Guía de Operaciones de Diameter

Tabla de Contenidos

1. Descripción General
2. Diameter en la Arquitectura IMS
3. Interfaces de Diameter
4. Gestión de Pares a través de OmniWeb
5. Códigos de Resultado de Diameter
6. Problemas Comunes

Descripción General

Diameter es el protocolo de autenticación, autorización y contabilidad (AAA) para la arquitectura IMS. OmniCSCF utiliza Diameter para comunicarse con elementos críticos de la red. Estos elementos incluyen el HSS, PCRF y OCS.

¿Qué es Diameter?

Diameter (RFC 6733) es el sucesor de RADIUS. Diameter admite escenarios AAA modernos:

- **Transporte confiable** a través de TCP/SCTP. RADIUS utiliza UDP.
- **Extensible** a través de módulos específicos de aplicación.
- **Arquitectura de par a par**. No es solo cliente-servidor.
- **Conexiones con estado** con monitoreo de watchdog.
- **Manejo de errores estandarizado** y códigos de resultado.

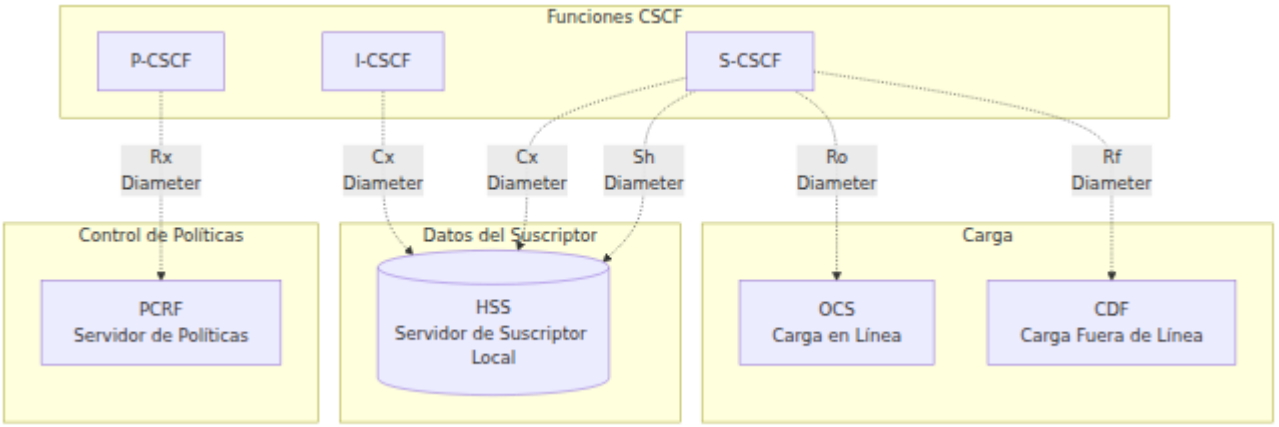
Diameter en CSCF

Cada componente CSCF utiliza interfaces de aplicación Diameter específicas:

CSCF	Interfaz	ID de Aplicación	Conectado a	Propósito
I-CSCF	Cx	16777216	HSS	Selección de S-CSCF, ubicación del usuario
S-CSCF	Cx	16777216	HSS	Autenticación del usuario, descarga de perfil
S-CSCF	Sh	16777217	HSS	Acceso a datos del usuario (opcional)
P-CSCF	Rx	16777236	PCRF	Control de política QoS y portadora
S-CSCF	Ro	4	OCS	Carga en línea (control de crédito)
S-CSCF	Rf	3	CDF	Carga fuera de línea (contabilidad)

Diameter en la Arquitectura IMS

Descripción General de la Red



Interfaces de Diameter

Interfaz Cx (CSCF ↔ HSS)

El I-CSCF y el S-CSCF utilizan la interfaz Cx para la autenticación de usuarios y la gestión de perfiles.

