Zelax-ST ММ-1017 (далее Криптомаршрутизатор) — это российский криптомаршрутизатор, который сочетает в себе высокую производительность и шифрование в соответствии с ГОСТ 28147-89. Шифрование и сетевую безопасность обеспечивает встроенный СКЗИ «Программный комплекс С-Терра Шлюз. Версия 4.1» (сертификаты ФСБ России по классам КС1, КС2, КС3, МЭ4, сертификат ФСТЭК России по 3 классу МЭ).

Криптомаршрутизатор позволяет строить высокопроизводительные надёжные сети передачи данных различного назначения и гарантирует защиту информации в соответствии с требованиями ФСБ России и ФСТЭК России при передаче её по недоверенным каналам связи.

Варианты применения оборудования представлены на Рис. 1 и Рис. 2.

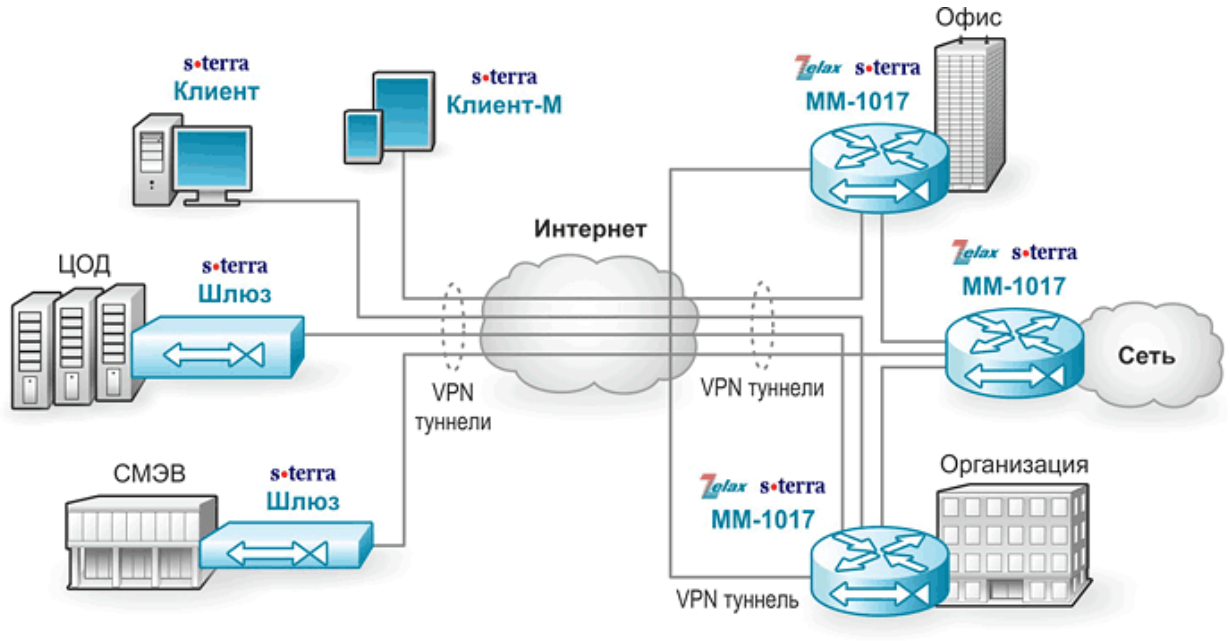


Рис. 1 Организация защищённой территориально-распределенной сети

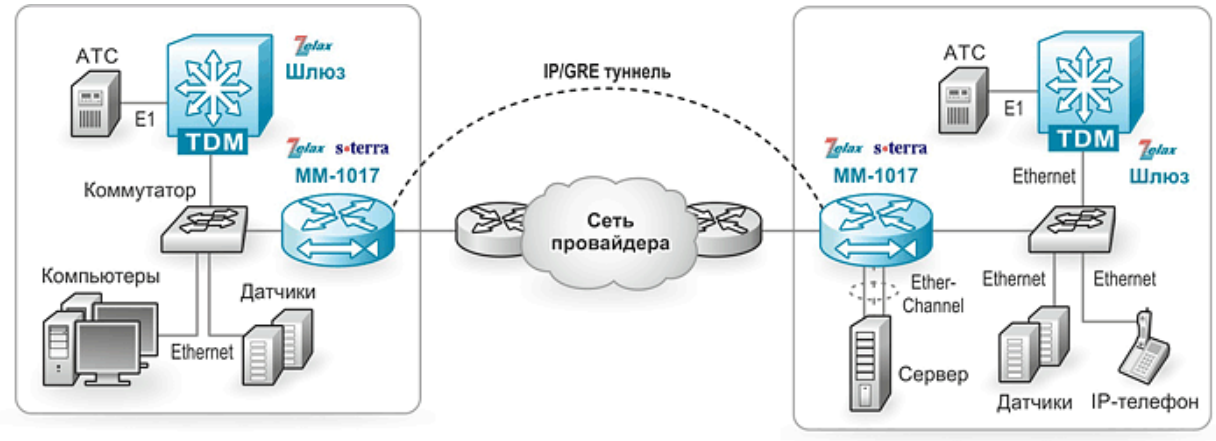


Рис. 2 Организация доверенного подключения через публичную сеть

2 Общие сведения об устройстве Криптомаршрутизатора

- Криптомаршрутизатор состоит из двух независимых модулей, расположенных в общем корпусе: модуля коммутации и криптомодуля;
- Модуль коммутации представляет собой плату, реализующую функции коммутатора Ethernet L3;
- Криптомодуль представляет собой плату, на которой реализована вычислительная система в архитектуре Intel x86 универсального назначения;
- В Криптомаршрутизатор устанавливается до двух съёмных блоков питания;
- Цепи электропитания обоих модулей объединены. Каждый блок питания питает оба модуля;
- Линии обмена информацией между модулями внутри корпуса не реализованы (отсутствуют);
- Управление модулем коммутации и криптомодулем раздельное, через специальные порты, физически соединенные с соответствующим модулем.

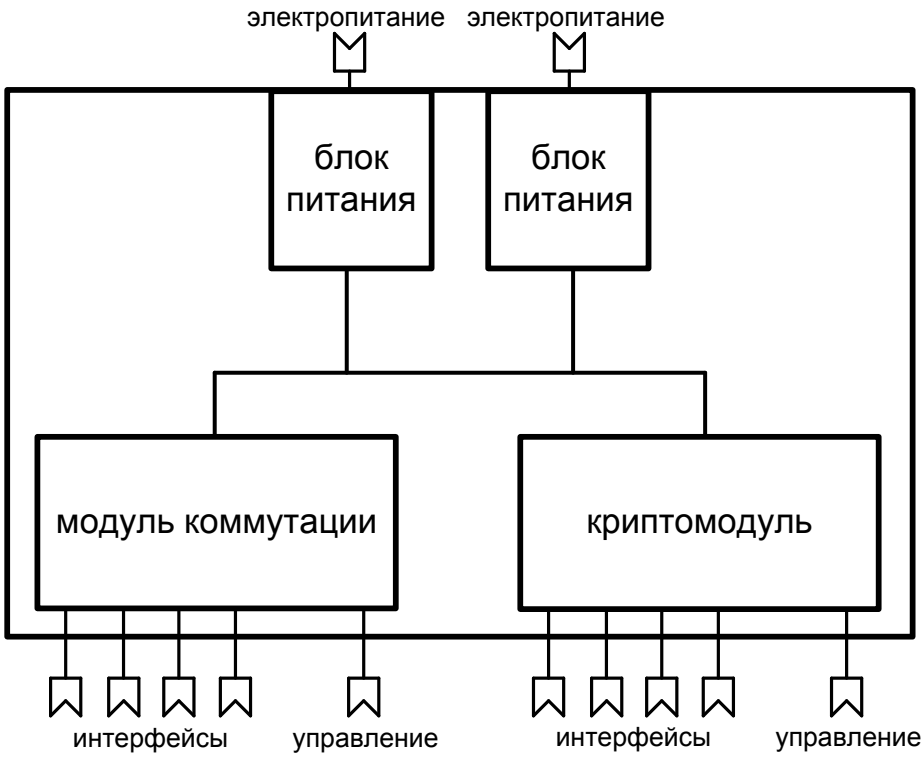


Рис. 3 Внутреннее устройство Криптомаршрутизатора

3 Структура изделия

Криптомаршрутизатор состоит из модуля коммутации и криптомодуля.

