# Diameter □作指南

## 目录


1. □述
2. IMS 架构中的 Diameter
3. Diameter 接口
4. 通过 OmniWeb 进行对等管理
5. Diameter 结果代码
6. 常见问题


## 概述

Diameter 是 IMS 架构的认证、授权和计费（AAA）协议。OmniCSCF 使用 Diameter 与关键网络元素进行通信。这些元素包括 HSS、PCRF 和 OCS。

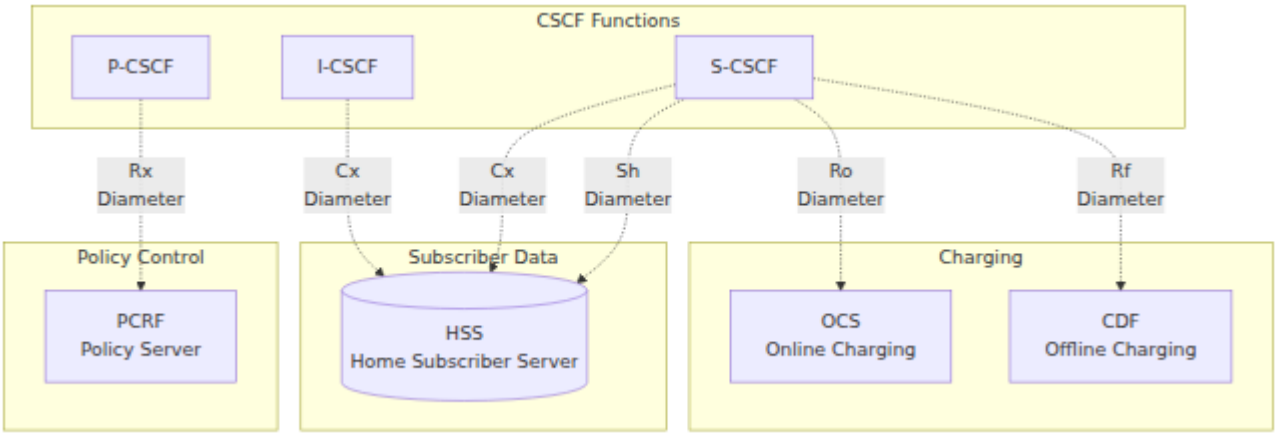
## 什么是 **Diameter**?

Diameter (RFC 6733) 是 RADIUS 的继任者。Diameter 支持现代 AAA 场景:

- 可靠传输 通过 TCP/SCTP。RADIUS 使用 UDP。
- 可扩展 通过特定应用模块
- 对等 架构。它不仅仅是客户端-服务器。
- 有状态 连接，带有看门狗监控
- 标准化 错误处理和结果代码

## **Diameter** 在 **CSCF** 中

每个 CSCF 组件使用特定的 Diameter 应用接口:



| CSCF | 接口 | 应用 ID | 连接到 | 目的 |
| --- | --- | --- | --- | --- |
| **I-CSCF** | Cx | 16777216 | HSS | S-CSCF 选择，用户位置 |
| **S-CSCF** | Cx | 16777216 | HSS | 用户认证，配置文件下载 |
| **S-CSCF** | Sh | 16777217 | HSS | 用户数据访问（可选） |
| **P-CSCF** | Rx | 16777236 | PCRF | QoS 策略和承载控制 |
| **S-CSCF** | Ro | 4 | OCS | 在线计费（信用控制） |
| **S-CSCF** | Rf | 3 | CDF | 离线计费（记账） |

# Diameter 在 IMS 架构中

网络概述

# Diameter 接口

## Cx 接口 (CSCF ↔ HSS)

I-CSCF 和 S-CSCF 使用 Cx 接口进行用户认证和配置文件管理。

**3GPP** 规范: TS 29.228

## **I-CSCF** 操作

用户授权请求 **(UAR) /** 用户授权应答 **(UAA)**:

- 目的: 查询 HSS 以获取 S-CSCF 分配或能力
- 触发: I-CSCF 接收到来自用户的 REGISTER
- 用例: I-CSCF 必须将注册路由到正确的 S-CSCF

位置信息请求 **(LIR) /** 位置信息应答 **(LIA)**:

- 目的: 查询 HSS 以获取用户当前的 S-CSCF
- 触发: I-CSCF 接收到终止用户的 INVITE 或 MESSAGE
- 用例: I-CSCF 必须将会话路由到用户的 S-CSCF

## **S-CSCF** 操作

多媒体认证请求 **(MAR) /** 多媒体认证应答 **(MAA)**:

- 目的: 从 HSS 获取认证向量
- 触发: 初始 REGISTER, 挑战之前
- 用例: S-CSCF 必须对用户进行 IMS AKA 认证挑战

服务器分配请求 **(SAR) /** 服务器分配应答 **(SAA)**:

- 目的: 通知 HSS 注册状态并下载用户配置文件
- 触发: 成功认证后, MAR/MAA 之后
- 用例: S-CSCF 下载用户的 IFC 和服务配置文件

SAA 中的 `User-Data` AVP 包含完整的用户配置文件。该配置文件包括:

- 公共身份
- 服务触发的初始过滤标准 (IFC)
- 订阅的媒体配置文件标识符
- 计费信息

注册终止请求 **(RTR) /** 注册终止应答 **(RTA)**:

- 目的：HSS 发起的注销。HSS 推送请求。
- 触发：行政注销或订阅变更
- 用例：HSS 指示 S-CSCF 注销用户

# Rx 接口 (P-CSCF ↔ PCRF)

Rx 接口��� IMS 会话提供策略和 QoS 控制。

**3GPP** 规范：TS 29.214

关于 **VoNR (5G NR)**：对于 VoNR 会话，PCF 通过 N5 AF 接口（Npcf_PolicyAuthorization，HTTP/2 SBI）授权媒体和 QoS。它不使用 Diameter Rx。因此这里的 Rx 接口适用于 4G/LTE 接入。

**AA** 请求 **(AAR) / AA** 应答 **(AAA)**：

- 目的：请求媒体会话的 QoS 授权
- 触发：SIP INVITE 中的 SDP 交换
- 用例：P-CSCF 请求 PCRF 授权承载资源

重新认证请求 **(RAR) /** 重新认证应答 **(RAA)**：

- 目的：PCRF 发起的策略更新。PCRF 推送请求。
- 触发：策略变更或承载修改
- 用例：PCRF 指示 P-CSCF 更新 QoS 策略

会话终止请求 **(STR) /** 会话终止应答 **(STA)**：

- 目的：释放 Rx 会话和承载资源
- 触发：呼叫终止。P-CSCF 接收到 BYE。
- 用例：P-CSCF 通知 PCRF 释放 QoS 资源

# Ro 接口 (S-CSCF ↔ OCS)

Ro 接口提供在线计费（信用控制）。

**3GPP** 规范：TS 32.299

信用控制请求 **(CCR) /** 信用控制应答 **(CCA)**：

- 目的：实时信用授权和扣款
- 触发：呼叫建立、中途呼叫或呼叫终止
- 用例：预付费计费和实时信用检查

类型：

- **CCR-**初始：在呼叫开始时请求信用
- **CCR-**更新：在呼叫过程中刷新配额
- **CCR-**终止：在呼叫结束时报告最终使用情况

# 通过 **OmniWeb** 进行对等管理

在 OmniWeb 中每个 CSCF 页面上的 **Diameter** 选项卡查看 Diameter 对等状态、支持的应用程序和队列深度。OmniWeb 是统一管理门户：<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>。

OmniWeb Diameter 选项卡显示每个 CSCF 的以下内容：

- 领域和 Diameter Origin-Host 身份
- 配置的对等体及其连接状态（I_Open、Closed 等）
- 每个对等体支持的 Diameter 应用程序，映射到 3GPP 接口名称（Cx/Dx、Sh/Dh、Rx、Ro、Gx、S6a/S6d 等）
- 工作队列长度和待处理事务
- 启用/禁用单个对等体的操作

对等状态

| 状态 | 描述 |
| --- | --- |
| **I_Open** | 连接已打开并正常运行 |
| **Closed** | 未建立连接 |
| **Wait-Conn-Ack** | 连接已发起。等待响应。 |
| **Wait-I-CEA** | CER 已发送。等待 CEA。 |

# Diameter 结果代码

以下表格列出了常见的结果代码及其含义：

| 代码 | 名称 | 含义 | □作 |
| --- | --- | --- | --- |
| **2xxx** | 成功 | | |
| 2001 | DIAMETER_SUCCESS | 操作成功 | 无 |
| **3xxx** | 协议错误 | | |
| 3002 | DIAMETER_UNABLE_TO_DELIVER | 无法路由到目标 | 检查对等连接 |
| 3003 | DIAMETER_REALM_NOT_SERVED | 该领域未被识别 | 验证领域配置 |
| 3007 | DIAMETER_APPLICATION_UNSUPPORTED | 该应用程序不受支持 | 检查应用程序 ID |
| **4xxx** | 暂时性故障 | | |
| 4001 | DIAMETER_AUTHENTICATION_REJECTED | 认证失败 | 检查凭据 |
| 4010 | DIAMETER_USER_UNKNOWN | 用户未配置 | 验证 HSS 配置 |
| **5xxx** | 永久性故障 | | |
| 5001 | DIAMETER_AVP_UNSUPPORTED | AVP 未被识别 | 检查协议版本 |
| 5002 | DIAMETER_UNKNOWN_SESSION_ID | 未找到会话 | 会话已过期或无效 |
| 5003 | DIAMETER_AUTHORIZATION_REJECTED | 未授权 | 检查用户权限 |
| 5012 | DIAMETER_UNABLE_TO_COMPLY | 无法处理请求 | 检查 HSS/PCRF/OCS |

| 代码 | 名称 | 含义 | □作 |
| --- | --- | --- | --- |
|  |  |  | 日志 |

# 常见问题

## 关键 **Diameter** 接口

当 Diameter 对等体出现故障时，影响和恢复紧迫性取决于受影响的接口：

| 接口 | 故障时影响 | 恢复优先级 |
| --- | --- | --- |
| **Cx (HSS)** | 无法进行新注册。没有 IFC 更新。 | 关键。立即恢复。 |
| **Rx (PCRF)** | 新呼叫没有 QoS | 高。几分钟内恢复。 |
| **Ro (OCS)** | 无法进行预付费计费。服务可以继续。 | 高。取决于策略。 |

---

### 对等连接故障

症状：对等体停留在 "Closed" 或 "Wait-Conn-Ack" 状态

诊断：

1. 验证网络连接：

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

2. 检查防火墙规则。端口 3868 TCP 必须开放。
3. 验证对等体配置（IP 地址，端口）
4. 检查对等体日志以获取连接尝试

解决方案：

- 修复网络和防火墙问题
- 验证对等体在端口 3868 上运行并监听
- 检查对等体是否具有正确的 CSCF 配置
- 在 OmniWeb Diameter 选项卡上使用 **Enable Peer** 重新尝试连接

---

## CER/CEA 交换故障

症状：对等体停留在 "Wait-I-CEA" 状态，或 CEA 有错误代码

常见错误：

- **5010 (NO_COMMON_APPLICATION)**：验证两个对等体是否支持相同的应用程序（例如，Cx = 16777216）
- **3003 (REALM_NOT_SERVED)**：验证 Origin-Realm 是否与对等体的预期领域匹配

解决方案：

- 检查 Diameter 配置中的应用程序 ID 和领域
- 确保对等体配置与 CSCF 预期匹配
- 查看 CSCF 后端日志以获取详细错误消息

---

## HSS Cx 接口问题

症状：注册失败和 MAR/MAA 超时

常见错误：

| 结果代码 | 含义 | 解决方案 |
| --- | --- | --- |
| 4010 | USER_UNKNOWN | 用户未在 HSS 中配置 |
| 4001 | AUTHENTICATION_REJECTED | IMPI 或凭据不正确 |
| 5012 | UNABLE_TO_COMPLY | HSS 内部错误。检查 HSS 日志。 |

解决方案：

- **USER_UNKNOWN**：在 HSS 中配置用户
- **AUTHENTICATION_REJECTED**：验证 HSS 中的 IMPI 和共享密钥
- **UNABLE_TO_COMPLY**：检查 HSS 日志和数据库连接

---

## PCRF Rx 接口问题

症状：呼叫成功但未应用 QoS。发生 AAR/AAA 超时。

常见问题：

- **PCRF** 故障：检查 OmniWeb Diameter 选项卡上的对等状态
- **Framed-IP-Address** 未被识别：PCRF 无法将 UE IP 映射到订阅者
- 策略未应用：检查 PCRF 策略规则。验证 PCEF 集成。

解决方案：

- 验证 PCRF 对等体是否处于 "I_Open" 状态
- 检查 PCRF 中的 UE IP 地址配置
- 验证 Gx 接口（PCRF 到 PCEF）是否正常

---

## OCS Ro 接口问题

症状：预付费呼叫失败。发生 CCR/CCA 超时。呼叫被阻止。

常见错误：

| 结果代码 | 含义 | 解决方案 |
| --- | --- | --- |
| 4012 | CREDIT_LIMIT_REACHED | 信用不足 |
| 5003 | AUTHORIZATION_REJECTED | 用户未获得预付费授权 |

解决方案：

- **CREDIT_LIMIT_REACHED**：对于没有信用的预付费用户是正常的
- **OCS** 超时：检查 OCS 可用性和对等状态
- **AUTHORIZATION_REJECTED**：验证用户是否在 OCS 中配置为预付费

---

### 性能下降

症状：Diameter 响应时间缓慢和高延迟

诊断：

1. 检查对等列表中的 "Last Used" 时间戳。它必须是最近的。
2. 监控 "Queue Length"。高值表示有积压。
3. 查看 CSCF 后端日志以获取超时警告

解决方案：

- 高延迟：调查 CSCF 和对等体之间的网络
- 高队列长度：检查对等系统负载（HSS/PCRF/OCS）
- 超时：如果网络延迟高，增加事务超时

## 最佳实践

### 作指南

对等管理：

- 在 OmniWeb Diameter 选项卡上监控对等状态
- 为对等故障事件设置外部监控
- 在维护窗口期间测试对等连接

容量规划：

- 根据注册和呼叫量估算 Diameter 事务速率
- 确保 HSS/PCRF/OCS 能够处理峰值事务速率
- 对于大规模部署，考虑 Diameter 路由代理（DRA）

故障排除：

- 在调查注册或呼叫故障时，首先检查对等状态
- 将 Diameter 故障与 SIP 故障关联（相同的 Call-ID 或用户）
- 查看 CSCF 后端日志以获取详细的 Diameter 事务跟踪

安全性：

- 在生产环境中使用 TLS 进行 Diameter 连接（如果支持 TLS）
- 使用防火墙限制 Diameter 对等访问。仅允许已知的对等体。
- 定期查看对等启用/禁用审计日志

# 限制和未来增强

## 当前实施

OmniWeb Diameter 选项卡提供：

- □ □□□□□□□□
- □ □□/禁用对等操作
- □ □□ ID 到接口名称的映射

## 尚未实施

以下功能 当前不可用。未来版本可以添加它们：

- **Diameter** 消息检查器：查看最近的 Diameter 事务和 AVP 详细信息
- 对等统计：每个对等体的消息计数、成功率和平均延迟
- 看门狗监控：实时 DWR/DWA 状态

## 解决方法

对于消息检查：检查 CSCF 后端日志，或启用 Diameter 调试日志

对于详细统计：从 Prometheus 端点查询指标。请参阅 指标参考 以获取完整的 CDP/Diameter 指标定义和监控设置。

对于手动重新连接：使用 OmniWeb Diameter 选项卡禁用然后重新启用对等体

## 相关文档

- **P-CSCF** 操作指南 - P-CSCF Rx 接口操作
- **I-CSCF** 操作指南 - I-CSCF Cx 接口操作
- **S-CSCF** 操作指南 - S-CSCF Cx、Ro 接口
- **5G SBI** 操作指南 - 用于 VoNR 的 N5/NRF 基于服务的接口（Rx 的 5G 对应）
- 指标参考 - CDP/Diameter 指标和监控
- **OmniWeb** - 通过 OmniWeb Diameter 选项卡进行 Diameter 对等管理
- **CSCF** 操作指南 - 一般 CSCF 操作

## **3GPP** 规范

- **TS 29.228**: Cx 和 Dx 接口 (CSCF-HSS)
- **TS 29.214**: Rx 接口 (P-CSCF-PCRF)
- **TS 32.299**: Diameter 计费应用 (Ro, Rf)
- **RFC 6733**: Diameter 基础协议

## 技术细节

### 实施

- **Diameter** 堆栈：集成的 Diameter 协议堆栈
- 管理接口：RPC 协议到 CSCF 后端
- 管理门户：OmniWeb (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>)

### 对等配置（部署）

每个 CSCF 节点都有一个 Diameter 对等配置文件：`pcscf.xml`、`icscf.xml` 或 `scscf.xml`。Ansible 在部署时渲染该文件。该文件定义了节点的 Diameter 身份以及它连接的 HSS/PCRF/DRA 对等体。结构在所有三个文件中是相同的。仅广告的应用程序不同。

| **XML** 字段 | 配置内容 | **Ansible** 源 |
| --- | --- | --- |
| `DiameterPeerFQDN` | 该节点的 Diameter origin-host FQDN | `<inventory_hostname>.epc.mnc<mnc>.m` |
| `DiameterPeerRealm` | 本地 Diameter 领域 | 如果定义则为 `ims_realm`，否则为 `epc.mnc<mnc>.mcc<mcc>.3gppnetwork.o` |
| `Vendor_Id` / `Product_Name` | CER 身份 | `10415` (3GPP) / `OmniCSCF` |
| `Peer` (直接模式) | 通过 SCTP:3868 直接对每个 `hss`-组主机 | 在 `ims_dra_support` 为 false 时按主机渲染 `grou` |
| `Peer` (DRA 模式) | 对每个 `dra`-组主机的对等体。当设置 `diameter_dra_ip` 时为显式 IP。 | 在 `ims_dra_support` 为 true 时按主机渲染 `group` |
| `Acceptor` | 本地绑定 FQDN 和端口以进行入站 Diameter (3868) | 节点 FQDN |
| `DefaultRoute` | 到 HSS/PCRF 对等体的领域路由默认路由（度量 1）或 DRA（度量 2） | 从 `groups['hss']` / `groups['dra']` 渲染 |

每个节点的广告应用程序：

| 节点（文件） | 应用程序 |
| --- | --- |
| P-CSCF (`pcscf.xml`) | **Rx** `16777236` (vendors 10415, 0) |
| I-CSCF (`icscf.xml`) | **Cx** `16777216` (vendors 10415, 13019, 0) + 基础计费 `4` |
| S-CSCF (`scscf.xml`) | **Cx** `16777216` (vendors 10415, 13019, 0) + 基础计费 `4` |

关键的 Ansible 变量如下。`plmn_id.mcc` 和 `plmn_id.mnc_longform` 构建所有 FQDN 和领域。`ims_realm` 覆盖 Diameter 领域。`ims_dra_support` 在直接对等和 DRA 对等之间切换。`diameter_dra_ip` 设置 DRA 对等体的静态 IP。`hss` 和 `dra` 库存组提供对等体和默认路由列表。当启用计费时，`RO_DESTINATION` 单独指向 S-CSCF 的 **Ro** 对等体（OCS）。XML 不处理此对等体。

通过部署工具编辑这些文件，而不是通过 OmniWeb。OmniWeb 仅提供监控和操作控制（启用/禁用）。

# I-CSCF 作与参考

Interrogating-CSCF 是 IMS 信令的家庭网络入站接入点。当用户注册时，用户到达此节点。当会话终止到家庭用户时，会话到达此节点。I-CSCF 不持有会话状态。I-CSCF 不终止媒体。I-CSCF 通过 Cx 查询 HSS。此查询决定哪个 Serving-CSCF 处理给定请求。在注册时，I-CSCF 授权身份和访问网络。然后，I-CSCF 发现 S-CSCF，或选择一个 S-CSCF 的能力。在终止请求时，I-CSCF 定位已经为用户服务的 S-CSCF。在 I-CSCF 选择 S-CSCF 后，I-CSCF 将请求转发给该 S-CSCF。I-CSCF 将响应转发回来。

# IMS 功能

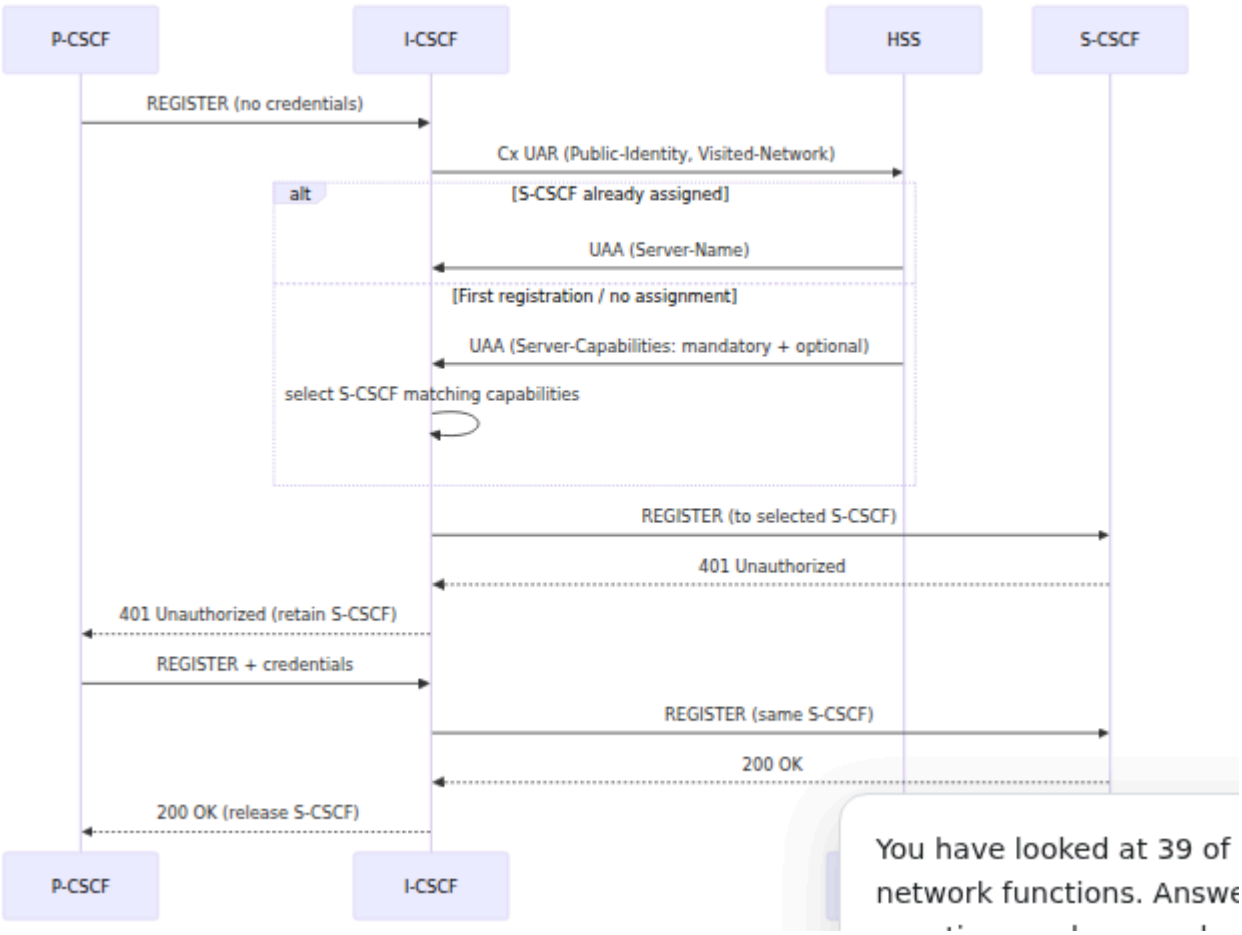
## 注册路由 (Cx UAR)

