

Documentação de Conformidade de Interceptação ANSSI R226

Propósito do Documento: Este documento fornece especificações técnicas necessárias para a autorização ANSSI R226 sob os Artigos R226-3 e R226-7 do Código Penal Francês para a Rede Central IMS OmniCSCF (Funções de Controle de Sessão de Chamadas).

Classificação: Documentação de Conformidade Regulatória

Autoridade Alvo: Agence nationale de la sécurité des systèmes d'information (ANSSI)

Regulamentação: R226 - Proteção da Privacidade da Correspondência e Interceptação Legal

1. ESPECIFICAÇÕES TÉCNICAS DETALHADAS

1.1 Identificação do Sistema

Nome do Produto: OmniCSCF IMS Core Network

Tipo de Produto: Rede Central do Subsistema Multimídia IP (IMS)

Função Principal: Controle de sessão de chamadas VoIP/VoLTE e entrega de serviços multimídia

Modelo de Implantação: Infraestrutura de telecomunicações local

Componentes da Rede:

- P-CSCF (Função de Controle de Sessão de Chamadas Proxy)
- E-CSCF (Função de Controle de Sessão de Chamadas de Emergência)
- I-CSCF (Função de Controle de Sessão de Chamadas Interrogante)
- S-CSCF (Função de Controle de Sessão de Chamadas Servidora)

Este sistema gerencia registro, autenticação, roteamento de sessões e controle de chamadas para redes do Subsistema Multimídia IP (IMS). As capacidades detalhadas de interceptação e características de criptografia são descritas nas seções abaixo.

1.2 Capacidades de Interceptação

1.2.1 Captura de Registro e Aquisição de Sessão

Captura de Registro SIP:

O sistema CSCF processa todos os registros SIP e mantém o estado completo do registro:

- **Identificadores de Usuário:**
 - IMPU (Identidade Pública Multimídia IP) - URI SIP (ex: sip:[+33612345678@ims.mnc001.mcc001.3gppnetwork.org](tel:+33612345678))
 - IMPI (Identidade Privada Multimídia IP) - Nome de usuário de autenticação (ex: user@ims.mnc001.mcc001.3gppnetwork.org)
 - IMSI (Identidade Internacional de Assinante Móvel) - A partir de cabeçalhos P ou HSS
 - MSISDN (Número de telefone móvel) - A partir de IMPU ou perfil de usuário HSS
- **Metadados de Registro:**
 - URI de contato (endereço de rede UE atual)
 - Cabeçalho de caminho (rota de volta através do P-CSCF)
 - Cabeçalho Service-Route (rota para S-CSCF)
 - String User-Agent (identificação do tipo de dispositivo)
 - Timestamp de expiração do registro

- Endereço IP e porta de origem
- Protocolo de transporte (TCP/UDP/TLS)
- Vetores de autenticação (RAND, AUTN, XRES, CK, IK do HSS)

- **Informações de Localização da Rede:**

- Cabeçalho P-Access-Network-Info (torre de celular, área de localização)
- P-Visited-Network-ID (identificação da rede de roaming)
- Endereço IP recebido (fonte real)
- Endereço P-CSCF (ponto de entrada da rede)

Captura de Sessão de Chamada:

O S-CSCF mantém o estado completo do diálogo SIP para todas as chamadas ativas:

- **Identificadores de Sessão:**

- Call-ID (identificador único da sessão)
- URIs e tags From/To
- Conjuntos de rota para ambas as partes
- Original-Dialog-ID (para rastreamento de interação do Servidor de Aplicação)

- **Metadados da Sessão:**

- Identidade do chamador (cabeçalho From, P-Asserted-Identity)
- Parte chamada (cabeçalho To, Request-URI)
- Timestamp de estabelecimento da sessão
- Timestamp de término da sessão
- Estado do diálogo (Early/Confirmed/Deleted)
- Números CSeq (sequenciamento de transação)

- **Informações de Mídia:**

- SDP (Protocolo de Descrição de Sessão) nos corpos das mensagens SIP
- Endereços do servidor de mídia (OmniTAS)
- Informações de codec (formatos de áudio/vídeo)

- Pontos finais de fluxo de mídia
- Alocações de porta RTP/RTCP

Identificação de Chamadas de Emergência:

O componente E-CSCF identifica e roteia chamadas de emergência:

- Detecção de número de emergência (112, 911, etc.)
- Captura de IMEI (Identidade Internacional de Equipamento Móvel)
- Mapeamento de IMEI para MSISDN (para retorno de chamada)
- Informações de localização da UE ou da rede
- Suporte ao protocolo HELD (HTTP-Enabled Location Delivery)
- Destino de roteamento de emergência (PSAP/AS de emergência)

1.2.2 Armazenamento e Processamento de Dados

IMPORTANTE: Somente Estado em Memória

Os componentes CSCF (P-CSCF, E-CSCF, I-CSCF, S-CSCF) mantêm **todos os dados de estado apenas em memória**. Não há **armazenamento de banco de dados persistente** de dados de registro ou sessão de chamada. Todos os vínculos de registro, estado do diálogo e associações de segurança IPsec são armazenados em memória e são perdidos na reinicialização do sistema.

Dados de Registro Ativo (Em Memória):

O sistema CSCF mantém estado em tempo real apenas:

Estado de Registro do P-CSCF:

- Dados de Associação de Segurança IPsec (pares SPI, portas, parâmetros de criptografia)
- Vínculos de contato da UE e endereços de rede
- Pontos finais e status do túnel IPsec
- Períodos de validade do registro

Estado de Registro do S-CSCF:

- Identidades públicas (IMPU) e estado atual do registro

- Vínculos de contato com cabeçalhos de caminho, User-Agent, endereços recebidos
- Mapeamentos de identidade privada (IMPI) para identidade pública
- Perfis de usuário do HSS (em cache durante o registro)

Estado de Sessão Ativo (Em Memória):

O S-CSCF mantém estado de chamada ativa apenas:

- Identificadores de chamada (Call-ID), identidades dos participantes (tags From/To)
- Conjuntos de rota e endereços de contato
- Estado da sessão (Early/Confirmed/Terminated)
- Informações de tempo da sessão

Sem CDR ou Rastreamento Histórico:

Os componentes CSCF **não** geram ou armazenam:

- Registros de Detalhes de Chamadas (CDRs)
- Registros de chamadas históricas
- Registros de registro históricos
- Rastreamento de eventos a longo prazo

Geração de CDR e Rastreamento Histórico: Todos os registros de detalhes de chamadas, dados de cobrança e rastreamento de chamadas históricas são tratados pelo **TAS (Servidor de Aplicação de Telefonia - OmniTAS)**, não pelos componentes CSCF.

Registro de Mensagens SIP/Diameter:

Os CSCFs podem gerar registros de eventos em tempo real para fins operacionais:

- **Registro de Mensagens SIP:** Registro opcional de mensagens SIP (INVITE, REGISTER, etc.)
- **Registro de Mensagens Diameter:** Registro opcional de transações Diameter (Cx, Rx, Ro)

- **Eventos do Sistema:** Mudanças de configuração, erros, falhas

Esses registros são logs operacionais transitórios, não registros de chamadas persistentes. A retenção de logs é configurável e tipicamente de curto prazo (horas a dias) apenas para fins de depuração.

1.2.3 Capacidades de Análise

Monitoramento em Tempo Real:

O painel de controle web Phoenix LiveView fornece:

- **Monitoramento de Registro:**
 - Visualizar todos os usuários registrados com paginação
 - Pesquisar por IMPU, contato, IMPI
 - Detalhes do registro (contato, caminho, user-agent, expiração)
 - Capacidade de desregistro forçado
- **Monitoramento de Diálogo:**
 - Visualização de sessões de chamadas ativas
 - Call-ID, URIs From/To, estado, duração
 - Capacidade de término de chamada (enviar BYE)
 - Atualização automática a cada 5 segundos
- **Status do Sistema:**
 - Status do par Diameter (HSS, PCRF, conectividade OCS)
 - Status do gateway frontend
 - Métricas de capacidade do sistema
 - Capacidade do túnel IPsec (P-CSCF)

Nota sobre Dados Históricos:

Os componentes CSCF não mantêm dados históricos. Para registros de chamadas históricas, CDRs e análise de padrões de comunicação, as autoridades de interceptação legal devem coordenar com **OmniTAS (Servidor**

de Aplicação de Telefonia), que lida com toda a geração de CDR e rastreamento de chamadas a longo prazo.

Visibilidade de Acionamento de Serviço em Tempo Real:

O S-CSCF processa Critérios de Filtro Iniciais (iFC) em tempo real:

- A avaliação de iFC determina quais Servidores de Aplicação são acionados para cada chamada
- Visibilidade em tempo real sobre quais serviços são invocados
- Decisões de roteamento do Servidor de Aplicação visíveis no fluxo de mensagens SIP

Status da Rede:

- Status de conectividade HSS (interface Diameter Cx)
- Distribuição de seleção do S-CSCF (I-CSCF)
- Padrões de roteamento de chamadas
- Tempos de resposta do Servidor de Aplicação
- Desempenho de transações Diameter

1.3 Capacidades de Contramedidas

1.3.1 Mecanismos de Proteção da Privacidade

Confidencialidade da Comunicação:

- **Túneis IPsec:** Túneis ESP (Encapsulating Security Payload) entre UE e P-CSCF
 - Criptografia: AES-CBC, AES-GCM
 - Autenticação: HMAC-SHA1, HMAC-SHA256
 - Derivação de chave a partir do IMS AKA (CK/IK do HSS)
 - Associações de segurança por UE
- **Suporte TLS/TLS:**
 - Suporte SIP sobre TLS (SIPS)

- Diameter sobre TLS (conexões HSS, PCRF, OCS)
- Autenticação baseada em certificado
- Perfeita Confidencialidade de Chave (PFS) via ECDHE/DHE

- **Cabeçalhos de Privacidade SIP:**

- P-Asserted-Identity (ID do chamador autenticado)
- Cabeçalho de privacidade (solicitação de supressão de ID do chamador)
- Suporte a sessões anônimas

Controle de Acesso:

- Autenticação e controle de acesso da interface web
- Interface BINRPC para painel de controle (porta 2046)
- Controles de acesso ao registro e separação de funções
- Autenticação SIP (AKA via HSS)
- Autenticação de pares Diameter

Registro de Auditoria:

- Registro abrangente de mensagens SIP e Diameter
- Eventos de registro/desregistro
- Eventos de estabelecimento e término de chamadas
- Ações administrativas via interface web
- Mudanças de configuração
- Sucesso/falha de autenticação

1.3.2 Recursos de Proteção de Dados

Segurança de Acesso:

- Controle de acesso baseado em função (RBAC)
- Contas de monitoramento somente leitura
- Controles de autenticação e autorização

Fortalecimento do Sistema:

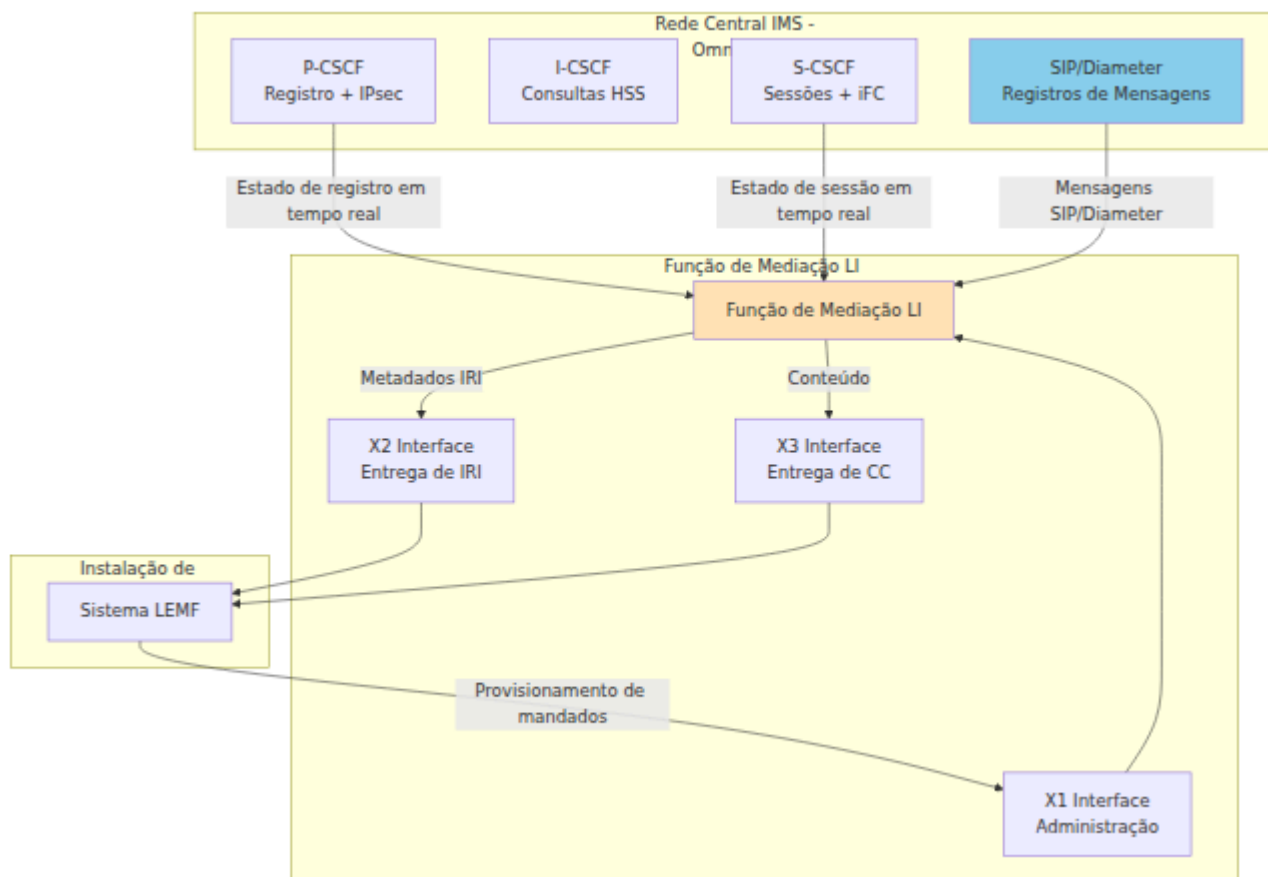
- Portas de rede expostas mínimas (5060 SIP, 3868 Diameter, 8086 Web UI)
- Verificação de sanidade de mensagens SIP
- Prevenção de loops Max-Forwards
- Limitação de taxa e proteção contra inundação
- Limites de tamanho de mensagem
- Isolamento de processos de trabalho

1.4 Pontos de Integração de Intercepção Legal

1.5.1 Arquitetura de Intercepção Legal ETSI

O sistema CSCF fornece a base para intercepção legal compatível com ETSI. Embora interfaces nativas X1/X2/X3 não estejam integradas, todos os pontos de acesso de dados necessários existem para integração com sistemas externos de Função de Mediação de Intercepção Legal (LIMF).

Interfaces LI Padrão ETSI:



Interface X1 - Função de Administração:

- **Propósito:** Provisionamento de mandados e alvos a partir da aplicação da lei
- **Direção:** LEMF → LIMF (bidirecional)
- **Funções:**
 - Ativar/desativar interceptação para alvos (IMPUs, IMSIs, MSISDNs)
 - Definir duração e período de validade da interceptação
 - Configurar critérios de filtragem (identidades, janelas de tempo)
 - Recuperar status de interceptação
- **Integração com CSCF:**
 - LIMF mantém banco de dados de mandados (lista de alvos - externa ao CSCF)
 - LIMF monitora o estado em tempo real do CSCF e os registros de mensagens para sessões correspondentes
 - LIMF filtra com base nos critérios provisionados por X1

Interface X2 - Entrega de IRI (Informações Relacionadas à Interceptação):

- **Propósito:** Entregar metadados da sessão para a aplicação da lei
- **Direção:** LIMF → LEMF (unidirecional)
- **Formato de Dados:** XML/ASN.1 compatível com ETSI TS 102 232
- **Conteúdo do CSCF:**
 - Identificadores de sessão (Call-ID, tags de diálogo)
 - Parte chamadora (URI From, P-Asserted-Identity, IMPU, IMSI, MSISDN)
 - Parte chamada (URI To, Request-URI, IMPU, IMSI, MSISDN)
 - Timestamps de registro
 - Timestamps de configuração/desmontagem da sessão
 - Localização da rede (P-Access-Network-Info, torre de celular, área de localização)
 - Endereços P-CSCF/S-CSCF (identificação do elemento de rede)
 - User-Agent (tipo de dispositivo)
 - Informações de roaming (P-Visited-Network-ID)

Interface X3 - Entrega de CC (Conteúdo da Comunicação):

- **Propósito:** Entregar o conteúdo real da comunicação
- **Direção:** LIMF → LEMF (unidirecional)
- **Formato de Dados:** Compatível com ETSI TS 102 232
- **Conteúdo do CSCF:**
 - Corpos de mensagens SIP (descrições de sessão SDP)
 - Endereços do servidor de mídia (para interceptação RTP)
 - Informações de codec
 - Mensagens instantâneas SIP MESSAGE (conteúdo do corpo)
 - Dados de aplicação (se roteados através do CSCF)

Nota: Para fluxos RTP de voz/vídeo, o LIMF também deve integrar-se com servidores de mídia (OmniTAS) para capturar o conteúdo real da mídia. O CSCF fornece informações de configuração da sessão (SDP) mostrando onde a mídia flui.

1.5.2 Fontes de Dados do CSCF para Interceptação Legal

1. Acesso a Dados de Registro:

Dados de Registro do P-CSCF:

- IMPU (identidade pública)
- URI de contato (endereço de rede UE)
- IP e porta recebidos
- Cabeçalho de caminho
- Expiração do registro
- Informações de SPI e porta IPsec
- String User-Agent

Dados de Registro do S-CSCF:

- Identidades públicas (IMPU), status de bloqueio, estado do registro
- Vínculos de contato com cabeçalhos de caminho, User-Agent, endereços recebidos
- Mapeamentos de identidade privada (IMPI) para identidade pública
- Perfis de usuário do HSS (formato XML incluindo detalhes do assinante)

Métodos de Acesso:

- Interfaces de acesso a dados somente leitura
- Interface de monitoramento da interface web
- Capacidade de registro de eventos em tempo real

2. Dados de Sessão Ativa:

Dados de Diálogo do S-CSCF:

- Call-ID (identificador único da sessão)
- URIs e tags From/To
- Números CSeq do chamador e da parte chamada
- Conjuntos de rota para ambas as partes
- Endereços de contato
- Estado do diálogo (Early, Confirmed, Deleted)
- Timestamp de início
- Valores de timeout

Métodos de Acesso:

- Monitoramento do estado do diálogo em tempo real
- Consulta por identificadores de sessão ou identificadores de partes
- Capacidades de exportação para análise forense

3. Registro de Mensagens SIP:

Captura de Log:

- Todas as mensagens SIP podem ser registradas (REGISTER, INVITE, MESSAGE, etc.)
- Níveis de log configuráveis
- Registro estruturado com timestamps
- Registro baseado em syslog ou arquivo

Análise de Log:

- Analisar cabeçalhos SIP para extração de identidade

- Extrair SDP para informações de mídia
- Rastrear sequências de mensagens (CSeq)
- Correlacionar solicitações e respostas

Exemplo de Entrada de Log:

```
INFO: INVITE sip:+33687654321@ims.mnc001.mcc001.3gppnetwork.org
SIP/2.0
From:
<sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org>;tag=abc123
To: <sip:+33687654321@ims.mnc001.mcc001.3gppnetwork.org>
Call-ID: f81d4fae-7dec-11d0-a765-
00a0c91e6bf6@ims.mnc001.mcc001.3gppnetwork.org
P-Asserted-Identity:
<sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org>
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-id-
3gpp=208011234567890
Content-Type: application/sdp

v=0
o=- 1234567890 1234567890 IN IP4 192.168.1.100
s=-
c=IN IP4 10.20.30.40
t=0 0
m=audio 49170 RTP/AVP 0 8
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
```

4. Registro de Mensagens Diameter:

Mensagens Cx (Comunicação HSS):

- UAR/UAA: Autorização de usuário (contém IMPU, IMPI)
- LIR/LIA: Informações de localização (contém IMPU, S-CSCF em serviço)
- MAR/MAA: Autenticação (contém IMPI, vetores de autenticação)
- SAR/SAA: Atribuição de servidor (contém IMPU, IMPI, XML de perfil de usuário)

Dados Diameter Disponíveis:

- IMSI (do perfil de usuário)
- MSISDN (do perfil de usuário)
- IMPUs associados (múltiplas identidades por assinante)
- Perfil de usuário (serviços, bloqueio, status de roaming)

Exemplo de Log:

```
Diameter Cx SAA recebido do HSS:  
User-Name: user@ims.mnc001.mcc001.3gppnetwork.org  
Public-Identity:  
sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org  
Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org  
Result-Code: 2001 (Sucesso)  
User-Data: <XML perfil de usuário com IMSI, MSISDN, iFC>
```

5. Dados de Chamadas de Emergência (E-CSCF):

Mapeamento de IMEI para MSISDN:

- O P-CSCF cria o mapeamento quando a UE se registra com IMEI
- TTL (Time-To-Live) de 24 horas
- Usado para retorno de chamada de emergência
- Sincronizado entre os nós do cluster P-CSCF

Retenção de Dados:

- Mapeamentos de IMEI para MSISDN retidos por 24 horas
- Disponíveis para correlação de retorno de chamada de emergência
- Acessíveis via interfaces de monitoramento

Logs de Chamadas de Emergência:

- Detecção de número de emergência (112, 911, etc.)
- Extração de IMEI de contato ou cabeçalhos P
- Informações de localização (do HELD ou P-Access-Network-Info)
- Roteamento PSAP (Ponto de Atendimento de Segurança Pública)
- Roteamento E-CSCF para AS de emergência

1.5.3 Capacidades de Integração para LIMF

O sistema fornece múltiplos métodos de integração para sistemas de Função de Mediação de Interceptação Legal (LIMF):

1. Acesso a Dados de Registro e Sessão:

- Acesso em tempo real a dados de registro (identidades, localizações, informações do dispositivo)
- Monitoramento de sessão ativa (estado da chamada, participantes, tempo)
- Capacidades de consulta histórica

2. Registro de Eventos:

- Registro de mensagens SIP com níveis de detalhe configuráveis
- Registro de mensagens Diameter para interações HSS
- Registros de eventos estruturados com timestamps

3. Monitoramento em Tempo Real:

- Monitoramento do status de registro ao vivo
- Rastreamento de sessão de chamada ativa
- Detecção de chamadas de emergência e informações de roteamento

Os métodos de integração suportam arquiteturas baseadas em polling e acionadas por eventos para conectividade LIMF.

1.5.4 Mapeamento de Dados do CSCF para Interfaces LI

Mapeamento de Dados do CSCF para IRI (X2):

Fonte de Dados do CSCF	Campo IRI	Exemplo de Dados
IMPU (cabeçalhos SIP/estado em memória)	Parte A	sip:+33612345678@ims.mnc001.mcc001.3gpp
IMPI (cabeçalhos SIP/estado em memória)	ID de Autenticação	user@ims.mnc001.mcc001.3gppnetwork.org
IMSI (perfil de usuário HSS)	ID do Assinante	208011234567890
MSISDN (perfil de usuário HSS)	Número de Telefone	+33612345678
Call-ID (cabeçalhos SIP/estado do diálogo)	ID da Sessão	f81d4fae-7dec-11d0-a765-00a0c91e6bf6@...
From/To (cabeçalhos SIP)	Parte A/Parte B	sip:+33612345678@... / sip:+33687654321@.
Timestamp de registro	Hora do Evento	2025-11-29T10:30:00Z

Fonte de Dados do CSCF	Campo IRI	Exemplo de Dados
(em memória)		
P-Access-Network-Info (cabeçalho SIP)	Localização	3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=208011
IP Recebido (contato SIP)	Endereço IP da UE	10.20.30.40:5060
Endereço P-CSCF (roteamento SIP)	Elemento de Rede	10.4.12.165:5060
Endereço S-CSCF (roteamento SIP)	Elemento de Rede	10.4.11.45:5060

Mapeamento de Dados do CSCF para CC (X3):

Fonte de Dados do CSCF	Campo CC	Exemplo de Dados
Corpo da mensagem SIP	Conteúdo da Mensagem Instantânea	"Olá, como você está?"
SDP no INVITE	Informações da Sessão de Mídia	Pontos finais RTP, codecs
Endereço do servidor de mídia	Alvo de Interceptação RTP	10.50.60.70:49170

Nota: Para conteúdo real de voz/vídeo (RTP), o LIMF deve coordenar com servidores de mídia (OmniTAS) para capturar fluxos RTP. O CSCF fornece apenas informações de configuração da sessão.

1.5 Interface de Monitoramento Baseada na Web

O sistema inclui um painel de controle baseado na web para monitoramento em tempo real e acesso administrativo:

Capacidades de Monitoramento:

- Status de registro em tempo real (assinantes ativos, localizações, informações do dispositivo)
- Monitoramento de sessão de chamada ativa (participantes, estado da chamada, tempo)
- Pesquisa e filtragem por identidade (IMPU, IMPI, IMSI, MSISDN)
- Status do túnel IPsec e monitoramento de capacidade
- Capacidades de exportação para análise forense

Segurança:

- Acesso criptografado por HTTPS/TLS
- Autenticação necessária
- Registro de auditoria de todas as ações administrativas

- Modos de acesso somente leitura para pessoal de monitoramento
-

2. CAPACIDADES DE CRIPTOGRAFIA E CRIPTOANÁLISE

2.1 Visão Geral das Capacidades Criptográficas

O OmniCSCF implementa múltiplas camadas de proteção criptográfica para sinalização e dados de assinantes. Esta seção documenta todas as capacidades criptográficas conforme exigido pela ANSSI.

2.2 Criptografia de Túnel IPsec ESP (UE para P-CSCF)

2.2.1 Implementação do Protocolo IPsec

Modo IPsec Suportado:

- ESP (Encapsulating Security Payload) - Protocolo IP 50
- Modo de transporte (não modo túnel)
- Protege a sinalização SIP entre UE e P-CSCF

Algoritmos de Criptografia Suportados:

O sistema com IPsec do kernel suporta:

- **AES-CBC (Padrão de Criptografia Avançada - Cadeia de Blocos de Cifras):**
 - AES-128-CBC (chave de 128 bits)
 - AES-192-CBC (chave de 192 bits)
 - AES-256-CBC (chave de 256 bits) - Recomendado
- **AES-GCM (Padrão de Criptografia Avançada - Modo Galois/Contador):**

- AES-128-GCM (chave de 128 bits com AEAD)
- AES-256-GCM (chave de 256 bits com AEAD) - Recomendado
- **3DES-CBC (Triple DES - Cadeia de Blocos de Cifras):**
 - Chave efetiva de 168 bits (depreciado, compatibilidade legada)
- **Criptografia NULL:**
 - Sem confidencialidade (somente autenticação)
 - Usado apenas para depuração ou cenários de conformidade específicos

Algoritmos de Autenticação Suportados:

- **HMAC-SHA1 (Código de Autenticação de Mensagem Baseado em Hash - SHA-1):**
 - Saída de 160 bits
 - Compatibilidade legada
- **HMAC-SHA256 (HMAC - SHA-256):**
 - Saída de 256 bits
 - Recomendado
- **HMAC-SHA384 (HMAC - SHA-384):**
 - Saída de 384 bits
- **HMAC-SHA512 (HMAC - SHA-512):**
 - Saída de 512 bits
- **HMAC-MD5:**
 - Saída de 128 bits
 - Depreciado, apenas compatibilidade legada

Derivação de Chaves:

As chaves IPsec (CK - Chave de Cifra, IK - Chave de Integridade) são derivadas da autenticação IMS AKA:

1. UE realiza autenticação AKA com S-CSCF/HSS
2. HSS gera CK (128 bits) e IK (128 bits)
3. S-CSCF entrega CK/IK ao P-CSCF via interface interna
4. P-CSCF usa CK/IK para estabelecer associações de segurança IPsec com UE
5. CK usado para criptografia ESP
6. IK usado para autenticação ESP

Parâmetros de Associação de Segurança:

- **Vida Útil:** Vinculada à expiração do registro SIP (tipicamente 599 segundos)
- **Proteção contra Repetição:** Habilitada (janela anti-repetição)
- **Números de Sequência:** 32 bits ou 64 bits (ESN - Números de Sequência Estendidos)
- **Perfeita Confidencialidade de Chave:** Não aplicável (chaves do AKA, não Diffie-Hellman)

Implementação:

A capacidade IPsec do P-CSCF:

- Interage com a pilha IPsec do kernel Linux (estrutura XFRM)
- Configura políticas de segurança e associações via API do kernel
- Alocação e gerenciamento de SPI (Índice de Parâmetro de Segurança)
- Alocação de porta para tráfego protegido

2.2.2 Capacidades de Configuração IPsec

Seleção de Conjunto de Cifras:

O P-CSCF pode ser configurado para preferir conjuntos de cifras específicos:

Preferido (segurança forte):

- ESP com AES-256-GCM e HMAC-SHA256

- ESP com AES-256-CBC e HMAC-SHA256

Suportado (compatibilidade):

- ESP com AES-128-CBC e HMAC-SHA1
- ESP com 3DES-CBC e HMAC-SHA1 (legado)

Gerenciamento de Chaves:

- IKE (Internet Key Exchange) NÃO é usado
- Chaves fornecidas via IMS AKA (CK/IK do HSS)
- Configuração manual de associação de segurança via XFRM do kernel
- Desmontagem automática de SA na expiração do registro

Ciclo de Vida do Túnel:

1. UE se registra → autenticação AKA → CK/IK gerados
2. P-CSCF recebe CK/IK do S-CSCF
3. P-CSCF aloca par de SPI (SPI do cliente, SPI do servidor)
4. P-CSCF aloca par de portas (porta do cliente, porta do servidor)
5. P-CSCF configura SAs IPsec do kernel usando CK/IK
6. P-CSCF envia parâmetros IPsec para UE no 200 OK (cabeçalho Security-Server)
7. UE configura SAs IPsec com os mesmos parâmetros
8. Todo o tráfego SIP subsequente flui através de túneis ESP
9. Na expiração do registro ou desregistro: SAs deletadas, recursos liberados

2.3 Criptografia TLS (SIP e Diameter)

2.3.1 TLS para SIP (SIPS)

Versões TLS Suportadas:

- **TLS 1.2** (RFC 5246) - Suportado
- **TLS 1.3** (RFC 8446) - Suportado (se suporte do kernel/biblioteca)
- **TLS 1.0/1.1** - Decretado (desabilitado por padrão)
- **SSL 2.0/3.0** - NÃO SUPORTADO (vulnerabilidades conhecidas)

Implementação TLS:

o sistema usa OpenSSL ou LibreSSL:

- Bibliotecas TLS padrão da indústria
- Implementações validadas criptograficamente
- Atualizações de segurança regulares

Conjuntos de Cifras Suportados:

TLS 1.3 (Preferido):

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (Suportado):

- ECDHE-RSA-AES256-GCM-SHA384 (Perfeita Confidencialidade de Chave)
- ECDHE-RSA-AES128-GCM-SHA256 (Perfeita Confidencialidade de Chave)
- ECDHE-ECDSA-AES256-GCM-SHA384 (Perfeita Confidencialidade de Chave)
- DHE-RSA-AES256-GCM-SHA384 (Perfeita Confidencialidade de Chave)
- DHE-RSA-AES128-GCM-SHA256 (Perfeita Confidencialidade de Chave)

Cifras fracas desabilitadas:

- Sem RC4
- Sem MD5
- Sem criptografia NULL
- Sem cifras de grau EXPORT
- Sem DES/3DES (depreciado)

Suporte a Certificados:

- **Certificados X.509** (formato padrão)
- **Chaves RSA:** mínimo de 2048 bits, recomendado 4096 bits
- **Chaves ECDSA:** curvas P-256, P-384, P-521 suportadas
- **Validação de cadeia de certificados**

- **Verificação de CRL (Lista de Revogação de Certificados)** (opcional)
- **OCSP (Protocolo de Status de Certificado Online)** (opcional)

Recursos TLS:

- **Perfeita Confidencialidade de Chave (PFS):** Via troca de chaves ECDHE/DHE
- **Indicação de Nome do Servidor (SNI):** Suportada
- **Retomada de Sessão TLS:** Suportada (otimização de desempenho)
- **Autenticação de Certificado do Cliente:** Suportada (TLS mútuo)

SIP sobre TLS (SIPS):

- Transporte: TCP com criptografia TLS
- Porta: 5061 (porta padrão SIPS)
- Usado para comunicação inter-CSCF (opcional)
- Usado para conexões de rede confiáveis

2.3.2 TLS para Diameter

Capacidades Diameter:

O sistema suporta:

- **Diameter sobre SCTP** (preferido para confiabilidade)
- **Diameter sobre TCP com TLS**
- **Porta:** 3868 (porta Diameter padrão)

Casos de Uso:

- **Interface Cx:** S-CSCF/I-CSCF para HSS (dados do assinante, autenticação)
- **Interface Rx:** P-CSCF para PCRF (política de QoS)
- **Interface Ro:** S-CSCF para OCS (cobrança online - se habilitado)

Configuração TLS para Diameter:

Mesmos conjuntos de cifras que SIP

- TLS 1.2/1.3

- Troca de chaves ECDHE/DHE (PFS)
- Criptografia AES-GCM
- Autenticação SHA256/SHA384

Autenticação Baseada em Certificado:

- Pares Diameter se autenticam via certificados TLS
- TLS mútuo (certificados de cliente e servidor)
- Validação de FQDN (Nome de Domínio Totalmente Qualificado) em certificados
- Validação de cadeia de CA confiável

2.4 Criptografia de Autenticação

2.4.1 Funções Criptográficas IMS AKA

Algoritmo 3GPP AKA (MILENAGE):

Usado para gerar vetores de autenticação (RAND, AUTN, XRES, CK, IK):

Funções Criptográficas:

- **f1:** Função de autenticação de mensagem (calcular MAC-A e MAC-S)
- **f2:** Função de resposta (calcular RES a partir de RAND e K)
- **f3:** Derivação de chave de cifra (calcular CK)
- **f4:** Derivação de chave de integridade (calcular IK)
- **f5:** Função de chave de anonimato (calcular AK para privacidade de IMSI)

Material de Chave:

- **K:** Chave permanente de assinante de 128 bits (armazenada em ISIM e HSS)
- **OPc:** Chave variante do operador (derivada de K e OP)
- **RAND:** Desafio aleatório de 128 bits
- **SQN:** Número de sequência de 48 bits (proteção contra repetição)

Sequência AKA:

1. HSS gera RAND (aleatório criptograficamente)
2. HSS calcula $MAC-A = f_1(K, RAND, SQN, AMF)$
3. HSS calcula $AUTN = (SQN \oplus AK) || AMF || MAC-A$
4. HSS calcula $XRES = f_2(K, RAND)$
5. HSS calcula $CK = f_3(K, RAND)$
6. HSS calcula $IK = f_4(K, RAND)$
7. HSS envia $\{RAND, AUTN, XRES, CK, IK\}$ para S-CSCF
8. S-CSCF desafia UE com RAND e AUTN
9. UE calcula $RES = f_2(K, RAND)$ usando ISIM
10. UE envia RES para S-CSCF
11. S-CSCF compara RES com XRES (validação de autenticação)

Propriedades de Segurança:

- **Autenticação Mútua:** UE verifica HSS via AUTN, HSS verifica UE via RES
- **Novidade da Chave:** RAND é aleatório, SQN previne repetição
- **Derivação de Chave:** CK e IK derivadas do segredo compartilhado K

2.4.2 Autenticação Digest HTTP

Para autenticação não IMS (se usada):

Algoritmo: MD5 (RFC 2617)

- **Função de Hash:** MD5 (saída de 128 bits)
- **Desafio-Resposta:** Baseado em nonce
- **Proteção contra Repetição:** Nonce com timestamp

Nota: HTTP Digest com MD5 é considerado fraco. IMS AKA é fortemente preferido.

2.5 Hashing e Integridade

2.5.1 Funções de Hash Disponíveis

o sistema pode usar (via OpenSSL/crypto do kernel):

- **SHA-256:** saída de 256 bits, recomendado
- **SHA-384:** saída de 384 bits
- **SHA-512:** saída de 512 bits
- **SHA-1:** saída de 160 bits, depreciado para uso em segurança
- **MD5:** saída de 128 bits, depreciado para uso em segurança

Uso:

- Construções HMAC para IPsec/TLS
- Verificação de integridade de dados
- Geração de nonce
- Detecção de duplicatas (hashing de Call-ID)

2.5.2 Integridade da Mensagem

Integridade da Mensagem SIP:

- **IPsec ESP:** HMAC-SHA256 para SIP autenticado sobre IPsec
- **TLS:** Autenticação de mensagem via MAC TLS
- **Digest SIP:** Integridade do cabeçalho de autenticação

Integridade da Mensagem Diameter:

- **TLS:** Diameter sobre TLS fornece autenticação de mensagem
- **HMAC:** Mensagens Diameter podem incluir AVPs HMAC para integridade

2.6 Geração de Números Aleatórios

Geração de Números Aleatórios Criptograficamente Segura:

o sistema depende de:

- **Linux kernel /dev/urandom:** PRNG (Gerador de Números Aleatórios Criptograficamente Seguro)
- **OpenSSL RAND_bytes():** CSPRNG (Gerador de Números Aleatórios Pseudo-Criptograficamente Seguro)

Uso:

- Alocação de SPI (valor inicial aleatório)
- Geração de Call-ID
- Geração de parâmetros de ramificação
- Geração de nonce para autenticação
- Geração de ID de sessão

2.7 Gerenciamento de Chaves

2.7.1 Gerenciamento de Certificados TLS

Armazenamento de Certificados:

- Armazenamento em sistema de arquivos com permissões restritas (0600)
- Localizado em: `/etc/system/tls/`
- Formato PEM para certificados e chaves

Geração de Certificado:

```
# Gerar chave privada RSA de 4096 bits
openssl genrsa -out system-key.pem 4096

# Gerar CSR (Solicitação de Assinatura de Certificado)
openssl req -new -key system-key.pem -out system.csr \
  -subj
"/C=FR/ST=IDF/L=Paris/O=0mnitouch/CN=scscf.ims.mnc001.mcc001.3gppnetv

# Certificado autoassinado (desenvolvimento/teste)
openssl x509 -req -days 365 -in system.csr \
  -signkey system-key.pem -out system-cert.pem

# Produção: Enviar CSR para CA confiável
```

Rotação de Certificado:

- Renovação anual de certificado recomendada
- Reinicialização do serviço de forma suave para carregar novos certificados
- Sem tempo de inatividade necessário

2.7.2 Gerenciamento de Chaves IPsec

Derivação de Chaves:

- CK (Chave de Cifra) e IK (Chave de Integridade) do IMS AKA
- Chaves de 128 bits do HSS
- Entregues de forma segura via Diameter Cx (sobre TLS)

Vida Útil da Chave:

- Vinculada à expiração do registro SIP (tipicamente 599 segundos)
- Re-keying na atualização do registro
- Destruição automática da chave no desregistro

Armazenamento da Chave:

- Efêmera (apenas em memória durante o registro ativo)
- Instaladas na pilha IPsec do kernel
- Sem armazenamento persistente de chaves
- Chaves descartadas quando SA deletada

2.8 Resistência à Criptoanálise

2.8.1 Seleção de Algoritmo

Defesa Contra Criptoanálise:

- **Sem algoritmos personalizados:** Apenas algoritmos padrão da indústria, revisados por pares
- **Tamanhos de chave fortes:** AES-256, RSA-4096, SHA-256
- **Criptografia autenticada:** AES-GCM (AEAD - Criptografia Autenticada com Dados Associados)
- **Perfeita Confidencialidade de Chave:** ECDHE/DHE em TLS
- **Atualizações regulares:** Patches de segurança OpenSSL/LibreSSL aplicados

Algoritmos Decretados Desabilitados:

- MD5 (colisões de hash)
- RC4 (fraquezas do cifra de fluxo)
- DES/3DES (tamanho de bloco pequeno, comprimento da chave)
- SSL 2.0/3.0 (vulnerabilidades de protocolo)
- TLS 1.0/1.1 (ataques BEAST, POODLE)

2.8.2 Mitigação de Ataques de Canal Lateral

Resistência a Ataques de Tempo:

- Comparação em tempo constante para respostas de autenticação
- Sem vazamentos de tempo em operações criptográficas (via OpenSSL)

Proteção de Memória:

- Isolamento da pilha IPsec do kernel
- Isolamento de memória do processo
- Sem swap para dados sensíveis (se configurado)

2.9 Conformidade e Padrões

Conformidade com Padrões Criptográficos:

- **NIST SP 800-52:** Diretrizes TLS
- **NIST SP 800-131A:** Transições de algoritmos criptográficos
- **RFC 7525:** Recomendações TLS
- **ETSI TS 133 203:** Segurança de acesso 3GPP (IMS AKA)
- **ETSI TS 133 210:** Segurança da camada de rede IP (IPsec)
- **3GPP TS 33.203:** Segurança de acesso para IMS
- **3GPP TS 33.210:** Segurança do domínio da rede

Regulamentações Criptográficas Francesas:

- Sem criptografia restrita à exportação (todos os algoritmos padrão)
- Meios criptográficos padrão (sem portas dos governos)
- Certificação de produtos criptográficos ANSSI (se necessário)

Guia de Operações do Diameter

Índice

1. [Visão Geral](#)
2. [Diameter na Arquitetura IMS](#)
3. [Interfaces Diameter](#)
4. [Gerenciamento de Pares via UI Web](#)
5. [Códigos de Resultado do Diameter](#)
6. [Problemas Comuns](#)

Visão Geral

Diameter é o protocolo de autenticação, autorização e contabilidade (AAA) utilizado em toda a arquitetura IMS. O OmniCall CSCF usa Diameter para se comunicar com elementos críticos da rede, incluindo HSS, PCRF e OCS.

O que é Diameter?

Diameter (RFC 6733) é o sucessor do RADIUS, projetado para cenários modernos de AAA:

- **Transporte confiável** via TCP/SCTP (vs. UDP no RADIUS)
- **Extensível** via módulos específicos de aplicação
- **Arquitetura ponto a ponto** (não apenas cliente-servidor)
- **Conexões com estado** com monitoramento de watchdog
- **Tratamento de erros** e códigos de resultado **padronizados**

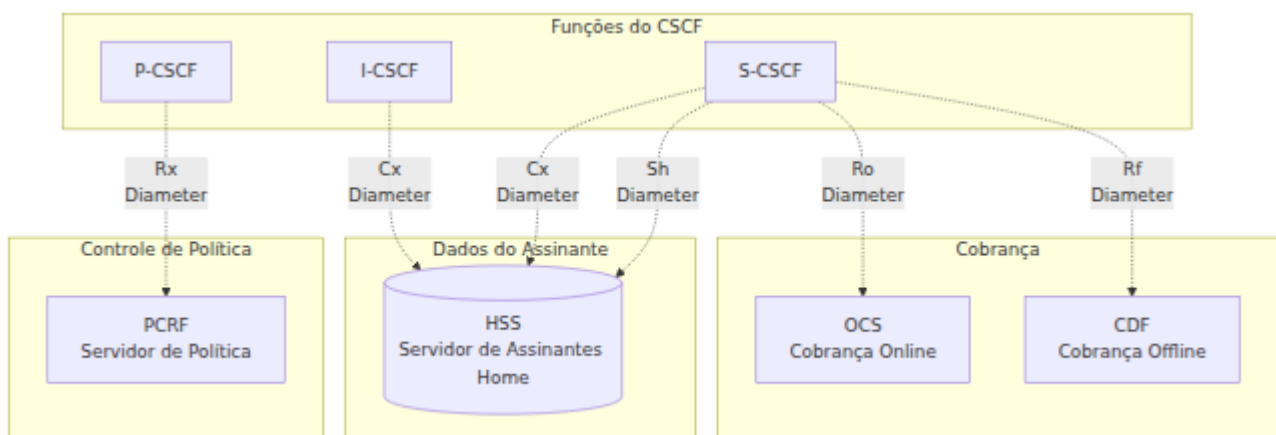
Diameter no CSCF

Cada componente do CSCF utiliza interfaces de aplicação Diameter específicas:

CSCF	Interface	ID da Aplicação	Conectado a	Propósito
I-CSCF	Cx	16777216	HSS	Seleção do S-CSCF, localização do usuário
S-CSCF	Cx	16777216	HSS	Autenticação do usuário, download de perfil
S-CSCF	Sh	16777217	HSS	Acesso a dados do usuário (opcional)
P-CSCF	Rx	16777236	PCRF	Controle de política de QoS e bearer
S-CSCF	Ro	4	OCS	Cobrança online (controle de crédito)
S-CSCF	Rf	3	CDF	Cobrança offline (contabilidade)

Diameter na Arquitetura IMS

Visão Geral da Rede



Interfaces Diameter

Interface Cx (CSCF ↔ HSS)

A interface Cx é utilizada pelo I-CSCF e S-CSCF para autenticação de usuários e gerenciamento de perfis.

