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.com
Сайт: http://www.s-terra.com

Программный комплекс С-Терра Шлюз. Версия 4.1

Руководство администратора

Руководство по установке и настройке NME-RVPN модуля (MCM)

РЛКЕ.00009-01 90 03

25.11.2014

Содержание

Руководство по установке и настройке NME-RVPN модуля (MCM) 4

Структура документа 4
Условные обозначения 4
Сетевой модуль NME-RVPN (MCM) 6
Интерфейсы модуля 7
Светодиодные индикаторы модуля 7
Кнопка Shutdown 8
Порт USB 8
Маршрутизаторы Cisco для установки модуля 9
Местоположение слотов, пригодных для установки модуля 9
Версия Cisco IOS 13
Меры безопасности и правила эксплуатации 14
Правила эксплуатации модуля 14
Рекомендации по безопасности 14
Предупреждение повреждений от электростатического разряда 15
Рекомендации по технической эксплуатации модуля 15
Предупреждения по технике безопасности 15
Установка модуля в маршрутизатор 17
Инструменты для установки модуля 17
Порядок действий при установке модуля 17
Установка и снятие заглушек передней панели 18
Подготовка слота для установки сетевого модуля 19
Установка сетевого модуля 24
Подсоединение модуля к сети Интернет 26
Настройка интерфейса маршрутизатора для связи с модулем 26
Инициализация программного комплекса S-Terra Gate при первом старте 28
Разграничение доступа 30
Поведение светодиодов в различных режимах работы модуля 43
Снятие сетевого модуля с маршрутизатора 44

 Copyright © S-Terra CSP 2003 -2014

Выключение сетевого модуля 44
Снятие сетевого модуля 44
Дополнительная информация....46
Cisco.com 46
S-Terra.com 46

 Copyright © S-Terra CSP 2003 -2014

Руководство по установке и настройке NME-RVPN модуля (MCM)

Структура документа

В разделе «Сетевой модуль NME-RVPN (MCM)» приведено описание модуля, световых индикаторов, интерфейсов и кнопок передней панели модуля.

В разделе «Маршрутизаторы Cisco для установки модуля» приведен список маршрутизаторов, на которые можно устанавливать модуль NME-RVPN.

В разделе «Меры безопасности и правила эксплуатации» даны рекомендации по сохранности оборудования, по предупреждению электростатического разряда, технической эксплуатации модуля, предупреждения по технике безопасности.

В разделе «Установка модуля в маршрутизатор» даны инструкции по установке модуля в маршрутизаторы Cisco.

В разделе «Инициализация программного комплекса S-Terra Gate» описывается инициализация программного комплекса при первом старте модуля.

В разделе «Поведение светодиодов в различных режимах работы модуля» описаны различные состояния модуля и работа светодиодов в этих состояниях.

В разделе «Снятие сетевого модуля с маршрутизатора» описаны два варианта выключения модуля и снятие его с маршрутизатора.

В разделе «Дополнительная информация» описаны другие источники получения информации на данную тему.

Условные обозначения

В этом документе используются следующие условные обозначения.

Таблица 1

Обозначение	Описание
Boldface font	Команды или ключевые слова.
Italic font	Переменные, которые надо заменить значением.
[ ]	Аргументы или ключевые слова, стоящие в квадратных скобках, являются необязательными.
{x|y|z}	Альтернативные варианты ключевых слов, стоящих в фигурных скобках, и разделенных вертикальными линиями. Нужно выбрать один вариант.
Screen font	Пример информации, высвечивающейся на экране.
`boldface screen font`	Пример информации, которую нужно ввести.
< >	Неотображаемые символы, например, пароль, …

Copyright © S-Terra CSP 2003 -2014

[ ]	Ответ по умолчанию, стоящий в квадратных скобках на системное приглашение.



Замечание

Этот символ означает – примите к сведению, замечание. Замечание содержит полезные предложения или ссылки на дополнительную информацию и материалы.



Подсказка

Этот символ означает, что следующая информация может быть вам полезна для решения проблемы.



Предостережение

Этот символ означает – читатель, будь осторожен. В этой ситуации ваши действия могут привести к поломке оборудования или потере данных.



Предупреждение

ВАЖНЫЕ СВЕДЕНИЯ ПО БЕЗОПАСНОСТИ

Этот символ предупреждает о наличии опасности. При неправильных действиях возможно получение травм. Перед началом работы с оборудованием необходимо ознакомиться с ситуациями, в которых возможно поражение электрическим током. Для предотвращения несчастных случаев выполняйте действия, описанные здесь.

 Copyright © S-Terra CSP 2003 -2014

Сетевой модуль NME-RVPN (MCM)

Модуль NME-RVPN (Network Module Enhanced Russian VPN) в исполнении MCM (Модуль Сетевой Модернизированный) производится в соответствии с технологическим процессом, согласованным с Центром ФСБ России «Порядком организации производства изделия «Модуль Сетевой Модернизированный (MCM)» в рамках подконтрольного технологического процесса на территории Российской Федерации».

В рамках установленного Порядка компания «С-Терра СиЭсПи» выступает в роли оператора контролируемого технологического процесса, цель которого – исключить вероятность внедрения в вычислительную среду эксплуатации средств криптографической защиты информации (СКЗИ) недокументированных вредоносных аппаратно-программных элементов.

Далее в документации этот модуль будем называть «Модуль NME-RVPN (MCM)» или «модуль».

Модуль работает на маршрутизаторах Cisco ISR второго поколения (серии 2900, 3900) и первого (серии 2800, 3800).

Аппаратно модуль представляет собой вычислительную платформу на базе процессора Intel Celeron M, 1 ГГц, 512 Мб RAM и 1 Гб постоянной памяти, размещенной на компакт-флеш карте.

Модуль работает независимо от ОС маршрутизатора, все обмены между ними производятся только по сети. Маршрутизаторы второго поколения работают под управлением ОС Cisco IOS, начиная с версии 15.x.x, а первого – версии 12.4(11)T или выше.

На модуль устанавливается продукт С-Терра Шлюз, функционирующий под управлением ОС Debian 6.0.6.

NME-RVPN (MCM) поддерживает до 500 IPsec туннелей.

Применяться модуль может для защиты трафика среднего офиса – несколько сотен рабочих мест. В составе маршрутизаторов серий 3900 и 3800, в которые можно установить от 2 до 4 модулей, может использоваться на узлах концентрации трафика множества региональных сетей, а также в крупных сетях удаленного доступа пользователей.

Внешний вид сетевого модуля NME-RVPN (MCM) представлен на Рисунок 1.

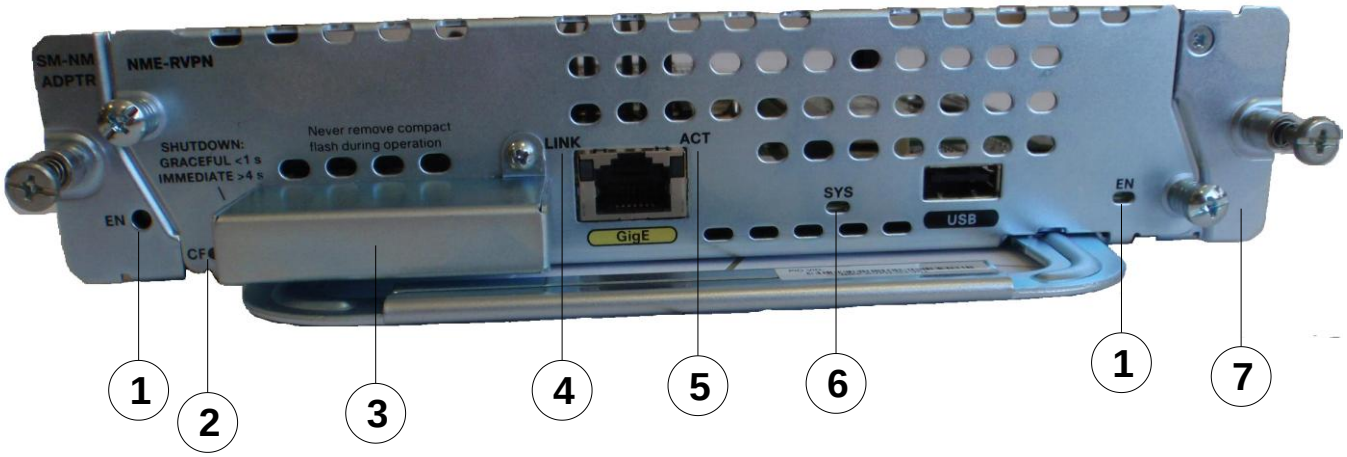


Рисунок 1

Copyright © S-Terra CSP 2003 -2014

На передней панели сетевого модуля находятся внешний сетевой интерфейс Gigabit Ethernet, светодиодные индикаторы (1,2,4,5,6), крышка компакт-флеш карты (3), кнопка SHUTDOWN и разъем USB. Сетевой модуль вставлен в сетевой модульный адаптер SM-NM ADPTR (7), внешний вид которого представлен на Рисунок 2.

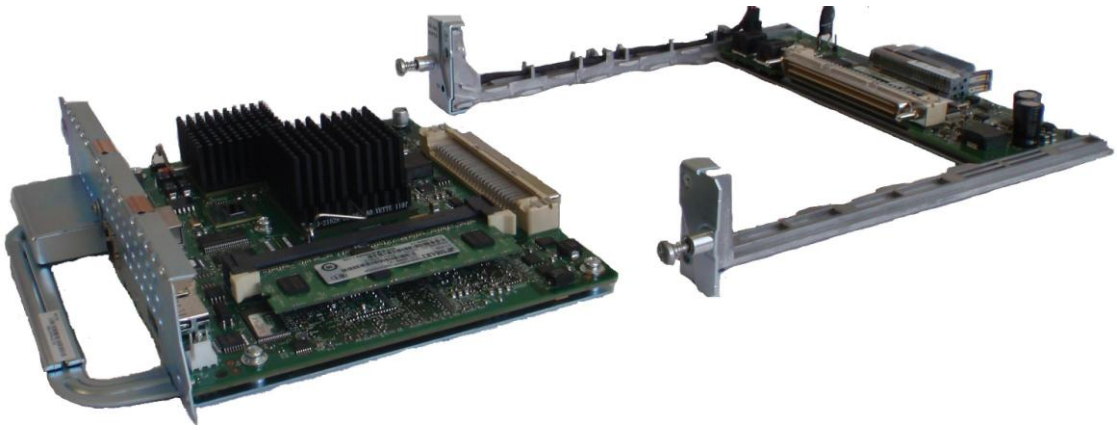


Рисунок 2

Консоль модуля не имеет разъема на передней панели и доступна только через команды IOS.

Интерфейсы модуля

Сетевой модуль имеет два интерфейса Gigabit Ethernet, один из которых является внешним для соединения с локальной сетью, а второй – внутренним для передачи данных между модулем и маршрутизатором. В IOS маршрутизатора соединение с модулем представлено как интерфейс `Special-Services-Engine`.

По ряду причин в продукте С-Терра Шлюз внешний интерфейс называется как `fastethernet 0/1`, а внутренний – `fastethernet 0/0`.

Светодиодные индикаторы модуля

На панели модуля имеются светодиодные индикаторы, название и назначение которых приведены в Таблица 2:

Таблица 2

Номер индикатора	Индикатор	Значение
1	EN	Индикатор обнаружения модуля (сетевого модульного адаптера) программным обеспечением маршрутизатора.
2	CF	Индикатор чтения/записи на компакт-флеш карту
4	LINK	Индикатор наличия соединения Gigabit Ethernet: Вкл. – соединение присутствует

 Copyright © S-Terra CSP 2003 -2014

		Выкл. – соединение отсутствует
5	ACT	Индикатор активности Gigabit Ethernet: Вкл. – интерфейс активен Выкл. – интерфейс неактивен
6	SYS	Индикатор состояния системы: Медленное мигание с периодом 4 сек – нормальный режим работы Частое мигание с периодом 0.5 сек – обнаружена неисправность.

Более подробное описание работы светодиодных индикаторов в различных режимах работы модуля представлено в главе «Поведение светодиодов в различных режимах работы модуля».

Кнопка Shutdown

На панели модуля находится кнопка SHUTDOWN, которая позволяет останавливать работу ОС модуля.

Нажатие кнопки SHUTDOWN и удержание ее меньше 1 секунды приводит к штатному завершению работы операционной системы и выключению питания модуля.

При повторном нажатии этой кнопки в течение такого же периода времени производится включение питания модуля.

Если случится, что модуль окажется в неработоспособном состоянии, то нажатие кнопки SHUTDOWN и удержание ее больше 4 секунд аналогично функции RESET (сброс, возврат в исходное состояние).

