Cisco Secure SRST配置示例

目录

简介

本文档提供 Cisco Secure Survivable Remote Site Telephony (SRST) 的示例配置。

位于远程站点并且连接到网关路由器的安全 Cisco IP 电话可以通过广域网安全地与 Cisco CallManager 通信。但如果广域网链路或 Cisco CallManager 断开，则所有通过远程电话的通信将变得不安全。为了应对这种情况，现在网关路由器可以在安全 SRST 模式下工作（当广域网链路或 Cisco CallManager 断开时将激活安全 SRST 模式）。当广域网链路或 Cisco CallManager 恢复时，Cisco CallManager 将恢复安全呼叫处理功能。

安全 SRST 提供新的 SRST 安全功能，例如身份验证、完整性和介质加密。身份验证向一方提供另一方是其所声明的身份的保证。完整性提供给定数据不会在实体之间变更的保证。加密暗示机密性，这意味着除了预定接收方以外，其他人无法读取该数据。这些安全功能为 SRST 语音呼叫提供了隐私保护，可防止语音安全规则违反和身份遭窃。

在以下情况下可实现 SRST 安全：

- 使用证书对终端设备进行身份验证。
- 使用 TCP 的传输层安全 (TLS) 对信令进行身份验证和加密。
- 使用 Secure Real-Time Transport Protocol (SRTP) 加密安全介质路径。
- 证书是由证书颁发机构 (CA) 生成和分发的。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

Public Key Infrastructure 要求

- 手动或使用 Network Time Protocol (NTP) 设置时钟。这将保证与 Cisco CallManager 的同步性。
- 如果尚未启用，请使用 **ip http server** 命令启用 IP HTTP 服务器（Cisco IOS® 处理器）。有关 Public Key Infrastructure (PKI) 部署的详细信息，请参阅 Cisco IOS Certificate Server。
- 如果证书服务器是您的启动配置的一部分，则在引导过程中，您可能会看到以下消息：`% Failed to find Certificate Server's trustpoint at startup % Failed to find Certificate Server's cert.`这些消息是提供信息的消息，指示由于启动配置尚未完全解析，因此暂时无法配置证书服务器。当启动配置已损坏时，这些消息对于调试非常有用。在引导过程之后，可以使用 **show crypto pki server** 命令验证证书服务器的状态。

SRST 的要求

- 当 SRST 处于活动状态时，无法注册安全 SRST 服务。因此，可以使用 **no call-manager-fallback** 命令来禁用 SRST。
- 有关安全 SRST 支持的 Cisco IP 电话、路由器、网络模块和编解码器列表，请参阅 Cisco IOS MGCP 网关的介质和信令身份验证和加密功能。
- 有关 Cisco SRST 的 Cisco IP 电话的最大数量、电话号码 (DN) 或虚拟语音端口的最大数量以及内存要求的最新信息，请参阅 Cisco Unified SRST 4.0 支持的固件、平台、内存和语音产品。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全 SRST 中支持的安全 Cisco IP 电话必须已安装证书并已启用加密。
- SRST 路由器必须具有证书。证书可由第三方或 Cisco IOS 证书颁发机构 (CA) 生成。Cisco IOS CA 可与 SRST 在同一网关中运行。
- 必须启用 Cisco CallManager 上的证书信任列表 (CTL)。有关完整说明，请参阅 Cisco IOS MGCP 网关的介质和信令身份验证和加密功能的*配置安全 IP 电话呼叫* 部分。
- 必须安装 Cisco CallManager 4.1(2) 或更高版本，并且该版本必须支持安全模式（身份验证和加密模式）。
- 运行安全SRST的网关路由器必须支持语音和已启用安全的Cisco IOS镜像(âÂ Â k9 âÂ Â 加密软件镜像)。支持两种镜像：高级 IP 服务（包括多种高级安全功能）和高级企业服务（包括完整的 Cisco IOS 软件）。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