当 REGISTER 到达时，I-CSCF 使用 Cx 用户授权请求 **(UAR)** 查询 HSS。I-CSCF 在转发 REGISTER 之前发送此查询。UAR 携带公共身份和访问网络标识符。这些值使 HSS 授权用户从该网络注册。答案 (UAA) 返回以下两种情况之一：

- 已分配的 **S-CSCF** 名称。 I-CSCF 直接使用此名称。重新注册返回到��有绑定的同一 S-CSCF。
- **S-CSCF** 能力。这些是一组选定 S-CSCF 必须满足的强制和可选能力值。HSS 在首次注册时返回这些值，或者当没有 S-CSCF 当前分配时。然后，I-CSCF 进行基于能力的选择（如下所述）。

I-CSCF 将 REGISTER 转发给选定的 S-CSCF。I-CSCF 在注册握手期间记住该 S-CSCF。经过身份验证的重新 REGISTER 跟随 401 挑战。I-CSCF 将此重新 REGISTER 路由到 同一 S-CSCF，而不再查询。I-CSCF 在 401 处于飞行状态时保留 S-CSCF。当注册完成 (2xx) 或最终失败时，I-CSCF 丢弃 S-CSCF。

一个不可用或返回格式错误答案的 HSS 产生 **503**。UAR 可以授权但不返回 S-CSCF 进行选择。在这种情况下，I-CSCF 回退到配置的默认 S-CSCF URI。



## 终止路由 **(Cx LIR)**

初始终止请求是 INVITE、SUBSCRIBE、MESSAGE、INFO 或 PUBLISH。在此请求上，I-CSCF 使用 Cx 位置信息请求 **(LIR)** 查询 HSS 以获取请求 URI 身份。答案 (LIA) 返回当前为用户服务的 S-CSCF 的名称。对于未注册但已配置服务的用户，LIA 返回能力。然后，I-CSCF 从这些能力中选择一个 S-CSCF。I-CSCF 将请求转发给该 S-CSCF。如果返回的 URI 未指定传输，I-CSCF 强制使用 TCP 传输到 S-CSCF。在转发请求之前，I-CSCF 删除任何入站的 STIR/SHAKEN `Identity` 头。

结果处理：

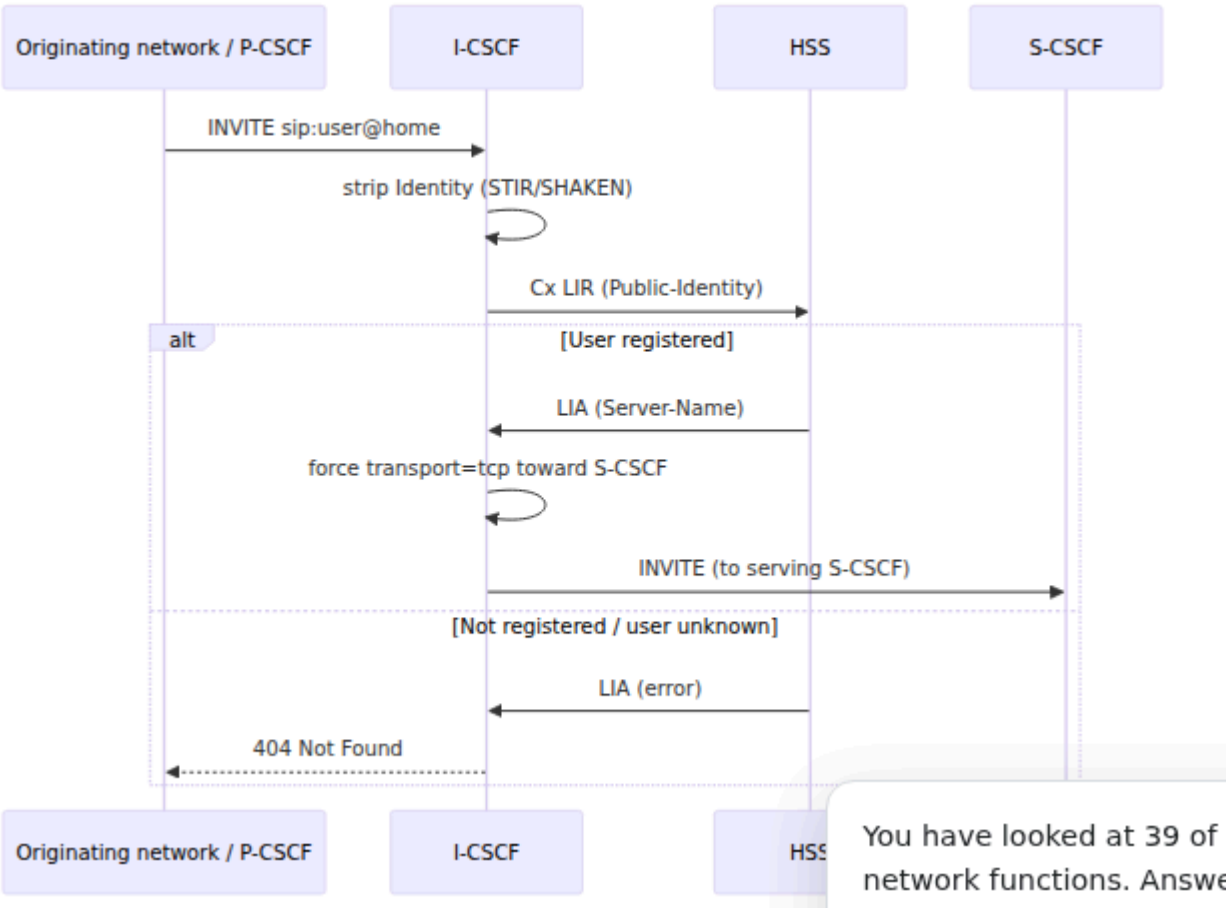
- 成功。 I-CSCF 选择 S-CSCF 并将请求转发给它。转发失败返回 **500**。
- 用户未找到 / 未注册。 I-CSCF 返回 **404 Not Found**。
- **HSS** 不可用。 I-CSCF 返回 **503**。

I-CSCF 不查询 CANCEL。I-CSCF 将 CANCEL 匹配到其现有事务并转发。I-CSCF 拒绝任何其他非初始、非 REGISTER 方法，并返回 **406** 和 `Allow` 列表。

## S-CSCF 选择 / 能力匹配

HSS 可以返回能力而不是分配的 S-CSCF 名称。在这种情况下，I-CSCF 从其 配置的 **S-CSCF** 集 中选择一个 S-CSCF。每个候选 S-CSCF 具有一个 SIP URI 和一组能力值。选择要求 S-CSCF 满足 所有强制 能力。在符合条件的候选者中，I-CSCF 优先选择匹配更多 可选 能力的候选者。多个候选者可以同样适合。这些候选者形成一个有序的候选列表。此列表使 I-CSCF 在失败时尝试备用。

I-CSCF 在请求的生命周期内将候选列表保存在事务内存中。这在尝试之间保留列表位置。转发的 REGISTER 可能会超时或返回 5xx/6xx。在这种情况下，I-CSCF 继续下一个候选 S-CSCF 并重试。当列表耗尽时，I-CSCF 停止。I-CSCF 在 401 挑战期间保留列表，因为同一 S-CSCF 必须处理经过身份验证的重试。I-CSCF 在成功或客户端错误的最终响应时丢弃列表。如果选择什么都没有，I-CSCF 回退到配置的默认 S-CSCF URI。



# 部署配置 (Ansible 注入)

Ansible 在部署时渲染 I-CSCF 的运行时配置 (`icscf.cfg`) 和其 Diameter 对等体表 (`icscf.xml`)。值来源于网络的 PLMN 身份 (MCC/MNC) 和节点的库存主机名。功能开关是 `#!define` 标志。定义的标志启用该功能。注释掉的标志禁用该功能。

### 身份 / 领域

| 名称 | 控制内容 | 值 / |
| --- | --- | --- |
| `NETWORKNAME` | 家庭 IMS 域。这是 Cx 目标领域 (`cxdx_dest_realm`)。I-CSCF 在路由对等或未知用户请求时检查此域。 | `ims.mnc<mnc>.mcc<mcc>.3gppnet` |
| `HOSTNAME` | 此节点的 FQDN (主机别名) | `<inventory_hostname>.ims.mnc<` |
| `ICSCF_USER_AGENT` | 节点发出的 `User-Agent` 头 | `User-Agent: Omnitouch I-CSCF` |
| `ICSCF_SERVER` | 节点发出的 `Server` 头 | `Server: Omnitouch I-CSCF <inv` |
| `SCSCF_URI` | 默认或备用 S-CSCF URI。当基于 UAR 的选择未返回 S-CSCF 时，I-CSCF 使用此 URI。 | `sip:scscf.ims.mnc<mnc>.mcc<mc` |

Ansible 从库存主机地址和 PLMN 模板 SIP 监听套接字 (UDP/TCP 5060, TLS 9090)。Ansible 还从这些值模板化主机别名 (`ims.…`, `icscf.ims.…`, `<host>.ims.…`)。

`CAPTURE_NODE` 是 Homer 捕获目标，`sip:<homer_host>:9060`。Ansible 仅在为部署启用 Homer 捕获时模板化此值。Homer 捕获需要 `enable_homer` 和 `homer` 库存组。`CAPTURE_NODE` 通过 HEP 将 SIP 信令复制到 Homer 进行追踪。

## **Diameter** 对等体配置

I-CSCF 的 Diameter 对等体表 (`icscf.xml`) 向 HSS 广告 **Cx** 应用程序 (`16777216`)。所有 CSCF 共享文件结构和填充它的 Ansible 变量。请参见 Diameter → 对等体配置 (部署)。

## 故障排除

注册失败或终止会话失败在 I-CSCF 显现。这些失败通常来自两个原因之一:

- **S-CSCF** 选择 / 分配。 HSS 可以返回能力而不是分配的 S-CSCF 名称。选择要求 S-CSCF 满足所有强制能力。如果没有候选者符合条件，I-CSCF 回退到配置的默认 S-CSCF URI。如果转发的 REGISTER 超时或返回 5xx/6xx，I-CSCF 将切换到下一个候选者，直到列表耗尽。确认配置的 S-CSCF 集及其能力值与 HSS 返回的内容匹配。
- 与 **HSS** 的 **Cx** 连接 **(UAR / LIR)**。I-CSCF 无法在没有 Cx UAR（在 REGISTER 上）或 LIR（在终止请求上）答案的情况下路由。不可用或格式错误的 HSS 答案产生 **503**。未知或未注册的用户产生 **404**。验证与 HSS 的 Cx 对等体是否正常。请参见 Diameter 操作。

## 呼叫流程

序列图与它们记录的功能一起出现：

- 通过 I-CSCF 注册 → 注册路由 (Cx UAR)
- 通过 I-CSCF 终止会话 → 终止路由 (Cx LIR)
- S-CSCF 故障转移 → S-CSCF 选择 / 能力匹配

## 相关文档

- S-CSCF 操作与参考
- 操作
- Diameter
- 指标参考
- OmniWeb - S-CSCF 列表、活动会话和 Cx Diameter 对等体状态：<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

# P-CSCF □作与参考

Proxy-CSCF 是 IMS 的 SIP 入口点，供用户设备使用。每个 REGISTER 和每个来自 UE 的会话首先到达这里。P-CSCF 建立并强制执行保护 UE 信令的访问安全关联。P-CSCF 插入到路由路径中。它在注册时添加 Path 头，在会话中添加记录路由。所有后续流量都通过此节点传输。该流量包括终止请求和对话中的消息。P-CSCF 检测 UE 访问技术以驱动媒体承载策略。P-CSCF 还根据 TS 23.167 向紧急会话入口点（E-CSCF）提供可用的呼叫线路身份。P-CSCF 仅是信令代理。媒体直接在 UE 和终止方之间流动。媒体从不通过此节点。

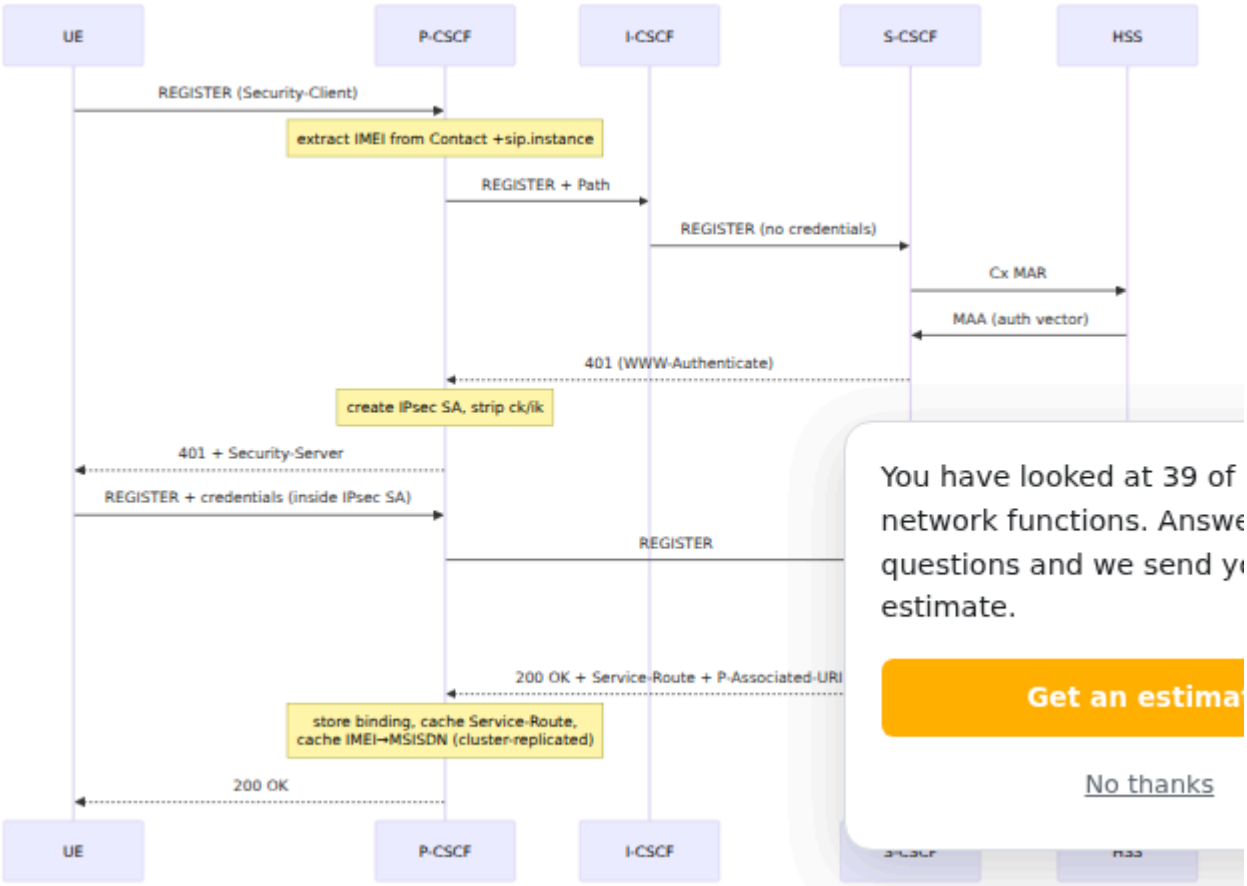
## IMS 功能

### 注册代理与 IPsec 安全关联

P-CSCF 是面向 UE 的注册代理。P-CSCF 将 REGISTER 转发到家庭网络（I-CSCF/S-CSCF）。在挑战/响应交换中，P-CSCF 与 UE 建立 IPsec ESP 安全关联。这是 IMS-AKA 过程的一部分。在注册期间，UE 和 P-CSCF 通过 `Security-Client` / `Security-Server` 头协商 SA 参数。从经过身份验证���重新 REGISTER 开始，SA 承载该 UE 的所有信令。

在转发的 REGISTER 中，P-CSCF 插入一个 **Path** 头。这将终止请求路由回同一节点。P-CSCF 强制注册过期为网络控制的值。P-CSCF 宣传 `path` 支持。在成功的 `200 OK` 中，P-CSCF 存储联系绑定。P-CSCF 缓存返回的 `Service-Route` 和 `P-Associated-URI`。这引导后续请求通过正确的家庭网络路径。

每个注册的 UE 使用来自每个部署资源池的一个安全关联。当 UE 注销（过期 0）或其注册失效时，P-CSCF 释放 SA。P-CSCF 拒绝标记为紧急（`;sos`）注册的 REGISTER。P-CSCF 直接在 INVITE 上处理紧急会话，而不是通过紧急注册。

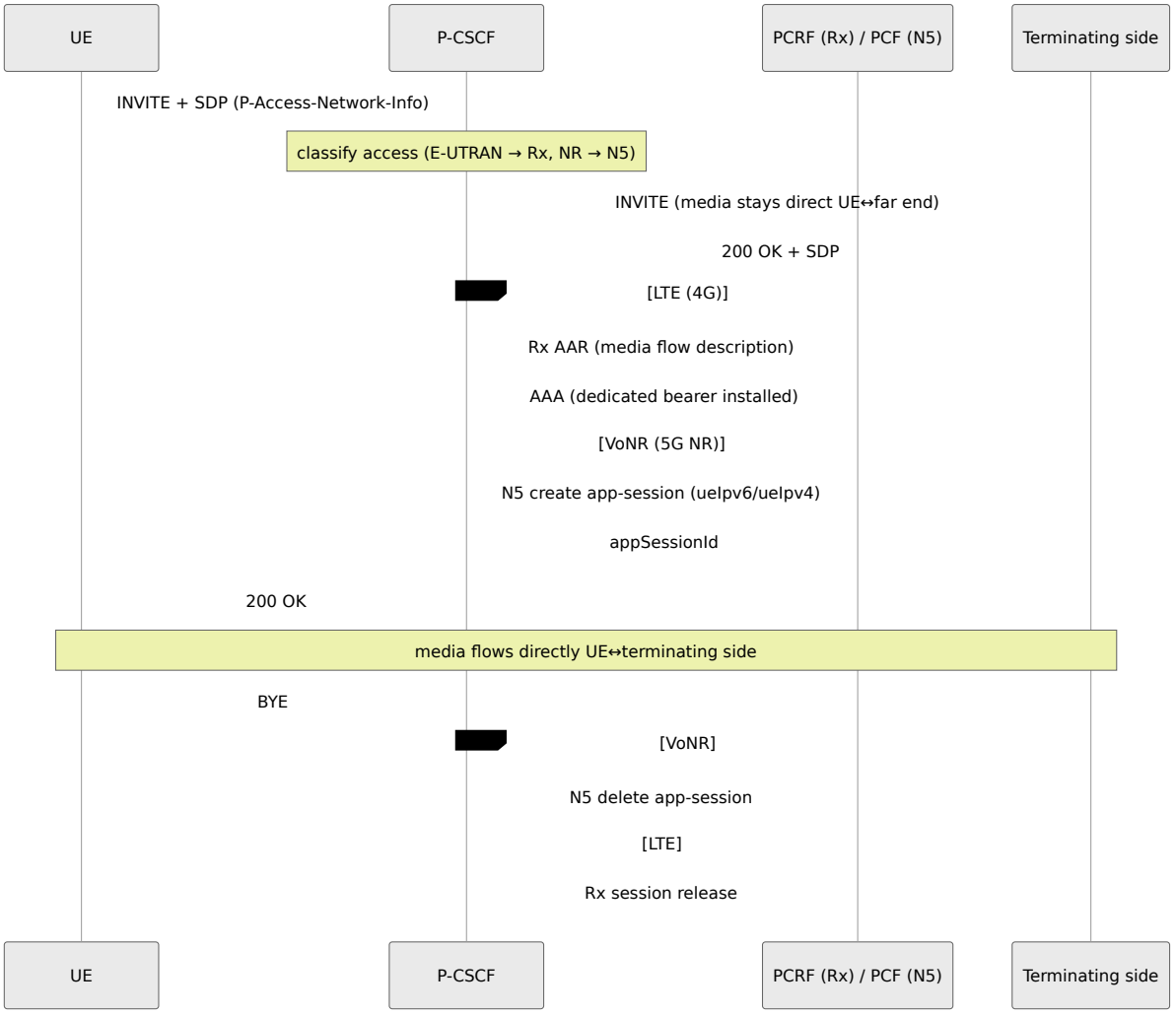


## 访问检测与 QoS / 策略控制

P-CSCF 从不转发媒体。P-CSCF 仍然通过策略平面授权专用媒体承载。P-CSCF 根据 `P-Access-Network-Info` 头（根据 TS 24.229 §5.2.6.3）对 UE 访问进行分类。LTE 报告 `3GPP-E-UTRAN`。5G NR 报告 `3GPP-NR`。WiFi 访问没有专用承载。P-CSCF 将 WiFi 访问排除在动态 QoS 之外。

- **4G / LTE** - P-CSCF 通过 **Diameter Rx** 授权媒体承载 QoS 到 PCRF。在应答腿（携带 SDP 的 `200 OK`）上，P-CSCF 发出授权/认证请求（AAR）。AAR 描述音频媒体流和视频媒体流（如有）。PCRF 然后安装相应的专用承载。P-CSCF 在对话重新 INVITE 时刷新授权。对话结束时，P-CSCF 释放授权。
- **VoNR (5G NR)** - P-CSCF 通过 **N5** 接口向 PCF 授权承载 QoS。P-CSCF 使用 `Npcf_PolicyAuthorization` 服务。P-CSCF 作为应用功能。当远端应答媒体时，P-CSCF 在 PCF 上创建应用会话。该会话使用 afAppId `VoNR`，一个带有 `ENABLED` 流状态的 `AUDIO` 媒体组件，以及用于 UE 媒体的流描述符。它还包括一个 AF 通知 URI，以便 PCF 回调。对话结束时，P-CSCF 删除该应用会话。

QoS 授权在发起（MO）和终止（MT）两条腿上运行。它以 UE 自身的 IP 地址为键。**UE** 地址绑定：P-CSCF 编码 UE 地址以匹配政策节点持有的 PDU 会话/承载绑定。P-CSCF 将 IPv6 UE 信号化为 `ueIpv6`，将 IPv4 UE 信号化为 `ueIpv4`。放置在 v4 字段中的 v6 地址永远不会与 PCF 绑定匹配。PCF 然后不会安装专用承载。



对于 VoNR，P-CSCF 通过 **NRF** 发现 定位服务 PCF。P-CSCF 注册为 AF。对于每个会话，P-CSCF 通过 NRF→BSF 链解析与 UE PDU 会话绑定的 PCF。这是唯一的 PCF 发现路径。