Порт USB

USB порт может использоваться для подключения ключевых носителей КриптоПро CSP или USB-флеш.

 Copyright © S-Terra CSP 2003 -2014

Маршрутизаторы Cisco для установки модуля

Сетевой модуль NME-RVPN (MCM) может устанавливаться в конфигурируемые слоты для сетевых модулей размером single-wide на маршрутизаторах Cisco 2911, 2921, 2951, 3925, 3945, 2811, 2821, 2851, 3825 и 3845.

Информацию и документацию об этих маршрутизаторах можно найти на www.cisco.com.

Местоположение слотов, пригодных для установки модуля

Маршрутизаторы серий 2900, 3900, 2800, 3800 имеют слоты для сетевых модулей различной ширины: single-wide, single-wide extended, double-wide и double-wide extended. Слоты большей ширины могут трансформироваться в слоты меньшей ширины с помощью разделителей и адаптеров. Для NME-RVPN (MCM) модулей требуются слоты single-wide. Номер слота указан на корпусе маршрутизатора слева от слота.

Note

Модуль NME-RVPN (MCM) поставляется в варианте для установки в слоты маршрутизаторов Cisco серий 2900 и 3900, т.е. вставленным в сетевой модульный адаптер (Рисунок 3).

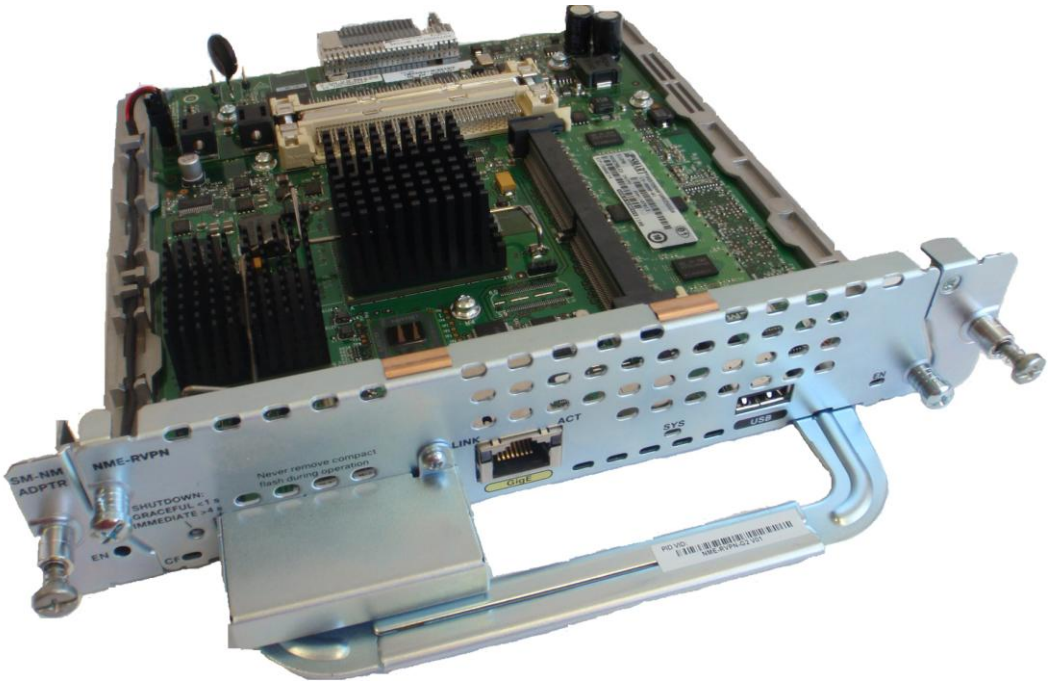


Рисунок 3

 Copyright © S-Terra CSP 2003 -2014

Опишем пригодные для модуля SM слоты на маршрутизаторах второго поколения.

На маршрутизаторе 2911 (Рисунок 4) имеется только один слот с номером 1, в который можно установить NME-RVPN (MCM) модуль. На Рисунок 4 этот слот помечен цифрой 1.

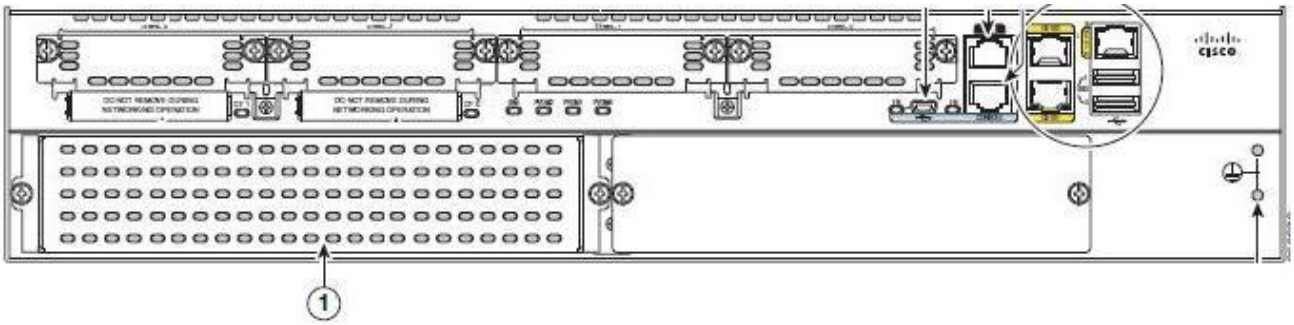


Рисунок 4

Маршрутизатор 2921 (Рисунок 5) тоже имеет только один слот, пригодный для установки single-wide или double-wide модуля. Это нижний слот, отмеченный на рисунке цифрой 2.

Маршрутизатор 2951 (Рисунок 5) имеет два слота для установки двух single-wide или одного double-wide модулей. Для установки модуля NME-RVPN (MCM) используются слоты, помеченные на рисунке цифрами 1 и 2.

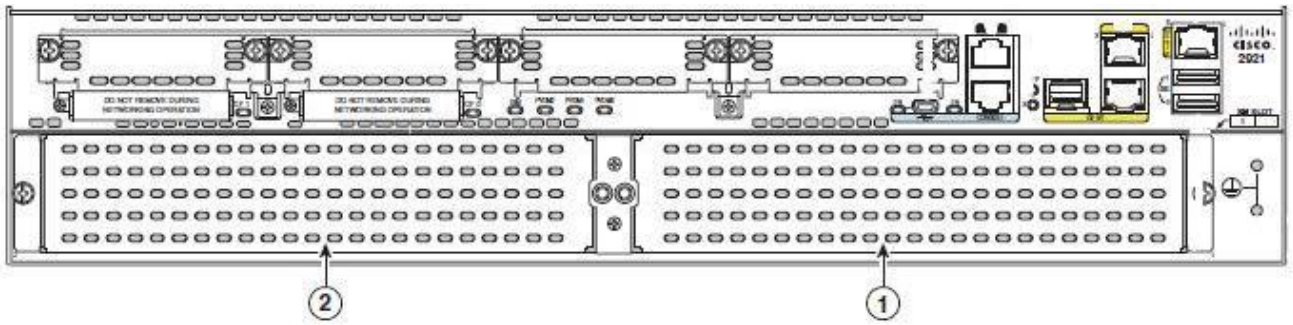


Рисунок 5

Маршрутизатор 3925 (Рисунок 6) имеет два слота, в которые могут размещаться модули single-wide и double-wide. Эти слоты с номерами 1 и 2 пригодны для размещения модуля NME-RVPN (MCM). На слот с номером 1 помечен цифрой 1, а с номером 2 – цифрой 2. В маршрутизатор 3925 одновременно можно устанавливать два модуля NME-RVPN (MCM).

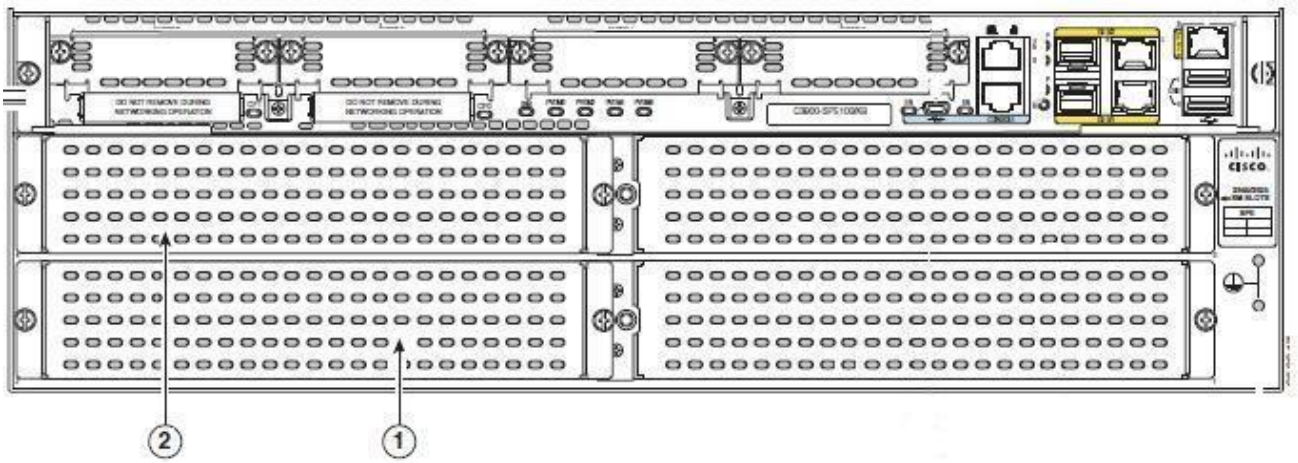


Рисунок 6

 Copyright © S-Terra CSP 2003 -2014

Маршрутизатор 3945 (Рисунок 7) имеет четыре слота, в которые могут размещаться модули single-wide и double-wide. Слоты с номерами 1, 2, 3, 4 являются пригодными для размещения модуля NME-RVPN (MCM). На слот с номером 1 помечен цифрой 1, с номером 2 – цифрой 2, с номером 3 – цифрой 3, а с номером 4 – цифрой 4. В слоты 1 и 3 могут быть размещены модули double-wide, поэтому для NME-RVPN (MCM) модуля их нужно трансформировать в слоты single-wide. В маршрутизатор 3845 одновременно можно устанавливать четыре модуля NME-RVPN (MCM).

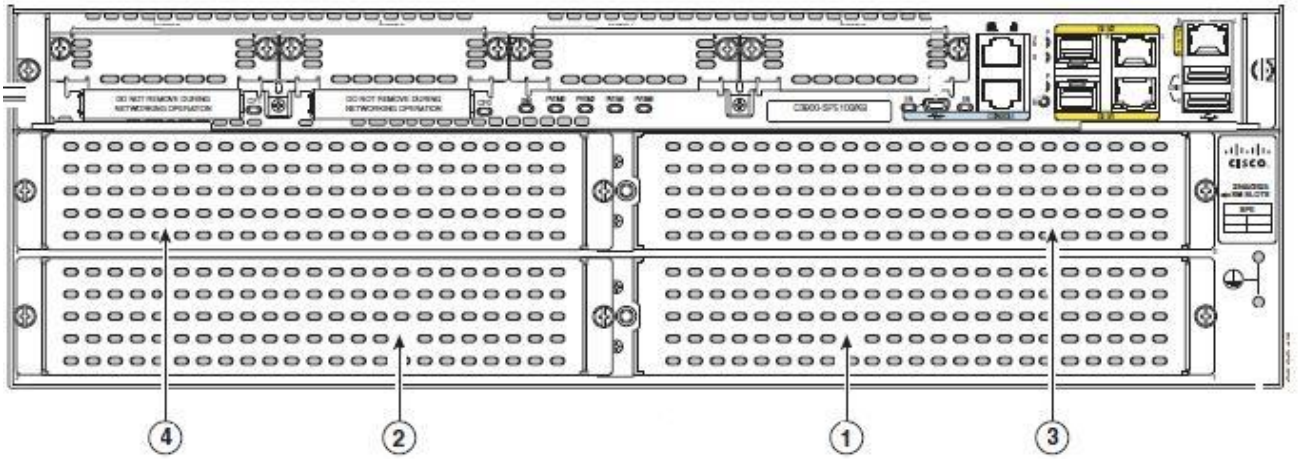


Рисунок 7

Далее опишем слоты для модуля на маршрутизаторах первого поколения.

На маршрутизаторе 2811 (Рисунок 8) имеется только один слот с номером 1, в который можно установить NME-RVPN (MCM) модуль. На Рисунок 8 этот слот помечен цифрой 1.