限制

一般限制

- 加密软件功能(âÂ Â k9 âÂ Â)在出口控制下。本产品包含加密功能，受美国和当地国家/地区进出口、运输和使用方面的相关法律约束。交付 Cisco 加密产品并不表示第三方拥有进出口、分发或使用加密的权利。进口商、出口商、分销商和用户应遵守美国和所在国家/地区法律法规。使用本产品，即表示同意遵守适用的法律法规。如果不能遵守美国和当地的法律，请立即退回本产品。适用于 Cisco 加密产品的美国法律的概要可在以下网站找到：http://www.cisco.com/wwl/export/crypto/tool/如果需要进一步的帮助，请通过向 export@cisco.com 发送电子邮件与我们联系。
- 在 Cisco IP 电话终点之间或从 Cisco IP 电话向网关终点发出 Secure Real-Time Transport Protocol (SRTP) 加密呼叫时，IP 电话上会显示一个锁图标。此锁仅指示该呼叫的 IP 段的安全性。而没有暗示 PSTN 段的安全性。
- 仅在单个路由器的范围内支持安全 SRST。

安全 SRST 模式下不支持的功能和软件

- 4.1(2) 之前的 Cisco CallManager 版本
- 安全等候音乐 (MoH)
- 安全转码或会议
- 安全 H.323 或 SIP
- 热备用路由器协议 (HSRP)

安全 SRST 模式下支持的呼叫

在安全 SRST 模式下仅支持语音呼叫。具体而言，支持以下语音呼叫：

- 基本呼叫
- 呼叫转移（占线、无人接听、全部）
- 共享线路（IP 电话）
- 呼叫转接（咨询转接和盲转接）
- 保留和继续

背景信息

Cisco IP 电话在 SRST 期间的明文后退

早于 Cisco IOS 软件版本 12.3(14)T 的 Cisco SRST 版本不能支持安全连接，也不能启用安全机制。如果SRST路由器没有能力在安全SRST上作为fallback modeâÂ Â 即不能完成与思科 CallManagerâÂ其证书没有被添加到Cisco IP电话的配置文件的 Â 的TLS握手。缺少 SRST 路由器证书会导致 Cisco IP 电话在处于 SRST 后退模式下时使用不安全的（明文）通信。Cisco IP 电话固件中内置了以明文模式检测和后退的功能。有关明文模式的详细信息，请参阅 Cisco IOS MGCP 网关的介质和信令身份验证和加密功能。

SRST 路由器和 TLS 协议

传输层安全 (TLS) 版本 1.0 在 Cisco IP 电话、安全 SRST 路由器和 Cisco CallManager 之间提供安全 TCP 信道。当 Cisco IP 电话注册到 Cisco CallManager 时，会建立 TLS 连接，这时 TLS 过程开始。如果 Cisco CallManager 配置为后退到 SRST，则还会建立 Cisco IP 电话和安全 SRST 路由

器之间的 TLS 连接。如果广域网链路或 Cisco CallManager 发生故障，则呼叫控制将恢复到 SRST 路由器。

SRST 路由器和 PKI

SRST 路由器和 Cisco CallManager 之间的证书传输对于安全 SRST 功能是必需的。Public Key Infrastructure (PKI) 命令用于生成、导入和导出安全 SRST 的证书。每个支持的 Cisco IP 电话的证书显示在此表中。

表 1 - 支持的 Cisco IP 电话和证书

Cisco IP 电话 7940	Cisco IP 电话 7960	Cisco IP 电话 7970
电话从证书权限代理功能 (CAPF) 接收可辨别编码规则 (DER) 格式的本地签名证书 (LSC)。证书文件名：59fe77ccd.0 文件名可能因 CAPF 证书主题名称和 CAPF 证书颁发者而异。如果 Cisco CallManager 使用第三方证书提供程序，则可能有多个 .0 文件（从两个到十个）。在配置过程中，必须分别导入每个 .0 证书文件。仅支持 Manual enrollment。	电话从证书权限代理功能 (CAPF) 接收可辨别编码规则 (DER) 格式的本地签名证书 (LSC)。证书文件名：59fe77ccd.0 文件名可能因 CAPF 证书主题名称和 CAPF 证书颁发者而异。如果 Cisco CallManager 使用第三方证书提供程序，则可能有多个 .0 文件（从两个到十个）。在配置过程中，必须分别导入每个 .0 证书文件。仅支持 Manual enrollment。	电话包含用于设备身份验证的厂商预装证书 (MIC)。如果 Cisco 7970 实施 MIC，则需要两个公共证书文件： • CiscoCA.pem（用于对证书进行身份验证的 Cisco Root CA） • a69d2e04.0（采用保密增强型邮件 (PEM) 格式） 如果 Cisco CallManager 使用第三方证书提供程序，则可能有多个 .0 文件（从两个到十个）。在配置过程中，必须分别导入每个 .0 证书文件。仅支持 Manual enrollment。

