Пример настройки функции SRST Cisco

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Ограничения
Общие сведения
Нейтрализация открытого текста Cisco IP Phone во время SRST
SRST-маршрутизаторы и протокол TLS
SRST-маршрутизаторы и инфраструктура открытых ключей (PKI)
Сервер учетных записей Cisco IOS на защищенных SRST-маршрутизаторах
Установка защищенного SRST на IP-телефон Cisco
Настройка
Схема сети
Перед настройкой
Конфигурации
Проверка
Проверка параметров учетных записей
Проверки регистрации сертификата
Проверка статуса телефона и регистраций
Устранение неполадок
Отладка параметров учетных записей
Отладка регистраций IP-телефона
Дополнительные сведения

Введение

Этот документ предоставляет пример конфигурации для Cisco Secure Survivable Remote Site Telephony (SRST).

Защищенные IP-телефоны Cisco, расположенные на удаленных узлах и присоединенные к шлюзовым маршрутизаторам, могут устанавливать защищенные соединения с Cisco CallManager через сеть WAN. При нарушении соединения сети WAN или отключения Cisco CallManager все соединения, установленные с помощью удаленных телефонов, становятся незащищенными. Во избежание подобной ситуации шлюзовые маршрутизаторы в настоящее время функционируют в режиме защищенной SRST, активирующемся при нарушении соединений сети WAN или сбоя Cisco CallManager. При восстановлении соединения сети WAN или подключения Cisco CallManager, это приложение восстанавливает функции обеспечения защищенных вызовов.

Защищенная SRST имеет новые функции обеспечения безопасности, такие как аутентификация, целостность данных и шифрование медиаданных. Функция аутентификации дает возможность участнику разговора быть уверенным, что его собеседник действительно является тем, кем он представился. Функция целостности предоставляет гарантию, что данные не подвергнутся изменениям при прохождении между собеседниками. Функция шифрования обеспечивает конфиденциальность, подразумевающую, что никто кроме нужного получателя не сможет прочитать передаваемые данные. Функция безопасности обеспечивает конфиденциальность голосовых вызовов SRST и защищает от посягательств на личную безопасность, а также от кражи информации, содержащейся в удостоверяющих личность документах.

Обеспечение безопасности SRST выполняется при следующих условиях:

- Оконечные устройства аутентифицируются с использованием сертификатов.
- Сигнализация аутентифицируется и шифруется с использованием протокола безопасности на транспортном уровне (TLS) для TCP.
- Защищенный маршрут данных шифруется с использованием протокола SRTP (защищенный транспортный протокол реального времени).
- Сертификаты генерируются и распространяются сертифицирующим центром (CA).

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

Требования инфраструктуры открытых ключей

- Установите время вручную либо с помощью сетевого протокола синхронизации времени (NTP). Данное действие обеспечивает синхронизацию времени с Cisco CallManager.
- **Запустите сервер IP HTTP (процессор Cisco IOS®) с помощью команды ip http server, если это не было сделано ранее.** Дополнительную информацию по использованию инфраструктуры открытых ключей (PKI) см. в документе Сервер сертификатов Cisco IOS.
- Если сервер сертификатов активирован в вашей стартовой конфигурации, данные сообщения могут отображаться во время загрузки:`% Failed to find Certificate Server's trustpoint at startup`

  `% Failed to find Certificate Server's cert.`Данные сообщения являются информационными и указывают на временную невозможность проведения настройки сервера сертификатов, т. к. анализ стартовой конфигурации не завершен. Данные сообщения применяются в процессе отладки в случае неработоспособности стартовой конфигурации. **Статус сервера сертификатов можно проверить после завершения загрузки с помощью команды show crypto pki server.**

Требования SRST

- Службы защищенной SRST не могут быть зарегистрированы при активной SRST.

Отключение SRST по этой причине возможно с помощью команды no call-manager-fallback.

- Список поддерживаемых IP-телефонов Cisco, маршрутизаторов, сетевых модулей и кодеков для защищенного SRST см. в документе Функция аутентификации средств связи и сигнализации и функция шифрования для шлюзов Cisco IOS MGCP.
- Обновляемую информацию по максимальному количеству IP-телефонов Cisco, телефонных номеров (DN) или виртуальных голосовых портов и требования к памяти для Cisco SRST см. в документе Микропрограммное обеспечение, платформы, память и программные продукты для голосовой передачи, поддерживаемые Cisco Unified SRST 4.0.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Защищенные IP-телефоны Cisco, поддерживаемые в защищенной SRST, должны иметь установленные сертификаты и активированную функцию шифрования.
- Маршрутизатор SRST должен иметь сертификат. Сертификат может быть сгенерирован третьей стороной или сертифицирующим центром (CA) Cisco IOS. Сертифицирующий орган Cisco IOS может функционировать на одном шлюзе с SRST.
- Список доверия сертификатов (CTL) должен быть запущен в Cisco CallManager. *Полную информацию см. в разделе Настройка защищенных вызовов IP-телефонии документа Аутентификация средств передачи данных и сигналов и функция шифрования для шлюзов Cisco IOS MGCP.*
- Должен быть установлен Cisco CallManager версии 4.1(2) или более поздней с поддержкой режима обеспечения безопасности (режим аутентификации и шифрования).
- Маршрутизатор/шлюзы, которые выполняют безопасный SRST, должны поддержать голос - и поддерживающие безопасность Образы Cisco IOS (образ криптографического программного обеспечения Г k9Г). Поддерживаются два образа: Advanced IP Services, включающие некоторые дополнительные функции безопасности, и Advanced Enterprise Services, включающая полное программное обеспечение Cisco IOS.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Ограничения

Основные ограничения

- Функции криптографического программного обеспечения (Г k9Г) находятся под

экспортным контролем. Данный программный продукт имеет криптографические функции и попадает под действие законодательства Соединенных Штатов Америки и местных законов, регулирующих импорт, экспорт, передачу и использование. Поставка криптографического программного обеспечения Cisco не подразумевает права третьей стороны на импорт, экспорт, распространение или использование криптографических средств. Импортеры, экспортеры, дистрибьюторы и пользователи несут ответственность за соблюдение законодательства США и местных законов. Используя данный продукт, вы принимаете на себя обязательства по соблюдению действующих законов и положений. Если вы не можете действовать в соответствии с требованиями законодательства США и местных законов, немедленно произведите возврат продукта.Ознакомиться с кратким содержанием законов США, регулирующих использование криптографических продуктов Cisco, можно на странице:http://www. cisco . com/wwl/export/crypto/tool/Для получения дополнительных консультаций свяжитесь с компанией, отправив письмо по адресу: export@cisco.com.