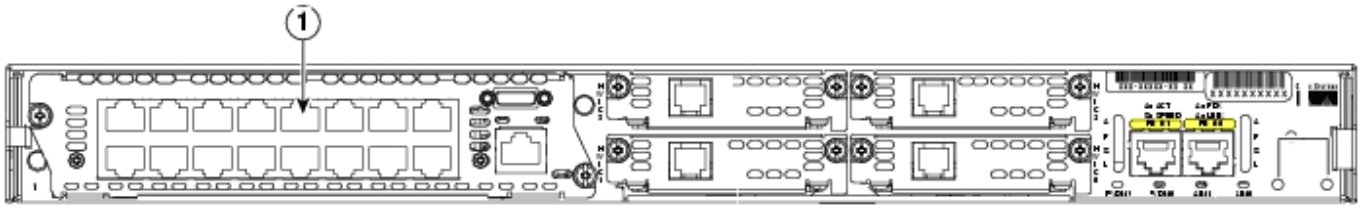


Рисунок 8

Маршрутизатор 2821 (Рисунок 9) тоже имеет только один слот, пригодный для установки single-wide и single-wide extended модулей. Это нижний слот с номером 1, отмеченный на рисунке цифрой 1. Верхний слот (цифра 2) – это слот расширения, не поддерживающий single-wide модули.

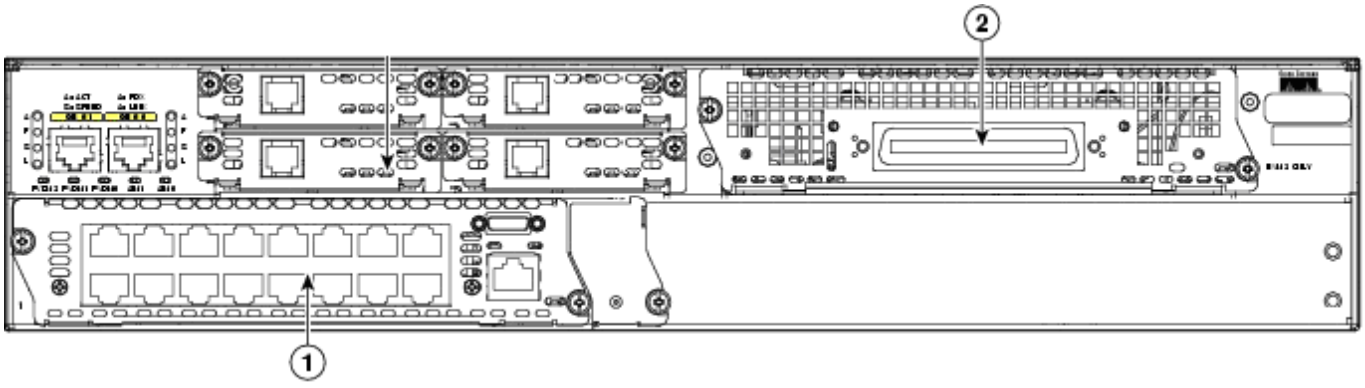


Рисунок 9

 Copyright © S-Terra CSP 2003 -2014

Нижний слот маршрутизатора 2851 поддерживает все виды модулей, в том числе double-wide, как показано на Рисунок 10. Для установки модуля NME-RVPN (MCM) используется только один слот с номером 1, помеченный на рисунке цифрой 1, который нужно трансформировать в слот размером single-wide.

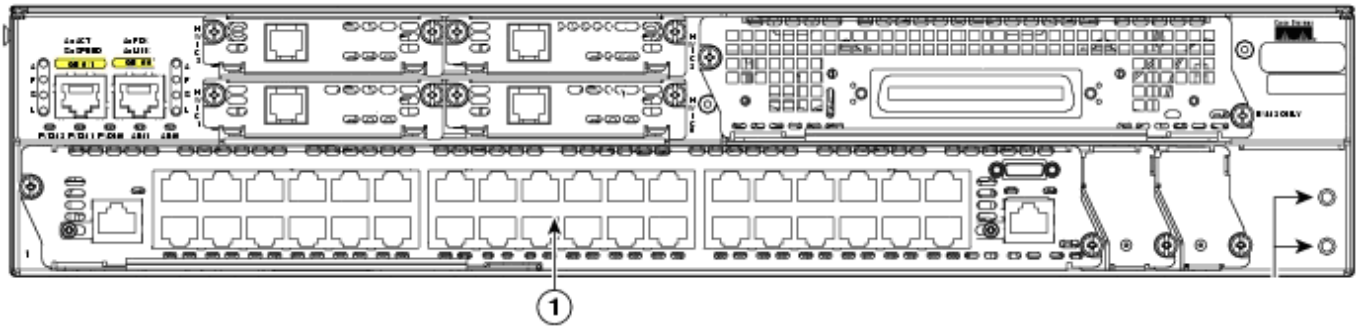


Рисунок 10

Маршрутизатор 3825 (Рисунок 11) имеет только два слота, в которые могут размещаться модули single wide и single-wide extended. Именно эти слоты с номерами 1 и 2 пригодны для размещения модуля NME-RVPN (MCM). На рисунке слот с номером 1 помечен цифрой 1, а с номером 2 – цифрой 2, который нужно трансформировать в слот меньшего размера. В маршрутизатор 3825 одновременно можно устанавливать два модуля NME-RVPN (MCM).

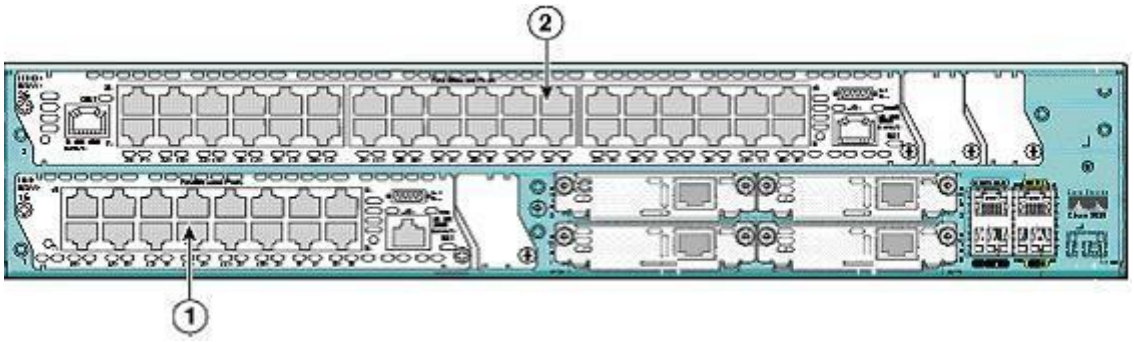


Рисунок 11

Маршрутизатор 3845 (Рисунок 12) имеет четыре слота, в которые могут размещаться модули single wide и single-wide extended. Слоты с номерами 1, 2, 3, 4 являются пригодными для размещения модуля NME-RVPN (MCM). На рисунке слот с номером 1 помечен цифрой 1, с номером 2 – цифрой 2, с номером 3 – цифрой 3, а с номером 4 – цифрой 4. В слоты 1 и 3 могут быть размещены модули double-wide и Extended double-wide, поэтому для NME-RVPN модуля их нужно трансформировать в слот single-wide. В маршрутизатор 3845 одновременно можно устанавливать четыре модуля NME-RVPN (MCM).

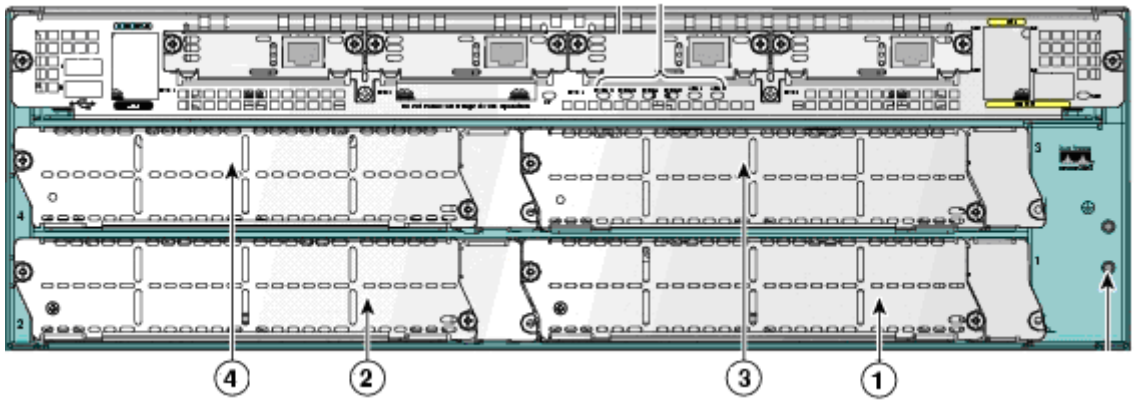


Рисунок 12

 Copyright © S-Terra CSP 2003 -2014

Версия Cisco IOS

На маршрутизаторах Cisco второго поколения должна быть установлена операционная система Cisco IOS, начиная с версии 15.x.x, на маршрутизаторах первого – версия 12.4(11)T или выше.

Получить информацию о версии установленной операционной системы можно по выводу команды `show version` в консоли маршрутизатора.

 Copyright © S-Terra CSP 2003 -2014

Меры безопасности и правила эксплуатации

В этой главе приведена информация, которую необходимо знать перед установкой и во время инсталляции модуля в маршрутизатор, а именно правила эксплуатации модуля и меры по технике безопасности.

Правила эксплуатации модуля

Рекомендуемые правила безопасности при установке модуля и его эксплуатации приведены в следующих четырех разделах:

- Рекомендации по безопасности.
- Предупреждение повреждений от электростатического разряда.
- Рекомендации по технической эксплуатации модуля.
- Предупреждения по технике безопасности.

Рекомендации по безопасности

При установке или снятии сетевого модуля с маршрутизатора для предотвращения опасных ситуаций следуйте следующим правилам безопасности:

- Храните инструменты вне вашего рабочего места, чтобы вы или кто-то другой не споткнулся о них и не упал.
- Устраните с вашего рабочего места возможные источники опасности. Такими источниками опасности являются мокрый пол, незаземленный удлинитель или отсутствие безопасного заземления.
- Перед началом работы с маршрутизатором отключите электропитание и выдерните из розетки вилку шнура питания.
- При установке или снятии сетевого модуля с маршрутизатора отключите электропитание маршрутизатора.
- Не работайте в одиночку в помещении, если существуют потенциально опасные условия.
- Разместите запасной выключатель электропитания в комнате, в которой вы работаете.
- При получении электротравмы пострадавшим действуйте следующим образом:
  - Будьте осторожны, чтобы не стать жертвой самому.
  - Выключите электропитание в комнате, используя запасной выключатель электропитания.
  - По возможности сообщите другому человеку, чтобы пострадавшему вызвали медицинскую помощь. В противном случае, определите состояние пострадавшего, и затем вызовите помощь.
  - При необходимости приступайте к выполнению искусственного дыхания и массажа сердца.

 Copyright © S-Terra CSP 2003 -2014

Предупреждение повреждений от электростатического разряда

Электростатический разряд может нанести ущерб оборудованию и повредить электрическую цепь. Электростатический разряд появляется при неправильной эксплуатации электронных печатных плат, которые используются в сетевом модуле, и может привести к полной или частичной поломке оборудования.

Всегда уделяйте внимание предотвращению электростатических разрядов при установке и снятии сетевого модуля:

- Проверьте, что корпус маршрутизатора заземлен.
- Наденьте на руку электростатический браслет и проверьте, что он имеет хороший контакт с вашей кожей.
- Подсоедините зажим браслета к неокрашенной части корпуса маршрутизатора, чтобы снять нежелательный электростатический разряд.
- Если не имеете электростатического браслета, то для снятия статического заряда прикоснитесь обеими руками к заземленному объекту, например, корпусу маршрутизатора.



Электростатический браслет и зажим должны использоваться правильно, чтобы гарантировать защиту от электростатического разряда. Периодически проверяйте, что величина сопротивления электростатического браслета находится в диапазоне от 1 до 10 Мега-Ом.

Рекомендации по технической эксплуатации модуля

Выполняйте следующие рекомендации по технической эксплуатации модуля:

- Храните модуль чистым и свободным от загрязнений во время и после установки.
- Если вы сняли крышку маршрутизатора, то храните ее в безопасном месте.
- Не производите действий, которые приводят к возникновению источника опасности или опасного оборудования.
- Не оставляйте оборудование на проходе во избежание его падения или порчи.
- Установку модуля, эксплуатацию и техническое обслуживание выполняйте, следуя инструкциям, описанным в документе.