Especificação 3GPP: TS 29.228

Operações do I-CSCF

User-Authorization-Request (UAR) / User-Authorization-Answer (UAA):

- **Propósito:** Consultar HSS para atribuição ou capacidades do S-CSCF
- **Gatilho:** REGISTER recebido do usuário
- **Caso de Uso:** I-CSCF precisa rotear o registro para o S-CSCF apropriado

Location-Info-Request (LIR) / Location-Info-Answer (LIA):

- **Propósito:** Consultar HSS para o S-CSCF atual do usuário
- **Gatilho:** INVITE ou MESSAGE recebido para o usuário final
- **Caso de Uso:** I-CSCF precisa rotear a sessão para o S-CSCF do usuário

Operações do S-CSCF

Multimedia-Auth-Request (MAR) / Multimedia-Auth-Answer (MAA):

- **Propósito:** Recuperar vetores de autenticação do HSS
- **Gatilho:** REGISTER inicial (antes do desafio)
- **Caso de Uso:** S-CSCF precisa desafiar o usuário para autenticação IMS AKA

Server-Assignment-Request (SAR) / Server-Assignment-Answer (SAA):

- **Propósito:** Informar o HSS sobre o estado do registro, baixar o perfil do usuário
- **Gatilho:** Autenticação bem-sucedida (após MAR/MAA)
- **Caso de Uso:** S-CSCF baixa IFC e perfil de serviço para o usuário

O AVP **User-Data** no SAA contém o perfil completo do usuário, incluindo:

- Identidades públicas
- Critérios de Filtro Inicial (IFC) para acionamento de serviços
- Identificadores de perfis de mídia assinados
- Informações de cobrança

Registration-Termination-Request (RTR) / Registration-Termination-Answer (RTA):

- **Propósito:** Desregistro iniciado pelo HSS (push do HSS)
- **Gatilho:** Desregistro administrativo, mudança de assinatura
- **Caso de Uso:** HSS instrui S-CSCF a desregistrar um usuário

Interface Rx (P-CSCF ↔ PCRF)

A interface Rx fornece controle de política e QoS para sessões IMS.

Especificação 3GPP: TS 29.214

AA-Request (AAR) / AA-Answer (AAA):

- **Propósito:** Solicitar autorização de QoS para a sessão de mídia
- **Gatilho:** Troca de oferta/resposta SDP no SIP INVITE
- **Caso de Uso:** P-CSCF solicita ao PCRF a autorização de recursos de bearer

Re-Auth-Request (RAR) / Re-Auth-Answer (RAA):

- **Propósito:** Atualização de política iniciada pelo PCRF (push do PCRF)
- **Gatilho:** Mudança de política, modificação de bearer
- **Caso de Uso:** PCRF instrui P-CSCF a atualizar a política de QoS

Session-Termination-Request (STR) / Session-Termination-Answer (STA):

- **Propósito:** Liberar a sessão Rx e recursos de bearer
- **Gatilho:** Término da chamada (BYE recebido)
- **Caso de Uso:** P-CSCF informa ao PCRF para liberar recursos de QoS

Interface Ro (S-CSCF ↔ OCS)

A interface Ro fornece cobrança online (controle de crédito).

Especificação 3GPP: TS 32.299

Credit-Control-Request (CCR) / Credit-Control-Answer (CCA):

- **Propósito:** Autorização e débito de crédito em tempo real
- **Gatilho:** Configuração de chamada, durante a chamada, término da chamada
- **Caso de Uso:** Cobrança pré-paga, verificações de crédito em tempo real

Tipos:

- **CCR-Initial:** Solicitar crédito no início da chamada
- **CCR-Update:** Atualizar cota durante a chamada
- **CCR-Terminate:** Relatar uso final no término da chamada

Gerenciamento de Pares via UI Web

O OmniCall CSCF fornece um painel de controle baseado na web para gerenciamento de pares Diameter.

Acesso: Navegue até a aba **Diameter** no painel de controle (`http://<cscf-server>:4000/diameter`)

Visualizando o Status do Par

A página de gerenciamento Diameter exibe:

Informações Resumidas

- **Realm:** Realm Diameter
- **Identidade:** Origin-Host Diameter
- **Contagem de Pares:** Número de pares configurados
- **Trabalhadores:** Contagem de trabalhadores CDP
- **Comprimento da Fila:** Transações pendentes
- **Tempo de Conexão:** Tempo limite de conexão (segundos)
- **Tempo de Transação:** Tempo limite de transação (segundos)
- **Aceitar Pares Desconhecidos:** Flag de política

Lista de Pares

Tabela de todos os pares Diameter com as seguintes colunas:

Coluna	Descrição
FQDN	Nome de domínio totalmente qualificado do par
Estado	Estado da conexão (I_Open, Closed, etc.)
Status	Habilitado ou Desabilitado
Último Usado	Tempo desde a última transação
Aplicações	Número de aplicações Diameter suportadas

Operações de Par

Habilitar Par:

1. Localize o par desabilitado na tabela
2. Clique no botão **Habilitar**
3. O par tentará estabelecer a conexão

Desabilitar Par:

1. Localize o par habilitado na tabela
2. Clique no botão **Desabilitar**
3. Confirme a ação
4. A conexão do par será encerrada de forma controlada

Ver Aplicações:

1. Clique na linha do par para expandir
2. Veja a lista de aplicações Diameter suportadas com nomes de interface

A visualização expandida do par mostra todas as aplicações Diameter suportadas:

- **16777216:10415** - 3GPP Cx/Dx (comunicação HSS para I-CSCF/S-CSCF)
- **16777236:10415** - 3GPP Rx (política de QoS do PCRF para P-CSCF)
- **16777238:0** - 3GPP Ro (Cobrança online)
- Outros IDs de aplicação suportados e IDs de fornecedor

O painel de controle mapeia automaticamente os IDs de Aplicação Diameter para nomes de interface 3GPP:

- **Cx/Dx** (16777216:10415)
- **Sh/Dh** (16777217:10415)
- **Rx** (16777236:10415)
- **Ro** (16777238:10415/0/5535/13019)
- **Gx** (16777224:10415)
- **S6a/S6d** (16777251:10415)
- E muitos mais (veja `diameter_live.ex` para a lista completa)

Estados dos Pares

Estado	Descrição
I_Open	Conexão aberta e operacional
Closed	Nenhuma conexão estabelecida
Wait-Conn-Ack	Conexão iniciada, aguardando resposta
Wait-I-CEA	CER enviado, aguardando CEA

Para gerenciamento detalhado de pares: Veja [Guia de Operações da UI Web](#)

Códigos de Resultado do Diameter

Códigos de resultado comuns e seus significados:

Código	Nome	Significado	Aç
2xxx	Sucesso		
2001	DIAMETER_SUCCESS	Operação bem-sucedida	Nenhum
3xxx	Erros de Protocolo		
3002	DIAMETER_UNABLE_TO_DELIVER	Não é possível rotear para o destino	Verifique conectividade do par
3003	DIAMETER_REALM_NOT_SERVED	Realm não reconhecido	Verifique configuração realm
3007	DIAMETER_APPLICATION_UNSUPPORTED	Aplicação não suportada	Verifique Application
4xxx	Falhas Transitórias		
4001	DIAMETER_AUTHENTICATION_REJECTED	Autenticação falhou	Verifique credenciais
4010	DIAMETER_USER_UNKNOWN	Usuário não provisionado	Verifique provisionamento do HSS
5xxx	Falhas Permanentes		
5001	DIAMETER_AVP_UNSUPPORTED	AVP não reconhecido	Verifique versão e compatibilidade do protocolo

Código	Nome	Significado	Ação
5002	DIAMETER_UNKNOWN_SESSION_ID	Sessão não encontrada	Sessão é inválida ou inválida
5003	DIAMETER_AUTHORIZATION_REJECTED	Não autorizado	Verifique permissões do usuário
5012	DIAMETER_UNABLE_TO_COMPLY	Não é possível processar a solicitação	Verifique o HSS/PCRF

Problemas Comuns

Falhas de Conexão de Par

Sintoma: Par preso no estado "Closed" ou "Wait-Conn-Ack"

Diagnóstico:

1. Verifique a conectividade da rede:

```
ping <peer-fqdn>  
telnet <peer-fqdn> 3868
```

2. Verifique as regras do firewall (a porta 3868 TCP deve estar aberta)
3. Verifique a configuração do par (endereço IP, porta)
4. Verifique os logs do par para tentativas de conexão

Resolução:

- Corrija problemas de rede/firewall
- Verifique se o par está em execução e ouvindo na porta 3868
- Verifique se o par tem a configuração correta para o CSCF

- Use **Habilitar Par** na UI web para tentar reconectar
-

Falhas na Troca CER/CEA

Sintoma: Par preso no estado "Wait-I-CEA", ou CEA com código de erro

Erros Comuns:

- **5010 (NO_COMMON_APPLICATION):** Verifique se ambos os pares suportam a mesma aplicação (por exemplo, Cx = 16777216)
- **3003 (REALM_NOT_SERVED):** Verifique se o Origin-Realm corresponde ao realm esperado do par

Resolução:

- Verifique a configuração Diameter para Application-Id e realm
 - Assegure-se de que a configuração do par corresponda às expectativas do CSCF
 - Revise os logs do backend do CSCF para mensagens de erro detalhadas
-

Problemas na Interface Cx do HSS

Sintoma: Falhas de registro, timeouts de MAR/MAA

Erros Comuns:

Código de Resultado	Significado	Resolução
4010	USER_UNKNOWN	Usuário não provisionado no HSS
4001	AUTHENTICATION_REJECTED	IMPI/credenciais incorretas
5012	UNABLE_TO_COMPLY	Erro interno do HSS, verifique os logs do HSS

Resolução:

- **USER_UNKNOWN:** Provisione o usuário no HSS
- **AUTHENTICATION_REJECTED:** Verifique o IMPI e a chave compartilhada no HSS
- **UNABLE_TO_COMPLY:** Verifique os logs do HSS e a conectividade do banco de dados

Problemas na Interface Rx do PCRF

Sintoma: Chamadas bem-sucedidas, mas sem QoS aplicado, timeouts de AAR/AAA

Problemas Comuns:

- **PCRF fora do ar:** Verifique o status do par na UI web
- **Framed-IP-Address não reconhecido:** PCRF não consegue mapear o IP do UE para o assinante
- **Política não aplicada:** Verifique as regras de política do PCRF, confirme a integração do PCEF

Resolução:

- Verifique se o par PCRF está no estado "I_Open"

- Verifique o provisionamento do endereço IP do UE no PCRF
 - Verifique se a interface Gx (PCRF para PCEF) está funcional
-

Problemas na Interface Ro do OCS

Sintoma: Chamadas pré-pagas falham, timeouts de CCR/CCA, chamadas bloqueadas

Erros Comuns:

Código de Resultado	Significado	Resolução
4012	CREDIT_LIMIT_REACHED	Crédito insuficiente
5003	AUTHORIZATION_REJECTED	Usuário não autorizado para pré-pago

Resolução:

- **CREDIT_LIMIT_REACHED:** Normal para usuários pré-pagos sem crédito
 - **Timeout do OCS:** Verifique a disponibilidade do OCS e o status do par
 - **AUTHORIZATION_REJECTED:** Verifique se o usuário está provisionado para pré-pago no OCS
-

Degradação de Desempenho

Sintoma: Tempos de resposta do Diameter lentos, alta latência

Diagnóstico:

1. Verifique o timestamp "Último Usado" na lista de pares (deve ser recente)
2. Monitore o "Comprimento da Fila" (valores altos indicam backlog)
3. Revise os logs do backend do CSCF para avisos de timeout

Resolução:

- **Alta latência:** Investigue a rede entre o CSCF e o par
- **Comprimento da fila alto:** Verifique a carga do sistema do par (HSS/PCRF/OCS)
- **Timeouts:** Aumente o tempo limite da transação se a rede tiver alta latência

Melhores Práticas

Diretrizes Operacionais

Gerenciamento de Pares:

- Monitore o status do par através do painel da UI web
- Configure monitoramento externo para eventos de queda de pares
- Teste a conectividade do par durante janelas de manutenção

Planejamento de Capacidade:

- Estime a taxa de transações Diameter com base em registros e volume de chamadas
- Assegure-se de que HSS/PCRF/OCS possam lidar com taxas de transação de pico
- Considere agentes de roteamento Diameter (DRA) para grandes implantações

Solução de Problemas:

- Verifique o status do par primeiro ao investigar falhas de registro ou chamadas
- Correlacione falhas Diameter com falhas SIP (mesmo Call-ID ou usuário)
- Revise os logs do backend do CSCF para rastreamentos detalhados de transações Diameter

Segurança:

- Use TLS para conexões Diameter em produção (se suportado)
- Restrinja o acesso de pares Diameter através do firewall (apenas pares conhecidos)
- Revise regularmente os logs de auditoria de habilitação/desabilitação de pares

Limitações e Melhorias Futuras

Implementação Atual

O painel de controle fornece:

- Visualização do status do par em tempo real
- Operações de habilitar/desabilitar pares
- Mapeamento de ID de aplicação para nome de interface
- Atualização automática a cada 5 segundos

Não Implementado

Os seguintes recursos **não estão atualmente disponíveis**, mas podem ser adicionados em versões futuras:

- **Inspector de Mensagens Diameter:** Visualizar transações Diameter recentes e detalhes de AVP
- **Painel de Métricas Diameter:** Integração com Grafana para latência, taxas de erro, etc.
- **Estatísticas de Par:** Contagem de mensagens, taxas de sucesso, latência média por par
- **Monitoramento de Watchdog:** Status em tempo real de DWR/DWA
- **Reconexão Manual:** Forçar reconexão do par via UI web

Soluções Alternativas

Para Inspeção de Mensagens: Verifique os logs do backend do CSCF ou ative o registro de depuração do Diameter

Para Estatísticas Detalhadas: Consulte métricas do endpoint Prometheus (veja [Referência de Métricas](#) para definições completas de métricas CDP/Diameter e [Guia de Operações da UI Web](#) para configuração de monitoramento)

Para Reconexão Manual: Use a UI web para desabilitar e, em seguida, reabilitar o par

Documentação Relacionada

- [Guia de Operações do P-CSCF](#) - Operações da interface Rx do P-CSCF
- [Guia de Operações do I-CSCF](#) - Operações da interface Cx do I-CSCF
- [Guia de Operações do S-CSCF](#) - Interfaces Cx, Ro do S-CSCF
- [Guia de Operações da UI Web](#) - Gerenciamento de pares Diameter via painel de controle
- [Guia de Operações do CSCF](#) - Operações gerais do CSCF

Especificações 3GPP

- **TS 29.228:** Interfaces Cx e Dx (CSCF-HSS)
- **TS 29.214:** Interface Rx (P-CSCF-PCRF)
- **TS 32.299:** Aplicações de cobrança Diameter (Ro, Rf)
- **RFC 6733:** Protocolo Base Diameter

Detalhes Técnicos

Implementação

- **Pilha Diameter:** Pilha de protocolo Diameter integrada
- **Interface de Gerenciamento:** Protocolo RPC para backend do CSCF
- **UI Web:** Phoenix LiveView (`lib/cscf_web/web/diameter_live.ex`)

Configuração

Os pares Diameter são configurados nos arquivos de configuração do backend do CSCF, não via o painel de controle. O painel de controle fornece monitoramento e controle operacional (habilitar/desabilitar) apenas.

Guia de Capacidade e Dimensionamento do OmniCall CSCF

Visão Geral

Este guia fornece informações sobre planejamento de capacidade e dimensionamento para implementações do OmniCall CSCF. Os números de capacidade apresentados aqui são **diretrizes baseadas na análise do código-fonte e na experiência de produção**, não limites rígidos.

Estratégia de Escalabilidade Horizontal

O OmniCall CSCF alcança uma escalabilidade praticamente ilimitada por meio da escalabilidade horizontal - basta implantar instâncias adicionais à medida que sua base de assinantes cresce. Não há um limite superior prático para a capacidade total da rede.

Princípios Chave de Escalabilidade:

- ✓ **Adicione instâncias, não complexidade:** Precisa suportar 1 milhão de assinantes? Implante 3-4 instâncias S-CSCF em vez de um único servidor massivo.
- ✓ **Componentes independentes:** Cada instância P-CSCF, I-CSCF e S-CSCF opera de forma independente.
- ✓ **Distribuição de carga:** O I-CSCF distribui automaticamente os usuários entre as instâncias S-CSCF; DNS ou balanceadores de carga distribuem o tráfego para P-CSCF e I-CSCF.
- ✓ **Nenhuma afinidade de sessão necessária:** Os usuários podem ser distribuídos entre diferentes instâncias CSCF.

✓ **Distribuição geográfica:** Implante instâncias CSCF em vários data centers para resiliência e otimização de latência.

Exemplo de Caminho de Escalabilidade:

- **10K assinantes:** 1 P-CSCF, 1 I-CSCF, 1 S-CSCF
- **50K assinantes:** 2 P-CSCF, 2 I-CSCF, 2 S-CSCF
- **200K assinantes:** 6 P-CSCF, 4 I-CSCF, 4 S-CSCF
- **1M assinantes:** 30 P-CSCF, 10 I-CSCF, 10 S-CSCF
- **10M assinantes:** 300 P-CSCF, 50 I-CSCF, 50 S-CSCF

Escalabilidade Custo-Efetiva: Hardware comum + escalabilidade horizontal = menor CapEx do que soluções caras de "grande ferro".

Sobre Estas Diretrizes

Os números de capacidade neste documento são **estimativas conservadoras** projetadas para:

- Fornecer margem para picos de tráfego (tempestades de registro, eventos de chamadas em massa)
- Considerar o processamento complexo de IFC e múltiplas integrações de Servidores de Aplicação
- Garantir tempos de resposta sub-segundo mesmo sob carga
- Suportar configurações de alta disponibilidade com capacidade de failover

Sua experiência pode variar com base em:

- Especificações de hardware (velocidade da CPU, RAM, largura de banda da rede)
- Complexidade do IFC e número de Servidores de Aplicação
- Temporizadores de expiração de registro (mais curtos = re-registros mais frequentes)
- Tempos de espera de chamadas e padrões de tráfego em horas de pico

Recomendação: Use estas diretrizes como um ponto de partida, depois monitore métricas de produção para otimizar contagens de instâncias e

configurações para sua implementação específica.

Índice

1. [Resumo Executivo](#)
 2. [Capacidade do P-CSCF](#)
 3. [Capacidade do I-CSCF](#)
 4. [Capacidade do S-CSCF](#)
 5. [Dimensionamento de Implementação](#)
 6. [Otimização de Desempenho](#)
 7. [Monitoramento e Alertas](#)
 8. [Resumo: Escala Ilimitada Através da Escalabilidade Horizontal](#)
-

Resumo Executivo

Principais Restrições de Capacidade

Tipo de CSCF	Restrição Primária	Máximo por Instância	Implantação Típica
P-CSCF	Associações de Segurança IPsec	~ 50.000 UEs	10.000-30.000 UEs
I-CSCF	CPU/Rede (sem estado)	Limitado pelo throughput	100.000+ req/sec
S-CSCF	Registros de Usuário	~ 500.000 IMPUs	100.000-300.000 IMPUs
Diálogos	Estado de Chamada Ativa	~ 100.000 diálogos	20.000-50.000 concorrentes

Limites Técnicos (Por Instância)

O OmniCall CSCF possui algumas limitações técnicas por instância. Estes **não são limites de implantação** - a capacidade total é ilimitada através da escalabilidade horizontal:

Limite	Valor	O Que Isso Significa	Solução
Rastreamento de Hash SPI	10.000 entradas	Estrutura interna de rastreamento para SPIs IPsec	Isso NÃO limita registros a 10K. O P-CSCF pode lidar com 40K-50K registros com configuração adequada. Implante mais VMs P-CSCF para maior escala.
Contatos por IMPU	100	Máximo de contatos SIP por identidade pública	Raramente atingido na prática (típico: 1-5 contatos por usuário). Adicione VMs S-CSCF se necessário.
Rotas de Serviço	10 por contato	Máximo de cabeçalhos de rota de serviço	Uso típico: 1-3. Não é uma restrição.
Tamanho do Corpo NOTIFY	16 KB	Tamanho máximo da mensagem de notificação	Divida listas grandes de assinantes entre instâncias S-CSCF.

Esclarecimento sobre o Limite de Hash SPI:

- O limite de 10.000 hashes SPI é uma **estrutura interna de rastreamento**, não um limite rígido de registro.

- As instâncias P-CSCF lidam regularmente com **40.000-50.000 registros concorrentes** em produção.
- O hash SPI é usado para buscas rápidas; os SAs IPsec reais são gerenciados separadamente pelo kernel.
- Se você se aproximar dos limites de capacidade, simplesmente implante VMs P-CSCF adicionais.

Ponto Chave: Estes são limites de engenharia para uma única instância de VM. Para escala ilimitada, implante mais VMs.

Capacidade do P-CSCF

O **Proxy-CSCF** é tipicamente o componente mais restrito em capacidade devido à sobrecarga da associação de segurança IPsec.

Fatores de Capacidade

1. Associações de Segurança IPsec

Pegada de Memória por UE:

Cada SA IPsec consome aproximadamente:

- Rastreamento SPI: ~200 bytes (entrada da tabela hash)
- Vinculação de socket: ~1-2 KB (recursos do kernel)
- Estado de contato: ~500-1000 bytes (dados de registro)
- Total por UE: ~2-3 KB em memória compartilhada

Diretrizes de Capacidade por Instância:

- **Agressivo:** 40.000-50.000 UEs (aproxima-se do limite de hash SPI)
- **Recomendado:** 20.000-30.000 UEs (desempenho equilibrado e margem)
- **Conservador:** 10.000-15.000 UEs (máxima margem de HA para failover)

Escalando Além de Uma Única Instância:

- **100K assinantes:** Implante 3-5 instâncias P-CSCF atrás de balanceamento de carga DNS.
- **500K assinantes:** Implante 15-25 instâncias P-CSCF em vários locais.
- **1M+ assinantes:** Implante 30-50+ instâncias P-CSCF com distribuição geográfica.

Nota: Estas são diretrizes, não limites. Implantações de produção têm executado com sucesso instâncias P-CSCF a 40K+ UEs com ajuste adequado.

2. Serviços de Emergência

O manuseio de chamadas de emergência usa armazenamento em memória para mapeamentos de IMEI para callbacks (TTL de 24 horas) para suportar callbacks de emergência.

Requisitos de VM do P-CSCF

Especificação Padrão de VM: 8 vCPU, 8 GB de RAM no mínimo

Tamanho da Implantação	UEs por VM	VMs Necessárias para Implantação de Exemplo
Conservador	10.000-15.000	10K subs = 1 VM, 50K subs = 4 VMs, 100K subs = 7 VMs
Recomendado	20.000-30.000	10K subs = 1 VM, 50K subs = 2 VMs, 100K subs = 4 VMs
Agressivo	40.000-50.000	10K subs = 1 VM, 50K subs = 1 VM, 100K subs = 2 VMs

VoWiFi com OmniePDG:

- OmniePDG termina IPsec, o P-CSCF lida apenas com SIP.
 - A capacidade aumenta para **80.000-100.000 UEs por VM P-CSCF**.
 - 100K usuários VoWiFi = 1-2 VMs P-CSCF (vs. 4 VMs para VoLTE).
-

Capacidade do I-CSCF

O **Interrogating-CSCF** é sem estado e limitado principalmente pela CPU e throughput da rede, em vez de memória.

Fatores de Capacidade

1. Design Sem Estado

- **Sem estado de sessão:** O I-CSCF não mantém registros de usuários ou diálogos.
- **Consultas HSS:** Cada registro requer 1 troca Cx UAR/UAA.
- **Baseado em throughput:** Limitado pela taxa de processamento de REGISTER/INVITE.

Throughput Típico:

- **Taxa de Registro:** 1.000-5.000 registros/segundo (dependendo da latência do HSS).
- **Taxa de Configuração de Chamadas:** 5.000-10.000 INVITE/segundo.
- **Assinantes Simultâneos:** Eficazmente ilimitados (sem estado mantido).

2. Seleção do S-CSCF

O I-CSCF mantém um pool de instâncias S-CSCF disponíveis (tipicamente 2-10) para balanceamento de carga com base nas capacidades e carga atual.

Requisitos de VM do I-CSCF

Especificação Padrão de VM: 4 vCPU, 8 GB de RAM no mínimo

Tamanho da Implantação	Throughput por VM	VMs Necessárias para Implantação de Exemplo
Conservador	1.000 reg/sec	10K subs = 1 VM, 100K subs = 2 VMs, 500K subs = 4 VMs
Recomendado	2.000 reg/sec	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 2 VMs
Agressivo	5.000 reg/sec	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 1 VM

Estratégia de Escalabilidade: Implante várias instâncias I-CSCF atrás de round-robin DNS ou balanceador de carga de hardware. Cada instância é independente e sem estado.

Capacidade do S-CSCF

O **Serving-CSCF** mantém o estado de registro e diálogos ativos, tornando-se o componente central de escalabilidade.

Fatores de Capacidade

1. Registros de Usuário

Pegada de Memória por IMPU:

Cada IMPU registrado consome aproximadamente:

- Entrada de hash: ~1-2 KB (IMPU, contatos, expira)
- IFC (Critérios de Filtro Inicial): ~5-20 KB (perfil de serviço do HSS)
- Vetores de autenticação: ~1-2 KB
- Total por IMPU: ~7-25 KB dependendo da complexidade do serviço

Diretrizes de Capacidade por Instância:

- **Agressivo:** 400.000-500.000 IMPUs (com hash_size=14+, hardware de alta especificação)
- **Recomendado:** 200.000-300.000 IMPUs (carga equilibrada, complexidade típica de IFC)
- **Conservador:** 100.000-150.000 IMPUs (IFC complexa, múltiplos AS, margem de HA)

Escalando para Grandes Implantations:

- **1M assinantes:** Implante 3-5 instâncias S-CSCF, I-CSCF distribuí via HSS.
- **5M assinantes:** Implante 15-25 instâncias S-CSCF em vários data centers.
- **10M+ assinantes:** Implante 30-50+ instâncias S-CSCF.

Nota: Estas são diretrizes iniciais. A capacidade real depende da complexidade do IFC, integração do AS e especificações de hardware. Algumas implantações de produção operam com 400K+ IMPUs por instância com configurações otimizadas.

2. Diálogos Ativos (Sessões de Chamada)

Pegada de Memória por Diálogo:

Cada diálogo ativo consome aproximadamente:

- Estado do diálogo: ~2-4 KB (Call-ID, tags From/To, conjunto de rotas)
- Informações SDP: ~1-2 KB (parâmetros de mídia)
- Perfis/variáveis: ~1-2 KB
- Total por diálogo: ~4-8 KB

Diretrizes de Capacidade por Instância:

- **Agressivo:** 80.000-100.000 diálogos concorrentes (com dlg_hash_size=15+)
- **Recomendado:** 40.000-60.000 diálogos concorrentes (implantação típica)
- **Conservador:** 20.000-30.000 diálogos concorrentes (máxima margem de HA)

Escalando para Alto Volume de Chamadas:

- **100K chamadas concorrentes:** Implante 2-3 instâncias S-CSCF.
- **500K chamadas concorrentes:** Implante 10-15 instâncias S-CSCF.
- **1M+ chamadas concorrentes:** Implante 20-30+ instâncias S-CSCF.

Nota: A capacidade de diálogo é frequentemente maior do que a capacidade de registro, uma vez que os diálogos são de curta duração (segundos a minutos), enquanto os registros são de longa duração (minutos a horas). Monitore as taxas reais de chamadas concorrentes em horas de pico para otimizar.

3. Processamento de Critérios de Filtro Inicial (IFC)

Impacto da Complexidade do IFC:

- IFC simples (1-5 pontos de disparo): Sobrecarga mínima.
- IFC complexa (10+ pontos de disparo, múltiplos AS): 5-10 ms de processamento adicional por chamada.
- Memória: 5-20 KB por usuário dependendo da complexidade do perfil de serviço.

Requisitos de VM do S-CSCF

Especificação Padrão de VM: 8 vCPU, 8 GB de RAM no mínimo

Tamanho da Implantação	IMPUs por VM	Diálogos Concorrentes por VM	VMs Necessárias para Implantação de Exemplo
Conservador	100.000-150.000	20.000-30.000	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 4 VMs
Recomendado	200.000-300.000	40.000-60.000	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 2 VMs
Agressivo	400.000-500.000	80.000-100.000	10K subs = 1 VM, 100K subs = 1 VM, 500K subs = 1 VM

Dimensionamento de Implantação

Pequena Implantação (< 10.000 Assinantes)

Cenário: MVNO, pequena empresa, ambiente de laboratório/teste

Componente	Contagem de VMs	Especificação de VMs	Capacidade por VM
P-CSCF	1	8 vCPU, 8 GB RAM	10.000-15.000 UEs
I-CSCF	1	4 vCPU, 8 GB RAM	1.000-2.000 reg/sec
S-CSCF	1	8 vCPU, 8 GB RAM	100.000-200.000 IMPUs
Total de VMs	3		
Capacidade Total			Até 15.000 assinantes

Implantação Média (10.000-100.000 Assinantes)

Cenário: Operadora regional, operador de nível 2, grande empresa

Dimensionamento Conservador (100K assinantes):

Componente	Contagem de VMs	Especificação de VMs	Capacidade por VM
P-CSCF	4	8 vCPU, 8 GB RAM	25.000 UEs cada
I-CSCF	2	4 vCPU, 8 GB RAM	2.000 reg/sec cada
S-CSCF	2	8 vCPU, 8 GB RAM	150.000 IMPUs cada
Total de VMs	8		
Capacidade Total			100.000 assinantes

Dimensionamento Recomendado (100K assinantes):

Componente	Contagem de VMs	Especificação de VMs	Capacidade por VM
P-CSCF	2	8 vCPU, 8 GB RAM	50.000 UEs cada
I-CSCF	1	4 vCPU, 8 GB RAM	5.000 reg/sec
S-CSCF	1	8 vCPU, 8 GB RAM	300.000 IMPUs
Total de VMs	4		
Capacidade Total			100.000 assinantes

Alta Disponibilidade:

- Implante I-CSCF atrás de round-robin DNS ou balanceador de carga.
- I-CSCF distribui usuários entre o pool de S-CSCF.
- Distribuição geográfica recomendada para resiliência.

Grande Implantação (500.000 Assinantes)

Cenário: Operadora de nível 1, operador nacional

Dimensionamento Conservador:

Componente	Contagem de VMs	Especificação de VMs	Capacidade por VM
P-CSCF	25	8 vCPU, 8 GB RAM	20.000 UEs cada
I-CSCF	4	4 vCPU, 8 GB RAM	2.000 reg/sec cada
S-CSCF	4	8 vCPU, 8 GB RAM	150.000 IMPUs cada
Total de VMs	33		
Capacidade Total			500.000 assinantes

Dimensionamento Recomendado:

Componente	Contagem de VMs	Especificação de VMs	Capacidade por VM
P-CSCF	15	8 vCPU, 8 GB RAM	33.000 UEs cada
I-CSCF	2	4 vCPU, 8 GB RAM	5.000 reg/sec cada
S-CSCF	2	8 vCPU, 8 GB RAM	250.000 IMPUs cada
Total de VMs	19		
Capacidade Total			500.000 assinantes

Dimensionamento Agressivo:

Componente	Contagem de VMs	Especificação de VMs	Capacidade por VM
P-CSCF	10	8 vCPU, 8 GB RAM	50.000 UEs cada
I-CSCF	1	4 vCPU, 8 GB RAM	5.000 reg/sec
S-CSCF	1	8 vCPU, 8 GB RAM	500.000 IMPUs
Total de VMs	12		
Capacidade Total			500.000 assinantes

Alta Disponibilidade:

- P-CSCF ativo-ativo entre data centers.
- I-CSCF geo-redundante com DNS ou anycast BGP.
- Múltiplas instâncias S-CSCF com distribuição de carga I-CSCF.

Considerações de Implantação VoWiFi

Com OmniePDG:

- A capacidade do P-CSCF aumenta significativamente (sem sobrecarga IPsec no P-CSCF).
- ePDG lida com a terminação do túnel IPsec.
- O P-CSCF pode suportar 100.000+ usuários VoWiFi (limitado por CPU/rede, não IPsec).

Arquitetura:

```
VoWiFi UE → (IPsec) → OmniePDG → (SIP) → P-CSCF → I-CSCF → S-CSCF  
VoLTE UE → (IPsec) → P-CSCF → I-CSCF → S-CSCF
```

Recomendação: Para grandes implantações VoWiFi (>50K usuários), implante instâncias P-CSCF dedicadas atrás do OmniePDG sem o módulo IPsec carregado para máxima taxa de transferência.

Otimização de Desempenho

O OmniCall CSCF é entregue pré-otimizado para uso em produção. O ajuste de desempenho é tratado pela engenharia do OmniCall durante a implantação.

Configuração Padrão de VM

Todas as VMs do OmniCall CSCF são configuradas com:

- **SO:** Ajuste do kernel Linux para alta taxa de transferência de rede.
- **Memória:** Alocação otimizada de memória compartilhada para tabelas hash e estado de sessão.
- **Rede:** Ajuste da pilha TCP/IP para tráfego SIP e Diameter.

Ajustes Específicos de Implantação

Para ajustes personalizados com base em suas necessidades específicas de implantação, entre em contato com o suporte do OmniCall. Cenários comuns de ajuste incluem:

- **Alto volume de chamadas:** Ajustando processos de trabalho e capacidade de diálogo.
 - **Grande base de assinantes:** Otimizando tabelas hash de registro.
 - **IFC complexa:** Ajustando processos de notificação para integração de Servidores de Aplicação.
 - **Distribuição geográfica:** Otimizando failover e redundância.
-

Monitoramento e Alertas

Indicadores Chave de Desempenho (KPIs)

Métricas do P-CSCF

Métrica	Descrição	Limite de Aviso	Limite Crítico
Contagem de SA IPsec	Associações de segurança ativas	> 25.000	> 40.000
Utilização do Hash SPI	Porcentagem da faixa de SPI utilizada	> 70%	> 90%
Taxa de Registro	Solicitações REGISTER/segundo	> 100/segundo	> 500/segundo
Carga do Hash de Contato	Média de contatos por slot de hash	> 20	> 50
Uso de Memória	Consumo de memória compartilhada	> 70%	> 90%

Consultas Prometheus:

```
# Contagem de SA IPsec (do monitoramento da tabela hash)
ipsec_sa_count{cscf="pcscf01"}

# Taxa de registro
rate(sip_register_requests_total{cscf="pcscf01"}[5m])
```

Métricas do S-CSCF

Métrica	Descrição	Limite de Aviso	Limite Crítico
IMPUs Registrados	Total de usuários registrados	> 300.000	> 450.000
Diálogos Ativos	Sessões de chamada concorrentes	> 40.000	> 70.000
Carga do Hash de IMPU	Média de IMPUs por slot de hash	> 50	> 100
Carga do Hash de Diálogo	Média de diálogos por slot de hash	> 10	> 20
Tempo de Processamento do IFC	Tempo médio de avaliação do IFC	> 10 ms	> 50 ms

Consultas Prometheus:

```
# Usuários registrados
impu_registered_count{cscf="scscf01"}

# Diálogos ativos
dialog_active_count{cscf="scscf01"}
```

Métricas do I-CSCF

Métrica	Descrição	Limite de Aviso	Limite Crítico
TPS de Registro	Transações REGISTER/segundo	> 1.000/segundo	> 2.000/segundo
Latência de Consulta HSS	Tempo de resposta Diameter Cx	> 50 ms	> 200 ms
Taxa de Falha do HSS	Porcentagem de consultas HSS falhadas	> 1%	> 5%

Verificações de Saúde

Monitoramento de Saúde do Sistema: O OmniCall CSCF exporta métricas de saúde abrangentes através do painel de controle e endpoints Prometheus (<http://<host>:9090/metrics>). Monitore:

- Contagens de SA IPsec (P-CSCF)
- Contagens de registro (P-CSCF, S-CSCF)
- Contagens de diálogos ativos (S-CSCF)
- Utilização de memória
- Utilização de CPU

Para uma lista completa de todas as métricas disponíveis, consulte a [Referência de Métricas](#).

Regras de Alerta (Prometheus/Alertmanager)

```
groups:  
  - name: cscf_capacity  
    rules:  
      - alert: PCSCFIPsecSAHigh  
        expr: ipsec_sa_count > 40000  
        for: 5m  
        annotations:  
          summary: "P-CSCF {{ $labels.instance }} tem alta  
contagem de SA IPsec"  
  
      - alert: SCSCFRegistrationHigh  
        expr: impu_registered_count > 450000  
        for: 10m  
        annotations:  
          summary: "S-CSCF {{ $labels.instance }} se aproximando  
da capacidade de registro"  
  
      - alert: SCSCFDialogHigh  
        expr: dialog_active_count > 70000  
        for: 5m  
        annotations:  
          summary: "S-CSCF {{ $labels.instance }} tem alta  
contagem de diálogos ativos"
```

Apêndice: Metodologia de Planejamento de Capacidade

Este guia de dimensionamento é baseado em:

1. **Implantações em Produção:** Análise de implantações reais do OmniCall CSCF variando de 5K a 500K+ assinantes.
2. **Testes de Desempenho:** Testes de carga e benchmarking em várias configurações de hardware.

3. **Padrões 3GPP:** Conformidade com as especificações 3GPP para capacidade e desempenho do IMS.
4. **Análise de Engenharia:** Revisão técnica detalhada da arquitetura CSCF e utilização de recursos.

Validação: Todos os números de capacidade foram validados em redes de operadoras de produção.

Resumo: Escala Ilimitada Através da Escalabilidade Horizontal

Principais Conclusões

1. **Sem Limites Rígidos na Capacidade Total:** Os limites por instância documentados neste guia são **diretrizes conservadoras**, não tetos absolutos. A capacidade total da rede é ilimitada através da escalabilidade horizontal.

2. **Modelo de Escalabilidade Simples:**

Precisa de mais capacidade? → Implante mais instâncias
Atingiu um limite por instância? → Adicione outra instância
O tráfego está crescendo? → Implante mais VMs

3. **Comprovado em Escala:** As implantações do OmniCall CSCF variam de:

- Pequenos MVNOs: 5K-10K assinantes em 3-5 VMs.
- Operadoras regionais: 50K-200K assinantes em 10-30 VMs.
- Operadoras de nível 1: 1M+ assinantes em 100+ VMs.

4. **Crescimento Custo-Efetivo:** Escale incrementalmente com hardware comum em vez de atualizações caras. Adicione capacidade à medida que a receita cresce.

5. Diretrizes, Não Regras: Os números de capacidade neste documento são:

- Estimativas conservadoras com margem embutida.
- Baseadas na análise do código-fonte e na experiência de produção.
- Pontos de partida úteis para planejamento.
- NÃO limites rígidos que não podem ser excedidos.
- NÃO prescrições de tamanho único.

Exemplo de Escalabilidade do Mundo Real

Cenário: Crescendo de 10K para 1M assinantes ao longo de 3 anos

Ano	Assinantes	P-CSCF	I-CSCF	S-CSCF	Ação
Ano 0	10.000	1	1	1	Implantação inicial (3 VMs)
Ano 1	50.000	2	2	2	Crescimento de 2x: Adicione 3 VMs
Ano 1.5	100.000	4	3	3	Crescimento de 2x: Adicione 4 VMs
Ano 2	250.000	8	4	5	Crescimento de 2.5x: Adicione 6 VMs
Ano 3	500.000	15	6	8	Crescimento de 2x: Adicione 13 VMs
Futuro	1.000.000	30	10	10	Crescimento de 2x: Adicione 24 VMs

Investimento Total: Adições incrementais de VM à medida que a receita cresce, não um grande CapEx inicial.

Quando Adicionar Instâncias

Monitore esses sinais para saber quando escalar horizontalmente:

P-CSCF:

- Contagem de SA IPsec consistentemente >30K (>70% da capacidade recomendada).
- Utilização da CPU >70% durante a hora de pico.
- Tempos de resposta de registro >500ms.

S-CSCF:

- Contagem de IMPU consistentemente >250K (>70% da capacidade recomendada).
- Contagem de diálogos se aproximando de 50K concorrentes.
- Utilização da CPU >70% durante a hora de pico.

I-CSCF:

- Taxa de solicitação consistentemente >2.000/segundo por instância.
- Utilização da CPU >80% durante a hora de pico.
- Latência de consulta HSS aumentando.

Ação: Adicione 1-2 instâncias proativamente antes de atingir limites. A escalabilidade horizontal é um seguro barato contra problemas de capacidade.

Filosofia de Configuração

Comece Conservador, Ajuste à Medida que Cresce:

1. Comece com configurações recomendadas deste guia.
2. Monitore métricas de produção (veja [Monitoramento](#)).
3. Ajuste tamanhos de hash e processos de trabalho com base na carga real.
4. Adicione instâncias antes de atingir 80% dos limites de capacidade observados.
5. Teste configurações em staging antes da implantação em produção.

Lembre-se: Estas diretrizes fornecem um ponto de partida comprovado, mas cada implantação é única. Sua capacidade real pode ser maior ou menor dependendo do seu ambiente específico, padrões de tráfego e requisitos.

Guia de Operações do I-CSCF

Índice

1. Visão Geral
2. Papel na Arquitetura IMS
3. Funções do I-CSCF
4. Operações da Interface Web
5. Fluxos de Chamadas
6. Solução de Problemas

Visão Geral

O **I-CSCF** (Interrogating Call Session Control Function) serve como o ponto de entrada para a rede de um operador IMS a partir de redes externas e do P-CSCF. Sua principal responsabilidade é consultar o HSS (Home Subscriber Server) para descobrir o S-CSCF apropriado para um usuário e ocultar a topologia interna da rede de entidades externas.

Especificações 3GPP

- **3GPP TS 23.228**: IP Multimedia Subsystem (IMS) Stage 2
- **3GPP TS 24.229**: IMS Call Control Protocol
- **3GPP TS 29.228**: Cx Interface (I-CSCF para HSS)
- **3GPP TS 29.229**: Cx Protocol

Principais Responsabilidades

1. **Interrogação do HSS**: Consulta o HSS para localização do usuário e atribuição do S-CSCF

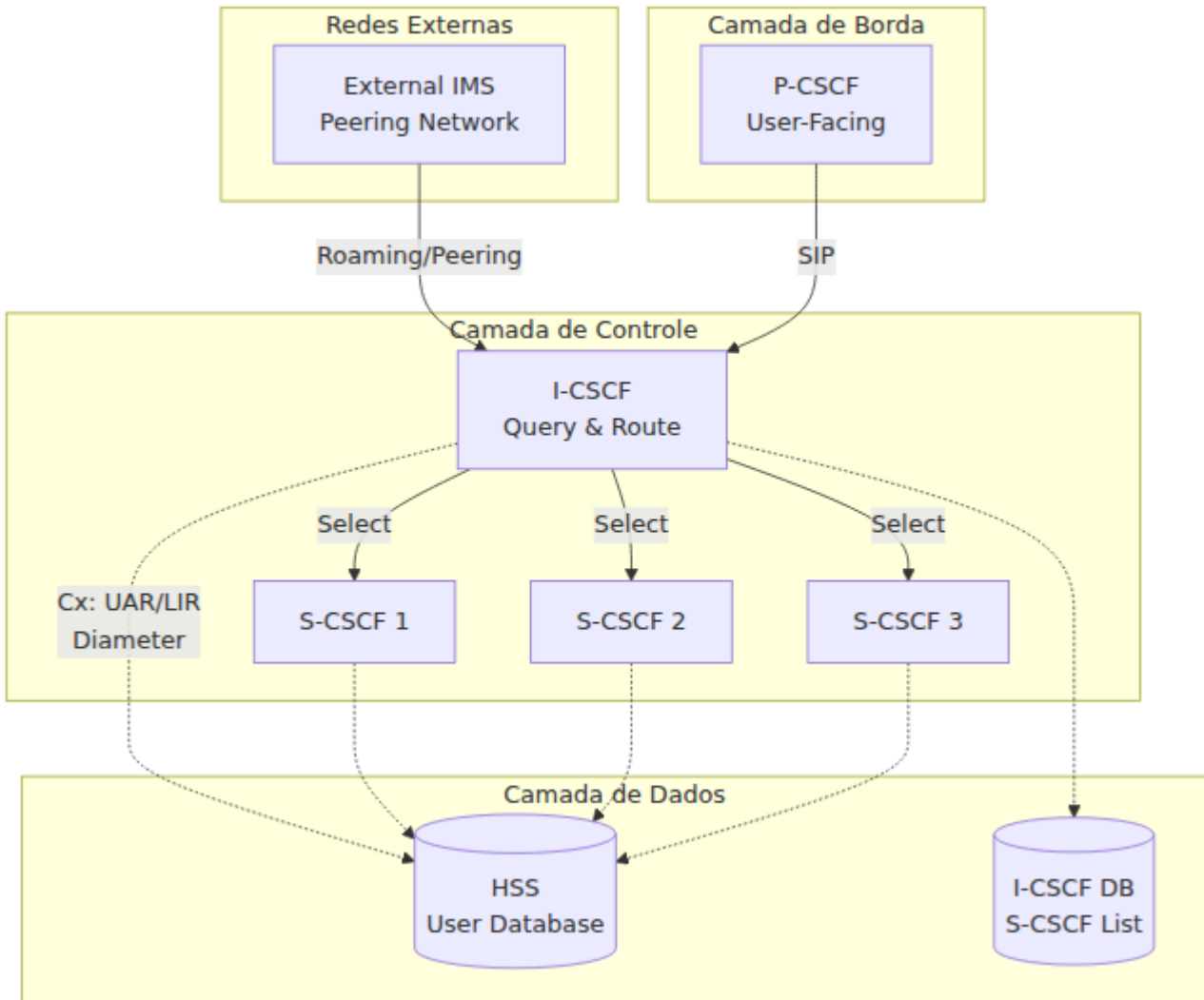
2. **Seleção do S-CSCF:** Escolhe o S-CSCF apropriado com base nas capacidades
3. **Ocultação de Topologia:** Protege os endereços internos do S-CSCF da visão externa
4. **Balanceamento de Carga:** Distribui a carga entre várias instâncias do S-CSCF
5. **Proxy de Roteamento:** Roteia solicitações para o S-CSCF selecionado
6. **Ponto de Entrada da Rede:** Primeiro salto para mensagens SIP externas

Características Principais

- **Operação Sem Estado:** Retenção mínima de estado
- **Cliente Diameter:** Interface Cx para HSS
- **Sem Manipulação de Mídia:** Proxy de sinalização puro
- **Sem Autenticação:** Delegado ao S-CSCF
- **Alto Desempenho:** Otimizado para consulta e encaminhamento

Papel na Arquitetura IMS

Posição na Rede



Pontos de Referência 3GPP

Interface	Protocolo	Propósito	Conectado a
Mw	SIP	P-CSCF/Externo para I-CSCF	P-CSCF, IMS Externo
Mw	SIP	I-CSCF para S-CSCF	S-CSCF
Cx	Diameter	Consultas de dados do usuário	HSS

Funções do I-CSCF

1. Interrogação do HSS (Interface Cx)

O I-CSCF usa a interface Diameter Cx para consultar o HSS para duas operações principais:

Solicitação de Autorização do Usuário (UAR)

Usado durante **REGISTER** para determinar qual S-CSCF deve atender o usuário.