- То, когда Безопасный Протокол транспорта в реальном времени (SRTP) зашифровал вызов, сделано между оконечными точками Cisco IP Phone или от Cisco IP Phone до оконечной точки шлюза, значок блокировки отображен на IP-телефонах. Замок указывает на обеспечение безопасности только для ответвления IP, относящегося к совершаемому вызову. Безопасность для ответвления PSTN не применяется.
- Защищенная SRST поддерживается только в пределах одного маршрутизатора.

Программное обеспечение и функции, неподдерживаемые в режиме защищенной SRST

- Версии Cisco CallManager ранее 4.1(2)
- Защищенный режим MoH (музыкальная заставка при удержании вызова)
- Защищенное транскодирование или конференц-связь
- Защищенный H.323 или протокол SIP
- Протокол маршрутизатора горячего резервирования (HSRP)

Поддерживаемые вызовы в режиме защищенной SRST

В режиме защищенной SRST поддерживаются только голосовые вызовы. Поддерживаются следующие голосовые вызовы:

- Обычный вызов
- Переадресация вызова (занято, нет ответа, все вызовы)
- Линия коллективного пользования (IP-телефоны)
- Перевод вызова на телефонный номер третьего абонента (с/без совершения консультативного вызова)
- Удержание и восстановление

Общие сведения

Нейтрализация открытого текста Cisco IP Phone во время SRST

Версии Cisco SRST ранее, чем программное обеспечение Cisco IOS версии 12.3(14)T не в состоянии поддержать безопасные соединения или включить безопасность. Если маршрутизатор SRST не способен к безопасному SRST как нейтрализация modeâ т.е. это не в состоянии завершить подтверждение связи TLS с Cisco CallManagerâ , ее сертификат не добавлен к файлу конфигурации Cisco IP Phone. Отсутствие сертификата SRST-

маршрутизатора приводит к использованию IP-телефоном Cisco незащищенного (открытый текст) соединения в режиме fallback SRST. Возможность обнаружения и нейтрализации неисправности в режиме открытого текста встроена в микропрограммное обеспечение IP-телефона Cisco. Дополнительную информацию по режиму открытого текста см. в документе Аутентификация средств передачи данных и сигналов и функция шифрования для шлюзов Cisco IOS MGCP.

SRST-маршрутизаторы и протокол TLS

Transport Layer Security (TLS) версии 1.0 обеспечивает защищенные TCP-каналы между IP-телефонами Cisco, SRST-маршрутизаторами и Cisco CallManager. Работа TLS начинается, когда IP-телефон Cisco устанавливает TLS-соединение в процессе регистрации с помощью Cisco CallManager. Если Cisco CallManager настроен на fallback для SRST, также устанавливается TLS-соединение между IP-телефонами Cisco и защищенным SRST-маршрутизатором. При неполадках Cisco CallManager или в соединении WAN, управление вызовами возвращается к SRST-маршрутизатору.

SRST-маршрутизаторы и инфраструктура открытых ключей (PKI)

Передача сертификатов между SRST-маршрутизатором и Cisco CallManager обязательна для функционирования защищенного SRST. Команды инфраструктуры открытых ключей (PKI) используются, чтобы генерировать, импортировать, и экспортировать сертификаты для безопасного SRST. Сертификаты для каждого поддерживаемого IP-телефона Cisco показаны в данной таблице.

Таблица 1 – Поддерживаемые сертификаты и IP-телефоны Cisco

Cisco IP Phone 7940	Cisco IP Phone 7960	IP-телефон Cisco 7970
Телефон получает локально значимый сертификат (LSC) от функции прокси сертифицирующего центра (CAPF) в формате DER. Имя файла сертификата: 59fe77ccd.0 имя файла может измениться на основе имени	Телефон получает локально значимый сертификат (LSC) от функции прокси сертифицирующего центра (CAPF) в формате DER. Имя файла сертификата: 59fe77ccd.0 имя файла может измениться на основе имени субъекта сертификата CAPF и издателя сертификата CAPF. Если Cisco CallManager использует стороннего поставщика сертификатов, возможно присутствие множества .0 файлов (от двух до десяти). Каждый .0 файл сертификата должен быть импортирован в индивидуальном порядке	Телефон содержит установленный производителем сертификат (MIC), используемый для аутентификации устройства. Если Cisco 7970 использует MIC, необходимы два открытых сертификационных файла: • CiscoCA.

субъекта сертификата CAPF и издателя сертификата CAPF. Если Cisco CallManager использует стороннего поставщика сертификатов, возможно присутствие множества .0 файлов (от двух до десяти). Каждый .0 файл сертификата должен быть импортирован в индивидуальном порядке в процессе настройки. Поддерживается только ручная регистрация.	в процессе настройки. Поддерживается только ручная регистрация.	pem (Cisco Root CA, используемый для аутентификации сертификата) • a69d2e04.0, в формате электронной почты с усовершенствованной защитой (PEM) Если Cisco CallManager использует стороннего поставщика сертификатов, возможно присутствие множества .0 файлов (от двух до десяти). Каждый .0 файл сертификата должен быть импортирован в индивидуальном порядке в процессе настройки. Поддерживается только ручная регистрация.

Сервер учетных записей Cisco IOS на защищенных SRST-маршрутизаторах

Защищенная SRST использует сервер учетных записей, функционирующий на защищенных

SRST-маршрутизаторах. Когда клиент, Cisco CallManager, запрашивает сертификат по каналу TLS, сервер учетных записей предоставляет сертификат SRST-маршрутизатора менеджеру звонков. Cisco CallManager помещает сертификат SRST-маршрутизатора в конфигурационный файл IP-телефона и загружает конфигурационные файлы в телефоны. Защищенный IP-телефон Cisco использует сертификат для аутентификации SRST-маршрутизатора во время fallback-операций. Сервер учетных записей функционирует на порту TCP 2445, устанавливаемом по умолчанию.