Предупреждения по технике безопасности

Следующие предупреждения по технике безопасности должны использоваться при работе с любыми маршрутизаторами, в том числе и с устанавливаемыми модулями.

 Copyright © S-Terra CSP 2003 -2014



Перед работой с оборудованием или рядом с блоком питания выдерните вилку шнура питания из розетки переменного тока.



Установку и замену оборудования может осуществлять только обученный и квалифицированный персонал.



Окончательная установка данного продукта должна выполняться в соответствии со всеми внутригосударственными законами и нормами.

 Copyright © S-Terra CSP 2003 -2014

Установка модуля в маршрутизатор

Перед установкой модуля ознакомьтесь с мерами безопасности и правилами эксплуатации в главе «Меры безопасности и правила эксплуатации».

В этой главе описаны действия, которые нужно выполнить при установке модуля в маршрутизатор.

Инструменты для установки модуля

Приведем список инструментов, которые потребуются при установке модуля в маршрутизатор:

- Отвертка номер 1 Philips или небольшая отвертка с плоской поверхностью
- Антистатический браслет для защиты от электростатического разряда.

Порядок действий при установке модуля

При установке модуля в маршрутизатор нужно выполнить следующие операции:

Cisco 2911, Cisco 2921, Cisco 2951, Cisco 3925, Cisco 3945 Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, Cisco 3845
Выключить электропитание маршрутизатора
Снять заглушку передней панели со слота маршрутизатора, который планируется использовать, если этот слот ранее не использовался
Подготовить сетевой слот для установки модуля, если данный слот использовался модулями другого размера
Установить сетевой модуль
Подключить сетевой модуль к сети Интернет
Включить электропитание маршрутизатора
Инициализировать продукт С-Терра Шлюз.

Чтобы установить сетевой модуль переходите к разделу «Установка сетевого модуля», в котором описаны подробно все инструкции.

 Copyright © S-Terra CSP 2003 -2014

Установка и снятие заглушек передней панели

Все полые слоты для сетевых модулей, в которые не установлен сетевой модуль, должны быть прикрыты заглушками передней панели (Рисунок 13), (Рисунок 14), чтобы направлять охлаждающий воздушный поток внутри корпуса и экранировать электромагнитное излучение.

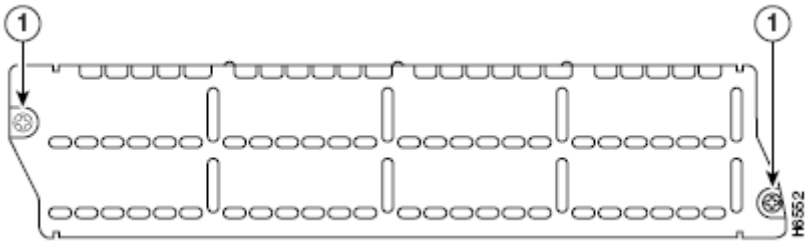


Рисунок 13

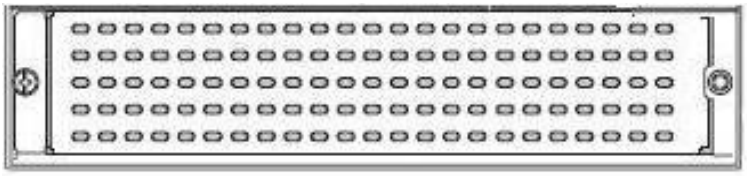


Рисунок 14

Note

Заглушки передней панели маршрутизатора могут устанавливаться только поверх слотов размером single-wide.

Note

Заглушки передней панели на маршрутизаторе Cisco 2951 является единым целым с разделителем слота, как показано на Рисунок 15.

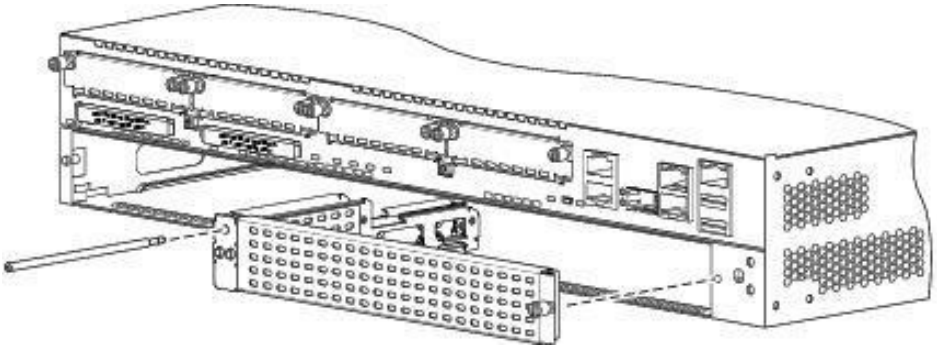


Рисунок 15

 Copyright © S-Terra CSP 2003 -2014

Снятие заглушки

Для снятия заглушки со слота сетевого модуля single-wide выполните следующие операции:

Шаг 1: Открутите монтажные винты, удерживающие заглушку (Рисунок 13), (Рисунок 14) отверткой номер 1 Philips или небольшой отверткой с плоской поверхностью.

Шаг 2: Снимите заглушку передней панели.



Сохраните заглушку передней панели для дальнейшего использования.

Установка заглушки

Для установки заглушки на слот, который использовался для сетевых модулей размером extended single-wide, double-wide или extended double-wide, необходимо данный слот трансформировать в слот размером single-wide. Процедура трансформации слотов разных размеров представлена в разделе «Подготовка слота для установки сетевого модуля».

После трансформации слота для установки заглушки передней панели выполните следующие шаги:

Шаг 1: Установите заглушку на слот. На Рисунок 13 и Рисунок 14 показана заглушка с винтами, предназначенная для прикрытия слота размером single-wide.

Шаг 2: Закрутите монтажные винты, которые удерживают заглушку на слоте.

Подготовка слота для установки сетевого модуля

На маршрутизаторах Cisco 2921, Cisco 2951, Cisco 3925, Cisco 3945, Cisco 2821, Cisco 2851, Cisco 3825, Cisco 3845 может потребоваться провести трансформацию слота перед установкой сетевого модуля NME-RVPN, если данный слот использовался как double-wide или extended double-wide.

Для подготовки слота выполните следующие действия:

Шаг 1: На маршрутизаторах Cisco серий 2800 и 3800 снимите адаптер слота с правой стороны слота маршрутизатора. Эта процедура описана в разделе «Снятие адаптера слота».

Шаг 2: Установите разделитель слота. Действия по установке разделителя приведены в разделе «Установка разделителя слота».

Шаг 3: На маршрутизаторах Cisco серий 2800 и 3800 установите адаптер с правой стороны слота, в который планируется установить модуль. Для этого выполните действия, описанные в разделе «Установка адаптера слота».

Шаг 4: Далее перейдите к выполнению Шага 5 раздела «Установка сетевого модуля».

Copyright © S-Terra CSP 2003 -2014

Снятие адаптера слота

Для снятия адаптера слота с правой стороны слота выполните следующие действия:

Шаг 1: Отвинтите монтажный винт на адаптере слота, используя отвертку с плоской поверхностью.

Шаг 2: Выньте адаптер из слота.

Шаг 3: Далее перейдите к установке разделителя слота.

Установка разделителя слота

Разделитель слота используется, чтобы создать слот размером single-wide для установки сетевого модуля. Разделитель слота, показанный на Рисунок 16, используется на маршрутизаторах Cisco 2951, 3925 и 3945. Разделитель слота для маршрутизаторов Cisco 2851, 3825 и 3845 показан на Рисунок 17.

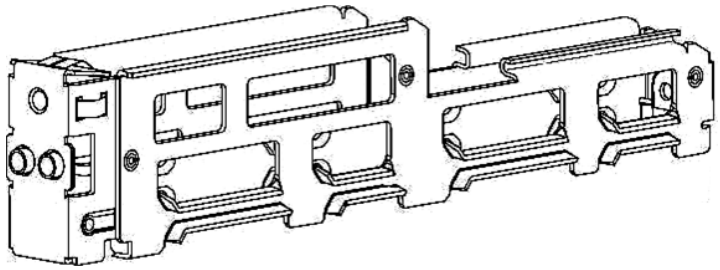


Рисунок 16

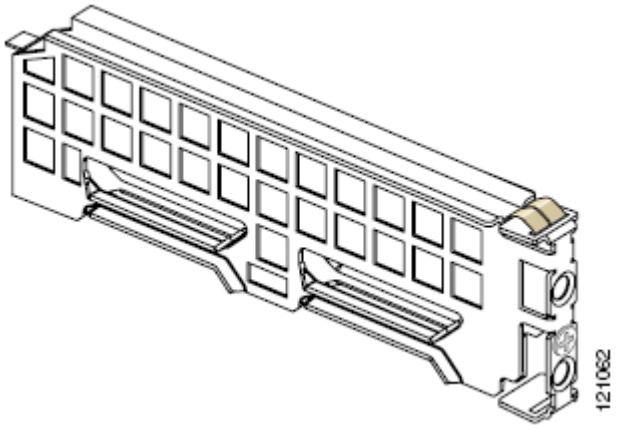


Рисунок 17

Для установки разделителя слота в маршрутизатор выполните следующие шаги:

Шаг 1: Снимите любые установленные сетевые модули, заглушки передней панели и адаптеры со слота маршрутизатора, который вы собираетесь использовать.

Шаг 2: Вставьте направляющую верхней части разделителя слота между двумя направляющими рельсами верхней части слота сетевого модуля, как показано на Рисунок 18 (на примере маршрутизатора Cisco 2951) и Рисунок 19 (маршрутизатор Cisco 2851).

 Copyright © S-Terra CSP 2003 -2014

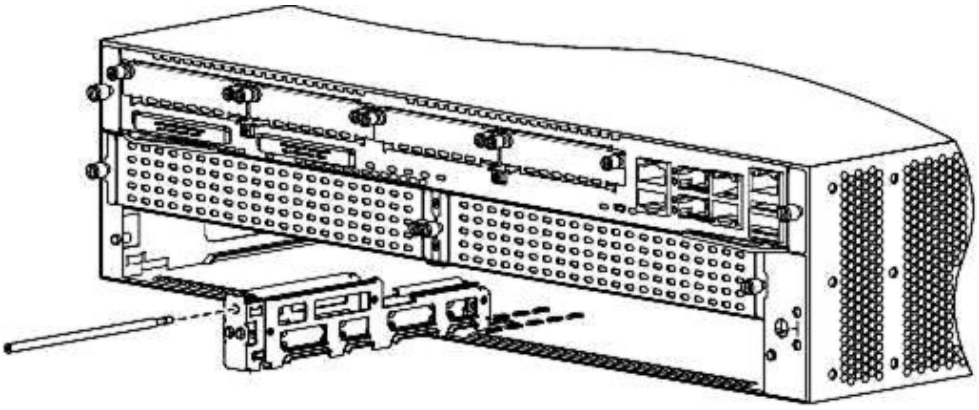


Рисунок 18

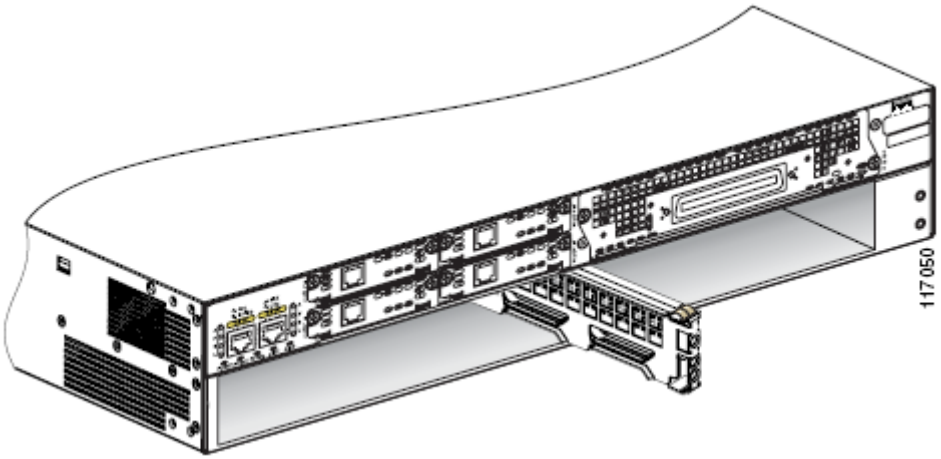


Рисунок 19

Шаг 3: Задвиньте разделитель в слот, пока он полностью не установится. Разделитель для маршрутизаторов Cisco 3925 и 3945 имеет длинный удерживающий винт, который вставляется в разделитель (Рисунок 18).