安全 SRST 路由器上的 Cisco IOS Credentials Server

安全 SRST 引入了在安全 SRST 路由器上运行的凭据服务器。当客户端 Cisco CallManager 通过 TLS 信道请求证书时，凭据服务器向 Cisco CallManager 提供 SRST 路由器证书。Cisco CallManager 将 SRST 路由器证书插入 Cisco IP 电话配置文件中，然后将配置文件下载到电话中。在后退操作期间，安全 Cisco IP 电话使用该证书对 SRST 路由器进行身份验证。凭据服务默认在 TCP 端口 2445 上运行。

五个新的 Cisco IOS 命令在 call-manager-fallback 模式下配置凭据服务器，并提供服务器调试和验

证功能：

- 凭证
- debug credentials
- ip source-address (credentials)
- show credentials
- trustpoint (credentials)

为 Cisco IP 电话建立安全 SRST

下图显示 SRST 路由器上的凭据服务器、Cisco CallManager 和 Cisco IP 电话的互联，它将为 Cisco IP 电话建立安全 SRST。

1. Cisco IP 电话配置 DHCP 并获得 TFTP 服务器地址。
2. Cisco IP 电话从 TFTP 服务器检索 CTL 文件。CTL 文件中包含电话应该信任的证书。
3. Cisco IP 电话打开传输层安全 (TLS) 协议信道并注册到 Cisco CallManager。

Cisco CallManager 将安全 SRST 路由器信息和 SRST 路由器证书导出到 Cisco IP 电话。电话将证书放入其配置中。一旦电话具有 SRST 证书，SRST 路由器便被认为是安全的。

如果Cisco IP电话配置作为âÂ Â authenticatedâÂ Â 或âÂ Â encryptedâÂ Â 和Cisco CallManager在混合模式配置，电话寻找在其配置文件的一SRST证书。如果找到 SRST 证书，它会打开到默认端口的备用 TLS 连接。默认端口是 Cisco IP 电话 TCP 端口加上 443，即 SRST 路由器上的端口 2443。只要没有辅助 Cisco CallManager，并且 SRST 配置为备份设备，便会自动连接到 SRST 路由器。

Cisco CallManager 必须配置为处于混合模式下，因为混合模式是其安全模式。

如果广域网发生故障，Cisco IP 电话会启动 SRST 注册。Cisco IP 电话通过默认端口注册到 SRST 路由器以进行安全通信。

配置

本部分提供有关如何配置本文档所述功能的信息。

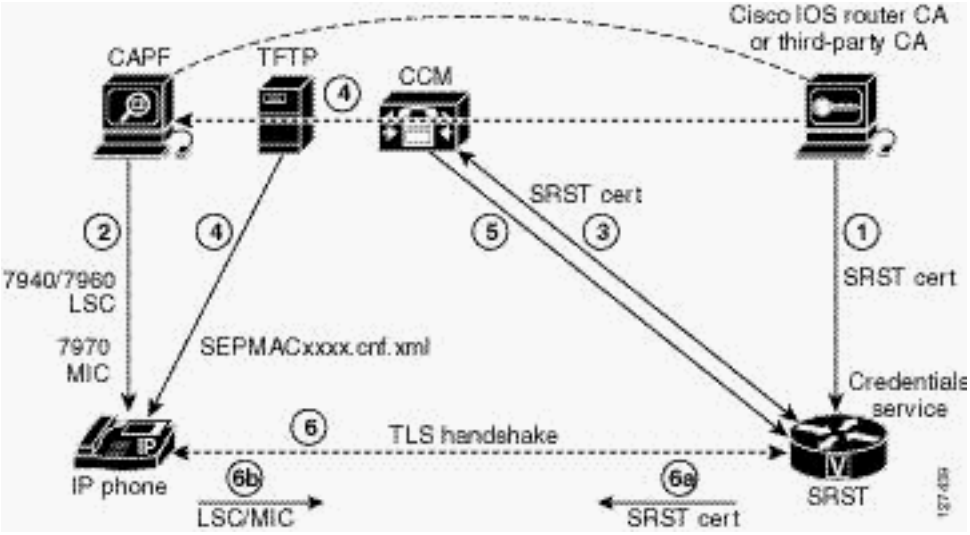
注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