## 紧急呼叫 **(E-CSCF)** 与呼叫线路身份 **- TS 23.167**

P-CSCF 是紧急入口点。P-CSCF 通过 INVITE 中的紧急服务 URN (`urn:service:sos`) 检测紧急会话。P-CSCF 将其直接路由到紧急应用服务器。这绕过了正常的注册检查。紧急 INVITE 通常不携带 **MSISDN**。因此，P-CSCF 为 PSAP 提供可用的呼叫线路身份。这适用于未知或匿名的呼叫者。这符合 TS 23.167 附录 K 和 TS 29.214 §4.4.6a。

有两个机制按此顺序解析身份：

1. 异步订阅查询 **PCRF**（主要）。 P-CSCF 向 PCRF 发出异步 Rx 订阅查询。该查询以 UE 源 IP 地址为键。P-CSCF 暂停 INVITE，直到答案返回。PCRF 返回 UE 的实时 IP-CAN 会话的 EPC 级身份。P-CSCF 按优先级选择一个 **MSISDN → IMSI → IMEISV**。该身份属于当前使用的 SIM，因此优先级最高。
2. 缓存的 **IMEI→MSISDN** 绑定（后备）。在每个成功的 REGISTER 中，P-CSCF 缓存一个绑定。该绑定将 UE IMEI（来自 Contact `+sip.instance`）映射到 MSISDN（来自 `P-Associated-URI`）。P-

CSCF 在所有 **P-CSCF** 节点之间复制该绑定。任何节点都可以解析身份，而不管 UE 注册在哪里。P-CSCF 仅在 PCRF 返回无身份或 Rx 查询无法发送时使用此绑定。该绑定是每个手机的，因此可以命名在同一手机中使用的早期 SIM。

P-CSCF 将解析的身份作为呼叫者 From URI 和 `sP-Asserted-Identity` 在 `sos.apn` 域上进行断言。P-CSCF 在回复和对话请求中始终一致地恢复身份。因此，即使对于最初匿名的呼叫者，PSAP 也会看到可用的回调身份。无论哪条路径解析身份，紧急 INVITE 都会像任何其他发起请求一样接收相同的媒体/QoS 和头部处理。然后，P-CSCF 将其转发到紧急应用服务器。

## 安全 / 防洪

P-CSCF 应用基于源的洪水保护。P-CSCF 对每个源 IP 限制请求速率。P-CSCF 禁止超过采样阈值的 IP，持续一段时间。P-CSCF 跟踪每个源 IP 的注册认证失败情况，使用短期计数器。P-CSCF 禁止在窗口内超过失败尝试阈值的源。这可以防止凭证猜测。P-CSCF 丢弃 UE 直接发送到节点本身的请求。P-CSCF 还丢弃格式错误的消息。在内存压力下，该节点以 `503` 丢弃新请求。

### 集群复制

P-CSCF 在 P-CSCF 节点之间复制与注册相关和紧急状态。特别是 P-CSCF 在节点之间同步 IMEI→MSISDN 紧急绑定。P-CSCF 在启动时进行完全同步。集群中的任何节点都可以服务终止流量并解析紧急呼叫身份。这在最初注册 UE 的节点无关。P-CSCF 不需要每个节点的配置。

## 部署配置（**Ansible** 注入）

Ansible 在部署时呈现 P-CSCF 运行时配置及其 Diameter 对等表（`pcscf.xml`）。大多数值源自网络 PLMN 身份（MCC/MNC）和节点库存主机名。Ansible 仅在部署库存包含相关网络功能时发出 5G SBI 和 PCF 块。

身份

| 名称 | 控制内容 | 值 / 派生 |
| --- | --- | --- |
| `NETWORKNAME` | 用于 `P-Visited-Network-ID` 和身份重写的家庭 IMS 域 | `ims.mnc<mnc>.mcc<mcc>.3gppnetwork.` |
| `HOSTNAME` | 此节点的 FQDN（也是其主机别名） | `<inventory_hostname>.ims.mnc<mnc>.` |
| `URI` | P-CSCF 自身的 SIP URI | `sip:<hostname>:5060` |
| `PCSCF_URL` | 用于 NAT 保持活动的 OPTIONS ping 的源 URI | `sip:<hostname>:5060` |
| `PCSCF_USER_AGENT` | 节点发出的 `User-Agent` 头 | `User-Agent: Omnitouch Proxy-CSCF <` |
| `PCSCF_SERVER` | 节点发出的 `Server` 头 | `Server: Omnitouch Proxy-CSCF <inve` |
| `DMQ_NOTIFICATION_ADDR` | P-CSCF 节点之间状态复制的集群通知地址 | `sip:pcscf.ims.mnc<mnc>.mcc<mcc>.3g` |

Ansible 从库存主机地址模板 SIP 监听套接字（UDP/TCP 5060，以及在定义 IPv6 地址时的 IPv6 5060）和 Prometheus HTTP 套接字（TCP 9090）。P-CSCF 在可用时在 IPv6 上前置 UEs。其后面的对等方保持 IPv4。Ansible 还根据主机名和 PLMN 构建 `PATH_HEADER` 和 `P_VISITED_NETWORK_ID_HEADER`。

## Rx / 策略控制（4G）

| 名称 | 控制内容 | 值 / 派生 |
| --- | --- | --- |
| `RX_DEST_REALM` | 向 PCRF 的 Diameter 目标域 | `{{ diameter_realm }}` |
| `PCRF_REALM` | PCRF 域 | `epc.mnc<mnc>.mcc<mcc>.3gppne` |
| `RX_AF_SIGNALING_IP` | 在 Rx AAR 中传递的 AF 信令 IP（此 P-CSCF） | 节点 `ansible_host`（仅在双 NAT 时覆盖[ |
| `RX_IMS_REG_DIALOG_DIRECTION` | Rx 注册的对话方向模式 | `3` |

固定的 Rx 媒体参数包括视频授权开启，64 kbit/s 的默认/最小音频带宽，RTCP 流包含，以及 24 小时的最大授权会话持续时间。

## 5G SBI / PCF（VoNR）

当部署库存包含 PCF 和 NRF 时发出。没有 NRF，P-CSCF 根本不加载 NRF 模块，VoNR 会话在没有动态 QoS 的情况下进行。

| 名称 | 控制内容 | 值 / 派生 |
| --- | --- | --- |
| `VONR_AF_NOTIF_URI` | PCF 回调的 AF 通知端点 | `http://<this host>:<pcscf_af_notif_port\|9999>/af` |
| `NRF_URI` | AF 注册和发现的 NRF 基础 URI | `http://<nrf host>:<nrf_sbi_port\|7777>` |
| `IMS_NRF_NF_IPV4` | 此 P-CSCF 的 NF IPv4 用于其 AF 注册 | 节点 `ansible_host` |
| `IMS_NRF_PLMN_MCC` / `IMS_NRF_PLMN_MNC` | 在 NRF 注册/发现中宣传的 PLMN | 来自 `plmn_id` |

**PCF** 发现：P-CSCF 作为 AF 向 NRF 注册。对于每个 VoNR 会话，P-CSCF 通过 NRF→BSF 链解析绑定到该 UE PDU 会话的 PCF。应用会话始终到达正确的每个用户 PCF。这包括多 PCF 5G 核心。这是唯一支持的发现路径。

### 尺寸 / 传输

| 名称 | 控制内容 | 值 |
| --- | --- | --- |
| `CAPTURE_NODE` | Homer SIP 捕获目标（仅在启用 Homer 捕获时模板化） | `sip:<homer host>:9060` |

基础配置调整 SIP（UDP）工作进程的数量和注册表哈希表的大小，以适应部署规模。iOS UE 的 TCP 连接生命周期缩短，以匹配其传输行为。

## Diameter 对等配置

P-CSCF Diameter 对等表（`pcscf.xml`）向 PCRF 广告 **Rx** 应用程序（`16777236`）。所有 CSCF 共享文件结构和填充它的 Ansible 变量。请参见 Diameter → 对等配置（部署）。Rx 仅在定义了 `WITH_RX` 时处于活动状态。

# 故障排除

## 注册 / IPsec 连接

无法注册的用户或注册超时通常指向 P-CSCF 访问安全或发现层，而不是家庭网络：

- **IPsec SA** 建立 - 移动设备必须完成 IMS-AKA `Security-Client` / `Security-Server` 协商。如果经过身份验证的重新 REGISTER 从未在 SA 内到达，请检查两件事。确认 UE 和 P-CSCF 就 SA 参数达成一致。确认没有中间设备剥离安全头。
- **NAT** 穿越 - 对于位于 NAT 后的设备，验证远端的 NAT 处理。验证保持活动的 OPTIONS ping 是否到达 UE。终止流量的针孔保持打开。
- **P-CSCF** 发现 - 验证 UE 是否发现正确的 P-CSCF 地址（通过 DNS、DHCP 或静态配置）。验证 SIP 监听套接字在接入网络上是否可达。

### 紧急呼叫问题

症状：紧急呼叫未路由到 PSAP，或 PSAP 收到无可用的呼叫线路身份（CLI）/回调号码。

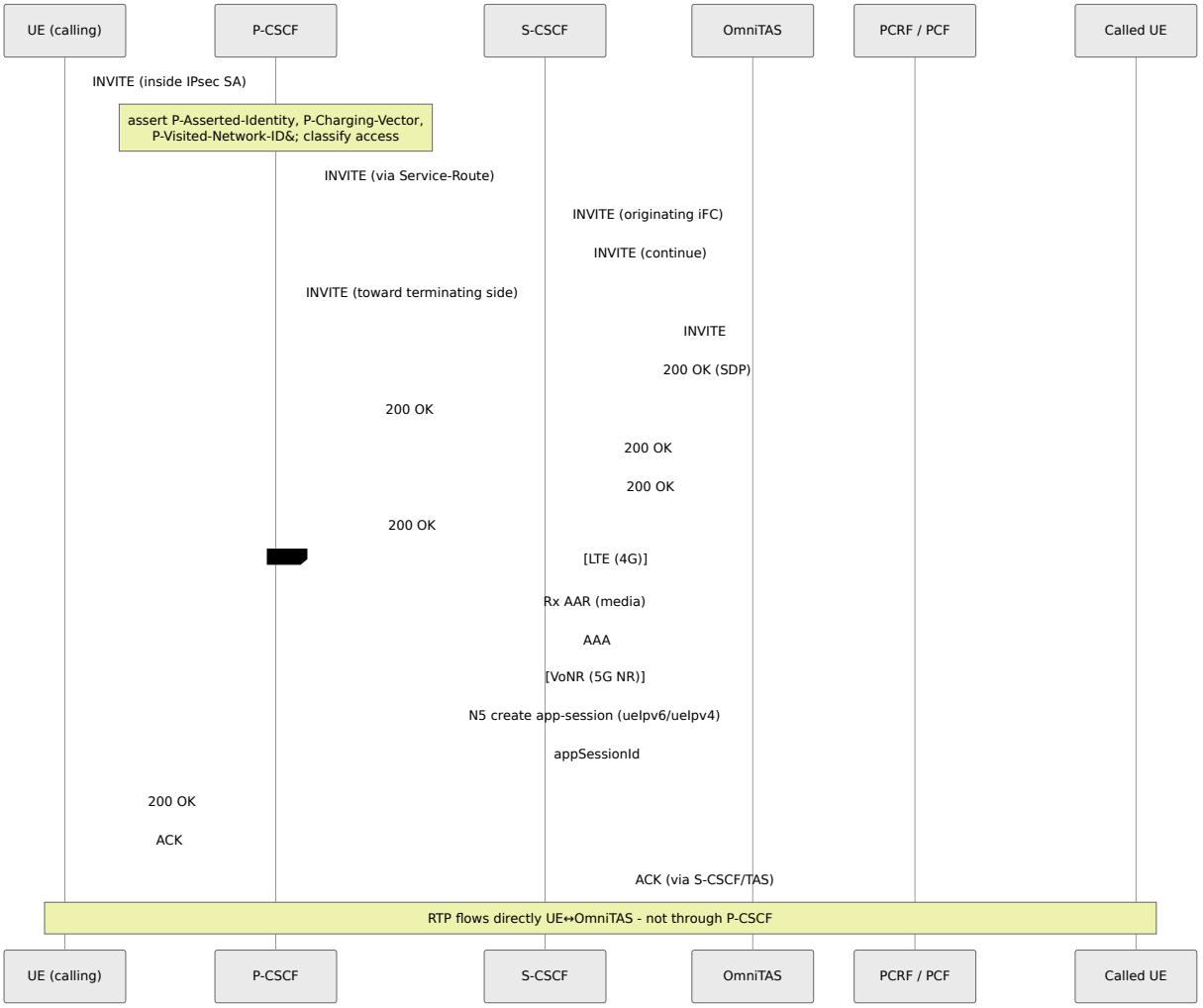
- 紧急检测 - P-CSCF 根据紧急服务 URN (`urn:service:sos`) 和拨打的紧急号码进行路由。确认 INVITE 是否携带预期的紧急指示。确认紧急路由绕过正常的注册检查。
- 匿名/未知呼叫者的 **CLI** 解析 - P-CSCF 首先向 PCRF 发送异步 Rx 订阅查询。该查询以 UE 源 IP 为键。P-CSCF 按优先级解析 EPC 身份 **MSISDN → IMSI → IMEISV**（TS 23.167 附录 K）。如果 PCRF 返回无身份，P-CSCF 将回退到缓存的 IMEI→MSISDN 绑定（集群复制，4 小时 TTL）。如果 PSAP 看到匿名呼叫者，请验证 Rx 订阅查询是否返回身份。否则，请验证 P-CSCF 是否在注册时缓存了绑定。OmniWeb 显示缓存的绑定映射。
- 位置可用性 - 验证 E911/E112 的位置信息是否可用。验证位置检索腿（LRF）是否可达。
- 测试路由 - 您可以在没有实际 PSAP 连接的情况下测试紧急呼叫路由。这确认检测、在 `sos.apn` 域上的身份断言以及路由到紧急应用服务器。

紧急会即使对于未注册用户、没有 SIM 或无效凭证的用户以及漫游用户也会成功。有关底层机制，请参见 紧急呼叫（E-CSCF）与呼叫线路身份 - TS 23.167。

# 呼叫流程

序列图与它们记录的功能一起出现。完整的会话阶梯如下：

- 注册与 IPsec SA → 注册代理与 IPsec 安全关联



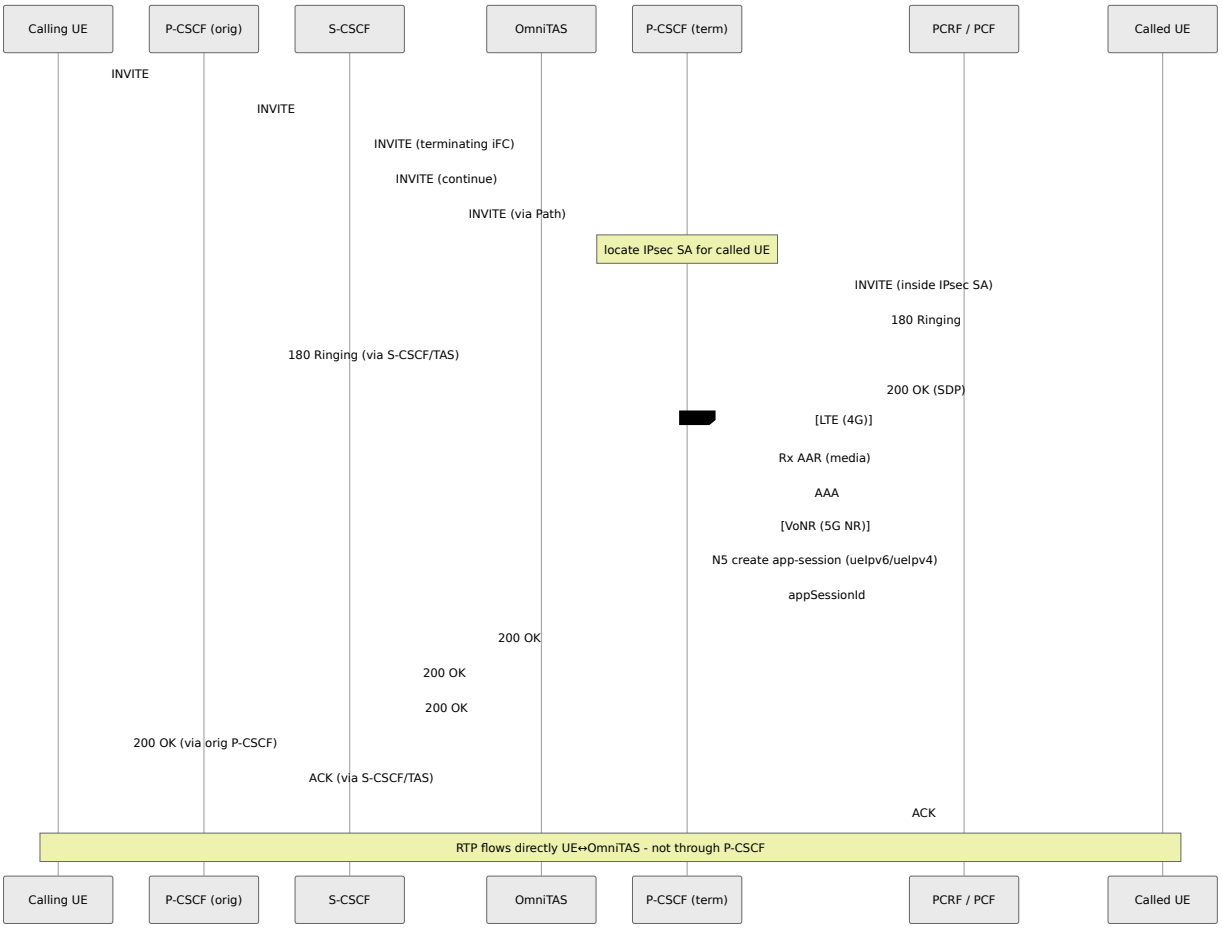
- 媒体 QoS / 策略（MO & MT） → 访问检测与 QoS / 策略控制
- 紧急会话 → 紧急呼叫（E-CSCF）与呼叫线路身份 - TS 23.167

## 移动发起呼叫（MO）

P-CSCF 通过 S-CSCF（通过缓存的 Service-Route）将发起呼叫路由到 TAS 以进行服务逻辑和计费。媒体保持直接。

## 移动终止呼叫（MT）

终止呼叫通过注册时记录在 Path 中的 P-CSCF 返回。P-CSCF 在被叫 UE 应答时授权 QoS。



# 相关文档

- 操作
- Diameter
- 基于服务的接口 (SBI)
- 指标参考
- OmniWeb - 注册联系人、哈希表（包括紧急 IMEI→MSISDN 映射）、NRF/PCF 发现和 Rx 对等状态: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

# 5G SBI □作指南

## 目录


1. □述
2. IMS 架构中的 SBI
3. N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)
4. Nnrf - NF 管理与发现 (P-CSCF ↔ NRF)
5. 何时使用 SBI 与 Diameter
6. 配置
7. 通过 OmniWeb 进行管理
8. 常见问题
9. 相关文档


## 概述

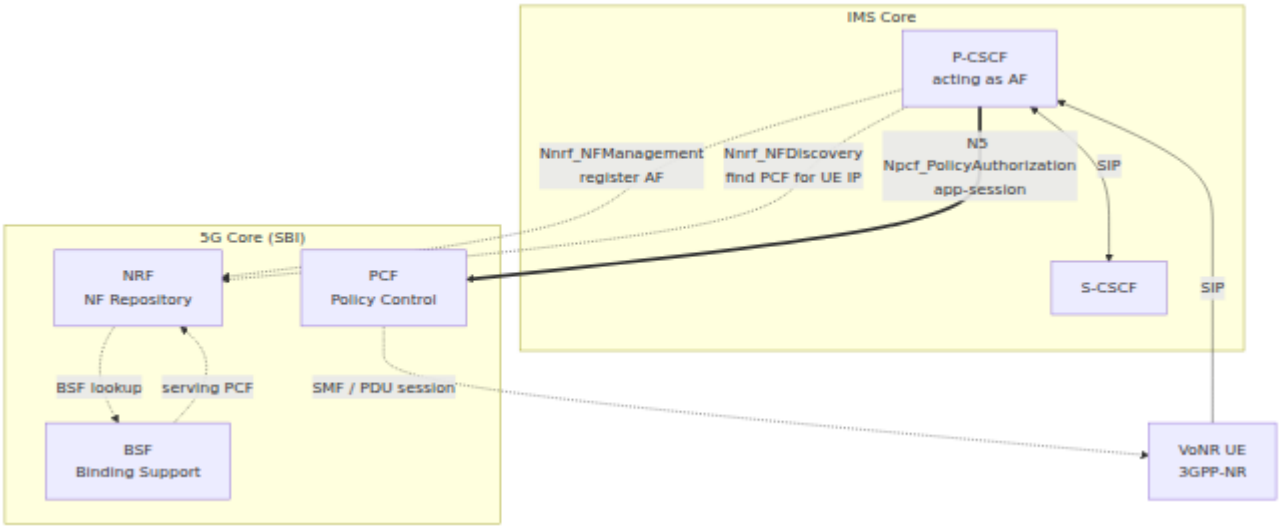
5G 核心是基于服务的。网络功能通过服务基接口 (SBI) 以 HTTP/2 和 JSON REST API 互相暴露。SBI 替代了 Diameter。对于 VoNR（新无线电语音），P-CSCF 作为 5G 应用功能 **(AF)**。P-CSCF 使用 SBI 授权媒体 QoS。P-CSCF 还使用 SBI 发现所需的网络功能。

SBI 替代了用于 VoLTE 的 Diameter Rx 路径。有关 4G/LTE 方面的信息，请参见 Diameter 操作。

## 什么是 **SBI**?

服务基接口 (3GPP TS 29.500) 与 Diameter 的不同之处在于：

- 传输：通过 TCP 的 HTTP/2。Diameter 使用 TCP 或 SCTP。
- 编码：由 OpenAPI 描述的 JSON 有效载荷。Diameter 使用 AVP。
- 模型：RESTful 资源。您可以创建、修改或删除 *app-session* 资源。Diameter 使用请求和应答命令对。
- 发现：**NRF** 动态查找生产者。Diameter 使用静态配置的对等体。
- 命名：服务使用名称 `Nxxx`（例如 `Npcf_PolicyAuthorization`，`Nnrf_NFDiscovery`）



## SBI 在 CSCF 中

P-CSCF 是唯一使用 SBI 的 CSCF 组件。作为 5G 应用功能 (AF)，P-CSCF 通过 N5 授权 VoNR 媒体 QoS 到 PCF。当启用 NRF 发现时，P-CSCF 向 NRF 注册并查询 NRF。

| 角色 | 服务 | 传输 | 连接到 | 目的 |
|---|---|---|---|---|
| **AF** | Npcf_PolicyAuthorization (N5) | HTTP/2 | PCF | 授权 VoNR 媒体和 QoS。创建一个 app-session。 |
| **NF (AF)** | Nnrf_NFManagement | HTTP/2 | NRF | 将 P-CSCF 注册为 AF 实例（可选） |
| **NF (AF)** | Nnrf_NFDiscovery | HTTP/2 | NRF → BSF | 发现绑定到 UE PDU 会话的 PCF（可选） |