Шаг 4: Закрутите удерживающие винты на передней панели разделителя слота отверткой (Рисунок 20). Когда разделитель слота полностью установлен, его передняя панель находится на одном уровне с панелью маршрутизатора, как показано на Рисунок 21.

 Copyright © S-Terra CSP 2003 -2014

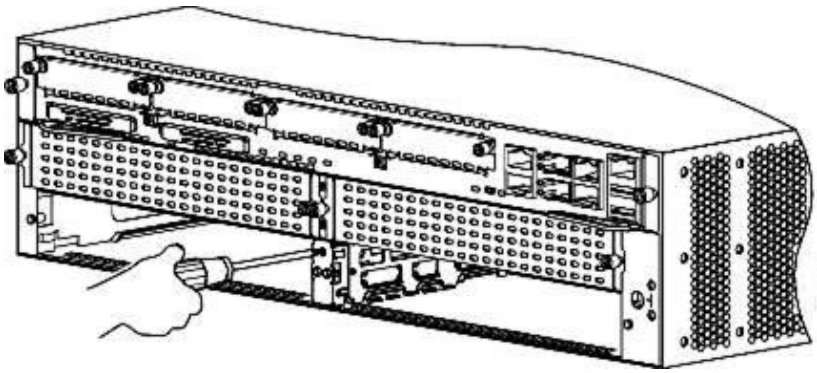


Рисунок 20

Шаг 5: На маршрутизаторах Cisco 2821, 2851, 3825, 3845 далее перейдите к установке адаптера слота, описанного в разделе «Установка адаптера слота». Для остальных маршрутизаторов Cisco – перейдите к выполнению Шага 5 раздела «Установка сетевого модуля».

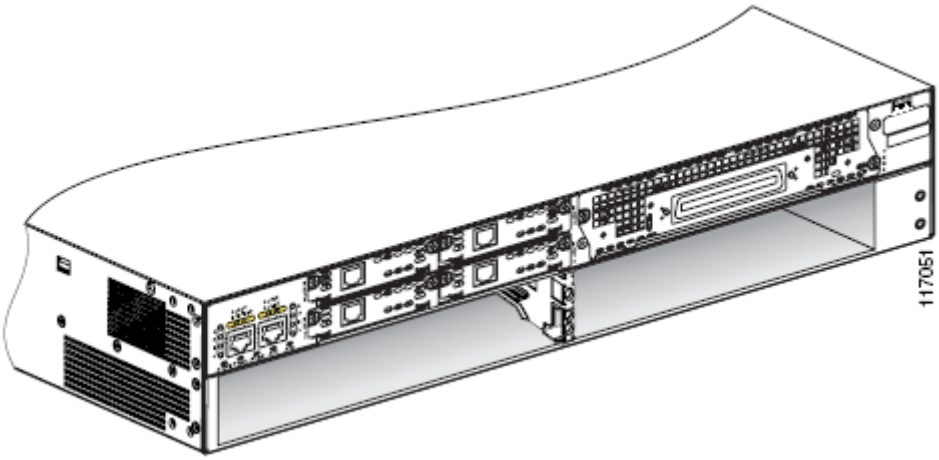


Рисунок 21

Установка адаптера слота

Установка адаптера слота позволяет инсталлировать сетевой модуль NME-RVPN (MCM) в слот большего размера. Образец адаптера слота представлен на Рисунок 22. Адаптер слота устанавливается только в маршрутизаторы Cisco 2821, 2851, 3825, 3845.

 Copyright © S-Terra CSP 2003 -2014

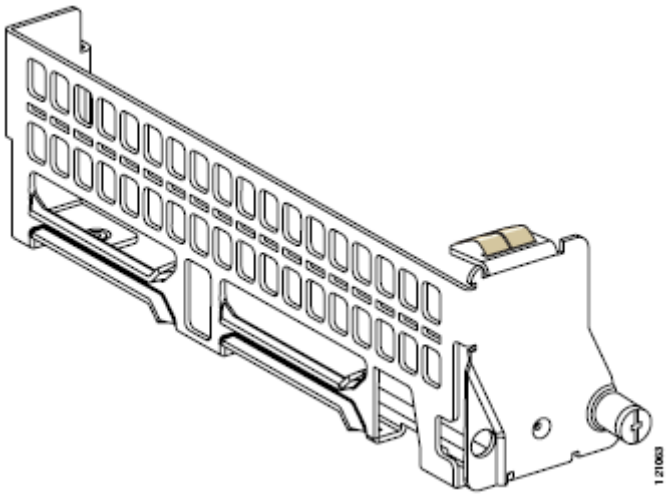


Рисунок 22

Для установки адаптера слота в маршрутизатор выполните следующие шаги:

Шаг 1: Снимите установленные сетевые модули со слота маршрутизатора, которые вы собираетесь использовать.

Шаг 2: Определите местоположение адаптера в слоте маршрутизатора. На Рисунок 23 представлено местоположение адаптеров слота (обозначены цифрой 2) и разделителя слота (обозначен цифрой 1).

Шаг 3: Поверните адаптер слота так, чтобы контакт на задней панели адаптера совпал с разъемом слота внутри маршрутизатора.

Tip

При правильном расположении адаптера монтажный винт на адаптере совпадает с отверстием под винт в корпусе маршрутизатора.

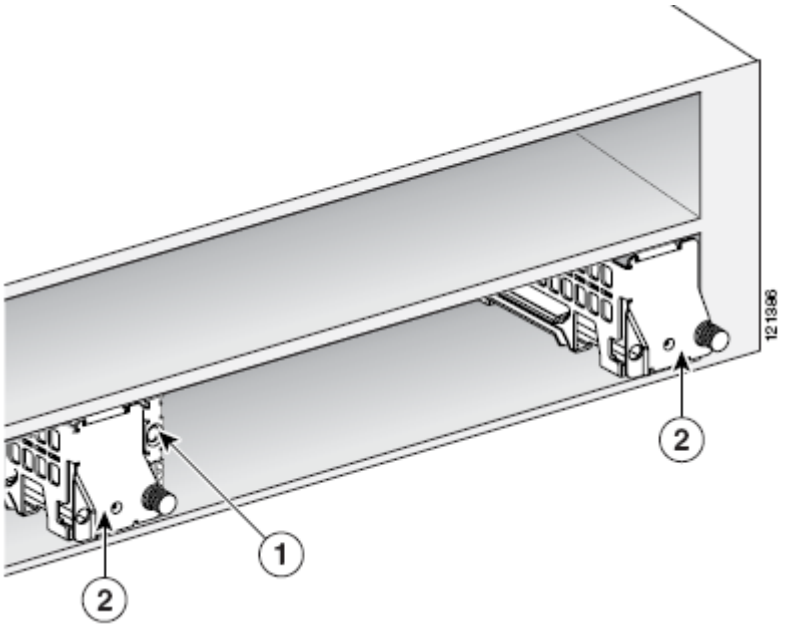


Рисунок 23

 Copyright © S-Terra CSP 2003 -2014

Шаг 4: Аккуратно вставьте адаптер в слот.

Шаг 5: Закрутите винт на адаптере слота отверткой, чтобы зафиксировать его в слоте.

Шаг 6: Далее перейдите к выполнению Шага 5 раздела «Установка сетевого модуля».

Установка сетевого модуля

Чтобы установить сетевой модуль выполните следующие шаги:

Шаг 1: Отключите электропитание маршрутизатора.



Перед выполнением описанных ниже действий убедитесь, что электропитание маршрутизатора выключено и вилка шнура питания выдернута из розетки.

Шаг 2: Отключите все сетевые кабели, включая телефонные, от задней панели маршрутизатора.

Шаг 3: Снимите заглушку передней панели слота, который намереваетесь использовать. В разделе «Местоположение слотов, пригодных для размещения модуля» приведена информация о слотах различных маршрутизаторов, в которые можно устанавливать сетевой модуль. Если данный слот использовался для сетевых модулей размером double-wide или extended double-wide, то этот слот нужно подготовить для установки, а на оставшийся слот установить заглушку передней панели. Снятие заглушки передней панели описано в разделе «Установка и снятие заглушек передней панели». Для подготовки слота переходите к выполнению Шага 4, а после снятия заглушки перейдите к выполнению Шага 5.



Сохраните заглушку передней панели для дальнейшего использования.

Шаг 4: Подготовьте слот для установки сетевого модуля. Порядок этих действий представлен в разделе «Подготовка слота для установки сетевого модуля».

Шаг 5: Для маршрутизаторов Cisco серий 2900 и 3900 расположите сетевой модуль, вставленный в сетевой модульный адаптер, на полозьях слота, как показано на Рисунок 24 (цифрой 1 обозначен сетевой модуль, а цифрой 2 – маршрутизатор).

 Copyright © S-Terra CSP 2003 -2014

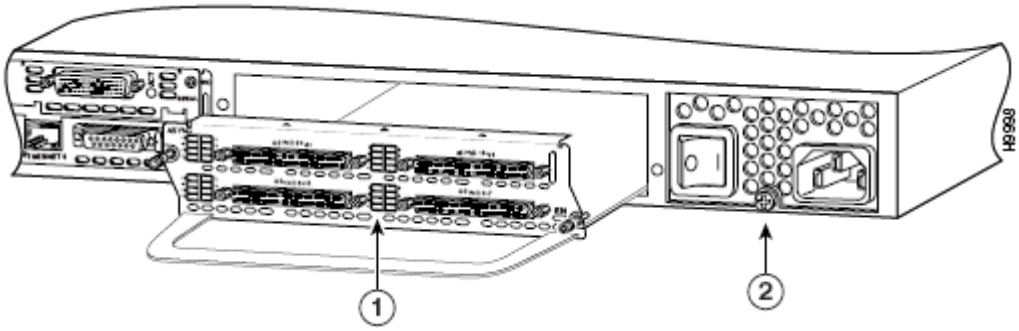


Рисунок 24

Note

Никогда не вставляйте в слот сетевой модульный адаптер без сетевого модуля.

Шаг 6: Для маршрутизаторов Cisco серий 2800 и 3800 сначала выньте сетевой модуль из сетевого модульного адаптера, раскрутив винты на модуле, удерживающие его в адаптере. На Рисунок 25 цифрой 1 помечен сетевой модуль, цифрой 2 – сетевой модульный адаптер. Разместите сетевой модуль на полозьях слота.

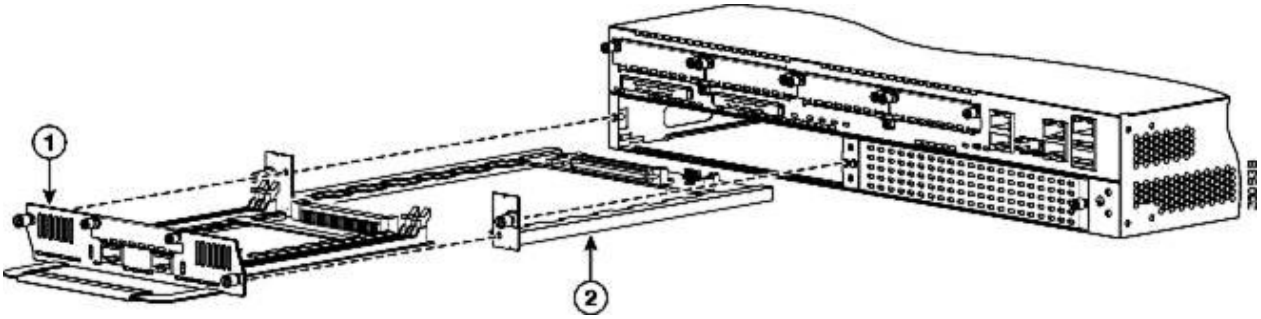


Рисунок 25

Шаг 7: Используя ручку сетевого модуля, аккуратно задвиньте сетевой модуль, чтобы разъем модуля (модульного адаптера) совместился с соответствующим разъемом слота внутри маршрутизатора.

Шаг 8: Для фиксации установленного модуля в слоте закрутите два винта на передней панели сетевого модуля (модульного адаптера).

Шаг 9: Подключите сетевой интерфейс Gigabit Ethernet модуля к сети Интернет. Этот пункт описан в разделе «Подключение модуля к сети Интернет».

Шаг 10: Включите шнур питания в сеть переменного тока и включите тумблер питания маршрутизатора.

Шаг 11: Проверьте, что светодиодный индикатор EN включен, это означает, что модуль NME-RVPN распознан IOS маршрутизатора.

Шаг 12: Перейдите к настройке сетевого модуля, описанной в разделе «Настройка сетевого модуля в маршрутизаторе».