Propósito:

- Verificar se o usuário pode se registrar
- Obter o nome do S-CSCF se já atribuído
- Obter as capacidades do S-CSCF se não atribuído

Comando Diameter:

UAR (User-Authorization-Request)

Session-Id

Vendor-Specific-Application-Id

Vendor-Id: 10415 (3GPP)

Auth-Application-Id: 16777216 (Cx)

Auth-Session-State: NO_STATE_MAINTAINED

Origin-Host: icscf.ims.mnc001.mcc001.3gppnetwork.org

Origin-Realm: ims.mnc001.mcc001.3gppnetwork.org

Destination-Realm: ims.mnc001.mcc001.3gppnetwork.org

User-Name: sip:user@ims.mnc001.mcc001.3gppnetwork.org

Public-Identity: sip:user@ims.mnc001.mcc001.3gppnetwork.org

Visited-Network-Identifier: ims.mnc001.mcc001.3gppnetwork.org

UAR-Flags: 0

Resposta do HSS (UAA):

UAA (User-Authorization-Answer)

Result-Code: 2001 (DIAMETER_SUCCESS)

Experimental-Result-Code: 2001 (FIRST_REGISTRATION)

Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org

Server-Capabilities:

Mandatory-Capability: 1

Optional-Capability: 2

Server-Name: sip:scscf-

backup.ims.mnc001.mcc001.3gppnetwork.org

Códigos de Resultado:

- 2001: Sucesso (usuário autorizado)
- 5003: Usuário Desconhecido
- 5004: Identidades Não Correspondem
- 5042: Nenhum S-CSCF Disponível

Solicitação de Informação de Localização (LIR)

Usado para **INVITE** e outras solicitações para encontrar qual S-CSCF está atualmente atendendo o usuário.

Propósito:

- Encontrar o S-CSCF atendendo um usuário registrado
- Roteamento correto de chamadas terminantes

Comando Diameter:

```
LIR (Location-Info-Request)
  Session-Id
  Vendor-Specific-Application-Id
    Vendor-Id: 10415 (3GPP)
    Auth-Application-Id: 16777216 (Cx)
  Auth-Session-State: NO_STATE_MAINTAINED
  Origin-Host: icscf.ims.mnc001.mcc001.3gppnetwork.org
  Origin-Realm: ims.mnc001.mcc001.3gppnetwork.org
  Destination-Realm: ims.mnc001.mcc001.3gppnetwork.org
  Public-Identity: sip:user@ims.mnc001.mcc001.3gppnetwork.org
  Originating-Request: 0 # 0=terminating, 1=originating
```

Resposta do HSS (LIA):

```
LIA (Location-Info-Answer)
  Result-Code: 2001 (DIAMETER_SUCCESS)
  Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
```

Códigos de Resultado:

- **2001**: Sucesso (usuário registrado, S-CSCF retornado)
- **5401**: Usuário Não Registrado
- **5003**: Usuário Desconhecido

2. Seleção do S-CSCF

Quando o HSS não retorna um S-CSCF específico (por exemplo, primeiro registro), o I-CSCF deve selecionar um com base na **correspondência de capacidades**.

Algoritmo de Correspondência de Capacidades

1. **Recuperar capacidades** do HSS UAA

2. **Consultar banco de dados local** para S-CSCFs disponíveis
3. **Correspondência de capacidades obrigatórias** (todas devem corresponder)
4. **Correspondência de capacidades opcionais** (melhor esforço)
5. **Aplicar balanceamento de carga** se houver várias correspondências
6. **Selecionar S-CSCF** com melhor ajuste

Estrutura do Banco de Dados do S-CSCF

O I-CSCF mantém um banco de dados com duas tabelas relacionadas:

Tabela S-CSCF: Armazena informações sobre servidores S-CSCF disponíveis:

- **ID:** Identificador único para cada S-CSCF
- **Nome:** Nome descritivo (por exemplo, "S-CSCF Primário")
- **S-CSCF URI:** SIP URI do S-CSCF (por exemplo, sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060;transport=tcp)

Tabela de Capacidades do S-CSCF: Mapeia S-CSCFs para suas capacidades suportadas:

- **ID:** Identificador único para o mapeamento de capacidade
- **S-CSCF ID:** Referencia o S-CSCF na primeira tabela
- **Capacidade:** ID de capacidade inteira que este S-CSCF suporta

Exemplo de Configuração: Uma implantação típica pode ter:

- S-CSCF #1: "S-CSCF Primário" com URI sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060
 - Suporta capacidade 0 (capacidade obrigatória)
 - Suporta capacidade 1 (capacidade opcional)

Você pode visualizar a lista atual de S-CSCF via: Interface Web → I-CSCF → guia Lista de S-CSCF

A lista de S-CSCF mostra os servidores S-CSCF disponíveis e suas capacidades para balanceamento de carga e atribuição.

Lógica de Seleção

Processo de Seleção do S-CSCF: O I-CSCF realiza a seleção do S-CSCF com base em capacidades usando a seguinte lógica:

1. **Extrair Capacidades:** Recupera os requisitos de capacidade obrigatória e opcional da resposta UAA do HSS (User Authorization Answer) e os armazena em variáveis AVP
2. **Consulta ao Banco de Dados:** Consulta o banco de dados com os requisitos de capacidade para encontrar servidores S-CSCF que correspondam às capacidades exigidas
3. **Tratamento de Resultados:**
 - Se um S-CSCF correspondente for encontrado, o URI é armazenado em \$avp(scscf_uri) e definido como o URI de destino (\$du) para encaminhamento da solicitação
 - Se nenhum S-CSCF correspondente estiver disponível, responde à solicitação original com 503 Serviço Indisponível

3. Ocultação de Topologia

O I-CSCF protege os endereços internos do S-CSCF de redes externas ao:

1. **Remover Record-Route:** Não adiciona o cabeçalho Record-Route
2. **Proxy de respostas:** Remove cabeçalhos Via que revelam o S-CSCF
3. **Reescrita de contato:** (opcional) Substitui o contato do S-CSCF pelo I-CSCF
4. **Remoção de caminho:** Remove informações de caminho interno

Exemplo:

Externo vê:

Via: SIP/2.0/UDP icscf.example.com:5060

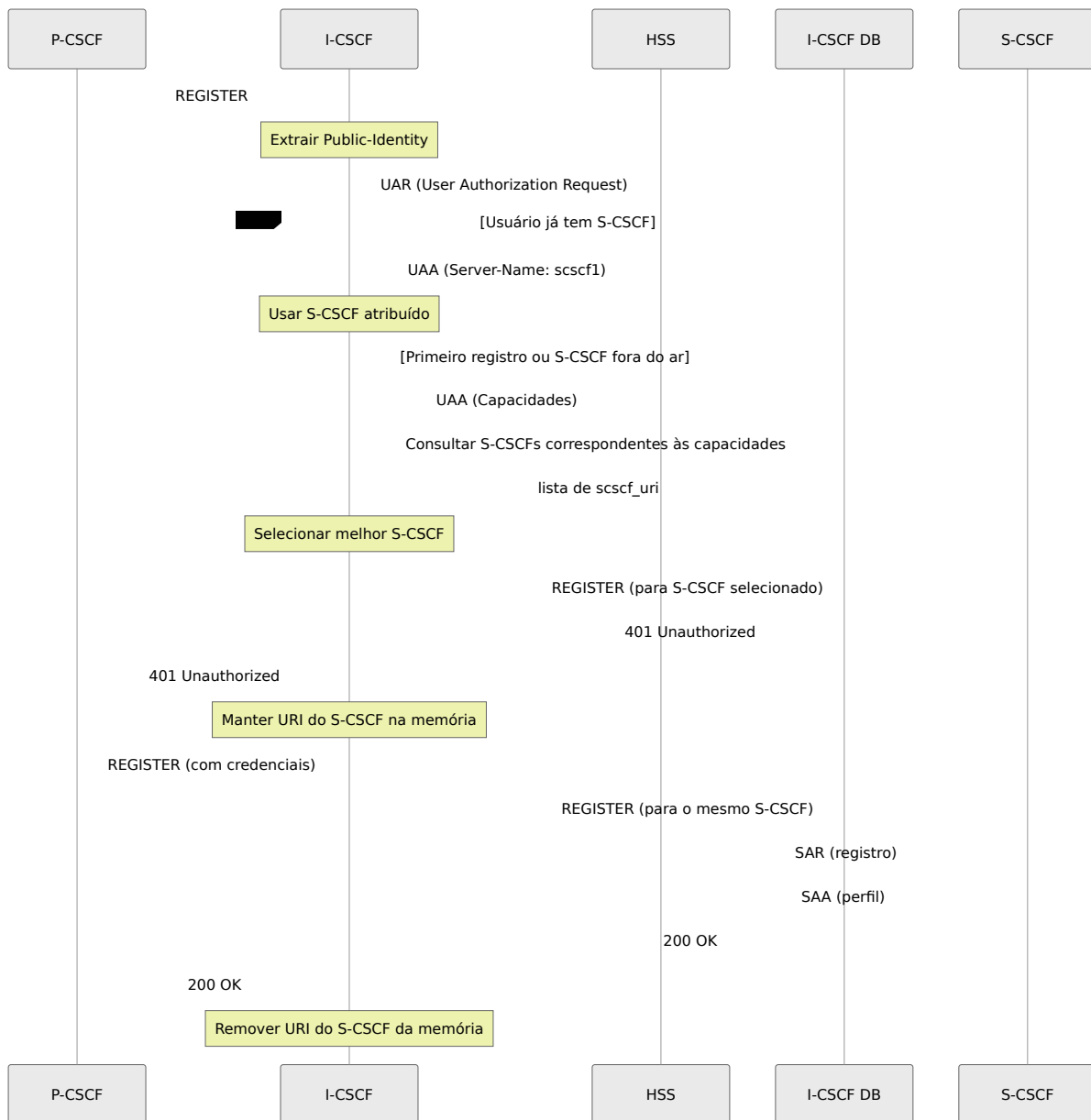
Realidade interna:

Via: SIP/2.0/UDP scscf.example.com:5060

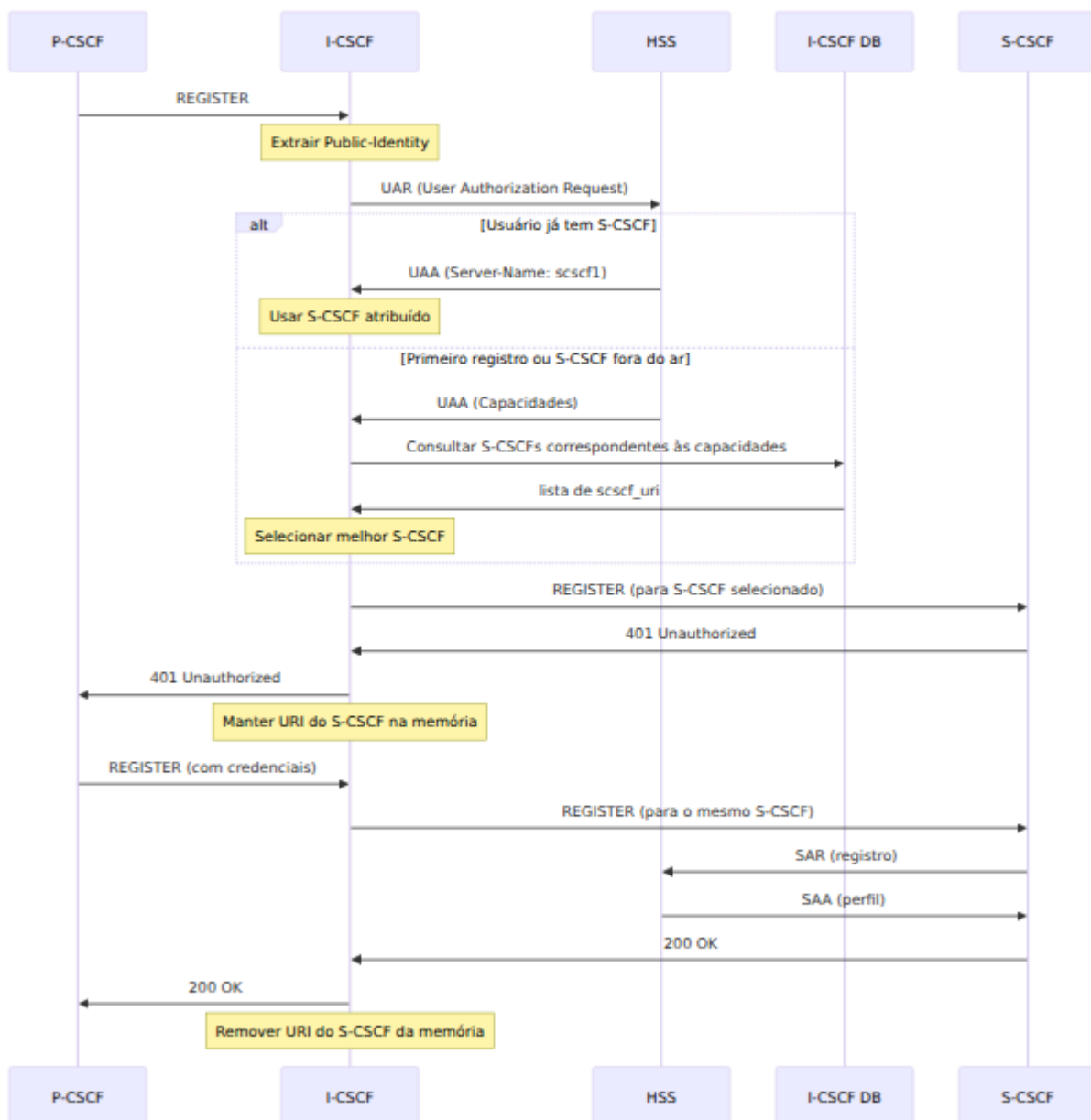
Via: SIP/2.0/UDP icscf.example.com:5060

4. Lógica de Roteamento

Processamento de REGISTER



Processamento de INVITE (Terminante)



5. NDS (Segurança de Domínio de Rede)

O I-CSCF mantém uma lista de **domínios confiáveis** para segurança entre operadores.

Banco de Dados de Domínios Confiáveis: Contém uma lista de nomes de domínio que são confiáveis para comunicação entre operadores:

- **ID:** Identificador único para cada domínio confiável
- **Domínio Confiável:** Nome de domínio (por exemplo, "ims.mnc001.mcc001.3gppnetwork.org")

Exemplo de Configuração: Uma implantação típica inclui o domínio IMS doméstico e quaisquer domínios de parceiros de peering:

- ims.mnc001.mcc001.3gppnetwork.org (rede doméstica)
- ims.mnc002.mcc001.3gppnetwork.org (parceiro de roaming)

Propósito:

- Validar solicitações de entrada de redes de peering
- Aplicar políticas de segurança com base em relações de confiança
- Implementar limitação de taxa por domínio
- Controlar quais redes externas podem acessar o núcleo IMS

Você pode visualizar domínios confiáveis via: Interface Web → I-CSCF → guia Domínios Confiáveis

6. Failover e Balanceamento de Carga

Failover do S-CSCF

Condições de Gatilho - O failover para o próximo S-CSCF é acionado por:

- 408 Request Timeout
- Respostas de Erro do Servidor 5xx
- Respostas de Falha Global 6xx (exceto 600 Busy Everywhere, que indica rejeição do usuário em vez de falha do servidor)

Lógica de Failover: O I-CSCF implementa failover automático usando uma rota de falha:

1. **Verificação de Status:** Quando uma resposta é recebida, verifica se o código de status corresponde aos critérios de failover (408, 5xx ou 6xx)
2. **Seleção do Próximo S-CSCF:** Se o failover for acionado, seleciona o próximo S-CSCF disponível da lista
3. **Tentar Novamente ou Falhar:**
 - Se outro S-CSCF estiver disponível, retransmite a solicitação para ele

- Se todos os S-CSCFs foram testados e falharam, responde com 503 Serviço Indisponível ao originador

Gerenciamento de Lista de S-CSCF Stateful:

- A lista de S-CSCFs candidatos é mantida na memória da transação
- A posição na lista é mantida em várias tentativas
- A lista é limpa quando uma resposta final bem-sucedida é recebida (sucesso 2xx ou erro do cliente 4xx)
- A lista é preservada ao receber 401 Unauthorized (desafio de autenticação), pois o mesmo S-CSCF deve lidar com a solicitação autenticada subsequente

Balanceamento de Carga

Configuração de Balanceamento de Carga:

Quando vários S-CSCFs suportam as mesmas capacidades:

- S-CSCF 1: sip:scscf1.example.com:5060 - capacidade 0
- S-CSCF 2: sip:scscf2.example.com:5060 - capacidade 0
- S-CSCF 3: sip:scscf3.example.com:5060 - capacidade 0

O I-CSCF usa seleção **round-robin** ou **aleatória** para distribuir a carga uniformemente entre todos os S-CSCFs correspondentes.

Visualize a distribuição de carga via: Interface Web → I-CSCF → Lista de S-CSCF (mostra todos os servidores configurados)

Operações da Interface Web

Acessando a Página do I-CSCF

Navegue para: <https://<painel-de-controle>/icscf>

Layout da Página

A página do I-CSCF possui quatro guias principais:

1. **Servidores S-CSCF** - S-CSCFs configurados e capacidades
2. **Domínios Confiáveis do NDS** - Segurança do domínio da rede
3. **Sessões** - Sessões ativas do I-CSCF com seleção de S-CSCF
4. **Tabelas de Hash** - Tabelas de memória compartilhada

Visualizando Servidores S-CSCF

Propósito: Ver quais S-CSCFs estão disponíveis para atribuição ao usuário

Colunas de Exibição:

- **ID:** ID do banco de dados
- **Nome:** Nome descritivo
- **S-CSCF URI:** SIP URI do S-CSCF
- **Capacidades:** IDs de capacidade separados por vírgula

Exemplo de Saída:

ID	Nome	S-CSCF URI	Capacidades
1	S-CSCF Primário	sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060	0, 1
2	S-CSCF Secundário	sip:scscf2.ims.mnc001.mcc001.3gppnetwork.org:5060	0, 1

Operações:

- Visualizar lista de S-CSCFs
- Verificar capacidades configuradas
- Verificar URIs do S-CSCF

Nota: Para adicionar/modificar S-CSCFs, coordene com os administradores do sistema. Novas entradas de S-CSCF requerem:

- Um nome (rótulo descritivo como "Novo S-CSCF")
- O URI do S-CSCF (por exemplo, sip:scscf3.example.com:5060;transport=tcp)
- IDs de capacidade associados (por exemplo, capacidades 0 e 1)

Visualizando Domínios Confiáveis do NDS

Propósito: Monitorar quais domínios de rede são confiáveis para peering

Colunas de Exibição:

- **ID:** ID do banco de dados
- **Domínio Confiável:** FQDN da rede confiável

Exemplo de Saída:

```
ID      Domínio Confiável
1      ims.mnc001.mcc001.3gppnetwork.org
2      ims.mnc002.mcc001.3gppnetwork.org
3      carrier.example.com
```

Operações:

- Visualizar domínios confiáveis
- Verificar relações de peering

Adicionando Domínios Confiáveis: Coordene com os administradores do sistema para adicionar novos domínios confiáveis. Cada entrada requer o nome de domínio totalmente qualificado (FQDN) da rede confiável (por exemplo, partner.example.com).

Monitorando Sessões Ativas

Propósito: Ver em tempo real a tomada de decisões do I-CSCF e a seleção do S-CSCF

Informações de Exibição:

- **Call-ID:** SIP Call-ID
- **Identidade do Usuário:** Identidade pública sendo consultada
- **S-CSCF Selecionado:** Qual S-CSCF foi escolhido
- **Correspondência de Capacidade:** Capacidades que corresponderam
- **Resultado UAR/LIR:** Código de resultado Diameter
- **Timestamp:** Quando a sessão foi criada

Casos de Uso:

1. Verificar se a seleção do S-CSCF está funcionando
2. Solucionar problemas de roteamento
3. Monitorar distribuição de carga entre S-CSCFs
4. Analisar correspondência de capacidades

Exemplo:

```
Call-ID: 3c26700857a87f84@10.4.12.165
Usuário: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
S-CSCF Selecionado:
sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060
Capacidades: mandatory=[0,1], optional=[]
Operação: UAR (Registro)
Resultado: 2001 (FIRST_REGISTRATION)
Timestamp: 2025-11-29 14:35:22
```

Gerenciamento de Tabelas de Hash

Semelhante ao P-CSCF, o I-CSCF pode usar tabelas de hash para cache ou lógica personalizada.

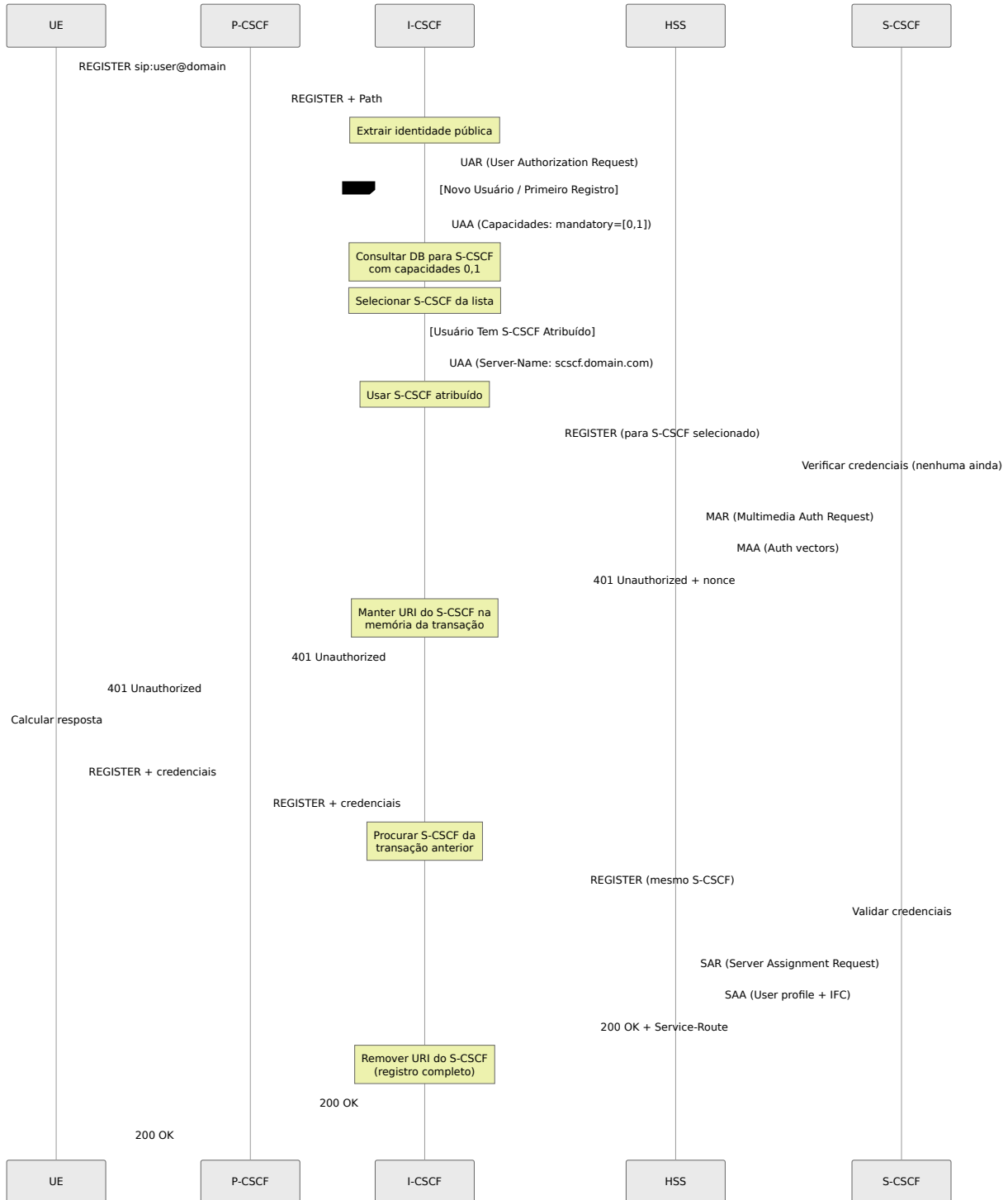
Casos de Uso Comuns:

- Cache de resultados UAR/LIR (TTL curto)
- Limitação de taxa por IP de origem
- Decisões de roteamento personalizadas

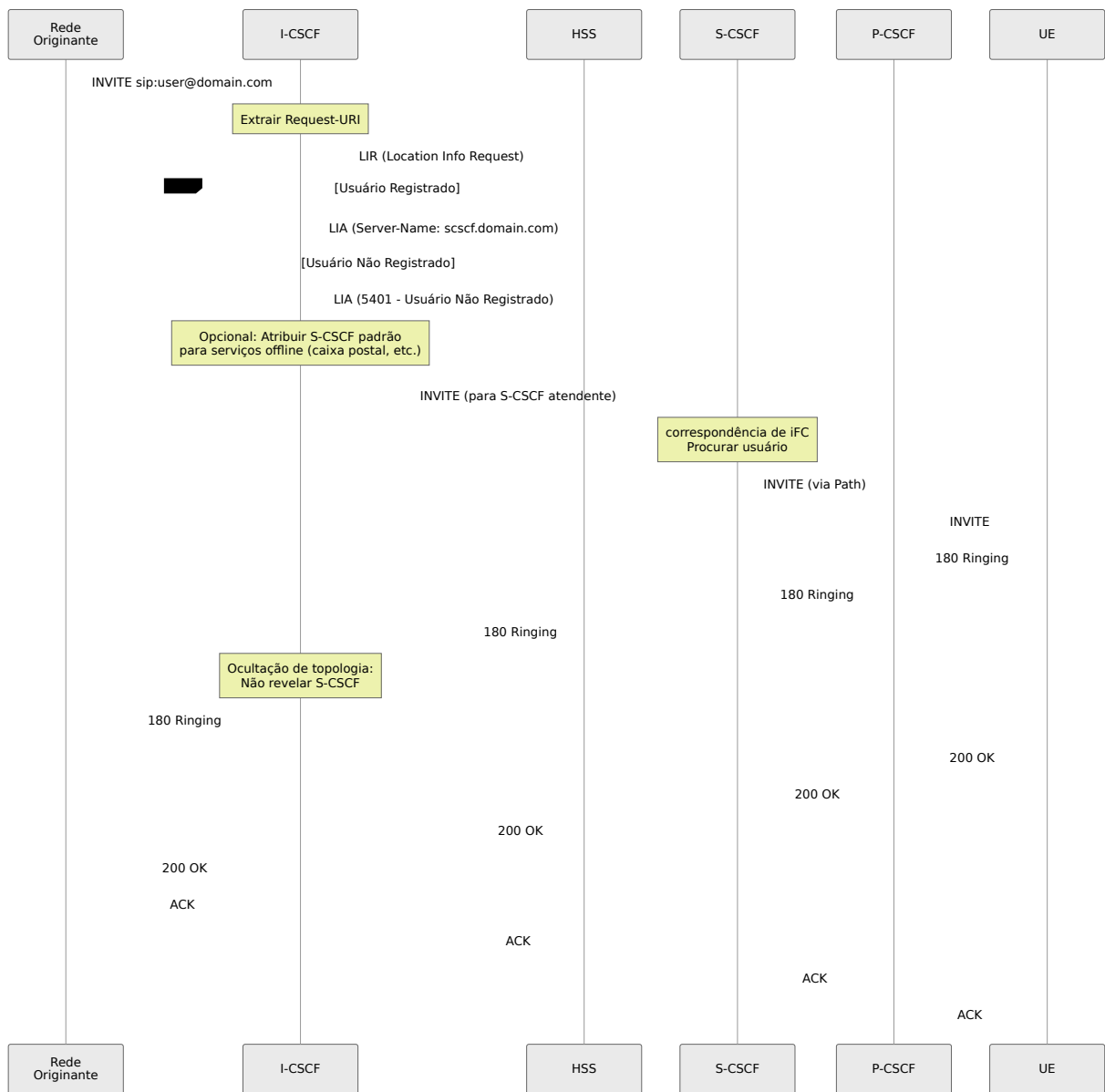
Operações: Mesmas do P-CSCF (listar, despejar, excluir, limpar)

Fluxos de Chamadas

Fluxo de Registro com I-CSCF



Fluxo de Chamada Terminante via I-CSCF

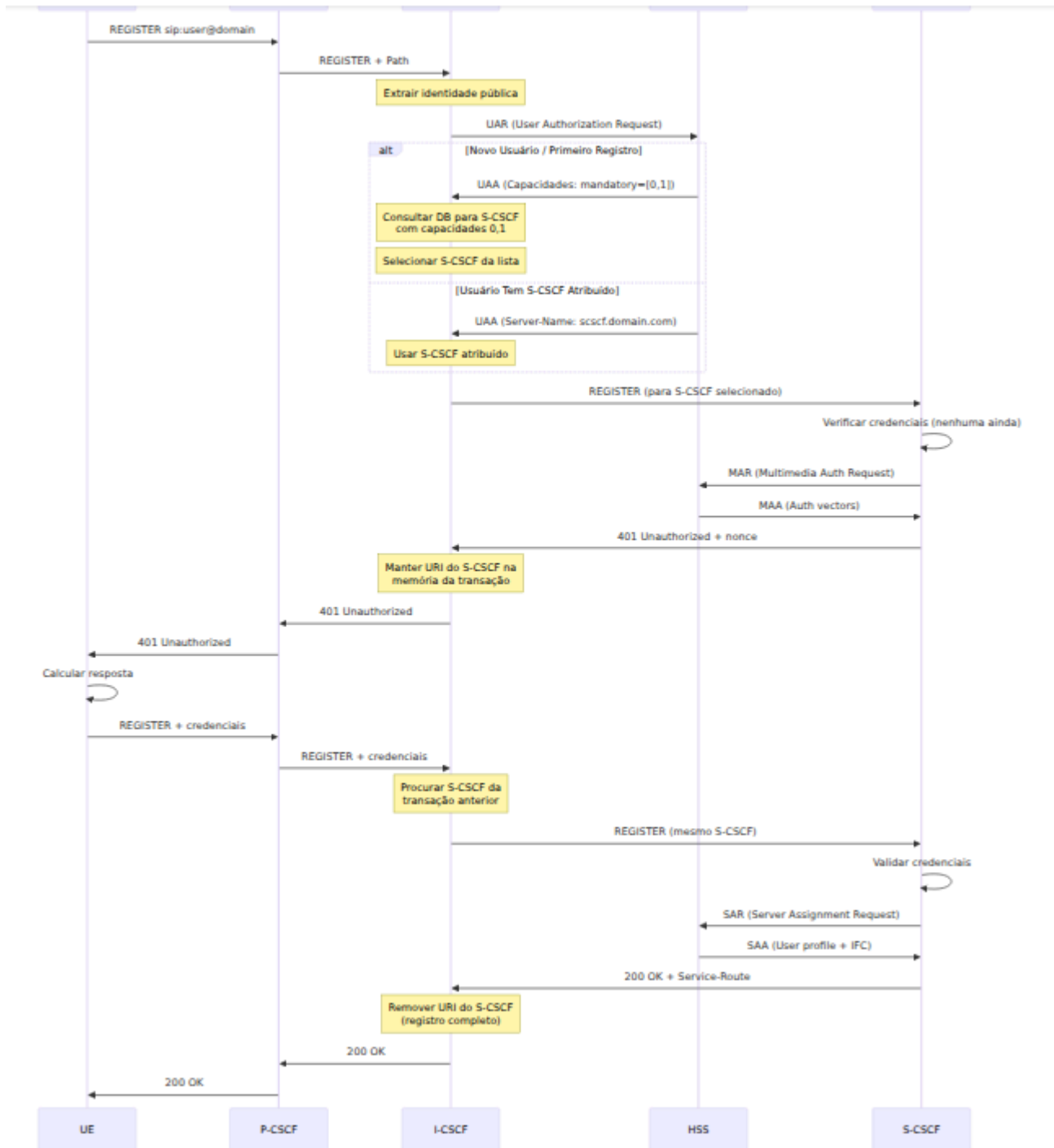


Fluxo de Failover do S-CSCF

Downloads

Portugues

Omnitouch Website



Solução de Problemas

Problemas de Conectividade com o HSS

Peer Diameter Fechado

Sintomas: Não é possível consultar o HSS, todos os registros falham

Passos de Diagnóstico:

1. Verifique o status do peer Diameter na Interface Web:
 - Navegue até a página Diameter
 - Selecione o nó I-CSCF
 - Verifique o estado do peer HSS
2. Verifique a conectividade de rede com o HSS (coordene com a equipe de rede se necessário)
3. Tente habilitar o peer via o painel de controle:
 - Navegue até a página Diameter
 - Encontre o peer HSS
 - Clique no botão "Habilitar"
4. Revise os logs do sistema via a página de Logs do painel de controle para mensagens CER/CEA (Capabilities Exchange) e erros Diameter
5. Coordene com os administradores do sistema para verificar a configuração Diameter se necessário

Timeout UAR/LIR

Sintomas: Registros/chamadas timeout, logs mostram timeout Diameter

Possíveis Causas:

- HSS sobrecarregado
- Latência de rede

- Realm de roteamento incorreto
- HSS não respondendo a este I-CSCF

Soluções:

1. Revise os logs do sistema para erros de timeout Diameter
2. Verifique se o peer HSS está conectado via o painel de controle (página Diameter)
3. Coordene com os administradores do sistema para:
 - Aumentar o timeout da transação Diameter se necessário
 - Verificar a configuração do realm de destino
 - Verificar os logs do HSS se acessíveis
4. Monitore o fluxo de mensagens Diameter via a página de Logs do painel de controle
5. Coordene com a equipe de rede para verificar se não há latência de rede ou problemas de roteamento para o HSS

Problemas de Seleção do S-CSCF

Nenhum S-CSCF Selecionado

Sintomas: 503 Serviço Indisponível, logs mostram "Nenhum S-CSCF disponível"

Passos de Diagnóstico:

1. Verifique a lista de S-CSCF via o painel de controle:
 - Navegue até I-CSCF → guia Servidores S-CSCF
 - Verifique se os S-CSCFs estão configurados com capacidades apropriadas
2. Revise os logs do sistema para capacidades UAA (User Authorization Answer) do HSS

3. Verifique a correspondência de capacidades entre o que o HSS retorna e o que está configurado no banco de dados do I-CSCF
4. Coordene com os administradores do sistema para:
 - Verificar a conectividade do banco de dados
 - Adicionar entradas de S-CSCF ausentes se necessário
 - Verificar se a configuração de capacidade corresponde às expectativas do HSS

S-CSCF Errado Selecionado

Sintomas: Chamadas roteadas para S-CSCF inesperado

Possíveis Causas:

- Desvio de capacidade
- Problema de balanceamento de carga
- Banco de dados fora de sincronia com o HSS

Soluções:

1. Monitore o rastreamento de sessões via o painel de controle:
 - Navegue até I-CSCF → guia Sessões
 - Revise as decisões de seleção do S-CSCF
2. Revise os logs do sistema para verificar se o HSS está atribuindo um nome específico do S-CSCF (o que substituiria a lógica de seleção)
3. Verifique se a lista de S-CSCF e as capacidades do banco de dados do I-CSCF correspondem às expectativas do HSS
4. Coordene com os administradores do sistema para revisar a configuração de correspondência de capacidades

Problemas de Roteamento

Solicitações Não Encaminhadas para S-CSCF

Sintomas: I-CSCF recebe solicitação, mas não encaminha

Passos de Diagnóstico:

1. Revise os logs do sistema via a página de Logs do painel de controle para erros de roteamento
2. Verifique se o URI do S-CSCF de destino está sendo definido corretamente (verifique os logs para decisões de roteamento)
3. Verifique a conectividade de rede com o S-CSCF (coordene com a equipe de rede)
4. Verifique se o S-CSCF selecionado está realmente acessível e respondendo
5. Coordene com os administradores do sistema para habilitar logs de depuração se necessário para uma análise mais profunda

S-CSCF Responde, Mas I-CSCF Não Relata

Sintomas: Wireshark mostra resposta para I-CSCF, mas não encaminhada

Possíveis Causas:

- Timeout de transação
- Desvio de cabeçalho Via
- Loop de Record-Route

Soluções:

1. Revise os logs do sistema para erros de correspondência de transação ou detecção de loop
2. Verifique se os cabeçalhos Via estão sendo processados corretamente (verifique os logs)
3. Coordene com os administradores do sistema para:
 - Aumentar o timeout da transação se necessário
 - Verificar se não há loops de roteamento SIP

Problemas de Banco de Dados

Conexão com o Banco de Dados Perdida

Sintomas: "Erro de conexão com o banco de dados" nos logs

Soluções:

1. Coordene com os administradores do sistema para:
 - Verificar se o serviço do banco de dados está em execução
 - Testar a conectividade do banco de dados
 - Habilitar reconexão automática se não estiver configurada
 - Reiniciar o serviço I-CSCF se necessário

Incompatibilidade de Esquema do Banco de Dados

Sintomas: Erros SQL nos logs sobre colunas/tabelas ausentes

Soluções:

1. Coordene com os administradores do sistema para:
 - Verificar se o esquema do banco de dados corresponde à estrutura esperada
 - Verificar se as tabelas `s_cscf`, `s_cscf_capabilities` e `nds_trusted_domains` existem e têm as colunas corretas
 - Recriar o esquema do banco de dados se necessário

Melhores Práticas

Alta Disponibilidade

1. Implantar várias instâncias do I-CSCF:

- Usar DNS SRV para balanceamento de carga
- Cada instância conecta-se ao mesmo HSS
- Compartilhar banco de dados (somente leitura para lista de S-CSCF)

2. Configuração DNS SRV:

```
_sip._udp.ims.example.com. SRV 10 50 5060 icscf01.example.com.  
_sip._udp.ims.example.com. SRV 10 50 5060 icscf02.example.com.  
_sip._tcp.ims.example.com. SRV 10 50 5060 icscf01.example.com.  
_sip._tcp.ims.example.com. SRV 10 50 5060 icscf02.example.com.
```

3. **Operação sem estado:** O I-CSCF não mantém o estado do diálogo, tornando o failover sem costura

Ajuste de Desempenho

1. **Processos de trabalho:** Defina uma alta contagem de trabalhadores para um desempenho ótimo de consulta
 - children=64 (valor alto otimizado para a carga de trabalho pesada de consultas do I-CSCF)
 - tcp_children=8 para lidar com conexões TCP
2. **Pooling de conexão com o banco de dados:** Use conexões persistentes para reduzir a sobrecarga de conexão
3. **Desabilitar recursos desnecessários** para reduzir a sobrecarga de processamento:
 - Sem manipulação de RTP (I-CSCF é apenas sinalização)
 - Sem serviços de presença
 - Registro mínimo em produção (defina para nível de info ou warning apenas)
4. **Otimizar Diameter** para alta taxa de transferência na interface Cx:
 - sessions_hash_size=4096 (tabela hash maior para melhor desempenho de pesquisa de sessão)
 - workers=4 (threads de trabalho Diameter dedicadas para operações Cx simultâneas)

Segurança

1. **Validar domínios confiáveis:** Verificar Via/P-Visited-Network-ID
2. **Limitação de taxa:** Prevenir ataques DoS no HSS limitando consultas UAR/LIR por IP de origem
 - Usar módulo pike para verificar a taxa de solicitações
 - Se o limite de taxa for excedido, responder com 503 Muitas Solicitações
 - Protege o HSS de ser sobrecarregado por inundações de consultas maliciosas
3. **TLS para HSS:** Usar Diameter sobre TLS (DTLS)
4. **Sanitizar cabeçalhos:** Remover cabeçalhos P não confiáveis de redes externas

Monitoramento

1. Métricas Chave:

- Taxa de sucesso do UAR
- Taxa de sucesso do LIR
- Latência média de consulta
- Distribuição do S-CSCF (balanceamento de carga)
- Uptime do peer Diameter

2. Consultas Prometheus:

```
# Taxa de sucesso do UAR
rate(icscf_uar_success[5m]) / rate(icscf_uar_total[5m])

# Latência média Diameter
rate(diameter_request_duration_sum[5m]) /
rate(diameter_request_duration_count[5m])
```

3. Alertas:

- Peer HSS fora do ar
- Todos os S-CSCFs indisponíveis
- Alta taxa de erro (>5%)

Manutenção do Banco de Dados

A manutenção do banco de dados é realizada pelos administradores do sistema. As principais tarefas de manutenção incluem:

1. **Manter a lista de S-CSCF atualizada:** Coordene com os administradores para garantir que a lista de S-CSCF no banco de dados corresponda às implantações reais
 - Verifique via interface web: Navegue até I-CSCF → guia Lista de S-CSCF
 - Verifique se todos os servidores S-CSCF ativos estão listados com capacidades corretas
2. **Podar sessões antigas:** Se os resultados UAR/LIR forem armazenados em cache, entradas antigas devem ser limpas periodicamente

Referência

Especificações 3GPP

- **TS 23.228:** Arquitetura IMS
- **TS 29.228:** Interface Cx (I-CSCF para HSS)
- **TS 29.229:** Protocolo Cx/Dx

RFCs Diameter

- **RFC 6733:** Protocolo Base Diameter
- **RFC 7155:** Traversal de NAT Diameter

Referência de Métricas do IMS CSCF

Este documento fornece uma referência abrangente para todas as métricas exportadas pelos componentes P-CSCF, I-CSCF e S-CSCF.

Acessando Métricas

Todos os componentes CSCF expõem métricas Prometheus na porta 9090:

```
http://<host>:9090/metrics
```

Cada host CSCF (P-CSCF, I-CSCF, S-CSCF) exporta suas próprias métricas. Configure seu servidor Prometheus para coletar dados de todos os hosts para uma cobertura de monitoramento completa.

Exemplo de Configuração do Prometheus:

```
scrape_configs:  
  - job_name: 'cscf_pcscf'  
    static_configs:  
      - targets: ['pcscf1.example.com:9090',  
                  'pcscf2.example.com:9090']  
  
  - job_name: 'cscf_icscf'  
    static_configs:  
      - targets: ['icscf1.example.com:9090']  
  
  - job_name: 'cscf_scscf'  
    static_configs:  
      - targets: ['scscf1.example.com:9090',  
                  'scscf2.example.com:9090']
```

Para orientações operacionais sobre monitoramento e alertas, consulte:

- [Guia de Operações da Interface Web](#)
- [Guia de Capacidade e Dimensionamento](#)

Monitoramento Através do Painel de Controle

O Painel de Controle do OmniCall CSCF fornece visibilidade em tempo real sobre o estado operacional que gera essas métricas. Enquanto as métricas são exportadas via Prometheus para análise histórica e alertas, o painel de controle mostra o estado atual de registros, diálogos e pares Diameter.

