Exemplo de configuração SRST segura da Cisco

Índice

Introdução

Este documento apresenta um exemplo de configuração da Cisco Secure Survivable Remote Site Telephony (SRST).

Telefones IP seguros da Cisco localizados em locais remotos e conectados a roteadores de gateway podem se comunicar de forma segura com o Cisco CallManager pela WAN. No entanto, se o link da WAN ou o Cisco CallManager forem desativados, todas as comunicações pelos telefones remotos se tornarão inseguras. Para resolver esse problema, agora os roteadores de gateway podem funcionar no modo SRST seguro, que é ativado quando o link da WAN ou o Cisco CallManager são desativados. Quando o link da WAN ou o Cisco CallManager é restaurado, o Cisco CallManager retoma os recursos de chamada segura.

O SRST seguro fornece novos recursos de segurança de SRST, como autenticação, integridade

e criptografia de mídia. A autenticação oferece a garantia a uma parte de que a outra parte é realmente quem diz ser. A integridade oferece a garantia de que os dados fornecidos não foram alterados entre as entidades. A criptografia implica confidencialidade, o que significa que ninguém pode ler os dados, exceto o destinatário pretendido. Esses recursos de segurança proporcionam privacidade para chamadas de voz SRST e protegem contra violações de segurança de voz e roubo de identidade.

A segurança de SRST ocorre quando:

- Os dispositivos finais são autenticados com certificados.
- A sinalização é autenticada e criptografada com Transport Layer Security (TLS) para TCP.
- Um caminho de mídia seguro é criptografado com Secure Real-Time Transport Protocol (SRTP).
- Os certificados são gerados e distribuídos por uma autoridade certificadora (CA).

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

Requisitos da infraestrutura da chave pública

- Ajuste o relógio, manualmente ou com o Network Time Protocol (NTP). Isso assegura a sincronização com o Cisco CallManager.
- Habilite o servidor IP HTTP (processador Cisco IOS®) com o **comando ip http server**, se ele já não estiver habilitado. Consulte o servidor de certificado Cisco IOS paõer mais informações sobre o desenvolvimento da public key infrastructure (PKI).
- Se o servidor certificado fizer parte de sua configuração de inicialização, você poderá ver essas mensagens durante o procedimento de inicialização:`% Failed to find Certificate Server's trustpoint at startup`

  `% Failed to find Certificate Server's cert.`Essas mensagens são informativas e indicam uma incapacidade temporária de configurar o servidor certificado, pois a configuração de inicialização ainda não está completamente analisada. As mensagens são úteis para debugar, caso a configuração de inicialização seja corrompida. Você pode verificar o status do servidor certificado após o procedimento de inicialização com o **comando show crypto pki server**.

Requisitos de SRST

- Os serviços seguros de SRST não podem ser registrados quando o SRST está ativo. Portanto, desabilite o SRST com o comando **no call-manager-fallback**.
- Consulte Autenticação de mídia e sinalização e recurso de criptografia para gateways MGCP do Cisco IOS para obter uma lista de telefones IP, roteadores, módulos de rede e codecs suportados pela Cisco para SRST seguro.
- Consulte Firmware, plataformas, memória e o Produtos de voz suportados pelo Cisco Unified SRST 4.0 para obter as informações mais atualizadas sobre o número máximo de telefones IP da Cisco, o número máximo de números de diretório (DNs) ou de portas de voz virtuais e os requisitos de memória para o Cisco SRST.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Os telefones IP seguros da Cisco suportados no SRST seguro devem ter os certificados instalados e a criptografia habilitada.
- O roteador SRST deve ter um certificado. Um certificado pode ser gerado por terceiros ou pela autoridade certificadora (CA) do Cisco IOS. A autoridade certificadora do Cisco IOS pode funcionar no mesmo gateway que o SRST.
- As Certificate trust lists (CTLs) no Cisco CallManager devem ser habilitadas. Para obter instruções completas, consulte a seção *Configuração das chamadas de telefonia IP* de Autenticação de mídia e sinalização e recurso de criptografia para gateways MGCP do Cisco IOS.
- O Cisco CallManager 4.1(2) ou posterior deve ser instalado e oferecer suporte ao modo de segurança (modo de autenticação e criptografia).
- Os gateway router que executam o SRST seguro devem apoiar as imagens IOS Cisco da voz e Segurança-permitida (uma imagem do software criptográfico do do do â do k9 do do â). Duas imagens são suportadas: Serviços de IP avançados, que incluem um número de recursos de segurança avançados, e Advanced Enterprise Services, que incluem o software Cisco IOS completo.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Restrições