 Copyright © S-Terra CSP 2003 -2014

Подсоединение модуля к сети Интернет

Для подсоединения модуля NME-RVPN (MCM) к сети Интернет используйте неэкранированную витую пару категории 5, чтобы соединить RJ-45 порт модуля с другим сетевым устройством. Gigabit Ethernet интерфейс автоматически распознает и поддерживает работу на скоростях 10, 100 и 1000 Mbps, Full или Half Duplex.

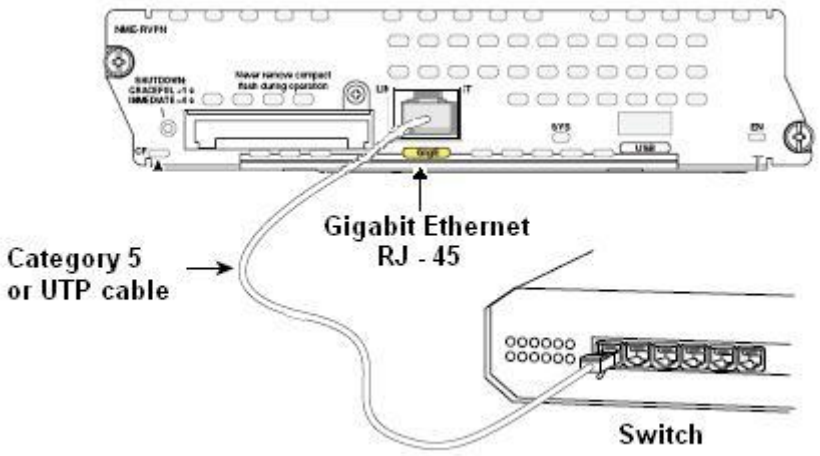


Рисунок 26

Настройка интерфейса маршрутизатора для связи с модулем

Шаг 1: Убедитесь, что IOS распознала NME-RVPN (MCM) модуль. Для этого используйте команду:

```
Router#  show running-config
```

Выводимая информация по этой команде должна содержать записи о модуле, установленного, например, в слот 1 примерно следующего вида:

```
......
interface Special-Services-Engine1/0
shutdown
no keepalive
.....
```

Шаг 2: Перейдите в конфигурационный режим консоли маршрутизатора:

```
Router#  configure terminal
```

Шаг 3: Назначьте IP-адрес/маску интерфейсу маршрутизатора для связи с модулем и активизируйте его, используя последовательность команд (например, для IP-адреса 192.168.0.254/24):

```
Router(config)#  interface Special-Services-Engine 1/0
Router(config-if)#  ip address 192.168.0.254 255.255.255.0
Router(config-if)#  no shutdown
```

 Copyright © S-Terra CSP 2003 -2014

```
Router(config-if) exit
Router(config) exit
Router#
```

Шаг 4: Далее перейдите к разделу «Инициализация программного комплекса S-Terra Gate при первом старте» для доступа к консоли модуля и его инициализации.

Copyright © S-Terra CSP 2003 -2014

Инициализация программного комплекса S-Terra Gate при первом старте

Сетевой модуль имеет разъем, с которого предварительно снята крышка и в него вставлена компакт-флеш карта.

Компакт-флеш карта на модуле содержит:

- установленную ОС Debian 6.0.6
- установленный и подготовленный к инициализации Продукт С-Терра Шлюз 4.1 со встроенной криптобиблиотекой от компании «С-Терра СиЭсПи»

  либо

- установленные и подготовленные к инициализации продукты С-Терра Шлюз 4.1 и СКЗИ «КриптоПро CSP 3.6R4/3.9».

Для работы установленных продуктов необходимо провести процедуру начальной инициализации. Для этого, прежде всего получите доступ к консоли модуля NME-RVPN (MCM) с помощью следующей команды:

```
Router# service-module Special-Services-Engine 1/0 session

Trying 192.168.0.254, 2066 ... Open
```

При каждом старте модуля NME-RVPN (MCM) в исполнении класса защиты КС2 и КС3 выполняется последовательный контроль целостности файлов следующего звена в цепочке загрузки системы вплоть до загрузки СКЗИ, а затем передача управления на него. Начальным звеном в этой цепочке, для которого не требуется проверка, является ПЗУ, в котором записан BIOS и загрузчик ОС. После включения питания управление передается BIOS, а затем на загрузчик ОС. Перезапись ПЗУ запрещена аппаратными средствами.

Осуществляется контроль целостности всех файлов, перечисленных в списке `/boot/hashes`, для исполнения Продукта класса защиты КС3 – в списках `/boot/hashes` и `/hashes.conf`. При нарушении целостности одного из файлов, выдается сообщение

```
<путь к файлу>: invalid
```

и дальнейшая проверка файлов прерывается с выдачей предупреждения, что через 10 секунд последует перезагрузка MCM и проверка начнется сначала:

```
System will be rebooted after 10 seconds...
```

При невозможности выполнить проверку всех файлов, выключите питание модуля кратковременным нажатием кнопки «`shutdown`» (меньше 1 сек) на передней панели модуля. Примерно через 10 секунд произойдет выключение модуля. Восстановите содержимое компакт-флеш карты из образа компакт-флеш, который входит в комплект поставки. Выполните эту процедуру согласно документу – «Инструкция по восстановлению и обновлению ПАК».

Успешная проверка целостности всех файлов завершается сообщением:

```
Continue loading...
```

После загрузки ОС появляется просьба запустить процесс инициализации:

```
System is not initialized.
Please run /opt/VPNagent/bin/init.sh to start initialization procedure
```

и приглашение для входа в ОС.

 Copyright © S-Terra CSP 2003 -2014

Шаг 1: Войдите в ОС. Для исполнения Продукта класса защиты КС1 для входа в систему используется:

имя пользователя – `root`
пароль – пустой.

Для исполнения Продукта класса защиты КС2 или КС3 для входа в систему используется:

имя пользователя – `administrator`
пароль – `s-terra`.
Затем необходимо ввести специальную команду `system`.

Шаг 2: Запустите скрипт `/opt/VPNagent/bin/init.sh` для старта процедуры начальной инициализации С-Терра Шлюз.

Во время выполнения инициализационный скрипт может быть прерван нажатием комбинации клавиш `Ctrl+C`.

При возникновении ошибки процесс инициализации прерывается и на экран выдается сообщение об ошибке.

Шаг 3: Выполняется только в случае использования СКЗИ «КриптоПро CSP. Запрашивается лицензионная информация для CryptoPro CSP: "`You have to enter license for CryptoPro CSP. Enter serial number:`". При вводе неверного номера лицензии предлагается ввести Лицензию еще раз.

Шаг 4: Инициализируется ДСЧ: "`You should initialize RNG. Press <Enter> to proceed…`"

Для исполнений класса защиты КС1 проводится «биологическая» инициализация начального значения ДСЧ: поэтому предлагается понажимать клавиши: "`Press keys… [ ]`". По окончании выдается сообщение "Initialization SUCCESS".

Для исполнений класса защиты КС2 и КС3 инициализация начального значения ДСЧ выполняется без участия пользователя.

Шаг 5: Далее запрашивается лицензионная информация на С-Терра Шлюз : "`You have to enter license for S-Terra Gate`". Предлагаются следующие пункты для ввода:

```
Available product codes:
GATE100
GATE100B
GATE100V
GATE1000
GATE1000V
GATE3000
GATE7000
GATE10000
RVPN
RVPNV
BELVPN
BELVPNV
UVPN
UVPNV
KZVPN
KZVPNV
Enter product code: (выберите RVPN или RVPNV)
Enter customer code:
Enter license number:
Enter license code:
```

 Copyright © S-Terra CSP 2003 -2014

Шаг 6: Следует вопрос о корректности введенных данных:"`Is the above data correct?`" После получения подтверждения инициализация продолжается без дополнительных вопросов. Если подтверждение не получено, то предлагается ввести Лицензию еще раз.

Шаг 7: Далее запускается vpn-демон (в случае исполнения Продукта класса защиты КС2 и КС3, vpn-демон запускаться не будет), создается пользователь "`cscons`" с назначенным ему начальным паролем "`csp`".

Если инициализация завершилась успешно, то выдается сообщение: "`Initialization complete`". При последующих стартах системы предупреждение о необходимости инициализации системы не выдается.

Если инициализация завершилась неуспешно, то об этом выдаётся соответствующее сообщение. При следующем старте комплекса администратору снова будет выдаваться предупреждение об инициализации.

Драйвер Продукта С-Терра Шлюз установлен на все обнаруженные сетевые интерфейсы.

Программный комплекс С-Терра Шлюз установлен в каталог `/opt/VPNagent`.

При инициализации С-Терра Шлюз устанавливается политика `Default Driver Policy = Passdhcp`, при которой интерфейсы шлюза безопасности пропускают только пакеты DHCP и в незащищенном виде.

Сразу после инициализации модуля (в случае исполнения Продукта класса защиты КС1) и при последующих его стартах автоматически запускается утилита `cspvpn_verify` для проверки целостности установленного Продукта S-Terra Gate, которая описана в документе «Специализированные команды». При нарушении целостности восстановите содержимое компакт-флеш карты из образа компакт-флеш, который входит в комплект поставки. Выполните эту процедуру согласно документу –- «Инструкции по восстановлению и обновлению ПАК».

В случае исполнения Продукта класса защиты КС1:

- для входа в Cisco-like интерфейс командной строки нужно использовать имя пользователя "`cscons`" (начальный пароль "`csp`")
- для входа в ОС предназначено имя "`root`" (изначально без пароля).

В случае исполнения класса защиты КС2 и КС3, имена пользователей задаются администратором. Подробнее описано в разделе «Разграничение доступа».

Разграничение доступа

Разграничение прав доступа пользователей к операционной системе и управлению программным комплексом выполняется на этапе аутентификации в исполнениях Продукта класса защиты КС2 и КС3.

В зависимости от уровня доступа, пользователь может быть привилегированным (администратор) и непривилегированным (пользователь с ограниченными возможностями). После аутентификации, в зависимости от уровня, каждый пользователь может выполнять свой определенный набор команд (см. «Команды уровня администратора», «Команды уровня пользователя»).

При аутентификации у пользователя запрашивается пароль и проверяется доступ по этому паролю к контейнеру с секретным ключом (имя пользователя связано с именем контейнера и уровнем доступа в конфигурационном файле). Эти действия выполняются специальной утилитой `auth_login`.

 Copyright © S-Terra CSP 2003 -2014

Изначально в конфигурационном файле `/opt/VPNagent/etc/auth_login.ini` присутствует пользователь `administrator`, для которого указан контейнер с секретным ключом (пароль к контейнеру – `s-terra)`. Измените пароль к контейнеру с ключевой парой, пересоздав заново контейнер.

Для разграничения прав доступа пользователей к операционной системе и управлению программным комплексом выполните следующие действия:

1. Создайте для пользователей контейнеры с секретными ключами, защищенные паролем.
2. Выполните необходимые настройки в конфигурационном файле `auth_login.ini`, где для каждого пользователя укажите уровень доступа и имя контейнера, а также некоторые дополнительные параметры (см. раздел «Настройки конфигурационного файла»).

Создание контейнеров с секретными ключами

В случае применения СКЗИ «КриптоПро CSP», для создания контейнера можно использовать утилиту `csptest` (утилита находится в каталоге `/opt/cprocsp/bin/ia32` или `/opt/cprocsp/bin/amd64)`, например:

```
csptest -keyset -newkeyset -container 'HDIMAGE\\contadmin' -machinekeyset -password 123456
```

В случае применения криптобиблиотеки от компании «С-Терра СиЭсПи», для создания контейнера используйте утилиту `cont_mgr` (описание утилиты приведено в документе «Специализированные команды»). Пример:

```
/opt/VPNagent/bin/cont_mgr create -cont contadmin –PIN 123456
```

Особенности подготовки контейнеров на платформе МСМ

В связи с тем, что платформа МСМ не оснащена физическим ДСЧ, в процедуре подготовки контейнеров при смене пароля или регистрации новых пользователей есть особенности, которые описаны ниже.

При подготовке контейнеров для «С-Терра Шлюз» на платформе МСМ возможны два варианта:

1. Администратор, используя СКЗИ «КриптоПро CSP», может создать контейнеры на своем рабочем месте и затем доставить их на МСМ.

   Для создания контейнера используйте утилиту `csptest` (пример см. выше).

   Выполните копирование контейнера с секретным ключом с одного ключевого носителя на другой следующей командой, например:

   ```
   csptest -keycopy -machinekeyset -src '\\.\media\src_cont' -dest '\\.\media\dst_cont'
   ```

   Если на модуле применяется криптобиблиотека компании «С-Терра СиЭсПи», доставленные контейнеры нужно конвертировать с помощью команды `cpkey_conv` (описание утилиты приведено в документе «Специализированные команды»).
2. Администратор, используя СКЗИ «КриптоПро CSP» (класс защиты КС2/КС3) и электронный замок «Соболь», может изготовить внешнюю гамму, доставить ее безопасным способом на МСМ и затем, используя утилиту `csptest` или `cont_mgr`, как это описано выше, создать на МСМ контейнеры с секретными ключами.