Gerenciamento do S-CSCF

Visualize registros ativos e dados de localização do usuário:

A contagem de registros visível na interface corresponde a métricas como `ims_usrloc_scscf_active_impus` e `ims_usrloc_scscf_active_contacts`.

Monitoramento de Pares Diameter

Monitore o status dos pares Diameter e os comprimentos das filas:

O comprimento da fila mostrado aqui corresponde à métrica `cdp_queueLength`.
O estado do par "I_Open" indica conexões saudáveis.

Cada par mostra as aplicações Diameter suportadas. Por exemplo:

- **16777216:10415 (Cx/Dx)** - Usado pelo I-CSCF e S-CSCF para comunicação HSS (UAR, LIR, MAR, SAR)
- **16777236:10415 (Rx)** - Usado pelo P-CSCF para política de QoS do PCRF
- **4 (Ro)** - Usado pelo S-CSCF para cobrança online

Esses correspondem a métricas como `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_registrar_scscf_sar_*`, e `ims_qos_*`.

Métricas do P-CSCF

Métricas CDP (Diameter)

Nome da Métrica	Significado
<code>cdp_average_response_time</code>	Tempo médio de resposta para requisições Diameter em milissegundos (calculado como $\text{replies_response_time} / \text{replies_received}$)
<code>cdp_queuelength</code>	Comprimento atual da fila de tarefas do trabalhador Diameter
<code>cdp_replies_received</code>	Número total de respostas Diameter recebidas
<code>cdp_replies_response_time</code>	Tempo total gasto aguardando respostas Diameter em milissegundos
<code>cdp_timeout</code>	Número de eventos de timeout em requisições Diameter

Estatísticas SIP do Core

Contadores de Requisições

Nome da Métrica	Significado
<code>core_rcv_requests</code>	Número total de requisições SIP recebidas
<code>core_rcv_requests_ack</code>	Número de requisições ACK recebidas
<code>core_rcv_requests_bye</code>	Número de requisições BYE recebidas
<code>core_rcv_requests_cancel</code>	Número de requisições CANCEL recebidas
<code>core_rcv_requests_info</code>	Número de requisições INFO recebidas
<code>core_rcv_requests_invite</code>	Número de requisições INVITE recebidas
<code>core_rcv_requests_message</code>	Número de requisições MESSAGE recebidas
<code>core_rcv_requests_notify</code>	Número de requisições NOTIFY recebidas
<code>core_rcv_requests_options</code>	Número de requisições OPTIONS recebidas
<code>core_rcv_requests_prack</code>	Número de requisições PRACK recebidas
<code>core_rcv_requests_publish</code>	Número de requisições PUBLISH recebidas
<code>core_rcv_requests_refer</code>	Número de requisições REFER recebidas
<code>core_rcv_requests_register</code>	Número de requisições REGISTER recebidas
<code>core_rcv_requests_subscribe</code>	Número de requisições SUBSCRIBE recebidas
<code>core_rcv_requests_update</code>	Número de requisições UPDATE recebidas

Contadores de Respostas (Geral)

Nome da Métrica	Significado
core_rcv_replies	Número total de respostas SIP recebidas
core_rcv_replies_18x	Número de respostas provisórias 180/181/183/186/187/189 recebidas
core_rcv_replies_1xx	Número de respostas 1xx (provisórias) recebidas
core_rcv_replies_2xx	Número de respostas 2xx (sucesso) recebidas
core_rcv_replies_3xx	Número de respostas 3xx (redirecionamento) recebidas
core_rcv_replies_4xx	Número de respostas 4xx (erro do cliente) recebidas
core_rcv_replies_5xx	Número de respostas 5xx (erro do servidor) recebidas
core_rcv_replies_6xx	Número de respostas 6xx (falha global) recebidas

Contadores de Respostas por Método (1xx)

Nome da Métrica	Significado
<code>core_rcv_replies_1xx_bye</code>	Número de respostas 1xx para requisições BYE
<code>core_rcv_replies_1xx_cancel</code>	Número de respostas 1xx para requisições CANCEL
<code>core_rcv_replies_1xx_invite</code>	Número de respostas 1xx para requisições INVITE
<code>core_rcv_replies_1xx_message</code>	Número de respostas 1xx para requisições MESSAGE
<code>core_rcv_replies_1xx_prack</code>	Número de respostas 1xx para requisições PRACK
<code>core_rcv_replies_1xx_refer</code>	Número de respostas 1xx para requisições REFER
<code>core_rcv_replies_1xx_reg</code>	Número de respostas 1xx para requisições REGISTER
<code>core_rcv_replies_1xx_update</code>	Número de respostas 1xx para requisições UPDATE

Contadores de Respostas por Método (2xx)

Nome da Métrica	Significado
<code>core_rcv_replies_2xx_bye</code>	Número de respostas 2xx (sucesso) para requisições BYE
<code>core_rcv_replies_2xx_cancel</code>	Número de respostas 2xx (sucesso) para requisições CANCEL
<code>core_rcv_replies_2xx_invite</code>	Número de respostas 2xx (sucesso) para requisições INVITE
<code>core_rcv_replies_2xx_message</code>	Número de respostas 2xx (sucesso) para requisições MESSAGE
<code>core_rcv_replies_2xx_prack</code>	Número de respostas 2xx (sucesso) para requisições PRACK
<code>core_rcv_replies_2xx_refer</code>	Número de respostas 2xx (sucesso) para requisições REFER
<code>core_rcv_replies_2xx_reg</code>	Número de respostas 2xx (sucesso) para requisições REGISTER
<code>core_rcv_replies_2xx_update</code>	Número de respostas 2xx (sucesso) para requisições UPDATE

Contadores de Respostas por Método (3xx)

Nome da Métrica	Significado
<code>core_rcv_replies_3xx_bye</code>	Número de respostas 3xx (redirecionamento) para requisições BYE
<code>core_rcv_replies_3xx_cancel</code>	Número de respostas 3xx (redirecionamento) para requisições CANCEL
<code>core_rcv_replies_3xx_invite</code>	Número de respostas 3xx (redirecionamento) para requisições INVITE
<code>core_rcv_replies_3xx_message</code>	Número de respostas 3xx (redirecionamento) para requisições MESSAGE
<code>core_rcv_replies_3xx_prack</code>	Número de respostas 3xx (redirecionamento) para requisições PRACK
<code>core_rcv_replies_3xx_refer</code>	Número de respostas 3xx (redirecionamento) para requisições REFER
<code>core_rcv_replies_3xx_reg</code>	Número de respostas 3xx (redirecionamento) para requisições REGISTER
<code>core_rcv_replies_3xx_update</code>	Número de respostas 3xx (redirecionamento) para requisições UPDATE

Contadores de Respostas por Método (4xx)

Nome da Métrica	Significado
<code>core_rcv_replies_4xx_bye</code>	Número de respostas 4xx (erro do cliente) para requisições BYE
<code>core_rcv_replies_4xx_cancel</code>	Número de respostas 4xx (erro do cliente) para requisições CANCEL
<code>core_rcv_replies_4xx_invite</code>	Número de respostas 4xx (erro do cliente) para requisições INVITE
<code>core_rcv_replies_4xx_message</code>	Número de respostas 4xx (erro do cliente) para requisições MESSAGE
<code>core_rcv_replies_4xx_prack</code>	Número de respostas 4xx (erro do cliente) para requisições PRACK
<code>core_rcv_replies_4xx_refer</code>	Número de respostas 4xx (erro do cliente) para requisições REFER
<code>core_rcv_replies_4xx_reg</code>	Número de respostas 4xx (erro do cliente) para requisições REGISTER
<code>core_rcv_replies_4xx_update</code>	Número de respostas 4xx (erro do cliente) para requisições UPDATE

Contadores de Respostas por Método (5xx)

Nome da Métrica	Significado
<code>core_rcv_replies_5xx_bye</code>	Número de respostas 5xx (erro do servidor) para requisições BYE
<code>core_rcv_replies_5xx_cancel</code>	Número de respostas 5xx (erro do servidor) para requisições CANCEL
<code>core_rcv_replies_5xx_invite</code>	Número de respostas 5xx (erro do servidor) para requisições INVITE
<code>core_rcv_replies_5xx_message</code>	Número de respostas 5xx (erro do servidor) para requisições MESSAGE
<code>core_rcv_replies_5xx_prack</code>	Número de respostas 5xx (erro do servidor) para requisições PRACK
<code>core_rcv_replies_5xx_refer</code>	Número de respostas 5xx (erro do servidor) para requisições REFER
<code>core_rcv_replies_5xx_reg</code>	Número de respostas 5xx (erro do servidor) para requisições REGISTER
<code>core_rcv_replies_5xx_update</code>	Número de respostas 5xx (erro do servidor) para requisições UPDATE

Contadores de Respostas por Método (6xx)

Nome da Métrica	Significado
<code>core_rcv_replies_6xx_bye</code>	Número de respostas 6xx (falha global) para requisições BYE
<code>core_rcv_replies_6xx_cancel</code>	Número de respostas 6xx (falha global) para requisições CANCEL
<code>core_rcv_replies_6xx_invite</code>	Número de respostas 6xx (falha global) para requisições INVITE
<code>core_rcv_replies_6xx_message</code>	Número de respostas 6xx (falha global) para requisições MESSAGE
<code>core_rcv_replies_6xx_prack</code>	Número de respostas 6xx (falha global) para requisições PRACK
<code>core_rcv_replies_6xx_refer</code>	Número de respostas 6xx (falha global) para requisições REFER
<code>core_rcv_replies_6xx_reg</code>	Número de respostas 6xx (falha global) para requisições REGISTER
<code>core_rcv_replies_6xx_update</code>	Número de respostas 6xx (falha global) para requisições UPDATE

Contadores de Códigos de Status Específicos

Nome da Métrica	Significado
core_rcv_replies_400	Número de respostas 400 Bad Request recebidas
core_rcv_replies_401	Número de respostas 401 Unauthorized recebidas
core_rcv_replies_402	Número de respostas 402 Payment Required recebidas
core_rcv_replies_403	Número de respostas 403 Forbidden recebidas
core_rcv_replies_404	Número de respostas 404 Not Found recebidas
core_rcv_replies_405	Número de respostas 405 Method Not Allowed recebidas
core_rcv_replies_406	Número de respostas 406 Not Acceptable recebidas
core_rcv_replies_407	Número de respostas 407 Proxy Authentication Required recebidas
core_rcv_replies_408	Número de respostas 408 Request Timeout recebidas
core_rcv_replies_409	Número de respostas 409 Conflict recebidas
core_rcv_replies_410	Número de respostas 410 Gone recebidas
core_rcv_replies_411	Número de respostas 411 Length Required recebidas
core_rcv_replies_413	Número de respostas 413 Request Entity Too Large recebidas
core_rcv_replies_414	Número de respostas 414 Request-URI Too Long recebidas

Nome da Métrica	Significado
core_rcv_replies_415	Número de respostas 415 Unsupported Media Type recebidas
core_rcv_replies_420	Número de respostas 420 Bad Extension recebidas
core_rcv_replies_480	Número de respostas 480 Temporarily Unavailable recebidas
core_rcv_replies_481	Número de respostas 481 Call/Transaction Does Not Exist recebidas
core_rcv_replies_482	Número de respostas 482 Loop Detected recebidas
core_rcv_replies_483	Número de respostas 483 Too Many Hops recebidas
core_rcv_replies_484	Número de respostas 484 Address Incomplete recebidas
core_rcv_replies_485	Número de respostas 485 Ambiguous recebidas
core_rcv_replies_486	Número de respostas 486 Busy Here recebidas
core_rcv_replies_487	Número de respostas 487 Request Terminated recebidas
core_rcv_replies_488	Número de respostas 488 Not Acceptable Here recebidas
core_rcv_replies_489	Número de respostas 489 Bad Event recebidas
core_rcv_replies_491	Número de respostas 491 Request Pending recebidas

Nome da Métrica	Significado
<code>core_rcv_replies_493</code>	Número de respostas 493 Undecipherable recebidas

Estatísticas de Encaminhamento e Erro

Nome da Métrica	Significado
<code>core_fwd_replies</code>	Número de respostas SIP encaminhadas
<code>core_fwd_requests</code>	Número de requisições SIP encaminhadas
<code>core_drop_replies</code>	Número de respostas SIP descartadas
<code>core_drop_requests</code>	Número de requisições SIP descartadas
<code>core_err_replies</code>	Número de respostas de erro
<code>core_err_requests</code>	Número de requisições de erro
<code>core_bad_URIs_rcvd</code>	Número de mensagens com URIs malformadas recebidas
<code>core_bad_msg_hdr</code>	Número de mensagens com cabeçalhos ruins/malformados
<code>core_unsupported_methods</code>	Número de requisições com métodos SIP não suportados

Rastreamento de Diálogos

Nome da Métrica	Significado
<code>dialog_ng_active</code>	Número de diálogos atualmente ativos (respondidos/confirmados)
<code>dialog_ng_early</code>	Número de diálogos precoces (tocando/estado provisório)
<code>dialog_ng_expired</code>	Número de diálogos que expiraram ou foram encerrados à força
<code>dialog_ng_processed</code>	Número total de diálogos processados desde a inicialização

Estatísticas de DNS

Nome da Métrica	Significado
<code>dns_failed_dns_request</code>	Número de consultas DNS falhadas
<code>dns_slow_dns_request</code>	Número de consultas DNS lentas (excedendo o limite)

IMS IPsec P-CSCF

Nome da Métrica	Significado
<code>ims_ipsec_pcscf_spi_free</code>	Número de valores SPI (Security Parameter Index) livres disponíveis para alocação
<code>ims_ipsec_pcscf_spi_total</code>	Capacidade total de SPI configurada para o sistema
<code>ims_ipsec_pcscf_spi_used</code>	Número de valores SPI atualmente alocados/usados
<code>ims_ipsec_pcscf_spi_utilization_pct</code>	Porcentagem de utilização do pool de SPI
<code>ims_ipsec_pcscf_worker_cache_size</code>	Tamanho do cache IPsec do processo trabalhador

IMS QoS (Interface Rx)

Métricas de Registro AAR

Nome da Métrica	Significado
ims_qos_active_registration_rx_sessions	Número de sessões de registro Rx ativas atualmente
ims_qos_registration_aars	Número total de mensagens AAR (Authorization-Authentication Request) de registro enviadas
ims_qos_successful_registration_aars	Número de transações AAR de registro bem-sucedidas
ims_qos_failed_registration_aars	Número de transações AAR de registro falhadas
ims_qos_registration_aar_avg_response_time	Tempo médio de resposta para mensagens AAR de registro em milissegundos
ims_qos_registration_aar_response_time	Tempo total de resposta para todas as mensagens AAR de registro em milissegundos
ims_qos_registration_aar_replies_received	Número total de respostas AAR de registro recebidas
ims_qos_registration_aar_timeouts	Número de timeouts de requisições AAR de

Nome da Métrica	Significado
	registro

Métricas de AAR de Mídia

Nome da Métrica	Significado
<code>ims_qos_active_media_rx_sessions</code>	Número de sessões de mídia Rx ativas atualmente
<code>ims_qos_media_rx_sessions</code>	Número total de sessões de mídia Rx criadas
<code>ims_qos_media_aars</code>	Número total de mensagens AAR de mídia enviadas
<code>ims_qos_successful_media_aars</code>	Número de transações AAR de mídia bem-sucedidas
<code>ims_qos_failed_media_aars</code>	Número de transações AAR de mídia falhadas
<code>ims_qos_media_aar_avg_response_time</code>	Tempo médio de resposta para mensagens AAR de mídia em milissegundos
<code>ims_qos_media_aar_response_time</code>	Tempo total de resposta para todas as mensagens AAR de mídia em milissegundos
<code>ims_qos_media_aar_replies_received</code>	Número total de respostas AAR de mídia recebidas
<code>ims_qos_media_aar_timeouts</code>	Número de timeouts de requisições AAR de mídia

Métricas ASR

Nome da Métrica	Significado
<code>ims_qos_asrs</code>	Número total de mensagens ASR (Abort-Session-Request) recebidas do PCRF

IMS USRLOC P-CSCF

Nome da Métrica	Significado
<code>ims_usrloc_pcscf_expired_contacts</code>	Número de vinculações de contato expiradas
<code>ims_usrloc_pcscf_registered_contacts</code>	Número de vinculações de contato atualmente registradas
<code>ims_usrloc_pcscf_registered_impus</code>	Número de IMPUs (Identidades Públicas do Usuário IMS) atualmente registradas

Banco de Dados MySQL

Nome da Métrica	Significado
<code>mysql_driver_errors</code>	Número de erros de driver/conexão MySQL

Módulo Pike (Bloqueio de IP)

Nome da Métrica	Significado
<code>pike_blocked_ips</code>	Número de endereços IP atualmente bloqueados (detecção de inundação)

Módulo Registrador

Nome da Métrica	Significado
<code>registrar_accepted_regs</code>	Número de requisições REGISTER aceitas (módulo registrador legado)
<code>registrar_rejected_regs</code>	Número de requisições REGISTER rejeitadas (módulo registrador legado)
<code>registrar_default_expire</code>	Tempo de expiração padrão para registros em segundos
<code>registrar_default_expires_range</code>	Configuração do intervalo de expiração padrão
<code>registrar_expires_range</code>	Intervalo de expiração configurado
<code>registrar_max_contacts</code>	Número máximo de contatos permitidos por AOR
<code>registrar_max_expires</code>	Tempo máximo de expiração permitido em segundos

Estatísticas de Script

Nome da Métrica	Significado
<code>script_register_failed</code>	Número de tentativas de registro que falharam na lógica do script de roteamento
<code>script_register_success</code>	Número de registros bem-sucedidos processados pelo script de roteamento
<code>script_register_time</code>	Tempo total gasto processando registros no script de roteamento (milissegundos)

Transporte SCTP

Nome da Métrica	Significado
<code>sctp_assoc_shutdown</code>	Número de encerramentos de associação SCTP iniciados localmente
<code>sctp_comm_lost</code>	Número de associações SCTP perdidas devido a falha de comunicação
<code>sctp_connect_failed</code>	Número de tentativas de associação SCTP de saída que falharam
<code>sctp_current_opened_connections</code>	Número de associações SCTP atualmente abertas
<code>sctp_current_tracked_connections</code>	Número de associações SCTP atualmente rastreadas
<code>sctp_established</code>	Número total de associações SCTP estabelecidas
<code>sctp_local_reject</code>	Número de associações SCTP de entrada rejeitadas localmente
<code>sctp_remote_shutdown</code>	Número de encerramentos de associação SCTP iniciados pelo par
<code>sctp_send_failed</code>	Número de operações de envio SCTP que falharam
<code>sctp_send_force_retry</code>	Número de tentativas forçadas em envios SCTP que falharam

Nome da Métrica	Significado
<code>sctp_sendq_full</code>	Número de tentativas de envio que falharam devido à fila de envio cheia

Memória Compartilhada

Nome da Métrica	Significado
<code>shmem_fragments</code>	Número de fragmentos no pool de memória compartilhada (indica fragmentação)
<code>shmem_free_size</code>	Quantidade de memória compartilhada livre em bytes
<code>shmem_max_used_size</code>	Máxima memória compartilhada usada desde a inicialização em bytes
<code>shmem_real_used_size</code>	Memória compartilhada realmente usada incluindo sobrecarga do alocador em bytes
<code>shmem_total_size</code>	Tamanho total do pool de memória compartilhada em bytes
<code>shmem_used_size</code>	Memória compartilhada atualmente usada (apenas dados do usuário) em bytes

Módulo SL (Sem Estado)

Contadores de Respostas Sem Estado por Classe

Nome da Métrica	Significado
sl_1xx_replies	Número de respostas sem estado 1xx enviadas
sl_2xx_replies	Número de respostas sem estado 2xx enviadas
sl_3xx_replies	Número de respostas sem estado 3xx enviadas
sl_4xx_replies	Número de respostas sem estado 4xx enviadas
sl_5xx_replies	Número de respostas sem estado 5xx enviadas
sl_6xx_replies	Número de respostas sem estado 6xx enviadas
sl_xxx_replies	Número de outras respostas sem estado enviadas

Contadores de Respostas Sem Estado Específicos

Nome da Métrica	Significado
sl_200_replies	Número de respostas sem estado 200 OK enviadas
sl_202_replies	Número de respostas sem estado 202 Accepted enviadas
sl_300_replies	Número de respostas sem estado 300 Multiple Choices enviadas
sl_301_replies	Número de respostas sem estado 301 Moved Permanently enviadas
sl_302_replies	Número de respostas sem estado 302 Moved Temporarily enviadas
sl_400_replies	Número de respostas sem estado 400 Bad Request enviadas
sl_401_replies	Número de respostas sem estado 401 Unauthorized enviadas
sl_403_replies	Número de respostas sem estado 403 Forbidden enviadas
sl_404_replies	Número de respostas sem estado 404 Not Found enviadas
sl_407_replies	Número de respostas sem estado 407 Proxy Authentication Required enviadas
sl_408_replies	Número de respostas sem estado 408 Request Timeout enviadas
sl_483_replies	Número de respostas sem estado 483 Too Many Hops enviadas

Nome da Métrica	Significado
sl_500_replies	Número de respostas sem estado 500 Server Internal Error enviadas

Estatísticas Gerais Sem Estado

Nome da Métrica	Significado
sl_sent_replies	Número total de respostas sem estado enviadas
sl_sent_err_replies	Número de respostas de erro sem estado enviadas
sl_received_ACKs	Número de mensagens ACK recebidas para transações sem estado
sl_failures	Número de falhas no envio de respostas sem estado

Transporte TCP

Nome da Métrica	Significado
<code>tcp_con_reset</code>	Número de conexões TCP redefinidas (RST recebido em conexão estabelecida)
<code>tcp_con_timeout</code>	Número de conexões TCP fechadas devido a timeout ocioso
<code>tcp_connect_failed</code>	Número de tentativas de conexão TCP de saída que falharam
<code>tcp_connect_success</code>	Número de conexões TCP de saída bem-sucedidas
<code>tcp_current_opened_connections</code>	Número de conexões TCP atualmente abertas
<code>tcp_current_write_queue_size</code>	Tamanho total atual das filas de escrita TCP em todas as conexões
<code>tcp_established</code>	Número total de conexões TCP estabelecidas (tanto de entrada quanto de saída)
<code>tcp_local_reject</code>	Número de conexões TCP de entrada rejeitadas localmente
<code>tcp_passive_open</code>	Número de conexões TCP de entrada aceitas
<code>tcp_send_timeout</code>	Número de operações de envio TCP que excederam o tempo limite (modo assíncrono)

Nome da Métrica	Significado
<code>tcp_sendq_full</code>	Número de tentativas de envio que falharam porque a fila de envio estava cheia

Módulo TM/TMX (Transação)

Contadores de Tipo de Transação

Nome da Métrica	Significado
<code>tmx_UAC_transactions</code>	Número de transações UAC (cliente) criadas
<code>tmx_UAS_transactions</code>	Número de transações UAS (servidor) criadas
<code>tmx_active_transactions</code>	Número de transações atualmente ativas
<code>tmx_inuse_transactions</code>	Número de transações atualmente em uso

Conclusão de Transação por Status

Nome da Métrica	Significado
<code>tmx_2xx_transactions</code>	Número de transações concluídas com resposta 2xx
<code>tmx_3xx_transactions</code>	Número de transações concluídas com resposta 3xx
<code>tmx_4xx_transactions</code>	Número de transações concluídas com resposta 4xx
<code>tmx_5xx_transactions</code>	Número de transações concluídas com resposta 5xx
<code>tmx_6xx_transactions</code>	Número de transações concluídas com resposta 6xx

Estatísticas de Resposta de Transação

Nome da Métrica	Significado
<code>tmx_rpl_absorbed</code>	Número de respostas absorvidas pela camada de transação (duplicatas)
<code>tmx_rpl_generated</code>	Número de respostas geradas localmente pelo módulo de transação
<code>tmx_rpl_received</code>	Número de respostas recebidas para transações
<code>tmx_rpl_relayed</code>	Número de respostas retransmitidas pelo módulo de transação
<code>tmx_rpl_sent</code>	Número de respostas enviadas pelo módulo de transação

USRLOC (Localização do Usuário)

Nome da Métrica	Significado
<code>usrloc_location_contacts</code>	Número de contatos no domínio 'location' (módulo usrloc padrão)
<code>usrloc_location_expires</code>	Número de contatos expirados no domínio 'location'
<code>usrloc_registered_users</code>	Número de usuários/AORs (Address of Records) registrados

Métricas do I-CSCF

O I-CSCF compartilha a maioria das estatísticas SIP do core com o P-CSCF (veja a seção Estatísticas SIP do Core do P-CSCF acima). As seguintes métricas são específicas para a funcionalidade do I-CSCF.

Contexto Operacional do I-CSCF

O I-CSCF mantém uma lista de instâncias S-CSCF disponíveis para balanceamento de carga:

O I-CSCF consulta o HSS para selecionar instâncias S-CSCF apropriadas para novos registros. O sucesso dessas operações é rastreado nas métricas UAR e LIR abaixo.

IMS I-CSCF (Interface Cx - Comunicação HSS)

O I-CSCF usa a interface Diameter Cx para se comunicar com o HSS (Home Subscriber Server) para consultas de localização e autorização do usuário.

Métricas UAR (User-Authorization-Request)

Nome da Métrica	Significado
<code>ims_icscf_uar_avg_response_time</code>	Tempo médio de resposta para mensagens UAR em milissegundos (calculado como $\text{uar_replies_response_time} / \text{uar_replies_received}$)
<code>ims_icscf_uar_replies_received</code>	Número total de respostas UAA (User-Authorization-Answer) recebidas do HSS
<code>ims_icscf_uar_replies_response_time</code>	Tempo total de resposta para todas as mensagens UAR em milissegundos
<code>ims_icscf_uar_timeouts</code>	Número de timeouts de requisições UAR

Métricas LIR (Location-Info-Request)

Nome da Métrica	Significado
<code>ims_icscf_lir_avg_response_time</code>	Tempo médio de resposta para mensagens LIR em milissegundos (calculado como $\text{lir_replies_response_time} / \text{lir_replies_received}$)
<code>ims_icscf_lir_replies_received</code>	Número total de respostas LIA (Location-Info-Answer) recebidas do HSS
<code>ims_icscf_lir_replies_response_time</code>	Tempo total de resposta para todas as mensagens LIR em milissegundos
<code>ims_icscf_lir_timeouts</code>	Número de timeouts de requisições LIR

Métricas Comuns

O I-CSCF também exporta as seguintes métricas comuns (documentadas na seção P-CSCF acima):

- **Métricas CDP (Diameter)** - Estatísticas do protocolo Diameter
- **Estatísticas SIP do Core** - Contadores de requisições/respostas por método e código de status
- **Estatísticas de DNS** - Métricas de consulta DNS
- **Banco de Dados MySQL** - Erros de conexão com o banco de dados
- **Módulo Pike** - Estatísticas de bloqueio de IP
- **Memória Compartilhada** - Estatísticas de uso de memória
- **Módulo SL (Sem Estado)** - Contadores de respostas sem estado
- **Transporte TCP** - Estatísticas de conexão TCP
- **Módulo TM/TMX (Transação)** - Rastreamento do estado da transação

Métricas do S-CSCF

O S-CSCF compartilha a maioria das estatísticas SIP do core com o P-CSCF e I-CSCF (veja a seção Estatísticas SIP do Core do P-CSCF acima). As seguintes métricas são específicas para a funcionalidade do S-CSCF.

Contexto Operacional do S-CSCF

O S-CSCF fornece informações detalhadas de localização do usuário e gerenciamento de IFC (Critérios de Filtro Iniciais):

A consulta de localização do usuário mostra IMPUs registrados com vinculações de contato e perfis de serviço. O número de contatos ativos e IMPUs é rastreado pelas métricas `ims_usrloc_scscf_active_contacts` e `ims_usrloc_scscf_active_impus`.

O IFC (Critérios de Filtro Iniciais) determina quais Servidores de Aplicação processam sessões SIP. O painel de controle permite despejar e testar regras IFC. O desempenho da avaliação do IFC pode impactar os tempos de configuração de chamadas rastreados nas métricas de transação (`tmx_*`).

IMS ISC (Controle de Serviço IMS)

O módulo IMS ISC lida com a avaliação dos Critérios de Filtro Iniciais (iFC) para determinar quais Servidores de Aplicação devem processar sessões SIP. Essas métricas rastreiam o desempenho e a eficácia das operações de correspondência de iFC.

Nome da Métrica	Significado
<code>ims_isc_ifc_match_attempts</code>	Número total de tentativas de correspondência de iFC realizadas
<code>ims_isc_ifc_match_time_total</code>	Tempo acumulado gasto realizando operações de correspondência de iFC em milissegundos
<code>ims_isc_ifc_nomatch_count</code>	Número de tentativas de correspondência de iFC em que nenhum critério de disparo correspondeu

Monitoramento de Desempenho: Calcule o tempo médio de correspondência de iFC como `ifc_match_time_total / ifc_match_attempts`. Tempos médios altos podem indicar critérios de filtro complexos ou gargalos de desempenho na seleção do Servidor de Aplicação. Uma alta proporção de `ifc_nomatch_count` para `ifc_match_attempts` pode indicar pontos de disparo mal configurados ou padrões de tráfego inesperados.

Autenticação IMS (Interface Cx - MAR)

O S-CSCF usa a interface Diameter Cx para autenticar usuários com o HSS via MAR (Multimedia-Auth-Request).

Nome da Métrica	Significado
ims_auth_mar_avg_response_time	Tempo médio de resposta para mensagens MAR em milissegundos (calculado como $\text{mar_replies_response_time} / \text{mar_replies_received}$)
ims_auth_mar_replies_received	Número total de respostas MAA (Multimedia-Auth-Answer) recebidas do HSS
ims_auth_mar_replies_response_time	Tempo total de resposta para todas as mensagens MAR em milissegundos
ims_auth_mar_timeouts	Número de timeouts de requisições MAR

Registrador IMS S-CSCF

Estatísticas de Registro

Nome da Métrica	Significado
<code>ims_registrar_scscf_accepted_regs</code>	Número de requisições REGISTER aceitas com sucesso
<code>ims_registrar_scscf_rejected_regs</code>	Número de requisições REGISTER rejeitadas
<code>ims_registrar_scscf_default_expire</code>	Tempo de expiração padrão para registros em segundos
<code>ims_registrar_scscf_default_expires_range</code>	Configuração do intervalo de expiração padrão
<code>ims_registrar_scscf_max_contacts</code>	Número máximo de contatos permitidos por registro
<code>ims_registrar_scscf_max_expires</code>	Tempo máximo de expiração permitido em segundos
<code>ims_registrar_scscf_notifies_in_q</code>	Número de mensagens NOTIFY pendentes na fila

Métricas SAR (Server-Assignment-Request)

Nome da Métrica	Significado
<code>ims_registrar_scscf_sar_avg_response_time</code>	Tempo médio de respos para mensagens SAR em milissegundos (calculac como $\text{sar_replies_response_ti} / \text{sar_replies_received}$)
<code>ims_registrar_scscf_sar_replies_received</code>	Número total de respostas SAA (Server-Assignment-Answer) recebidas do HSS
<code>ims_registrar_scscf_sar_replies_response_time</code>	Tempo total de resposta para todas as message SAR em milissegundos
<code>ims_registrar_scscf_sar_timeouts</code>	Número de timeouts de requisições SAR

IMS USRLOC S-CSCF

Nome da Métrica	Significado
<code>ims_usrloc_scscf_active_contacts</code>	Número de vinculações de contato registradas ativas atualmente
<code>ims_usrloc_scscf_active_impus</code>	Número de IMPUs (Identidades Públicas do Usuário IMS) registradas ativas atualmente
<code>ims_usrloc_scscf_active_subscriptions</code>	Número de assinaturas ativas atualmente
<code>ims_usrloc_scscf_contact_collisions</code>	Número de colisões de hash na tabela de hash de contatos
<code>ims_usrloc_scscf_impus_collisions</code>	Número de colisões de hash na tabela de hash de IMPU
<code>ims_usrloc_scscf_subscription_collisions</code>	Número de colisões de hash na tabela de hash de assinaturas

Rastreamento de Diálogos

O S-CSCF rastreia o estado do diálogo para chamadas ativas:

Nome da Métrica	Significado
<code>dialog_ng_active</code>	Número de diálogos atualmente ativos (respondidos/confirmados)
<code>dialog_ng_early</code>	Número de diálogos precoces (tocando/estado provisório)
<code>dialog_ng_expired</code>	Número de diálogos que expiraram ou foram encerrados à força
<code>dialog_ng_processed</code>	Número total de diálogos processados desde a inicialização

Métricas Comuns

O S-CSCF também exporta as seguintes métricas comuns (documentadas na seção P-CSCF acima):

- **Métricas CDP (Diameter)** - Estatísticas do protocolo Diameter
- **Estatísticas SIP do Core** - Contadores de requisições/respostas por método e código de status (observação: o S-CSCF normalmente tem mais `fwd_requests` e `fwd_replies`, pois roteia entre pontos finais)
- **Estatísticas de DNS** - Métricas de consulta DNS
- **Banco de Dados MySQL** - Erros de conexão com o banco de dados
- **Módulo Pike** - Estatísticas de bloqueio de IP
- **Memória Compartilhada** - Estatísticas de uso de memória
- **Módulo SL (Sem Estado)** - Contadores de respostas sem estado
- **Transporte TCP** - Estatísticas de conexão TCP
- **Módulo TM/TMX (Transação)** - Rastreamento do estado da transação (observação: o S-CSCF normalmente tem transações UAC e UAS, pois atua como cliente e servidor)

Guia de Operações P-CSCF/E-CSCF

Índice

1. [Visão Geral](#)
2. [Papel na Arquitetura IMS](#)
3. [Funções do P-CSCF](#)
4. [Funções do E-CSCF](#)
5. [Operações da Interface Web](#)
6. [Fluxos de Chamadas](#)
7. [Solução de Problemas](#)

Visão Geral

O **P-CSCF** (Proxy Call Session Control Function) é o primeiro ponto de contato para Equipamentos de Usuário (UE) na rede IMS. Ele atua como um proxy de borda que gerencia segurança, aplicação de QoS e roteamento de chamadas de emergência. Nesta implementação, o P-CSCF também funciona como o **E-CSCF** (Emergency CSCF) para serviços de emergência.

Importante: Em nossas implantações, o **P-CSCF não retransmite mídia por padrão**. A mídia flui diretamente entre o UE e o **OmniTAS** (Servidor de Aplicação de Telefonia) ou outros pontos finais de mídia. O P-CSCF é puramente um proxy de sinalização SIP.

Especificações 3GPP

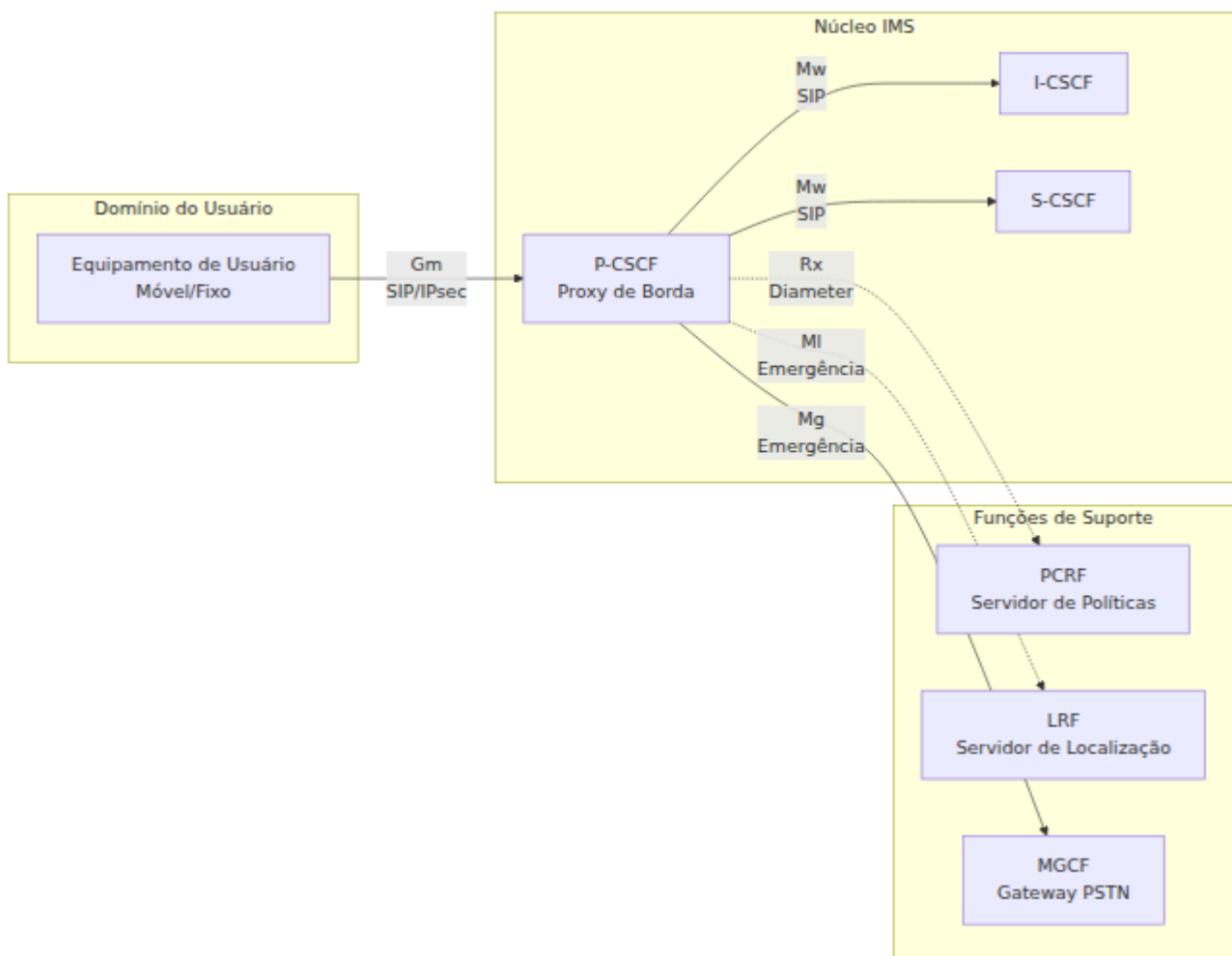
- **3GPP TS 23.228:** Subsistema de Mídia IP (IMS) Fase 2
- **3GPP TS 24.229:** Protocolo de Controle de Chamadas IMS
- **3GPP TS 33.203:** Segurança de acesso para IMS
- **3GPP TS 23.167:** Sessões de emergência do Subsistema de Mídia IP (IMS)

Principais Responsabilidades

1. **Primeiro Ponto de Contato:** Proxy SIP inicial do UE no IMS
2. **Aplicação de Segurança:** Estabelecimento e gerenciamento de túneis IPsec
3. **Controle de QoS:** Interfaces com PCRF via Rx para aplicação de políticas
4. **Serviços de Emergência:** Roteia chamadas de emergência e fornece pesquisa IMEI para MSISDN (função E-CSCF)
5. **Compressão:** Suporte a SigComp para otimização de largura de banda
6. **Suporte a Transporte:** Suporta UDP e TCP

Papel na Arquitetura IMS

Posição na Rede



Pontos de Referência 3GPP

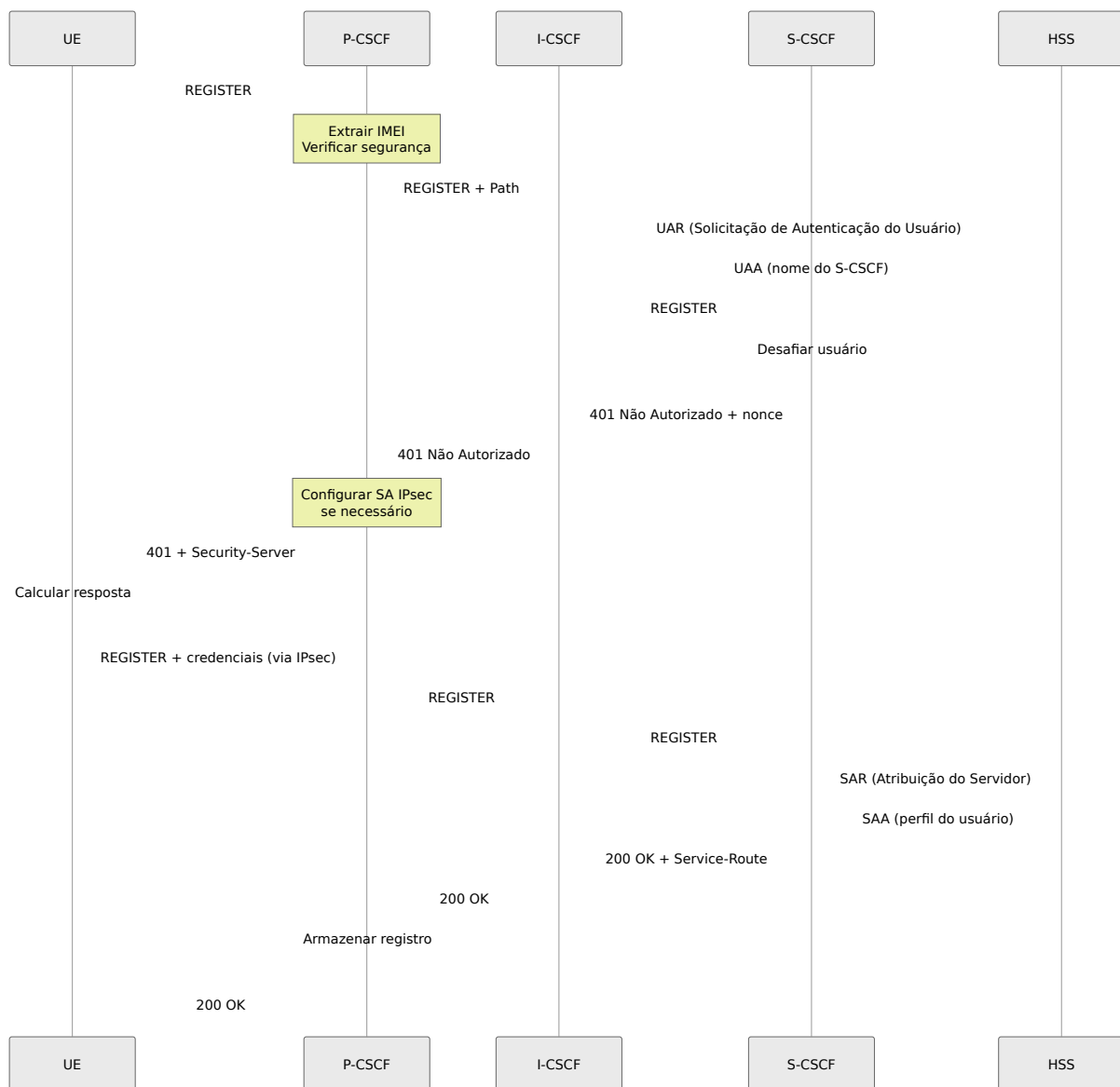
Interface	Protocolo	Propósito	Conectado a
Gm	SIP/IPsec	UE para P-CSCF	Equipamento de Usuário
Mw	SIP	P-CSCF para I-CSCF/S-CSCF	Núcleo IMS
Rx	Diameter	Controle de QoS/Política	PCRF
MI	HTTP/HELD	Recuperação de localização	LRF (E-CSCF)
Mg	SIP	Chamadas de emergência	MGCF/E-CSCF

Funções do P-CSCF

1. Tratamento de Registro

O P-CSCF é o primeiro salto para mensagens SIP REGISTER de UEs.

Fluxo de Registro



Principais Recursos

Inserção do Cabeçalho Path:

```
Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
```

- Garante que solicitações subsequentes sejam roteadas de volta pelo P-CSCF
- Requerido por RFC 3327 para IMS

Aplicação do Timer de Registro:

- Força a expiração do registro para 599 segundos

- Substitui valores solicitados pelo UE para controle da rede

Extração de IMEI:

- Extrai IMEI do cabeçalho Contact: `+sip.instance="<urn:gsma:imei:...>"`
- Armazena em tabela hash para mapeamento de chamadas de emergência

Tratamento Específico de Transporte:

- Dispositivos iOS: Estende a vida útil do TCP para evitar desconexão prematura

2. Funções de Segurança

Gerenciamento de Túneis IPsec

O P-CSCF estabelece túneis IPsec ESP com UEs para sinalização SIP segura.