Especificación 3GPP: TS 29.228

Operaciones del I-CSCF

Solicitud de Autorización de Usuario (UAR) / Respuesta de Autorización de Usuario (UAA):

- **Propósito**: Consultar al HSS sobre la asignación o capacidades del S-CSCF.
- **Disparador**: El I-CSCF recibe un REGISTRO del usuario.
- **Caso de Uso**: El I-CSCF debe enrutar el registro al S-CSCF correcto.

Solicitud de Información de Ubicación (LIR) / Respuesta de Información de Ubicación (LIA):

- **Propósito**: Consultar al HSS sobre el S-CSCF actual del usuario.

- **Disparador**: El I-CSCF recibe una INVITACIÓN o MENSAJE para el usuario que termina.
- **Caso de Uso**: El I-CSCF debe enrutar la sesión al S-CSCF del usuario.

Operaciones del S-CSCF

Solicitud de Autenticación Multimedia (MAR) / Respuesta de Autenticación Multimedia (MAA):

- **Propósito**: Recuperar vectores de autenticación del HSS.
- **Disparador**: El REGISTRO inicial, antes del desafío.
- **Caso de Uso**: El S-CSCF debe desafiar al usuario para la autenticación IMS AKA.

Solicitud de Asignación de Servidor (SAR) / Respuesta de Asignación de Servidor (SAA):

- **Propósito**: Informar al HSS sobre el estado del registro y descargar el perfil del usuario.
- **Disparador**: Autenticación exitosa, después de MAR/MAA.
- **Caso de Uso**: El S-CSCF descarga el IFC y el perfil de servicio para el usuario.

El AVP `User-Data` en el SAA contiene el perfil completo del usuario. Este perfil incluye:

- Identidades públicas
- Criterios de Filtro Inicial (IFC) para el desencadenamiento de servicios
- Identificadores de perfiles de medios suscritos
- Información de carga

Solicitud de Terminación de Registro (RTR) / Respuesta de Terminación de Registro (RTA):

- **Propósito**: Desregistro iniciado por el HSS. El HSS envía la solicitud.
- **Disparador**: Desregistro administrativo o cambio de suscripción.
- **Caso de Uso**: El HSS instruye al S-CSCF para desregistrar a un usuario.

Interfaz Rx (P-CSCF ↔ PCRF)

La interfaz Rx proporciona control de políticas y QoS para sesiones IMS.

Especificación 3GPP: TS 29.214

Nota sobre VoNR (5G NR): Para sesiones VoNR, el PCF autoriza medios y QoS a través de la interfaz N5 AF (Npcf_PolicyAuthorization, HTTP/2 SBI). No utiliza Diameter Rx. Por lo tanto, la interfaz Rx aquí se aplica al acceso 4G/LTE.

Solicitud AA (AAR) / Respuesta AA (AAA):

- **Propósito**: Solicitar autorización de QoS para una sesión de medios.
- **Disparador**: El intercambio de oferta/respuesta SDP en una INVITACIÓN SIP.
- **Caso de Uso**: El P-CSCF solicita al PCRF que autorice los recursos de portadora.

Solicitud de Reautenticación (RAR) / Respuesta de Reautenticación (RAA):

- **Propósito**: Actualización de políticas iniciada por el PCRF. El PCRF envía la solicitud.
- **Disparador**: Un cambio de política o modificación de portadora.
- **Caso de Uso**: El PCRF instruye al P-CSCF para actualizar la política de QoS.

Solicitud de Terminación de Sesión (STR) / Respuesta de Terminación de Sesión (STA):

- **Propósito**: Liberar la sesión Rx y los recursos de portadora.
- **Disparador**: Terminación de la llamada. El P-CSCF recibe un BYE.
- **Caso de Uso**: El P-CSCF informa al PCRF para liberar los recursos de QoS.

Interfaz Ro (S-CSCF ↔ OCS)

La interfaz Ro proporciona carga en línea (control de crédito).