# SBI 在 IMS 架构中

对于 VoNR，P-CSCF 检测 5G 接入。P-CSCF 通过 NRF→BSF 链发现服务 PCF。然后，P-CSCF 向该 PCF POST 一个政策授权 app-session。此 app-session 保留语音承载 QoS。

# N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)

**N5** 参考点承载 `Npcf_PolicyAuthorization` 服务。在 VoNR 通话中，P-CSCF 在 PCF 上创建一个 *app-session* 资源。该 app-session 描述了会话所需的媒体。然后，PCF 在 UE 5G PDU 会话上安装正确的 QoS。

## App-session 请求

P-CSCF 向 PCF app-sessions 集合 POST 一个 `ascReqData` 对象。默认集合为 `http://<pcf>/npcf-policyauthorization/v1/app-sessions`。该对象包含以下字段：

| 字段 | 值 | 备注 |
| --- | --- | --- |
| `notifUri` | AF 通知 URI | PCF 发送 app-session 事件通知的地址。这是配置的 AF 通知端点。 |
| `suppFeat` | `3f` | 支持的特性位图 |
| `ueIpv4` / `ueIpv6` | UE ﷺ IP | 必须与 PCF 绑定到 SMF PDU 会话的地址族匹配 |
| `afAppId` | `VoNR` | 应用标识符 |
| `medComponents` | 音频媒体组件 | `mediaType: AUDIO`，`fStatus: ENABLED`，具有流描述（`permit out 17 from <ue-ip> to any`） |

> 注意事项 - 地址族。 PCF 通过 UE IP 地址将 app-session 绑定到 SMF PDU 会话。您必须将 IPv6 PDU 会话中的 UE 编码为 `ueIpv6`。`ueIpv4` 中的 v6 地址永远不匹配。`ueIpv6` 中的 v4 地址永远不匹配。在这些情况下，PCF 会拒绝授权或静默丢弃授权。P-CSCF 会自动从 SIP 源地址选择 `ueIpv6` 或 `ueIpv4`。

### 生命周期

- 创建 - 当 P-CSCF 处理 VoNR INVITE 或早期媒体时，POST app-session。
- 通知 - PCF 回调 `notifUri` 以获取会话事件。
- 删除 - 当对话结束时，P-CSCF 拆除 app-session。这会释放保留的 QoS。

Diameter Rx 使用 `Rx_AAR` 和 `Rx_STR`。N5 没有持久的对等连接。每个 app-session 是与为该 UE 发现的 PCF 的独立 HTTP/2 事务。

# Nnrf - NF 管理与发现 (P-CSCF ↔ NRF)

P-CSCF 使用 NRF 发现为每个 VoNR 会话查找 PCF。NRF 发现是唯一的 PCF 发现路径。

## NF 注册 (Nnrf_NFManagement)

P-CSCF 将自己注册为 AF 实例与 NRF。P-CSCF 使用稳定的每主机实例标识。重启时重用一次注册。防止 NRF 积累过时的 AF 注册。

## PCF 发现 (Nnrf_NFDiscovery)

对于 VoNR 会话，P-CSCF 使用 UE 源 IP 查询 NRF。此查询发现为该 UE PDU 会话提供服务的 PCF。**NRF → BSF** 链解决该查询。BSF 持有 UE-IP 到服务-PCF 的绑定。发现的端点成为 N5 目标。如果 P-CSCF 找不到绑定，它将跳过该通话的动态 QoS。会话将继续进行，而不进行专用承载保留。

# 何时使用 SBI 与 Diameter

P-CSCF 从 `P-Access-Network-Info` 头中推导接入类型（根据 TS 24.229 §5.2.6.3）。LTE 报告 `3GPP-E-UTRAN`。5G NR 报告 `3GPP-NR`。P-CSCF 排除了 WiFi（`3GPP-IEEE-802.11`），因为 WiFi 没有专用承载。

| 接入 | **`P-Access-Network-Info`** | **QoS** 路径 | 对等 |
|---|---|---|---|
| 5G NR (VoNR) | `3GPP-NR` | **N5 SBI** (`Npcf_PolicyAuthorization`) | PCF |
| LTE (VoLTE) | `3GPP-E-UTRAN` | **Diameter Rx** | PCRF |
| WiFi | `3GPP-IEEE-802.11` | 无（没有专用承载） | - |

P-CSCF 为每个会话发现 N5 路径的 PCF。它使用 NRF → BSF → 服务-PCF 链。

## 配置

部署工具根据部署提供 SBI 行为。请勿手动编辑 SBI 行为。相关设置如下：

| 设置 | 目的 |
| --- | --- |
| AF 通知端点 | P-CSCF 向 PCF 广告的用于 app-session 事件通知的回调 URL |
| NRF 端点 | 用于 AF 注册和 PCF 发现的 NRF 地址 |
| 家庭 PLMN 身份 (MCC / MNC) | P-CSCF 向 NRF 提供的家庭网络身份 |
| AF 实例身份 | 用于 NRF 注册的稳定每主机身份。重启时重用单个注册。 |

OmniWeb 显示实时的 NRF 注册状态。OmniWeb 还显示每个会话发现的 PCF 绑定。请参见下文。

## 通过 **OmniWeb** 进行管理

Omnitouch 移除了内置的网页控制面板。OmniWeb P-CSCF 页面中的 **NRF** 选项卡显示 NRF 注册状态、发现的 PCF 绑定和 5G/N5 状态。请参见 OmniWeb 文档。

## 常见问题

| 症状 | 可能原因 | □作 |
| --- | --- | --- |
| 找不到 UE 的 PCF 绑定（在呼叫设置时记录） | NRF 或 BSF 尚未为 UE PDU 会话绑定。或者 UE IP 与会话锚点不同。 | 确认 UE PDU 会话已建立。确认 BSF 持有绑定。呼叫在没有动态 QoS 的情况下继续。 |
| PCF 拒绝或忽略 app-session | UE IP 编码在错误的地址族中（`ueIpv4` 与 `ueIpv6`） | 验证 SIP 源地址族与 PDU 会话匹配。请参见上面的地址族注意事项。 |
| 过时的 AF 注册在 NRF 上累积 | AF 实例身份在重启之间不稳定 | 使每主机 AF 实例身份稳定 |
| 5G 呼叫完全没有 N5 流�? | P-CSCF 未将接入检测为 `3GPP-NR`。或者 NRF 无法访问，因此 P-CSCF 未发现 PCF。 | 检查 `P-Access-Network-Info`。验证 NRF 端点是否可达。 |
| VoNR 呼叫设置但没有专用承载 | P-CSCF 未创建 app-session，因为发现失败。或者 P-CSCF 过早拆除了 app-session。 | 将 P-CSCF N5 POST 与 PCF 关联。检查 HTTP/2 连接性和超时。 |

## 相关文档

- Diameter 操作 - 用于 VoLTE (4G/LTE) 的 Rx、Cx 和 Ro Diameter 接口
- P-CSCF 操作 - VoNR 接入检测、N5 QoS 和 NRF 发现的上下文
- 指标参考 - P-CSCF 指标
- OmniWeb 文档 - 管理门户中的 NRF 和 5G 状态

# S-CSCF 作与参考

Serving-CSCF 是 IMS 的本地网络 SIP 注册器和会话控制点。它通过 Cx（MAR/SAR）对用户进行身份验证，并存储注册绑定。它下载用户的服务配置文件（初始过滤标准）。它位于每个发起和终止会话的信令路径中。从这个位置，它通过 ISC 接口触发应用服务器，确认呼叫者的身份，并将会话路由到终止方、应用服务器或 PSTN。HSS 为该用户记录此 S-CSCF 的名称。因此，该用户的所有后续流量都经过此节点。

# IMS 功能

## 注册与身份验证

S-CSCF 是权威注册器。它对 UE 进行挑战。它根据来自 HSS 的 Cx 身份验证向量验证响应。成功后，它记录联系绑定并下载用户的服务配置文件。

注册过程如下：

1. 算法选择。 S-CSCF 使用 UE 在其授权头中提供的算法进行挑战。如果 UE 不提供算法，S-CSCF 默认使用 SIP Digest（MD5）。SIP Digest 适用于非 IMS 软电话。默认情况下，S-CSCF 对每个 REGISTER 进行身份验证��
2. 挑战（**MAR**）。 S-CSCF 收到未凭证的 REGISTER。它通过 Cx Multimedia-Auth-Request 请求 HSS 的身份验证向量。HSS 在响应中返回向量（对于 AKA：RAND、AUTN、XRES、CK、IK）。S-CSCF 回复 **401 Unauthorized**，并带有 `WWW-Authenticate` 头。该头携带 nonce（源自 RAND）和所选算法。如果 HSS 拒绝身份，注册失败 **403**。如果 HSS 不可用或返回格式错误的答案，注册失败 **503**。
3. 验证。 UE 重新发送 REGISTER 及其计算的响应。S-CSCF 检查响应与存储的向量是否匹配。它在公共身份上匹配。
4. 重新同步。如果 UE 报告序列号（SQN）不匹配，S-CSCF 将 AUTS 令牌转发给 HSS 以进行重新同步。然后 S-CSCF 使用新向量重新挑战。
5. 服务器分配（**SAR**）。经过成功身份验证后，S-CSCF 发送 Cx Server-Assignment-Request。分配类型为首次注册时的 REGISTRATION，或在刷新时的重新注册。响应返回用户的数据（服务配置文件和 IFC）。S-CSCF 将用户数据保存在内存中。拒绝的分配或没有 IMS 服务配置文件的用户将失败 **403**。HSS 超时将失败 **503**。
6. 绑定与服务路由。 S-CSCF 将联系绑定与 P-CSCF 路径一起存储。该路径允许终止请求通过相同的 P-CSCF 返回。200 OK 携带服务路由��因此 UE 通过此 S-CSCF 发送后续请求。S-CSCF 每个公共身份最多保留 `maxcontact` 个联系（请参见 S-CSCF 配置中的 usrloc 参数）。多个设备在不同 SIM 上共享的号码（例如手机和智能手表）每个设备保留一个联系：每个设备使用其自己的私有身份（IMPI，源自其 IMSI）在共享公共身份下注册，联系通过联系 URI 匹配。终止呼叫可以分叉到每个设备（请参见终止呼叫处理）。过期时间固定为 599 秒。

7. 第三方注册 / 注册事件。 S-CSCF 还根据 REGISTER 触发的初始过滤标准评估注册。此评估会触发第三方 REGISTER 到任何匹配的应用服务器。注册事件包通知订阅实体注册状态。S-CSCF 在注销时拆除订阅。

You have looked at 39 of
network functions. Answe
questions and we send y

## 一个号码上的多个设备（共享号码）

为了在多个设备上提供一个号码（例如手机和智能手表），S-CSCF 必须在共享公共身份下为每个设备保留一个联系，并将终止呼叫分叉到所有设备。相关的 usrloc / registrar 参数如下:

| 参数 | 值 | 目的 |
| --- | --- | --- |
| `ims_usrloc_scscf maxcontact` | `10` | 每个公共身份的最大联系数。曾为 `1`（单个联系，第二个设备覆盖第一个）。 |
| `ims_usrloc_scscf maxcontact_3gpp` | `10` | 3GPP 联系的相同限制。 |
| `ims_registrar_scscf max_contacts` | `10` | 注册方的联系限制，与 usrloc 保持一致。 |
| `ims_usrloc_scscf maxcontact_behaviour` | `2` | 仅在超过限制时覆盖最旧的联系。 |
| `ims_registrar_scscf append_branches` | `1` | 在终止 `lookup("location")` 时，将每个注册的联系作为并行分支附加，以便呼叫分叉到所有设备。 |

注意：

- `maxcontact` 是按 公共身份 ���数，而不是按设备计数。联系通过联系 URI 匹配，因此每个设备（每个私有身份 / IMSI）在共享公共身份下保留自己的联系。
- 该号码必须在 HSS 中作为共享公共身份进行配置（一个 IMS 订阅，其成员共享该号码）。请参见 HSS “共享公共用户身份”文档。
- 提高 `maxcontact` 适用于所有号码。单个设备的号码不受影响（仍然只有一个联系）。从新联系重新注册而不注销旧联系的设备在旧联系过期之前保留旧联系；终止分叉尝试两个，过时的分支快速失败。

## 通过 **IFC**（**ISC**）触发服务

S-CSCF 根据用户下载的 初始过滤标准 评估每个初始请求。每个 IFC 具有优先级触发点、应用服务器地址和默认处理值。触发点是服务点触发器（方法、请求 URI、SIP 头、会话案例、SDP）的布尔组合。默认处理值是在 AS 失败时继续会话或终止会话。触发点使用合取或析取范式。您可以对单个触发器进行分组和否定。

S-CSCF 按优先级顺序遍历配置文件以处理相关的会话案例。匹配时，它通过 ISC 将请求转发到应用服务器。S-CSCF 使用 原始对话标识符（**ODI**）标记请求。它还插入 **P-Served-User** 头（RFC 5502），标识被服务的用户和会话案例。这些标记使 AS 能够将请求返回到链中的离开点。当 AS 将请求路由回来时，S-CSCF 识别 ODI。然后，它在最后匹配的标准之后恢复 IFC 评估，而不是重新开始。

默认处理控制 AS 失败行为。应用服务器返回 408 或 5xx。然后 S-CSCF 继续到下一个标准（继续会话）或放弃该腿，具体取决于 IFC 的规定。

## 发起呼叫处理

当请求在其顶部路由头中带有发起指示符，或当它从发起应用服务器返回时，请求为 发起。然后 S-CSCF:

- 分配发起对话上下文并记录路由，以便它将对话中的请求识别为发起腿。
- 确认身份。请求不来自 AS。S-CSCF 删除任何客户端提供的 `P-Asserted-Identity`。它用在注册时验证的身份替换身份。这是该腿的经过身份验证的呼叫线路身份。
- 评估发起 IFC，并将匹配项转发到应用服务器通过 ISC。
- 号码规范化。请求 URI 带有 `phone-context`。S-CSCF 在路由之前将请求 URI 重写为本地网络的 `tel:` URI。
- **PSTN / ENUM**。对于 E.164 目的地，S-CSCF 通过 ENUM 解析号码。在 ENUM 未命中时，S-CSCF 将呼叫发送到 PSTN 断点网关，并在网关集之间进行故障转移。如果请求携带漫游的传输和漫游功能指示（`Feature-Caps: +g.3gpp.trf`），S-CSCF 将其路由到该 TRF。
- 计费向量。发起呼叫携带 `P-Charging-Vector` 以进行运营商间计费关联。
- 如果启用了在线计费，S-CSCF 在呼叫继续之前发送信用控制请求（请参见计费）。

S-CSCF 将非 PSTN 目的地转发到终止方。如果同一个 S-CSCF 为终止用户提供服务，则终止处理在本地继续。

## 终止呼叫处理

当请求的请求 URI 是本地服务的身份时，请求为 终止。然后 S-CSCF:

1. 分配终止对话上下文并记录路由，以便它将对话中的请求识别为终止腿。
2. 恢复原始请求 URI。对于非 INVITE 方法，它评估终止 IFC 并将匹配项转发到应用服务器通过 ISC。对于 INVITE，IFC 转发遵循 AS 返回周期。
3. 如果启用了终止在线计费，S-CSCF 在继续之前发送终止方信用控制请求。
4. 位置解析。 S-CSCF 检索被服务用户的注册联系。它通过在注册时记录在路径中的 P-CSCF 将请求转发到每个联系。当多个设备共享公共身份（共享号码）时，`append_branches` 将请求并行分叉到每个注册的联系，以便所有设备响铃。如果用户没有绑定，S-CSCF 返回 **404 Not Found**。
5. S-CSCF 收到对 当前未注册 身份的 INVITE。首先，它通过 Cx Server-Assignment-Request 类型 UNREGISTERED_USER 从 HSS 获取未注册服务配置文件。这使得终止未注册服务能够运行（例如，语音邮件）。HSS 超时将失败 **503**。缺少配置文件将失败 **403**。

S-CSCF 在出口时应用隐私。如果请求声明 `Privacy: id`，S-CSCF 在消息离开 S-CSCF 之前删除 `P-Asserted-Identity`。

## 计费（可选）

通过 Diameter **Ro** 对 OCS 进行在线计费是可选的。您可以根据部署启用它（请参见下面的计费标志）。启用时，S-CSCF 在允许 INVITE 之前发送信用控制请求。S-CSCF 将答案映射到 SIP 响应（例如，资金不足 → 402，信用限额达到 → 486，未知计费用户 → 403）。Service-Context-Id 标识被计费的服务。S-CSCF 从配置参考中列出的计费参数组装此标识符。

在生产中，这通常是 禁用 的。TAS 代替执行计费。TAS 正确计算补充服务（转发、转移、漫游腿），而 S-CSCF 无法端到端观察。将 S-CSCF Ro 计费视为可选功能，而不是默认功能。

## 存在 / 注册事件

S-CSCF 不充当一般的存在服务器。S-CSCF 接受注册事件（`Event: reg`）的 `SUBSCRIBE` 请求（200 OK）。S-CSCF 不提供一般的存在订阅。S-CSCF 仅接受来自注册用户的注册事件 `PUBLISH`。这样的 PUBLISH 更新已发布的注册状态。否则，S-CSCF 将拒绝它 **403**。此配置没有用户可用性（PIDF）存在处理。

# 部署配置（**Ansible** 注入）

Ansible 在部署时呈现 S-CSCF 的运行时配置及其 Diameter 对等表（`scscf.xml`）。下面的值源自网络的 PLMN 身份（MCC/MNC）和节点的库存主机名。

## 身份 / 领域

| 名称 | 控制内容 | 值 / 派生 |
| --- | --- | --- |
| `NETWORKNAME` | 本地 IMS 域。它是 Cx 目标领域和在号码规范化中使用的 `phone-context` | `ims.mnc<mnc>.mcc<mcc>.3gppnetwork.org` |
| `HOSTNAME` | 此节点的 FQDN（主机别名，以及启用 Ro 时的 Diameter origin-host） | `<inventory_hostname>.ims.mnc<mnc>.mcc` |
| `URI` | S-CSCF 自身的 SIP URI。它是注册��和身份验证身份 | `sip:<hostname>:5060` |
| `SCSCF_USER_AGENT` | 节点发出的 `User-Agent` 头 | `User-Agent: Omnitouch S-CSCF <invento` |
| `ISC_MY_URI` | 主机令牌，用于标识此 S-CSCF 的 ODI 路由，当 AS 返回请求时 | `<inventory_hostname>` |
| `ENUM_SUFFIX` | E.164→URI 解析的 ENUM | `mnc<mnc>.mcc<mcc>.3gppnetwork.org.` |

| 名称 | 控制内容 | 值 / 派生 |
| --- | --- | --- |
| | 域后缀，用于发起 PSTN 绑定号码 | |

Ansible 从库存主机地址和 PLMN 模板 SIP 监听套接字（UDP/TCP 5060，TLS 9090）和主机别名。

## 身份验证 - `REG_AUTH_DEFAULT_ALG`

S-CSCF 在必须选择一个而不是回显 UE 请求的算法时应用的默认身份验证算法。选项：

| 值 | 含义 / 何时使用 |
| --- | --- |
| `AKAv1-MD5` | 3GPP IMS-AKA（TS 33.203）。用于带有 IPsec SA 的 USIM/ISIM VoLTE/VoNR 的标准。用于普通移动用户。 |
| `AKAv2-MD5` | 增强的 IMS-AKA 变体。仅在 UE 和 HSS 特别协商 AKAv2 时使用。 |
| `MD5` | 普通 SIP HTTP Digest（无 AKA，无 IPsec）。用于无法进行 AKA 的非 IMS / 软电话客户端。 |
| `CableLabs-Digest` | PacketCable/CableLabs 摘要配置文件。电缆网络部署。 |
| `3GPP-Digest` | 3GPP SIP Digest（TS 33.203 附录 N）。基于密码，无 ISIM。固定电话 / 非 UICC 用户。 |
| `TISPAN-HTTP_DIGEST_MD5` | ETSI TISPAN NASS/HTTP-Digest 配置文件。TISPAN 固定宽带用户。 |
| `HSS-Selected` | 默认。 S-CSCF 不施加算法。HSS 在身份验证答案中返回每个用户的方案。使用此选项，S-CSCF 挑战每个用户使用 HSS 提供的任何内容（移动设备的 AKA，固定设备的 Digest 等）。 |

该算法不会更改以下默认值。S-CSCF 默认对每个 REGISTER 进行身份验证（请参见 `WITH_AUTH`）。Cx 目标领域是本地网络域（`NETWORKNAME`）。S-CSCF 在公共身份上匹配身份验证向量。向量在 599 秒后过期。

## 计费（**Ro**） - 标志和对等

| 名称 | 控制内容 | 值 |
| --- | --- | --- |
| `WITH_RO` | 启用发起 Diameter Ro 信用控制，在发出 INVITE 之前 | define / undef（默认：undef） |
| `WITH_RO_TERM` | 启用终止侧 Diameter Ro 信用控制 | define / undef（默认：undef） |
| `RO_DESTINATION` | OCS Diameter 目标主机（目标领域是本地网络域） | OCS FQDN，例如 `hssocs.voiceblue.com` |
| `RO_FORCED_PEER` | 将信用控制路由固定到特定的 Diameter 对等。此选项绕过领域路由 | 对等 ID（例如 `32260@3gpp.org`）；默认关闭 |
| `RO_ROOT` | Service-Context-Id 根 | `32260@3gpp.org` |
| `RO_EXT` | Service-Context-Id 扩展 | `ext` |
| `RO_MNC` | Service-Context-Id 的 MNC 组件 | 例如 `07` |
| `RO_MCC` | Service-Context-Id 的 MCC 组件 | 例如 `262` |
| `RO_RELEASE` | Service-Context-Id 的 3GPP 版本 | 例如 `8` |

功能标志（`WITH_*`）

| 标志 | 定义时的效果 |
| --- | --- |
| `WITH_AUTH` | 对每个 REGISTER 进行身份验证（不仅仅是 Digest/MD5 客户端）。在模板中默认启用。 |
| `WITH_RO` | 启用通过 Diameter Ro 进行发起在线计费。 |
| `WITH_RO_TERM` | 启用通过 Diameter Ro 进行终止在线计费。 |

仅当为部署启用 Homer 捕获时，Ansible 会模板 `CAPTURE_NODE`（Homer 捕获目标）。`CAPTURE_NODE` 将 SIP 信令复制到 Homer 进行跟踪。

## Diameter 对等配置

S-CSCF 的 Diameter 对等表（`scscf.xml`）向 HSS 广告 **Cx** 应用程序（`16777216`）以及基本计费。文件结构和填充它的 Ansible 变量在所有 CSCF 之间共享。请参见 Diameter → 对等配置（部署）。当 Ro 计费启用时，`RO_DESTINATION` 指向 OCS 对等，而不是 XML。