Restrições gerais

- As características de software criptográfico (do do â do k9 do do â) estão sob controles de exportação. Esse produto contém recursos criptográficos e está sujeito às leis locais e dos Estados Unidos que regem importação, exportação, transferência e uso. A entrega de produtos criptográficos Cisco não implica a autoridade de terceiros para importar, exportar, distribuir ou usar a criptografia. Os importadores, exportadores, distribuidores e usuários são responsáveis pela conformidade com as leis dos EUA e dos demais países. Ao usar esse produto, você concorda em obedecer às leis e os regulamentos aplicáveis. Se você não puder obedecer às leis dos EUA e dos demais países, devolva o produto imediatamente.Um resumo das leis dos EUA que regem os produtos criptográficos da Cisco pode ser encontrado em:http://www.cisco.com/wwl/export/crypto/tool/Se você precisar de mais ajuda, entre em contato enviando um email para export@cisco.com.
- Quando uma chamada criptografada pelo Secure Real-Time Transport Protocol (SRTP) é feita entre pontos de extremidade de telefones IP da Cisco ou de um Telefone IP da Cisco para um ponto de extremidade, um ícone de bloqueio é exibido nos telefones IP. O bloqueio

indica segurança somente para a parte do IP da chamada. A segurança da parte do PSTN não está implícita.
- O SRST seguro é suportado somente no âmbito de um único roteador.

Recursos não suportados e software no modo SRST seguro

- Versões do Cisco CallManager anteriores à 4.1(2)
- Música segura em espera (MoH)
- Transcodificação ou conferências seguras
- H.323 ou SIP seguro
- Hot Standby Router Protocol (HSRP)

Chamadas suportadas no modo SRST seguro

Somente as chamadas de voz são suportadas no modo SRST seguro. Estas chamadas de voz são especificamente suportadas:

- Chamada básica
- Encaminhamento de chamada (ocupado, sem resposta, tudo)
- Linha compartilhada (telefones IP)
- Transferência de chamada (consulta e oculta)
- Em espera e retomar

Informações de Apoio

Fallback de texto simples de telefones IP da Cisco durante o SRST

As versões do Cisco SRST anteriores ao software Cisco IOS Release 12.3(14)T não podem oferecer suporte a conexões seguras nem habilitar a segurança. Se um roteador de SRST não é capaz do SRST seguro porque um do do modeâ da reserva isto é, ele não pode terminar um handshake de TLS com do de Cisco CallManagerâ seu certificado não é adicionado ao arquivo de configuração do Cisco IP Phone. A ausência de um certificado do roteador SRST faz com que o telefone IP da Cisco use uma comunicação não segura (texto simples) quando está no modo de fallback de SRST. A capacidade de detectar e fazer fallback no modo de texto simples é criada no firmware do telefone IP da Cisco. Consulte Autenticação de mídia e sinalização e recurso de criptografia para gateways MGCP do Cisco IOS para obter mais informações sobre o modo de texto simples.

Roteadores SRST e o protocolo TLS

A Transport Layer Security (TLS) Versão 1.0 fornece os canais TCP seguros entre telefones IP da Cisco, roteadores SRST seguros e o Cisco CallManager. O processo de TLS começa quando o telefone IP da Cisco estabelece uma conexão TLS quando se registra no Cisco CallManager. Se o Cisco CallManager estiver configurado para fallback para SRST, a conexão TLS entre os telefones IP da Cisco e o roteador SRST seguro também será estabelecida. Se o link WAN ou o Cisco CallManager falhar, o controle de chamadas é revertido para o roteador SRST.