Пять новых команд Cisco IOS используются для настройки сервера учетных записей в fallback-режиме менеджера звонков и предоставляют возможность отладки и проверки сервера:

- учетные данные
- debug credentials
- ip source-address (credentials)
- show credentials
- trustpoint (credentials)

Установка защищенного SRST на IP-телефон Cisco

На схеме показано сетевое взаимодействие сервера учетных записей на SRST-маршрутизаторе, Cisco CallManager и IP-телефона Cisco, которое необходимо для обеспечения защищенного SRST для IP-телефона Cisco.

1. IP-телефон производит настройку DHCP и получает адрес TFTP-сервера.
2. IP-телефон получает CTL-файл с сервера TFTP. CTL-файл содержит сертификаты, принимаемые телефоном.
3. IP-телефон Cisco открывает канал протокола TLS и регистрируется в Cisco CallManager.

Cisco CallManager экспортирует информацию и сертификат защищенного SRST-маршрутизатора в IP-телефон Cisco. Телефон помещает сертификат в свой конфигурационный файл. Как только телефон получает SRST-сертификат, SRST-маршрутизатор признается защищенным.

Если Cisco IP Phone настроен как â authenticatedâ или â encryptedâ , и Cisco CallManager настроен в смешанном режиме, телефон ищет сертификат SRST в своем файле конфигурации. В случае нахождения SRST-сертификата, телефон устанавливает предварительное TLS-соединение на порту по умолчанию. Портом по умолчанию является TCP-порт IP-телефона Cisco плюс 443, на SRST-маршрутизаторе это порт 2443.

Соединение с SRST-маршрутизатором происходит автоматически, до момента появления вторичного Cisco CallManager и пока SRST настроена как резервирующее устройство.

Cisco CallManager должен быть настроен в смешанном режиме, этот режим является защищенным.

В случае сбоя WAN IP-телефон Cisco начинает регистрацию SRST. IP-телефон Cisco регистрируется с помощью SRST-маршрутизатора на порту, установленном по умолчанию, для обеспечения защищенной связи.

Настройка

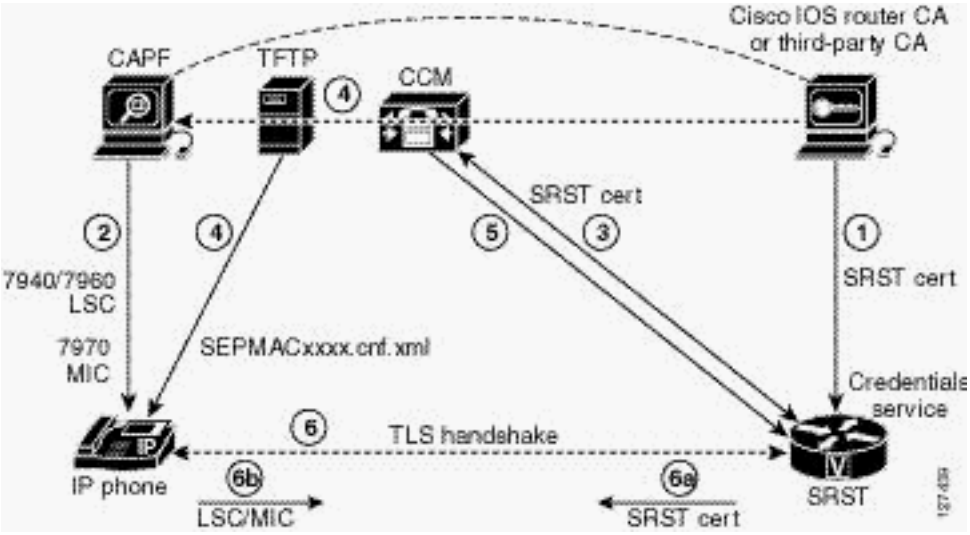
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Защищенный SRST-маршрутизатор и IP-телефоны Cisco должны запрашивать взаимную аутентификацию во время TLS-соединения. TLS-соединение происходит в момент регистрации телефона на SRST-маршрутизаторе до или после нарушения WAN-соединения. Пример конфигурации не включает в себя использование стороннего сертифицирующего органа. Для генерирования сертификатов предполагается использование сервера сертификатов Cisco IOS.

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме. На схеме показан процесс аутентификации и шифрования защищенного SRST.



1. Сервер сертификатов, являющийся сертификационным маршрутизатором Cisco IOS или сторонним поставщиком сертификатов, предоставляет сертификат устройства на SRST-шлюз для запуска службы учетных записей. Также сертификат может быть сгенерирован SRST-маршрутизатором с сервером Cisco IOS CA.Маршрутизатор CA является окончательной точкой доверия для функции прокси (представителя) сертифицирующего центра (CAPF). Дополнительную информацию по CAPF см. в документе Руководство по безопасности Cisco CallManager.

2. CAPF – это процесс, в ходе которого поддерживаемые устройства могут запрашивать локально значимый сертификат (LSC). Утилита CAPF генерирует криптографическую пару и сертификат, специфичный для CAPF, копирует данный сертификат на все серверы Cisco CallManager в группе и предоставляет LSC в IP-телефон Cisco. LSC требуется IP-телефонам, не имеющим предустановленного производителем сертификата (MIC). Cisco 7970 снабжен MIC и не нуждается в прохождении процесса CAPF.
3. Cisco CallManager запрашивает SRST-сертификат с сервера учетных записей, и сервер предоставляет необходимый сертификат.
4. Для каждого устройства Cisco CallManager использует TFTP-процесс и вставляет сертификат в конфигурационный файл SEPMACxxxx.cnf.xml IP-телефона Cisco.
5. Cisco CallManager предоставляет SRST-маршрутизатору файлы в формате PEM, содержащие сертификационную информацию телефона. Файлы PEM предоставляются в SRST-маршрутизатор вручную. После получения PEM-файлов, маршрутизатор может аутентифицировать IP-телефон и проверить источник его сертификата в процессе TLS-соединения.
6. Между IP-телефоном Cisco и SRST-маршрутизатором происходит TLS-соединение, обмен сертификатами, взаимная аутентификация и регистрация.SRST-маршрутизатор отправляет свой сертификат, и телефон сравнивает данный сертификат с полученным от Cisco CallManager в Шаге 4.IP-телефон Cisco предоставляет SRST-маршрутизатору сертификаты LSC и MIC, и маршрутизатор сравнивает данные сертификаты с PEM-файлами, полученными в Шаге 5.**Примечание:** Среды зашифрованы автоматически однажды телефон, и сертификатами маршрутизатора обмениваются, и TLS подключение установлен с маршрутизатором SRST.