3.1 Модуль коммутации

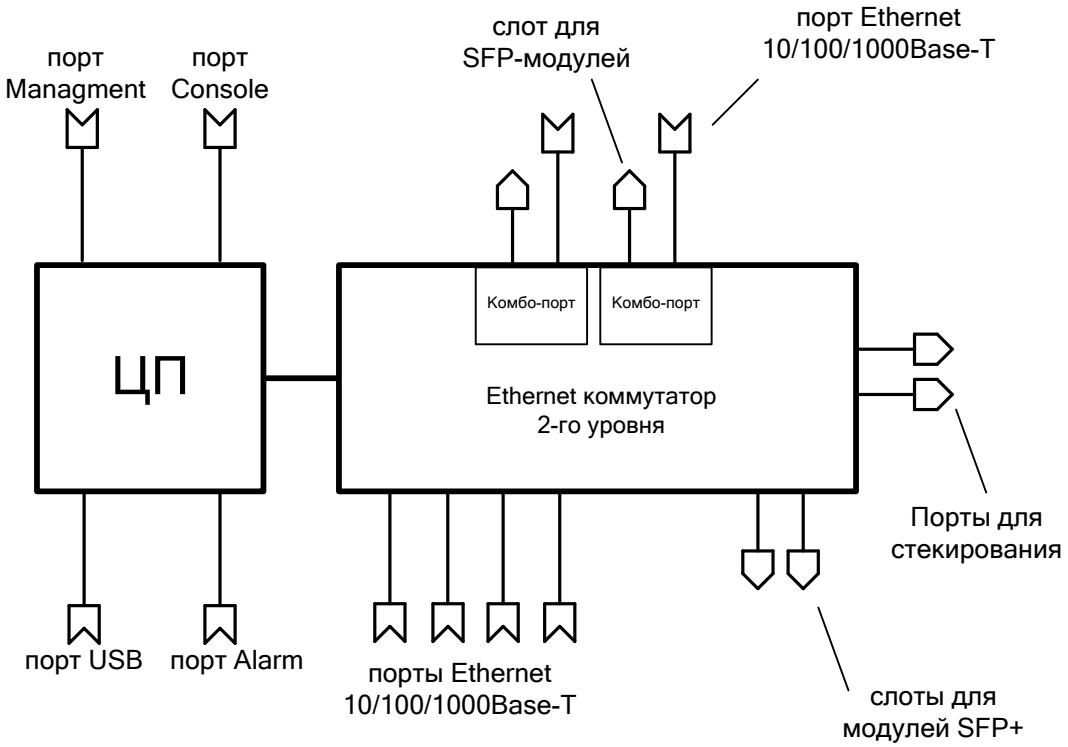


Рис. 4 Структурная схема модуля коммутации

Модуль коммутации содержит:

- процессор;
- порт Alarm;
- порт USB;
- коммутатор Ethernet 2-го уровня;
- 20 портов Ethernet 10/100/1000Base-T;
- четыре слота для установки модулей SFP/SFP+;
- четыре комбинированных порта 1000Base-T/1000Base-X, с возможностью установки SFP-модулей;
- управляющий порт Ethernet 10/100/1000Base-T;
- управляющий порт Console.

3.2 Криптомодуль

Криптомаршрутизатор содержит криптомодуль.

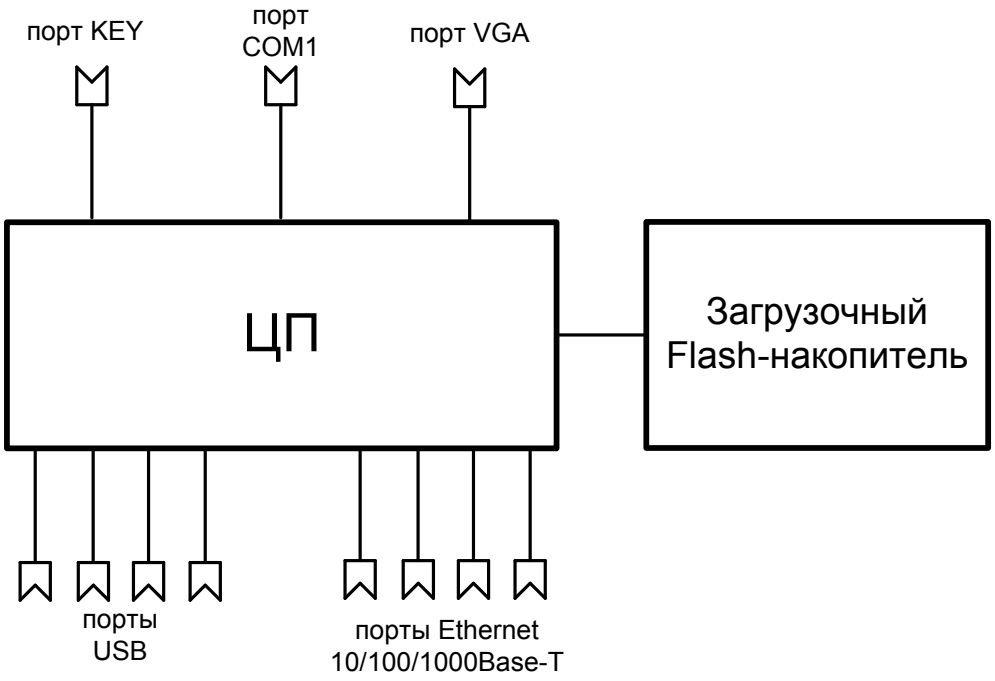


Рис. 5 Структурная схема криптомодуля

Криптомодуль содержит:

- процессор;
- загрузочный Flash-накопитель (SSD-диск или СЗН «СПДС-USB-01»);
- четыре порта USB;
- четыре порта Ethernet 10/100/1000Base-T;
- порт VGA для подключения монитора;
- порт KEY для подключения внешнего считывателя идентификатора;
- управляющий порт COM1.

3.3 Порт

Порт представляет собой соединитель (разъём), к которому с помощью кабеля подключается то или иное устройство или линия связи (Рис. 4). Порт реализует определённый интерфейс.

3.4 Слот

Слот — разъём для установки модуля SFP, SFP+.

3.5 Центральный процессор

Центральный процессор — компонент, размещённый в базовом модуле и предназначенный для обработки данных, поступающих на его интерфейсы.

3.6 Ethernet-коммутатор

Ethernet-коммутатор — компонент, размещённый в базовом модуле и предназначенный для обработки данных, поступающих на его интерфейсы. Ethernet-коммутатор осуществляет коммутацию пакетов, поступающих через порты Ethernet.

4 Комплект поставки

В комплект поставки Криптомаршрутизатора входят:

- изделие выбранного исполнения;
- консольный кабель RJ-45;
- переходник A-006;
- патч-корд Gigabit Ethernet (длиной 50 см);
- комплект для установки в 19" стойку;
- заглушки для SFP+ и SFP-слотов;
- упаковочная коробка;
- компакт-диск с документацией Zelax;
- компакт-диск с документацией «S-Terra Product Line Documentation» («Программный комплекс С-Терра Шлюз. Версия 4.1» Руководство администратора, «Программный продукт С-Терра КП. Версия 4.1» Руководство администратора, Правила пользования, Формуляры, копия сертификата соответствия ФСБ России, копия сертификата соответствия ФСТЭК России);
- дистрибутивы «Программного комплекса С-Терра Шлюз. Версия 4.1» и «Программного продукта С-Терра КП. Версия 4.1» – один из дисков:
    - «С-Терра Шлюз ST КС1, КС2. Версия 4.1. Релиз 14905»;
    - «С-Терра Шлюз ST КС3. Версия 4.1. Релиз 14905»;
- комплект для восстановления – CD «S-Terra Gate Disk Image» (образ SSF-диска и Приложение к Инструкции по восстановлению);
- ПО для восстановления – CD «S-Terra Gate Recovery CD» (ПО для восстановления образа диска и Инструкция по восстановлению) [1].