在 TLS 握手期间，安全 SRST 路由器和 Cisco IP 电话必须请求相互身份验证。TLS 握手发生在电话注册到 SRST 路由器时（在广域网链路发生故障之前或之后）。此配置示例不包括第三方 CA 的

使用。它假设使用 Cisco IOS Certificate Server 来生成您的证书。

网络图

本文档使用此图所示的网络设置。下图说明了安全 SRST 身份验证和加密的过程。



1. CA 服务器（不管它是 Cisco IOS 路由器 CA 还是第三方 CA）向 SRST 网关颁发设备证书，从而启用凭据服务。或者，证书也可以由配备 Cisco IOS CA 服务器的 SRST 路由器自行生成。CA 路由器是证书权限代理功能 (CAPF) 的最终信任点。有关 CAPF 的详细信息，请参阅 Cisco CallManager 安全指南。
2. CAPF 是一个进程，其中支持的设备可以请求本地签名证书 (LSC)。CAPF 实用程序生成 CAPF 特定的密钥对和证书，将此证书复制到集群中的所有 Cisco CallManager 服务器，并将 LSC 提供给 Cisco IP 电话。没有厂商预装证书 (MIC) 的 Cisco IP 电话需要 LSC。Cisco 7970 配备有 MIC，因此不需要经过 CAPF 进程。
3. Cisco CallManager 从凭据服务器请求 SRST 证书，而凭据服务器会用证书作为响应。
4. Cisco CallManager 对每个设备都使用 TFTP 进程并将证书插入 Cisco IP 电话的 SEPMACxxxx.cnf.xml 配置文件中。
5. Cisco CallManager 向 SRST 路由器提供包含电话证书信息的 PEM 格式文件。PEM 文件需要手动提供给 SRST 路由器。当 SRST 路由器中包含 PEM 文件时，它可以在 TLS 握手期间，对 IP 电话进行身份验证并验证 IP 电话证书的颁发者。
6. TLS 握手发生，交换证书，并且在 Cisco IP 电话和 SRST 路由器之间进行相互身份验证和注册。SRST 路由器发送其证书，电话将此证书与它在步骤 4 中从 Cisco CallManager 接收的证书进行比较验证。Cisco IP 电话向 SRST 路由器提供 LSC 或 MIC，然后路由器使用它在步骤 5 中接收的 PEM 格式文件来验证 LSC 或 MIC。**注意：** 电话和路由器证书进行交换，并且与 SRST 路由器建立 TLS 连接后，会自动加密介质。

在您配置之前

Cisco CallManager

完成这些步骤：

1. 在 SRST 路由器上运行凭据服务后，需要向 Cisco CallManager 添加 SRST 引用，因为 Cisco CallManager 会连接 SRST 路由器以获取其设备证书。有关如何向 Cisco CallManager 添加 SRST 的完整信息，请参阅 Cisco CallManager 管理指南 4.1(2) 版的 *Survivable Remote Site*

Telephony 配置 部分。

2. 必须在 Cisco CallManager 上配置 SRST 后退。为此，请为 SRST 分配设备池。有关向 Cisco CallManager 添加设备池的完整信息，请参阅 Cisco CallManager 管理指南 4.1(2) 版的*设备池配置* 部分。
3. 必须在 Cisco CallManager 中配置证书权限代理功能 (CAPF)。CAPF 进程允许支持的设备（例如 Cisco CallManager）从 Cisco IP 电话请求 LSC 证书。CAPF 实用程序生成 CAPF 特定的密钥对和证书，并将该证书复制到集群中的所有 Cisco CallManager 服务器。有关如何在 Cisco CallManager 中配置 CAPF 的完整说明，请参阅 Cisco CallManager 4.0(1) 的 Cisco IP 电话身份验证和加密。