Roteadores SRST e PKI

A transferência de certificados entre um roteador SRST e o Cisco CallManager é obrigatória para a funcionalidade SRST segura. Os comandos da Public key infrastructure (PKI) são usados para

gerar, importar e exportar os certificados para o SRST seguro. Os certificados de cada telefone IP da Cisco suportado são mostrados nesta tabela.

Tabela 1 - Telefones IP e certificados suportados da Cisco

Telefone IP 7940 da Cisco	Telefone IP 7960 da Cisco	Telefone IP 7970 da Cisco
O telefone recebe o certificado de importância local (LSC) da Certificate Authority Proxy Function (CAPF) no formato Distinguished Encoding Rules (DER). Nome do arquivo do certificado: 59fe77ccd.0 que o nome de arquivo pode mudar baseado no nome do sujeito do certificado CAPF e no emissor de certificado CAPF. Se o Cisco CallManager usar um fornecedor de certificado de terceiros, pode haver diversos arquivos .0 (de dois a dez). Cada arquivo de certificado .0 deve ser importado individualmente durante a configuração. Somente o registro manual é suportado.	O telefone recebe o certificado de importância local (LSC) da Certificate Authority Proxy Function (CAPF) no formato Distinguished Encoding Rules (DER). Nome do arquivo do certificado: 59fe77ccd.0 que o nome de arquivo pode mudar baseado no nome do sujeito do certificado CAPF e no emissor de certificado CAPF. Se o Cisco CallManager usar um fornecedor de certificado de terceiros, pode haver diversos arquivos .0 (de dois a dez). Cada arquivo de certificado .0 deve ser importado individualmente durante a configuração. Somente o registro manual é suportado.	O telefone contém um certificado instalado pelo fabricante (MIC) usado para autenticação do dispositivo. Se o Cisco 7970 implementar o MIC, serão necessários dois arquivos públicos de certificado: • CiscoCA.pem (autoridade certificadora de raiz da Cisc

		o, usada para autenticar o certificado) • a69d2e04.0, no formato Privacy Enhanced Mail (PEM) Se o Cisco CallManager usar um fornecedor de certificado de terceiros, pode haver diversos arquivos .0 (de dois a dez). Cada arquivo de certificado .0 deve ser importado individua

		lmente durante a configur ação. Somente o registro manual é suportad o.

Servidor de credenciais do Cisco IOS em roteadores SRST seguros

O SRST seguro apresenta um servidor de credenciais executado em um roteador SRST seguro. Quando o cliente, o Cisco CallManager, solicita um certificado através do canal TLS, o servidor de credenciais fornece o certificado do roteador SRST ao Cisco CallManager. O Cisco CallManager insere o certificado do roteador SRST no arquivo de configuração do telefone IP da Cisco e baixa os arquivos de configuração para os telefones. O telefone IP seguro da Cisco usa o certificado para autenticar o roteador SRST durante operações de fallback. O serviço de credenciais é executado na porta TCP 2445 padrão.

Cinco novos comandos do Cisco IOS configuram o servidor de credenciais no modo de fallback do gerenciador de chamadas e fornecem recursos de verificação e debugação do servidor:

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

Estabelecimento do SRST seguro para o telefone IP da Cisco

Esse diagrama mostra o entrelaçamento do servidor de credenciais no roteador SRST, no Cisco CallManager e no telefone IP da Cisco, que estabelece o SRST seguro para o telefone IP da Cisco.

1. O telefone IP da Cisco configura o DHCP e obtém o endereço do servidor TFTP.
2. O telefone IP da Cisco recupera um arquivo CTL do servidor TFTP. O arquivo CTL contém os certificados nos quais o telefone deve confiar.
3. O telefone IP da Cisco abre um canal de protocolo Transport Layer Security (TLS) e se registra no Cisco CallManager.

O Cisco CallManager exporta informações do roteador SRST e o certificado do roteador SRST para o telefone IP da Cisco. O telefone coloca o certificado em sua configuração. Quando o telefone tiver o certificado SRST, o roteador SRST será considerado seguro.