В печатном виде поставляются:

- Копия сертификата соответствия ФСБ России;
- Копия сертификата ФСТЭК на «Программный комплекс С-Терра Шлюз. Версия 4.1»;
- Голографический специальный защитный знак ФСТЭК России;
- Лицензия на использование «Программного комплекса С-Терра Шлюз. Версия 4.1»;
- Лицензионное соглашение о праве пользования «Программным комплексом С-Терра Шлюз. Версия 4.1» производства ООО «С-Терра СиЭсПи»;
- Инструкция по инициализации программного комплекса – «Инициализация С-Терра Шлюз» при первом старте»;
- Приложение к Инструкции по восстановлению ПАК.

В комплект поставки MM-1017-1000M-KC3 и MM-1017-3000-KC3 дополнительно входят:

- Идентификаторы DS1992 - 2 шт.;
- Считыватель – 1 шт.;
- Диск с ПО и документацией на СКЗИ «Соболь»;
- Документация на СКЗИ «Соболь» в печатном виде:
    - паспорт СКЗИ «Соболь»;
    - наклейка (ФСТЭК России);
    - копия сертификата ФСТЭК России;
- Ключ активации сервиса прямой технической поддержки уровня "Стандартный" для ПАК "Соболь".

[1] Кроме случаев поставки ПК «С-Терра Шлюз», предустановленного на СПДС-USB-01

5 Модификации

Табл. 1. Модификации устройств

Модификация Криптомаршрутизатора	Производительность шифрования (IMIX трафик), Мбит/с	Производительность шифрования (TCP трафик), Мбит/с	Класс защиты	Дополнительные элементы обеспечения класса защиты
MM-1017-1000M-КС1	200	до 340	КС1	-
MM-1017-1000M-КС2	200	до 340	КС2	СЗН «СПДС-USB-01»
MM-1017-1000M-КС3	200	до 340	КС3	ПАК «Соболь»
MM-1017-3000-КС1	370	до 600	КС1	-
MM-1017-3000-КС2	370	до 600	КС2	СЗН «СПДС-USB-01»
MM-1017-3000-КС3	370	до 600	КС3	ПАК «Соболь»

Криптомаршрутизаторы по умолчанию не оснащаются блоками питания. Блоки питания приобретаются отдельно.

Табл. 2. Дополнительно приобретаемые лицензии

Наименование	Тип лицензии
G-1000M-3000-CD-UPD-КС1	Лицензия для активации на Криптомаршрутизаторе версий MM-1017-1000M-КС1 режима Криптомаршрутизатора MM-1017-3000-КС1
G-1000M-3000-CD-UPD-КС2	Лицензия для активации на Криптомаршрутизаторе версий MM-1017-1000M-КС2 режима Криптомаршрутизатора MM-1017-3000-КС2
G-1000M-3000-CD-UPD-КС3	Лицензия для активации на Криптомаршрутизаторе версий MM-1017-1000M-КС3 режима Криптомаршрутизатора MM-1017-3000-КС3

6 Технические данные

6.1 Технические характеристики

6.1.1 Функциональные возможности

Интерфейсы:

- 10Base-T (IEEE 802.3);
- 100Base-TX(IEEE 802.3u);
- 1000Base-X (IEEE 802.3z);
- 1000Base-T (IEEE 802.3ab);
- 10GBase (IEEE 802.3ae).

Протоколы 2-го уровня:

- 802.1d (STP), 802.1w (RSTP);
- 802.1s (MSTP);
- MRPP;
- Root Guard;
- BPDU Forwarding;
- BPDU Guard;
- LLDP, LLDP-MED;
- UDLD;
- Loopback Detection;
- IGMP Snooping v1, v2, v3;
- IGMP Snooping Fast Leave;
- Multicast VLAN Registration (MVR);
- MLD Snooping v1, v2;
- DHCP Snooping;
- DHCP relay;
- DHCP опции 37, 38, 82;
- промежуточный агент PPPoE;
- 802.3ad (LACP) агрегация портов: до 128 групп, до 8 портов в группе;
- управление потоком: 802.3x, backpressure;
- предотвращение блокировки (HOL).

VLAN:

- 802.1Q;
- 802.1Q-in-Q: на основе портов, Selective, Flexible;
- GARP, GVRP;
- количество поддерживаемых VLAN: 4095;
- VLAN на основе портов;
- VLAN на основе протокола (по содержимому поля EtherType);
- VLAN Translation;
- MAC VLAN;
- Voice VLAN;
- Private VLAN.

Маршрутизация:

- количество поддерживаемых L3 интерфейсов: 1024;
- таблица маршрутизации: 13312 записей;
- IPv4 и IPv6;
- Black hole route;
- RIP v1/v2;
- OSPF v2/v3;
- BGP4/BGP4+;
- VRRP/VRRPv3;
- ISATAP tunnel, GRE tunnel;
- BFD;
- статическая маршрутизация;
- PBR.

IPv6:

- IPv6 списки доступа;
- QoS на основе IPv6;
- IPv6 MVR;
- IPv6 MLD snooping;
- IPv6 ND snooping;
- IPv6 Stateless Auto Configuration;
- IPv6 ICMP;
- IPv6 ND;
- IPv6 Multicast Address Types.

Многоадресная рассылка:

- статические маршруты;
- PIM-DM, PIM-SM, PIM-SSM, MSDP.

Качество обслуживания (QoS):

- классификация трафика на основе: номера порта, MAC-адреса источника и назначения, VLAN ID, 802.1p, IPv4-адреса источника и назначения, IPv6-адреса источника и назначения, номера порта TCP/UDP, типа протокола, DiffServ (ToS, IP precedence), временного диапазона;
- ограничения полосы пропускания с шагом 1 кбит/с;
- количество очередей на каждом порту: 8;
- типы очередей: Strict Priority, WRR, SWRR, DWRR, SDWRR, WRED;
- полисинг трафика.

Сетевые службы и протоколы:

- NAT/NAT-T;
- PAT;
- DHCP-сервер, DHCP-клиент;
- межсетевой экран.

Аутентификация:

- ГОСТ Р 34.10-2012;
- AAA (RADIUS/TACACS+);
- списки контроля доступа (ACL);
- поддержка токенов: Aladdin, Актив, MultiSoft.

Криптографические библиотеки:

- ST — встроенная, компании «С-Терра СиЭсПи»;
- CP — внешняя, компании «КРИПТО-ПРО».

Криптографические алгоритмы:

- классы защищённости: КС1, КС2, КС3 (КС2, КС3 — при использовании АПМДЗ);
- шифрование: ГОСТ 28147-89, DES-CBC (IV32), 3DES-K168-CBC, IDEA-CBC, AES-K128-CBC, AES-K192-CBC, AES-K256-CBC, NULL;
- ЭП: DSA, RSA, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;
- контроль целостности: MD5, SHA1, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012;
- совместимость с PKI и LDAP службами зарубежных и российских производителей;
- комбинированное преобразование ESP_GOST-4M-IMIT.

VPN:

- IP/IP туннели;
- IP/GRE туннели;
- DMVPN;
- количество IPssec туннелей: в зависимости от типа лицензии.

Управление и контроль работы:

- С-Терра КП 4.1;
- командная строка (CLI), два уровня доступа: мониторинг, управление;
- Telnet;
- SSH;
- Console;
- Web-интерфейс (SSL);
- IPv4/v6-управление;

- BootP/DHCP-клиент;
- SNMP v1, v2c, v3;
- SNMP Trap;
- Dying GASP;
- RMON v1, v2, v3, v9;
- локальный журнал событий;
- Syslog;
- sFlow;
- TFTP/FTP-клиент;
- TFTP/FTP-сервер;
- DHCP-сервер;
- Telnet-сервер;
- DNS Relay;
- DNS client;
- SNTP/NTP;
- зеркалирование портов (SPAN/RSPAN): one-to-one, many-to-one, на основе потока трафика;
- OAM 802.3ah, 802.3ag;
- IEEE 802.3a (Energy Efficient Ethernet).