Configuração do IPsec:

A funcionalidade do IPsec é configurada com os seguintes parâmetros:

- **Endereço de escuta:** 10.4.12.165 (endereço IP do P-CSCF para pontos finais IPsec)
- **Porta do cliente (base):** 5100 (porta inicial para tráfego UE → P-CSCF)
- **Porta do servidor (base):** 6100 (porta inicial para tráfego P-CSCF → UE)
- **Faixa de portas:** Pool configurável de portas (tipicamente 1000-10000 portas)
- **Início do ID SPI:** 4096 (valor inicial para alocação do Índice de Parâmetro de Segurança)
- **Faixa de ID SPI:** 100000 (número de pares de SPI disponíveis para alocação)
- **Máx. conexões:** 20 (máximo de associações de segurança IPsec simultâneas por trabalhador)

Gerenciamento de SPI e Portas

Cada túnel IPsec entre um UE e o P-CSCF requer identificadores exclusivos para manter o tráfego separado e seguro. O sistema gerencia dois tipos de recursos:

Índices de Parâmetro de Segurança (SPIs):

Cada túnel IPsec usa DOIS SPIs - um para cada direção:

- **spi-c** (SPI do cliente): Identifica pacotes enviados do UE para o P-CSCF
- **spi-s** (SPI do servidor): Identifica pacotes enviados do P-CSCF para o UE

Os SPIs são alocados em pares a partir de um pool configurado. O sistema é tipicamente configurado com:

- Valor inicial do SPI: 4096
- Faixa disponível: 100.000 valores de SPI
- Isso fornece capacidade para 50.000 túneis simultâneos (pares são alocados como números consecutivos pares/ímpares)

Alocação de Portas:

Cada túnel também usa portas UDP exclusivas no P-CSCF:

- **porta do cliente**: Porta do P-CSCF onde recebe pacotes IPsec do UE
- **porta do servidor**: Porta do P-CSCF onde envia pacotes IPsec para o UE

Configuração típica de portas:

- Valor inicial da porta do cliente: 5100
- Valor inicial da porta do servidor: 6100
- Faixa de portas: 10.000 portas disponíveis
- As portas retornam ao início quando a faixa é esgotada

Como Funciona a Alocação de Recursos:

Quando um UE se registra e solicita proteção IPsec:

1. **Primeiro Registro**: Recebe spi-c=4096, spi-s=4097, porta do cliente=5100, porta do servidor=6100
2. **Segundo Registro**: Recebe spi-c=4098, spi-s=4099, porta do cliente=5101, porta do servidor=6101
3. **Terceiro Registro**: Recebe spi-c=4100, spi-s=4101, porta do cliente=5102, porta do servidor=6102

E assim por diante...

Após 10.000 registros, as portas retornam ao início (5100, 6100), enquanto os SPIs continuam a incrementar. Isso permite mais túneis do que portas disponíveis, desde que os UEs tenham endereços IP diferentes.

Limites de Recursos:

O número máximo de túneis IPsec simultâneos é determinado pelo limite que for atingido primeiro:

- Capacidade da faixa de SPI (tipicamente 50.000 pares)
- Capacidade da faixa de portas (tipicamente 10.000 portas)
- Memória do sistema e capacidade de processamento

Monitoramento via Interface Web:

Navegue até a página do P-CSCF → Estatísticas IPsec (se disponível) para visualizar:

- Número de túneis IPsec ativos
- Número de pares SPI/porta disponíveis
- Percentual de utilização

Se você observar falhas de registro com erros relacionados ao IPsec, isso pode indicar:

- Esgotamento do pool de SPI (todos os 50.000 pares em uso)
- Esgotamento do pool de portas (todas as 10.000 portas em uso)
- Túneis antigos não sendo limpos corretamente

Quando os Recursos São Liberados:

Os SPIs e portas são retornados ao pool disponível quando:

- Um UE se desregistra (envia REGISTER com Expires: 0)
- Um registro expira sem ser renovado
- Um túnel IPsec é destruído manualmente via interface web
- O administrador do sistema limpa túneis obsoletos

Planejamento de Capacidade:

Para planejamento de implantação:

- Cada túnel ativo usa aproximadamente 1KB de memória
- A implantação típica em produção suporta de 10.000 a 50.000 túneis simultâneos
- Monitore tendências de utilização para prever quando a expansão de capacidade é necessária
- Se regularmente exceder 80% de utilização, coordene com os administradores do sistema para aumentar as faixas de SPI/porta

Configuração da Associação de Segurança (SA):

1. O UE envia REGISTER com o cabeçalho `Security-Client`:

```
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; ealg=null;
                 spi-c=12345; spi-s=67890; port-c=5100; port-
s=6100
```

2. O P-CSCF responde com `Security-Server`:

```
Security-Server: ipsec-3gpp; alg=hmac-sha-1-96; ealg=null;
                 spi-c=11111; spi-s=22222; port-c=5100; port-
s=6100
```

3. O P-CSCF cria políticas IPsec usando `setkey`:

```
# Cliente para Servidor
spdadd <ue-ip>[5100] <pcscf-ip>[6100] any -P out ipsec
esp/transport//require;

# Servidor para Cliente
spdadd <pcscf-ip>[6100] <ue-ip>[5100] any -P in ipsec
esp/transport//require;
```

4. Todas as mensagens SIP subsequentes usam o túnel IPsec

Algoritmos Suportados:

- **Autenticação:** hmac-md5-96, hmac-sha-1-96
- **Criptografia:** null, des-ede3-cbc, aes-cbc (preferido: null para LTE)

3. Tratamento de Mídia

Nota Importante: Em nossas implantações, **o P-CSCF NÃO retransmite mídia por padrão**. A mídia (RTP/SRTP) flui diretamente do UE para **OmniTAS** (Servidor de Aplicação de Telefonia) ou outros pontos finais de mídia. O P-CSCF lida apenas com sinalização SIP.

A mídia flui diretamente entre UEs e o OmniTAS (Servidor de Aplicação de Telefonia), contornando completamente o P-CSCF para tráfego RTP/SRTP:

```
UE <----- SIP -----> P-CSCF <----- SIP -----> S-CSCF <-----  
SIP -----> OmniTAS  
      <----- RTP/SRTP (direto para TAS) -----  
----->
```

O P-CSCF lida apenas com sinalização SIP. Toda a mídia (voz, vídeo) é estabelecida diretamente entre o UE e o OmniTAS.

4. Aplicação de QoS e Políticas (Interface Rx)

Integração Diameter Rx

Propósito: Coordenar QoS com PCRF para estabelecimento de bearer

Configuração Diameter:

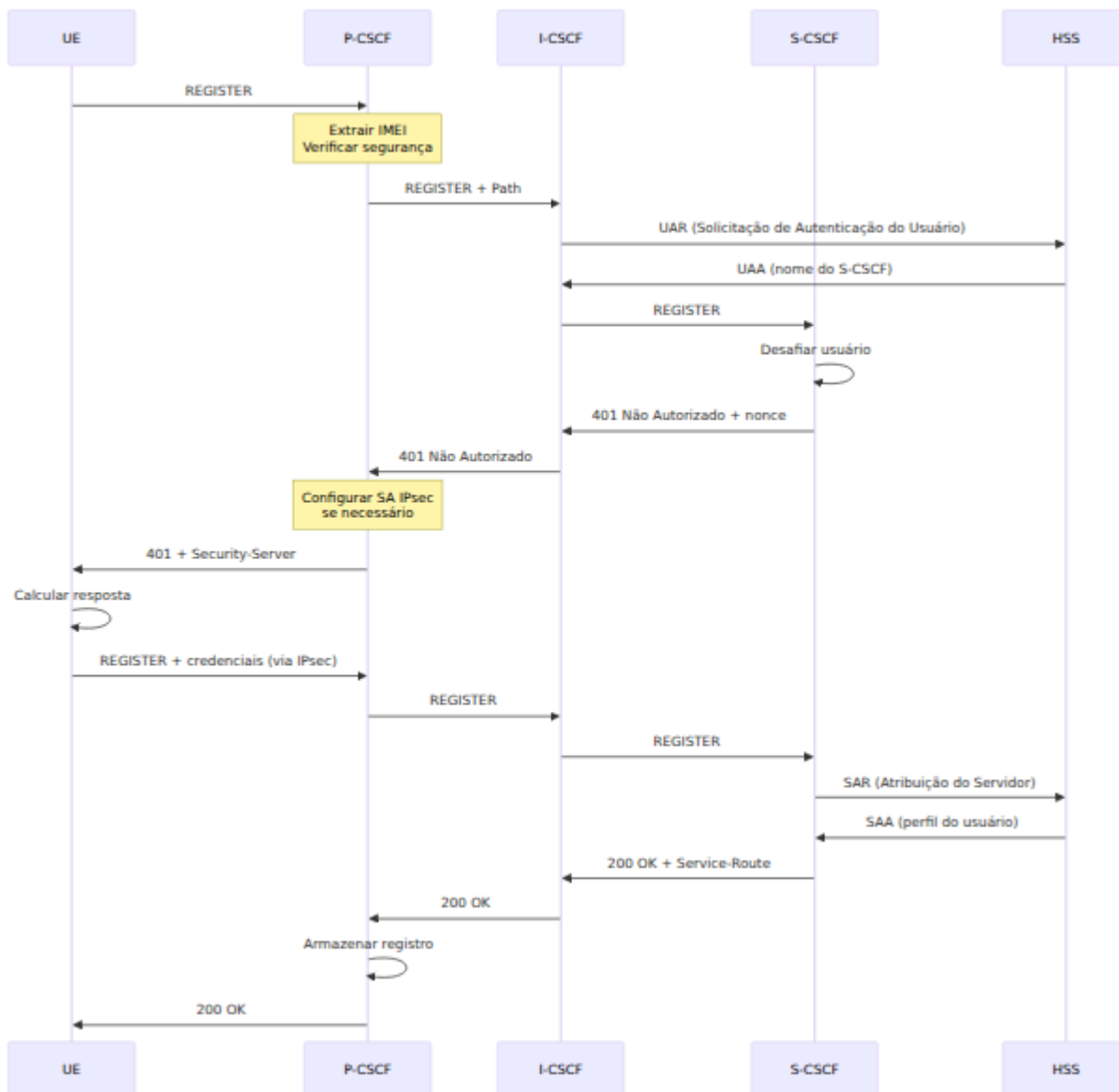
O P-CSCF conecta-se ao PCRF via Diameter na porta 3868 usando a aplicação Rx (ID da Aplicação 16777236, ID do Fornecedor 10415).

Operações Rx:

1. **AAR (Solicitação de Autorização e Autenticação):** Solicitar QoS para fluxo de mídia

2. **AAA (Resposta de Autorização e Autenticação)**: PCRF concede/nega
3. **STR (Solicitação de Terminação de Sessão)**: Liberar QoS no final da chamada

Fluxo de Mensagens AAR



Informações de Mídia Enviadas ao PCRF:

- Descrição do fluxo (IP, porta, protocolo)
- Requisitos de largura de banda (uplink/downlink)
- Tipo de mídia (áudio, vídeo)
- Status do fluxo (habilitado, desabilitado)

5. Proteção Anti-Flood

Configuração do Módulo Pike (Limitação de Taxa): O módulo pike fornece proteção contra inundações com estas configurações:

- **Unidade de tempo de amostragem:** 2 segundos - janela de tempo para medir a taxa de solicitações
- **Densidade de solicitações por unidade:** 16 solicitações permitidas por janela de 2 segundos de um único IP
- **Latência de remoção:** 300 segundos (5 minutos) - duração que um IP é bloqueado após exceder o limite

Rastreamento de Autenticações Falhadas: O P-CSCF rastreia tentativas de autenticação falhadas para prevenir ataques de força bruta:

- Mantém um contador em tabela hash para tentativas de autenticação falhadas por IP de origem
- Incrementa o contador em caso de falha de autenticação com expiração de 120 segundos
- Se um IP exceder 10 tentativas falhadas dentro de 120 segundos, bloqueia o IP com 403 Muitas Tentativas Falhadas
- Impede que atacantes adivinhem credenciais de usuário

Funções do E-CSCF

O P-CSCF inclui funcionalidade E-CSCF para tratamento de chamadas de emergência.

Detecção de Chamadas de Emergência

URIs SIP Reconhecidas:

- `urn:service:sos` (emergência geral)
- `urn:service:sos.police`
- `urn:service:sos.ambulance`
- `urn:service:sos.fire`

- urn:service:sos.marine
- urn:service:sos.mountain

Lógica de Detecção: Chamadas de emergência são detectadas examinando o Request-URI:

- Verifica se o método é INVITE (solicitação de configuração de chamada)
- Verifica se o Request-URI corresponde a padrões de emergência:
 - Formato URN: urn:service:sos* (URNs SOS definidos na RFC 5031)
 - Emergência norte-americana: 911
 - Emergência europeia/internacional: 112
- Se uma chamada de emergência for detectada, roteia para o bloco de tratamento de EMERGÊNCIA para processamento especial

Mapeamento de IMEI para MSISDN para Chamadas de Emergência

Por que isso é necessário: Quando os usuários fazem chamadas de emergência (por exemplo, 911, 112, urn:service:sos), o UE frequentemente **não fornece o MSISDN (número de telefone)** na mensagem SIP. Os serviços de emergência (PSAP - Ponto de Atendimento de Segurança Pública) precisam saber o número de telefone do chamador para fins de retorno de chamada. Para resolver isso, o P-CSCF/E-CSCF mantém um mapeamento de IMEI (identificador do dispositivo) para MSISDN.

Como Funciona:

1. Durante o Registro (quando o MSISDN é conhecido):

- Extrai IMEI do parâmetro +sip.instance do cabeçalho Contact (formato: urn:gsma:imei:123456-78-901234-5)
- Extrai MSISDN da identidade pública do usuário (IMPU) no nome de usuário do cabeçalho From
- Armazena o mapeamento IMEI → MSISDN em uma tabela hash com TTL de 24 horas (86400 segundos)
- Exemplo: imei_msisdn["urn:gsma:imei:123456789012345"] = "12015551234"

- **Em implantações em cluster:** Replica automaticamente o mapeamento para todos os outros nós P-CSCF no cluster

2. **Durante a Chamada de Emergência** (quando o MSISDN pode estar ausente):

- Extrai IMEI do parâmetro +sip.instance do cabeçalho Contact da chamada de emergência
- Realiza uma pesquisa na tabela hash para recuperar o MSISDN associado a este IMEI
- Se o MSISDN for encontrado no mapeamento:
 - Adiciona o cabeçalho P-Asserted-Identity com o MSISDN completo (sip:+12015551234@domínio)
 - Isso fornece ao PSAP o número de retorno de chamada para o chamador de emergência

Alta Disponibilidade - Sincronização de Multi-Nó:

Em implantações de produção com múltiplos nós P-CSCF para redundância, os mapeamentos IMEI→MSISDN são sincronizados automaticamente entre todos os nós:

Comportamento de Replicação em Cluster:

Quando um UE se registra no **Nó P-CSCF 1**:

1. O Nó 1 cria o mapeamento IMEI→MSISDN localmente
2. O Nó 1 imediatamente transmite o mapeamento para todos os outros nós P-CSCF no cluster
3. **Nó P-CSCF 2, Nó 3**, etc. recebem a atualização e criam cópias locais idênticas
4. Todos os nós agora têm o mesmo mapeamento IMEI→MSISDN

Por que isso é importante:

Se um UE se registrou através do Nó P-CSCF 1, mas faz uma chamada de emergência que é roteada para o Nó P-CSCF 2 (devido a balanceamento de carga ou failover), o Nó 2 já tem o mapeamento IMEI→MSISDN e pode fornecer o número de retorno de chamada ao PSAP.

Mecanismo de Sincronização:

A sincronização acontece via mensagens baseadas em SIP entre os nós P-CSCF:

- Usa mensagens SIP personalizadas para propagar atualizações da tabela hash
- As mensagens são enviadas em formato JSON contendo o IMEI, MSISDN e TTL
- A transmissão é automática e transparente - nenhuma intervenção do operador é necessária
- As atualizações são transmitidas para todos os membros do cluster em milissegundos

Impacto nas Operações:

- **Resiliência:** Chamadas de emergência funcionam corretamente, independentemente de qual nó P-CSCF manipula a chamada
- **Sem Ponto Único de Falha:** Qualquer nó P-CSCF pode fornecer o número de retorno de chamada para qualquer UE registrada
- **Automático:** A sincronização é integrada e não requer configuração ou intervenção manual
- **Monitoramento:** Via interface web, navegue até P-CSCF → Tabelas Hash → imei_msisdn para ver mapeamentos em cada nó

Requisitos de Configuração do Cluster:

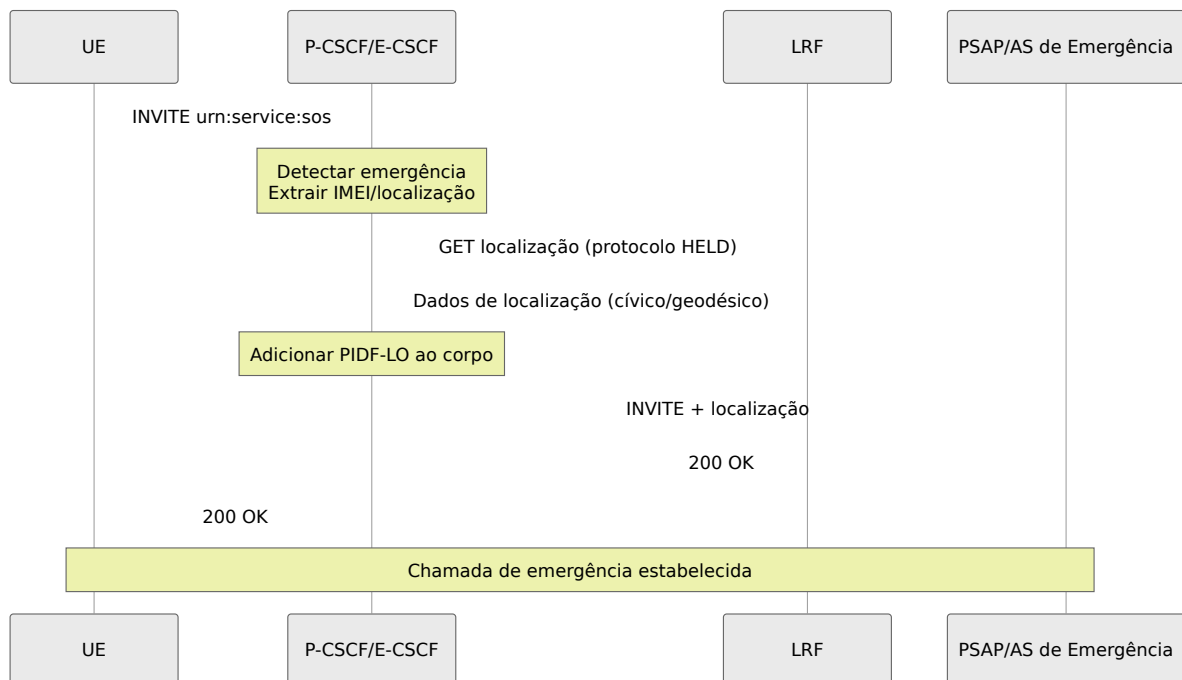
Para que a sincronização da tabela hash funcione:

- Todos os nós P-CSCF devem ser configurados com os endereços uns dos outros
- Os nós se descobrem automaticamente através de notificações de disponibilidade
- A conectividade de rede deve permitir tráfego SIP entre todos os nós P-CSCF
- Se a sincronização falhar, verifique se as regras de firewall permitem comunicação entre nós

Cenário de Exemplo:

1. Usuário registra: IMEI=123456789012345, MSISDN=12015551234
 → Armazenado: imei_msisdn[123456789012345] = 12015551234
2. Usuário disca 911: INVITE urn:service:sos (MSISDN não no cabeçalho From)
 → P-CSCF extrai IMEI do Contact: 123456789012345
 → P-CSCF pesquisa: imei_msisdn[123456789012345] → 12015551234
 → P-CSCF adiciona cabeçalho: P-Asserted-Identity:
 <sip:+12015551234@...>
 → PSAP recebe chamada com número de retorno: +12015551234

Roteamento de Emergência



Recursos de Chamadas de Emergência:

- Ignora verificação de registro
- Adiciona PIDF-LO (Formato de Dados de Presença - Objeto de Localização)
- Roteia para servidor de aplicação de emergência ou PSAP
- Tratamento prioritário (preempção de chamadas normais)
- Informação de localização do LRF ou do UE

Operações da Interface Web

Acessando a Página do P-CSCF

Navegue para: `https://<painel-de-controle>/pcscf`

Layout da Página

A página do P-CSCF tem três guias principais:

1. **Contatos Registrados** - Registros ativos
2. **Localização do Usuário** - Pesquisa por IMSI/IP
3. **Tabelas Hash** - Tabelas de memória compartilhada

Visualizando Contatos Registrados

Colunas de Exibição:

- **AoR** (Endereço de Registro): Identidade SIP do usuário
- **Contato**: URI de contato do dispositivo
- **Expira**: Timestamp de expiração do registro
- **IP Público**: Endereço IP público do UE
- **Recebido**: IP realmente recebido (se diferente do Contato)
- **Path**: Cabeçalho Path para roteamento
- **ID da Sessão Rx**: Sessão Diameter Rx (se QoS ativo)

Recursos:

- Atualização automática a cada 5 segundos
- Pesquisa por AoR ou Contato parcial
- Classificação por coluna (clique no cabeçalho)
- Linhas expansíveis para detalhes completos

Exemplo de Saída:

AoR: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
Contato: sip:12015551234@10.4.12.100:5060;transport=udp
Expira: 2025-11-29 14:30:15
IP Público: 10.4.12.100
Recebido: 10.4.12.100:52341
Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
Sessão Rx: rx-pcscf-session-12345

Pesquisando Localização do Usuário

Opções de Pesquisa:

- Por IMSI: `imsi:310150123456789`
- Por IP: `10.4.12.100`

Casos de Uso:

1. Encontrar qual usuário está usando um IP específico
2. Verificar se o IMSI está registrado
3. Verificar status do túnel IPsec
4. Verificar rotas de serviço

Gerenciamento de Tabelas Hash

Tabelas Comuns:

Tabela	Propósito	Tamanho Típico
<code>imei_msisdn</code>	Mapeamento de emergência IMEI→MSISDN	100-1000 entradas
<code>service_routes</code>	Rotas de serviço em cache	Por registro
<code>dialog_out</code>	Rastreamento de diálogo de saída	Por chamada

Operações:

- **Listar Tabelas:** Clique na guia "Tabelas Hash"
- **Dump da Tabela:** Clique no nome da tabela para visualizar o conteúdo
- **Excluir Entrada:** Clique em "Excluir" ao lado da entrada
- **Limpar Tabela:** Clique em "Limpar" para limpar toda a tabela (use com cautela!)

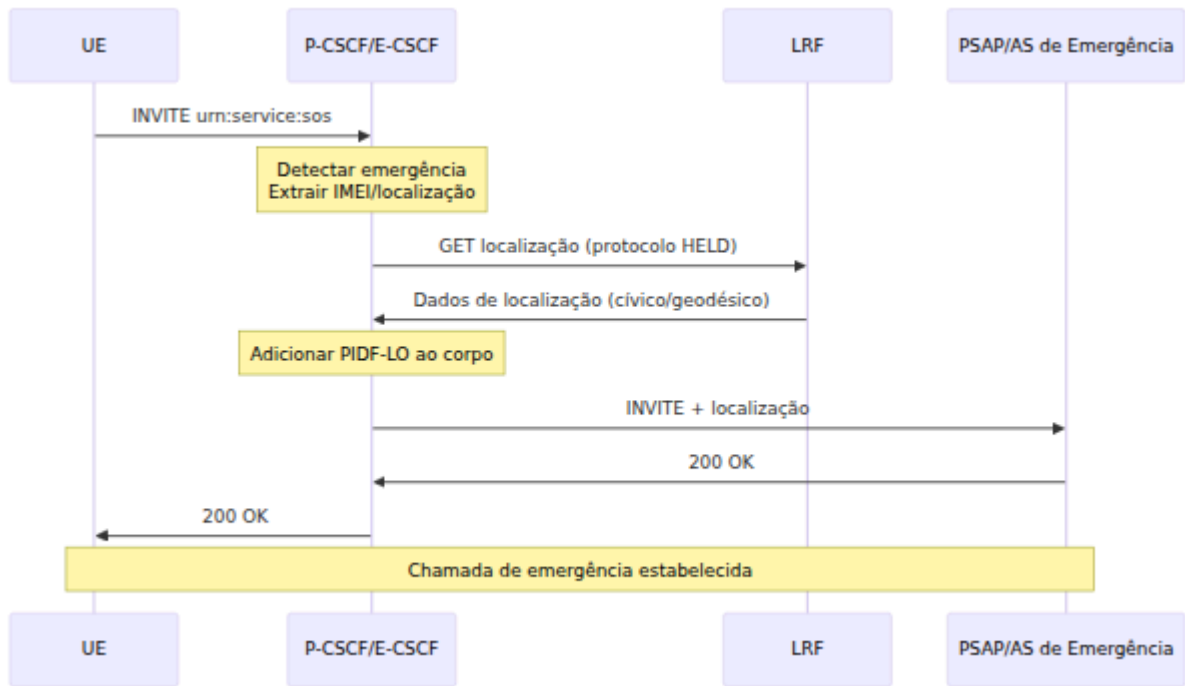
Exemplo de Entrada:

```
Chave: urn:gsma:imei:123456-78-901234-5  
Valor: 310150123456789  
TTL: 86400 segundos (24 horas)
```

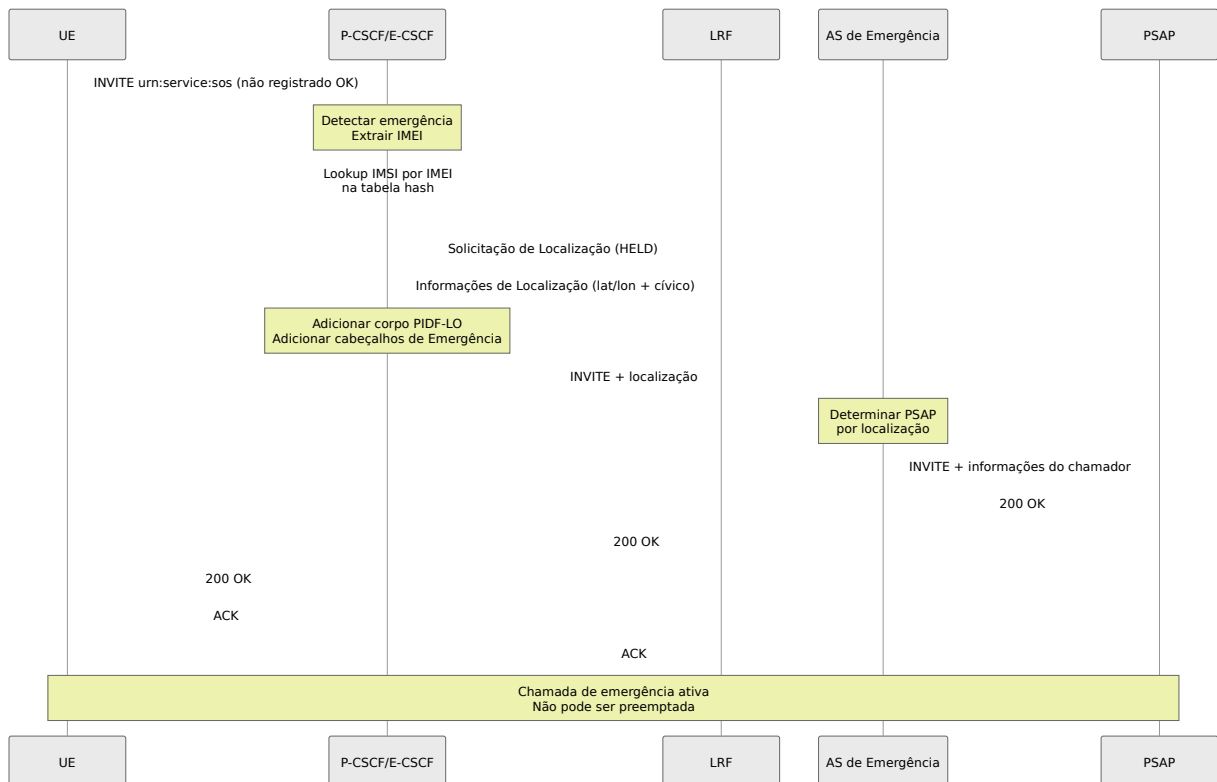
Fluxos de Chamadas

Chamada Originando do Móvel (MO)

Todas as chamadas originadas são roteadas através do TAS (OmniTAS) para lógica de serviço e cobrança:



Fluxo de Chamada de Emergência



Solução de Problemas

Problemas de Registro

UE Não Consegue Registrar

Sintomas: UE recebe 408 Timeout ou nenhuma resposta

Passos de Diagnóstico:

1. Verifique o status de registro via o painel de controle:
 - Navegue até a página do P-CSCF
 - Verifique a guia "Contatos Registrados"
 - Verifique se o usuário aparece na lista
2. Revise os logs do sistema via a página de Logs do painel de controle para erros
3. Verifique a conectividade de rede entre o UE e o P-CSCF
4. Verifique se as regras de firewall permitem tráfego SIP (porta 5060 UDP/TCP)
5. Coordene com os administradores do sistema se o serviço P-CSCF parecer estar fora do ar

Túnel IPsec Não Estabelecido

Sintomas: Desafio 401 enviado, mas re-REGISTER falha

Passos de Diagnóstico:

1. Revise os logs do sistema via a página de Logs do painel de controle para erros relacionados ao IPsec
2. Verifique se o UE está enviando o cabeçalho Security-Client no REGISTER inicial

3. Verifique se o UE está usando portas IPsec (5100 cliente, 6100 servidor) no re-REGISTER
4. Verifique se o endereço recebido corresponde ao ponto final esperado do túnel IPsec
5. Coordene com os administradores do sistema para verificar se os módulos do kernel IPsec estão carregados e se não existem conflitos de porta

Problemas de Chamadas

Chamadas Não Roteiam para o UE

Sintomas: INVITE para P-CSCF, mas UE não toca

Passos de Diagnóstico:

1. Verifique se o registro existe via o painel de controle:
 - Navegue até a página do P-CSCF
 - Verifique a guia "Contatos Registrados"
 - Pesquise o usuário e verifique se o registro está ativo
2. Verifique se o cabeçalho Path foi armazenado no registro
3. Verifique se as chamadas estão sendo enviadas para o endereço de contato correto
4. Revise os logs do sistema para erros de roteamento
5. Verifique se o caminho de rede do P-CSCF para o UE é acessível

Áudio de Uma Via

Sintomas: Uma parte não consegue ouvir a outra

Nota: Em nossas implantações, **o P-CSCF não retransmite mídia**. A mídia flui diretamente entre UE e OmniTAS. Se você está enfrentando áudio de uma via, o problema provavelmente está nos pontos finais ou no roteamento da rede, não no P-CSCF.

Passos de Diagnóstico:

1. Verifique se o SDP no INVITE/200 OK contém endereços IP e portas corretas (revise via logs do sistema ou captura de pacotes, se disponível para administradores)
2. Verifique se as regras de firewall permitem tráfego RTP/SRTP entre UE e OmniTAS
3. Verifique a configuração de NAT se o UE estiver atrás de NAT
4. Verifique se o ponto final de mídia do OmniTAS é acessível a partir do UE (conectividade de rede)
5. Coordene com os administradores do sistema para análise de captura de pacotes, se necessário

Chamadas de Emergência Falham

Sintomas: Chamadas urn:service:sos rejeitadas

Passos de Diagnóstico:

1. Verifique a tabela hash IMEI→MSISDN via o painel de controle:
 - Navegue até P-CSCF → guia Tabelas Hash
 - Verifique se a tabela `imei_msisdn` contém entradas
 - Verifique se o IMEI do chamador tem um mapeamento
2. Teste primeiro com um usuário registrado fazendo uma chamada de emergência (para isolar problemas de registro vs. roteamento de emergência)
3. Revise os logs do sistema via a página de Logs do painel de controle para erros de roteamento de emergência
4. Verifique a configuração do Servidor de Aplicação de Emergência
5. Coordene com os administradores do sistema para revisar a configuração da rota de emergência, se necessário

Problemas de Desempenho

Alta Utilização de CPU

Possíveis Causas:

- Muitos registros
- Acionamento do pike anti-flood
- Consultas lentas no banco de dados

Soluções:

1. Verifique a contagem de registros via o painel de controle:
 - Navegue até P-CSCF → guia Contatos Registrados
 - Revise o número total de registros ativos
2. Revise os logs do sistema para bloqueios do Pike anti-flood
3. Coordene com os administradores do sistema para escalar horizontalmente (adicionar mais instâncias P-CSCF), se necessário

Alta Utilização de Memória

Possíveis Causas:

- Crescimento da tabela hash
- Tabela de diálogo não sendo limpa
- Vazamento de memória

Soluções:

1. Revise as tabelas hash via o painel de controle:
 - Navegue até P-CSCF → guia Tabelas Hash
 - Verifique tamanhos de tabela e contagens de entradas
2. Limpe entradas antigas via o painel de controle:
 - Selecione a tabela hash problemática

- Use a operação "Limpar" se necessário (use com cautela - limpa toda a tabela)
3. Coordene com os administradores do sistema para reiniciar o serviço P-CSCF se um vazamento de memória for suspeito

Problemas Diameter/Rx

Par Diameter do PCRF Fechado

Sintomas: O par Diameter mostra estado "Fechado" na Interface Web

Passos de Diagnóstico:

1. Verifique o status do par Diameter via o painel de controle:
 - Navegue até a página Diameter
 - Selecione o nó P-CSCF
 - Verifique o estado do par PCRF (deve ser "I_Open" quando conectado)
2. Verifique a conectividade de rede com o PCRF (coordene com a equipe de rede, se necessário)
3. Tente habilitar o par via o painel de controle:
 - Navegue até a página Diameter
 - Encontre o par PCRF
 - Clique no botão "Habilitar"
4. Revise os logs do sistema via a página de Logs do painel de controle para erros de conexão Diameter
5. Coordene com os administradores do sistema para verificar a configuração Diameter, se necessário

QoS Não Funciona

Sintomas: Chamadas se conectam, mas nenhum bearer de QoS é estabelecido

Passos de Diagnóstico:

1. Revise os logs do sistema via o painel de controle para mensagens AAR (Solicitação de Autorização e Autenticação) e AAA (Resposta de Autorização e Autenticação)
2. Verifique o código de resultado da resposta do PCRF (deve ser 2001 para sucesso)
3. Verifique se o par PCRF está conectado (veja seção anterior)
4. Verifique se as informações de mídia no SDP estão sendo enviadas corretamente ao PCRF
5. Coordene com os administradores do sistema para verificar a configuração de QoS, se necessário

Melhores Práticas

Segurança

1. **Sempre use IPsec** para dispositivos móveis (LTE/5G)
2. **Habilite TLS** para clientes fixos/empresariais
3. **Configure anti-flood** (Pike) para proteção contra DoS
4. **Limite tentativas de autenticação** falhadas para prevenir força bruta
5. **Use cifras fortes** para TLS (desative SSLv2/v3)
6. **Rotacione regularmente** chaves IPsec (via re-registro)

Desempenho

1. **Ajuste hash_size** com base nos registros esperados:
 - 1.000 usuários: hash_size=10 (cria $2^{10} = 1.024$ buckets hash)
 - 10.000 usuários: hash_size=13 (cria $2^{13} = 8.192$ buckets hash)
 - 100.000 usuários: hash_size=16 (cria $2^{16} = 65.536$ buckets hash)
2. **Ajuste processos de trabalho** com base nos núcleos da CPU:

- Defina filhos para corresponder ao número de núcleos da CPU para processamento SIP
- Defina tcp_children para 2× núcleos da CPU para manipulação de conexões TCP

3. Use **mlock_pages** para prevenir swapping:

- Habilite mlock_pages=yes para bloquear páginas de memória compartilhada na RAM
- Previne degradação de desempenho devido ao swapping de memória para disco

4. **Desative o cache DNS** para ambientes IMS:

- Defina dns_cache_init=off para usar consultas DNS frescas
- Necessário para balanceamento de carga baseado em DNS dinâmico SRV

5. **Habilite balanceamento de carga SRV**:

- Defina dns_srv_lb=yes para distribuir tráfego entre vários servidores
- Usa registros DNS SRV para distribuição automática de carga

Monitoramento

1. **Habilite métricas Prometheus** (porta 9090 na configuração) - Veja [Referência de Métricas](#) para todas as métricas P-CSCF disponíveis
2. **Monitore tendências de contagem de registros**
3. **Rastreie a saúde do par Diameter** (Rx para PCRF)
4. **Alerta sobre altas taxas de erro** nos logs
5. **Monitore a contagem de diálogos** (sessões ativas)
6. **Verifique o uso de memória** regularmente

Alta Disponibilidade

1. **Implante múltiplas instâncias P-CSCF**
2. **Use DNS SRV** para balanceamento de carga:

```
_sip._udp.pcscf.example.com. SRV 10 50 5060
pcscf01.example.com.
_sip._udp.pcscf.example.com. SRV 10 50 5060
pcscf02.example.com.
```

3. **Evite estado** sempre que possível (proxy sem estado)
4. **Use banco de dados compartilhado** para dados persistentes (se necessário)
5. **Monitore via interface web** usando verificações de saúde do painel de controle

Serviços de Emergência

1. **Sempre permita** chamadas de emergência, mesmo se não registradas
2. **Armazene mapeamento IMEI→MSISDN** durante o registro
3. **Defina TTL** para tabela hash de emergência (86400 = 24 horas)
4. **Teste regularmente** com PSAP de teste
5. **Garanta conectividade LRF** para localização
6. **Tratamento prioritário** para chamadas de emergência

Referência

Recursos Técnicos Adicionais

Para administradores de sistema e desenvolvedores, a documentação técnica do módulo está disponível online para os componentes de software subjacentes.

Especificações 3GPP

- **TS 23.228:** Arquitetura IMS
- **TS 24.229:** Perfil SIP IMS
- **TS 33.203:** Segurança de Acesso

- **TS 23.167**: Serviços de Emergência
- **TS 29.214**: Interface Rx (PCRF)

RFCs

- **RFC 3261**: SIP
- **RFC 3327**: Cabeçalho Path
- **RFC 3608**: Cabeçalho Service-Route
- **RFC 3GPP-IMS**: P-Headers (P-Asserted-Identity, etc.)
- **RFC 5626**: Outbound (gerenciamento de conexão)

Guia de Operações do S-CSCF

Índice

1. Visão Geral
2. Papel na Arquitetura IMS
3. Funções do S-CSCF
4. Operações da Interface Web
5. Fluxos de Chamadas
6. Solução de Problemas

Visão Geral

O **S-CSCF** (Serving Call Session Control Function) é o servidor central de controle de sessão no núcleo IMS. Ele realiza registro, autenticação, roteamento de sessão e acionamento de serviços. O S-CSCF é o registrador autoritativo para usuários em sua rede local e mantém o estado completo da sessão para todas as chamadas.

Especificações 3GPP

- **3GPP TS 23.228**: Subsistema de Mídia IP (IMS) Etapa 2
- **3GPP TS 24.229**: Protocolo de Controle de Chamadas IMS
- **3GPP TS 29.228**: Interface Cx (S-CSCF para HSS)
- **3GPP TS 29.229**: Protocolos Cx e Dx
- **3GPP TS 23.218**: Interface ISC (S-CSCF para AS)
- **3GPP TS 32.260**: Cobrança IMS

Principais Responsabilidades

1. **Autoridade de Registro:** Registrador SIP autoritativo para usuários da rede local
2. **Autenticação:** Valida credenciais de usuários via HSS
3. **Roteamento de Sessão:** Roteia chamadas de origem e término
4. **Acionamento de Serviços:** Invoca Servidores de Aplicação com base em iFC (Critérios de Filtro Iniciais)
5. **Gerenciamento de Perfis de Usuário:** Armazena e aplica perfis de serviço do HSS
6. **Presença:** Gerencia SUBSCRIBE/PUBLISH/NOTIFY para serviços de presença
7. **Interconexão PSTN:** Roteia para/de redes PSTN legadas

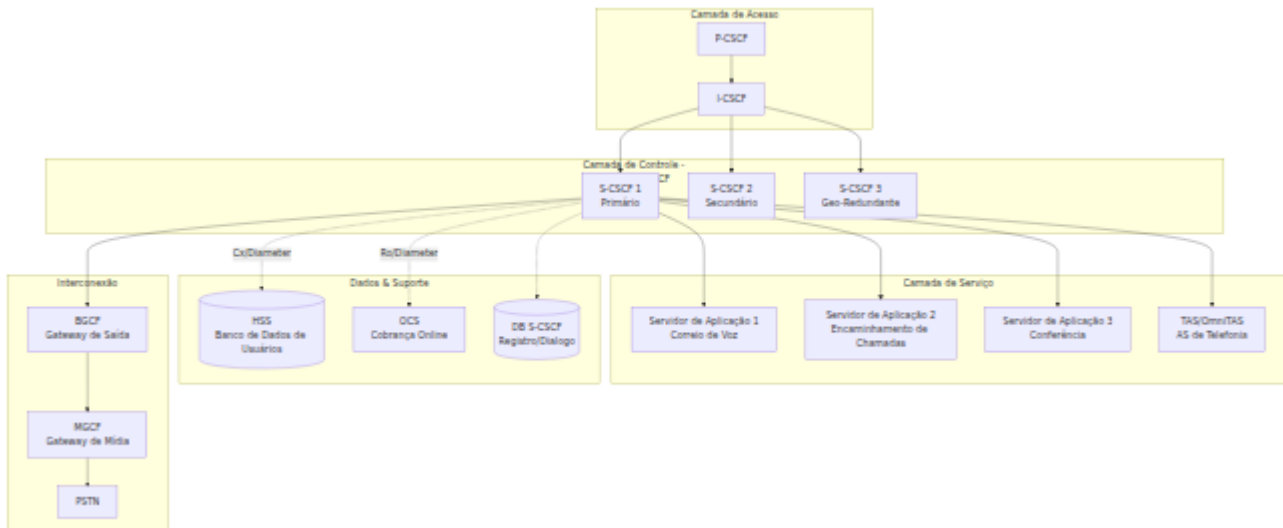
Nota sobre Cobrança: Embora o S-CSCF tenha a capacidade de realizar cobrança online via a interface Ro para um OCS (Sistema de Cobrança Online), **em nossas implementações, essa funcionalidade é tipicamente desativada.** A cobrança é tratada pelo **TAS (Servidor de Aplicação de Telefonia)**, onde pode contabilizar adequadamente cenários complexos, como encaminhamento de chamadas, transferência de chamadas, roaming em redes 2G/3G e outros serviços suplementares que o S-CSCF sozinho não pode rastrear com precisão.