# 故障排除

### 注册失败

症状：用户无法注册，注册超时，REGISTER 上的 4xx/5xx。

- **HSS** 连接（**Cx**） - S-CSCF 依赖 HSS 回应 Cx MAR（身份验证向量）和 SAR（服务配置文件）。如果 MAR/SAR 超时或返回格式错误的答案，注册将失败 **503**。请验证到 HSS 的 Cx 对等是否正常并响应。请参见 Diameter 操作。
- 身份验证失败 - 确认用户的凭据已在 HSS 中配置，并且 HSS 生成了身份验证向量（MAR/MAA）。请验证挑战算法是否是 UE 支持的算法（USIM/ISIM 的 AKA/Milenage，非 IMS 客户端的 Digest）。被拒绝的身份将失败 **403**。
- **S-CSCF** 分配 / 容量 - 没有 IMS 服务配置文件的用户，或被拒绝的服务器分配（SAR），将失败 **403**。请确认 S-CSCF 的能力与 I-CSCF 选择的内容匹配。还要确认节点是否具有注册容量。

### 呼叫设置失败

症状：呼叫无法建立，4xx/5xx SIP 错误。

- 用户未注册 - 请验证发起和终止身份是否均已 IMS 注册。对没有联系绑定的身份的终止 INVITE 返回 **404**。对于具有已配置服务的未注册终止身份，S-CSCF 获取未注册的配置文件（Cx SAR UNREGISTERED_USER）。此处的 HSS 超时将失败 **503**。
- **IFC /** 服务触发 - 请验证 S-CSCF 是否从 HSS 下载了 IFC（SAR/SAA），并且触发点是否与会话案例匹配。检查通过 ISC 调用的任何应用服务器（OmniTAS、OmniMessage）是否可达。默认处理控制 AS 失败是否继续该腿或放弃它。
- **QoS** - P-CSCF 授权呼叫的媒体 QoS（Rx 到 PCRF 用于 VoLTE，N5 到 PCF 用于 VoNR）。如果呼叫 ``接但没有媒体路径，请检查 P-CSCF 上的策略腿。
- 路由 - 对于 E.164 目的地，请验证 ENUM 解析和 PSTN 网关故障转移。请验证离开本地网络的呼叫的漫游/离网路由。

### 短信发送问题

症状：短信未通过IMS发送，或回退到传统SMSC。

- **IFC触发OmniMessage** - 验证订阅者的IFC是否在SIP MESSAGE方法上触发OmniMessage，并且其优先级是否足够高以触发。使用模拟短信测试IFC匹配。
- **SMSC集成** - 验证OmniMessage与SMSC（MAP/SMPP）的连接性，以及SIP MESSAGE ↔ SMS PDU转换是否完整。
- 内容类型 - 验证SIP MESSAGE是否携带`Content-Type: application/vnd.3gpp.sms`和正确的字符集编码（GSM-7, UCS-2）。

## 呼叫流程

序列图嵌入了它们所记录的功能：

- 注册与认证 → 注册与认证
- 发起会话 → 发起呼叫处理
- 终止会话 → 终止呼叫处理

## 相关文档

- 操作

- Diameter
- 基于服务的接口 (SBI)
- 指标参考
- OmniWeb - 注册、对话和Diameter对等状态: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

# ANSSI R226 拦截合规文档

文档目的：本文档提供 ANSSI R226 授权所需的技术规格。这些规格适用于法国刑法第 R226-3 和 R226-7 条款。它们涵盖了 OmniCSCF IMS 核心网络（呼叫会话控制功能）。

分类：监管合规文档

目标机构：法国国家信息系统安全局（ANSSI）

法规： R226 - 保护通信隐私和合法拦截

---

## 1. 详细技术规格

### 1.1 系统识别

产品名称： OmniCSCF IMS 核心网络
产品类型： IP 多媒体子系统（IMS）核心网络
主要功能： VoIP/VoLTE 呼叫会话控制和多媒体服务交付
部署模型：本地电信基础设施

网络组件：

- P-CSCF（代理呼叫会话控制功能）
- E-CSCF（紧急呼叫会话控制功能）
- I-CSCF（查询呼叫会话控制功能）
- S-CSCF（服务呼叫会话控制功能）

该系统处理 IP 多媒体子系统（IMS）网络的注册、认证、会话路由和呼叫控制。以下部分描述了拦截能力和加密特性。

### 1.2 拦截能力

#### 1.2.1 注册和会话获取

**SIP** 注册捕获：

CSCF 系统处理所有 SIP 注册。它保持完整的注册状态：

- 用户标识符：
  - IMPU（IP 多媒体公共身份） - SIP URI（例如，sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org）
  - IMPI（IP 多媒体私有身份） - 认证用户名（例如，user@ims.mnc001.mcc001.3gppnetwork.org）
  - IMSI（国际移动用户身份） - 来自 P 头或 HSS
  - MSISDN（手机号码） - 来自 IMPU 或 HSS 用户配置文件
- 注册元数据：
  - 联系 URI（实际 UE 网络地址）
  - 路径头（通过 P-CSCF 返回的路由）
  - 服务路由头（路由到 S-CSCF）
  - 用户代理字符串（设备类型识别）
  - 注册过期时间戳
  - 源 IP 地址和端口
  - 传输协议（TCP/UDP/TLS）
  - 认证向量（RAND、AUTN、XRES、CK、IK 来自 HSS）
- 网络位置信息：
  - P-Access-Network-Info 头（基站、位置区域）
  - P-Visited-Network-ID（漫游网络标识）
  - 接收的 IP 地址（实际来源）
  - P-CSCF 地址（网络入口点）

呼叫会话捕获：

S-CSCF 保持所有活动呼叫的完整 SIP 对话状态：

- 会话标识符：
  - Call-ID（唯一会话标识符）
  - From/To URI 和标签
  - 双方的路由集

    - Original-Dialog-ID（用于应用服务器交互跟踪）

- 会话元数据：
    - 呼叫者身份（From 头，P-Asserted-Identity）
    - 被叫方（To 头，请求 URI）
    - 会话建立时间戳
    - 会话终止时间戳
    - 对话状态（早期/确认/删除）
    - CSeq 编号（事务排序）
- 媒体信息：
    - SIP 消息体中的 SDP（会话描述协议）
    - 媒体服务器地址（OmniTAS）
    - 编解码器信息（音频/视频格式）
    - 媒体流端点
    - RTP/RTCP 端口分配

紧急呼叫识别：

E-CSCF 组件识别紧急呼叫并进行路由：

- 紧急号码检测（112、911 等）
- IMEI（国际移动设备身份）捕获
- IMEI 到 MSISDN 的映射（用于回拨）
- 来自 UE 或网络的位置
- HELD（HTTP 启用的位置交付）协议支持
- 紧急路由目的地（PSAP/紧急 AS）

呼叫身份确定（根据 **3GPP TS 23.167**）：

系统建立在紧急腿上呈现的经过认证的呼叫线路身份，如下所示：

- 已知呼叫者（注册）： 系统从注册的 IMPU 中获取身份。在适用的情况下，它还使用 P-CSCF 持有的缓存 IMEI→MSISDN 绑定。
- 未知/匿名呼叫者（未经认证的紧急呼叫，没有注册身份）： P-CSCF 通过 Diameter Rx 接口从 PCRF 解析 EPC 级身份。它使用异��的 `Rx_AAR_Subscription`，由 UE 源 IP 地址绑定。系统按优先级选择身份 **MSISDN**

→ **IMSI → IMEISV**。它将解析的值作为 **P-Asserted-Identity** 断言在 `sos.apn` 域上。

在这两种情况下，结果 P-Asserted-Identity 是呈现给 PSAP 和 LI 接口的经过认证的呼叫线路身份。它是网络断言的身份，而不仅仅是近似值。

### 1.2.2 数据存储和处理

重要提示：仅在内存状态

CSCF 组件（P-CSCF、E-CSCF、I-CSCF、S-CSCF）仅将 所有状态数据保存在内存中。没有对注册或呼叫会话数据的持久数据库存储。系统将所有注册绑定、对话状态和 IPsec 安全关联保存在内存中。系统在重启时会丢失这些数据。

活动注册数据（内存中）：

CSCF 系统仅保持实时状态：

**P-CSCF** 注册状态：

- IPsec 安全关联数据（SPI 对、端口、加密参数）
- UE 联系绑定和网络地址
- IPsec 隧道端点和状态
- 注册有效期

**S-CSCF** 注册状态：

- 公共身份（IMPU）和当前注册状态
- 带有路径头、用户代理、接收地址的联系绑定
- 私有身份（IMPI）到公共身份的映射
- 来自 HSS 的用户配置文件（在注册期间缓存）

活动会话状态（内存中）：

S-CSCF 仅保持活动呼叫状态：

- 呼叫标识符（Call-ID）、参与者身份（From/To 标签）
- 路由集和联系地址
- 会话状态（早期/确认/终止）
- 会话时间信息

无 **CDR** 或历史跟踪：

CSCF 组件不生成或存储：

- 呼叫详细记录（CDR）
- 历史呼叫记录
- 历史注册记录
- 长期事件跟踪

**CDR** 生成和历史跟踪： **TAS**（电话应用服务器 **- OmniTAS**）处理所有呼叫详细记录、计费数据和历史呼叫跟踪。CSCF 组件不处理它们。

**SIP/Diameter** 消息日志记录：

CSCF 可以生成实时事件日志以供操作使用：

- **SIP** 消息日志记录：可选的 SIP 消息日志记录（INVITE、REGISTER 等）
- **Diameter** 消息日志记录：可选的 Diameter 事务日志记录（Cx、Rx、Ro）
- 系统事件：配置更改、错误、故障

这些日志是瞬态操作日志，而不是持久的呼叫记录。您可以配置日志保留。保留时间通常是短期的（几小时到几天），仅用于调试。

### 1.2.3 分析能力

实时监控：

OmniWeb 管理门户（<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>）提供：

- 注册监控：
  - 查看所有注册用户，带分页
  - 按 IMPU、联系、IMPI 搜索
  - 注册详细信息（联系、路径、用户代理、过期）
  - 强制注销能力
- 对话监控：
  - 活动呼叫会话视图

    - Call-ID□From/To URI□□□□□□□□
    - □□□□□□□□□ BYE□
    - □ 5 □□□□□
- □□□□□
    - Diameter □□□□□HSS□PCRF□OCS □□□
    - □□□□□□
    - □□□□□□
    - IPsec □□□□□P-CSCF□

□□□□□□□□□□

CSCF □□□□□□□□□□**OmniTAS**□□□□□□□□□ □□□□ CDR □□□□□□□□□□□□□□□□□□□□CDR □□ □□□□□□□□□□□□□□□□ OmniTAS □□□

□□□□□□□□□□

S-CSCF □□□□□□□□□□□iFC□□

- iFC □□□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□
- □□□□□□□□□□ SIP □□□□□□

□□□□□

- HSS □□□□□Diameter Cx □□□
- S-CSCF □□□□□I-CSCF□
- □□□□□□
- □□□□□□□□□
- Diameter □□□□

# 1.3 □□□□

### 1.3.1 □□□□□□

□□□□□□

- **IPsec** 隧道：UE 和 P-CSCF 之间的 ESP（封装安全负载）隧道
  - 加密：AES-CBC、AES-GCM
  - 认证：HMAC-SHA1、HMAC-SHA256
  - 从 IMS AKA 派生密钥（CK/IK 来自 HSS）
  - 每个 UE 的安全关联
- **TLS/TLS** 支持：
  - SIP over TLS（SIPS）支持
  - Diameter over TLS（HSS、PCRF、OCS 连接）
  - 基于证书的认证
  - 完美前向保密（PFS）通过 ECDHE/DHE
- **SIP** 隐私头：
  - P-Asserted-Identity（经过认证的来电 ID）
  - 隐私头（请求来电 ID 抑制）
  - 匿名会话支持

访问控制：

- OmniWeb 认证和基于角色的访问控制
- BINRPC 管理接口（端口 2046）
- 注册访问控制和角色分离
- SIP 认证（通过 HSS 的 AKA）
- Diameter 对等认证

审计日志：

- 全面的 SIP 和 Diameter 消息日志记录
- 注册/注销事件
- 呼叫建立和终止事件
- 通过 OmniWeb 的管理操作
- 配置更改
- 认证成功/失败

### 1.3.2 数据保护特性

访问安全:

- 基于角色的访问控制（RBAC）
- 只读监控账户
- 认证和授权控制

系统加固:

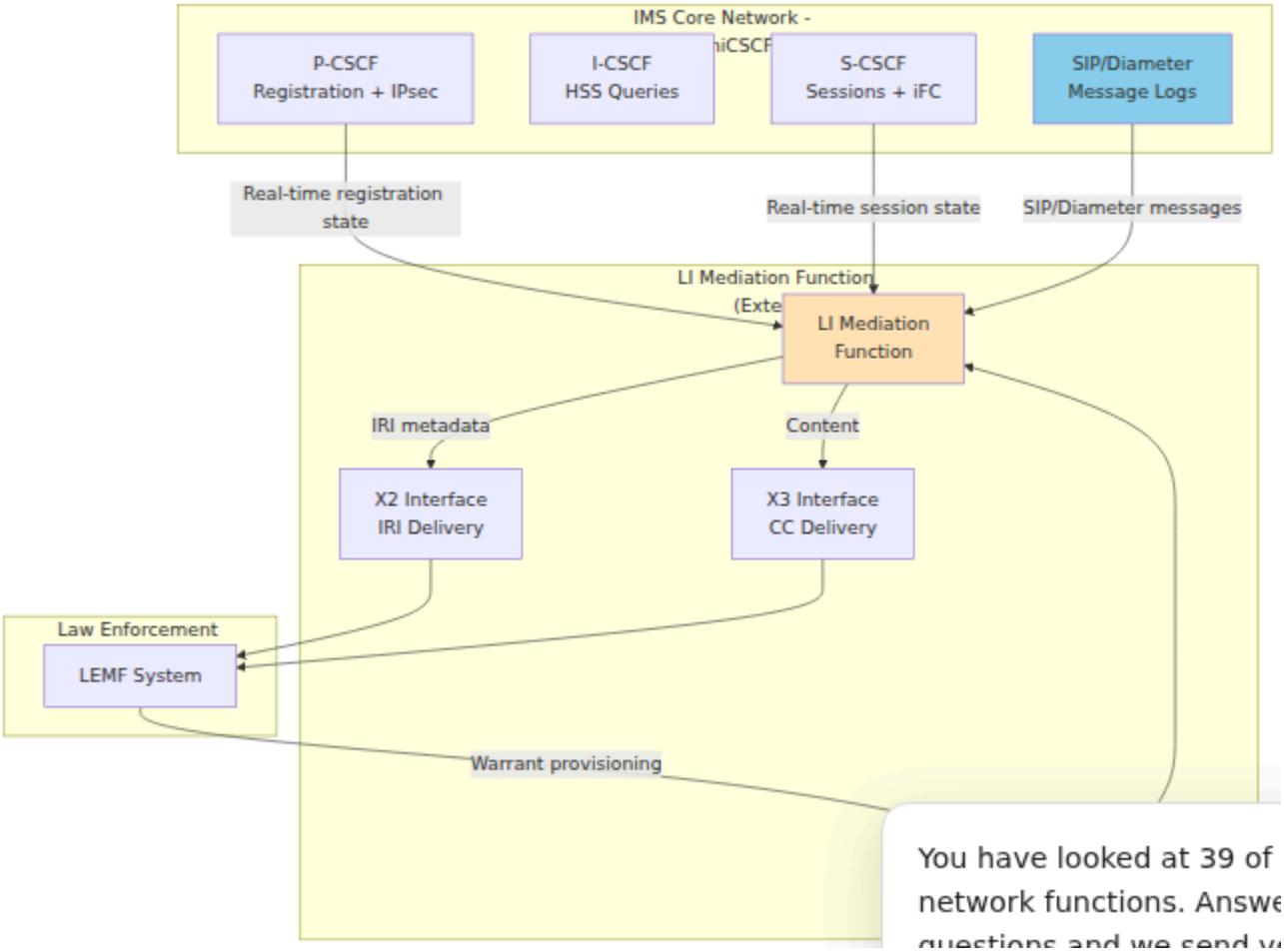
- 最小暴露的网络端口（5060 SIP、3868 Diameter、2046 BINRPC 管理）
- SIP 消息合理性检查
- Max-Forwards 循环预防
- 速率限制和防洪保护
- 消息大小限制
- 工作进程隔离

## 1.4 合法拦截集成点

### 1.5.1 ETSI 合法拦截架构

CSCF 系统为符合 ETSI 的合法拦截提供基础。系统不内置原生 X1/X2/X3 接口。所有必要的数据访问点均存在，以便���外部合法拦截中介功能（LIMF）系统集成。

标准 **ETSI LI** 接口:



**X1** 接口 **-** 管理功能:

- 目的：来自执法机构的令状和目标提供
- 方向： LEMF → LIMF（双向）
- 功能:
  - 为目标（IMPU、IMSI、MSISDN）激活/停用拦截
  - 设置拦截持续时间和有效期
  - 配置过滤标准（身份、时间窗口）
  - 检索拦截状态
- 与 **CSCF** 的集成:
  - LIMF 保持令状数据库（目标列表，外部于 CSCF）
  - LIMF 监控 CSCF 实时状态和消息日志以匹配会话
  - LIMF 根据 X1 提供的标准进行过滤

**X2** 接口 **- IRI**（拦截相关信息）交付:

- 目的：向执法机构交付会话元数据
- 方向： LIMF → LEMF（单向）

- 数据格式：符合 ETSI TS 102 232 的 XML/ASN.1
- 来自 **CSCF** 的内容：
  - 会话标识符（Call-ID、对话标签）
  - 呼叫方（From URI、P-Asserted-Identity、IMPU、IMSI、MSISDN）
  - 被叫方（To URI、请求 URI、IMPU、IMSI、MSISDN）
  - 注册时间戳
  - 会话建立/拆除时间戳
  - 网络位置（P-Access-Network-Info、基站、位置区域）
  - P-CSCF/S-CSCF 地址（网络元素识别）
  - 用户代理（设备类型）
  - 漫游信息（P-Visited-Network-ID）

**X3** 接口 **- CC**（通信内容）交付：

- 目的：交付实际通信内容
- 方向： LIMF → LEMF（单向）
- 数据格式：符合 ETSI TS 102 232
- 来自 **CSCF** 的内容：
  - SIP 消息体（SDP 会话描述）
  - 媒体服务器地址（用于 RTP 拦截）
  - 编解码器信息
  - SIP MESSAGE 即时消息（正文内容）
  - 应用数据（如果通过 CSCF 路由）

注意：对于语音/视频 RTP 流，LIMF 还必须与媒体服务��（OmniTAS）集成。此集成捕获实际媒体内容。CSCF 提供会话设置信息（SDP）。此信息显示媒体流向何处。

### 1.5.2 CSCF 数据源用于合法拦截

**1.** 注册数据访问：

**P-CSCF** 注册数据：

- IMPU（公共身份）
- 联系 URI（UE 网络地址）
- 接收的 IP 和端口

- 路径头
- 注册过期
- IPsec SPI 和端口信息
- 用户代理字符串

**S-CSCF** 注册数据：

- 公共身份（IMPU）、禁止状态、注册状态
- 带有路径头、用户代理、接收地址的联系绑定
- 私有身份（IMPI）到公共身份的映射
- 来自 HSS 的用户配置文件（包含用户详细信息的 XML 格式）

访问方法：

- 只读数据访问接口
- OmniWeb 监控接口
- 实时事件日志记录

**2.** 活动会话数据：

**S-CSCF** 对话数据：

- Call-ID（唯一会话标识符）
- From/To URI 和标签
- 呼叫者和被叫者 CSeq 编号
- 双方的路由集
- 联系地址
- 对话状态（早期、确认、删除）
- 开始时间戳
- 超时值

访问方法：

- 实时对话状态监控
- 按会话标识符或方标识符查询
- 法医分析的导出能力

### 3. SIP 消息日志记录:

日志捕获:

- 所有 SIP 消息均可记录（REGISTER、INVITE、MESSAGE 等）
- 可配置的日志级别
- 带时间戳的结构化日志
- Syslog 或基于文件的日志记录

日志分析:

- 解析 SIP 头以提取身份
- 提取 SDP 以获取媒体信息
- 跟踪消息序列（CSeq）
- 关联请求和响应

示例日志条目:

```
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. Diameter** 消息日志记录:

**Cx** 消息（**HSS** 通信）：

- UAR/UAA: 用户授权（包含 IMPU、IMPI）
- LIR/LIA: 位置信息（包含 IMPU、服务 S-CSCF）
- MAR/MAA: 认证（包含 IMPI、认证向量）
- SAR/SAA: 服务器分配（包含 IMPU、IMPI、用户配置文件 XML）

可用的 **Diameter** 数据:

- IMSI（来自用户配置文件）
- MSISDN（来自用户配置文件）
- 相关的 IMPU（每个用户多个身份）
- ��户配置文件（服务、禁止、漫游状态）

日志示例:

```
Diameter Cx SAA received from 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 (Success)
User-Data: <XML user profile with IMSI, MSISDN, iFC>
```

**5.** 紧急呼叫数据（**E-CSCF**）：

**IMEI** 到 **MSISDN** 映射:

- P-CSCF 在 UE 使用 IMEI 注册时创建映射（htable `emergency_imei_msisdn_map`）
- 4 小时 TTL（14400s 自动过期）
- 用于紧急回拨
- 在 P-CSCF 集群节点之间复制

数据保留:

- IMEI 到 MSISDN 的映射保留 4 小时（14400s）

- 可用于紧急回拨关联
- 可通过监控接口访问

紧急呼叫日志：

- 紧急号码检测（112、911 等）
- 从联系或 P 头提取 IMEI
- 位置信息（来自 HELD 或 P-Access-Network-Info）
- PSAP（公共安全应答点）路由
- E-CSCF 到紧急 AS 路由

### 1.5.3 LIMF 的集成能力

该系统为合法拦截中介功能（LIMF）系统提供了几种集成方法：

1. 注册和会话数据访问：
    - 实时访问注册数据（身份、位置、设备信息）
    - 活动会话监控（呼叫状态、参与者、时间）
    - 历史查询能力
2. 事件日志记���：
    - SIP 消息日志记录，具有可配置的详细级别
    - Diameter 消息日志记录用于 HSS 交互
    - 带时间戳的结构化事件日志
3. 实时监控：
    - 实时注册状态监控
    - 活动呼叫会话跟踪
    - 紧急呼叫检测和路由信息

集成方法支持 LIMF 连接的轮询基础和事件驱动架构。

### 1.5.4 CSCF 数据映射到 LI 接口

**CSCF** 数据到 **IRI**（**X2**）映射：

| **CSCF** 数据源 | **IRI** 字段 | 数据示例 |
| --- | --- | --- |
| IMPU（SIP 头/内存状态） | A 方 | sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org |
| IMPI（SIP 头/内存状态） | 认证 ID | user@ims.mnc001.mcc001.3gppnetwork.org |
| IMSI（HSS 用户配置文件） | 用户 ID | 208011234567890 |
| MSISDN（HSS 用户配置文件） | 电话号码 | +33612345678 |
| Call-ID（SIP 头/对话状态） | 会话 ID | f81d4fae-7dec-11d0-a765-00a0c91e6bf6@... |
| From/To（SIP 头） | A 方/B 方 | sip:+33612345678@... / sip:+33687654321@... |
| 注册时间戳（内存中） | 事件时间 | 2025-11-29T10:30:00Z |
| P-Access-Network-Info（SIP 头） | 位置 | 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=208011234567890 |
| 接收的 IP（SIP 联系） | UE IP | 10.20.30.40:5060 |

| **CSCF** 数据源 | **IRI** 字段 | 数据示例 |
| --- | --- | --- |
| | 地址 | |
| P-CSCF 地址（SIP 路由） | 网络元素 | 10.4.12.165:5060 |
| S-CSCF 地址（SIP 路由） | 网络元素 | 10.4.11.45:5060 |

**CSCF** 数据到 **CC**（**X3**）映射：

| **CSCF** 数据源 | **CC** 字段 | 数据示例 |
| --- | --- | --- |
| SIP MESSAGE 正文 | 即时消息内容 | "你好，你好吗？" |
| INVITE 中的 SDP | 媒体会话信息 | RTP 端点、编解码器 |
| 媒体服务器地址 | RTP 拦截目标 | 10.50.60.70:49170 |

注意：对于实际语音/视频内容（RTP），LIMF 必须与媒体服务器（OmniTAS）协调以捕获 RTP 流。CSCF 仅提供会话设置信息。

关于紧急呼叫身份（**A** 方）的说明：对于正常（注册）呼叫，系统从注册的 IMPU / P-Asserted-Identity 中推导 A 方。对于未知/匿名紧急呼叫，P-CSCF 从 PCRF 通过 Diameter Rx 解析 A 方（`Rx_AAR_Subscription`，由 UE 源 IP 绑定，优先级为 MSISDN → IMSI → IMEISV）。P-CSCF 将此身份作为 P-Asserted-Identity 断言在 `sos.apn` 域上，符合 3GPP TS 23.167。这是此类呼叫在 X2/IRI 接口上传递的经过认证的呼叫线路身份。

## 1.5 基于 Web 的监控接口

**OmniWeb** 提供监控和管理访问。OmniWeb 是统一管理门户（<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>）。它提供对 CSCF 组件的实时监控和管理访问：

监控能力：

- 实时注册和会话监控（活动用户、位置、设备信息、呼叫状态、时间）
- 按 IMPU、IMPI、IMSI 或 MSISDN 搜索身份
- IPsec 隧道状态和容量监控
- 法医分析的导出能力

安全性：

- HTTPS/TLS 加密访问
- 需要认证
- 基于角色的访问控制（RBAC），包括监控人员的只读访问模式
- 所有管理操作的审计日志记录

---

# 2. 加密和密码分析能力

## 2.1 加密能力概述

OmniCSCF 实现了多个加密保护层，用于信令和用户数据。本节记录了 ANSSI 要求的所有加密能力。

## 2.2 IPsec ESP 隧道加密（UE 到 P-CSCF）

### 2.2.1 IPsec 协议实现

支持的 **IPsec** 模式：

- ESP（封装安全负载） - IP 协议 50
- 传输模式（非隧道模式）
- 保护 UE 和 P-CSCF 之间的 SIP 信令

支持的加密算法：

该系统与内核 IPsec 支持：

- **AES-CBC**（高级加密标准 - 密码块链接）：

    - AES-128-CBC（128 位密钥）
    - AES-192-CBC（192 位密钥）
    - AES-256-CBC（256 位密钥） - 推荐
- **AES-GCM**（高级加密标准 **- Galois/**计数模式）：
    - AES-128-GCM（128 位密钥，带 AEAD）
    - AES-256-GCM（256 位密钥，带 AEAD） - 推荐
- **3DES-CBC**（三重 **DES -** 密码块链接）：
    - 168 位有效密钥（已弃用，遗留兼容性）
- **NULL** 加密：
    - 无机密性（仅认证）
    - 仅用于调试或特定合规场景

支持的认证算法：

- **HMAC-SHA1**（基于哈希的消息认证码 **- SHA-1**）：
    - 160 位输出
    - 遗留兼容性
- **HMAC-SHA256**（**HMAC - SHA-256**）：
    - 256 位输出
    - 推荐
- **HMAC-SHA384**（**HMAC - SHA-384**）：
    - 384 位输出
- **HMAC-SHA512**（**HMAC - SHA-512**）：
    - 512 位输出
- **HMAC-MD5**：
    - 128 位输出

- 已弃用，仅用于遗留兼容性

密钥派生：

系统从 IMS AKA 认证派生 IPsec 密钥（CK - 加密密钥，IK - 完整性密钥）：

1. UE 与 S-CSCF/HSS 执行 AKA 认证
2. HSS 生成 CK（128 位）和 IK（128 位）
3. S-CSCF 通过内部接口将 CK/IK 传递给 P-CSCF
4. P-CSCF 使用 CK/IK 与 UE 建立 IPsec 安全关联
5. CK 用于 ESP 加密
6. IK 用于 ESP 认证

安全关联参数：

- 生命周期：与 SIP 注册过期相关（通常为 599 秒）
- 重放保护：启用（防重放窗口）
- 序列号： 32 位或 64 位（ESN - 扩展序列号）
- 完美前向保密：不适用（密钥来自 AKA，而非 Diffie-Hellman）

实现：

P-CSCF 的 IPsec 能力：

- 与 Linux 内核 IPsec 堆栈（XFRM 框架）接口
- 通过内核 API 配置安全策略和关联
- SPI（安全参数索引）分配和管理
- 保护流量的端口分配

### 2.2.2 IPsec 配置能力

密码套件选择：

您可以配置 P-CSCF 优先选择特定的密码套件：

推荐（强安全性）：

- ESP 使用 AES-256-GCM 和 HMAC-SHA256
- ESP 使用 AES-256-CBC 和 HMAC-SHA256

支持（兼容性）：

- ESP 使用 AES-128-CBC 和 HMAC-SHA1
- ESP 使用 3DES-CBC 和 HMAC-SHA1（遗留）

密钥管理：

- 不使用 IKE（互联网密钥交换）
- 密钥通过 IMS AKA 提供（CK/IK 来自 HSS）
- 通过内核 XFRM 手动设置安全关联
- 注册过期时自动拆除 SA

隧道生命周期：

1. UE 注册 → AKA 认证 → 生成 CK/IK
2. P-CSCF 从 S-CSCF 接收 CK/IK
3. P-CSCF 分配 SPI 对（客户端 SPI、服务器 SPI）
4. P-CSCF 分配端口对（客户端端口、服务器端口）
5. P-CSCF 使用 CK/IK 配置内核 IPsec SA
6. P-CSCF 在 200 OK 中向 UE 发送 IPsec 参数（Security-Server 头）
7. UE 使用相同参数配置 IPsec SA
8. 所有后续 SIP 流量通过 ESP 隧道流动
9. 在注册过期或注销时：删除 SA，释放资源

# 2.3 TLS 加密（SIP 和 Diameter）

## 2.3.1 SIP 的 TLS（SIPS）

支持的 **TLS** 版本：

- **TLS 1.2**（RFC 5246） - 支持
- **TLS 1.3**（RFC 8446） - 支持（如果内核/库支持）
- **TLS 1.0/1.1** - 已弃用（默认禁用）
- **SSL 2.0/3.0** - 不支持（已知漏洞）

**TLS** 实现：

系统使用 OpenSSL 或 LibreSSL:

- 行业标准 TLS 库
- 经过密码学验证的实现
- 定期安全更新

支持的密码套件:

**TLS 1.3**（推荐）:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

**TLS 1.2**（支持）:

- ECDHE-RSA-AES256-GCM-SHA384（完美前向保密）
- ECDHE-RSA-AES128-GCM-SHA256（完美前向保密）
- ECDHE-ECDSA-AES256-GCM-SHA384（完美前向保密）
- DHE-RSA-AES256-GCM-SHA384（完美前向保密）
- DHE-RSA-AES128-GCM-SHA256（完美前向保密）

禁用弱密码:

- 无 RC4
- 无 MD5
- 无 NULL 加密
- 无 EXPORT 级密码
- 无 DES/3DES（已弃用）

证书支持:

- **X.509** 证书（标准格式）
- **RSA** 密钥：最小 2048 位，推荐 4096 位
- **ECDSA** 密钥：支持 P-256、P-384、P-521 曲线
- 证书链验证
- **CRL**（证书撤销列表）检查（可选）

- **OCSP**（在线证书状态协议）（可选）

**TLS** 特性：

- 完美前向保密（**PFS**）：通过 ECDHE/DHE 密钥交换
- 服务器名称指示（**SNI**）：支持
- **TLS** 会话恢复：支持（性能优化）
- 客户端证书认证：支持（双向 TLS）

**SIP over TLS**（**SIPS**）：

- 传输：带 TLS 加密的 TCP
- 端口：5061（标准 SIPS 端口）
- 用于 CSCF 之间的通信（可选）
- 用于受信网络连接

### 2.3.2 Diameter 的 TLS

**Diameter** 能力：

系统支持以下内容：

- **Diameter over SCTP**（首选以确保可靠性）
- **Diameter over TCP with TLS**
- 端口：3868（标准 Diameter 端口）

用例：

- **Cx** 接口：S-CSCF/I-CSCF 到 HSS（用户数据、认证）
- **Rx** 接口：P-CSCF 到 PCRF（QoS 策略）
- **Ro** 接口：S-CSCF 到 OCS（在线计费 - 如果启用）

**Diameter** 的 **TLS** 配置：

与 SIP 相同的密码套件

- TLS 1.2/1.3
- ECDHE/DHE 密钥交换（PFS）
- AES-GCM 加密

- SHA256/SHA384 认证

基于证书的认证：

- Diameter 对等通过 TLS 证书进行认证
- 双向 TLS（客户端和服务器证书）
- 证书中的 FQDN（完全合格域名）验证
- 受信 CA 链验证

## 2.4 认证密码学

### 2.4.1 IMS AKA 加密功能

**3GPP AKA 算法（MILENAGE）：**

用于生成认证向量（RAND、AUTN、XRES、CK、IK）：

加密功能：

- **f1**：消息认证功能（计算 MAC-A 和 MAC-S）
- **f2**：响应功能（根据 RAND 和 K 计算 RES）
- **f3**：加密密钥派生（计算 CK）
- **f4**：完整性密钥派生��计算 IK）
- **f5**：匿名密钥功能（计算 IMSI 隐私的 AK）

密钥材料：

- **K**：128 位永久用户密钥（存储在 ISIM 和 HSS 中）
- **OPc**：操作员变体密钥（从 K 和 OP 派生）
- **RAND**：128 位随机挑战
- **SQN**：48 位序列号（重放保护）

**AKA 序列：**

1. HSS 生成 RAND（密码学随机）
2. HSS 计算 MAC-A = f1(K, RAND, SQN, AMF)
3. HSS 计算 AUTN = (SQN ⊕ AK) || AMF || MAC-A
4. HSS 计算 XRES = f2(K, RAND)

5. HSS 计算 CK = f3(K, RAND)
6. HSS 计算 IK = f4(K, RAND)
7. HSS 将 {RAND, AUTN, XRES, CK, IK} 发送给 S-CSCF
8. S-CSCF 用 RAND 和 AUTN 挑战 UE
9. UE 使用 ISIM 计算 RES = f2(K, RAND)
10. UE 将 RES 发送给 S-CSCF
11. S-CSCF 将 RES 与 XRES 进行比较（认证验证）

安全属性：

- 双向认证：UE 通过 AUTN 验证 HSS，HSS 通过 RES 验证 UE
- 密钥新鲜度：RAND 是随机的，SQN 防止重放
- 密钥派生：CK 和 IK 从共享秘密 K 派生

### 2.4.2 HTTP 摘要认证

对于非 IMS 认证（如果使用）：

算法：MD5（RFC 2617）

- 哈希函数：MD5（128 位输出）
- 挑战-响应：基于随机数
- 重放保护：带时间戳的随机数

注意：HTTP 摘要与 MD5 被认为是弱的。强烈建议使用 IMS AKA。

## 2.5 哈希和完整性

### 2.5.1 可用的哈希函数

系统可以使用以下哈希函数（通过 OpenSSL/内核加密）：

- **SHA-256**：256 位输出，推荐
- **SHA-384**：384 位输出
- **SHA-512**：512 位输出
- **SHA-1**：160 位输出，已弃用用于安全用途
- **MD5**：128 位输出，已弃用用于安全用途

使用：

- HMAC 构造用于 IPsec/TLS
- 数据完整性验证
- 随机数生成
- 重复检测（呼叫 ID 哈希）

### 2.5.2 消息完整性

**SIP** 消息完整性：

- **IPsec ESP**：HMAC-SHA256 用于经过认证的 SIP over IPsec
- **TLS**：通过 TLS MAC 进行消息认证
- **SIP** 摘要：认证头完整性

**Diameter** 消息完整性：

- **TLS**：Diameter over TLS 提供消息认证
- **HMAC**：Diameter 消息可以包含 HMAC AVP 以确保完整性

## 2.6 随机数生成

密码学安全的随机数生成：

系统依赖以下内容：

- **Linux** 内核 **/dev/urandom**：密码学安全的 PRNG
- **OpenSSL RAND_bytes():** CSPRNG（密码学安全伪随机数生成器）

使用：

- SPI 分配（随机起始值）
- 呼叫 ID 生成
- 分支参数生成
- 认证的随机数生成
- 会话 ID 生成

# 2.7 密钥管理

## 2.7.1 TLS 证书管理

证书存储：

- 文件系统存储，权限受限（0600）
- 位于：`/etc/system/tls/`
- 证书和密钥的 PEM 格式

证书生成：

```
# 生成 RSA 4096 位私钥
openssl genrsa -out system-key.pem 4096

# 生成 CSR（证书签署请求）
openssl req -new -key system-key.pem -out system.csr \
  -subj
"/C=FR/ST=IDF/L=Paris/O=Omnitouch/CN=scscf.ims.mnc001.mcc001.3gppnetw

# 自签名证书（开发/测试）
openssl x509 -req -days 365 -in system.csr \
  -signkey system-key.pem -out system-cert.pem

# 生产：将 CSR 提交给受信 CA
```

证书轮换：

- 建议每年更新证书
- 优雅地重启服务以加载新证书
- 不需要停机

## 2.7.2 IPsec 密钥管理

密钥派生：

- CK（加密密钥）和 IK（完整性密钥）来自 IMS AKA
- 来自 HSS 的 128 位密钥
- 通过 Diameter Cx 安全传递（通过 TLS）

密钥生命周期：

- 与 SIP 注册过期相关（通常为 599 秒）
- 注册刷新时重新密钥
- 注销时自动销毁密钥

密钥存储：

- 短暂（仅在活动注册期间保存在内存中）
- 安装在内核 IPsec 堆栈中
- 无持久密钥存储
- 删除 SA 时丢弃密钥

# 2.8 密码分析抵抗

## 2.8.1 算法选择

抵御密码分析：

- 无自定义算法：仅使用行业标准、经过同行评审的算法
- 强密钥大小：AES-256、RSA-4096、SHA-256
- 经过认证的加密：AES-GCM（AEAD - 带关联数据的经过认证的加密）
- 完美前向保密：TLS 中的 ECDHE/DHE
- 定期更新：应用 OpenSSL/LibreSSL 安全补丁

禁用已弃用的算法：

- MD5（哈希碰撞）
- RC4（流密码弱点）
- DES/3DES（小块大小、密钥长度）
- SSL 2.0/3.0（协议漏洞）
- TLS 1.0/1.1（BEAST、POODLE 攻击）

## 2.8.2 侧信道攻击缓解

时间攻击抵抗：

- 对认证响应进行恒定时间比较

- 在加密操作中没有时间泄漏（通过 OpenSSL）

内存保护：

- 内核 IPsec 堆栈隔离
- 进程内存隔离
- 对敏感数据不使用交换（如果配置）

## 2.9 合规性和标准

加密标准合规性：

- **NIST SP 800-52**：TLS 指南
- **NIST SP 800-131A**：加密算法过渡
- **RFC 7525**：TLS 建议
- **ETSI TS 133 203**：3GPP 接入安全（IMS AKA）
- **ETSI TS 133 210**：IP 网络层安全（IPsec）
- **3GPP TS 33.203**：IMS 的接入安全
- **3GPP TS 33.210**：网络域安全

法国加密法规：

- 无出口限制的加密（所有标准算法）
- 标准加密手段（无政府后门）
- ANSSI 加密产品认证（如有需要）

# IMS CSCF 指标参考

本文档是 P-CSCF、I-CSCF 和 S-CSCF 组件导出的所有指标的参考。

## 访问指标

所有 CSCF 组件在 9090 端口上公开 Prometheus 指标:

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

每个 CSCF 主机（P-CSCF、I-CSCF、S-CSCF）导出其自己的指标。要获得全面的监控覆盖，请配置您的 Prometheus 服务器以抓取所有主机。

示例 **Prometheus** 配置:

```
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']
```

有关监控和警报的指导，请参见:

- 通过 OmniWeb 和 Grafana 进行监控

# 通过 **OmniWeb** 和 **Grafana** 进行监控

在 **OmniWeb** 中查看操作状态，这是统一的��理门户：<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>。操作状态包括注册、对话和 Diameter 对等状态。OmniWeb 嵌入 Grafana 仪表板，以实现实时和历史可见性。这些仪表板包括 S-CSCF 注册和用户位置视图。指标 `ims_usrloc_scscf_active_impus` 和 `ims_usrloc_scscf_active_contacts` 支持这些视图。仪表板还显示 Diameter 对等状态和队列深度。指标 `cdp_queuelength` 和接口指标 `ims_icscf_uar_*`、`ims_icscf_lir_*`、`ims_auth_mar_*`、`ims_registrar_scscf_sar_*` 和 `ims_qos_*` 支持这些视图。

本参考中的 Prometheus 指标支持这些 Grafana 仪表板。它们还支持您配置的任何自定义警报。

---

# P-CSCF 指标

## CDP (Diameter) 指标

| 指标名称 | 意义 |
| --- | --- |
| `cdp_average_response_time` | Diameter 请求的平均响应时间（以毫秒为单位，计算方式为 replies_response_time / replies_received） |
| `cdp_queuelength` | Diameter 工作队列任务的当前长度 |
| `cdp_replies_received` | 接收到的 Diameter 回复总数 |
| `cdp_replies_response_time` | 等待 Diameter 回复的总时间（以毫秒为单位） |
| `cdp_timeout` | Diameter 请求的超时事件数量 |

## 核心 **SIP** 统计

请求计数器

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_requests` | 接收到的 SIP 请求总数 |
| `core_rcv_requests_ack` | 接收到的 ACK 请求数量 |
| `core_rcv_requests_bye` | 接收到的 BYE 请求数量 |
| `core_rcv_requests_cancel` | 接收到的 CANCEL 请求数量 |
| `core_rcv_requests_info` | 接收到的 INFO 请求数量 |
| `core_rcv_requests_invite` | 接收到的 INVITE 请求数量 |
| `core_rcv_requests_message` | 接收到的 MESSAGE 请求数量 |
| `core_rcv_requests_notify` | 接收到的 NOTIFY 请求数量 |
| `core_rcv_requests_options` | 接收到的 OPTIONS 请求数量 |
| `core_rcv_requests_prack` | 接收到的 PRACK 请求数量 |
| `core_rcv_requests_publish` | 接收到的 PUBLISH 请求数量 |
| `core_rcv_requests_refer` | 接收到的 REFER 请求数量 |
| `core_rcv_requests_register` | 接收到的 REGISTER 请求数量 |
| `core_rcv_requests_subscribe` | 接收到的 SUBSCRIBE 请求数量 |
| `core_rcv_requests_update` | 接收到的 UPDATE 请求数量 |

回复计数器（一般）

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_replies` | 接收到的 SIP 回复总数 |
| `core_rcv_replies_18x` | 接收到的 180/181/183/186/187/189 临时响应数量 |
| `core_rcv_replies_1xx` | 接收到的 1xx（临时）响应数量 |
| `core_rcv_replies_2xx` | 接收到的 2xx（成功）响应数�? |
| `core_rcv_replies_3xx` | 接收到的 3xx（重定向）响应数量 |
| `core_rcv_replies_4xx` | 接收到的 4xx（客户端错误）响应数量 |
| `core_rcv_replies_5xx` | 接收到的 5xx（服务器错误）响应数量 |
| `core_rcv_replies_6xx` | 接收到的 6xx（全局失败）响应数量 |

按方法分类的回复计数器（**1xx**）

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_replies_1xx_bye` | 对 BYE 请求的 1xx 响应数量 |
| `core_rcv_replies_1xx_cancel` | 对 CANCEL 请求的 1xx 响应数量 |
| `core_rcv_replies_1xx_invite` | 对 INVITE 请求的 1xx 响应数量 |
| `core_rcv_replies_1xx_message` | 对 MESSAGE 请求的 1xx 响应数量 |
| `core_rcv_replies_1xx_prack` | 对 PRACK 请求的 1xx 响应数量 |
| `core_rcv_replies_1xx_refer` | 对 REFER 请求的 1xx 响应数量 |
| `core_rcv_replies_1xx_reg` | 对 REGISTER 请求的 1xx 响应数量 |
| `core_rcv_replies_1xx_update` | 对 UPDATE 请求的 1xx 响应数量 |

按方法分类的回复计数器（**2xx**）

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_replies_2xx_bye` | 对 BYE 请求的 2xx（成功）响应数量 |
| `core_rcv_replies_2xx_cancel` | 对 CANCEL 请求的 2xx（成功）响应数量 |
| `core_rcv_replies_2xx_invite` | 对 INVITE 请求的 2xx（成功）响应数量 |
| `core_rcv_replies_2xx_message` | 对 MESSAGE 请求的 2xx（成功）响应数量 |
| `core_rcv_replies_2xx_prack` | 对 PRACK 请求的 2xx（成功）响应数量 |
| `core_rcv_replies_2xx_refer` | 对 REFER 请求的 2xx（成功）响应数量 |
| `core_rcv_replies_2xx_reg` | 对 REGISTER 请求的 2xx（成功）响应数量 |
| `core_rcv_replies_2xx_update` | 对 UPDATE 请求的 2xx（成功）响应数量 |

按方法分类的回复计数器（**3xx**）

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_replies_3xx_bye` | 对 BYE 请求的 3xx（重定向）响应数量 |
| `core_rcv_replies_3xx_cancel` | 对 CANCEL 请求的 3xx（重定向）响应数量 |
| `core_rcv_replies_3xx_invite` | 对 INVITE 请求的 3xx（重定向）响应数量 |
| `core_rcv_replies_3xx_message` | 对 MESSAGE 请求的 3xx（重定向）响应数量 |
| `core_rcv_replies_3xx_prack` | 对 PRACK 请求的 3xx（重定向）响应数量 |
| `core_rcv_replies_3xx_refer` | 对 REFER 请求的 3xx（重定向）响应数量 |
| `core_rcv_replies_3xx_reg` | 对 REGISTER 请求的 3xx（重定向）响应数量 |
| `core_rcv_replies_3xx_update` | 对 UPDATE 请求的 3xx（重定向）响应数量 |

按方法分类的回复计数器（**4xx**）

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_replies_4xx_bye` | 对 BYE 请求的 4xx（客户端错误）响应数量 |
| `core_rcv_replies_4xx_cancel` | 对 CANCEL 请求的 4xx（客户端错误）响应数量 |
| `core_rcv_replies_4xx_invite` | 对 INVITE 请求的 4xx（客户端错误）响应数量 |
| `core_rcv_replies_4xx_message` | 对 MESSAGE 请求的 4xx（客户端错误）响应数量 |
| `core_rcv_replies_4xx_prack` | 对 PRACK 请求的 4xx（客户端错误）响应数量 |
| `core_rcv_replies_4xx_refer` | 对 REFER 请求的 4xx（客户端错误）响应数量 |
| `core_rcv_replies_4xx_reg` | 对 REGISTER 请求的 4xx（客户端错误）响应数量 |
| `core_rcv_replies_4xx_update` | 对 UPDATE 请求的 4xx（客户端错误）响应数量 |

按方法分类的回复计数器（**5xx**）

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_replies_5xx_bye` | 对 BYE 请求的 5xx（服务器错误）响应数量 |
| `core_rcv_replies_5xx_cancel` | 对 CANCEL 请求的 5xx（服务器错误）响应数量 |
| `core_rcv_replies_5xx_invite` | 对 INVITE 请求的 5xx（服务器错误）响应数量 |
| `core_rcv_replies_5xx_message` | 对 MESSAGE 请求的 5xx（服务器错误）响应数量 |
| `core_rcv_replies_5xx_prack` | 对 PRACK 请求的 5xx（服务器错误）响应数量 |
| `core_rcv_replies_5xx_refer` | 对 REFER 请求的 5xx（服务器错误）���应数量 |
| `core_rcv_replies_5xx_reg` | 对 REGISTER 请求的 5xx（服务器错误）响应数量 |
| `core_rcv_replies_5xx_update` | 对 UPDATE 请求的 5xx（服务器错误）响应数量 |

按方法分类的回复计数器（**6xx**）

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_replies_6xx_bye` | 对 BYE 请求的 6xx（全局失败）响应数量 |
| `core_rcv_replies_6xx_cancel` | 对 CANCEL 请求的 6xx（全局失败）响应数量 |
| `core_rcv_replies_6xx_invite` | 对 INVITE 请求的 6xx（全局失败）响应数量 |
| `core_rcv_replies_6xx_message` | 对 MESSAGE 请求的 6xx（全局失败）响应数量 |
| `core_rcv_replies_6xx_prack` | 对 PRACK 请求的 6xx（全局失败）响应数量 |
| `core_rcv_replies_6xx_refer` | 对 REFER 请求的 6xx（全局失败）响应数量 |
| `core_rcv_replies_6xx_reg` | 对 REGISTER 请求的 6xx（全局失败）响应数量 |
| `core_rcv_replies_6xx_update` | 对 UPDATE 请求的 6xx（全局失败）响应数量 |

特定状态码计数器

| 指标名称 | 意义 |
| --- | --- |
| core_rcv_replies_400 | 接收到的 400 Bad Request 响应数量 |
| core_rcv_replies_401 | 接收到的 401 Unauthorized 响应数量 |
| core_rcv_replies_402 | 接收到的 402 Payment Required 响应数量 |
| core_rcv_replies_403 | 接收到的 403 Forbidden 响应数量 |
| core_rcv_replies_404 | 接收到的 404 Not Found 响应数量 |
| core_rcv_replies_405 | 接收到的 405 Method Not Allowed 响应数量 |
| core_rcv_replies_406 | 接收到的 406 Not Acceptable 响应数量 |
| core_rcv_replies_407 | 接收到的 407 Proxy Authentication Required 响应数量 |
| core_rcv_replies_408 | 接收到的 408 Request Timeout 响应数量 |
| core_rcv_replies_409 | 接收到的 409 Conflict 响应数量 |
| core_rcv_replies_410 | 接收到的 410 Gone 响应数量 |
| core_rcv_replies_411 | 接收到的 411 Length Required 响应数量 |
| core_rcv_replies_413 | 接收到的 413 Request Entity Too Large 响应数量 |
| core_rcv_replies_414 | 接收到的 414 Request-URI Too Long 响应数量 |
| core_rcv_replies_415 | 接收到的 415 Unsupported Media Type 响应数量 |
| core_rcv_replies_420 | 接收到的 420 Bad Extension 响应数量 |
| core_rcv_replies_480 | 接收到的 480 Temporarily Unavailable 响应数量 |
| core_rcv_replies_481 | 接收到的 481 Call/Transaction Does Not Exist 响应数量 |

| 指标名称 | 意义 |
| --- | --- |
| `core_rcv_replies_482` | 接收到的 482 Loop Detected 响应数量 |
| `core_rcv_replies_483` | 接收到的 483 Too Many Hops 响应数量 |
| `core_rcv_replies_484` | 接收到的 484 Address Incomplete 响应数量 |
| `core_rcv_replies_485` | 接收到的 485 Ambiguous 响应数量 |
| `core_rcv_replies_486` | 接收到的 486 Busy Here 响应数量 |
| `core_rcv_replies_487` | 接收到的 487 Request Terminated 响应数量 |
| `core_rcv_replies_488` | 接收到的 488 Not Acceptable Here 响应数量 |
| `core_rcv_replies_489` | 接收到的 489 Bad Event 响应数量 |
| `core_rcv_replies_491` | 接收到的 491 Request Pending 响应数量 |
| `core_rcv_replies_493` | 接收到的 493 Undecipherable 响应数量 |

转发和错误统计



| 指标名称 | 意义 |
| --- | --- |
| `core_fwd_replies` | 转发的 SIP 回复数量 |
| `core_fwd_requests` | 转发的 SIP 请求数量 |
| `core_drop_replies` | 丢弃的 SIP 回复数量 |
| `core_drop_requests` | 丢弃的 SIP 请求数量 |
| `core_err_replies` | 错误回复数量 |
| `core_err_requests` | 错误请求数量 |
| `core_bad_URIs_rcvd` | 接收到的带有格式错误的 URI 的消息数量 |
| `core_bad_msg_hdr` | 带有错误/格式错误的头部的消息数量 |
| `core_unsupported_methods` | 带有不支持的 SIP 方法的请求数量 |

## 对话跟踪

| 指标名称 | 意义 |
| --- | --- |
| `dialog_ng_active` | 当前活动（已接听/确认）对话的数量 |
| `dialog_ng_early` | 早期对话的数量（响铃/临时���态） |
| `dialog_ng_expired` | 已过期或被强制终止的对话数量 |
| `dialog_ng_processed` | 自启动以来处理的对话总数 |

## DNS 统计

| 指标名称 | 意义 |
| --- | --- |
| `dns_failed_dns_request` | 失败的 DNS 查询数量 |
| `dns_slow_dns_request` | 慢 DNS 查询的数量（超过阈值） |

## IMS IPSec P-CSCF

| 指标名称 | 意义 |
| --- | --- |
| `ims_ipsec_pcscf_spi_free` | 可用于分配的空闲 SPI（安全参数索引）值的数量 |
| `ims_ipsec_pcscf_spi_total` | 系统配置的总 SPI 容量 |
| `ims_ipsec_pcscf_spi_used` | 当前分配/使用的 SPI 值的数量 |
| `ims_ipsec_pcscf_spi_utilization_pct` | SPI 池利用率的百分比 |
| `ims_ipsec_pcscf_worker_cache_size` | 工作进程 IPSec 缓存的大小 |

## IMS QoS (Rx 接口)

注册 **AAR** 指标

| 指标名称 | 意义 |
| --- | --- |
| `ims_qos_active_registration_rx_sessions` | 当前活动的注册 Rx 会话数量 |
| `ims_qos_registration_aars` | 发送的注册 AAR（授权-认证请求）消息的总数量 |
| `ims_qos_successful_registration_aars` | 成功的注册 AAR 事务数量 |
| `ims_qos_failed_registration_aars` | 失败的注册 AAR 事务数量 |
| `ims_qos_registration_aar_avg_response_time` | 注册 AAR 消息的平均响应时间（以毫秒为单位） |
| `ims_qos_registration_aar_response_time` | 所有注册 AAR 消息的总响应时间（以毫秒为单位） |
| `ims_qos_registration_aar_replies_received` | 接收到的注册 AAR 回复的总数量 |
| `ims_qos_registration_aar_timeouts` | 注册 AAR 请求超时的数量 |

媒体 **AAR** 指标

| 指标名称 | 意义 |
| --- | --- |
| `ims_qos_active_media_rx_sessions` | 当前活动的媒体 Rx 会话数量 |
| `ims_qos_media_rx_sessions` | 创建的媒体 Rx 会话的总数量 |
| `ims_qos_media_aars` | 发送的媒体 AAR 消息的总数量 |
| `ims_qos_successful_media_aars` | 成功的媒体 AAR 事务数量 |
| `ims_qos_failed_media_aars` | 失败的媒体 AAR 事务数量 |
| `ims_qos_media_aar_avg_response_time` | 媒体 AAR 消息的平均响应时间（以毫秒为单位） |
| `ims_qos_media_aar_response_time` | 所有媒体 AAR 消息的总响应时间（以毫秒为单位） |
| `ims_qos_media_aar_replies_received` | 接收到的媒体 AAR 回复的总数量 |
| `ims_qos_media_aar_timeouts` | 媒体 AAR 请求超时的数量 |

### **ASR** 指标

| 指标名称 | 意义 |
| --- | --- |
| `ims_qos_asrs` | 接收到的 ASR（中止会话请求）消息的总数量 |

## **P-CSCF** 用户位置

| 指标名称 | 意义 |
| --- | --- |
| `ims_usrloc_pcscf_expired_contacts` | 过期联系绑定的数量 |
| `ims_usrloc_pcscf_registered_contacts` | 当前注册的联系绑定数量 |
| `ims_usrloc_pcscf_registered_impus` | 当前注册的 IMPUs（IMS 公共用户身份）数量 |

## MySQL 数据库

| 指标名称 | 意义 |
| --- | --- |
| `mysql_driver_errors` | MySQL 驱动/连接错误的数量 |

## 防洪（IP 阻止）

| 指标名称 | 意义 |
| --- | --- |
| `pike_blocked_ips` | 当前被阻止的 IP 地址数量（洪水检测） |

## 注册模块

| 指标名称 | 意义 |
| --- | --- |
| `registrar_accepted_regs` | 接受的 REGISTER 请求数量（传统注册模块） |
| `registrar_rejected_regs` | 拒绝的 REGISTER 请求数量（传统注册模块） |
| `registrar_default_expire` | 注册的默认过期时间（以秒为单位） |
| `registrar_default_expires_range` | 默认过期范围设置 |
| `registrar_expires_range` | 配置的过期范围 |
| `registrar_max_contacts` | 每个 AOR 允许的最大联系数量 |
| `registrar_max_expires` | 允许的最大过期时间（以秒为单位） |

脚本统计

| 指标名称 | 意义 |
| --- | --- |
| `script_register_failed` | 在路由脚本逻辑中失败的注册尝试数量 |
| `script_register_success` | 路由脚本处理的成功注册数量 |
| `script_register_time` | 在路由脚本中处理注册所花费的总时间（以毫秒为单位） |

## SCTP 传输

| 指标名称 | 意义 |
| --- | --- |
| `sctp_assoc_shutdown` | 本地发起的 SCTP 关联关闭的数量 |
| `sctp_comm_lost` | 由于通信故障而丢失的 SCTP 关联数量 |
| `sctp_connect_failed` | 失败的外发 SCTP 关联尝试数量 |
| `sctp_current_opened_connections` | 当前打开的 SCTP 关联数量 |
| `sctp_current_tracked_connections` | 当前跟踪的 SCTP 关联数量 |
| `sctp_established` | 建立的 SCTP 关联的总数量 |
| `sctp_local_reject` | 本地拒绝的传入 SCTP 关联数量 |
| `sctp_remote_shutdown` | 对等方发起的 SCTP 关联关闭数量 |
| `sctp_send_failed` | 失败的 SCTP 发送操作数量 |
| `sctp_send_force_retry` | 失败的 SCTP 发送操作上强制重试的数量 |
| `sctp_sendq_full` | 由于发送队列已满而失败的发送尝试数量 |

### 共享内存

| 指标名称 | 意义 |
| --- | --- |
| `shmem_fragments` | 共享内存池中的片段数量（指示碎片化） |
| `shmem_free_size` | 以字节为单位的可用共享内存量 |
| `shmem_max_used_size` | 自启动以来使用的最大共享内存（以字节为单位） |
| `shmem_real_used_size` | 实际使用的共享内存，包括分配器开销（以字节为单位） |
| `shmem_total_size` | 共享内存池的总大小（以字节为单位） |
| `shmem_used_size` | 当前使用的共享内存（仅用户数据，以字节为单位） |

## **SL**（无状态）模块

按类别分类的无状态回复计数器

| 指标名称 | 意义 |
| --- | --- |
| `sl_1xx_replies` | 发送的 1xx 无状态回复数量 |
| `sl_2xx_replies` | 发送的 2xx 无状态回复数量 |
| `sl_3xx_replies` | 发送的 3xx 无状态回复数量 |
| `sl_4xx_replies` | 发送的 4xx 无状态回复数量 |
| `sl_5xx_replies` | 发送的 5xx 无状态回复数量 |
| `sl_6xx_replies` | 发送的 6xx 无状态回复数量 |
| `sl_xxx_replies` | 发送的其他无状态回复数量 |

特定无状态回复计数器

| 指标名称 | 意义 |
| --- | --- |
| `sl_200_replies` | 发送的 200 OK 无状态回复数量 |
| `sl_202_replies` | 发送的 202 Accepted 无状态回复数量 |
| `sl_300_replies` | 发送的 300 Multiple Choices 无状态回复数量 |
| `sl_301_replies` | 发送的 301 Moved Permanently 无状态回复数量 |
| `sl_302_replies` | 发送的 302 Moved Temporarily 无状态回复数量 |
| `sl_400_replies` | 发送的 400 Bad Request 无状态回复数量 |
| `sl_401_replies` | 发送的 401 Unauthorized 无状态回复数量 |
| `sl_403_replies` | 发送的 403 Forbidden 无状态回复数量 |
| `sl_404_replies` | 发送的 404 Not Found 无状态回复数量 |
| `sl_407_replies` | 发送的 407 Proxy Authentication Required 无状态回复数量 |
| `sl_408_replies` | 发送的 408 Request Timeout 无状态回复数量 |