6.1.2 Конструктивное исполнение и электропитание

Криптомаршрутизатор выполнен в металлическом корпусе с габаритными размерами 440x490x44 мм, массой не более 6 кг. Криптомаршрутизатор имеет активное охлаждение.
Питание Криптомаршрутизатора осуществляется с помощью сменных блоков питания. Виды данных блоков питания приведены в Табл. 3.

Табл. 3 Модификации блоков питания

Модификация	Мощность, Вт	Напряжение электропитания
ZES-3-PSM-AC220-150W	150	~100..240В, 50..60 Гц
ZES-3-PSM-DCH-150W	150	=36…72В

Криптомаршрутизатор поддерживает «горячую» замену блоков питания.

6.1.3 Условия эксплуатации

Условия эксплуатации изделий:
- температура окружающей среды — от 0 до 50 °С;
- относительная влажность воздуха — от 5 до 95 % без конденсата;
- режим работы — круглосуточный;
- наработка на отказ — 50000 часов.

Криптомаршрутизатор должен быть подключен к системе электропитания с заземлением.

6.2 Порты изделия

6.2.1 Порт Ethernet модуля коммутации

- физический интерфейс: 10Base-T/100Base-TX/1000Base-T;
- режимы обмена: полудуплексный или дуплексный;
- автоматическое согласование параметров (AutoNegotiation) 802.3/802.3u;
- авто MDI/MDI-X;
- тип разъема: розетка RJ-45 (назначение контактов указано в пункте 14.1).

6.2.2 SFP+ слот модуля коммутации

SFP+ слот предназначен для установки SFP/SFP+ модулей.
- SFP-слот соответствует спецификации: SFF-8074i;
- скорость передачи: 1/10 Гбит/с.

Допускается “горячая” замена модуля (hot-swap).

6.2.3 Порт Console модуля коммутации

Порт Console шлюза выполняет функции устройства типа DCE и имеет цифровой интерфейс RS-232 (разъем RJ-45).

- скорость асинхронного обмена — 115200 бит/с;
- количество битов данных — 8;
- контроль по четности или нечетности отсутствует;
- количество стоп-битов — 1;
- управление потоком данных отсутствует.

6.2.4 Порт MGMT модуля коммутации

Порт предназначен для внеполосного управления модулем коммутации по протоколам telnet, ssh и через web-интерфейс.

- физический интерфейс: 10Base-T/100Base-TX/1000Base-T,
- тип разъема: розетка RJ-45.

6.2.5 Порт Alarm модуля коммутации

Содержит разъем типа «сухой контакт», предназначенный для сигнализации об аварии в модуле коммутации.

- тип разъема: розетка RJ-45.

6.2.6 Порт USB модуля коммутации

Порт предназначен для подключения внешнего накопителя к модулю коммутации.

- тип разъема: USB тип A.

6.2.7 Порт Ethernet криптомодуля

- физический интерфейс: 10Base-T/100Base-TX/1000Base-T;
- режимы обмена: полудуплексный или дуплексный;
- автоматическое согласование параметров (AutoNegotiation) 802.3/802.3u;
- авто MDI/MDI-X;
- тип разъема: розетка RJ-45 (назначение контактов указано в пункте 14.1).

6.2.8 Консольный порт COM1 криптомодуля

Порт COM1 шлюза выполняет функции устройства типа DTE и имеет цифровой интерфейс RS-232 (разъем DB-9M).

- скорость асинхронного обмена — 115200 бит/с;
- количество битов данных — 8;
- контроль по четности или нечетности отсутствует;
- количество стоп-битов — 1;
- управление потоком данных отсутствует.

6.2.9 Порт KEY криптомодуля

Порт предназначен для подключения к криптомодулю внешнего считывателя идентификатора.

- тип разъема: RJ-12.

6.2.10 Порт USB криптомодуля

Порт предназначен для подключения внешних устройств к криптомодулю.

- тип разъема: USB тип A.

6.2.11 Порт VGA криптомодуля

Порт предназначен для подключения монитора к криптомодулю.

- тип разъема: DE15F.

6.3 Внешний вид

6.3.1 Передняя панель

На передней панели расположены следующие элементы:

- светодиодные индикаторы;
- разъемы портов Ethernet;
- разъемы SFP+ слотов;
- разъемы SFP слотов;
- разъем порта Console;
- разъем USB;
- разъем порта Alarm;
- утопленная кнопка Mode;
- разъем COM1;
- утопленная кнопка RST.

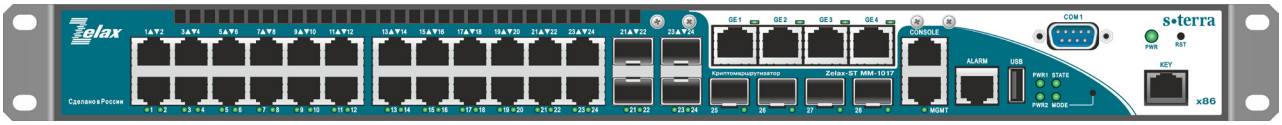


Рис. 6 Вид передней панели MM-1017

6.3.2 Индикаторы, расположенные на передней панели

На передней панели изделия расположены следующие индикаторы: PWR, PWR1, PWR2, STATE, LNK/ACT, MODE, FAN.

Табл. 4. Описание индикаторов передней панели ZES-32xx

Индикатор	Состояние	Описание
LNK/ACT	Мигает	Линия исправна, идёт приём/передача данных
	Светится	Линия исправна, данные не передаются
	Не светится	Порт выключен
PWR1/PWR2	Светится	Напряжение питания подано
	Не светится	Напряжение питания отсутствует
PWR	Светится	Напряжение питания подано на криптомодуль
	Не светится	Напряжение питания отсутствует подано на криптомодуле
STATE	Мигает	Инициализация модуля коммутации
	Светится	Модуль коммутации работает нормально.
MODE	Мигает	Включен режим отображения состояния PoE на светодиодах LNK/ACT портов модуля коммутации. В данной модификации PoE не поддерживается.
	Не светится	Отключен режим отображения состояния PoE на светодиодах LNK/ACT портов модуля коммутации. В данной модификации PoE не поддерживается.

6.3.3 Задняя панель

На задней панели расположены следующие элементы:

- два слота для установки сменных блоков питания;
- порт VGA;
- четыре разъёма USB;
- клемма заземления.

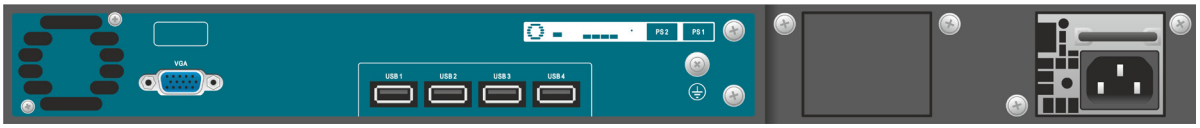


Рис. 7 Вид задней панели MM-1017 с установленным блоком питания

7 Установка и подключение Криптомаршрутизатора

Установка Криптомаршрутизатора должна производиться в сухом отапливаемом помещении. Перед установкой необходимо произвести внешний осмотр Криптомаршрутизатора с целью выявления механических повреждений корпуса и соединительных элементов.

Перед подключением Криптомаршрутизатора следует внимательно изучить настоящее руководство.

Если Криптомаршрутизатор хранился при температуре ниже 0 С, перед первым включением его необходимо выдержать при комнатной температуре не менее двух часов.

7.1 Установка

Установите Криптомаршрутизатор в 19-дюймовую стойку или на ровную поверхность (например, стол).

Следует иметь в виду, что:

- каждое устройство в стойке при работе выделяет тепло, поэтому устройства не должны размещаться в стойке вплотную;
- детали стойки или расположенных в ней устройств не должны закрывать вентиляционные отверстия Криптомаршрутизатора.