Especificación 3GPP: TS 32.299

Solicitud de Control de Crédito (CCR) / Respuesta de Control de Crédito (CCA):

- **Propósito**: Autorización y débito de crédito en tiempo real.
- **Disparador**: Configuración de llamada, durante la llamada o terminación de llamada.
- **Caso de Uso**: Carga prepaga y verificaciones de crédito en tiempo real.

Tipos:

- **CCR-Inicial**: Solicitar crédito al inicio de la llamada.
- **CCR-Actualizar**: Refrescar la cuota durante la llamada.
- **CCR-Terminar**: Informar el uso final al final de la llamada.

Gestión de Pares a través de OmniWeb

Vea el estado de los pares Diameter, aplicaciones soportadas y profundidades de cola en la pestaña **Diameter** de cada página CSCF en OmniWeb. OmniWeb es el portal de gestión unificado: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>.

La pestaña Diameter de OmniWeb muestra lo siguiente por CSCF:

- Identidad del dominio y del host de origen de Diameter.
- Pares configurados y su estado de conexión (I_Open, Closed, etc.).
- Aplicaciones Diameter soportadas por par, mapeadas a nombres de interfaz 3GPP (Cx/Dx, Sh/Dh, Rx, Ro, Gx, S6a/S6d, y otros).
- Longitud de la cola de trabajadores y transacciones pendientes.
- Operaciones de habilitar/deshabilitar para pares individuales.

Estados de los Pares

Estado	Descripción
I_Open	La conexión está abierta y operativa.
Closed	No se ha establecido conexión.
Wait-Conn-Ack	La conexión está iniciada. Está esperando una respuesta.
Wait-I-CEA	El CER ha sido enviado. Está esperando el CEA.

Códigos de Resultado de Diameter

La siguiente tabla enumera los códigos de resultado comunes y sus significados:

Código	Nombre	Significado	Ac
2xxx	**Éxito**		
2001	DIAMETER_SUCCESS	Operación exitosa	Ninguna
3xxx	**Errores de Protocolo**		
3002	DIAMETER_UNABLE_TO_DELIVER	No se puede enrutar al destino	Verificar conectiv par
3003	DIAMETER_REALM_NOT_SERVED	El dominio no es reconocido	Verificar configur dominio
3007	DIAMETER_APPLICATION_UNSUPPORTED	La aplicación no es soportada	Verificar Applicat
4xxx	**Fallos Transitorios**		
4001	DIAMETER_AUTHENTICATION_REJECTED	La autenticación falló	Verificar credenc
4010	DIAMETER_USER_UNKNOWN	El usuario no está provisionado	Verificar aprovisi del HSS
5xxx	**Fallos Permanentes**		
5001	DIAMETER_AVP_UNSUPPORTED	El AVP no es reconocido	Verificar versión protoco

Código	Nombre	Significado	Ac
5002	DIAMETER_UNKNOWN_SESSION_ID	La sesión no se encuentra	La sesió es inváli
5003	DIAMETER_AUTHORIZATION_REJECTED	No autorizado	Verificar permiso usuario
5012	DIAMETER_UNABLE_TO_COMPLY	No se puede procesar la solicitud	Verificar registro HSS/PCI

Problemas Comunes

Interfaces Críticas de Diameter

Cuando un par Diameter se cae, el impacto y la urgencia de recuperación dependen de la interfaz afectada:

Interfaz	Impacto si está Caída	Prioridad de Recuperación
Cx (HSS)	No hay nuevos registros. No hay actualizaciones de IFC.	Crítico. Recuperar inmediatamente.
Rx (PCRF)	No hay QoS para nuevas llamadas.	Alto. Recuperar en minutos.
Ro (OCS)	No hay carga prepaga. El servicio puede continuar.	Alto. Depende de la política.

Fallos de Conexión de Pares

Síntoma: El par está atascado en el estado "Closed" o "Wait-Conn-Ack".