| `sl_483_replies` | 发送的 483 Too Many Hops 无状态回复数量 |
| `sl_500_replies` | 发送的 500 Server Internal Error 无状态回复数量 |

无状态一般统计

| 指标名称 | 意义 |
| --- | --- |
| `sl_sent_replies` | 发送的无状态回复总数 |
| `sl_sent_err_replies` | 发送的无状态错误回复数量 |
| `sl_received_ACKs` | 接收到的无状态事务的 ACK 消息数量 |
| `sl_failures` | 无状态回复发送失败的数量 |

## TCP 传输

| 指标名称 | 意义 |
| --- | --- |
| `tcp_con_reset` | TCP 连接重置的数量（在已建立连接上接收到 RST） |
| `tcp_con_timeout` | 由于空闲超时而关闭的 TCP 连接数量 |
| `tcp_connect_failed` | 失败的外发 TCP 连接尝试数量 |
| `tcp_connect_success` | 成功的外发 TCP 连接数量 |
| `tcp_current_opened_connections` | 当前打开的 TCP 连接数量 |
| `tcp_current_write_queue_size` | 当前所有连接的 TCP 写队列的总大小 |
| `tcp_established` | 建立的 TCP ���接的总数量（包括传入和外发） |
| `tcp_local_reject` | 本地拒绝的传入 TCP 连接数量 |
| `tcp_passive_open` | 接受的传入 TCP 连接数量 |
| `tcp_send_timeout` | 超时的 TCP 发送操作数量（异步模式） |
| `tcp_sendq_full` | 由于发送队列已满而失败的发送尝试数量 |

# TM/TMX（事务）模块

事务类型计数器

| 指标名称 | 意义 |
| --- | --- |
| `tmx_UAC_transactions` | 创建的 UAC（客户端）事务数量 |
| `tmx_UAS_transactions` | 创建的 UAS（服务器）事务数量 |
| `tmx_active_transactions` | 当前活动的事务数量 |
| `tmx_inuse_transactions` | 当前正在使用的事务数量 |

按状态分类的事务完成情况

| 指标名称 | 意义 |
| --- | --- |
| `tmx_2xx_transactions` | 以 2xx 响应完成的事务数量 |
| `tmx_3xx_transactions` | 以 3xx 响应完成的事务数量 |
| `tmx_4xx_transactions` | 以 4xx 响应完成的事务数量 |
| `tmx_5xx_transactions` | 以 5xx 响应完成的事务数量 |
| `tmx_6xx_transactions` | 以 6xx 响应完成的事务数量 |

事务回复统计

| 指标名称 | 意义 |
| --- | --- |
| `tmx_rpl_absorbed` | 由事务层吸收的回复数量（重复） |
| `tmx_rpl_generated` | 由事务模块本地生成的回复数量 |
| `tmx_rpl_received` | 接收到的事务回复数量 |
| `tmx_rpl_relayed` | 由事务模块转发的回复数量 |
| `tmx_rpl_sent` | 由事务模块发送的回复数量 |

用户位置

| 指标名称 | 意义 |
| --- | --- |
| `usrloc_location_contacts` | 'location' 域中的联系数量（标准 usrloc 模块） |
| `usrloc_location_expires` | 'location' 域中过期的联系数量 |
| `usrloc_registered_users` | 注册用户/AOR（地址记录）的数量 |

---

# I-CSCF 指标

I-CSCF 与 P-CSCF 共享大多数核心 SIP 统计数据。请参见上面的 P-CSCF 核心 SIP 统计部分。以下指标特定于 I-CSCF。

## I-CSCF 作上下文

I-CSCF 保持可用 S-CSCF 实例的列表以进行负载均衡。对于新的注册，I-CSCF 查询 HSS 以选择正确的 S-CSCF 实例。下面的 UAR 和 LIR 指标跟踪这些操作的成功情况。

# IMS I-CSCF (Cx 接口 - HSS 通信)

I-CSCF 使用 Diameter Cx 接口与 HSS（家庭用户服务器）进行通信。它发送用户位置和授权查询。

**UAR**（用户授权请求）指标

| 指标名称 | 意义 |
| --- | --- |
| `ims_icscf_uar_avg_response_time` | UAR 消息的平均响应时间（以毫秒为单位，计算方式为 uar_replies_response_time / uar_replies_received） |
| `ims_icscf_uar_replies_received` | 从 HSS 接收到的 UAA（用户授权应答）回复的总数量 |
| `ims_icscf_uar_replies_response_time` | 所有 UAR 消息的总响应时间（以毫秒为单位） |
| `ims_icscf_uar_timeouts` | UAR 请求超时的数量 |

**LIR**（位置信息请求）指标

| 指标名称 | 意义 |
| --- | --- |
| `ims_icscf_lir_avg_response_time` | LIR 消息的平均响应时间（以毫秒为单位，计算方式为 lir_replies_response_time / lir_replies_received） |
| `ims_icscf_lir_replies_received` | 从 HSS 接收到的 LIA（位置信息应答）回复的总数量 |
| `ims_icscf_lir_replies_response_time` | 所有 LIR 消息的总响应时间（以毫秒为单位） |
| `ims_icscf_lir_timeouts` | LIR 请求超时的数量 |

公共指标

I-CSCF 还导出以下公共指标。上面的 P-CSCF 部分记录了这些指标。

- **CDP (Diameter)** 指标 - Diameter 协议统计

- 核心 **SIP** 统计 - 按方法和状态码的请求/回复计数器
- **DNS** 统计 - DNS 查询指标
- **MySQL** 数据库 - 数据库连接错误
- 防洪 - IP 阻止统计
- 共享内存 - 内存使用统计
- **SL**（无状态）模块 - 无状态回复计数器
- **TCP** 传��� - TCP 连接统计
- **TM/TMX**（事务）模块 - 事务状态跟踪

---

# S-CSCF 指标

S-CSCF 与 P-CSCF 和 I-CSCF 共享大多数核心 SIP 统计数据。请参见上面的 P-CSCF 核心 SIP 统计部分。以下指标特定于 S-CSCF。

## S-CSCF □作上下文

S-CSCF 提供详细的用户位置信息。它还管理 IFC（初始过滤标准）。

用户位置查找显示注册的 IMPUs 及其联系绑定和服务配置文件。指标 `ims_usrloc_scscf_active_contacts` 和 `ims_usrloc_scscf_active_impus` 跟踪活动联系和 IMPUs 的数量。

IFC（初始过滤标准）确定哪些应用服务器处理 SIP 会话。IFC 评估性能可能会改变呼叫设置时间。事务指标（`tmx_*`）跟踪这些时间。

## IMS ISC (IMS 服务控制)

IMS ISC 模块评估初始过滤标准（iFC）。它确定哪些应用服务器必须处理 SIP 会话。这些指标跟踪 iFC 匹配操作的性能和效果。

| 指标名称 | 意义 |
| --- | --- |
| `ims_isc_ifc_match_attempts` | 执行的 iFC 匹配尝试的总数量 |
| `ims_isc_ifc_match_time_total` | 执行 iFC 匹配操作所花费的累计时间（以毫秒为单位） |
| `ims_isc_ifc_nomatch_count` | 没有触发条件匹配的 iFC 匹配尝试的数量 |

性能监控：计算平均 iFC 匹配时间为 `ifc_match_time_total / ifc_match_attempts`。高平均时间可能表明过滤标准复杂。它还可能表明应用服务器选择的性能限制。高比例的 `ifc_nomatch_count` 与 `ifc_match_attempts` 可能表明触发点不正确。它还可能表明意外的流量模式。

## IMS 认证（Cx 接口 - MAR）

S-CSCF 使用 Diameter Cx 接口通过 HSS 进行用户认证。它发送 MAR（多媒体认证请求）。

| 指标名称 | 意义 |
| --- | --- |
| `ims_auth_mar_avg_response_time` | MAR 消息的平均响应时间（以毫秒为单位，计算方式为 mar_replies_response_time / mar_replies_received） |
| `ims_auth_mar_replies_received` | 从 HSS 接收到的 MAA（多媒体认证应答）回复的总数量 |
| `ims_auth_mar_replies_response_time` | 所有 MAR 消息的总响应时间（以毫秒为单位） |
| `ims_auth_mar_timeouts` | MAR 请求超时的数量 |

## IMS 注册 S-CSCF

注册统计

| 指标名称 | 意义 |
| --- | --- |
| `ims_registrar_scscf_accepted_regs` | 成功接受的 REGISTER 请求数量 |
| `ims_registrar_scscf_rejected_regs` | 拒绝的 REGISTER 请求数量 |
| `ims_registrar_scscf_default_expire` | 注册的默认过期时间（以秒为单位） |
| `ims_registrar_scscf_default_expires_range` | 默认过期范围配置 |
| `ims_registrar_scscf_max_contacts` | 每个注册允许的最大联系数量 |
| `ims_registrar_scscf_max_expires` | 允许的最大过期时间（以秒为单位） |
| `ims_registrar_scscf_notifies_in_q` | 队列中待处理的 NOTIFY 消息数量 |

**SAR**（服务器分配请求）指标

| 指标名称 | 意义 |
| --- | --- |
| `ims_registrar_scscf_sar_avg_response_time` | SAR 消息的平均响应时间（以毫秒为单[ 算方式为 sar_replies_response_ti / sar_replies_received） |
| `ims_registrar_scscf_sar_replies_received` | 从 HSS 接收到的 SAA（服务器分配[ 答）回复的总数量 |
| `ims_registrar_scscf_sar_replies_response_time` | 所有 SAR 消息的总响应时间（以毫秒为[ 位） |
| `ims_registrar_scscf_sar_timeouts` | SAR 请求超时的数量 |

## S-CSCF 用户位置

| 指标名称 | 意义 |
| --- | --- |
| `ims_usrloc_scscf_active_contacts` | 当前活动的注册联系绑定数量 |
| `ims_usrloc_scscf_active_impus` | 当前活动的注册 IMPUs（IMS 公共用户身份）数量 |
| `ims_usrloc_scscf_active_subscriptions` | 当前活动的订阅数量 |
| `ims_usrloc_scscf_contact_collisions` | 联系哈希表中的哈希冲突数量 |
| `ims_usrloc_scscf_impu_collisions` | IMPU 哈希表中的哈希冲突数量 |
| `ims_usrloc_scscf_subscription_collisions` | 订阅哈希中的哈希冲突数量 |

### 对话跟踪

S-CSCF 跟踪活动呼叫的对话状态：

| 指标名称 | 意义 |
| --- | --- |
| `dialog_ng_active` | 当前活动（已接听/确认）对话的数量 |
| `dialog_ng_early` | 早期对话的数量（响铃/临时状态） |
| `dialog_ng_expired` | 已过期或被强制终止的对话数量 |
| `dialog_ng_processed` | 自启动以来处理的对话总数 |

### 公共指标

S-CSCF 还导出以下公共指标。上面的 P-CSCF 部分记录了这些指标。

- **CDP (Diameter)** 指标 - Diameter 协议统计

- 核心 **SIP** 统计 - 按方法和状态码的请求/回复计数器（注意：S-CSCF 在端点之间路由。它通常具有更高的 fwd_requests 和 fwd_replies。）
- **DNS** 统计 - DNS 查询指标
- **MySQL** 数据库 - 数据库连接错误
- 防洪 - IP 阻止统计
- 共享内存 - 内存使用统计
- **SL**（无状态）模块 - 无状态回复计数器
- **TCP** 传输 - TCP 连接统计
- **TM/TMX**（事务）模块 - 事务状态跟踪（注意：S-CSCF 同时充当客户端和服务器。它通常同时具有 UAC 和 UAS 事务。）

# 多身份场景（共享号码和多MSISDN）

本指南解释了OmniCSCF如何处理IMS支持的两种“一位用户，多种身份”模型。它涵盖了注册、终止呼叫分叉、分叉拒绝行为和发起呼叫身份选择。它记录了每个网络元素所看到的内容。

这两种模型是独立的。用户可以使用其中一种、两种或都不使用。

- 共享公共用户身份（一个号码，多个设备）。一个号码由多个设备在不同的SIM卡上提供服务。手机和智能手表是常见的例子。每个设备都有自己的IMSI（私有身份，IMPI）。这些设备共享一个公共身份（IMPU，即号码）。
- 多**MSISDN**（一个设备，多个号码）。一个用户（一个IMSI）有多个号码。个人号码和业务号码在同一设备上是常见的例子。该设备将其所有号码注册为公共身份。

## 目录


1. 身份模型
2. 注册
3. 终止呼叫到共享号码
4. 分叉拒绝行为
5. 应用服务器所见
6. 终止呼叫到多MSISDN用户
7. 发起呼叫和呼叫线路身份
8. 参考


## 身份模型

3GPP TS 23.228定义了IMS身份模型。私有身份（IMPI）用于识别用于身份验证的订阅。公共身份（IMPU）是其他用户拨打的号码或SIP URI。一个订阅可以持有多个公共身份。多个私有身份可以共享一个公共身份。

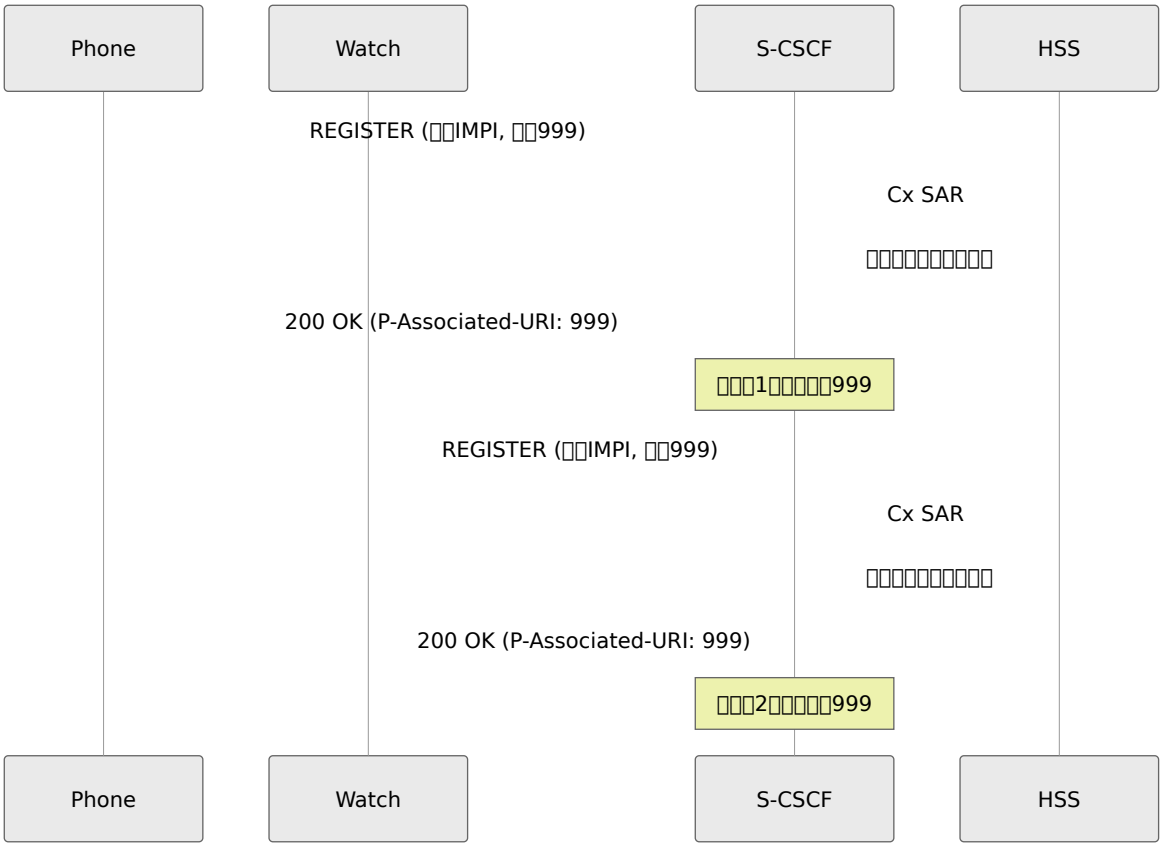
HSS持有该模型。S-CSCF在注册时通过用户数据下载它（Cx服务器分配，TS 29.228）。一起注册的公共身份集合是隐式注册集（TS 23.228）。

## 注册

每个设备使用其自己的私有身份进行身份验证。S-CSCF对每��REGISTER进行挑战，并根据Cx身份验证向量验证响应（请参见S-CSCF指南）。成功后，S-CSCF为每个设备存储一个联系绑定。

对REGISTER的200 OK携带一个**P-Associated-URI**头。该头列出了用户隐式注册集中每个公共身份。设备从该头中学习其号码。

- 共享号码。每个设备使用自己的私有身份在同一公共身份下注册。S-CSCF为每个设备保留一个联系。S-CSCF通过联系URI匹配联系人，因此设备不会相互覆盖。S-CSCF为每个公共身份最多保留`maxcontact`个联系人。将`maxcontact`设置为共享号码的设备的最大数量。
- 多**MSISDN**。设备使用其一个私有身份进行注册。200 OK P-Associated-URI列出用户的所有号码。对任何号码的终止呼叫都到达该设备。



Phone
Watch
S-CSCF
HSS
REGISTER (手机IMPI, 号码999)
Cx SAR
用户数据（共享身份）
200 OK (P-Associated-URI: 999)
联系人1存储于号码999
REGISTER (手表IMPI, 号码999)
Cx SAR
用户数据（共享身份）
200 OK (P-Associated-URI: 999)
联系人2存储于号码999
Phone
Watch
S-CSCF
HSS

## 终止呼叫到共享号码

对共享号码的呼叫必须响铃每个设备。S-CSCF进行分叉。当S-CSCF通过`lookup("location")`解析终止位置时，`append_branches`参数将每个注册的联系人作为并行分支附加。S-CSCF同时向所有设备发送INVITE（并行分叉，TS 24.229和RFC 3261第16节）。

第一个回答的设备获胜。S-CSCF将该设备的200 OK转发给呼叫者。S-CSCF向每个其他分支发送CANCEL。其他设备停止响铃。

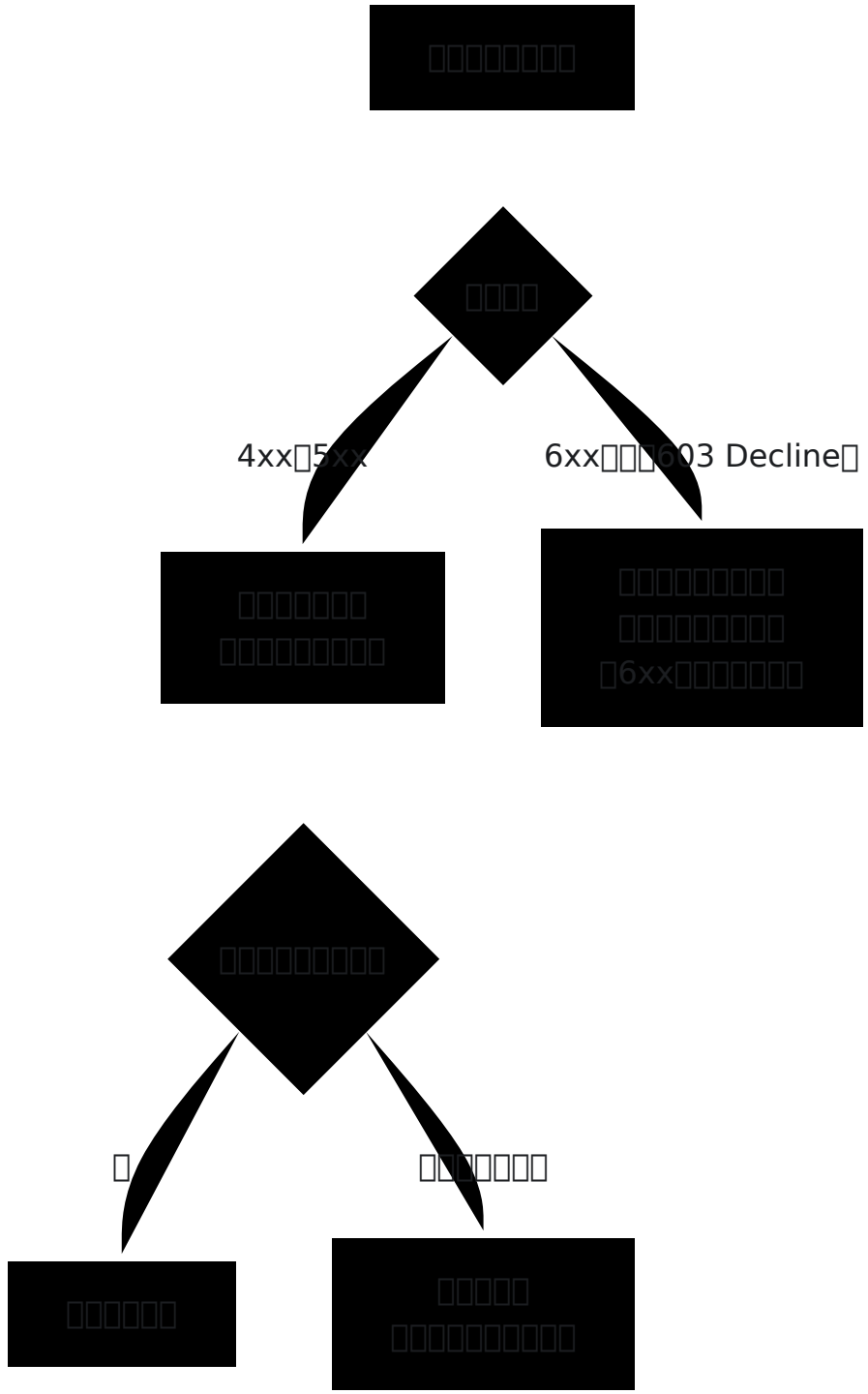
S-CSCF指南记录了`append_branches`和`maxcontact`参数。

## 分叉拒绝行为

设备可以拒绝分叉呼叫而不是接听。响应代码决定其他设备是否继续响铃。这遵循RFC 3261第16.7节中的并行分叉响应规则。S-CSCF事务层应用这些规则。

| 设备响应 | 意义 | 对其他设备的影响 | 呼叫者结果 |
| --- | --- | --- | --- |
| **200 OK** | 设备已接听 | S-CSCF向其他设备发送CANCEL。它们停止响铃。 | 呼叫连接到第一个接听的设备。 |
| **4xx**（例如 **486 Busy Here**, **480 Temporarily Unavailable**） | 该设备无法接听呼叫 | 其他设备继续响铃。该分支退出。 | 呼叫者在每个设备失败后才看到失败。然后S-CSCF转发最优先的最终响应。 |
| **5xx**（例如 **500 Server Internal Error**） | 该分支上的服务器错误 | 其他设备继续响铃。该分支退出。 | 同4xx：只有在每个分支失败后，失败才到达呼叫者。 |
| **6xx**（例如 **603 Decline**, **600 Busy Everywhere**） | 对整个身份的拒绝，而不仅仅是一个设备 | S-CSCF向其他设备发送CANCEL。它们停止响铃。 | 呼叫者收到6xx。 |
| 无响应（超时） | 设备无法访问 | 其他设备继续响铃。该分支超时（`fr_inv_timer`）。 | 同4xx：只有在每个分支失败后，失败才到达呼叫者。 |

关键区别在于6xx与4xx/5xx。4xx或5xx仅是一个分支的失败，因此分叉继续。6xx是对身份的全局拒绝，因此S-CSCF取消整个分叉。要在所有用户设备上同时拒绝呼叫，设备必须发送6xx。要在一个设备上拒绝而其他设备继续响铃，设备必须发送4xx。



## 应用服务器所见

MMTel应用服务器（TAS）位于分叉之前的终止路径中。S-CSCF通过终止初始过滤标准触发TAS。TAS应用其服务。然后TAS将会话返回给S-CSCF。S-CSCF解析联系人并进行分叉。

因此，TAS处理一个指向共享身份的终止会话。TAS看不到单个设备分支。分叉对它是透明的。TAS看到的是合并结果：

- 一个响铃指示，
- 然后是单个获胜的200 OK，或者
- 聚合的最终失败，或者
- 6xx拒绝。

TAS控制是否S-CSCF进行分叉。对于共享身份，TAS允许分叉，因此S-CSCF响铃每个设备。对于单设备身份，TAS设置 `Request-Disposition: no-fork`，因此S-CSCF将呼叫发送到一个��系人。TAS根据共享身份中的成员数量做出此决定，它通过Sh从HSS读取该信息。每个设备的响应处理保持在S-CSCF内部。

## 拒绝和语音信箱决策

一个常见的问题是TAS是否看到一个设备拒绝呼叫，而其他设备仍然响铃，以便TAS可以将呼叫者转发到语音信箱。它不会。 TAS只看到整个分叉的最终结果。分叉在S-CSCF内部，位于TAS的下游。

- 发送**486 Busy Here**的一个设备不会单独到达TAS。其他设备继续响铃。S-CSCF保持事务开放。TAS没有被通知。
- TAS仅在分叉解析时接收最终响应。当设备接听（200）、每个设备都失败，或设备发送6xx时，分叉解析完成。
- 当每个设备失败时，S-CSCF为整个分叉选择一个最终响应。它在分支中选择最优先的响应（RFC 3261第16.7节）。S-CSCF将该代码返回给TAS。TAS看不到单独的每个设备代码。
- 然后，TAS将其通信转发逻辑应用于该最终代码。TAS根据其配置的条件将呼叫者转发到语音信箱（例如，486时的忙碌通信转发，或超时时的无回复）。因此，语音信箱在整个分叉失败时到达，而不是当一个设备拒绝时。

**6xx**（例如603 Decline）是不同的。发送6xx的设备取消整个分叉。S-CSCF将6xx返回给TAS。TAS���其视为对身份的明确拒绝。TAS是否转发到语音信箱取决于为拒绝呼叫配置的通信转发规则。

简而言之：每个设备的“该设备拒绝，因此在其他设备继续响铃的同时将呼叫者发送到语音信箱”的行为在网络分叉中是不可能的。语音信箱是整个共享身份的属性。呼叫者仅在整个分叉失败时到达它。

实例：每个设备返回**480**

两个设备共享一个号码。一个呼叫分叉到两个设备。两个设备在几毫秒内都以480 Temporarily Unavailable拒绝。以下是在线路上发生的事情：

1. S-CSCF接收到两个480响应。每个响应携带其设备的头部（其自己的 `User-Agent`、其自己的 `To` 标签和设备添加的任何额外头部）。两个共享分叉的Call-ID和CSeq。
2. S-CSCF选择一个480响应并向上游转发。它转发该分支的实际响应（标准代理处理：它移除自己的 `Via` 并保留其余部分）。转发的480保留所选设备的 `User-Agent`、其 `Reason` 头（例如 `Reason: Q.850;cause=18`）和任何额外头部。这是一个真实的单设备响应，而不是合并的。

3. 所选响应不是“最后一个拒绝的设备”。S-CSCF根据其事务规则选择分支。当每个分支返回相同代码时，选择遵循分支顺序，而不是回复顺序��不要依赖转发的480（及其`User-Agent`）来自哪个设备。只有响应代码是可靠的。
4. 应用服务器看到那个480，应用通信转发以处理不可达的订阅者（480映射到CFNRc），并将呼叫者转发到语音信箱。呼叫者通过200 OK连接到语音信箱。

如果设备返回不同的拒绝代码，S-CSCF根据RFC 3261第16.7节选择最优先的一个，应用服务器根据该单一代码采取行动。

实例：一个设备拒绝，另一个设备接听

两个设备共享一个号码。一个呼叫分叉到两个设备。一个设备以480拒绝。另一个设备响铃然后接听。以下是在线路上发生的事情：

1. 第一个设备的480到达，甚至在第二个设备响铃之前。S-CSCF不会在此480上结束分叉。4xx仅结束该分支。S-CSCF继续等待第二个设备。
2. 第二个设备发送180响铃，然后发送200 OK。
3. 200 OK获胜。S-CSCF将200转发给呼叫者。呼叫者连接到接听的设备。
4. 之前的480被丢弃。它是一个失败的分支。呼叫者从未看到它，呼叫不会转到语音信箱。

这确认了核心规则：以4xx拒绝的设备不能阻止其他设备接听。只有6xx（或每个分支失败）才能阻止呼叫连接。

# 终止呼叫到多**MSISDN**用户

多MSISDN用户有一个设备和多���号码。对任何号码的呼叫都到达该设备。呼叫者拨打的号码保留在请求URI中，因此设备可以向用户显示拨打的号码（例如，将业务呼叫与个人呼叫分开）。

所有号码属于一个隐式注册集。因此，每个号码解析到相同的设备联系人。S-CSCF以与其他呼叫相同的方式解析终止位置。没有分叉，因为只有一个设备。

要配置多MSISDN用户，将每个号码作为公共身份添加到HSS中的一个IMS订阅中。然后对REGISTER的200 OK列出P-Associated-URI中的每个号码。请参见HSS多MSISDN文档。

## 向共享号码发送消息

IMS上的SMS使用SIP MESSAGE请求（TS 24.341）。对共享号码的消息到达每个设备，方式���呼叫分叉到每个设备相同。S-CSCF解析注册的联系人并将消息发送给每个联系人。共享号码上的每个设备都接收到该消息。

对多MSISDN号码的消息到达该设备，方式与对其任何号码的呼叫到达该设备相同。

## 发起呼叫和呼叫线路身份

用户在发起呼叫时呈现呼叫线路身份（CLI）。多MSISDN用户可以呈现任何自己的号码。例如，用户在业务呼叫中呈现业务号码，在个人呼叫中呈现个人号码。设备在P-Preferred-Identity头中选择号码（TS 24.229）。

P-CSCF断言身份。设备不这样做。P-CSCF在每个发起请求上应用以下规则：

1. P-CSCF移除设备发送的任何P-Asserted-Identity。设备不被信任以断言其自身身份。

2. 如果设备发送P-Preferred-Identity，P-CSCF将其与用户注册的身份进行检查。如果它是其中之一，P-CSCF将在P-Asserted-Identity头中断言它。
3. 如果设备未发送P-Preferred-Identity，或发送的身份未注册到用户，P-CSCF将断言用户的默认（主）公共身份。

远端用户最终看到的身份还取决于应用服务器策略。MMTel应用服务器可以覆盖断言的身份（例如，网络可以将每个呼叫标准化为用户的主号码，或应用呼叫线路识别限制）。要向远端呈现非主号码，应用服务器必须保留P-CSCF断言的身份。请参见应用服务器文档以获取CLI策略。

请参见P-CSCF指南以获取身份断言配置。

# 参考

## 分叉中的响应代码

| 代码 | 名称 | 类别 | 分叉效果 |
| --- | --- | --- | --- |
| 180 | 响铃 | 1xx | 进展。该分支仍然活跃。 |
| 200 | OK | 2xx | 接听。获胜分叉。取消其他分支。 |
| 486 | 此处忙 | 4xx | 该分支失败。其他设备继续响铃。 |
| 480 | 暂时不可用 | 4xx | 该分支失败。其他设备继续响铃。 |
| 408 | 请求超时 | 4xx | 该分支失败。其他设备继续响铃。 |
| 600 | 到处忙 | 6xx | 全局拒绝。取消整个分叉。 |
| 603 | 拒绝 | 6xx | 全局拒绝。取消整个分叉。 |

## 相关**S-CSCF**参数

| 参数 | 目的 |
| --- | --- |
| `ims_usrloc_scscf` `maxcontact` | 每个公共身份保留的最大联系人。将其设置为共`???`号码的设备的最大数量。 |
| `ims_registrar_scscf` `append_branches` | 设置为`1`时，终止`lookup("location")`并行分叉到每个注册的联系人。 |
| `tm` `fr_inv_timer` | INVITE分支超时。未响应的设备在此计时器到期时失败。 |

请参见S-CSCF指南以获取完整的参数参考。

## 3GPP和IETF参考

| 规范 | 相关性 |
| --- | --- |
| 3GPP TS 23.228 | IMS架构，公共和私有身份，隐式注册集 |
| 3GPP TS 24.229 | IMS SIP配置，发起和终止身份处理 |
| 3GPP TS 29.228 | Cx接口，用户数据，共享公共身份 |
| RFC 3261第16.7节 | 代理响应处理和并行分叉拒绝处理 |