Перед настройкой

Cisco CallManager

Выполните следующие действия:

1. При запуске службы учетных записей на SRST-маршрутизаторе SRST-ссылка должна быть добавлена в Cisco CallManager, т.к. Cisco CallManager осуществляет соединение с маршрутизатором для получения его сертификата. *Полную информацию по добавлению SRST в менеджер звонков Cisco см. в разделе Настройка отказоустойчивого удаленного узла телефонии Cisco документа Руководство по управлению Cisco CallManager, версия 4.1(2).*
2. Функция SRST-fallback должна быть настроена на Cisco CallManager. Для этого назначьте совокупность устройств для SRST. *Полную информацию по добавлению совокупности устройств в менеджер звонков см. в разделе Настройка совокупности устройств документа Руководство по управлению Cisco CallManager, версия 4.1(2).*
3. Функции прокси (представителя) сертифицирующего центра (CAPF) должна быть настроена в Cisco CallManager. Процесс CAPF позволяет поддерживаемым устройствам, таким как Cisco CallManager, запрашивать сертификаты LSC у IP-телефонов Cisco. Утилита CAPF генерирует криптографическую пару и сертификат, специфичный для CAPF, копирует данный сертификат на все серверы Cisco CallManager в группе. Полную информацию по настройке CAPF в Cisco CallManager см.

в документе Аутентификация и шифрование IP-телефона Cisco для Cisco CallManager 4.0(1).

Предупреждения по безопасности

- **Команда grant auto позволяет генерировать сертификаты и должна быть активирована после определения основного сертифицирующего органа. Для обеспечения дополнительной безопасности команда grant auto не должна постоянно находиться в активном состоянии и должна быть отключена после генерирования сертификатов.**
- Лучшие условия безопасности достигаются при защите порта службы учетных записей с помощью механизма Control Plane Policing (CoPP). Механизм Control plane policing защищает шлюз и поддерживает пересылку пакетов и состояние протоколов несмотря на высокую загрузку трафика. Дополнительную информацию см. в документе посвященном этому механизму Control Plane Policing. Пример конфигурации также показан в разделе Конфигурация 2 данного документа.

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация 1â Настраивает ваш маршрутизатор согласно этому примеру **show running config**.
- Конфигурация 2â оптимальный метод безопасности должна защитить учетный сервисный порт с контролем уровня управления. **При использовании механизма Control Plane Policing настройте маршрутизатор согласно данному примеру show running-config.**