Características Principais

- **Com Estado:** Mantém o estado completo do diálogo
- **Lógica de Serviço:** Executa regras de roteamento complexas e acionamentos de serviços
- **Integração com HSS:** Sincronização contínua com o banco de dados de usuários
- **Interface de Servidor de Aplicação:** ISC (Controle de Serviço IMS)
- **CSCF Mais Complexo:** Maior configuração e mais recursos

Papel na Arquitetura IMS

Posição na Rede



Pontos de Referência 3GPP

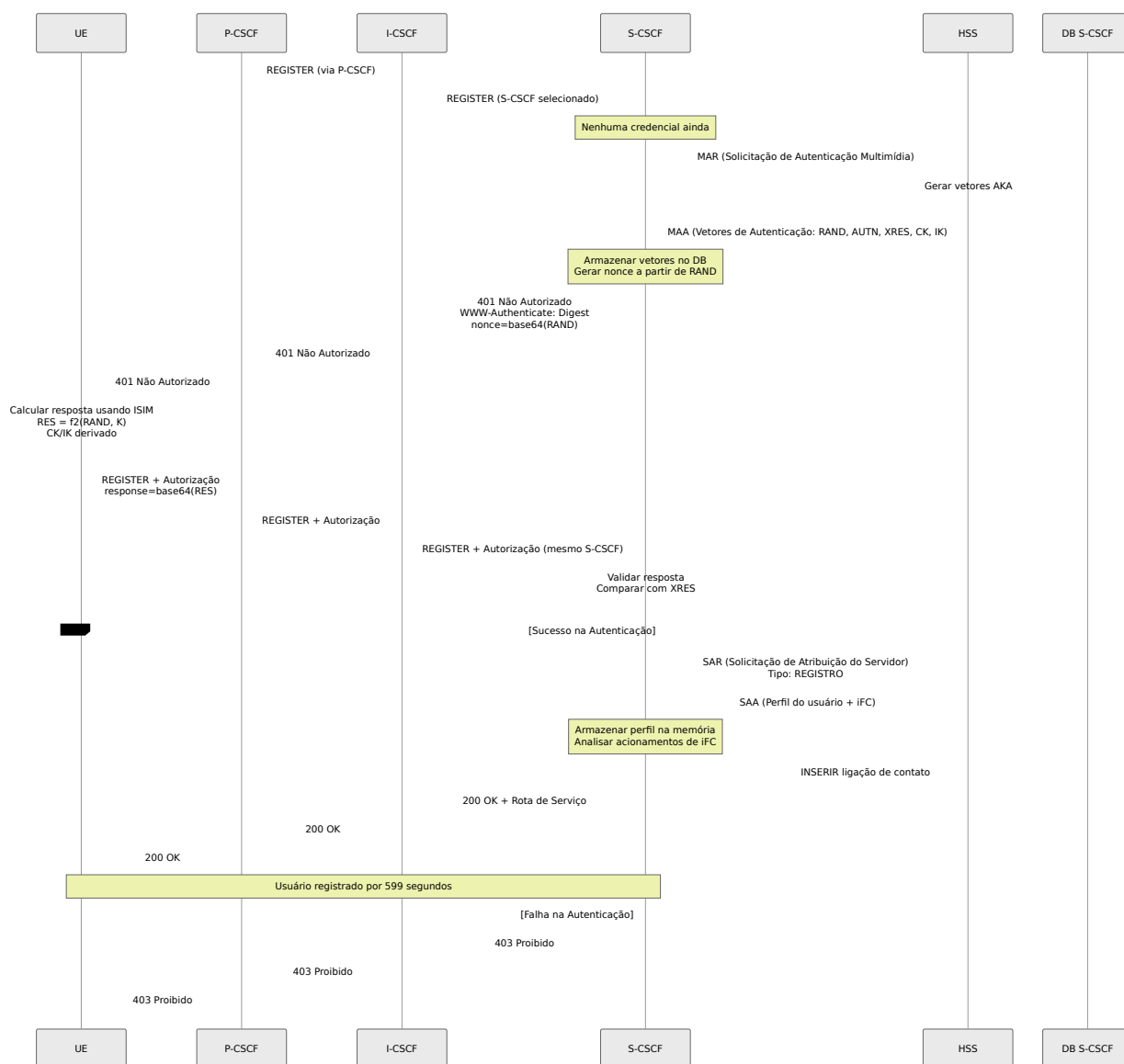
Interface	Protocolo	Propósito	Conectado a
Mw	SIP	I-CSCF/P-CSCF para S-CSCF	I-CSCF, P-CSCF
ISC	SIP	S-CSCF para Servidor de Aplicação	AS, TAS
Cx	Diameter	Dados do usuário, autenticação, registro	HSS
Ro	Diameter	Cobrança online (em tempo real)	OCS
Rf	Diameter	Cobrança offline (CDR)	CDF/CGF
Mi	SIP	S-CSCF para BGCF	BGCF (roteamento PSTN)

Funções do S-CSCF

1. Registro e Autenticação

O S-CSCF é o registrador autoritativo que valida as credenciais do usuário e armazena as ligações de registro.

Fluxo de Registro com Autenticação



Algoritmos de Autenticação Suportados

Configuração: O S-CSCF é configurado com os seguintes parâmetros de autenticação:

- Tempo limite do vetor de autenticação: 599 segundos
- Tamanho do hash de dados de autenticação: 1024 buckets
- Verifica apenas IMPU para autenticação (não IMPI)

Algoritmos Suportados:

- **AKAv1-MD5**: 3GPP AKA com MD5 (mais comum para LTE/5G)
- **AKAv2-MD5**: AKA aprimorado
- **MD5**: Digest HTTP
- **CableLabs-Digest**: PacketCable/IMS para redes de cabo
- **3GPP-Digest**: Variante Digest-MD5
- **TISPAN-HTTP_DIGEST_MD5**: ETSI TISPAN
- **HSS-Selecionado**: Permitir que o HSS escolha o algoritmo

Fluxo AKA:

1. **RAND**: Desafio aleatório (128 bits)
2. **AUTN**: Token de autenticação para provar a identidade do HSS
3. **XRES**: Resposta esperada do UE
4. **CK/IK**: Chave de Cifra / Chave de Integridade para IPsec

Geração de Nonce:

```
nonce = base64(RAND) + ":" + algorithm_indicator
```

Validação de Resposta:

```
UE_response = base64(RES)
Expected = base64(XRES)

if (UE_response == Expected) {
    # Sucesso na autenticação
} else {
    # Falha na autenticação
}
```

Re-Sincronização AKA

Se o número de sequência (SQN) do UE estiver fora de sincronia com o HSS:

Processo:

1. UE envia AUTS (token de sincronização de autenticação) no cabeçalho de Autorização
2. S-CSCF extrai AUTS do cabeçalho
3. S-CSCF envia MAR (Solicitação de Autenticação Multimídia) com AUTS para HSS
4. HSS re-sincroniza seu número de sequência e envia novos vetores de autenticação
5. S-CSCF recebe novos vetores e continua o fluxo de autenticação

Parâmetros de Registro

O S-CSCF é configurado com os seguintes parâmetros de registro:

Tempos de Expiração de Registro:

- Expira: padrão/min/max: 599 segundos (aproximadamente 10 minutos)
- Expiração padrão/min/max de assinatura: 599 segundos

Gerenciamento de Contatos:

- Máximo de contatos por IMPU: 1 (registro de dispositivo único)
- Comportamento máximo de contato: Sobrescrever o mais antigo (quando o limite é excedido, remover o contato mais antigo)

2. Banco de Dados de Localização do Usuário (USRLOC)

O S-CSCF mantém um banco de dados de usuários registrados e suas ligações de contato.

Estrutura do Banco de Dados

O S-CSCF mantém várias tabelas de banco de dados para armazenar informações de registro e usuário:

Tabela IMPU: Armazena Identidades Públicas Multimídia IP (os URIs SIP com os quais os usuários se registram). Cada IMPU tem atributos como:

- Identidade pública (sip:user@domain.com)
- Tipo (identidade de usuário público vs. identidade de serviço público)
- Status de proibição
- Estado de registro (registrado/não registrado)
- Endereços de função de cobrança (CCF1, CCF2, ECF1, ECF2)

Tabela de Contato IMPU: Armazena as ligações de contato reais para cada IMPU, incluindo:

- URI de contato (onde alcançar o dispositivo)
- Tempo de expiração
- Cabeçalho de caminho (rota de volta através do P-CSCF)
- String User-Agent
- Endereço recebido (IP real de onde o REGISTER veio)

Tabela de Assinantes: Mapeia IMPIs (Identidades Privadas) para seus IMPUs associados. Uma identidade privada pode ter várias identidades públicas.

Tabela de Perfil de Serviço: Armazena o perfil XML do usuário recebido do HSS durante o registro, incluindo Critérios de Filtro Iniciais (iFC) para acionamento de serviços.

Configuração da Tabela Hash

O S-CSCF usa uma tabela hash em memória para buscas rápidas de registro. Para implementações com mais de 20.000 usuários, o tamanho da hash deve ser ajustado adequadamente (por exemplo, 8.192 buckets para ~50.000 usuários) para manter o desempenho de busca.

Gerenciando Registros via Interface Web

Todas as operações de localização de usuários podem ser realizadas através da **interface da web do painel de controle** em `/scscf`:

- **Aba Lista de Registro:** Visualizar todos os usuários registrados com paginação e pesquisa

- **Aba Localização do Usuário:** Consultar detalhes específicos do IMPU, incluindo todas as ligações de contato
- **Ações Rápidas:** Pesquisar, desregistrar, despejar IFC e testar operações de IFC

A interface da web fornece uma visão em tempo real do status de registro, ligações de contato e permite ações administrativas, como desregistro forçado quando necessário para solução de problemas.

3. Critérios de Filtro Iniciais (iFC) e Acionamento de Serviços

O S-CSCF avalia **iFC** (Critérios de Filtro Iniciais) do perfil de serviço do usuário para determinar quando invocar Servidores de Aplicação.

Estrutura de iFC (XML)

Exemplo do Perfil do Usuário HSS:

```

<IMSSubscription>
  <PrivateID>user@ims.mnc001.mcc001.3gppnetwork.org</PrivateID>
  <ServiceProfile>
    <PublicIdentity>

<Identity>sip:user@ims.mnc001.mcc001.3gppnetwork.org</Identity>
  <IdentityType>0</IdentityType>  <!-- 0=identidade de usuário
público -->
  </PublicIdentity>

  <InitialFilterCriteria>
    <Priority>0</Priority>  <!-- Menor = maior prioridade -->
    <TriggerPoint>
      <ConditionTypeCNF>1</ConditionTypeCNF>  <!-- 0=DNF, 1=CNF
-->
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>INVITE</Method>
      </SPT>
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <SessionCase>0</SessionCase>  <!-- 0=originando -->
      </SPT>
    </TriggerPoint>
    <ApplicationServer>

<ServerName>sip:tas.ims.mnc001.mcc001.3gppnetwork.org</ServerName>
  <DefaultHandling>0</DefaultHandling>  <!--
0=SESSÃO_CONTINUADA, 1=SESSÃO_TERMINADA -->
  </ApplicationServer>
</InitialFilterCriteria>

  <InitialFilterCriteria>
    <Priority>1</Priority>
    <TriggerPoint>
      <ConditionTypeCNF>0</ConditionTypeCNF>  <!-- DNF -->
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <RequestURI>^sip:\+1800.*</RequestURI>  <!-- Gratuito --
>

```

```
</SPT>
</TriggerPoint>
<ApplicationServer>
  <ServerName>sip:tollfree-as.example.com</ServerName>
  <DefaultHandling>0</DefaultHandling>
</ApplicationServer>
</InitialFilterCriteria>
</ServiceProfile>
</IMSSubscription>
```

Acionamentos de Ponto de Serviço (SPT)

Tipos de SPT:

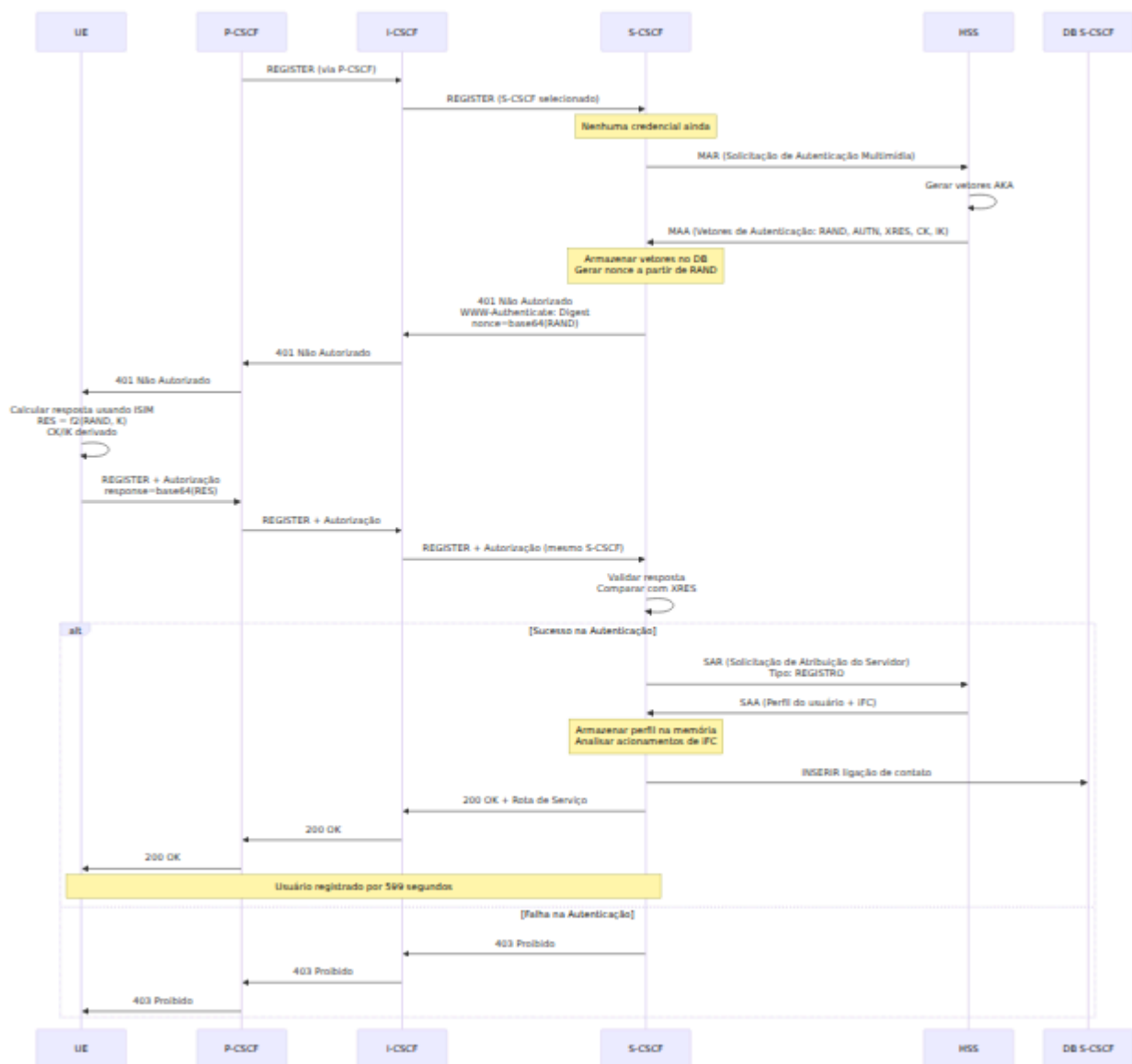
1. **Método:** Método SIP (INVITE, MESSAGE, SUBSCRIBE, etc.)
2. **RequestURI:** Regex no Request-URI
3. **SIPHeader:** Verificar a presença/valor do cabeçalho SIP
4. **SessionCase:** Originando (0), Terminando (1), Terminando Não Registrado (2)
5. **SessionDescription:** Conteúdo SDP (tipo de mídia, codec, etc.)

Lógica:

- **CNF** (Forma Normal Conjuntiva): E de OU - (A OU B) E (C OU D)
- **DNF** (Forma Normal Disjuntiva): OU de E - (A E B) OU (C E D)

Grupo: SPTs com o mesmo número de grupo são OR'd juntos, depois os grupos são AND'd (para CNF).

Fluxo de Correspondência de iFC



Teste de iFC via Interface Web

O painel de controle fornece duas operações através da interface web:

1. **Despejar iFC:** Mostrar todos os iFC para um usuário - exibe a estrutura XML completa de pontos de acionamento e roteamento de Servidores de Aplicação
2. **Testar iFC:** Simular uma chamada para ver qual AS seria acionado - testa um cenário de chamada hipotético com IMPU especificado, URI de origem e URI de destino para determinar qual iFC corresponderia

Fluxo de Trabalho da Interface Web:

1. Navegar até a página S-CSCF

2. Clicar na aba "IFC"
3. Inserir IMPU
4. Escolher "Despejar IFC" ou "Testar IFC"
5. Visualizar estrutura detalhada de iFC com pontos de acionamento e roteamento de AS

4. Gerenciamento de Diálogos

O S-CSCF mantém o estado completo do diálogo SIP para todas as chamadas ativas.

Banco de Dados de Diálogos

O S-CSCF mantém uma tabela de diálogo que rastreia chamadas ativas com as seguintes informações:

- Call-ID (identificador único para o diálogo SIP)
- URIs e tags de From/To
- Números de sequência do chamador e do chamado (CSeq)
- Conjuntos de rota para ambas as partes
- Endereços de contato
- Informações de socket
- Estado do diálogo e timestamps
- Valores de timeout

Estados do Diálogo

Os diálogos transitam por três estados:

- **Inicial:** Resposta provisória recebida (ex: 180 Tocando)
- **Confirmado:** 200 OK recebido e ACK enviado/recebido (chamada ativa)
- **Deletado:** BYE enviado/recebido (chamada encerrada)

Configuração do Diálogo

O módulo de diálogo é configurado para:

- Detectar roteamento espiral (mesmo pedido passando várias vezes)

- Manter perfis separados para os lados de origem e término
- Persistir diálogos no banco de dados (modo de gravação com atualizações periódicas)
- Definir timeouts específicos do diálogo
- Rastrear conjuntos de rota para roteamento adequado em diálogo

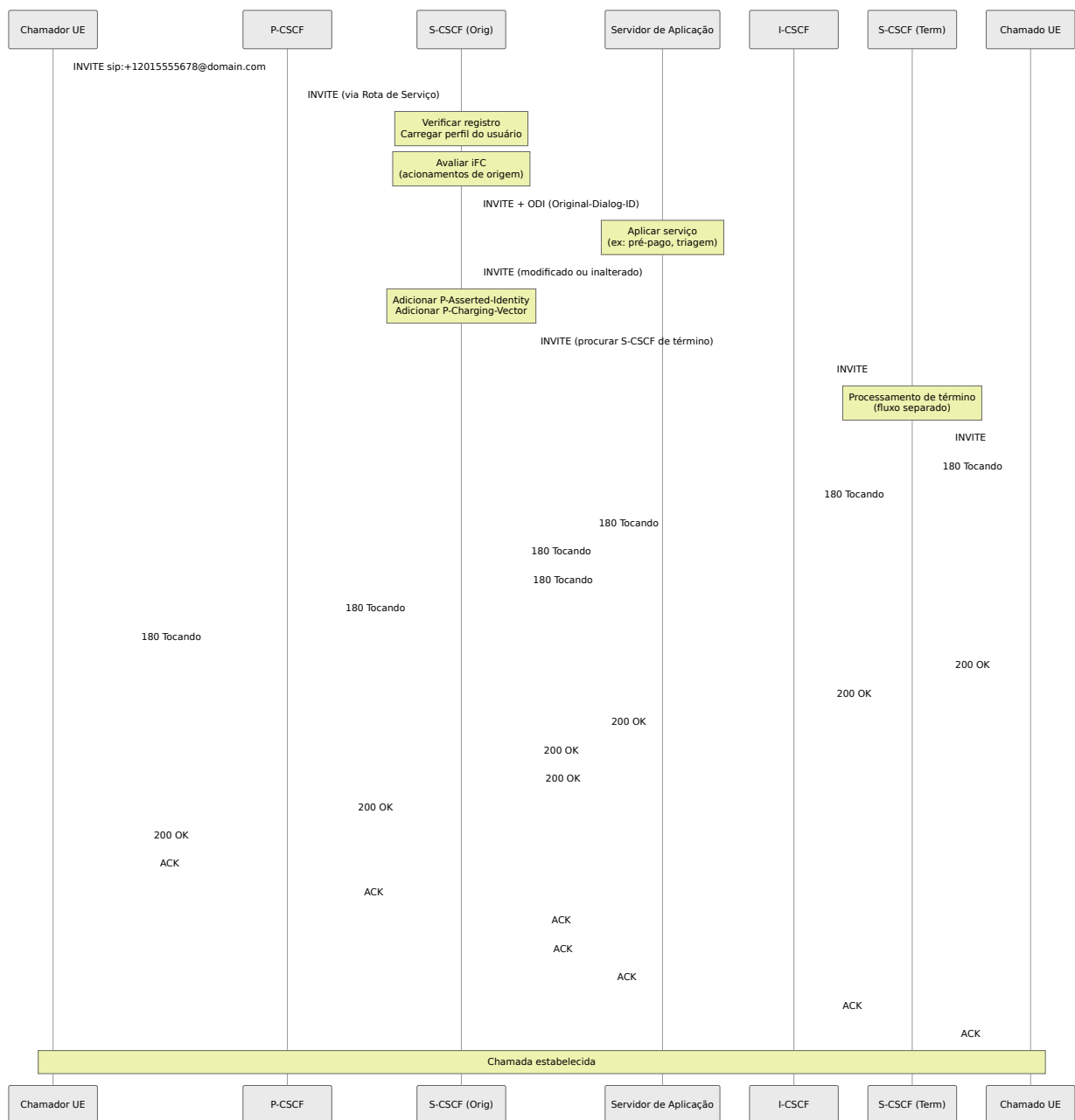
Operações da Interface Web:

1. Navegar até S-CSCF → aba Diálogos
2. Visualizar chamadas ativas com:
 - Call-ID
 - URIs de From/To
 - Estado (Inicial/Confirmado)
 - Hora de início
 - Timeout
3. Clicar em "Encerrar Diálogo" para encerrar chamada específica
4. Clicar em "Encerrar Todos os Diálogos Ativos" para terminação em massa de emergência

5. Manipulação de Chamadas de Origem

Quando um usuário registrado inicia uma chamada, o S-CSCF a processa como uma sessão **de origem**.

Fluxo de Chamadas de Origem



Configuração de Rota de Origem

Processamento de Chamadas de Origem: O S-CSCF realiza várias etapas de validação e roteamento ao processar chamadas de origem:

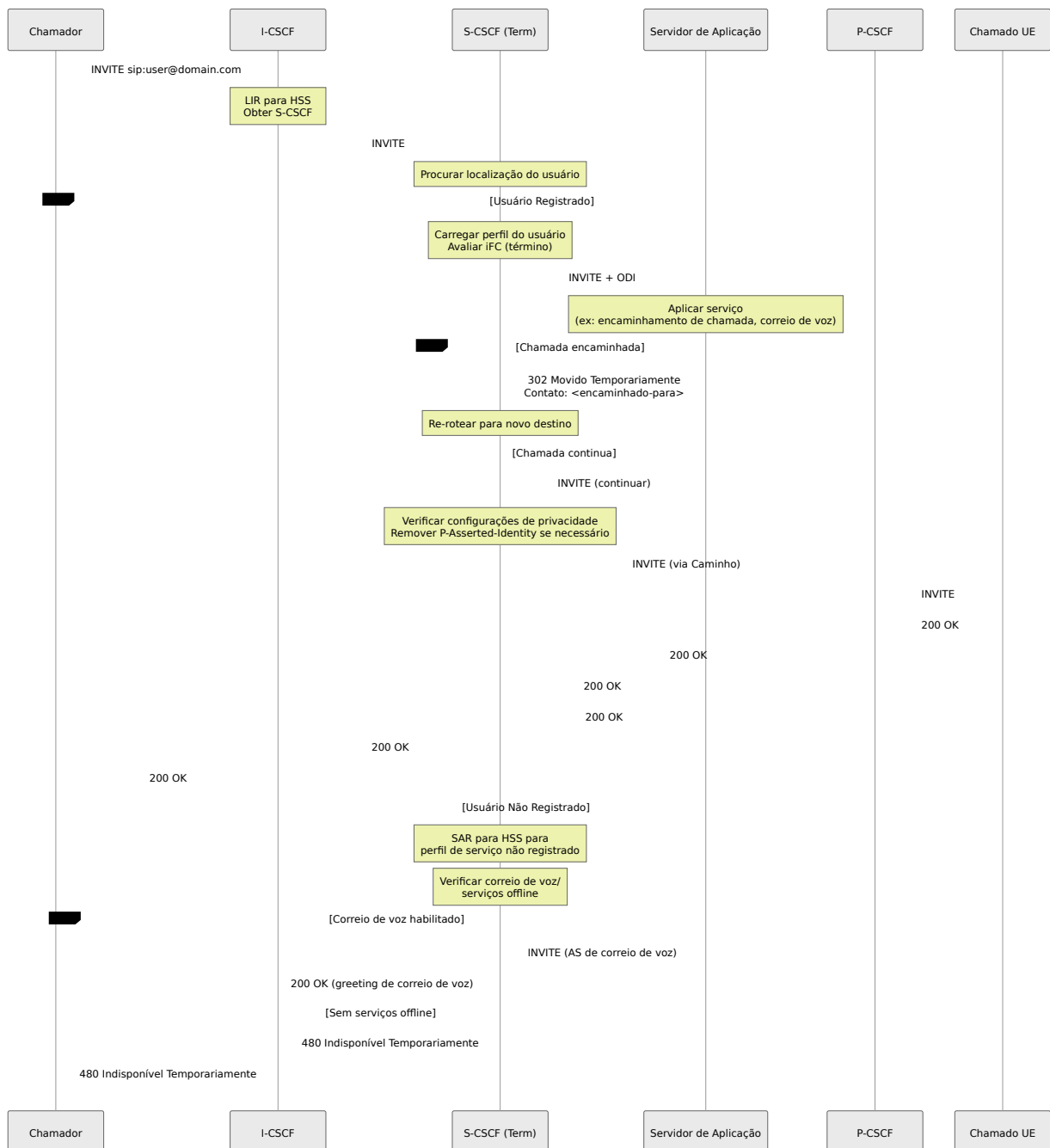
- 1. Verificação de Registro:** Verifica se o usuário chamador está atualmente registrado. Se não, a chamada é rejeitada com uma resposta 403 Proibido.
- 2. Gerenciamento de Cabeçalho de Identidade:**
 - Remove quaisquer cabeçalhos P-Asserted-Identity existentes da solicitação

- Adiciona um novo cabeçalho P-Asserted-Identity contendo a identidade do chamador autenticado
3. **Correlação de Cobrança:** Cria e adiciona um cabeçalho P-Charging-Vector contendo:
 - Identificador de Cobrança IMS (icid) gerado a partir do Call-ID e timestamp
 - Identificador de Operador de Origem (orig-ioi) para cobrança entre operadores
 4. **Acionamento de Serviços:** Avalia os Critérios de Filtro Iniciais (iFC) para acionamentos de sessão de origem para determinar se algum Servidor de Aplicação deve ser invocado
 5. **Cobrança Online** (se habilitada): Inicia uma Solicitação de Controle de Crédito Diameter Ro (CCR) com tipo de evento "0" (solicitação inicial) para chamadas de origem
 6. **Rastreamento de Diálogo:** Atribui a chamada ao perfil de diálogo "orig" (de origem) para fins de rastreamento
 7. **Decisão de Roteamento:** Roteia a chamada para tratamento PSTN (se o destino for um número de telefone) ou para o I-CSCF de término para roteamento IMS

6. Manipulação de Chamadas de Término

Quando uma chamada é destinada a um usuário registrado, o S-CSCF a processa como **término**.

Fluxo de Chamadas de Término



Configuração de Rota de Término

Processamento de Chamadas de Término: O S-CSCF lida com chamadas de término tentando primeiro localizar o usuário chamado e, em seguida, aplicando a lógica de serviço apropriada:

- Consulta de Localização do Usuário:** Consulta o banco de dados de registro para determinar se o usuário chamado está atualmente registrado
 - Usa o nome de usuário e domínio do Request-URI para construir o IMPU

- Recupera ligações de contato e informações de roteamento se registrado

2. Se o Usuário NÃO Estiver Registrado:

- Tenta recuperar o perfil de serviço não registrado do HSS via Solicitação de Atribuição do Servidor (SAR)
- Se bem-sucedido, avalia iFC para acionamentos de sessão "terminando" (ex: correio de voz, serviços offline)
- Se nenhum serviço não registrado estiver disponível, responde com 480 Indisponível Temporariamente

3. Se o Usuário ESTIVER Registrado:

- Avalia iFC para acionamentos de sessão "terminando" para determinar a invocação do Servidor de Aplicação
- Inicia a cobrança online (se habilitada) enviando Diameter Ro CCR com tipo de evento "0" para chamadas de término
- Atribui a chamada ao perfil de diálogo "term" (de término) para rastreamento
- Encaminha o INVITE para o P-CSCF registrado usando o cabeçalho Path armazenado durante o registro

7. Interconexão PSTN via OmniTAS

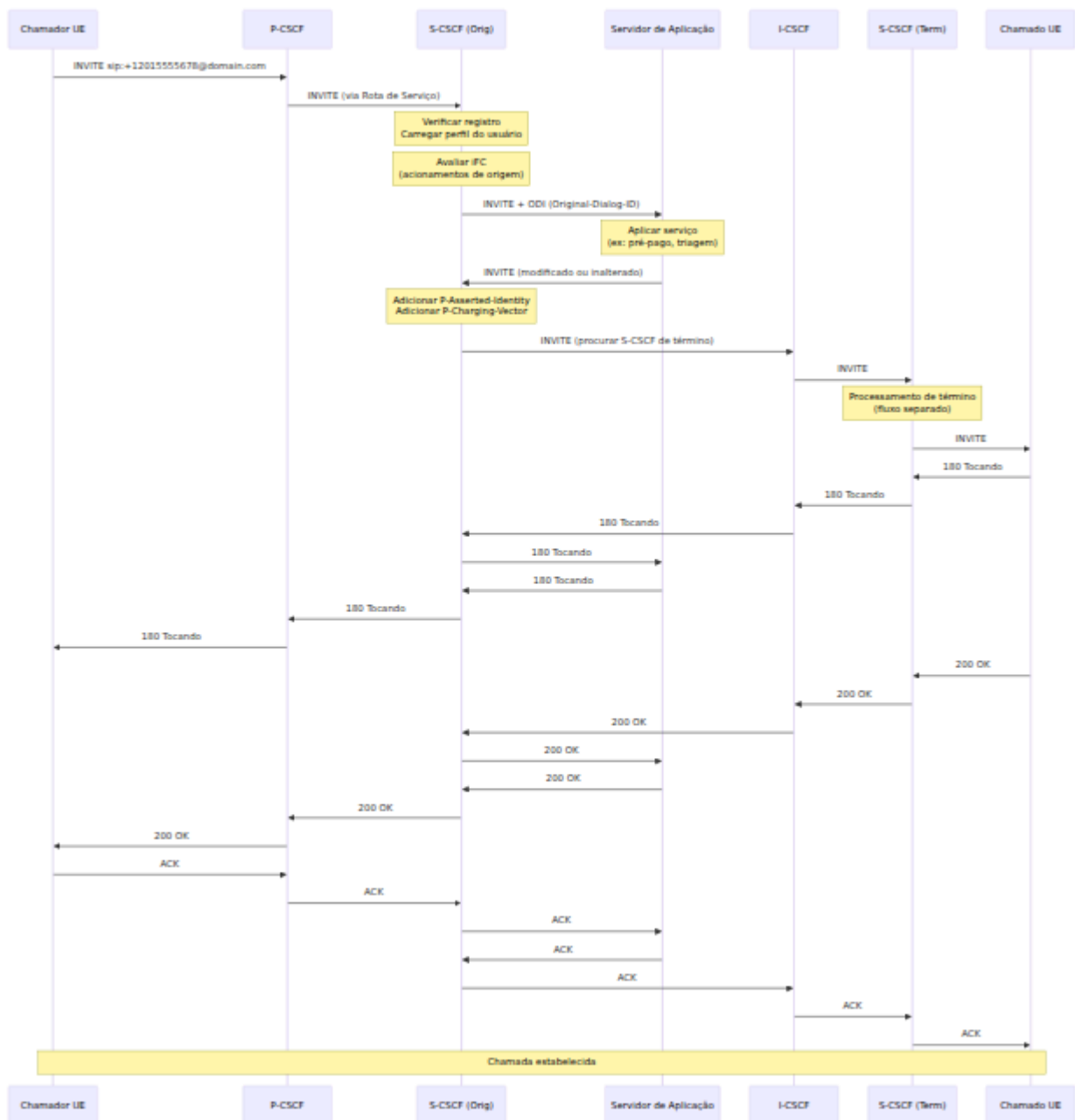
O S-CSCF roteia chamadas para/de PSTN via a **interface Mi** para o **BGCF (Função de Controle de Gateway de Saída)**, que está integrada ao OmniTAS em nossa implementação.

Interface Mi - S-CSCF para BGCF

Ponto de Referência 3GPP: Mi (interface SIP entre S-CSCF e BGCF)

A interface Mi é usada quando o S-CSCF determina que uma chamada precisa ser direcionada para a PSTN. Em nossa arquitetura, a funcionalidade BGCF está incorporada diretamente no OmniTAS, portanto, todas as chamadas de origem móvel (MO) destinadas a números PSTN são roteadas para o OmniTAS.

Fluxo de Roteamento PSTN



Como Funciona o Roteamento PSTN:

1. **Detecção do Número de Destino:** O S-CSCF examina o Request-URI para determinar se o destino é um número de telefone (formato E.164 como +12015551234)
2. **Roteio para OmniTAS:** Para destinos PSTN, o S-CSCF roteia a chamada via a interface Mi para o OmniTAS, que inclui a funcionalidade BGCF integrada
3. **Processamento BGCF no OmniTAS:** O OmniTAS determina o ponto de saída PSTN apropriado com base em:

- Análise do número de destino (código de país, código de área)
- Regras de roteamento de menor custo
- Grupos de troncos disponíveis
- Seleção de operadora

4. **Saída PSTN:** O OmniTAS lida com a interação real do gateway de mídia para completar a chamada para a rede PSTN

Detalhes da Interface Mi:

- **Protocolo:** SIP
- **Propósito:** Roteio de chamadas destinadas à PSTN do S-CSCF para BGCF
- **Direção:** S-CSCF → OmniTAS (com BGCF)
- **Tipos de Chamadas:** Chamadas de origem móvel (MO) para números PSTN

Configuração: O S-CSCF é configurado para reconhecer destinos PSTN (números de telefone) e roteá-los para o OmniTAS. Quando o OmniTAS é usado como o TAS (Servidor de Aplicação de Telefonia), ele inclui intrinsecamente as capacidades BGCF, eliminando a necessidade de um componente BGCF separado.

8. Arquitetura de Cobrança

O S-CSCF possui capacidade embutida para interface com um OCS (Sistema de Cobrança Online) via a interface Diameter Ro para controle de crédito em tempo real. No entanto, **em nossas implementações, a cobrança do S-CSCF é tipicamente desativada** em favor de realizar a cobrança no nível do **TAS (Servidor de Aplicação de Telefonia)**.

Por que a Cobrança é Feita no TAS em vez de S-CSCF

Vantagens da Cobrança Baseada em TAS:

1. **Cenários de Encaminhamento de Chamadas:** Quando uma chamada é encaminhada, o S-CSCF apenas vê o INVITE inicial para o destino original. Ele não tem visibilidade na lógica de encaminhamento ou no destino final. O TAS, no entanto, lida com o serviço de encaminhamento e sabe:

- Quem iniciou a chamada
- Para quem a chamada foi originalmente
- Para onde a chamada foi encaminhada
- Duração da chamada encaminhada
- Parte correta a ser cobrada (chamador, encaminhador ou ambos)

2. **Roaming 2G/3G:** Quando assinantes estão em roaming em redes legadas 2G/3G, chamadas podem contornar completamente o núcleo IMS e rotearem através da infraestrutura de comutação de circuitos. O TAS integra os domínios IMS e CS (Comutação de Circuitos) e pode:

- Detectar quando um assinante está em roaming em 2G/3G
- Aplicar as cobranças de roaming apropriadas
- Rastrear a duração da chamada entre tipos de rede
- Lidar com transferências entre os domínios IMS e CS

3. **Transferência de Chamadas:** Semelhante ao encaminhamento de chamadas, transferências de chamadas envolvem mudanças no meio da chamada que o S-CSCF não rastreia:

- Transferências cegas (entrega imediata)
- Transferências atendidas (consulta e depois entrega)
- Transferência para correio de voz
- Transferências multipartidárias

4. **Chamadas em Conferência:** Conferências multipartidárias requerem lógica de cobrança especial:

- Quem iniciou a conferência
- Quantos participantes
- Duração que cada participante esteve na chamada
- Tarifas diferentes para o iniciador da conferência vs. participantes

5. **Serviços Suplementares:** Serviços como espera de chamada, retenção de chamada e chamada em três vias requerem que o TAS entenda o estado do serviço:

- Múltiplas chamadas simultâneas por usuário

- Eventos de retenção/retorno
- Chamadas mescladas

6. **Lógica Pré-paga vs. Pós-paga:** O TAS pode aplicar diferentes estratégias de cobrança:

- Pré-pago: Verificações de crédito em tempo real e corte de chamada
- Pós-pago: Geração de CDR para faturamento mensal
- Híbrido: Tarifas diferentes para diferentes recursos de serviço

7. **Flexibilidade de Avaliação:** O TAS tem o contexto completo para aplicar regras de avaliação complexas:

- Preços de acordo com o horário
- Preços baseados em destino (local, longa distância, internacional)
- Descontos por volume
- Tarifas promocionais
- Minutos de pacote vs. cobranças por excesso

Limitações de Cobrança do S-CSCF:

- Apenas vê o diálogo SIP básico (INVITE → 200 OK → BYE)
- Sem conhecimento de serviços suplementares
- Não pode rastrear mudanças de estado de chamada no meio da chamada
- Contexto limitado para decisões de avaliação
- Não entende a atividade do domínio CS

Interface Ro do S-CSCF (Disponível, mas Desativada por Padrão)

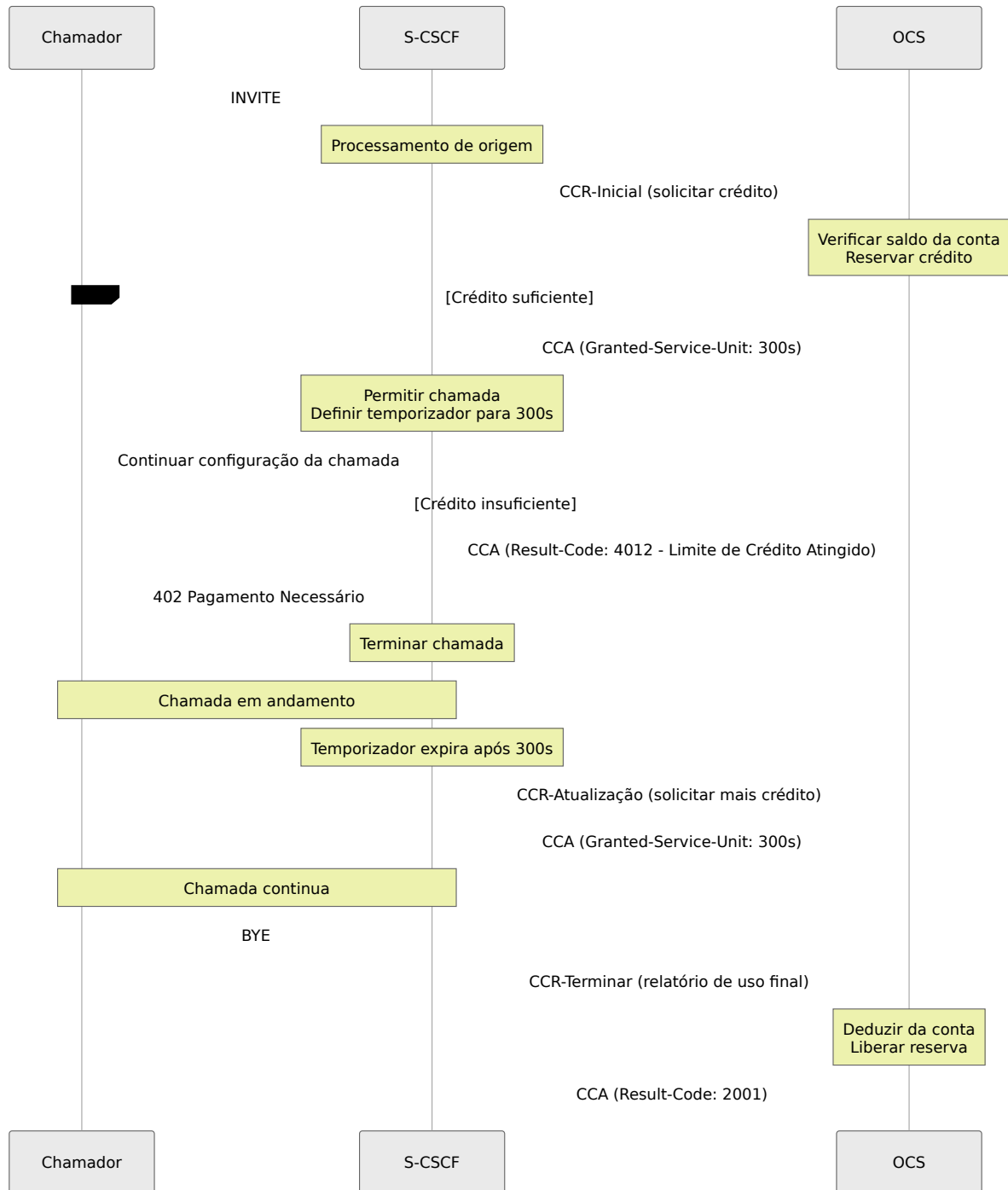
Embora não utilizada em produção, o S-CSCF suporta cobrança online via Diameter Ro. Essa capacidade permanece na configuração, mas está desativada.

Como a Cobrança do S-CSCF Funcionaria (Se Habilitada)

Se a cobrança do S-CSCF fosse habilitada, o sistema usaria a interface Diameter Ro (ID da Aplicação 4) para se comunicar com um OCS. O S-CSCF seria configurado com as informações do par OCS (FQDN, realm, porta 3868) e

enviaria Solicitações de Controle de Crédito (CCR) em três pontos-chave no ciclo de vida da chamada:

Fluxo CCR (Se Habilitado):



Quando a Cobrança Seria Acionada:

- CCR-Inicial:** Enviado quando o INVITE é recebido, antes de permitir que a chamada prossiga. O OCS verifica o saldo da conta e concede crédito

(permitindo a chamada) ou nega (chamada rejeitada com 402 Pagamento Necessário).

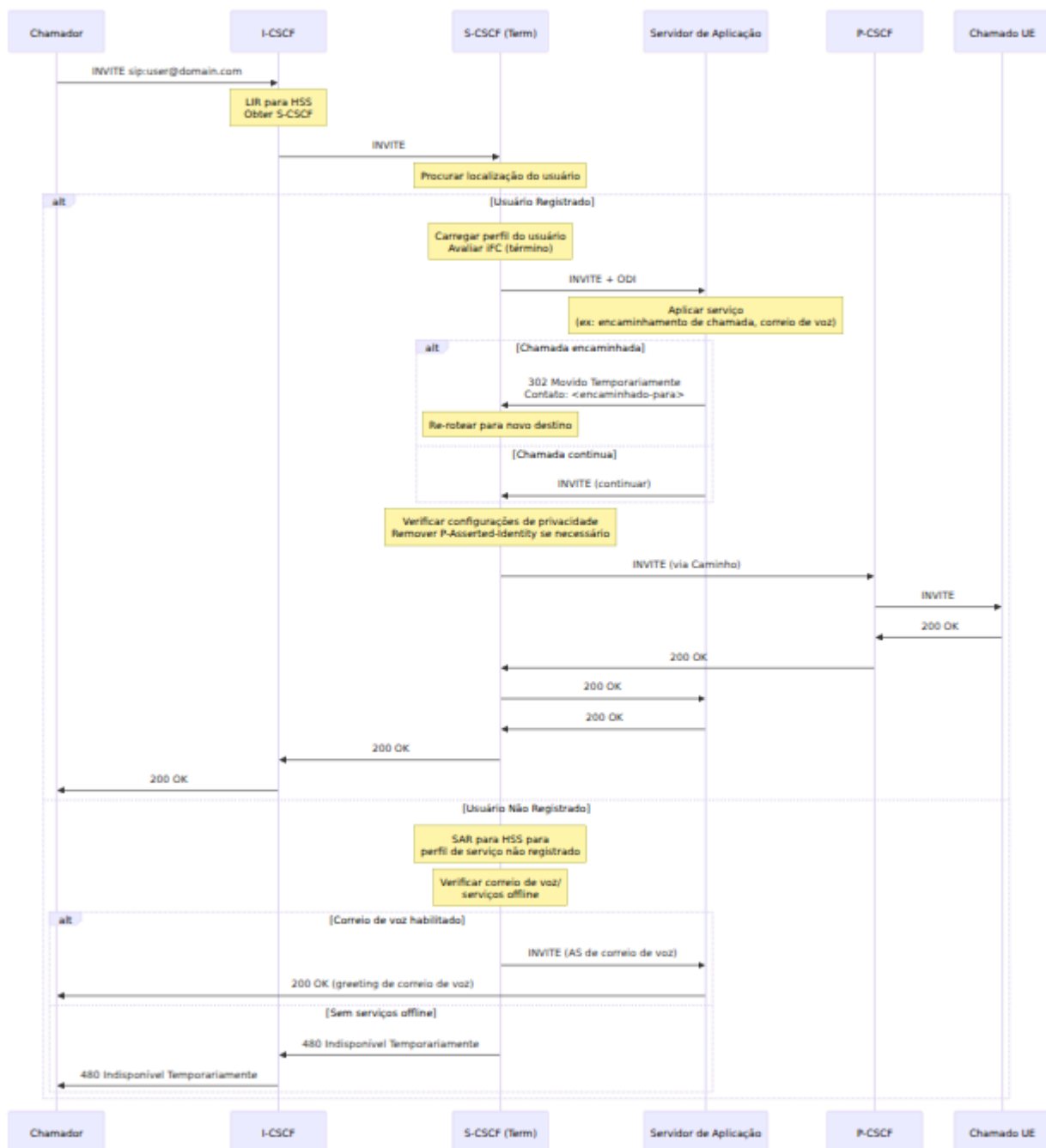
2. **CCR-Atualização:** Enviado periodicamente durante a chamada com base no tempo de Granted-Service-Unit do OCS (ex: a cada 300 segundos). Isso garante que chamadas longas não excedam o crédito disponível.
3. **CCR-Terminar:** Enviado quando a chamada termina (BYE recebido ou timeout do diálogo), relatando o uso final ao OCS para dedução da conta.