7.2 Подключение

Последовательность подключения:

- установите сменный блок питания, предварительно сняв защитную планку на задней панели Криптомаршрутизатора;
- разъём IEC C13 кабеля питания (входящего в комплект поставки) вставьте в разъём на блоке питания Криптомаршрутизатора. Вставьте вилку на другом конце кабеля питания в розетку электросети;
- убедитесь в том, что на передней панели Криптомаршрутизатора светится индикатор PWR, а также индикаторы PWR1/PWR2 в соответствии с используемыми блоками питания;
- после подачи питания Криптомаршрутизатор выполняет процедуру самотестирования и начальной загрузки.

7.3 Начальная загрузка криптомодуля

Процесс начальной загрузки криптомодуля для разных классов защиты описан в документе «Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64», а именно:

для класса защиты КС1 – раздел «Подготовка ПАК исполнения класса защиты КС1 к инициализации»;

для класса защиты КС2 с S-Terra Gate на СЗН «СПДС-USB-01» – раздел «Подготовка ПАК исполнения класса защиты КС1, КС2 с СЗН «СПДС-USB-01» к инициализации»;

для класса защиты КС3 – раздел «Подготовка ПАК исполнения класса защиты КС3 к инициализации».

8 Управление

Управление модулем коммутации и криптомодулем осуществляется независимо.

8.1 Управление модулем коммутации

8.1.1 Способы управления

Настройка параметров и управление модулем коммутации осуществляется:

- через порт Console при подключении к нему внешнего терминала, в качестве которого может использоваться персональный компьютер;
- через любой порт Ethernet. При подключении через порт Ethernet, управление осуществляется посредством SNMP, Telnet, SSH или Web-интерфейса.

Внимание! Для подключения через порт Ethernet необходимо создать интерфейс VLAN (см. п. 8.1.1.2) и присвоить ему IP-адрес.

8.1.1.1 Управление через порт Console

Управление модулем коммутации осуществляется через порт Console, к которому подключается устройство типа DTE, выполняющее функцию терминала (далее для краткости это устройство именуется терминалом). Подключение терминала к порту Console изделия производится с помощью консольного кабеля RJ-45, поставляемого в комплекте с Криптомаршрутизатором.

Порт терминала должен быть настроен следующим образом:

- асинхронная скорость передачи данных должна быть равна 115200 бит/с;
- число битов данных — 8;
- контроль по четности или нечётности отсутствует;
- число стоп-битов — 1;
- управление потоком данных отсутствует.

8.1.1.2 Настройка модуля коммутации для управления

1. Присвоение IP-адреса интерфейсу VLAN1.

```
switch>en
switch#config terminal
switch(config)#interface vlan 1
switch(config-if-vlan1)#ip address 172.25.1.201 255.255.255.0
```

2. Создание учетной записи пользователя.

```
switch>en
switch#config terminal
switch(config)#username admin privilege 15 password 0 1234
```

Внимание! После завершения этапов 1 и 2 следует выполнить команду **write**, чтобы сохранить настройки в энергонезависимую память.

8.1.1.3 Управление по протоколам Telnet, SSH и SNMP

Управление модулем коммутации посредством протоколов Telnet, SSH и SNMP осуществляется через порт Ethernet. Для управления модулем коммутации по протоколу Telnet могут использоваться программы Telnet или Hyper Terminal, входящие в операционную систему Windows или аналогичные программы других систем. Перед подключением через порт Ethernet необходимо создать интерфейс VLAN и присвоить ему IP-адрес (см. п. 8.1.1.2).

Для управления посредством протоколов SSH и SNMP на модуле коммутации должны быть произведены дополнительные настройки, описанные в соответствующих разделах руководства по настройке.

8.1.1.4 Управление через Web-интерфейс

Управление модулем коммутации посредством Web-интерфейса осуществляется через порты Ethernet. Для управления модулем коммутации через Web-интерфейс можно использовать браузер (например, Chrome, Mozilla, Safari, Internet Explorer, Opera и т.п.). Перед подключением через порт Ethernet необходимо создать интерфейс VLAN и присвоить ему IP-адрес (см. п. 8.1.1.2). Функция HTTPS-сервера включена на модуле коммутации по умолчанию.

8.1.2 Интерфейс пользователя и режимы работы

Интерфейс пользователя основан на использовании командной строки (CLI — Command Line Interface). Пользователь вводит команду в виде последовательности символов в командной строке, расположенной в нижней части экрана терминала. Результаты выполнения команды выводятся в оставшуюся часть экрана, при этом текст сообщений сдвигается снизу (от командной строки) вверх по мере его поступления.

Для разграничения прав доступа к командам управления существуют два режима:

- пользовательский режим, при котором разрешён доступ к командам мониторинга. В этом режиме нельзя изменять конфигурацию модуля коммутации;
- привилегированный режим, при котором разрешён доступ к командам мониторинга и изменения конфигурации модуля коммутации.

В Табл. 5 приведены основные режимы управления, команды входа и выхода из них и состояние командной строки.

Табл. 5. Режимы управления

Режим	Вход осуществляется	Вид командной строки	Описание	Выход из режима выполняется
Пользовательский	нажатием клавиши “Enter”	Switch>	Доступны команды мониторинга	-
Привилегированный	в пользовательском режиме выполнением команды enable	Switch#	Доступны команды мониторинга и настройки, а также режимы конфигурирования	командой exit
Конфигурирования общесистемных параметров модуля коммутации	в привилегированном режиме выполнением команды configure terminal	Switch(config)#	Доступны команды настройки общесистемных параметров модуля коммутации	командой exit
Конфигурирования интерфейсов	в режиме конфигурирования общесистемных параметров модуля коммутации выполнением команды interface с указанием типа и номера интерфейса	Switch(config-if)#	Доступны команды настройки параметров интерфейсов	командой exit
Настройки пула адресов DHCP	в режиме конфигурирования общесистемных параметров модуля коммутации выполнением команды ip dhcp pool <name>	Switch(dhcp-name-config)#	Доступны команды настройки параметров пула dhcp	командой exit
Настройки списков доступа	в режиме конфигурирования общесистемных параметров модуля	Switch(config-ip-std-nacl-name)# или Switch(config-	Доступны команды настройки параметров стандартного и	командой exit

	коммутации выполнением команды ip access-list {standard | extended} <name>	ip-ext-nacl-name)#	расширенного списков доступа	
Настройки маршрутизации	в режиме конфигурирования общесистемных параметров модуля коммутации выполнением команды router bgp | ipv6 | ldp | msdp | ospf | rip | vrrp	switch(config-router)#	Доступны команды настройки параметров протоколов маршрутизации	командой exit

8.1.2.1 Синтаксис команд

Синтаксис команд, вводимых в командной стоке модуля коммутации:

команда <переменная> { **параметр** | … | параметр } [**параметр**]

где:

Команда — строго заданная последовательность символов, определяющая дальнейшие параметры.

Параметр — ключевое слово, IP-адрес, маска сети, IP-адрес с маской, MAC-адрес, число, слово, строка.

Команда и параметры отделяются друг от друга пробелами.

При описании синтаксиса команд используются следующие обозначения:
- в фигурных скобках {} указываются обязательные параметры;
- в квадратных скобках [] указываются необязательные параметры;
- символ “|” обозначает логическое “или” — выбор между различными параметрами;
- ключевые слова выделяются жирным шрифтом.

Для исполнения набранной команды необходимо нажать клавишу “Enter”.

Для получения контекстной справки используется символ “?”.

При нажатии клавиши табуляции “Tab” происходит автоматическое доопределение сокращенных названий команд и некоторых типов параметров до их полного вида, или, в случае, когда несколько команд начинаются с одинаковых символов, до их общей части.

Последние десять введенных команд хранятся в буфере. Чтобы воспользоваться ранее введенной командой, необходимо нажать клавишу “↑” (вверх) или “↓” (вниз).

8.1.2.2 Контекстная справка

Для получения контекстной справки используется символ “?”. Данная операция доступна во всех режимах.

При вводе символа “?” выводится список команд, доступных в данном режиме.