 Copyright © S-Terra CSP 2003 -2014

Для изготовления внешней гаммы в командной строке запустите утилиту `genkpim`, например:

```
genkpim.exe 500 12121111 f:\gamma
```

`500` – необходимое количество случайных отрезков гаммы для записи на носитель,

`12121111` – номер комплекта внешней гаммы (8 символов в 16-ричном коде),

`f:\gamma` – путь на носителе, по которому будет записан файл с внешней гаммой.

В результате выполнения команды создается файл `kis_1`, который записывается на носитель по пути `f:\gamma` дублированием в два каталога: `DB1` и `DB2`.

Далее действия будут различаться в зависимости от используемого СКЗИ:

- В случае использования СКЗИ «КриптоПро CSP», выполните копирование файлов с внешней гаммой с носителя на MCM в следующие каталоги: `/var/opt/cprocsp/dsrf/db1/` и `/var/opt/cprocsp/dsrf/db2/` соответственно.
- В случае использования криптобиблиотеки от компании «С-Терра СиЭсПи», выполните копирование одного файла с внешней гаммой с носителя на MCM, в каталог `/var/s-terra/ext-gamma`. Переименуйте файл с внешней гаммой в `eg_data`.
  В конфигурационном файле `/etc/S-Terra/skzi.conf` пропишите путь до каталога с внешней гаммой:

  ```
  ExtGammaPath=/var/s-terra/ext-gamma
  ```

Надёжно удалите файлы с внешней гаммой с носителя. После этого перезагрузите модуль и создайте контейнеры с секретными ключами.

Настройки конфигурационного файла

Настройки утилиты `auth_login` выполняются в конфигурационном файле `/opt/VPNagent/etc/auth_login.ini`, представляющем обычный текстовый файл.

Строки, начинающиеся с восклицательного знака (!), считаются комментариями и игнорируются. Пустые строки игнорируются.

В начале файла идут опциональные глобальные настройки, а затем – секции.

Глобальные настройки – автологин

Задается глобальный параметр – автологин. Для выполнения автологина необходимо, чтобы далее в настройках присутствовал администратор (пользователь с параметром `role=admin`), у которого указан пустой пароль. Этот администратор должен быть первым по счету.

```
autostart={ on | off }
```

`on` автологин включен. При первом старте утилиты делается попытка выполнить автологин.

`off` автологин отключен (значение по умолчанию).

Секции

В каждой секции задаются параметры отдельного пользователя.

```
[<section_name>]
```

 Copyright © S-Terra CSP 2003 -2014

```
<param_name>=<param_val>
```

где

`<section_name>` имя секции задает имя пользователя

`<param_name>` имя параметра,

`<param_val>` значение параметра.

Возможные параметры:

`role={ admin | user }`

`admin`	администратор
`user`	пользователь (значение по умолчанию)

`container=<container_name>`

`container_name`	имя контейнера, к которому производится проверка доступа. Обязательный параметр.

`public_key=<public_key_file_path>`

`public_key_file_path`	путь к файлу с публичным ключом. Опциональная защита от подмены контейнера: проверка подписи с использованием публичного ключа, сохраненного отдельно от контейнера. При отсутствии параметра – подпись не проверяется.

Экспортировать публичный ключ из контейнера в файл, при использовании СКЗИ «КриптоПро CSP» можно выполнив команду:

```
/opt/cprocsp/bin/ia32/csptest -keyset -container '<container_name>' -keytype signature -machinekeyset -export <public_key_file_path>
```

Примечание: если в контейнере присутствует только ключ типа exchange, следует заменить в команде `-keytype signature` на `-keytype exchange`.

Экспортировать публичный ключ из контейнера в файл, при использовании криптобиблиотеки компании «С-Терра СиЭсПи» можно выполнив команду:

```
/opt/VPNagent/bin/cont_mgr export -cont <container_name> -PIN <container_passwor> -ext <public_key_file_path>
```

`config_user=<cs_console_user>`

`cs_console_user`	пользователь ОС, от имени которого происходит вход в режим конфигурирования (запуск cs_console). Имеет смысл только для администратора. Пользователь <cs_console_user> обязательно должен присутствовать в ОС и иметь cs_console в качестве Shell. При отсутствии параметра делается попытка подставить имя администратора в качестве <cs_console_user>. Если <cs_console_user> отсутствует в ОС или его Shell отличен от cs_console, cs_console запускается от имени пользователя `root`.

Пример конфигурационного файла

Ниже приведен пример файла `auth_login.ini` в случае применения СКЗИ «КриптоПро CSP».

```
! This is a comment
```

 Copyright © S-Terra CSP 2003 -2014

```
autostart=on

[admin]
role=admin
container=HDIMAGE\\admincont
public_key=/opt/VPNagent/etc/admincont_public_key
config_user=cscons

[user]
role=user
container=HDIMAGE\\usercont
public_key=/opt/VPNagent/etc/usercont_public_key
```

Пример конфигурационного файла при использовании криптобиблиотеки компании «С-Терра СиЭсПи».

```
! This is a comment

autostart=on

[admin]
role=admin
container=file://admincont
public_key=/opt/VPNagent/etc/admincont_public_key
config_user=cscons

[user]
role=user
container= file://usercont
public_key=/opt/VPNagent/etc/usercont_public_key
```

Описание работы утилиты

При старте утилита `auth_login` пишет свое название:

```
S-Terra Gate administrative console.
```

Если утилита запускается первый раз после рестарта системы и разрешен автологин, то для первого, присутствующего в настройках конфигурационного файла администратора, проверяется доступ по пустому паролю к его контейнеру с секретным ключом. При успешной проверке запускается сервис безопасности:

```
Performing autostart as user <admin_name>
```

 Copyright © S-Terra CSP 2003 -2014

```
Configuring IPsec driver:
Starting IPsec daemon...done.
Autostart finished
```

Если автологин не разрешен, то запрашивается имя пользователя (пустое имя пользователя не допускается – при этом выдается повторный запрос):

```
login as:
```

Далее запрашивается пароль (пустой пароль допускается):

```
<name>'s password:
```

Производится проверка, не заблокирован ли данный пользователь (подробнее см. подраздел «Ограничение на количество попыток входа в систему»). На данном этапе может быть выдано сообщение:

```
% The maximum number of login attempts for user <name> has been reached.
User has been blocked
```

Сообщение может появиться .в следующих случаях:

- Реальный пользователь (описанный в файле `/opt/VPNagent/etc/auth_login.ini`) ранее исчерпал допустимые попытки входа в систему и теперь заблокирован.
- Попытка входа в систему неизвестным (не описанным в файле `/opt/VPNagent/etc/auth_login.ini`) пользователем.
- Поврежден (имеет некорректный формат) файл, в котором хранится количество оставшихся попыток входа в систему данного пользователя.
- Системная ошибка (не удалось прочитать или записать количество оставшихся попыток).

Пользователь не может отличить эти ситуации. Однако в логе, доступном администратору, эти ситуации можно различить по коду ошибки в сообщении.

Производится проверка полученного имени и пароля. Если проверка не пройдена:

Выполняется остановка исполнения на промежуток времени от 1 до 3 секунд.

На консоль выдается сообщение об ошибке:

```
% Access denied
```

Если у пользователя еще остались допустимые попытки входа в систему, выдается сообщение об их количестве:

```
% You have <n> attempt(s) left
```

где <n> – число оставшихся попыток (от 1 до 9).

Если была использована последняя попытка входа в систему, выдается сообщение о блокировке пользователя:

```
% The maximum number of login attempts for user <name> has been
reached. User has been blocked
```

Выполняется остановка исполнения на 1 секунду.

ОС автоматически перезапускает утилиту для повторения попытки аутентификации

При использовании криптобиблиотеки компании «С-Терра СиЭсПи», при проверке полученного имени и пароля возможо отсутствие инициализированного ДСЧ (например, при первом входе в систему). В этом случае:

На консоль выдается сообщение:

 Copyright © S-Terra CSP 2003 -2014

```
RNG initialization is required. Press Enter to continue...
```

Когда пользователь нажимает на `Enter`, запускается программа `rnd_mgr`. Происходит инициализация ДСЧ:

Если присутствует соответствующая аппаратная поддержка (например «Соболь») или если присутствует внешняя гамма, инициализация проходит неинтерактивно.

В противном случае вызывается интерактивная инициализация.

После успешной инициализации на консоль выдается сообщение от утилиты:

```
Successfully initialized RNG.
```

В случае успешной аутентификации, пользователь получает доступ к определенному набору команд. Пользователю выдается приглашение командного интерпретатора. Вид приглашения зависит от уровня доступа пользователя:

для администратора: `hostname#`

для пользователя: `hostname>`,

где

`hostname` – имя хоста, на котором работает программа.

Ключевые слова команд можно сокращать до того количества символов, при котором их можно однозначно идентифицировать.

При выполнении команд (включая `configure`) работают специальные сочетания клавиш:

Прерывание выполнения запущенного процесса: CTRL+^ (CTRL+SHIFT+6). При работе через консоль Cisco IOS (стандартный режим работы программы) следует нажать указанное сочетание клавиш два раза, поскольку Cisco IOS перехватывает CTRL+^.

Если указанное выше сочетание клавиш не работает (например, внешний процесс завис), можно нажать на CTRL+| – в этом случае будет послан SIGKILL – неперехватываемый сигнал, по которому выполнение внешней программы безусловно прекращается.

Поддерживаются специальные команды редактирования командной строки, аналогичные Cisco-like консоли (см. документ «Cisco-like команды»).

Ограничение на количество попыток входа в систему

Для каждого пользователя допускается 10 попыток входа в систему. Если все попытки входа в систему оказываются неуспешными, пользователь блокируется. При успешном входе в систему количество оставшихся попыток входа в систему возвращается к своему начальному значению (10).

Счетчик допустимого количества попыток входа в систему хранится в файле: `/var/cspvpn/auth_login_count.<name>`, где `<name>` – имя пользователя.

Отсутствие файла обозначает, что допускаются 10 попыток входа в систему.

Файл будет создан при первой попытке входа соответствующим пользователем. Пользователь должен быть описан в конфигурационном файле `/opt/VPNagent/etc/auth_login.ini`. Для неизвестного пользователя, отсутствующего в файле `auth_login.ini`, файл со счетчиком не создается.

Администратор может разблокировать пользователя, удалив соответствующий файл со счетчиком (`/var/cspvpn/auth_login_count.<name>`). **Примечание: если будут заблокированы все администраторы, вход в систему будет невозможен**.

 Copyright © S-Terra CSP 2003 -2014

Формат файла `/var/cspvpn/auth_login_count.<name>` – бинарный (Owner – root. Group – root. Mode – 0600.). Длина файла – 1 байт. В этом байте в виде числа хранится количество оставшихся попыток входа в систему.

Если в файле хранится число 0 –- это обозначает, что пользователь заблокирован. Если файл имеет неправильный формат (длина отлична от 1 или прочитанное число больше 10), то пользователь также фактически заблокирован. Отличить данную ситуацию от предыдущей можно по коду ошибки (см. раздел «Протоколирование событий», Таблица 4).

Команды уровня администратора

Вход в режим настройки системы (запуск системного shell):

`system`

Команда необходима для начальной настройки системы и в аварийных ситуациях. В остальных случаях рекомендуется пользоваться командой

`configure`

Сначала на консоль выдается сообщение:

```
Entering system shell...
```

Далее запускается интерактивная сессия системного shell.

При выходе из системного shell выдается сообщение:

```
Leaving system shell...
```

При необходимости аварийного завершения выполнения системного shell можно использовать сочетания клавиш `CTRL+^ (CTRL+SHIFT+6)` или `CTRL+|`.

Запуск сервиса безопасности (аналогично `/etc/init.d/vpngate start`):

`start`

Остановка работы системы. Сначала останавливается сервис безопасности, затем происходит останов ОС:

`stop`

Перезагрузка системы. Сначала останавливается сервис безопасности, затем происходит перезагрузка ОС:

`reboot`

Вход в режим настройки С-Терра Шлюз (запуск cs_console – Cisco-like интерфейс командной строки):

`configure`

Если заданный в настройках пользователь, под которым должен производиться вход в конфигурационный режим, отсутствует в ОС или его Shell отличается от `cs_console`, `cs_console` запускается от имени пользователя `root` с выдачей предупреждения в лог и на консоль:

```
% Warning: configuring as user root. Check the 'config_user' setting
in /opt/VPNagent/etc/auth_login.ini
```

Сначала на консоль выдается сообщение:

```
Entering cs_console...
```

Далее запускается `cs_console`.