Конфигурация 1

```
Router#show running-config . . . !--- Define Cisco
CallManager. ccm-manager fallback-mgcp ccm-manager mgcp
ccm-manager music-on-hold ccm-manager config server
10.1.1.13 ccm-manager config ! !--- Define root CA. !---
For SRST routers to provide secure communications, there
must be a !--- CA server that issues the device
certificate in the network. !--- The CA server can be a
third-party CA or one generated from a !--- Cisco IOS
certificate server. The Cisco IOS certificate server !--
- provides a certificate generation option to users who
do not !--- have a third-party CA in their network. The
Cisco IOS certificate !--- can run on the SRST router or
on a different Cisco IOS router. crypto pki server
srstcaserver database level complete database url nvram
issuer-name CN=srstcaserver ! !--- The secure SRST
router needs to define a trustpoint. That is, !--- it
must obtain a device certificate from the CA server. The
procedure !--- is called certificate enrollment. Once
enrolled, the secure SRST router !--- can be recognized
by Cisco CallManager as a secure SRST router. There !---
are three options to enroll the secure SRST router to a
CA server: !--- autoenrollment, cut and paste, and TFTP.
When the CA server is a !--- Cisco IOS certificate
server, autoenrollment can be used. Otherwise, manual !-
-- enrollment is required. Manual enrollment refers to
cut and paste or TFTP. !--- Issue the enrollment URL
command for autoenrollment and the !--- crypto pki
```

```
authenticate command in order to authenticate the SRST
router. !--- Issue the crypto ca enroll command in order
to obtain the SRST router !--- certificate from the CA.
crypto pki trustpoint srstca enrollment url
http://10.1.1.22:80 revocation-check none ! crypto pki
trustpoint srstcaserver revocation-check none rsakeypair
srstcaserver ! !--- Define the CTL/7970/7960 trustpoint
to authenticate secure SRST. !--- Repeat the enrollment
procedure for each phone or PEM file. crypto pki
trustpoint 7970 enrollment terminal revocation-check
none ! crypto pki trustpoint PEM enrollment terminal
revocation-check none ! crypto pki trustpoint 7960
enrollment terminal revocation-check none ! !--- This is
the SRST router device certificate. crypto pki
certificate chain srstca certificate 02 308201AD
30820116 A0030201 02020102 300D0609 2A864886 F70D0101
04050030 17311530 13060355 0403130C 73727374 63617365
72766572 301E170D 30343034 31323139 35323233 5A170D30
35303431 32313935 3232335A 30343132 300F0603 55040513
08443042 39453739 43301F06 092A8648 86F70D01 09021612
6A61736F 32363931 2E636973 636F2E63 6F6D305C 300D0609
2A864886 F70D0101 01050003 4B003048 024100D7 0CC354FB
5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19 C98F9BAE
AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7
A23E6155 FA2ED743 3FB8B902 03010001 A330302E 300B0603
551D0F04 04030205 A0301F06 03551D23 04183016 8014F829
CE97AD60 18D05467 FC293963 C2470691 F9BD300D 06092A86
4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185
D7F0D565 CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D
99CBD267 EB8ADF9D 9E43A5F2 FB2B18A0 34AF6564 11239473
41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E B586FE67
00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7
0B8C2752 C3AF4A66 BD007348 D013000A EA3C206D CF quit
certificate ca 01 30820207 30820170 A0030201 02020101
300D0609 2A864886 F70D0101 04050030 17311530 13060355
0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 34353136 5A170D30 37303431 32313934 3531365A
30173115 30130603 55040313 0C737273 74636173 65727665
7230819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6
32154E99 105CA989 9619993F CC72C525 7357EBAC E6335A32
2AAF9391 99325BFD 9B8355EB C10F8963 9D8FC222 EE8AC831
71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130
0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
01FF0404 03020186 301D0603 551D0E04 160414F8 29CE97AD
6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD
300D0609 2A864886 F70D0101 04050003 8181007A F71B25F9
73D74552 25DFD03A D8D1338F 6792C805 47A81019 795B5AAE
035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55
BB23C66A C80A3A57 5EE85FF8 C1B1A540 E818CE6D 58131726
BB060974 4E1A2F4B E6195522 122457F3 DEDBAAD7 3780136E
B112A6 quit crypto pki certificate chain srstcaserver
certificate ca 01 30820207 30820170 A0030201 02020101
300D0609 2A864886 F70D0101 04050030 17311530 13060355
0403130C 73727374 63617365 72766572 301E170D 30343034
31323139 34353136 5A170D30 37303431 32313934 3531365A
30173115 30130603 55040313 0C737273 74636173 65727665
7230819F 300D0609 2A864886 F70D0101 01050003 818D0030
81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6
```

```
32154E99 105CA989 9619993F CC72C525 7357EBAC E6335A32
2AAF9391 99325BFD 9B8355EB C10F8963 9D8FC222 EE8AC831
71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130
0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
01FF0404 03020186 301D0603 551D0E04 160414F8 29CE97AD
6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD
300D0609 2A864886 F70D0101 04050003 8181007A F71B25F9
73D74552 25DFD03A D8D1338F 6792C805 47A81019 795B5AAE
035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55
BB23C66A C80A3A57 5EE85FF8 C1B1A540 E818CE6D 58131726
BB060974 4E1A2F4B E6195522 122457F3 DEDBAAD7 3780136E
B112A6 quit crypto pki certificate chain 7970
certificate ca 353FB24BD70F14A346C1F3A9AC725675 308203A8
30820290 A0030201 02021035 3FB24BD7 0F14A346 C1F3A9AC
72567530 0D06092A 864886F7 0D010105 0500302E 31163014
06035504 0A130D43 6973636F 20537973 74656D73 31143012
06035504 03130B43 41502D52 54502D30 3032301E 170D3033
31303130 32303138 34395A17 0D323331 30313032 30323733
375A302E 31163014 06035504 0A130D43 6973636F 20537973
74656D73 31143012 06035504 03130B43 41502D52 54502D30
30323082 0120300D 06092A86 4886F70D 01010105 00038201
0D003082 01080282 010100C4 266504AD 7DC3FD8D 65556FA6
308FAE95 B570263B 575ABD96 1CC8F394 5965D9D0 D8CE02B9
F808CCD6 B7CD8C46 24801878 57DC4440 A7301DDF E40FB1EF
136212EC C4F3B50F BCAFBB4B CD2E5826 34521B65 01555FE4
D4206776 03368357 83932638 D6FC953F 3A179E44 67255A73
45C69DEE FB4D221B 21D7A3AD 38184171 8FD8C271 42183E65
09461434 736C77CC F380EEBF 632C7B3F A5F92AA6 A8EF3490
8724A84F 4DAF7FD7 0928F585 764D3558 3C0FE9AF 1ED8763F
A299A802 970004AD 1912D265 7DE335B4 BCB6F789 DC68B9FA
C8FDF85E 8A28AD8F 0F4883C0 77112A47 141DBEE0 948FBE53
FE67B308 D40C8029 87BD790E CDAB9FD7 A190C1A2 A462C5F2
4A6E0B02 0103A381 C33081C0 300B0603 551D0F04 04030201
86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
0E041604 1452922B E288EE2E 098A4E7E 702C56A5 9AB4D49B
96306F06 03551D1F 04683066 3064A062 A060862D 68747470
3A2F2F63 61702D72 74702D30 30322F43 65727445 6E726F6C
6C2F4341 502D5254 502D3030 322E6372 6C862F66 696C653A
2F2F5C5C 6361702D 7274702D 3030325C 43657274 456E726F
6C6C5C43 41502D52 54502D30 30322E63 726C3010 06092B06