Diagnóstico:

1. Verifique la conectividad de la red:

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

2. Verifique las reglas del firewall. El puerto 3868 TCP debe estar abierto.
3. Verifique la configuración del par (dirección IP, puerto).
4. Revise los registros del par para intentos de conexión.

Resolución:

- Solucionar los problemas de red y firewall.
- Verificar que el par esté en funcionamiento y escuchando en el puerto 3868.
- Comprobar que el par tenga la configuración correcta para el CSCF.
- Utilizar **Habilitar Par** en la pestaña Diameter de OmniWeb para reintentar la conexión.

Fallos en el Intercambio CER/CEA

Síntoma: El par está atascado en el estado "Wait-I-CEA", o el CEA tiene un código de error.

Errores Comunes:

- **5010 (NO_COMMON_APPLICATION)**: Verifique que ambos pares soporten la misma aplicación (por ejemplo, Cx = 16777216).
- **3003 (REALM_NOT_SERVED)**: Verifique que el Origin-Realm coincida con el dominio esperado del par.

Resolución:

- Verifique la configuración de Diameter para el Application-Id y el dominio.
- Asegúrese de que la configuración del par coincida con las expectativas del CSCF.
- Revise los registros del backend del CSCF para mensajes de error detallados.

Problemas de la Interfaz Cx del HSS

Síntoma: Fallos de registro y tiempos de espera de MAR/MAA.

Errores Comunes:

Código de Resultado	Significado	Resolución
4010	USER_UNKNOWN	El usuario no está provisionado en el HSS.
4001	AUTHENTICATION_REJECTED	El IMPI o las credenciales son incorrectas.
5012	UNABLE_TO_COMPLY	Error interno del HSS. Verifique los registros del HSS.

Resolución:

- **USER_UNKNOWN**: Provisionar el usuario en el HSS.
- **AUTHENTICATION_REJECTED**: Verificar el IMPI y el secreto compartido en el HSS.
- **UNABLE_TO_COMPLY**: Revisar los registros del HSS y la conectividad de la base de datos.

Problemas de la Interfaz Rx del PCRF

Síntoma: Las llamadas tienen éxito pero no se aplica QoS. Ocurren tiempos de espera de AAR/AAA.

Problemas Comunes:

- **PCRF caído**: Verifique el estado del par en la pestaña Diameter de OmniWeb.
- **Framed-IP-Address no reconocido**: El PCRF no puede mapear la IP del UE al suscriptor.
- **Política no aplicada**: Verifique las reglas de política del PCRF. Verifique la integración del PCEF.

Resolución:

- Verifique que el par PCRF esté en el estado "I_Open".
- Verifique el aprovisionamiento de la dirección IP del UE en el PCRF.
- Asegúrese de que la interfaz Gx (PCRF a PCEF) esté funcional.

Problemas de la Interfaz Ro del OCS

Síntoma: Las llamadas prepago fallan. Ocurren tiempos de espera de CCR/CCA. Las llamadas están bloqueadas.

Errores Comunes:

Código de Resultado	Significado	Resolución
4012	CREDIT_LIMIT_REACHED	Crédito insuficiente.
5003	AUTHORIZATION_REJECTED	El usuario no está autorizado para prepago.

Resolución:

- **CREDIT_LIMIT_REACHED**: Normal para usuarios prepago sin crédito.
- **Timeout del OCS**: Verifique la disponibilidad del OCS y el estado del par.
- **AUTHORIZATION_REJECTED**: Verifique que el usuario esté provisionado para prepago en el OCS.

Degradación del Rendimiento

Síntoma: Tiempos de respuesta de Diameter lentos y alta latencia.

Diagnóstico:

1. Verifique la marca de tiempo "Último Usado" en la lista de pares. Debe ser reciente.
2. Monitoree la "Longitud de Cola". Valores altos indican un retraso.
3. Revise los registros del backend del CSCF para advertencias de tiempo de espera.