 Copyright © S-Terra CSP 2003 -2014

При выходе из `cs_console` выдается сообщение:

```
Leaving cs_console...
```

Следует учитывать, что приглашения командного интепретатора `cs_console` аналогичны приглашениям командного интерпретатора программы. Для того чтобы их отличать, рекомендуется ориентироваться на приведенные выше сообщения.

При необходимости аварийного завершения выполнения `cs_console` можно использовать сочетания клавиш `CTRL+^ (CTRL+SHIFT+6)` или `CTRL+|`

Администратору также доступны команды уровня пользователя.

Команды уровня пользователя

Выдача версии продукта (аналогична запуску утилиты `/opt/VPNagent/bin/vershow`):

`show version`

Выдача информации о текущей конфигурации (аналогична запуску утилиты `/opt/VPNagent/bin/lsp_mgr show`):

`show config`

Выдача текущей информации о статусе защиты (аналогична запуску утилиты `/opt/VPNagent/bin/sa_mgr show`):

`show status`

Выход из утилиты приведет к перезапуску утилиты и запросу имени пользователя:

`exit`

Сообщения об ошибках при вводе команд

При вводе синтаксически неправильной команды выдается сообщение об ошибке следующего вида:

```
          ^
% Invalid input detected at '^' marker.
```

Маркер `'^'` указывает на первый ошибочный символ, встреченный при разборе строки.

Если введена незавершенная команда, то выдается сообщение:

```
% Incomplete command
```

Если введена команда, допускающая неоднозначное толкование (как правило, из-за чрезмерного сокращения ключевых слов), выдается сообщение:

```
Ambiguous command: "<введенная_команда>"
```

Протоколирование событий

В процессе работы выдаются сообщения в syslog с использованием `facility=authpriv`.

Список сообщений приведен в Таблица 3.

Таблица 3

Severity	Сообщение	Пояснение
err	% Error: failed to read settings from	Не удалось прочитать настройки

 Copyright © S-Terra CSP 2003 -2014

	/opt/VPNagent/etc/auth_login.ini	программы. Отсутствует или испорчен файл. Программа аварийно завершается.
err	% Error: failed to set the root identity	Не удалось выставить идентификатор пользователя root. В нормальной ситуации не должно возникать. Программа аварийно завершается.
err	% Internal error: parser initialization failed	Внутренняя ошибка: проблемы с инициализацией парсера. В нормальной ситуации не должно возникать. Программа аварийно завершается.
err	% Error: failed to read the command list from /opt/VPNagent/etc/auth_login_cmd.xml	Не удалось прочитать базу команд. Отсутствует или испорчен файл. Программа аварийно завершается.
err	Autostart failed	Не удалось выполнить автологин.
info	Autostart failed. Error code: <err_code>	Не удалось выполнить автологин. Выдается вместе с предыдущим сообщением, но с использованием severity=info. Система должна быть настроена так, чтобы сообщения с уровнем info не были доступны не идентифицированному пользователю.
err	Attempt to login as user <name> failed	Не пройдена проверка имени оператора и пароля.
info	Attempt to login as user <name> failed. Error code: <err_code>	Не пройдена проверка имени оператора и пароля. Выдается вместе с предыдущим сообщением, но с использованием severity=info. Система должна быть настроена так, чтобы сообщения с уровнем info не были доступны не идентифицированному пользователю.
err	Failed to set the autostart marker	Не удалось выставить признак выполненного автологина. Может приводить к тому, что попытка выполнения автологина будет делаться при каждом старте утилиты (неопасная ситуация). В нормальной ситуации не должно возникать.
notice	User <name> logged in	Оператор с именем <name> успешно получил доступ.

 Copyright © S-Terra CSP 2003 -2014

notice	Autostart performed as user <name>	Автологин выполнен успешно от имени оператора <name>.
notice	User <name> called command: <command>	Оператор <name> выполнил команду <command>
notice	User <name> logged out	Оператор <name> вышел из программы
warning	% Warning: configuring as user root. Check the 'config_user' setting in /opt/VPNagent/etc/auth_login.ini	Конфигурирование (запуск cs_console) выполняется от имени пользователя root. Проверьте настройку config_user в файле.
warning	Failed to open the container. Try to initialize RNG.	Не удалось открыть контейнер. Попытка инициализировать ДСЧ. (При использовании криптобиблиотеки от компании «С-Терра СиЭсПи»)

В сообщениях с уровнем info, говорящих об ошибке аутентификации (попытка автологина или входа оператора) пишется код ошибки. Возможные сообщения приведены в Таблица 4.

Таблица 4

Код ошибки	Пояснение
1	В настройках отсутствует администратор (только для сообщения "Autostart failed").
2	Неизвестное имя оператора (отсутствует в настройках; только для сообщения "Attempt to login as user <name> failed").
3	Контейнер не найден.
4	Не удалось загрузить публичный ключ (public_key ссылается на несуществующий или ошибочный файл).
5	Не удалось подписать тестовые данные. Наиболее вероятная причина - введен неправильный пароль.
6	Не удалось проверить подпись. Наиболее вероятные причины - подмененный контейнер или ошибочный публичный ключ.
7	Не удалось получить из контейнера подходящий ключ для подписи тестовых данных.
8	Криптографическая проблема. Наиболее вероятные причины – «КриптоПро» не установлено, не зарегистрировано или нарушена его целостность.
9	Пользователь исчерпал допустимые попытки входа в систему и теперь заблокирован.
10	Поврежден (имеет некорректный формат) файл, в котором хранится количество оставшихся попыток входа в систему данного пользователя

 Copyright © S-Terra CSP 2003 -2014

	или Системная ошибка (не удалось прочитать или записать количество оставшихся попыток).

Сообщения, выдаваемые на консоль

Список сообщений выдаваемых на консоль приведен в Таблица 5.

Таблица 5

Сообщение	Тип	Дублирование в syslog	Пояснение
S-Terra Gate administrative console	информационное		Стартовое сообщение.
Performing autostart as user <admin_name>	информационное		Начало автологина.
Autostart finished	информационное		Завершение автологина.
% Error: failed to read settings from /opt/VPNagent/etc/auth_login.ini	ошибка	+	Не удалось прочитать настройки из файла.
% Error: failed to set the root identity	ошибка	+	Не удалось выставить идентификатор пользователя root.
% Internal error: parser initialization failed	ошибка	+	Внутренняя ошибка: проблемы с инициализацией парсера.
% Error: failed to read the command list from /opt/VPNagent/etc/auth_login_cmd.xml	ошибка	+	Не удалось прочитать базу команд.
% Warning: configuring as user root. Check the 'config_user' setting in /opt/VPNagent/etc/auth_login.ini	предупреждение	+	Конфигурирование (запуск cs_console) выполняется от имени пользователя root. Проверьте настройку config_user в файле.
% Access denied	ошибка		Отказ в доступе.

 Copyright © S-Terra CSP 2003 -2014

% System error, can not spawn process.	ошибка		Не удалось породить новый процесс.
% System error, can not run external application.	ошибка		
% System error, can not create pipe.	ошибка		В нормальной ситуации не должно возникать.
% System error, input redirection to child process failed. Error code: <errno>	ошибка		Не удалось запустить внешнее приложение.
% Warning: Terminal setup failed. Interactive applications could be broken.	ошибка		
Entering cs_console...	информационное		В нормальной ситуации не должно возникать. Возможно не установлен продукт или нарушена его целостность.
Leaving cs_console...	информационное		Системная ошибка.
RNG initialization is required. Press Enter to continue...	информационное		Требуется инициализация ДСЧ. Нажмите Enter для продолжения... (При использовании криптобиблиотеки от компании «С-Терра СиЭсПи»)

 Copyright © S-Terra CSP 2003 -2014

Поведение светодиодов в различных режимах работы модуля

Для быстрой диагностики состояния модуля можно воспользоваться светодиодными индикаторами на его передней панели. В Таблица 6 приведены различные состояния модуля и соответствующее поведение светодиодных индикаторов.

Таблица 6

	Состояние модуля	Поведение светодиодов
1	Если IOS не распознал модуль	EN и остальные индикаторы - не горят
2	До инсталляции продукта	EN – горит остальные – не горят
3	При включении маршрутизатора, при старте или рестарте модуля	SYS и CF – горят в течение 10 сек и гаснут
4	После инсталляции продукта, в нормальном режиме работы модуля	SYS – медленно мигает CF – горит когда производится запись/чтение на компакт-флеш карте
5	При неправильном функционировании и из-за ошибки при старте системы, неправильной конфигурации сетевых интерфейсов или если не запускается vpnsvc1 или какой-либо другой важный процесс системы	SYS – часто мигает (с периодом 0.5 сек)
6	При выключении системы с помощью кнопки shutdown или команды poweroff.	SYS – перестает мигать и горит постоянно, пока процесс shutdown не завершится. По завершению процесса: SYS – гаснет, а CF – зажигается, это указывает на то, что модуль готов к выключению питания (или к повторному старту)..

[1] vpnsvc (vpn service) - процесс, который устанавливает IPsec-соединения, работает по протоколам ISAKMP, SNMP, LDAP, проверяет сертификаты, загружает и интерпретирует native-конфигурацию (LSP).

 Copyright © S-Terra CSP 2003 -2014

Снятие сетевого модуля с маршрутизатора

Выключение сетевого модуля

Перед выключением маршрутизатора выполните выключение модуля. Возможны два варианта выключения модуля.

Вариант 1

Шаг 1: Войдите в систему сетевого модуля пользователем с правами администратора, например, `root` и введите пароль:

```
cspgate login: root

password:
```

Шаг 2: Выключите питание модуля командой:

```
cspgate:~# poweroff
```

Дождитесь окончания выполнения команды.

Вариант 2

Шаг 1: Подготовка к выключению питания модуля осуществляется кратковременным нажатием кнопки «shutdown» (меньше 1 сек) на передней панели модуля. Примерно через 10 секунд произойдет выключение модуля.

Снятие сетевого модуля

Шаг 1: Отключите электропитание маршрутизатора и отсоедините шнур питания от сети переменного тока.

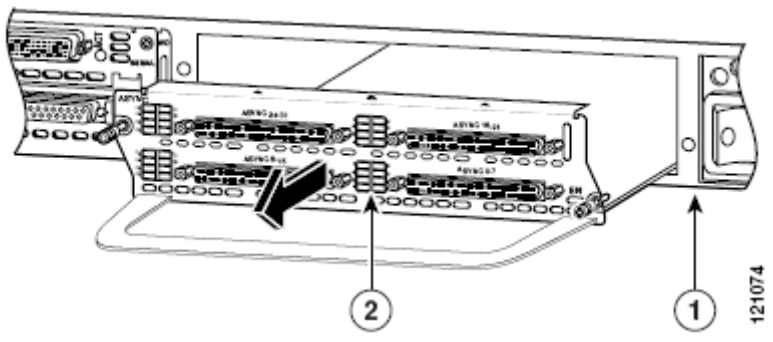


Рисунок 27

 Copyright © S-Terra CSP 2003 -2014

Шаг 2: На маршрутизаторах Cisco серий 2900 и 3900 открутите винты, удерживающие сетевой модульный адаптер в слоте. На маршрутизаторах серий 2800 и 3800 открутите два винта, удерживающих модуль в слоте.

Шаг 3: Взявшись за ручку модуля, выньте модуль или сетевой модульный адаптер с модулем из слота.



Чтобы избежать повреждения модуля всегда используйте ручку сетевого модуля. Не прикасайтесь к монтажной плате.

 Copyright © S-Terra CSP 2003 -2014

Дополнительная информация

Cisco.com

Для получения документации по продуктам компании Cisco Systems и дополнительной информации можно обратиться на сайт www.cisco.com.

Информацию по технической поддержке и документации можно посмотреть по адресу:

http://www.cisco.com/techsupport

Информация по продуктам, документации и технической поддержке так же доступна на российском сайте компании Cisco Systems по адресу:

http://www.cisco.com/global/RU/index.shtml

S-Terra.com

Получить информацию по продуктам компании «С-Терра СиЭсПи» можно по адресу:

http://www.s-terra.com/products/productline/

С документацией по работе с продуктами компании можно ознакомиться по адресу: http://www.s-terra.com/support/documents/

Информацию по технической поддержке можно посмотреть по адресу:

http://www.s-terra.com/support/support/

Copyright © S-Terra CSP 2003 -2014