Se o Cisco IP Phone está configurado como o do do authenticatedâ do do do â ou e CallManager da Cisco do do encryptedâ do do do â está configurado em modo misturado, o telefone procura um certificado SRST em seu arquivo de configuração. Se ele encontrar um

certificado SRST, abrirá uma conexão TLS de espera com a porta padrão. A porta padrão é a porta TCP do telefone IP da Cisco mais 443, que é a porta 2443 em um roteador SRST. A conexão com o roteador SRST acontece automaticamente, desde que não haja um Cisco CallManager secundário e o SRST esteja configurado como dispositivo de backup.

O Cisco CallManager deve ser configurado em modo misto, que é seu modo seguro.

Em caso da falha da WAN, o telefone IP da Cisco inicia o registro do SRST. O telefone IP da Cisco se registra no roteador SRST na porta padrão para comunicações seguras.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

O roteador SRST seguro e os telefones IP da Cisco devem solicitar a autenticação mútua durante o cumprimento de TLS. O cumprimento de TLS ocorre quando o telefone se registra no roteador SRST, antes ou depois da falha do link da WAN. O exemplo de configuração não inclui o uso de uma autoridade certificadora de terceiros. Ele assume que o uso do servidor certificado do Cisco IOS gera seus certificados.

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama. O diagrama ilustra o processo de autenticação e criptografia segura de SRST.

1. A autoridade autenticadora do servidor, seja uma autoridade autenticadora do roteador do Cisco IOS ou uma autoridade autenticadora de terceiros, emite um certificado de dispositivo para o gateway SRST, que permite o serviço das credenciais. Opcionalmente, o certificado pode ser gerado automaticamente pelo roteador SRST com um servidor da autoridade autenticadora do Cisco IOS.O roteador da autoridade autenticadora é o ponto de confiança definitivo para Certificate Authority Proxy Function (CAPF). Consulte o Guia de Segurança do Cisco CallManager para obter mais informações sobre a CAPF.
2. A CAPF é um processo onde os dispositivos suportados podem solicitar um certificado de importância local. O utilitário CAPF gera um par de chaves e um certificado específico da CAPF, copia esse certificado para todos os servidores do Cisco CallManager no cluster e fornece o LSC ao telefone IP da Cisco. Um LSC é exigido para os telefones IP da Cisco que não têm um certificado instalado pelo fabricante (MIC). O Cisco 7970 é equipado com um MIC e, portanto, não precisa passar pelo processo de CAPF.
3. O Cisco CallManager solicita o certificado SRST do servidor de credenciais, e o servidor de credenciais responde com o certificado.
4. Para cada dispositivo, o Cisco CallManager usa o processo TFTP e insere o certificado no arquivo de configuração SEPMACxxxx.cnf.xml do telefone IP da Cisco.
5. O Cisco CallManager fornece os arquivos de formato PEM que contêm as informações do certificado do telefone ao roteador SRST. Os arquivos PEM são fornecidos ao roteador SRST manualmente. Quando o roteador SRST tem os arquivos PEM, pode autenticar o

telefone IP e validar o emissor do certificado do telefone IP durante o cumprimento de TLS.
6. O cumprimento de TLS ocorre, os certificados são trocados e a autenticação mútua e o registro ocorrem entre o telefone IP da Cisco e o roteador SRST.O roteador SRST envia seu certificado e o telefone valida o certificado para o certificado que recebeu do Cisco CallManager na etapa 4.O telefone ip da Cisco fornece o roteador SRST o LSC ou o MIC, e o roteador valida o LSC ou o MIC com os arquivos de formato PEM que recebeu na etapa 5.**Nota:** A mídia é criptografada automaticamente quando os certificados de telefone e roteador são trocados e a conexão TLS é estabelecida com o roteador SRST.