Resolución:

- **Alta latencia**: Investigue la red entre el CSCF y el par.
- **Alta longitud de cola**: Verifique la carga del sistema del par (HSS/PCRF/OCS).
- **Tiempos de espera**: Si la red tiene alta latencia, aumente el tiempo de espera de transacción.

Mejores Prácticas

Directrices Operativas

Gestión de Pares:

- Monitoree el estado de los pares en la pestaña Diameter de OmniWeb.
- Configure monitoreo externo para eventos de caída de pares.
- Pruebe la conectividad de los pares durante las ventanas de mantenimiento.

Planificación de Capacidad:

- Estime la tasa de transacciones de Diameter a partir de los registros y el volumen de llamadas.
- Asegúrese de que el HSS/PCRF/OCS pueda manejar tasas de transacción pico.
- Para implementaciones grandes, considere agentes de enrutamiento Diameter (DRA).

Solución de Problemas:

- Verifique el estado del par primero cuando investigue fallos de registro o llamada.
- Correlacione fallos de Diameter con fallos de SIP (mismo Call-ID o usuario).
- Revise los registros del backend del CSCF para trazas de transacciones Diameter detalladas.

Seguridad:

- Utilice TLS para conexiones Diameter en producción, si TLS es soportado.
- Restringa el acceso de pares Diameter con el firewall. Permita solo pares conocidos.
- Revise regularmente los registros de auditoría de habilitación/deshabilitación de pares.

Limitaciones y Mejoras Futuras

Implementación Actual

La pestaña Diameter de OmniWeb proporciona:

- □ Visualización del estado de los pares en tiempo real.
- □ Operaciones de habilitar/deshabilitar pares.
- □ Mapeo de ID de aplicación a nombres de interfaz.

No Implementado

Las siguientes características **no están actualmente disponibles**. Las versiones futuras pueden agregarlas:

- **Inspector de Mensajes Diameter**: Ver transacciones Diameter recientes y detalles de AVP.
- **Estadísticas de Pares**: Conteos de mensajes, tasas de éxito y latencia promedio por par.
- **Monitoreo de Watchdog**: Estado DWR/DWA en tiempo real.

Soluciones Alternativas

Para Inspección de Mensajes: Revise los registros del backend del CSCF, o habilite el registro de depuración de Diameter.

Para Estadísticas Detalladas: Consulte las métricas desde el punto final de Prometheus. Consulte Referencia de Métricas para definiciones completas de métricas CDP/Diameter y configuración de monitoreo.

Para Reconexión Manual: Utilice la pestaña Diameter de OmniWeb para deshabilitar y luego volver a habilitar el par.

Documentación Relacionada

- **Guía de Operaciones del P-CSCF** - Operaciones de la interfaz Rx del P-CSCF.
- **Guía de Operaciones del I-CSCF** - Operaciones de la interfaz Cx del I-CSCF.
- **Guía de Operaciones del S-CSCF** - Interfaces Cx, Ro del S-CSCF.
- **Guía de Operaciones del SBI 5G** - Interfaces basadas en servicios N5/NRF utilizadas para VoNR (el equivalente 5G a Rx).
- **Referencia de Métricas** - Métricas y monitoreo de CDP/Diameter.
- **OmniWeb** - Gestión de pares Diameter a través de la pestaña Diameter de OmniWeb.
- **Guía de Operaciones del CSCF** - Operaciones generales del CSCF.

Especificaciones 3GPP

- **TS 29.228**: Interfaces Cx y Dx (CSCF-HSS).
- **TS 29.214**: Interfaz Rx (P-CSCF-PCRF).
- **TS 32.299**: Aplicaciones de carga Diameter (Ro, Rf).
- **RFC 6733**: Protocolo Base Diameter.