Пример. Использование контекстной справки для получения списка команд, доступных в пользовательском режиме.

```
switch>?
Exec commands:
  clear               Reset functions
  copy                Copy file
  crypto              Ssh crypto key clear command
  debug               Debugging functions
  disable             Turn off privileged mode command
  enable              Turn on privileged mode command
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  no                  Negate a command or set its default
```

```
  ping                Send ipv4 echo messages
  ping6               Send ipv6 echo messages
  public-key          public key
  show                Show running system information
  telnet              Connect remote computer
  traceroute          Trace route to destination
  traceroute6         Trace route to IPv6 destination
  virtual-cable-test  Start virtual cable test
  who                 Display who is on vty
```

При вводе символа “?” через пробел после команды выводится список параметров данной команды.

Пример. Использование контекстной справки для получения списка параметров команды **copy**.

```
switch#copy ?
  WORD            Copy source file name, <1-128> character(local-filename or
                  ftp://user:password@ip|host-name/remote-filename or
                  tftp://ip|host-name/remote-filename or
                  sftp://user:password@ip|host-name/remote-filename).
  running-config  Copy from current system configuration
```

8.1.2.3 Сообщения об ошибках

В Табл. 6 приведены сообщения об ошибках, которые могут выводиться во время работы с командной строкой.

Табл. 6. Сообщения об ошибках, выводимые при работе с командной строкой

Сообщение об ошибке	Описание ошибки
Unrecognized command or illegal parameter!	Введенная команда не существует, либо имеется ошибка в области значений параметра, его формате или типе
Ambiguous command	Возможно не менее двух интерпретаций введенной команды
Invalid command or parameter	Команда распознана, однако не найдено правильной записи параметра
This command is not exist in current mode	Команда распознана, однако такая команда не может использоваться в текущем режиме.
Please configure precursor command "*" at first!	Команда распознана, однако предварительные условия, необходимые для выполнения этой команды, еще не созданы
syntax error : missing "" before the end of command line!	Знаки двойных кавычек не образуют пару

8.2 Управление криптомодулем

8.2.1 Способы управления

Настройка параметров и управление криптомодулем осуществляется:

- через консольный порт COM1 при подключении к нему внешнего терминала, в качестве которого может использоваться персональный компьютер;
- через любой порт Ethernet. При подключении через порт Ethernet, управление осуществляется посредством SSH или удаленно централизованно с использованием «Программного продукта С-Терра КП. Версия 4.1».

8.2.1.1 Управление через порт COM1

Управление криптомодулем осуществляется через порт COM1, к которому подключается устройство типа DTE, выполняющее функцию терминала (далее для краткости это устройство именуется терминалом). Подключение терминала к порту COM1 изделия производится с помощью консольного кабеля RJ-45 и переходника A-006, к которому подключается консольный кабель, поставляемый в комплекте с Криптомаршрутизатором.

Порт терминала должен быть настроен следующим образом:
- асинхронная скорость передачи данных должна быть равна 115200 бит/с;
- число битов данных — 8;
- контроль по четности или нечётности отсутствует;
- число стоп-битов — 1;
- управление потоком данных отсутствует.

Локально настройка криптомодуля выполняется в следующем порядке:
1. Выполните инициализацию продукта С-Терра Шлюз на криптомодуле согласно документу «Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64» и разделу «Инициализация S-Terra Gate при первом старте».
2. При использовании С-Терра Шлюз класса защиты КС3 выполните разграничение прав доступа к ОС и управлению, используя раздел «Разграничение доступа» документа документу «Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64».
3. Выполните настройки интерфейсов, изменение паролей и др., следуя документу «Настройка шлюза».
4. Создайте политику безопасности криптомодуля, используя сценарии, размещенные на сайте http://www.s-terra.ru/resheniya/application_scenarios_products/ и http://www.s-terra.ru/resheniya/product_features/, а также описание команд в документе «Cisco-like команды”, или создание политики безопасности в виде текстового файла, представленного в документе «Создание конфигурационного файла».
5. При выходе из конфигурационного режима консоли произойдет загрузка конфигурации. Текстовый конфигурационный файл загружается командой lsp_mgr load, описанной в документе «Специализированные утилиты».

8.2.1.2 Удаленное централизованное управление

Удаленное централизованное управление криптомодулем осуществляется с использованием «Программного продукта С-Терра КП. Версия 4.1». С-Терра КП состоит из двух частей – Сервера управления и Клиента управления, который устанавливается на криптомодуль. Связь между Клиентом управления и Сервером управления происходит по защищенному каналу IPsec.

Настройка криптомодуля выполняется в следующем порядке:
6. Выполните локально инициализацию продукта С-Терра Шлюз на криптомодуле согласно документу «Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64» и разделу «Инициализация S-Terra Gate при первом старте».
7. При использовании С-Терра Шлюз класса защиты КС3 выполните разграничение прав доступа к ОС и управлению, используя раздел «Разграничение доступа» документа документу «Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64».
8. Выполните настройки интерфейсов, изменение паролей и др., следуя документу «Настройка шлюза».
9. Создайте доверенный защищенный канал для управления, описанный в разделе «Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза» документа «Настройка шлюза».
10. Создайте политику безопасности криптомодуля, используя сценарии, размещенные на сайте http://www.s-terra.ru/resheniya/application_scenarios_products/ и http://www.s-terra.ru/resheniya/product_features/., а также описание команд в документе «Cisco-like команды”, или создание политики безопасности в виде текстового файла, представленного в документе «Создание конфигурационного файла», «Специализированные утилиты».
11. При выходе из конфигурационного режима произойдет загрузка конфигурации.

8.2.1.3 Управление по протоколу SSH

Управление криптомодулем посредством протокола SSH осуществляется через порт Ethernet. Для управления устройством по протоколу SSH могут использоваться программы Putty, Hyper Terminal, входящие в операционную систему Windows, или другие. Удаленное управление должно выполняться по доверенному защищенному каналу IPsec, для построения которого используется продукт С-Терра Клиент, устанавливаемый на рабочем месте администратора.

Настройка криптомодуля выполняется в следующем порядке:

1. Выполните локально инициализацию продукта С-Терра Шлюз на криптомодуле согласно документу «Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64» и разделу «Инициализация S-Terra Gate при первом старте».
2. При использовании С-Терра Шлюз класса защиты КС3 выполните разграничение прав доступа к ОС и управлению, используя раздел «Разграничение доступа» документа документу «Инициализация S-Terra Gate на вычислительных системах архитектуры Intel x86/x86-64».
3. Выполните настройки интерфейсов, изменение паролей и др., следуя документу «Настройка шлюза».
4. Создайте доверенный защищенный канал для управления, описанный в разделе «Построение VPN туннеля между шлюзом S-Terra Gate 4.1 и рабочим местом администратора для удаленной настройки шлюза» документа «Настройка шлюза».
5. Создайте политику безопасности криптомодуля, используя сценарии, размещенные на сайте http://www.s-terra.ru/resheniya/application_scenarios_products/ и http://www.s-terra.ru/resheniya/product_features/., а также описание команд в документе «Cisco-like команды", или создание политики безопасности в виде текстового файла, представленного в документе «Создание конфигурационного файла», «Специализированные утилиты».
6. При выходе из конфигурационного режима произойдет загрузка конфигурации.

8.2.2 Интерфейс пользователя и режимы работы

Интерфейс пользователя при управлении через порт COM1 и SSH основан на использовании командной строки (CLI — Command Line Interface).

Для разграничения прав доступа к командам управления существуют два режима:

- пользовательский режим, при котором разрешён доступ к командам мониторинга. В этом режиме нельзя изменять настройки шлюза;
- привилегированный режим, при котором разрешён доступ к командам настройки терминала, системным командам, управления соединениями, работы с конфигурацией, задания политики безопасности шлюза.

В Табл. 7 приведены основные режимы управления, команды входа и выхода из них и состояние командной строки.