Implementação Real: Como essa funcionalidade de cobrança está desativada em nossas implementações, o S-CSCF simplesmente roteia chamadas sem quaisquer verificações de controle de crédito. Toda a lógica de cobrança é tratada a montante pelo TAS, que tem total visibilidade sobre o fluxo completo da chamada e o contexto do serviço.

9. Presença e SUBSCRIBE/PUBLISH

O S-CSCF gerencia a presença SIP para o status de disponibilidade do usuário.

Arquitetura de Presença



Configuração de Presença

A funcionalidade de presença do S-CSCF é configurada com:

- **Máximo expira:** 3600 segundos (1 hora) - duração máxima da assinatura
- **Estado padrão:** "ativo" - estado de presença padrão é ativo
- **Suporte a PIDF:** Habilitado - permite modificação de documentos PIDF (Formato de Dados de Informação de Presença)

Manipulação de PUBLISH

Processamento de Publicação de Presença: Quando o S-CSCF recebe uma solicitação PUBLISH (usada para atualizar o status de presença):

1. **Detecção de Método:** Verifica se a solicitação recebida é um método PUBLISH
2. **Verificação de Autorização:** Verifica se o usuário está atualmente registrado no banco de dados de localização. Se não registrado, responde com 403 Proibido
3. **Atualização de Presença:** Processa a solicitação PUBLISH para atualizar as informações de presença do usuário no banco de dados de presença
4. **Tratamento de Erros:** Se o tratamento de presença falhar (ex: erro de banco de dados, documento de presença malformatado), responde com 500 Erro de Servidor

Manipulação de SUBSCRIBE

Processamento de Assinatura de Presença: Quando o S-CSCF recebe uma solicitação SUBSCRIBE (usada para observar a presença de outro usuário):

1. **Detecção de Método:** Verifica se a solicitação recebida é um método SUBSCRIBE
2. **Verificação de Tipo de Evento:** Examina o cabeçalho Event para determinar o tipo de assinatura
 - Se o Evento for "reg" (pacote de evento de registro), esta é uma assinatura para mudanças de estado de registro
 - Para assinaturas de eventos de registro, realiza Solicitação de Atribuição do Servidor (SAR) ao HSS se o usuário não estiver registrado, para obter o perfil de serviço
 - Avalia iFC para acionamentos de "subscribe" para determinar se algum Servidor de Aplicação deve lidar com a assinatura
3. **Processamento de Assinatura de Presença:** Trata a solicitação SUBSCRIBE para criar ou atualizar uma assinatura de observador de presença
4. **Tratamento de Erros:** Se o processamento da assinatura falhar, responde com 500 Erro de Servidor

Operações da Interface Web

Acessando a Página S-CSCF

Navegar para: `https://<painel-de-controle>/scscf`

Layout da Página

A página S-CSCF tem cinco abas principais:

1. **Lista de Registro** - Lista paginada de usuários registrados
2. **Localização do Usuário** - Consultar detalhes específicos do IMPU
3. **Diálogos** - Sessões de chamadas ativas
4. **IFC** - Gerenciamento e teste de Critérios de Filtro Iniciais
5. **Tabelas Hash** - Tabelas de memória compartilhada

Aba Lista de Registro

Propósito: Visualizar todos os usuários registrados com paginação

Colunas de Exibição:

- **IMPU:** Identidade Pública Multimídia IP (URI SIP)
- **Contatos:** Número de ligações de contato registradas
- **Estado:** Estado de registro (Registrado/Não Registrado)
- **Expira:** Timestamp de expiração do registro

Recursos:

- Paginação (50 usuários por página)
- Pesquisa por IMPU ou contato
- Ordenar por coluna
- Clicar na linha para expandir e ver detalhes de contato

Exemplo:

```
IMPU: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
```

```
Contatos: 1
```

```
Estado: Registrado
```

```
Expira: 2025-11-29 15:45:30
```

```
[Expandir para ver:]
```

```
Contato: sip:12015551234@10.4.12.100:5060;transport=tcp
```

```
Caminho:
```

```
<sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
```

```
User-Agent: Android IMS Client v1.0
```

```
Recebido: 10.4.12.100:52341
```

Ações Rápidas:

- **Pesquisar:** Pesquisa rápida para IMPU específico
- **Despejar IFC:** Visualizar Critérios de Filtro Iniciais para usuário
- **Testar IFC:** Simular chamada para testar acionamento de AS
- **Desregistrar:** Forçar desregistro (usar com cautela!)

Aba Localização do Usuário

Propósito: Consulta detalhada de um IMPU específico

Operações:

1. Inserir IMPU (ex: `sip:user@domain.com`)
2. Clicar em "Consultar"
3. Visualizar informações detalhadas:
 - Todos os contatos registrados
 - Cabeçalho de Rota de Serviço
 - Timestamps de registro
 - Cabeçalhos de caminho
 - IMPIs associados (Identities Privadas)

Casos de Uso:

- Solucionar por que o usuário não pode receber chamadas
- Verificar detalhes de registro
- Verificar ligações de contato
- Verificar rotas de serviço

Aba Diálogos

Propósito: Monitorar e gerenciar sessões de chamadas ativas

Colunas de Exibição:

- **Call-ID:** SIP Call-ID
- **From URI:** Identidade do chamador
- **To URI:** Identidade do chamado
- **Estado:** Inicial (tocando) ou Confirmado (atendido)
- **Hora de Início:** Quando o diálogo foi criado
- **Timeout:** Valor de timeout do diálogo

Operações:

- **Atualizar:** Atualização manual (atualização automática a cada 5s)
- **Encerrar Diálogo:** Encerrar chamada específica (envia BYE)
- **Encerrar Todos os Diálogos Ativos:** Terminação em massa de emergência

Exemplo:

```
Call-ID: 3c26700857a87f84@10.4.12.165
From: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
To: sip:+12015555678@ims.mnc001.mcc001.3gppnetwork.org
Estado: Confirmado
Hora de Início: 2025-11-29 15:30:15
Timeout: 360000 segundos
```

[Botão Encerrar Diálogo]

Atenção: Encerrar diálogos terminará imediatamente chamadas ativas. Usar apenas para solução de problemas ou situações de emergência.

Aba IFC

Propósito: Visualizar e testar Critérios de Filtro Iniciais para acionamento de serviços

A aba IFC fornece duas operações principais: Despejar IFC (recuperar e exibir um iFC de um usuário do HSS) e Testar IFC (simular um cenário de chamada para ver quais Servidores de Aplicação seriam acionados).

Operação Despejar IFC

1. Inserir IMPU: `sip:user@domain.com`
2. Clicar em "Despejar IFC"
3. Visualizar estrutura detalhada de iFC:
 - Ordem de prioridade
 - Pontos de acionamento (condições SPT)
 - URIs do Servidor de Aplicação
 - Tratamento padrão

Exemplo de Saída:

```
<InitialFilterCriteria>
  <Priority>0</Priority>
  <TriggerPoint>
    <ConditionTypeCNF>1</ConditionTypeCNF>
    <SPT>
      <Group>0</Group>
      <Method>INVITE</Method>
    </SPT>
    <SPT>
      <Group>0</Group>
      <SessionCase>0</SessionCase>  <!-- Originando -->
    </SPT>
  </TriggerPoint>
</ApplicationServer>

<ServerName>sip:tas.ims.mnc001.mcc001.3gppnetwork.org</ServerName>
  <DefaultHandling>0</DefaultHandling>
</ApplicationServer>
</InitialFilterCriteria>
```

Operação Testar IFC

1. Inserir IMPU: `sip:user@domain.com`
2. Inserir URI de Origem: `sip:user@domain.com` (parte chamadora)
3. Inserir URI de Destino: `sip:+12015555678@domain.com` (parte chamada)
4. Clicar em "Testar IFC"
5. Visualizar resultados:
 - Qual iFC correspondeu
 - Quais Servidores de Aplicação seriam invocados
 - Em que ordem (prioridade)

Casos de Uso:

- Verificar configuração de acionamento de serviço
- Solucionar por que AS não está sendo invocado
- Testar novo iFC antes de implantar em produção
- Entender o fluxo de chamadas para cenários específicos

Aba Tabelas Hash

Semelhante ao P-CSCF e I-CSCF, gerenciar tabelas hash de memória compartilhada.

Tabelas Hash Comuns do S-CSCF:

- `auth`: Cache de vetores de autenticação
- `profile`: Perfis de usuário em cache (se utilizado)
- Tabelas personalizadas para lógica de serviço

Fluxos de Chamadas

Fluxo Completo de Registro

Veja a seção "1. Registro e Autenticação" acima para o diagrama de sequência detalhado.

Fluxo Completo de Chamadas de Origem

Veja a seção "5. Manipulação de Chamadas de Origem" acima para o diagrama de sequência detalhado.

Fluxo Completo de Chamadas de Término

Veja a seção "6. Manipulação de Chamadas de Término" acima para o diagrama de sequência detalhado.

Solução de Problemas

Problemas de Registro

Usuário Não Consegue Registrar - 403 Proibido

Causas Possíveis:

- Usuário não provisionado no HSS
- HSS inacessível
- Falha na autenticação
- Proibição aplicada

Passos Diagnósticos:

1. Verifique a conectividade do HSS via o painel de controle:
 - Navegue até a página Diameter
 - Selecione o nó S-CSCF
 - Verifique se o par HSS aparece como "I_Open" (conectado)
2. Revise os logs do S-CSCF para o fluxo de mensagens MAR/MAA (Solicitação/Resposta de Autenticação Multimídia)
3. Verifique se o usuário existe no HSS (se acessível)
4. Verifique os logs do S-CSCF para vetores de autenticação recebidos do HSS
5. Teste com um algoritmo de autenticação diferente, se suportado

Usuário Não Consegue Registrar - 500 Erro de Servidor

Causas Possíveis:

- Conexão com o banco de dados perdida
- Falha SAR/SAA
- Erro de módulo

Soluções:

1. Verifique a conectividade do banco de dados a partir do servidor S-CSCF (verifique se o banco de dados é acessível e se as credenciais estão corretas)
2. Revise os logs do S-CSCF para o fluxo de mensagens SAR/SAA (Solicitação/Resposta de Atribuição do Servidor) Diameter

3. Reinicie o serviço S-CSCF, se necessário, para recuperar de erros de módulo

Problemas de Roteamento de Chamadas

Chamadas Não Roteadas para o Usuário

Sintomas: INVITE chega ao S-CSCF, mas não é encaminhado para o P-CSCF

Passos Diagnósticos:

1. Verifique se o usuário está registrado via a interface web do painel de controle:
 - Navegue até S-CSCF → aba Localização do Usuário
 - Insira o IMPU e clique em "Consultar"
 - Verifique se o usuário aparece como registrado com ligações de contato
2. Verifique se as ligações de contato existem e se o cabeçalho Path está presente
3. Revise os logs do S-CSCF para o processamento da rota de término
4. Teste com um destino diferente para isolar o problema

Servidor de Aplicação Não Acionado

Sintomas: iFC deve corresponder, mas AS não é invocado

Passos Diagnósticos:

1. Despeje iFC via a interface web do painel de controle:
 - Navegue até S-CSCF → aba IFC
 - Insira o IMPU
 - Clique em "Despejar IFC"
 - Revise os pontos de acionamento e URIs do Servidor de Aplicação
2. Teste a correspondência de iFC via a interface web:

- Navegue até S-CSCF → aba IFC
 - Insira IMPU, URI de origem e URI de destino
 - Clique em "Testar IFC"
 - Verifique qual iFC deveria ter correspondido
3. Verifique se o perfil do usuário foi carregado do HSS revisando os logs
 4. Verifique se a SAA (Resposta de Atribuição do Servidor) do HSS continha o XML do perfil do usuário
 5. Revise os logs do S-CSCF para erros de análise de iFC

Problemas de Diálogo

Diálogos Não Terminando Após BYE

Sintomas: Diálogo permanece no banco de dados após o término da chamada

Soluções:

1. Verifique diálogos ativos via o painel de controle:
 - Navegue até S-CSCF → aba Diálogos
 - Revise a contagem e os estados dos diálogos
2. Verifique a detecção de BYE nos logs do módulo de diálogo
3. Verifique as configurações de timeout do diálogo na configuração
4. Encerrar manualmente o diálogo via o painel de controle:
 - Navegue até S-CSCF → aba Diálogos
 - Encontre o diálogo preso
 - Clique em "Encerrar Diálogo"
5. Revise o banco de dados em busca de entradas de diálogo órfãs e limpe se necessário

Problemas de Cobrança

Timeout de CCR

Nota: Em nossas implementações, a cobrança do S-CSCF é tipicamente desativada. A cobrança é tratada pelo TAS. Se você está vendo erros relacionados à cobrança, verifique se a cobrança do S-CSCF não foi acidentalmente habilitada.

Sintomas: Chamadas falham com erros de cobrança (se a cobrança estiver habilitada)

Causas Possíveis:

- OCS inacessível
- Par Diameter Ro fora do ar
- Timeout de transação muito curto

Soluções:

1. Verifique o status do par OCS via o painel de controle:
 - Navegue até a página Diameter
 - Selecione o nó S-CSCF
 - Verifique se o par OCS aparece como "I_Open" (conectado)
2. Teste a conectividade de rede do OCS a partir do servidor S-CSCF
3. Revise a configuração do timeout de transação Diameter
4. Verifique os logs do S-CSCF para o fluxo de mensagens CCR/CCA e erros

Crédito Insuficiente - Todas as Chamadas Falham

Nota: Este problema se aplica apenas se a cobrança do S-CSCF estiver habilitada (o que normalmente não está em nossas implementações).

Sintomas: Usuários recebem 402 Pagamento Necessário para todas as chamadas

Soluções:

1. Verifique se a cobrança do S-CSCF deve realmente estar habilitada (normalmente deve estar desativada)
2. Verifique o saldo do OCS para contas de teste se a cobrança estiver intencionalmente habilitada
3. Revise os códigos de resultado CCA (Resposta de Controle de Crédito) nos logs do S-CSCF
4. Considere desativar a cobrança do S-CSCF e usar a cobrança baseada no TAS em vez disso

Problemas de PSTN

Chamadas para PSTN Falham - 503 Nenhum Gateway Disponível

Causas Possíveis:

- Nenhum MGCF/gateway configurado
- Todos os gateways fora do ar
- Dispatcher não carregado

Soluções:

1. Coordene com os administradores do sistema para verificar se os gateways PSTN estão configurados
2. Teste a conectividade do gateway a partir do servidor S-CSCF (alcance de rede, resposta SIP)
3. Revise a configuração do gateway com os administradores do sistema
4. Adicione gateways ausentes, se necessário, via administradores do sistema

Problemas de Desempenho

Alta Utilização de CPU

Causas Possíveis:

- Muitos diálogos
- Consultas lentas ao banco de dados
- Sobrecarga de avaliação de iFC

Soluções:

1. Verifique a contagem de diálogos via o painel de controle:
 - Navegue até S-CSCF → aba Diálogos
 - Revise o número de diálogos ativos
2. Otimize tabelas de banco de dados (diálogo, impu, impu_contact) se as consultas ao banco de dados estiverem lentas
3. Adicione índices ao banco de dados se necessário (em impu.impu, dialog.callid, etc.)
4. Ajuste a contagem de processos de trabalho na configuração se necessário (aumente de 4 para 8 por carga alta)

Melhores Práticas

Alta Disponibilidade

1. **Implantar múltiplos S-CSCFs** com banco de dados compartilhado
2. **Usar capacidades** para seleção de S-CSCF no I-CSCF
3. **Replicação de banco de dados:** Master-master ou master-slave
4. **Persistência de sessão:** Modo de diálogo de gravação
5. **Verificações de saúde:** Monitorar contagens de registro e diálogo

Segurança

1. **Sempre autenticar** usuários via HSS
2. **Validar P-Asserted-Identity** apenas de fontes confiáveis

3. **Limitar taxa** de registros e chamadas por usuário
4. **Sanitar cabeçalhos** de redes não confiáveis
5. **Usar TLS** para Diameter (Cx, Ro)

Desempenho

1. **Ajustar hash_size para localização de usuários:** O tamanho da hash deve ser definido com base na contagem de usuários esperada. Por exemplo, hash_size=13 (que equivale a $2^{13} = 8192$ buckets) é apropriado para aproximadamente 50.000 usuários
2. **Cache de perfis de usuários:** Se o HSS suportar, habilite o cache de perfil para reduzir solicitações Diameter SAR
3. **Otimizar iFC:** Mantenha as condições de Ponto de Acionamento (SPT) simples e minimize o número de regras de iFC por usuário para reduzir a sobrecarga de avaliação
4. **Usar operações assíncronas para Diameter:** Configure o processamento assíncrono para MAR (autenticação), SAR (registro) e CCR (cobrança) para evitar bloquear processos de trabalho
5. **Monitorar o desempenho do banco de dados regularmente:** Acompanhe os tempos de execução de consultas, otimize índices e garanta que o pool de conexões esteja funcionando de forma eficiente

Monitoramento

Para uma lista completa de todas as métricas do S-CSCF, veja a [Referência de Métricas](#).

Métricas-chave a serem acompanhadas:

- Taxa de sucesso de registro
- Taxa de sucesso MAR/SAR/LIR
- Contagem de diálogos (chamadas ativas)
- Tempo de avaliação de iFC
- Latência de consulta ao banco de dados

- Uptime do par Diameter
- Tempo de configuração de chamadas

Referência

Especificações 3GPP

- **TS 23.228**: Arquitetura IMS
- **TS 24.229**: Protocolo SIP IMS
- **TS 29.228**: Interface Cx
- **TS 23.218**: Interface ISC
- **TS 32.260**: Cobrança IMS

Guia de Operações da Interface Web

Índice

1. [Visão Geral](#)
2. [Acessando o Painel de Controle](#)
3. [Gerenciamento de P-CSCF](#)
4. [Gerenciamento de I-CSCF](#)
5. [Gerenciamento de S-CSCF](#)
6. [Gerenciamento de Par Diameter](#)
7. [Operações de Tabela Hash](#)
8. [Visualização de Logs](#)
9. [Monitoramento e Métricas](#)

Visão Geral

A Interface Web OmniCall CSCF fornece um painel de controle abrangente para monitoramento e gerenciamento em tempo real de todos os componentes CSCF (P-CSCF, I-CSCF, S-CSCF). A interface é construída sobre o Phoenix LiveView e fornece:

- **Visibilidade em tempo real** sobre registros, chamadas ativas e estado do sistema
- **Gerenciamento de tabelas hash** para estruturas de dados em memória críticas para desempenho
- **Monitoramento de pares Diameter** e controle
- **Métricas Prometheus** para monitoramento do sistema
- **Visualização de logs ao vivo** para solução de problemas

Arquitetura

O painel de controle se comunica com instâncias de backend CSCF para:

- Consultar registros de usuários e dados de localização
- Inspecionar diálogos ativos (chamadas)
- Gerenciar pares Diameter
- Visualizar e manipular tabelas hash
- Acessar a configuração de Critérios de Filtro Iniciais (IFC)

Acessando o Painel de Controle

Acesso Padrão

O painel de controle é acessível via HTTP no servidor CSCF:

```
http://<cscf-server>:4000/
```

Porta Padrão: 4000 (configurável em `ControlPanel.Supervisor`)

Configuração

O painel de controle requer configuração do host CSCF em `config/config.exs` ou `config/runtime.exs`:

```
config :cscf, :cscf_hosts,  
  pcscf: [  
    {host: "10.4.12.165", port: 9060, label: "P-CSCF 1"}  
  ],  
  icscf: [  
    {host: "10.4.12.166", port: 9060, label: "I-CSCF 1"}  
  ],  
  scscf: [  
    {host: "10.4.12.167", port: 9060, label: "S-CSCF 1"}  
  ]
```

Navegação

O painel de controle fornece abas de navegação para cada componente CSCF:

- **P-CSCF** - `/pcscf` - Contatos de registro e tabelas hash
- **I-CSCF** - `/icscf` - Lista de S-CSCF, domínios NDS, sessões
- **S-CSCF** - `/scscf` - Registros, diálogos, gerenciamento de IFC
- **Diameter** - `/diameter` - Status e controle de pares Diameter
- **Logs** - `/logs` - Visualização de logs ao vivo

Gerenciamento de P-CSCF

URL: `/pcscf`

Recursos

O painel P-CSCF exibe contatos registrados e informações da tabela hash das instâncias P-CSCF.

Aba de Contatos Registrados

Exibe todos os registros IMS atuais visíveis para o P-CSCF:

Coluna	Descrição
IMSI	IMSI do assinante ou identificador de contato
Estado	Estado do registro (registrado, não registrado)
Expira	Tempo até o registro expirar
Caminho	Cabeçalho SIP Path para roteamento

Operações:

- **Clique na linha** para expandir e visualizar informações detalhadas do contato, incluindo:
 - AoR completo (Endereço de Registro)
 - Endereço IP do UE
 - Detalhes do caminho
 - Estatísticas (slots máximos, registros)

Aba de Tabelas Hash

Gerencie tabelas hash do P-CSCF. Veja [Operações de Tabela Hash](#) abaixo.

Atualizações em Tempo Real

A visualização do P-CSCF atualiza automaticamente a cada 5 segundos para mostrar o status atual do registro.

Gerenciamento de I-CSCF

URL: `/icscf`

Recursos

O painel I-CSCF fornece monitoramento das operações do I-CSCF, incluindo seleção de S-CSCF e rastreamento de sessões.

Aba de Lista de S-CSCF

Exibe todos os servidores S-CSCF configurados conhecidos pelo I-CSCF:

- **ID:** Identificador do S-CSCF
- **Nome:** FQDN do S-CSCF
- **Capacidades:** Número de capacidades suportadas

Aba de Domínios NDS

Mostra domínios NDS (Segurança de Domínio de Rede) confiáveis configurados no I-CSCF.

Aba de Sessões

Exibe sessões ativas do I-CSCF, incluindo:

- **Call-ID:** SIP Call-ID
- **Candidatos a S-CSCF:** Lista de servidores S-CSCF considerados para atribuição
 - Nome do S-CSCF
 - Pontuação de seleção
 - Idade (tempo desde que o candidato foi adicionado)

Aba de Tabelas Hash

Gerencie tabelas hash do I-CSCF. Veja [Operações de Tabela Hash](#) abaixo.

Gerenciamento de S-CSCF

URL: `/scscf`

O painel S-CSCF é o mais rico em recursos, fornecendo gerenciamento abrangente de registros, diálogos e IFC.

Aba de Listar Registros

Navegue por todos os registros ativos com paginação:

Recursos:

- **Controles de paginação:** Offset e limite para grandes bancos de dados de registro
- **Detalhes do registro** para cada IMPU:
 - Identidade pública do usuário (IMPU)
 - Estado do registro
 - Número do slot
 - Detalhes de contato com User-Agent e expiração
 - Call-ID

Ações Rápidas para cada registro:

- **Lookup:** Visualizar informações detalhadas do IMPU
- **Dump IFC:** Visualizar Critérios de Filtro Iniciais para o usuário
- **Testar IFC:** Testar correspondência de IFC para chamadas simuladas
- **Deregister:** Remover registro administrativamente

Aba de Localização do Usuário

Consultar e inspecionar dados de localização do usuário:

- Visualizar status de localização do usuário bruto do S-CSCF
- **Formulário de Lookup IMPU:** Consultar identidade pública do usuário específica
- Exibe detalhes completos do registro, incluindo contatos, estado e metadados

Aba de Diálogos

Gerencie sessões de chamadas ativas (diálogos):

Coluna	Descrição
ID do Diálogo	Identificador h_entry:h_id
Call-ID	SIP Call-ID
De	URI da parte que chama
Para	URI da parte chamada
Estado	Estado do diálogo

Operações:

- **Encerrar Diálogo:** Terminar chamada específica (envia BYE)
- **Encerrar Todos:** Terminar todas as chamadas ativas (com confirmação)

Aba de IFC

Ferramentas de Critérios de Filtro Iniciais para gerenciamento de acionamento de serviços:

Dump IFC

Recuperar e exibir todas as regras de IFC para um dado IMPU:

- Identidade pública
- Identidade privada
- Contagem de perfis de serviço
- **Critérios de Filtro** para cada perfil de serviço:
 - Prioridade (ordem de execução)
 - Tratamento padrão (SESSION_CONTINUED vs SESSION_TERMINATED)
 - Nome do Servidor de Aplicação
 - Flags de inclusão de REGISTER
 - **Detalhes do Ponto de Acionamento:**
 - Tipo de condição (DNF ou CNF)
 - Acionadores de Ponto de Serviço (SPTs):
 - METHOD, HEADER, SESSION_CASE, REQUEST_URI, etc.
 - Flags de negação

A exibição do IFC inclui:

- Distintivos de prioridade codificados por cor
- Explicações lógicas do ponto de acionamento expansíveis
- DNF (Forma Normal Disjuntiva) = OU de E
- CNF (Forma Normal Conjuntiva) = E de OU

Testar IFC

Testar quais Servidores de Aplicação seriam acionados para uma sessão simulada:

Entrada:

- URI (identidade pública do assinante)

- Direção (originando ou terminando)
- Método (INVITE, REGISTER, MESSAGE, SUBSCRIBE)
- URI de Solicitação (destino)

Saída:

- Status de registro
- Contagem de IFC correspondentes
- Lista de Servidores de Aplicação acionados com índice de IFC

Aba de Tabelas Hash

Gerencie tabelas hash do S-CSCF. Veja [Operações de Tabela Hash](#) abaixo.

Gerenciamento de Par Diameter

URL: `/diameter`

Recursos

Monitore e controle conexões de pares Diameter (interfaces Cx, Rx, Ro).

Informações Resumidas

O painel exibe:

- **Realm:** Realm Diameter
- **Identidade:** Origin-Host Diameter
- **Contagem de Pares:** Número de pares configurados
- **Trabalhadores:** Contagem de trabalhadores CDP
- **Comprimento da Fila:** Transações pendentes
- **Tempo de Conexão:** Tempo limite de conexão (segundos)
- **Tempo de Transação:** Tempo limite de transação (segundos)
- **Aceitar Pares Desconhecidos:** Flag de política

Lista de Pares

Tabela de todos os pares Diameter:

Coluna	Descrição
FQDN	Nome de domínio totalmente qualificado do par
Estado	Estado da conexão (I_Open, Closed, etc.)
Status	Habilitado ou Desabilitado
Último Usado	Tempo desde a última transação
Aplicações	Número de aplicações Diameter suportadas

Operações:

- **Habilitar Par:** Ativar par desabilitado
- **Desabilitar Par:** Desativar par (com confirmação)
- **Clique na linha:** Expanda para visualizar aplicações suportadas

Mapeamento de Aplicações

O painel de controle mapeia automaticamente IDs de Aplicação Diameter para nomes de interface 3GPP:

- **Cx/Dx** (16777216:10415) - Assinatura/Autorização IMS
- **Sh/Dh** (16777217:10415) - Acesso a Dados do Usuário
- **Rx** (16777236:10415) - Controle do Plano de Mídia IMS
- **Ro** (16777238:10415/0) - Cobrança Online
- **Gx** (16777224:10415) - Controle de Política
- **S6a/S6d** (16777251:10415) - LTE/EPC MME-HSS
- E muitos mais (veja fonte: `diameter_live.exe`)

Atualizações em Tempo Real

O status do par Diameter atualiza automaticamente a cada 5 segundos.

Operações de Tabela Hash

Visão Geral

Os componentes CSCF usam tabelas hash em memória para dados críticos de desempenho. O painel de controle fornece visibilidade e gerenciamento dessas tabelas.

Tabelas Hash Disponíveis

As tabelas variam de acordo com o tipo de CSCF. Exemplos comuns:

Tabela Hash	CSCF	Propósito
imei_msisdn	P-CSCF	Mapeamento de retorno de chamada de emergência
service_routes	P-CSCF	Rotas de serviço em cache
auth	S-CSCF	Vetores de autenticação
Várias	Todas	Cache específico do componente

As tabelas hash são estruturas de dados em memória usadas para operações críticas de desempenho.

Visualizando Tabelas Hash

Acesso: Navegue para qualquer painel CSCF → Aba Tabelas Hash

1. Visualizar lista de todas as tabelas hash com estatísticas:

- Nome da tabela
- Contagem de itens

- Tamanho
2. **Selecione a tabela** para visualizar entradas
 3. **Classifique** por nome, itens ou tamanho

Visualizando Conteúdos da Tabela Hash

Clique em uma tabela para inspecionar todas as entradas:

- **Chave:** Chave da tabela hash
- **Valor:** Valor armazenado
- **Ações:** Botão de exclusão

Gerenciando Entradas Hash

Excluir Entrada Única

1. Selecione a tabela hash
2. Localize a entrada
3. Clique no botão **Excluir** (ícone de lixeira)
4. Confirme a ação

Resultado: Entrada removida da tabela hash

Limpar Tabela Inteira

1. Selecione a tabela hash
2. Clique no botão **Limpar Tabela**
3. **AVISO:** Confirma antes de limpar TODAS as entradas
4. Confirme a ação

Resultado: Todas as entradas removidas da tabela

Cuidado: Limpar tabelas pode causar interrupção temporária do serviço:

- Limpeza de `imei_msisdn`: Chamadas de emergência podem falhar até o novo registro
- Limpeza de `auth`: Desafios de autenticação em andamento falharão

- Limpeza de `service_routes`: Próxima solicitação será roteada via descoberta do I-CSCF

Visualização de Logs

URL: `/logs`

Recursos

Visualize logs de aplicação em tempo real a partir do painel de controle.

Recursos (implementação na dependência ControlPanel):

- Streaming de logs ao vivo
- Filtragem de nível de log
- Capacidades de busca e filtragem

Monitoramento e Métricas

Integração Prometheus

O OmniCall CSCF expõe métricas Prometheus para monitoramento e alerta.

Endpoint de Métricas:

```
http://<host>:9090/metrics
```

Cada host CSCF (P-CSCF, I-CSCF, S-CSCF) expõe métricas na porta 9090. Configure o Prometheus para coletar todos os hosts para visibilidade completa.

Para uma referência completa de todas as métricas P-CSCF, I-CSCF e S-CSCF, veja a [Referência de Métricas](#).

Métricas Disponíveis

As seguintes métricas são expostas pela aplicação do painel de controle OmniCall CSCF. Para métricas de componentes CSCF (SIP, Diameter, IMS, etc.), veja a [Referência de Métricas](#).

Métricas de VM

- `vm_memory_total` - Memória total da VM Erlang (bytes)
- `vm_memory_processes_used` - Memória usada por processos (bytes)
- `vm_memory_binary` - Memória binária (bytes)
- `vm_memory_ets` - Memória da tabela ETS (bytes)
- `vm_total_run_queue_lengths_total` - Comprimento total da fila de execução
- `vm_system_counts_process_count` - Contagem de processos
- `vm_system_counts_atom_count` - Contagem de átomos
- `vm_system_counts_port_count` - Contagem de portas

Métricas HTTP do Phoenix

- `phoenix_endpoint_stop_duration` - Duração da solicitação HTTP (milissegundos)
- `phoenix_router_dispatch_stop_duration` - Duração do despacho do roteador (milissegundos)

Métricas LiveView

- `phoenix_live_view_mount_stop_duration` - Duração de montagem do LiveView (milissegundos)

Métricas de Integração de Backend CSCF

- `cscf_backend_request_count` - Contagem de solicitações RPC de backend
 - Tags: `host`, `command`, `result`
- `cscf_backend_request_duration` - Duração RPC de backend (milissegundos)
 - Tags: `host`, `command`
- `cscf_backend_error_count` - Contagem de erros RPC de backend

- Tags: `host`, `error_type`

Painéis do Grafana

Status Atual: Métricas são expostas via endpoint Prometheus. Painéis do Grafana pré-construídos não estão atualmente incluídos, mas podem ser criados usando as métricas disponíveis.

Painéis de Dashboard Recomendados:

- Latência RPC de backend por comando
- Tendências de contagem de registros
- Tendências de contagem de diálogos
- Taxas de erro de backend
- Uso de memória da VM Erlang
- Desempenho de montagem do LiveView

Integração

Configure o Prometheus para coletar métricas de todos os hosts CSCF:

```
scrape_configs:
  - job_name: 'cscf_pcscf'
    static_configs:
      - targets: ['pcscf1.example.com:9090',
'pcscf2.example.com:9090']

  - job_name: 'cscf_icscf'
    static_configs:
      - targets: ['icscf1.example.com:9090',
'icscf2.example.com:9090']

  - job_name: 'cscf_scscf'
    static_configs:
      - targets: ['scscf1.example.com:9090',
'scscf2.example.com:9090']
```

Melhores Práticas

Diretrizes Operacionais

Monitoramento:

- Monitore métricas Prometheus para saúde do sistema
- Fique atento a erros RPC de backend
- Acompanhe o crescimento da memória da VM Erlang

Gerenciamento de Tabela Hash:

- Evite limpar tabelas em produção, a menos que absolutamente necessário
- Monitore o crescimento do tamanho da tabela para potenciais problemas de memória
- Use exclusão seletiva em vez de limpeza total da tabela

Solução de Problemas:

- Use Logs Ao Vivo para depuração em tempo real
- Verifique o status do par Diameter antes de investigar falhas de registro
- Verifique a conectividade do backend CSCF se o painel de controle mostrar erros

Desempenho:

- A atualização automática do painel de controle é de 5 segundos por padrão
- Listas de registro grandes usam paginação para evitar problemas de desempenho
- Operações de tabela hash são pesadas em leitura; minimize operações de gravação durante horários de pico

Documentação Relacionada

- **Guia de Operações do P-CSCF** - Operações específicas do P-CSCF
- **Guia de Operações do I-CSCF** - Operações específicas do I-CSCF

- **Guia de Operações do S-CSCF** - Operações específicas do S-CSCF
- **Guia de Operações do Diameter** - Gerenciamento de pares Diameter
- **Guia de Operações do CSCF** - Operações gerais do CSCF e solução de problemas

Guia de Operações do OmniCall CSCF

Índice

1. [Visão Geral](#)
2. [Entendendo a Arquitetura IMS](#)
3. [Fluxos de Sessão de Chamada](#)
4. [Componentes do CSCF](#)
5. [Operações Comuns](#)
6. [Solução de Problemas](#)
7. [Documentação Adicional](#)
8. [Glossário](#)

Visão Geral

OmniCall CSCF é uma solução IMS (IP Multimedia Subsystem) abrangente que fornece funções de Controle de Sessão de Chamada de nível carrier para provedores de serviços móveis e **fixos**. Construído sobre tecnologia open-source comprovada e aprimorado com capacidades de gerenciamento de nível empresarial, o OmniCall CSCF oferece a infraestrutura central de controle de sessão necessária para VoLTE, VoWiFi, RCS e serviços tradicionais de VoIP fixo.

O que é IMS?

O IP Multimedia Subsystem (IMS) é a arquitetura padronizada pela 3GPP para a entrega de serviços multimídia baseados em IP. Ele fornece:

- **Controle de sessão** para serviços de voz, vídeo e mensagens
- Gerenciamento de **Qualidade de Serviço (QoS)** para comunicações em tempo real
- **Convergência de serviços** em redes móveis, fixas e WiFi

- **Interoperabilidade baseada em padrões** com outros operadores e redes
- Capacidades de **Rich Communication Services (RCS)**
- **Convergência Fixa-Móvel (FMC)** para entrega de serviços unificados

OmniCall CSCF implementa todas as funções principais do CSCF definidas na 3GPP TS 23.228, fornecendo uma solução completa de núcleo IMS pronta para produção.

Componentes do OmniCall CSCF

OmniCall CSCF fornece gerenciamento completo de todos os elementos de rede do CSCF:

- **P-CSCF** (Proxy-CSCF) - Proxy de borda voltado para o usuário e âncora de segurança
- **E-CSCF** (Emergency-CSCF) - Roteamento de serviços de emergência (integrado com P-CSCF)
- **I-CSCF** (Interrogating-CSCF) - Ponto de entrada da rede e ocultação de topologia
- **S-CSCF** (Serving-CSCF) - Controle de sessão central, registro e acionamento de serviços

Capacidades Principais

Funções de Rede:

- Controle de sessão IMS totalmente compatível com 3GPP
- **Compatível com GSMA IR.92/IR.94** - Funciona com qualquer dispositivo compatível com padrões, sem necessidade de pacotes personalizados de operadora
- Suporte a VoLTE, VoWiFi e RCS
- Integração de serviço SIP fixo
- Suporte a serviços de emergência (E911/E112) com serviços de localização
- Ocultação de topologia e segurança de rede
- Associações de segurança baseadas em IPsec

- Integração de AAA e políticas baseadas em Diameter

Recursos de Serviço:

- Gerenciamento de sessão de chamada em tempo real
- Acionamento de serviços via Critérios de Filtro Iniciais (IFC)
- Integração de Servidor de Aplicação (AS) via interface ISC
- Integração de cobrança (online e offline)
- Aplicação de políticas de QoS via integração com PCRF
- Suporte a multi-inquilinos para cenários MVNO

Gerenciamento e Operações:

- Monitoramento em tempo real via painel de controle baseado na web
- Integração de métricas Prometheus (veja [Referência de Métricas](#))
- API RESTful para automação
- Cluster distribuído para alta disponibilidade
- Solução de problemas e diagnósticos ao vivo

Componentes Integrados:

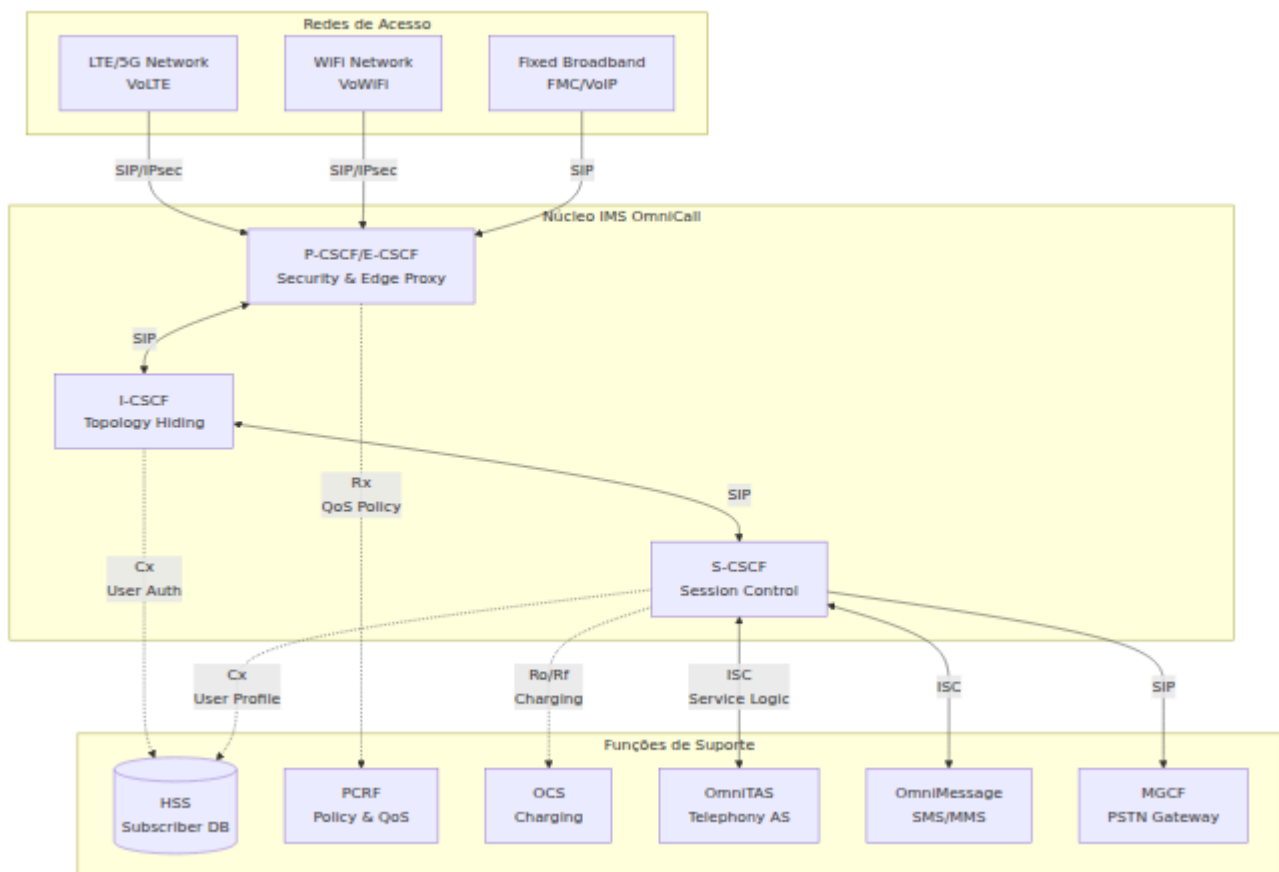
- **OmniePDG:** Evolved Packet Data Gateway para VoWiFi (compatível com IR.94)
- **OmniTAS:** Servidor de Aplicação de Telefonia para serviços suplementares
- **OmniMessage:** Servidor de Aplicação SMS/MMS (3GPP TS 24.341)

Para uso detalhado do painel de controle, veja [Operações da Interface Web](#).

Entendendo a Arquitetura IMS

Arquitetura da Rede IMS

A solução OmniCall CSCF está no coração da arquitetura IMS, fornecendo a camada de controle de sessão que conecta o equipamento do usuário aos serviços e gerencia todas as sessões de chamada.



Como os CSCFs Trabalham Juntos

As funções do CSCF trabalham como um sistema coordenado para lidar com sessões IMS:

1. P-CSCF - Primeiro Ponto de Contato

- O equipamento do usuário (dispositivos móveis, WiFi ou fixos) estabelece conexões seguras com o P-CSCF
- Fornece associações de segurança IPsec para dispositivos móveis
- Atua como o ponto de aplicação de políticas de QoS via integração com PCRF
- Lida com a travessia de NAT e ancoragem de mídia
- Roteia chamadas de emergência para a funcionalidade E-CSCF
- Mantém informações de localização do usuário

2. I-CSCF - Gateway de Rede & Balanceador de Carga

- Oculta a topologia interna da rede de redes externas

- Consulta o HSS para selecionar o S-CSCF apropriado para os usuários
- Realiza balanceamento de carga do S-CSCF com base em capacidades
- Atua como o ponto de entrada/saída para cenários de roaming
- Aplica Segurança de Domínio de Rede (NDS/TLS)

3. **S-CSCF** - Controlador de Sessão Central

- Realiza registro e autenticação de usuários
- Mantém o estado da sessão para todas as chamadas ativas
- Aplica políticas de roteamento e lógica de serviço
- Aciona Servidores de Aplicação com base em IFC (Critérios de Filtro Iniciais)
- Integra-se com sistemas de cobrança (online e offline)
- Gerencia serviços suplementares

Integração com Sistemas de Suporte

OmniCall CSCF integra-se com funções de suporte IMS via interfaces Diameter padrão 3GPP:

Interface	De → Para	Propósito	Especificação 3GPP
Cx	I-CSCF/S-CSCF ↔ HSS	Autenticação de usuário, recuperação de perfil, atribuição de S-CSCF	TS 29.228
Dx	I-CSCF ↔ SLF	Localizador de assinatura para ambientes multi-HSS	TS 29.229
Rx	P-CSCF ↔ PCRF	Autorização de política de QoS, controle de fluxo de mídia	TS 29.214
Ro	S-CSCF → OCS	Cobrança online (controle de crédito)	TS 32.299
Rf	S-CSCF → CDF	Cobrança offline (geração de CDR)	TS 32.299
ISC	S-CSCF ↔ AS	Acionamento de serviços e invocação de servidor de aplicação	TS 23.228
Sh	AS ↔ HSS	Acesso do servidor de aplicação aos dados do usuário	TS 29.328

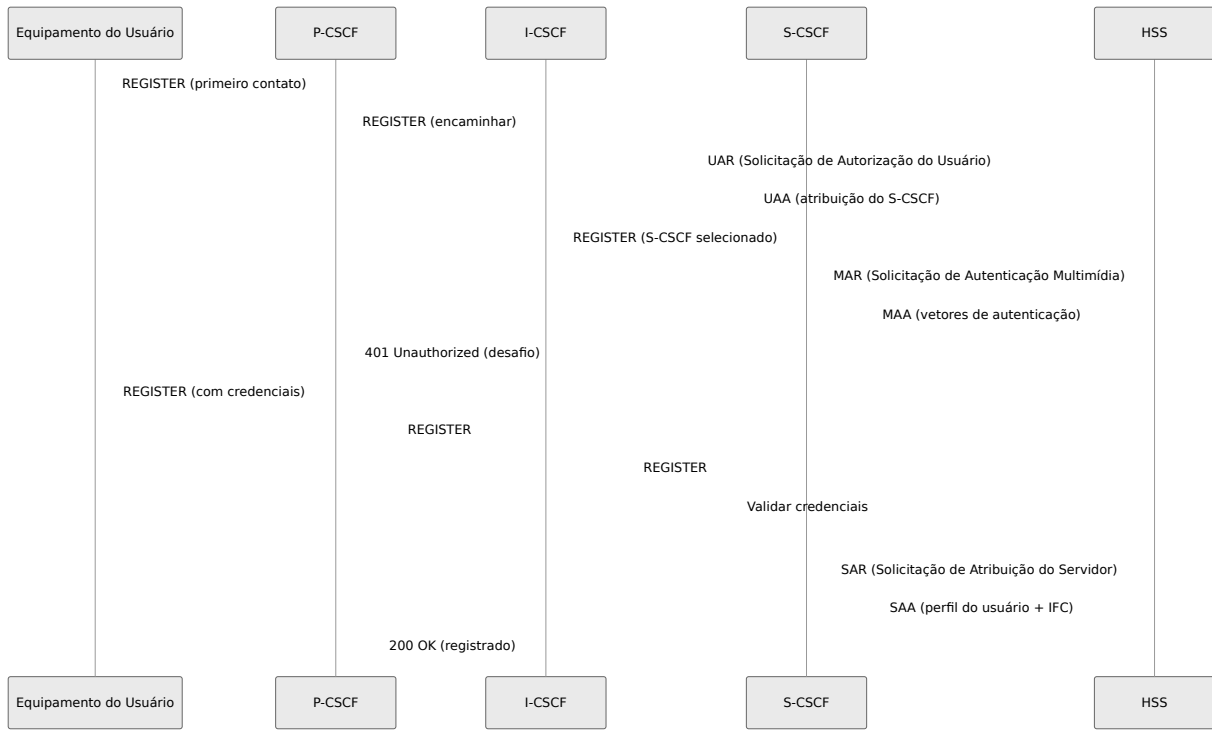
Para gerenciamento de pares Diameter, veja [Operações Diameter](#).