01040182 37150104 03020100 300D0609 2A864886 F70D0101
05050003 82010100 56838CEF C4DA3AD1 EA8FBB15 2FFE6EE5
50A1972B D4D7AF1F D298892C D5A2A76B C3462866 13E0E55D
DC0C4B92 5AA94B6E 69277F9B FC73C697 11266E19 451C0FAB
A55E6A28 901A48C5 B9911EE6 348A8920 0AEDE1E0 B6EA781C
FFD97CA4 B03C0E34 0E5B0649 8B0A34C9 B73A654E 09050C1F
4DA53E44 BF78443D B08C3A41 2EEEB873 78CB8089 34F9D16E
91512F0D 3A8674AD 0991ED1A 92841E76 36D7740E CB787F11
685B9E9D 0C67E85D AF6D05BA 3488E86D 7E2F7F65 6918DE0F
BD3C7F67 D8A33F70 9C4A596E D9F62B3B 1EDEE854 D5882AD4
3D71F72B 8FAB7F3C 0B5F0759 D9828F83 954D7BB1 57A638EC
7D72BFF1 8933C16F 760BCA94 4C5B1931 67947A4F 89A1BDB5
quit crypto pki certificate chain PEM certificate ca
7612F960153D6F9F4E42202032B72356 308203A8 30820290
A0030201 02021076 12F96015 3D6F9F4E 42202032 B7235630
0D06092A 864886F7 0D010105 0500302E 31163014 06035504
0A130D43 6973636F 20537973 74656D73 31143012 06035504
03130B43 41502D52 54502D30 3031301E 170D3033 30323036
32333237 31335A17 0D323330 32303632 33333633 345A302E
31163014 06035504 0A130D43 6973636F 20537973 74656D73
31143012 06035504 03130B43 41502D52 54502D30 30313082
```

```
0120300D 06092A86 4886F70D 01010105 00038201 0D003082
01080282 010100AC 55BBED18 DE9B8709 FFBC8F2D 509AB83A
21C1967F DEA7F4B0 969694B7 80CC196A 463DA516 54A28F47
5D903B5F 104A3D54 A981389B 2FC7AC49 956262B8 1C143038
5345BB2E 273FA7A6 46860573 CE5C998D 55DE78AA 5A5CFE14
037D695B AC816409 C6211F0B 3BBF09CF B0BBB2D4 AC362F67
0FD145F1 620852B3 1F07E2F1 AA74F150 367632ED A289E374
AF0C5B78 CE7DFB9F C8EBBE54 6ECF4C77 99D6DC04 47476C0F
36E58A3B 6BCB24D7 6B6C84C2 7F61D326 BE7CB4A6 60CD6579
9E1E3A84 8153B750 5527E865 423BE2B5 CB575453 5AA96093
58B6A2E4 AA3EF081 C7068EC1 DD1EBDDA 53E6F0D6 E2E0486B
109F1316 78C696A3 CFBA84CC 7094034F C1EB9F81 931ACB02
0103A381 C33081C0 300B0603 551D0F04 04030201 86300F06
03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
14E917B1 82C71FCF ACA91B6E F4A9269C 70AE05A0 9A306F06
03551D1F 04683066 3064A062 A060862D 68747470 3A2F2F63
61702D72 74702D30 30312F43 65727445 6E726F6C 6C2F4341
502D5254 502D3030 312E6372 6C862F66 696C653A 2F2F5C5C
6361702D 7274702D 3030315C 43657274 456E726F 6C6C5C43
41502D52 54502D30 30312E63 726C3010 06092B06 01040182
37150104 03020100 300D0609 2A864886 F70D0101 05050003
82010100 AB64FDEB F60C32DC 360F0E10 5FE175FA 0D574AB5
02ACDCA3 C7BBED15 A4431F20 7E9286F0 770929A2 17E4CDF4
F2629244 2F3575AF E90C468C AE67BA08 AAA71C12 BA0C0E79
E6780A5C F814466C 326A4B56 73938380 73A11AED F9B9DE74
1195C48F 99454B8C 30732980 CD6E7123 8B3A6D68 80B97E00
7F4BD4BA 0B5AB462 94D9167E 6D8D48F2 597CDE61 25CFADCC
5BD141FB 210275A2 0A4E3400 1428BA0F 69953BB5 50D21F78
43E3E563 98BCB2B1 A2D4864B 0616BACD A61CD9AE C5558A52
B5EEAA6A 08F96528 B1804B87 D26E4AEE AB7AFFE9 2FD2A574
BAFE0028 96304A8B 13FB656D 8FC60094 D5A53D71 444B3CEF
79343385 3778C193 74A2A6CE DC56275C A20A303D quit crypto
pki certificate chain 7960 certificate ca F301 308201F7
30820160 A0030201 020202F3 01300D06 092A8648 86F70D01
01050500 3041310B 30090603 55040613 02555331 1A301806
0355040A 13114369 73636F20 53797374 656D7320 496E6331
16301406 03550403 130D4341 50462D33 35453038 33333230
1E170D30 34303430 39323035 3530325A 170D3139 30343036
32303535 30315A30 41310B30 09060355 04061302 5553311A
30180603 55040A13 11436973 636F2053 79737465 6D732049
6E633116 30140603 55040313 0D434150 462D3335 45303833
33323081 9F300D06 092A8648 86F70D01 01010500 03818D00
30818902 818100C8 BD9B6035 366B44E8 0F693A47 250FF865
D76C35F7 89B1C4FD 1D122CE0 F5E5CDFF A4A87EFF 41AD936F
E5C93163 3E55D11A AF82A5F6 D563E21C EB89EBFA F5271423
C3E875DC E0E07967 6E1AAB4F D3823E12 53547480 23BA1A09
295179B6 85A0E83A 77DD0633 B9710A88 0890CD4D DB55ADD0
964369BA 489043BB B667E60F 93954B02 03010001 300D0609
2A864886 F70D0101 05050003 81810056 60FD3AB3 6F98D2AD
40C309E2 C05B841C 5189271F 01D864E8 98BCE665 2AFBCC8C
54007A84 8F772C67 E3047A6C C62F6508 B36A6174 B68C1D78
C2228FEA A89ECEFB CC8BA9FC 0F30E151 431670F9 918514D9
868D1235 18137F1E 50DFD32E 1DC29CB7 95EF4096 421AF22F
5C1D5804 B83F8E8E 95B04F45 86563BFE DF976C5B FB490A quit
! ! no crypto isakmp enable ! !--- Enable IPsec. crypto
isakmp policy 1 authentication pre-share lifetime 28800
crypto isakmp key cisco123 address 10.1.1.13 !--- The
crypto key must match the key configured on Cisco
CallManager. ! !--- The crypto IPSec configuration must
match your Cisco CallManager !--- configuration. crypto
ipsec transform-set rtpset esp-des esp-md5-hmac ! !
crypto map rtp 1 ipsec-isakmp set peer 10.1.1.13 set
transform-set rtpset match address 116 ! ! interface
FastEthernet0/0 ip address 10.1.1.22 255.255.255.0
```

```
duplex auto speed auto crypto map rtp ! interface
FastEthernet0/1 no ip address shutdown duplex auto speed
auto ! ip classless ! ip http server no ip http secure-
server ! ! !--- Define the traffic to be encrypted by
IPsec. access-list 116 permit ip host 10.1.1.22 host
10.1.1.13 ! ! control-plane ! ! call application
alternate DEFAULT ! ! voice-port 1/0/0 ! voice-port
1/0/1 ! voice-port 1/0/2 ! voice-port 1/0/3 ! voice-port
1/1/0 timing hookflash-out 50 ! voice-port 1/1/1 !
voice-port 1/1/2 ! voice-port 1/1/3 ! !--- Enable the
MGCP voice protocol. mgcp mgcp call-agent 10.1.1.13 2427
service-type mgcp version 0.1 mgcp dtmf-relay voip codec
all mode out-of-band mgcp rtp unreachable timeout 1000
action notify mgcp package-capability rtp-package mgcp
package-capability sst-package no mgcp package-
capability fxr-package no mgcp timer receive-rtcp mgcp
sdp simple mgcp fax t38 inhibit mgcp rtp payload-type
g726r16 static ! mgcp profile default ! ! dial-peer
voice 81235 pots application mgcpapp destination-pattern
81235 port 1/1/0 forward-digits all ! dial-peer voice
81234 pots application mgcpapp destination-pattern 81234
port 1/0/0 ! dial-peer voice 999100 pots application
mgcpapp port 1/0/0 ! dial-peer voice 999110 pots
application mgcpapp port 1/1/0 ! ! !--- Enable the
credentials service on the gateway. !--- Cisco
CallManager takes the certificate retrieved from the
secure SRST !--- device certificate and places it in the
configuration file of the !--- Cisco IP phone. Activate
credentials service on all SRST routers. !--- Enable the
SRST router to receive messages from Cisco CallManager.
The !--- IP address is the preexisting router IP
address, typically one of the !--- addresses of the
Ethernet port of the router. The default port number is
2445. credentials ip source-address 10.1.1.22 port 2445
!--- Specify the name of the trustpoint that is to be
associated with the SRST !--- router certificate. The
trustpoint name must be the same as the one already !---
declared. trustpoint srstca ! ! !--- Enable SRST mode on
the SRST router to support Cisco IP phone functions.
call-manager-fallback secondary-dialtone 9 transfer-
system full-consult ip source-address 10.1.1.22 port
2000 max-ephones 15 max-dn 30 transfer-pattern ..... . .
.
```