Табл. 7. Режимы управления

Режим	Вход осуществляется	Вид командной строки	Описание	Выход из режима выполняется
Пользовательский	cs_console	sterragate>	Доступны команды мониторинга	-
Привилегированный	в пользовательском режиме выполнением команды enable и паролем по умолчанию “csp”	sterragate#	Доступны команды мониторинга и настройки, а также режимы конфигурирования	командой exit
Конфигурирование общесистемных параметров	в привилегированном режиме выполнением команды configure terminal	sterragate(config)#	Доступны команды настройки политики безопасности	командой end
Конфигурирования интерфейсов	в режиме конфигурирования общесистемных параметров выполнением команды interface с указанием типа и	sterragate(config-if)#	Доступны команды настройки параметров интерфейсов	командой exit

	номера интерфейса			
Настройки списков доступа	в режиме конфигурирования выполнением команды ip access-list {standard | extended} <name>	sterragate (config-ip-std-nacl)# или Switch(config-ip-ext-nacl)#	Доступны команды настройки параметров стандартного и расширенного списков доступа	командой exit
Настройки ISAKMP политики	в режиме конфигурирования выполнением команды crypto isakmp policy	sterragate (config-isakmp)#	Доступны команды настройки для защиты обменов первой фазы IKE	командой exit
Настройки IPsec политики	в режиме конфигурирования выполнением команды crypto map	sterragate (config-crypto-map)#	Доступны команды настройки для защиты обменов второй фазы IKE	командой exit
Настройки QoS	в режиме конфигурирования выполнением команды class map	sterragate (config-cmap)#	Доступны команды классификации и маркирования трафика	

8.2.2.1 Контекстная справка

Для получения контекстной справки используется символ “?”. Данная операция доступна во всех режимах.

При вводе символа “?” выводится список команд, доступных в данном режиме.

8.2.2.2 Сообщения об ошибках

Все сообщения об ошибках, которые могут выводиться во время работы с командной строкой, представлены в документе с описанием команд «Cisco-like команды».

9 Сохранение и загрузка конфигурации

9.1 Сохранение и загрузка конфигурации модуля коммутации

Все действия, описанные в этом разделе, доступны как через интерфейс командной строки (CLI), так и через Web-интерфейс.

9.1.1 Сохранение конфигурации

Во избежание потери рабочей конфигурации, связанной с перезагрузкой или отключением питания, выполните команду **copy running-config startup-config** или **write**.

Пример. Сохранение рабочей конфигурации.

```
switch#copy running-config startup-config
Write running-config to current startup-config successful
switch#%Jan 01 00:10:16 2006 Write configuration successfully!
```

9.1.2 Сохранение конфигурации на сервере

Процедура сохранения конфигурации заключается в копировании файла с настройками из энергонезависимой памяти модуля коммутации (Flash-память) на сервер. При этом используется один из протоколов FTP (File Transfer Protocol) или TFTP (Trivial File Transfer Protocol).

Для сохранения файла с настройками выполните следующие действия:

1. Включите сервер FTP/TFTP.
2. Подключите один из портов модуля коммутации к сети. Примеры подключения показаны на Рис. 8.

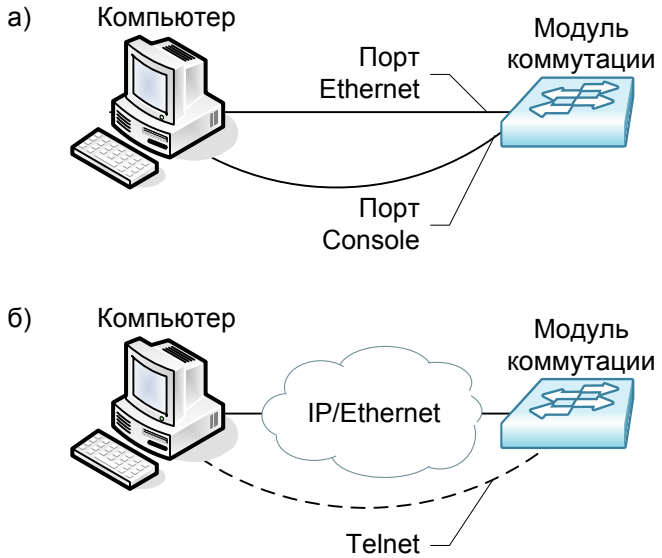


Рис. 8. Примеры подключения модуля коммутации для сохранения и загрузки конфигурации или обновления программного обеспечения

3. Настройте модуль коммутации для управления (см. п. 8.1.1.2).
4. Скопируйте файл с настройками на сервер TFTP, используя команду copy с указанием следующих параметров:
   - тип конфигурации: running-config — рабочая конфигурация или startup-config — загрузочная конфигурация;
   - тип сервера, на который будет производиться сохранение: tftp — сервер TFTP;
   - IP-адрес сервера;
   - имя сохраняемого файла.

Пример. Сохранение рабочей конфигурации в файл с именем backup-config.cfg на сервер TFTP, имеющий IP-адрес 172.25.1.100.

```
switch#copy running-config tftp://172.25.1.100/backup-config.cfg
Confirm copy file [Y/N]:y
Begin to send file, please wait...

File transfer complete.
close tftp client.
switch#
```

9.1.3 Загрузка конфигурации с сервера

Процедура загрузки конфигурации заключается в копировании файла с настройками с сервера в энергонезависимую память модуля коммутации (Flash-память). При этом используется TFTP (Trivial File Transfer Protocol).

Для загрузки файла с настройками выполните следующие действия:

1. Включите на компьютере сервер TFTP.
2. Подключите один из портов модуля коммутации к сети. Примеры подключения показаны на Рис. 8.
3. Настройте модуль коммутации для управления (см. п. 8.1.1.2).
4. Скопируйте файл с настройками с сервера FTP/TFTP, используя команду copy с указанием следующих параметров:
   - тип сервера, с которого будет производиться копирование: ftp — сервер FTP или tftp — сервер TFTP;
   - файл, в который будут скопированы настройки: startup.cfg — загрузочная конфигурация;
   - IP-адрес сервера;
   - имя копируемого файла.

Пример. Загрузка настроек из файла с именем backup-config.cfg с сервера TFTP, имеющего IP-адрес 172.16.1.100, в загрузочную конфигурацию модуля коммутации.

```
switch#copy tftp://172.25.1.100/backup-config.cfg startup.cfg
Confirm to overwrite the existed destination file?  [Y/N]:y
Begin to receive file, please wait...

File transfer complete.
Recv total 1071 bytes
Write ok.
close tftp client.
```

9.2 Сохранение и загрузка конфигурации криптомодуля

9.2.1 Сохранение конфигурации

При управлении с использованием командной строки во избежание потери рабочей cisco-like конфигурации, связанной с перезагрузкой или отключением питания, выполните команду: **copy running-config file**.

Пример. Сохранение рабочей конфигурации в файл test1, выполняется в привилегированном режиме cisco-like консоли.

```
sterragate#copy running-config file:test1
```

При управлении с использованием командной строки рабочую конфигурацию можно сохранить в виде LSP-конфигурации в текстовом виде, выполнив команду **lsp_mgr show**.

Пример. Сохранение рабочей конфигурации в файл /var/cspvpn/test2.lsp, выполняется из bash.

```
sterragate# /opt/VPNagent/bin/lsp_mgr show > /var/cspvpn/test2.lsp
```

Сохраненные конфигурации можно хранить на внешнем носителе или сервере.

9.2.2 Сохранение конфигурации на Сервере управления

При управлении шлюзом с использованием «Программного продукта С-Терра КП. Версия 4.1» созданную конфигурацию можно сохранить на Сервере управления в виде целого проекта во вкладке VPN data maker, используя предложение меню Save as.

9.2.3 Загрузка конфигурации

Процедура загрузки сохраненной cisco-like конфигурации заключается в копировании файла на SSD-диск или СЗН «СПДС-USB-01» и выполнении команды configure replace file.

Пример. Загрузка рабочей cisco-like конфигурации из файла test1, выполняется в привилегированном режиме cisco-like консоли.

```
sterragate#configure replace file file:test1
```

Загрузка сохраненной LSP-конфигурации заключается в копировании файла на SSD-диск или СЗН «СПДС-USB-01» и выполнении команды **lsp_mgr load**.

Пример. Загрузка рабочей LSP-конфигурации из файла /var/cspvpn/test2.lsp, выполняется из bash.

```
sterragate# /opt/VPNagent/bin/lsp_mgr load –f /var/cspvpn/test2.lsp
```

9.2.4 Загрузка конфигурации с Сервера управления

Загрузка сохраненной конфигурации на Сервере управления выполняется обычным штатным образом, описанным в документе «Программный продукт С-Терра КП. Версия 4.1».