安全注意事项

- 使用 **grant auto** 命令可以颁发证书，在定义根 CA 时必须激活该命令。但是，出于安全考虑，**grant auto** 命令不能一直保持活动状态，颁发证书后必须将其禁用。
- 安全最佳做法是使用 Control Plane Policing 保护凭据服务端口。Control Plane Policing 可以保护网关并保持数据包转发和协议状态，而不管流量负载有多大。有关控制层面的详细信息，请参阅 Control Plane Policing。本文档的配置 2 部分中也会显示一个配置示例。

配置

本文档使用以下配置：

- 配置1 âÂ Â 根据此**show running-config**示例配置您的路由器。
- 配置2 âÂ Â A最佳安全做法是保护有控制平面策略的凭证服务端口。如果使用 Control Plane Policing，请按照此部分 **show running-config** 示例配置您的路由器。

配置 1

```
Router#show running-config...!--- Define Cisco
CallManager.ccm-manager fallback-mgcpccm-manager mgcpccm-
manager music-on-holdccm-manager config server 10.1.1.13ccm-
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 quitcrypto 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 quitcrypto 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
quitcrypto 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 quitcrypto 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 28800crypto 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 serverno 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.mgcpmgcp call-agent
10.1.1.13 2427 service-type mgcp version 0.1mgcp dtmf-relay
voip codec all mode out-of-bandmgcp rtp unreachable timeout
1000 action notifymgcp package-capability rtp-packagemgcp
package-capability sst-packageno mgcp package-capability fxr-
packageno mgcp timer receive-rtcpmgcp sdp simplemgcp fax t38
inhibitmgcp 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
........
```

配置 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 2445access-list
140 deny ip any any!--- Define class-map sccp-class.class-map
match-all sccp-class match access-group 140policy-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
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

验证凭据设置

要验证 SRST 路由器上提供给 Cisco CallManager 以在安全 SRST 后退期间使用的凭据设置，请发出 **show credentials** 命令。

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

验证证书注册

如果您将 Cisco IOS Certificate Server 用作您的 CA，请发出 **show running-config** 命令以验证证书是否已注册，或发出 **show crypto pki server** 命令以验证 CA 服务器的状态。

1. 发出 **show running-config** 命令以验证是否已创建 CA 服务器 (01) 证书和设备 (02) 证书。此示例显示已注册的证书。`! 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. 发出 **show crypto pki server** 命令以验证引导过程后 CA 服务器的状态。`Router#`**`show crypto pki server`**`Certificate Server srstcaserver:Status: enabledServer's configuration is locked (enter "shut" to unlock it)Issuer name: CN=srstcaserverCA cert fingerprint: AC9919F5 CAFE0560 92B3478A CFF5EC00Granting mode is: autoLast certificate issued serial number: 0x2CA certificate expiration timer: 13:46:57 PST Dec 1 2007CRL NextUpdate timer: 14:54:57 PST Jan 19 2005Current storage dir: nvramDatabase Level: Complete - all issued certs written as <serialnum>.cer`

验证电话状态和注册

要对 IP 电话状态和注册进行验证或故障排除，请在特权 EXEC 模式下完成以下步骤。

1. 发出 **show ephone** 命令以显示已注册的 Cisco IP 电话及其功能。此命令还显示用于安全 SRST 时的身份验证和加密状态。在本示例中，身份验证和加密状态为活动且具有 TLS 连接。`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 IDLEephone-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 IDLEephone-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. 发出 **show ephone offhook** 命令以显示 Cisco IP 电话状态和所有摘机电话的质量。在本示例中，身份验证和加密状态为活动且具有 TLS 连接，并且存在活动安全呼叫。`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 25616via 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 -1ephone-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. 发出 **show voice call status** 命令以显示 Cisco SRST 路由器上所有语音端口的呼叫状态。此命令不适用于两个 POTS 拨号对等体之间的呼叫。

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

关于如何排除故障的更多信息，请参阅相关信息