Конфигурация 2

```
!--- Allow trusted host traffic. access-list 140 deny
tcp host 10.1.1.11 any eq 2445 !--- Rate-limit all other
traffic. access-list 140 permit tcp any any eq 2445
access-list 140 deny ip any any !--- Define class-map
sccp-class. class-map match-all sccp-class match access-
group 140 policy-map control-plane-policy class sccp-
class police 8000 1500 1500 conform-action drop exceed-
action drop !--- Define aggregate control plane service
for the active Route Processor. control-plane service-
policy input control-plane-policy
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

Проверка параметров учетных записей

Для проверки параметров учетных записей SRST-маршрутизатора, предоставляемых в Cisco CallManager для использования во время защищенного SRST-fallback, используйте команду show credentials.

```
Router#show credentials Credentials IP: 10.1.1.22 Credentials PORT: 2445 Trustpoint: srstca
```

Проверки регистрации сертификата

Если в качестве сертифицирующего устройства был использован сервер сертификатов Cisco IOS, используйте команду show running-config для проверки регистрации сертификата или команду show crypto pki server для проверки статуса CA-сервера.

1. Используйте команду show running-config для проверки создания CA-сервера (01) и сертификатов устройств (02). В данном примере показаны зарегистрированные сертификаты.
```
! SRST router device certificate.
crypto pki certificate chain srstca
 certificate 02
  308201AD 30820116 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 35323233 5A170D30 35303431 32313935 3232335A 30343132 300F0603
  55040513 08443042 39453739 43301F06 092A8648 86F70D01 09021612 6A61736F
  32363931 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
  4B003048 024100D7 0CC354FB 5F7C1AE7 7A25C3F2 056E0485 22896D36 6CA70C19
  C98F9BAE AE9D1F9B D4BB7A67 F3251174 193BB1A3 12946123 E5C1CCD7 A23E6155
  FA2ED743 3FB8B902 03010001 A330302E 300B0603 551D0F04 04030205 A0301F06
  03551D23 04183016 8014F829 CE97AD60 18D05467 FC293963 C2470691 F9BD300D
  06092A86 4886F70D 01010405 00038181 007EB48E CAE9E1B3 D1E7A185 D7F0D565
  CB84B17B 1151BD78 B3E39763 59EC650E 49371F6D 99CBD267 EB8ADF9D 9E43A5F2
  FB2B18A0 34AF6564 11239473 41478AFC A86E6DA1 AC518E0B 8657CEBB ED2BDE8E
  B586FE67 00C358D4 EFDD8D44 3F423141 C2D331D3 1EE43B6E 6CB29EE7 0B8C2752
  C3AF4A66 BD007348 D013000A EA3C206D CF
  quit
 certificate ca 01
  30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  17311530 13060355 0403130C 73727374 63617365 72766572 301E170D 30343034
  31323139 34353136 5A170D30 37303431 32313934 3531365A 30173115 30130603
  55040313 0C737273 74636173 65727665 7230819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281 8100C3AF EE1E4BB1 9922A8DA 2BB9DC8E 5B1BD332
  1051C9FE 32A971B3 3C336635 74691954 98E765B1 059E24B6 32154E99 105CA989
  9619993F CC72C525 7357EBAC E6335A32 2AAF9391 99325BFD 9B8355EB C10F8963
  9D8FC222 EE8AC831 71ACD3A7 4E918A8F D5775159 76FBF499 5AD0849D CAA41417
  DD866902 21E5DD03 C37D4B28 0FAB0203 010001A3 63306130 0F060355 1D130101
  FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
  160414F8 29CE97AD 6018D054 67FC2939 63C24706 91F9BD30 1F060355 1D230418
  30168014 F829CE97 AD6018D0 5467FC29 3963C247 0691F9BD 300D0609 2A864886
  F70D0101 04050003 8181007A F71B25F9 73D74552 25DFD03A D8D1338F 6792C805
  47A81019 795B5AAE 035400BB F859DABF 21892B5B E71A8283 08950414 8633A8B2
  C98565A6 C09CA641 88661402 ACC424FD 36F23360 ABFF4C55 BB23C66A C80A3A57
  5EE85FF8 C1B1A540 E818CE6D 58131726 BB060974 4E1A2F4B E6195522 122457F3
  DEDBAAD7 3780136E B112A6
  quit
```
2. Используйте команду show crypto pki server для проверки статуса CA-сервера после

процедуры загрузки.
```
Router#show crypto pki server Certificate Server srstcaserver: Status: enabled Server's configuration is locked (enter "shut" to unlock it) Issuer name: CN=srstcaserver CA cert fingerprint: AC9919F5 CAFE0560 92B3478A CFF5EC00 Granting mode is: auto Last certificate issued serial number: 0x2 CA certificate expiration timer: 13:46:57 PST Dec 1 2007 CRL NextUpdate timer: 14:54:57 PST Jan 19 2005 Current storage dir: nvram Database Level: Complete - all issued certs written as <serialnum>.cer
```

Проверка статуса телефона и регистраций

Для проверки или отладки статуса IP-телефона и регистрации выполните следующие действия в привилегированном EXEC-режиме.

1. **Используйте команду show ephone для отображения зарегистрированных IP-телефонов Cisco и их возможностей.** Данная команда также отображает статус аутентификации и шифрования при использовании для защищенного SRST. В данном примере аутентификация и шифрование активны при TLS-соединении.
```
Router#show ephone ephone-1 Mac:1000.1111.0002 TCP socket:[5] activeLine:0 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 IP:10.1.1.40 32626 7970 keepalive 390 max_line 8 button 1: dn 14 number 2002 CM Fallback CH1 IDLE ephone-2 Mac:1000.1111.000B TCP socket:[12] activeLine:0 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 IP:10.1.1.40 32718 7970 keepalive 390 max_line 8 button 1: dn 21 number 2011 CM Fallback CH1 IDLE ephone-3 Mac:1000.1111.000A TCP socket:[16] activeLine:0 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 IP:10.1.1.40 32862 7970 keepalive 390 max_line 8 button 1: dn 2 number 2010 CM Fallback CH1 IDLE
```
2. **Используйте команду show ephone offhook для отображения статуса IP-телефона Cisco и качества для всех неподключенных телефонов.** В данном примере аутентификация и шифрование активны при TLS-соединении, и имеется активный защищенный звонок.
```
Router#show ephone offhook ephone-1 Mac:1000.1111.0002 TCP socket:[5] activeLine:1 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 :0 IP:10.1.1.40 32626 7970 keepalive 391 max_line 8 button 1: dn 14 number 2002 CM Fallback CH1 CONNECTED Active Secure Call on DN 14 chan 1 :2002 10.1.1.40 29632 to 10.1.1.40 25616 via 10.1.1.40 G711Ulaw64k 160 bytes no vad Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0 Jitter 0 Latency 0 callingDn 22 calledDn -1 ephone-2 Mac:1000.1111.000B TCP socket:[12] activeLine:1 REGISTERED in SCCP ver 5 + Authentication + Encryption with TLS connection mediaActive:1 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 IP:10.1.1.40 32718 7970 keepalive 391 max_line 8 button 1: dn 21 number 2011 CM Fallback CH1 CONNECTED Active Secure Call on DN 21 chan 1 :2011 10.1.1.40 16382 to 10.1.1.40 16382 via 10.1.1.40 G711Ulaw64k 160 bytes no vad Tx Pkts 295 bytes 49468 Rx Pkts 277 bytes 46531 Lost 0 Jitter 0 Latency 0 callingDn -1 calledDn 11
```
3. **Используйте команду show voice call status для отображения статуса вызовов всех голосовых портов SRST-маршрутизатора Cisco.** Данная команда неприменима для вызовов между двумя точками подключения узлов.
```
Router#show voice call status CallID CID ccVdb Port DSP/Ch Called # Codec Dial-peers 0x1164 2BFE 0x8619A460 50/0/35.0 2014 g711ulaw 20035/20027 0x1165 2BFE 0x86144B78 50/0/27.0 *2014 g711ulaw 20027/20035 0x1166 2C01 0x861043D8 50/0/21.0 2012 g711ulaw 20021/20011 0x1168 2C01 0x860984C4 50/0/11.0 *2012 g711ulaw 20011/20021 0x1167 2C04 0x8610EC7C 50/0/22.0 2002 g711ulaw 20022/20014 0x1169 2C04 0x860B8894 50/0/14.0 *2002 g711ulaw 20014/20022 0x116A 2C07 0x860A374C 50/0/12.0 2010 g711ulaw 20012/20002 0x116B 2C07 0x86039700 50/0/2.0 *2010 g711ulaw 20002/20012 0x116C 2C0A 0x86119520 50/0/23.0 2034 g711ulaw 20023/20020 0x116D 2C0A 0x860F9150 50/0/20.0 *2034 g711ulaw 20020/20023 0x116E 2C0D 0x8608DC20 50/0/10.0 2022 g711ulaw 20010/20008 0x116F 2C0D 0x86078AD8 50/0/8.0 *2022 g711ulaw 20008/20010 0x1170 2C10 0x861398F0 50/0/26.0 2016 g711ulaw 20026/20028 0x1171 2C10 0x8614F41C 50/0/28.0 *2016 g711ulaw 20028/20026 0x1172 2C13 0x86159CC0 50/0/29.0 2018 g711ulaw 20029/20004 0x1173 2C13 0x8604E848 50/0/4.0 *2018 g711ulaw 20004/20029 0x1174 2C16 0x8612F04C 50/0/25.0 2026 g711ulaw 20025/20030 0x1175 2C16 0x86164F48 50/0/30.0 *2026 g711ulaw 20030/20025 0x1176 2C19 0x860D8C64 50/0/17.0 2032
```