10 Восстановление заводских настроек

10.1 Восстановление заводских настроек модуля коммутации

10.1.1 Восстановление заводской конфигурации с использованием командной строки

При необходимости возврата модуля коммутации к заводским настройкам выполните последовательность команд **set default,** после чего команды **write** и **reload**.

Пример. Возврат к заводским настройкам.

```
Switch#set default
Are you sure? [Y/N] = y
Switch#write
Switch#%Sep 04 10:45:10 2015 Switch configuration has been set default!
```

10.1.2 Сброс пароля с использованием загрузчика

В случае, когда пароль на доступ в привилегированный режим модуля коммутации утрачен, можно выполнить временный сброс пароля до следующей перезагрузки. Для этого выполните следующие действия:

1. Во время загрузки модуля коммутации нажмите на клавиатуре сочетание клавиш “ctrl+b” для перехода в режим BootROM и дождитесь появления приглашения [Boot];
2. Выполните скрытую команду nopassword;
3. Выполните команду run.

Пример. Сброс пароля и загрузка с использованием загрузчика.

```
[Boot]: nopassword
clear password ok

[Boot]: run

Loading flash:/nos.img ...
```

Модуль коммутации будет загружен и, при переходе в привилегированный режим, пароль не будет запрашиваться. После чего можно изменить пароль с помощью команды enable password.

10.2 Восстановление заводских настроек криптомодуля

10.2.1 Восстановление заводской конфигурации

При необходимости возврата устройства к заводским настройкам необходимо выполнить процедуру восстановления, описанную в разделе «Инструкция по восстановлению и обновлению ПАК с использованием UP_Flash» документа «Инструкции по восстановлению и обновлению ПАК».

11 Загрузка новой версии программного обеспечения

Загрузка новой версии программного обеспечения криптомодуля не предусмотрена, так как во время сертификации происходит фиксация контрольных сумм программного кода.

11.1 Загрузка новой версии программного обеспечения в модуль коммутации

Обновление ПО модуля коммутации можно выполнить двумя способами - с использованием интерфейса командной строки (CLI) либо в режиме загрузчика (BootROM). Процесс обновления заключается в копировании файлов с сервера во Flash-память модуля коммутации. При этом используется один из протоколов FTP (File Transfer Protocol) или TFTP (Trivial File Transfer Protocol).

ПО состоит из двух файлов:

- nos.img - файл образа системы, содержит драйверы аппаратного обеспечения модуля коммутации и ПО текущей версии;
- boot.rom - загрузчик системы модуля коммутации.

11.1.1 Обновление модуля коммутации с использованием командной строки

Для загрузки программного обеспечения выполните следующие действия:

1. Подключите компьютер, содержащий архив программного обеспечения, к модулю коммутации как показано на Рис. 8.
2. Включите на компьютере сервер FTP/TFTP.
3. Настройте модуль коммутации для управления (см. п. 8.1.1.2).
4. Выполните загрузку файла boot.rom (команда copy):

```
switch#copy tftp://172.25.1.100/boot.rom boot.rom
Confirm to overwrite the existed destination file?  [Y/N]:y
Begin to receive file, please wait...
#########################################################################
#########
File transfer complete.
Recv total 437376 bytes

Begin to write local file, please wait...

Write ok.
close tftp client.
```

5. Выполните загрузку файла nos.img (команда copy):

```
switch#copy tftp://172.25.1.100/nos.img nos.img
Confirm to overwrite the existed destination file?  [Y/N]:y
Begin to receive file, please wait...
Get Img file size success, Img file size is:11888141(bytes).
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
#########################################################################
########
File transfer complete.
Recv total 11888141 bytes

Begin to write local file, please wait...

Write ok.
```

```
close tftp client.
```

6. Выполните перезагрузку модуля коммутации (команда reload).

11.1.2 Обновление модуля коммутации с использованием загрузчика

Внимание! В режиме загрузчика возможно обновление только файла boot.rom

Для загрузки программного обеспечения выполните следующие действия:

1. Подключите компьютер, содержащий архив программного обеспечения, к модулю коммутации к порту Management и Console.
2. Включите на компьютере сервер TFTP.
3. Во время загрузки модуля коммутации нажмите на клавиатуре сочетание клавиш “ctrl+b” для перехода в режим BootROM и дождитесь появления приглашения [Boot].

```
U-Boot 2011.12 (Apr 01 2015 - 11:04:21)

System is booting, please wait...

Net Initialization Skipped


Bootrom version: 7.2.16

Creation date: Apr  1 2015 - 11:04:19


Testing RAM...
0x08000000 RAM OK.

[Boot]:
```

4. Введите команду “setconfig”, чтобы задать IP-адрес модуля коммутации в режиме BootROM и IP-адрес сервера.

```
[Boot]: setconfig
Host IP Address: [10.1.1.1] 172.25.1.201
Server IP Address: [10.1.1.2] 172.25.1.100
```

5. Выполните загрузку и запись файла boot.rom (команды load и write).

```
[Boot]: load boot.rom
Using rtl8390#0 device
TFTP from server 172.25.1.100; our IP address is 172.25.1.201
Filename 'boot.rom'.
Load address: 0x81000000
Loading: ##############################
done
Bytes transferred = 437376 (6ac80 hex)
[Boot]: write boot.rom
File exists, overwrite? (Y/N)[N] y

Writing flash:/boot.rom...
0 bytes written, 437376 bytes skipped

Write flash:/boot.rom OK.
```

6. Выполните перезагрузку модуля коммутации (команда reboot).

12 Рекомендации по устранению неисправностей

Изделие представляет собой сложное микропроцессорное устройство, поэтому устранение неисправностей, если они не связаны с очевидными причинами возможно только на предприятии-изготовителе или в его представительствах.

При возникновении вопросов, связанных с эксплуатацией изделия, обращайтесь, пожалуйста, в службу технической поддержки компании С-Терра или компании Zelax.

13 Гарантии изготовителя

Изделие прошло предпродажный прогон в течение 168 часов. Изготовитель гарантирует соответствие изделия техническим характеристикам при соблюдении пользователем условий эксплуатации.

Срок гарантии указан в гарантийном талоне изготовителя.

Изготовитель обязуется в течение гарантийного срока безвозмездно устранять выявленные дефекты путём ремонта или замены изделия или его модулей.

Если в течение гарантийного срока:

- пользователем были нарушены условия эксплуатации, приведенные в п. 6.1.3, или на изделие были поданы питающие напряжения, не соответствующие указанным в п.6.1.2;
- изделию нанесены механические повреждения;
- порты изделия повреждены внешним опасным воздействием,

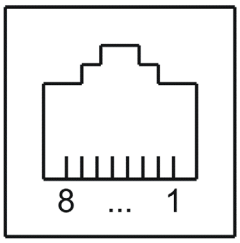
то ремонт осуществляется за счет пользователя.

Доставка неисправного изделия в ремонт осуществляется пользователем.

Гарантийное обслуживание прерывается, если пользователь произвел самостоятельный ремонт изделия (в том числе, замену встроенного предохранителя).

14 Приложения

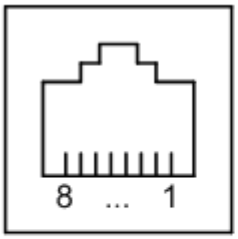
14.1 Приложение 1. Назначение контактов портов Ethernet 10/100/1000Base-T



Розетка RJ-45

Номер контакта	Наименование сигнала
1	Bi-directional A+ (приём-передача)
2	Bi-directional A- (приём-передача)
3	Bi-directional B+ (приём-передача)
4	Bi-directional C+ (приём-передача)
5	Bi-directional C- (приём-передача)
6	Bi-directional B- (приём-передача)
7	Bi-directional D+ (приём-передача)
8	Bi-directional D- (приём-передача)

14.2 Приложение 2. Назначение контактов порта Console



Розетка RJ-45

Номер контакта	Наименование сигнала
1	Не используется
2	Не используется
3	TD
4	Сигнальная земля
5	Сигнальная земля
6	RD
7	Не используется
8	Не используется