Antes de configurar

Cisco CallManager

Conclua estes passos:

1. Quando o serviço de credenciais forem executados no roteador SRST, uma referência SRST ao Cisco CallManager precisará ser adicionada, pois o Cisco CallManager se conecta ao roteador SRST para o certificado do dispositivo. Consulte a *seção Survivable Remote Site Telephony* do Guia de Administração do Cisco CallManager, Release 4.1(2) para obter informações completas sobre como adicionar o SRST ao Cisco CallManager.
2. O fallback do SRST deve ser configurado no Cisco CallManager. Para fazer isso, atribua o pool de dispositivos ao SRST. Consulte a *seção de Configuração do pool de dispositivos* do Guia de Administração do Cisco CallManager, Release 4.1(2) para obter informações completas sobre como adicionar um pool de dispositivos ao Cisco CallManager.
3. A Certificate Authority Proxy Function (CAPF) deve ser configurada no Cisco CallManager. O processo CAPF permite que os dispositivos suportados, como o Cisco CallManager, solicitem certificados LSC dos telefones IP da Cisco. O utilitário CAPF gera um par de chaves e um certificado específico da CAPF e copia esse certificado para todos os servidores do Cisco CallManager no cluster. Consulte Autenticação e Criptografia de telefone IP da Cisco para Cisco CallManager 4.0(1) para obter instruções completas sobre como configurar o CAPF no Cisco CallManager.

Cuidados de segurança

- O **comando grant auto** permite que os certificados sejam emitidos e devem ser ativados quando você define sua autoridade autenticadora raiz. No entanto, por motivos de segurança, o **comando grant auto** não deve permanecer ativo e deve ser desativado depois que os certificados forem emitidos.
- Uma prática recomendada de segurança é proteger a porta do serviço de credenciais com a política de plano de controle. A política de plano de controle protege o gateway e mantém encaminhamentos de pacote e estados de protocolo, apesar de uma carga de tráfego pesada. Consulte Políticas de plano de controle para obter mais informações sobre os planos de controle. Um exemplo de configuração também aparece na seção Configuração 2 deste documento.

Configurações

Este documento utiliza as seguintes configurações:

- O do do â da configuração 1 configura seu roteador de acordo com este exemplo da executar-**configuração da mostra**.
- O melhor prática da Segurança do A do do â da configuração 2 é proteger a porta do serviço das credenciais com Policiamento do plano de controle. Se você usa o políticas de plano de controle, configure seu roteador de acordo com este exemplo **show running-config**.

Configuração 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 ..... . .
.
```

Configuração 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Verificar configurações da credencial

Para verificar se as configurações de credencial no roteador SRST são fornecidas ao Cisco CallManager para o uso durante o fallback de SRST seguro, emita o comando **show credentials**.

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

Verificar o registro do certificado

Se você usou o servidor certificado do Cisco IOS como sua autoridade certificadora, emita o comando **show running-config** a fim de verificar o certificado de registro ou o comando do servidor crypto do pki a fim de verificar o status do servidor da autoridade certificadora.

1. Emita o comando **show running-config** a fim de verificar a criação dos certificados do servidor da autoridade certificadora (01) e do dispositivo (02). Esse exemplo mostra os certificados registrados.
```
! 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. Emita o **comando show crypto pki server** a fim de verificar o status do servidor da autoridade certificadora após um procedimento de inicialização.`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
```

Verificar os registros e o status do telefone

Para verificar ou corrigir o status e o registro do telefone IP, siga estas etapas no modo EXEC privilegiado.

1. Emita o comando **show ephone** a fim de exibir telefones IP registrados da Cisco e seus recursos. Esse comando também exibe o status da autenticação e da criptografia quando usado para o SRST seguro. Nesse exemplo, o status da autenticação e da criptografia é ativado com uma conexão TLS.`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. Emita o comando **show ephone offhook** a fim de exibir o status e a qualidade do telefone IP da Cisco para todos os telefones que estão fora do gancho. Nesse exemplo, o status da autenticação e da criptografia é ativado com uma conexão TLS, e há uma chamada ativa segura.
```
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. Emita o comando **show voice call status** a fim de exibir o status de chamada para todas as portas de voz no roteador Cisco SRST. Esse comando não é aplicável a chamadas entre dois dial peers POTS.
```
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
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para obter informações adicionais sobre de como pesquisar defeitos, veja a informação relacionada