```
g711ulaw 20017/20018 0x1177 2C19 0x860E4008 50/0/18.0 *2032 g711ulaw 20018/20017 0x1178
2C1C 0x860CE3C0 50/0/16.0 2004 g711ulaw 20016/20019 0x1179 2C1C 0x860EE8AC 50/0/19.0 *2004
g711ulaw 20019/20016 0x117A 2C1F 0x86043FA4 50/0/3.0 2008 g711ulaw 20003/20024 0x117B 2C1F
0x861247A8 50/0/24.0 *2008 g711ulaw 20024/20003 0x117C 2C22 0x8608337C 50/0/9.0 2020
g711ulaw 20009/20031 0x117D 2C22 0x8616F7EC 50/0/31.0 *2020 g711ulaw 20031/20009 0x117E
2C25 0x86063990 50/0/6.0 2006 g711ulaw 20006/20001 0x117F 2C25 0x85C6BE6C 50/0/1.0 *2006
g711ulaw 20001/20006 0x1180 2C28 0x860ADFF0 50/0/13.0 2029 g711ulaw 20013/20034 0x1181 2C28
0x8618FBBC 50/0/34.0 *2029 g711ulaw 20034/20013 0x1182 2C2B 0x860C3B1C 50/0/15.0 2036
g711ulaw 20015/20005 0x1183 2C2B 0x860590EC 50/0/5.0 *2036 g711ulaw 20005/20015 0x1184 2C2E
0x8617A090 50/0/32.0 2024 g711ulaw 20032/20007 0x1185 2C2E 0x8606E234 50/0/7.0 *2024
g711ulaw 20007/20032 0x1186 2C31 0x861A56E8 50/0/36.0 2030 g711ulaw 20036/20033 0x1187 2C31
0x86185318 50/0/33.0 *2030 g711ulaw 20033/20036 18 active calls found
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Для дополнительных сведений о том, как устранить неполадки, посмотрите Дополнительные сведения