Fluxos de Sessão de Chamada

Entender como os CSCFs processam diferentes tipos de sessões é essencial para operações e solução de problemas.

Fluxo de Registro IMS

Quando um dispositivo se registra na rede IMS, os CSCFs coordenam para autenticar e autorizar o usuário:

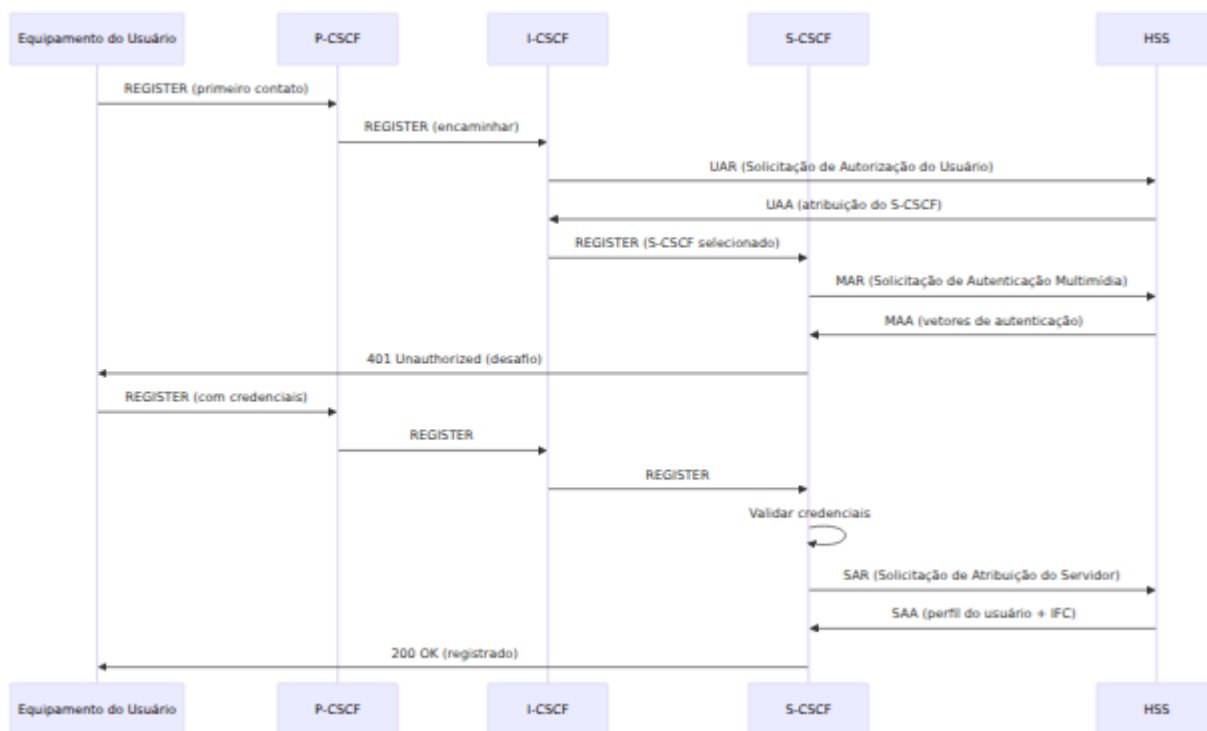


Pontos Chave:

- **P-CSCF** mantém a associação de segurança IPsec com o UE
- **I-CSCF** consulta o HSS para encontrar/atribuir S-CSCF
- **S-CSCF** realiza autenticação e armazena o perfil do usuário
- O perfil de serviço do usuário (IFC) determina quais Servidores de Aplicação serão acionados

Fluxo de Chamada Originada por M?vel

Quando um usuário registrado inicia uma chamada:

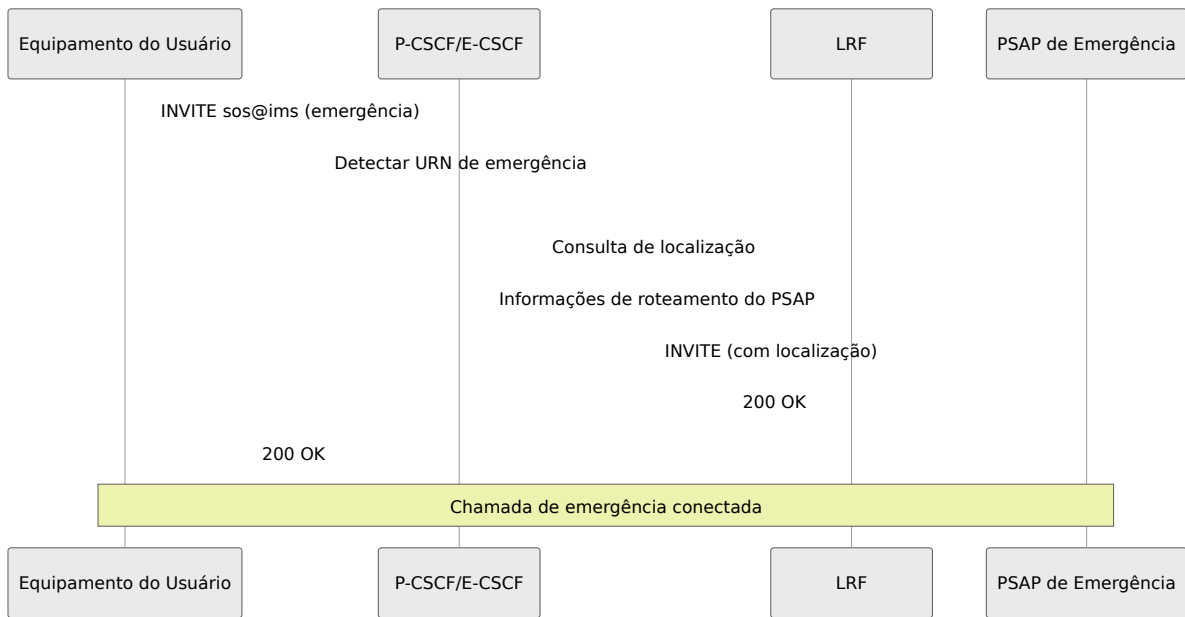


Pontos Chave:

- **P-CSCF** coordena com PCRF para estabelecimento de bearer QoS
- **S-CSCF** avalia IFC para determinar o acionamento do serviço
- **OmniTAS** fornece serviços de aplicação de telefonia (encaminhamento de chamadas, triagem, etc.)
- **OmniMessage** lida com tráfego SMS/MMS quando acionado por IFC
- Para monitorar chamadas ativas, veja [Gerenciamento de Diálogo S-CSCF](#)

Fluxo de Chamada de Emergência (E-CSCF)

Chamadas de emergência recebem tratamento especial para garantir conectividade mesmo sem registro completo no IMS:

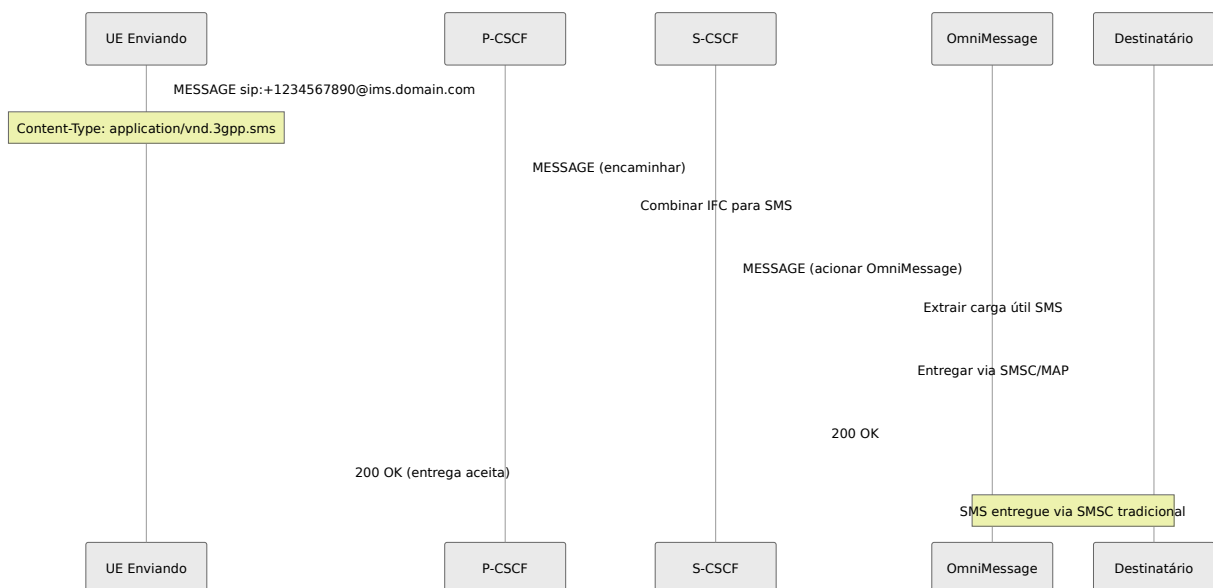


Pontos Chave:

- A funcionalidade E-CSCF está integrada ao **P-CSCF**
- Funciona mesmo para usuários não registrados ou em roaming
- Inclui armazenamento de número de retorno para serviços de emergência
- Para operações de emergência, veja **Serviços de Emergência P-CSCF**

SMS sobre IMS - Originado por Móvel (3GPP TS 24.341)

Quando um usuário envia um SMS via IMS, o OmniMessage gerencia a entrega da mensagem:

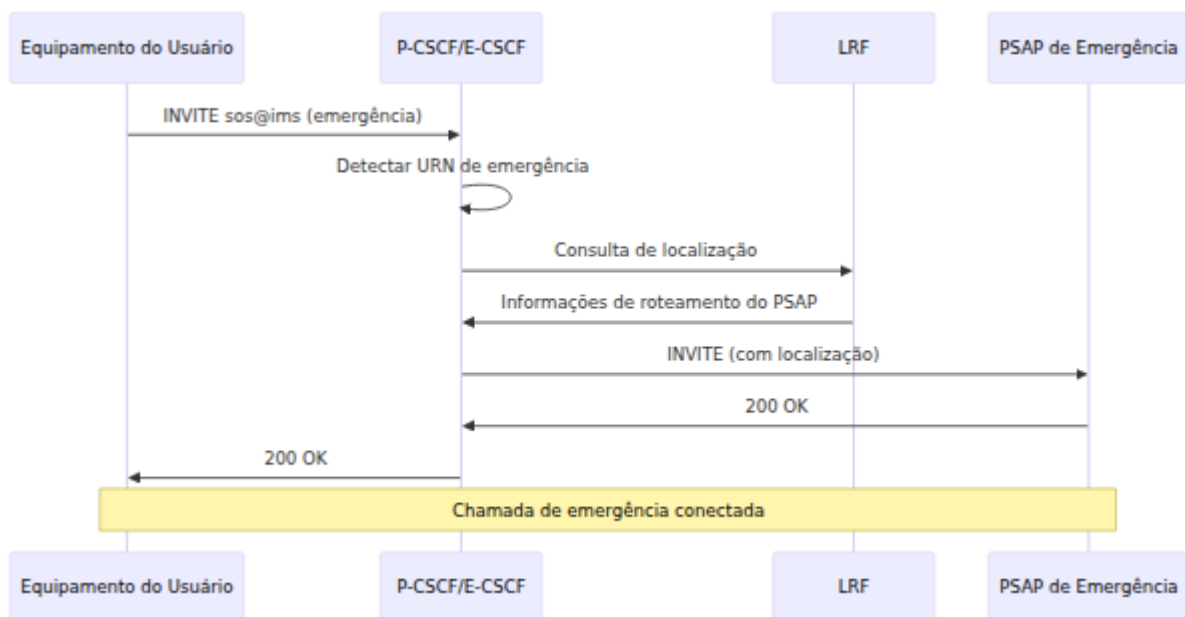


Pontos Chave:

- SMS codificado no método SIP MESSAGE conforme 3GPP TS 24.341
- Content-Type: `application/vnd.3gpp.sms` identifica a carga útil SMS
- **S-CSCF** IFC aciona **OmniMessage** para tráfego SMS
- OmniMessage se integra à infraestrutura tradicional de SMSC
- Suporta conjuntos de caracteres GSM-7, UCS-2 e mensagens concatenadas

SMS sobre IMS - Terminado por Móvel (3GPP TS 24.341)

Quando um SMS chega para um usuário registrado no IMS, o OmniMessage o roteia via IMS:



Pontos Chave:

- SMSC encaminha SMS para **OmniMessage** via protocolos tradicionais (MAP/SMPP)
- OmniMessage converte para o método SIP MESSAGE
- **S-CSCF** roteia com base no IMPU registrado
- Suporta relatórios de entrega e notificações de status
- Retorno ao SMS tradicional se o usuário não estiver registrado no IMS

Para operações e monitoramento de SMS, veja [Gerenciamento IFC S-CSCF](#).

Cenários de Roaming

OmniCall CSCF suporta **roaming roteado pela casa** conforme exigido pelos padrões 3GPP/GSMA:

Roaming Roteado pela Casa: Quando os usuários fazem roaming em uma rede visitada, todas as sessões IMS são roteadas de volta através do S-CSCF da rede de origem. Isso garante:

- Experiência de serviço consistente, independentemente da localização
- Controle da rede de origem sobre acionamento de serviços e cobrança
- Acordos de roaming simplificados entre operadores
- Conformidade com os padrões GSMA PRD IR.92 e IR.94

O I-CSCF da rede visitada consulta o HSS da casa e roteia solicitações de registro/sessão para o S-CSCF da casa, que então invoca servidores de aplicação da rede de origem (OmniTAS, OmniMessage, etc.).

Para detalhes de configuração de roaming, veja [Segurança de Domínio de Rede I-CSCF](#).

Componentes do CSCF

P-CSCF/E-CSCF - Proxy de Borda e Âncora de Segurança

O **Proxy-CSCF** é o primeiro elemento IMS que o equipamento do usuário contata. Ele serve como a fronteira de segurança e ponto de aplicação de políticas.

Funções Principais:

- **Gerenciamento de Associação de Segurança:** Estabelece e mantém túneis IPsec com dispositivos móveis para proteção de sinalização e mídia

- **Aplicação de Política de QoS:** Coordena com PCRF via interface Rx para autorizar e aplicar bearers de QoS
- **Travessia de NAT:** Lida com a travessia de NAT para dispositivos atrás de NAT/firewalls
- **Compressão:** Suporte a SigComp para redes com largura de banda restrita
- **Rota de Serviço:** Mantém a rota de serviço para solicitações subsequentes

Serviços de Emergência (E-CSCF):

- Roteamento de chamadas de emergência integrado sem exigir registro completo no IMS
- Manipulação de informações de localização para E911/E112
- Mapeamento de IMEI para número de retorno para chamadas de emergência
- Integração com LRF (Função de Recuperação de Localização)

Tipos de Acesso Suportados:

- LTE/5G (VoLTE) via IPsec
- WiFi (VoWiFi) via IPsec
- Banda larga fixa via SIP
- Gateways residenciais de cabo/DSL

Para operações detalhadas, veja [Documentação P-CSCF](#).

I-CSCF - Ocultação de Topologia e Balanceamento de Carga

O **Interrogating-CSCF** atua como o ponto de contato dentro da rede de um operador para conexões de outras redes ou da mesma rede.

Funções Principais:

- **Ocultação de Topologia:** Protege a estrutura interna da rede de redes externas

- **Atribuição de S-CSCF:** Consulta o HSS via interface Cx para atribuir S-CSCF a novos usuários
- **Seleção de S-CSCF:** Seleciona o S-CSCF apropriado com base em capacidades e carga
- **Proxy de Roteamento:** Roteia solicitações de entrada para o S-CSCF atribuído
- **Segurança de Domínio de Rede:** Aplica NDS/TLS para segurança entre operadores

Recursos Chave:

- **Suporte a Multi-S-CSCF:** Distribui usuários entre várias instâncias de S-CSCF
- **Correspondência de Capacidades:** Combina requisitos do usuário com capacidades do S-CSCF
- **Suporte a Roaming:** Lida com cenários de roaming roteado pela casa e local
- **Localizador de Assinatura:** Suporte à interface Dx para ambientes multi-HSS

Casos de Uso:

- Ponto de interconexão para parceiros de roaming
- Distribuição de carga entre o cluster de S-CSCF
- Roteamento geográfico para recuperação de desastres
- Segregação de tráfego MVNO

Para operações detalhadas, veja [Documentação I-CSCF](#).

S-CSCF - Controlador de Sessão Central

O **Serving-CSCF** é o componente central da rede IMS, fornecendo controle de sessão e inteligência de serviço.

Funções Principais:

- **Registro:** Autentica usuários e mantém vínculos de registro

- **Controle de Sessão:** Gerencia todos os estados de chamada (estabelecimento de diálogo, modificação, término)
- **Acionamento de Serviço:** Avalia Critérios de Filtro Iniciais (IFC) para invocar Servidores de Aplicação
- **Roteamento:** Roteia solicitações SIP com base na lógica de serviço e preferências do usuário
- **Integração de Cobrança:** Coordena com sistemas de cobrança online (OCS) e offline (CDF)

Acionamento de Serviço via IFC: O S-CSCF usa Critérios de Filtro Iniciais baseados em XML baixados do HSS para determinar quando roteirizar chamadas através de Servidores de Aplicação (como **OmniTAS** para serviços de telefonia e **OmniMessage** para SMS/MMS):

- **Pontos de Acionamento:** Correspondência no método SIP, Request-URI, Session-Case (originando/terminando)
- **Baseado em Prioridade:** IFC processado em ordem de prioridade
- **Encadeamento de Serviços:** Múltiplos AS podem ser invocados em sequência (por exemplo, OmniTAS → OmniMessage)
- **Tratamento Padrão:** Comportamento configurável quando AS está inacessível

Serviços Suportados:

- Encaminhamento de chamadas (ocupado, sem resposta, incondicional)
- Bloqueio de chamadas (saindo, entrando, roaming)
- Triagem e filtragem de chamadas
- Tradução e roteamento de números
- Cobrança pré-paga/pós-paga
- Rastreamento de uso e aplicação de cotas
- Serviços suplementares (espera de chamada, hold, transferência)

Recursos de Escalabilidade:

- Armazenamento de diálogo distribuído
- Manipulação de sessão com estado
- Perfis de usuário baseados em banco de dados

- Escalonamento horizontal via distribuição I-CSCF

Para operações detalhadas, veja [Documentação S-CSCF](#).

Gerenciamento de Interface Diameter

OmniCall CSCF fornece gerenciamento abrangente de pares Diameter em todos os componentes do CSCF.

Aplicações Diameter Suportadas:

Aplicação	Interface	App ID	Usado Por	Propósito
3GPP Cx	Cx	16777216	I-CSCF, S-CSCF	Autenticação de usuário, recuperação de perfil
3GPP Dx	Dx	16777216	I-CSCF	Localização de assinatura em multi-HSS
3GPP Rx	Rx	16777236	P-CSCF	Autorização de política, controle de QoS
3GPP Ro	Ro	4 (CC)	S-CSCF	Cobrança online (controle de crédito)
3GPP Rf	Rf	3 (Accounting)	S-CSCF	Cobrança offline (CDR)
3GPP Sh	Sh	16777217	AS	Acesso a dados do usuário a partir de AS

Capacidades Diameter:

- Descoberta automática de pares via DNS
- Suporte a failover e redundância
- Gerenciamento de conexão e watchdog
- Estatísticas e monitoramento por par
- Habilitar/desabilitar pares dinamicamente

Para operações e solução de problemas Diameter, veja [Guia de Gerenciamento Diameter](#).

Operações Comuns

OmniCall CSCF fornece capacidades operacionais abrangentes através de seu painel de controle baseado na web. Esta seção cobre tarefas operacionais comuns e sua importância.

Gerenciamento de Registro

Entendendo os Registros IMS:

O registro IMS é um processo de dois níveis:

- **Contato P-CSCF:** O equipamento do usuário estabelece conexão IPsec/SIP com o P-CSCF
- **Registro S-CSCF:** Registro completo no IMS com autenticação via HSS

Principais Operações de Registro:

- **Visualizar registros ativos** em P-CSCF e S-CSCF
- **Consultar usuários específicos** por IMPU, IMSI ou endereço IP
- **Monitorar estado de registro** (autenticado, ativo, expirado)
- **Forçar desregistro** para solução de problemas ou fins administrativos
- **Rastrear expiração de registro** para identificar problemas de re-registro

Para procedimentos detalhados de registro, veja:

- [Gerenciamento de Contato P-CSCF](#)

- [Operações de Registro S-CSCF](#)
-

Monitoramento de Sessão de Chamada

Gerenciamento de Diálogo (Sessão):

O S-CSCF mantém o estado de todas as sessões IMS ativas (chamadas). Os operadores podem:

- **Monitorar diálogos ativos** incluindo Call-ID, participantes e estado da sessão
- **Visualizar detalhes do diálogo** como SDP (parâmetros de mídia), conjuntos de rota e temporizadores
- **Encerrar diálogos** para solução de problemas ou situações de emergência
- **Rastrear duração da sessão** e detectar sessões longas ou travadas

Estados da Sessão:

- **Inicial:** Chamada está tocando, ainda não atendida
- **Confirmada:** Chamada ativa com mídia fluindo
- **Terminada:** Chamada encerrada normalmente

Para procedimentos de monitoramento de chamadas, veja [Gerenciamento de Diálogo S-CSCF](#).

Acionamento de Serviço e Gerenciamento de IFC

Crítérios de Filtro Iniciais (IFC) determinam quando e como o S-CSCF roteia sessões para servidores de aplicação como **OmniTAS** e **OmniMessage**.

Operações IFC:

- **Despejar IFC do usuário** para visualizar o perfil de serviço configurado a partir do HSS

- **Testar correspondência de IFC** com cenários de chamada simulados
- **Verificar roteamento de AS** para garantir a invocação adequada do serviço
- **Depurar falhas de serviço** examinando a avaliação do ponto de acionamento

Exemplo de Estrutura IFC:

```
<InitialFilterCriteria>
  <Priority>10</Priority>
  <TriggerPoint>
    <SPT><Method>INVITE</Method></SPT>
    <SPT><SessionCase>0</SessionCase><!-- Originando --></SPT>
  </TriggerPoint>
  <ApplicationServer>
    <ServerName>sip:omnitas.ims.example.com</ServerName>
    <DefaultHandling>0</DefaultHandling><!-- Deve invocar -->
  </ApplicationServer>
</InitialFilterCriteria>
```

Para testes e solução de problemas de IFC, veja [Operações IFC S-CSCF](#).

Gerenciamento de Pares Diameter

Monitorando Conectividade Diameter:

OmniCall CSCF depende de interfaces Diameter para HSS, PCRF e integração de cobrança. Os operadores podem:

- **Monitorar status do par** (I_Open = conectado, Closed = desconectado)
- **Visualizar capacidades do par** (aplicações Diameter suportadas)
- **Habilitar/desabilitar pares** para manutenção ou teste de failover
- **Rastrear estatísticas do par** (solicitações, falhas, timeouts)

Conexões Diameter Críticas:

- **Cx para HSS** (I-CSCF, S-CSCF): Autenticação de usuários e perfis

- **Rx para PCRF** (P-CSCF): Política de QoS e controle de bearer
- **Ro para OCS** (S-CSCF): Cobrança online e controle de crédito

Para solução de problemas Diameter, veja [Guia de Operações Diameter](#).

Gerenciamento de Serviços de Emergência

Operações E-CSCF:

O tratamento de chamadas de emergência requer atenção operacional especial:

- **Monitorar mapeamentos de IMEI para número de retorno** para chamadas de emergência
- **Verificar disponibilidade de informações de localização** para E911/E112
- **Testar roteamento de chamadas de emergência** sem conexão real com PSAP
- **Gerenciar registro de emergência** para dispositivos não provisionados

Os serviços de emergência funcionam mesmo para:

- Usuários não registrados
- Usuários sem SIM/credenciais inválidas
- Usuários em roaming de outras redes

Para operações de emergência, veja [Serviços de Emergência P-CSCF](#).

Gerenciamento de Tabelas Hash

Estruturas de Dados em Memória Compartilhada:

Os nós CSCF usam tabelas hash em memória para dados críticos de desempenho:

Tabela Hash	CSCF	Propósito	TTL
imei_msisdn	P-CSCF	Mapeamento de retorno de chamada de emergência	24 horas
service_routes	P-CSCF	Rotas de serviço em cache	Expiração de registro
auth	S-CSCF	Vetores de autenticação	Timeout de desafio

Operações:

- **Visualizar conteúdos da tabela** para solução de problemas
- **Excluir entradas específicas** para limpar dados obsoletos
- **Limpar tabelas inteiras** para recuperação de emergência (usar com cautela)

Para operações detalhadas da interface, veja o [Guia de Operações da Interface Web](#).

Solução de Problemas

Esta seção cobre problemas operacionais comuns e suas estratégias de resolução.

Falhas de Registro

Sintomas: Usuários incapazes de se registrar na rede IMS, timeouts de registro

Causas Raiz Comuns:

1. Problemas de Conectividade com HSS

- Verifique o status do par Diameter Cx no **I-CSCF** e **S-CSCF**
- Verifique se o HSS está acessível e respondendo a solicitações UAR/MAR

- Verifique problemas de roteamento Diameter

2. Falhas de Autenticação

- Verifique se as credenciais do usuário estão provisionadas no HSS
- Verifique a geração de vetores de autenticação (MAR/MAA)
- Verifique a compatibilidade do algoritmo AKA (Milenage)

3. Conectividade P-CSCF

- Verifique o estabelecimento de SA IPsec para dispositivos móveis
- Verifique a travessia de NAT para dispositivos atrás de NAT
- Verifique a descoberta do P-CSCF (DNS, DHCP ou configuração estática)

4. Atribuição de S-CSCF

- Verifique a lógica de seleção de S-CSCF do I-CSCF
- Verifique se as capacidades do S-CSCF correspondem aos requisitos do usuário
- Verifique a capacidade do S-CSCF (limites de registro)

Para solução de problemas detalhada, veja guias específicos de componentes:

- [Solução de Problemas P-CSCF](#)
- [Solução de Problemas I-CSCF](#)
- [Solução de Problemas S-CSCF](#)

Falhas na Configuração de Chamadas

Sintomas: Chamadas falham ao estabelecer, recebem erros SIP 4xx/5xx

Causas Raiz Comuns:

1. Usuário Não Registrado

- Verifique se os usuários de origem e destino estão registrados no IMS
- Verifique o status de registro via [S-CSCF](#)

2. Problemas de IFC/Acionamento de Serviço

- Verifique se o IFC baixado do HSS (verifique SAR/SAA)
- Teste a correspondência de IFC para o cenário de chamada
- Verifique a disponibilidade do OmniTAS/OmniMessage se acionado

3. Problemas de QoS/PCRF

- Verifique o status do par Diameter Rx no P-CSCF
- Verifique a autorização da política de QoS do PCRF
- Verifique se os recursos de bearer estão disponíveis na rede de acesso

4. Falhas de Roteamento

- Verifique o roteamento de destino (ENUM, tradução de números)
- Verifique a configuração de interconexão/MGCF para chamadas PSTN
- Verifique o roteamento de roaming para chamadas off-net

Problemas de Conectividade Diameter

Sintomas: Par Diameter mostra estado "Closed", operações expirando

Passos de Diagnóstico:

1. **Verifique o Status do Par:** Use o painel de controle para visualizar o estado do par Diameter
2. **Verifique a Conectividade de Rede:** Teste a acessibilidade IP para o par Diameter (porta 3868)
3. **Verifique as Capacidades:** Verifique se os IDs de Aplicação correspondem entre os pares
4. **Revise o Watchdog:** Verifique as trocas de watchdog Diameter (DWR/DWA)

Interfaces Diameter Críticas:

Interface	Impacto se Desligada	Prioridade de Recuperação
Cx (HSS)	Sem novos registros, sem atualizações de IFC	Crítica - imediata
Rx (PCRF)	Sem QoS para novas chamadas	Alta - dentro de minutos
Ro (OCS)	Sem cobrança pré-paga, o serviço pode continuar	Alta - depende da política

Para solução de problemas Diameter, veja [Guia de Operações Diameter](#).

Problemas de Entrega de SMS

Sintomas: SMS não entregue via IMS, retorno ao SMSC legado

Causas Raiz Comuns:

1. OmniMessage Não Acionado

- Verifique se o IFC está configurado para acionar OmniMessage para solicitações MESSAGE
- Verifique a prioridade do IFC (deve ser maior que outros AS)
- Teste a correspondência de IFC com SMS simulado

2. Integração com SMSC

- Verifique a conectividade do OmniMessage com a SMSC (MAP/SMPP)
- Verifique a conversão de formato de mensagem (SIP MESSAGE ↔ SMS PDU)
- Verifique o roteamento de assinantes na SMSC

3. Problemas de Tipo de Conteúdo

- Verifique `Content-Type: application/vnd.3gpp.sms` no SIP MESSAGE

- Verifique a codificação do conjunto de caracteres (GSM-7, UCS-2)

Para solução de problemas de SMS, veja [Gerenciamento IFC S-CSCF](#).

Problemas de Chamada de Emergência

Sintomas: Chamadas de emergência não roteadas para PSAP, localização não incluída

Causas Raiz Comuns:

1. Detecção E-CSCF

- Verifique a detecção de URN de emergência (urn:service:sos)
- Verifique as regras de roteamento de emergência no P-CSCF
- Verifique a conectividade com LRF

2. Informações de Localização

- Verifique o cabeçalho de localização no SIP INVITE
- Verifique o mapeamento de IMEI para número de retorno para chamadas de emergência
- Teste a recuperação de localização do LRF

3. Roteamento PSAP

- Verifique a configuração da tabela de roteamento do PSAP
- Verifique a geração de ESQK (Chave de Consulta de Serviço de Emergência)
- Verifique a conexão/tronco com o PSAP

Para operações de serviços de emergência, veja [Serviços de Emergência P-CSCF](#).

Degradação de Desempenho

Sintomas: Configuração de chamada lenta, atrasos de registro, alta latência

Diagnóstico:

1. **Monitore Métricas Prometheus:** Verifique as métricas de desempenho do CSCF (veja [Referência de Métricas](#) para definições completas de métricas)
2. **Desempenho do Banco de Dados:** Verifique os tempos de consulta do banco de dados S-CSCF
3. **Latência de Rede:** Verifique a latência entre os nós CSCF
4. **Utilização de Recursos:** Monitore CPU, memória e rede nos servidores CSCF

Considerações de Escalabilidade:

- **P-CSCF:** ~50.000 SAs IPsec por instância (VoLTE); 100.000+ via OmniePDG (VoWiFi)
- **I-CSCF:** Stateless, escala horizontalmente (1.000-5.000 registros/segundo por instância)
- **S-CSCF:** 100.000-500.000 registros por instância; 20.000-100.000 diálogos simultâneos

Para planejamento de capacidade e dimensionamento detalhado, veja o [Guia de Capacidade e Dimensionamento](#).

Para monitoramento de desempenho e métricas, veja o [Guia de Operações da Interface Web](#).

Documentação Adicional

Guias de Operações Específicos de Componentes

Para operações detalhadas e solução de problemas para cada componente CSCF:

- [Guia de Operações P-CSCF/E-CSCF](#) - Proxy de borda, associações de segurança, serviços de emergência

- **Guia de Operações I-CSCF** - Seleção de S-CSCF, ocultação de topologia, roaming
- **Guia de Operações S-CSCF** - Registro, gerenciamento de diálogo, operações IFC
- **Guia de Operações Diameter** - Gerenciamento e solução de problemas de pares Diameter
- **Guia de Operações da Interface Web** - Uso do painel de controle, monitoramento e administração
- **Referência de Métricas** - Referência completa de todas as métricas Prometheus do P-CSCF, I-CSCF e S-CSCF
- **Guia de Capacidade e Dimensionamento** - Dimensionamento de implantação, planejamento de capacidade, ajuste de desempenho

Conformidade Regulatória

- **Conformidade de Interceptação ANSSI R226** - Capacidades de interceptação legal conforme exigido pelas autoridades regulatórias francesas

Referência de Padrões 3GPP

OmniCall CSCF implementa as seguintes especificações 3GPP:

Especificação	Título	Relevância
TS 23.228	IP Multimedia Subsystem (IMS) - Stage 2	Arquitetura central do IMS
TS 24.229	Protocolo de controle de chamada multimídia IP (SIP)	Perfil SIP IMS
TS 29.228	Interfaces Cx e Dx (CSCF-HSS)	Dados do usuário e autenticação
TS 29.214	Interface Rx (P-CSCF-PCRF)	Controle de política de QoS
TS 32.299	Cobrança - Aplicações Diameter	Cobrança online/offline
TS 24.341	SMS sobre redes IP	SMS sobre IMS
TS 23.167	Serviços de emergência	E-CSCF e chamadas de emergência

Conformidade com Padrões GSMA

OmniCall CSCF é totalmente compatível com perfis IMS da GSMA, garantindo interoperabilidade com dispositivos prontos para o mercado:

IR.92 - Perfil IMS para Voz e SMS (VoLTE)

GSMA PRD IR.92 define o perfil IMS obrigatório para serviços VoLTE, garantindo que dispositivos comerciais funcionem perfeitamente sem configuração personalizada da operadora ou atrasos na certificação de dispositivos.

Principais Benefícios do IR.92 para OmniCall CSCF:

- ✓ **Suporte a Dispositivos de Mercado Aberto:** Qualquer smartphone compatível com IR.92 funciona imediatamente—sem pacotes personalizados de operadora, APNs proprietárias ou provisionamento especial necessário
- ✓ **Perfil SIP Padronizado:** Dispositivos usam cabeçalhos SIP padrão, autenticação e fluxos de registro conforme definido na 3GPP TS 24.229
- ✓ **Interoperabilidade de Codec:** Suporte a codec obrigatório (AMR-WB para HD Voice) garante qualidade de voz consistente em todos os dispositivos
- ✓ **SMS sobre IMS:** Integração com **OmniMessage** fornece entrega de SMS baseada em padrões (TS 24.341) para qualquer dispositivo compatível com IR.92
- ✓ **Serviços de Emergência:** Manipulação de números de emergência E.164 (911, 112, etc.) funciona em todos os dispositivos compatíveis sem configuração especial
- ✓ **Consistência de Roaming:** Roaming roteado pela casa garante que os usuários tenham a mesma experiência VoLTE ao visitar outras redes compatíveis com IR.92

O que isso significa: Os operadores podem lançar serviços VoLTE imediatamente com dispositivos de consumo existentes (iPhone, Samsung, Google Pixel, etc.) sem esperar pela certificação personalizada de dispositivos ou atualizações de pacotes de operadora.

IR.94 - Perfil IMS para Voz, Vídeo e SMS (VoWiFi)

GSMA PRD IR.94 estende o IR.92 para incluir Voz sobre WiFi, permitindo serviços VoLTE sobre redes WiFi não confiáveis.

Arquitetura VoWiFi com OmniCall:



Componentes VoWiFi:

- **OmniePDG:** Evolved Packet Data Gateway - Fornece terminação de túnel IPsec para acesso WiFi não confiável

- **OmniCall P-CSCF:** Lida com registros VoWiFi de forma idêntica ao VoLTE (mesmas rotas de serviço, mesmo acionamento de IFC)
- **Transferência Sem Costura:** Dispositivos podem se mover entre LTE e WiFi sem interrupção de chamada

Benefícios do IR.94:

- Os mesmos benefícios do IR.92 se aplicam ao VoWiFi
- Dispositivos descobrem automaticamente o ePDG via DNS (sem configuração manual)
- Um único registro IMS cobre tanto VoLTE quanto VoWiFi
- Extensão de cobertura interna sem femtocells ou DAS

Para operações e solução de problemas do ePDG, veja [Documentação OmniePDG](#).

Outros Padrões GSMA

- **IR.51** - Estrutura do Banco de Dados de Roaming GSMA
- **IR.88** - Diretrizes de Roaming LTE
- **AA.80** - Configuração de Dispositivos IMS/RCS e Serviços de Suporte

Diferenciação do Produto

Por que escolher OmniCall CSCF?

- ✓ **Suporte a Dispositivos Plug-and-Play:** Compatível com GSMA IR.92/IR.94 - funciona com iPhones, Androids e dispositivos fixos prontos para o mercado sem pacotes personalizados de operadora ou atrasos na certificação de dispositivos
- ✓ **Solução IMS Completa:** Todos os componentes CSCF (P/I/S/E) mais OmniePDG para VoWiFi em uma plataforma unificada
- ✓ **Convergência Fixa-Móvel:** Núcleo IMS unificado para serviços móveis (VoLTE/VoWiFi), banda larga fixa e serviços de telefonia por cabo

- ✓ **Provisionamento Zero Touch:** Descoberta de dispositivo baseada em padrões (DNS, DHCP) significa que os usuários podem trocar cartões SIM entre dispositivos sem suporte de TI
- ✓ **Gerenciamento Empresarial:** Painel de controle baseado na web com monitoramento em tempo real, diagnósticos e solução de problemas
- ✓ **Escalabilidade de Nível Carrier:** Escalonamento horizontal para suportar milhões de assinantes com tempos de configuração de chamada de sub-segundo
- ✓ **Ecosistema de Servidores de Aplicação:** Integração perfeita com OmniTAS (serviços de telefonia) e OmniMessage (SMS/MMS)
- ✓ **Serviços de Emergência:** E-CSCF embutido com suporte a E911/E112, serviços de localização e manipulação de chamadas de retorno
- ✓ **Interoperabilidade em Primeiro Lugar:** Total conformidade com 3GPP e GSMA garante que acordos de roaming e interconexão funcionem imediatamente
- ✓ **Comprovado em Produção:** Implantado em redes de nível 1, nível 2 e MVNO em todo o mundo atendendo milhões de assinantes

Glossário

Termos da Arquitetura IMS

- **3GPP:** 3rd Generation Partnership Project - Organismo de padrões para telecomunicações móveis
- **AKA:** Authentication and Key Agreement - Mecanismo de segurança para IMS
- **AoR:** Address of Record - Identidade SIP (por exemplo, sip:user@domain.com)
- **CSCF:** Call Session Control Function - Entidade de controle de sessão IMS
- **DAS:** Distributed Antenna System - Solução de cobertura interna

- **E-CSCF**: Emergency CSCF - Função de roteamento de chamadas de emergência
- **ePDG**: Evolved Packet Data Gateway - Ponto de terminação de túnel IPsec para acesso WiFi não confiável
- **ENUM**: E.164 Number Mapping - Tradução de números baseada em DNS
- **ESQK**: Emergency Service Query Key - Identificador de chamada de emergência
- **FMC**: Fixed-Mobile Convergence - Serviços unificados em tipos de acesso
- **GSMA**: GSM Association - Organização de padrões da indústria móvel
- **HD Voice**: High Definition Voice - Áudio de banda larga usando codec AMR-WB
- **HSS**: Home Subscriber Server - Banco de dados de assinantes e autenticação
- **I-CSCF**: Interrogating CSCF - Ponto de entrada da rede e ocultação de topologia
- **IFC**: Initial Filter Criteria - Regras de acionamento de serviço baseadas em XML
- **IMS**: IP Multimedia Subsystem - Arquitetura 3GPP para serviços baseados em IP
- **IMPU**: IP Multimedia Public Identity - Identidade pública do usuário (URI SIP ou URI tel)
- **IMSI**: International Mobile Subscriber Identity - Identificador do assinante
- **IR.92**: GSMA IMS Profile for Voice and SMS - Padrão de interoperabilidade VoLTE
- **IR.94**: GSMA IMS Profile for Conversational Video - Padrão de interoperabilidade VoWiFi
- **ISC**: IMS Service Control - Interface entre S-CSCF e Servidores de Aplicação
- **LRF**: Location Retrieval Function - Serviços de localização de emergência
- **MGCF**: Media Gateway Control Function - Interconexão PSTN
- **MVNO**: Mobile Virtual Network Operator - Operador sem infraestrutura de rádio própria
- **NDS**: Network Domain Security - Segurança entre operadores (TLS/IPsec)
- **P-CSCF**: Proxy CSCF - Proxy de borda e primeiro ponto de contato

- **PSAP:** Public Safety Answering Point - Central de atendimento de serviços de emergência
- **RCS:** Rich Communication Services - Serviços de mensagens aprimorados
- **S-CSCF:** Serving CSCF - Controle de sessão central e registro
- **SPT:** Service Point Trigger - Condição de correspondência no IFC (Método, Request-URI, etc.)
- **SWu:** Interface 3GPP entre UE e ePDG (IPsec/IKEv2)
- **UE:** User Equipment - Dispositivo do usuário (telefone, tablet, terminal fixo)
- **VoLTE:** Voice over LTE - Serviços de voz via rede de dados LTE
- **VoWiFi:** Voice over WiFi - Serviços de voz via redes WiFi não confiáveis

Termos do Protocolo Diameter

- **AAA:** Authentication, Authorization, Accounting
- **AVP:** Attribute-Value Pair - Elemento de dados da mensagem Diameter
- **CCR/CCA:** Credit-Control-Request/Answer - Mensagens de cobrança online
- **CDF:** Charging Data Function - Coletor de cobrança offline
- **Cx:** Interface Diameter entre I-CSCF/S-CSCF e HSS
- **Diameter:** Protocolo AAA usado em IMS (evolução do RADIUS)
- **Dx:** Interface Diameter entre I-CSCF e SLF (localizador de assinatura)
- **DWR/DWA:** Device-Watchdog-Request/Answer - Verificação de saúde do par
- **MAR/MAA:** Multimedia-Auth-Request/Answer - Solicitação de vetor de autenticação
- **OCS:** Online Charging System - Cobrança em tempo real e controle de crédito
- **PCRF:** Policy and Charging Rules Function - Servidor de política de QoS
- **Rf:** Interface Diameter para cobrança offline (contabilidade)
- **Ro:** Interface Diameter para cobrança online (controle de crédito)
- **Rx:** Interface Diameter entre P-CSCF e PCRF (autorização de QoS)
- **SAR/SAA:** Server-Assignment-Request/Answer - Download do perfil do usuário
- **Sh:** Interface Diameter entre AS e HSS (acesso a dados do usuário)

- **SLF:** Subscription Locator Function - Localização do HSS em ambiente multi-HSS
- **UAR/UAA:** User-Authorization-Request/Answer - Seleção do S-CSCF

Termos do Produto OmniCall

- **OmniCall CSCF:** Solução completa IMS CSCF (este produto)
- **OmniePDG:** Evolved Packet Data Gateway - Terminação de túnel IPsec para VoWiFi (compatível com IR.94)
- **OmniTAS:** Servidor de Aplicação de Telefonia - Fornece serviços de telefonia suplementares
- **OmniMessage:** Servidor de Aplicação de Mensagens - SMS/MMS sobre IMS (TS 24.341)

Termos do Protocolo SIP

- **Diálogo:** Estado de sessão SIP entre dois pontos finais
- **INVITE:** Método SIP para estabelecimento de sessão (chamadas)
- **MESSAGE:** Método SIP para mensagens instantâneas (incluindo SMS sobre IMS)
- **REGISTER:** Método SIP para registro de usuário
- **SDP:** Session Description Protocol - Parâmetros de mídia (codecs, portas)
- **SIP:** Session Initiation Protocol - Protocolo de sinalização para IMS