Detalles Técnicos

Implementación

- **Pila Diameter**: Pila de protocolo Diameter integrada.
- **Interfaz de Gestión**: Protocolo RPC al backend del CSCF.
- **Portal de Gestión**: OmniWeb (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>).

Configuración de Pares (Despliegue)

Cada nodo CSCF tiene un archivo de configuración de par Diameter: `pcscf.xml`, `icscf.xml` o `scscf.xml`. Ansible renderiza el archivo en el momento del despliegue. El archivo define la identidad Diameter del nodo y los pares HSS/PCRF/DRA a los que se conecta. La estructura es idéntica en los tres archivos. Solo la aplicación anunciada difiere.

Campo XML	Qué configura	Fuente de Ansi
`DiameterPeerFQDN`	El FQDN del host de origen Diameter de este nodo	`<inventory_hostname>.epc.mnc<mnc>.m`
`DiameterPeerRealm`	El dominio Diameter local	`ims_realm` si está definido, de lo contra `epc.mnc<mnc>.mcc<mcc>.3gppnetwork.o`
`Vendor_Id` / `Product_Name`	La identidad CER	`10415` (3GPP) / `OmniCSCF`
`Peer` (modo directo)	Par directo a cada host del grupo `hss` a través de SCTP:3868	renderizado por host en `groups['hss']` es falso
`Peer` (modo DRA)	Par a cada host del grupo `dra`. IP explícita cuando `diameter_dra_ip` está configurada.	renderizado por host en `groups['dra']` es verdadero
`Acceptor`	FQDN local y puerto para Diameter entrante (3868)	FQDN del nodo
`DefaultRoute`	Ruta predeterminada de enrutamiento al par HSS/PCRF (métrica 1) o al DRA (métrica 2)	renderizado desde `groups['hss']` / `gro`

Aplicación(es) anunciada(s) por nodo:

Nodo (archivo)	Aplicación(es)
P-CSCF (`pcscf.xml`)	**Rx** `16777236` (vendedores 10415, 0)
I-CSCF (`icscf.xml`)	**Cx** `16777216` (vendedores 10415, 13019, 0) + contabilidad base `4`
S-CSCF (`scscf.xml`)	**Cx** `16777216` (vendedores 10415, 13019, 0) + contabilidad base `4`

Las variables clave de Ansible son las siguientes. `plmn_id.mcc` y `plmn_id.mnc_longform` construyen todos los FQDN y dominios. `ims_realm` anula el dominio Diameter. `ims_dra_support` alterna entre emparejamiento directo y DRA. `diameter_dra_ip` establece la IP estática para el par DRA. Los grupos de inventario `hss` y `dra` proporcionan las listas de pares y rutas predeterminadas. Cuando se habilita la carga, `RO_DESTINATION` se dirige al par **Ro** (OCS) del S-CSCF por separado. El XML no aborda este par.

Edite estos archivos a través de las herramientas de despliegue, no a través de OmniWeb. OmniWeb proporciona monitoreo y control operativo (habilitar/deshabilitar) únicamente.

Operaciones y Referencia de I-CSCF

El Interrogating-CSCF es el punto de contacto de entrada de la red local para la señalización IMS. Un suscriptor llega a este nodo cuando se registra. Una sesión llega a este nodo cuando la sesión termina hacia un suscriptor local. El I-CSCF no mantiene estado de sesión. El I-CSCF no termina ningún medio. El I-CSCF consulta al HSS a través de Cx. Esta consulta decide qué Serving-CSCF maneja una solicitud dada. Al registrarse, el I-CSCF autoriza la identidad y la red visitada. Luego, el I-CSCF descubre el S-CSCF, o las capacidades del S-CSCF para seleccionar uno. En una solicitud de terminación, el I-CSCF localiza el S-CSCF que ya atiende al usuario. Después de que el I-CSCF elige un S-CSCF, el I-CSCF reenvía la solicitud a ese S-CSCF. El I-CSCF retransmite las respuestas de vuelta.

Funciones IMS

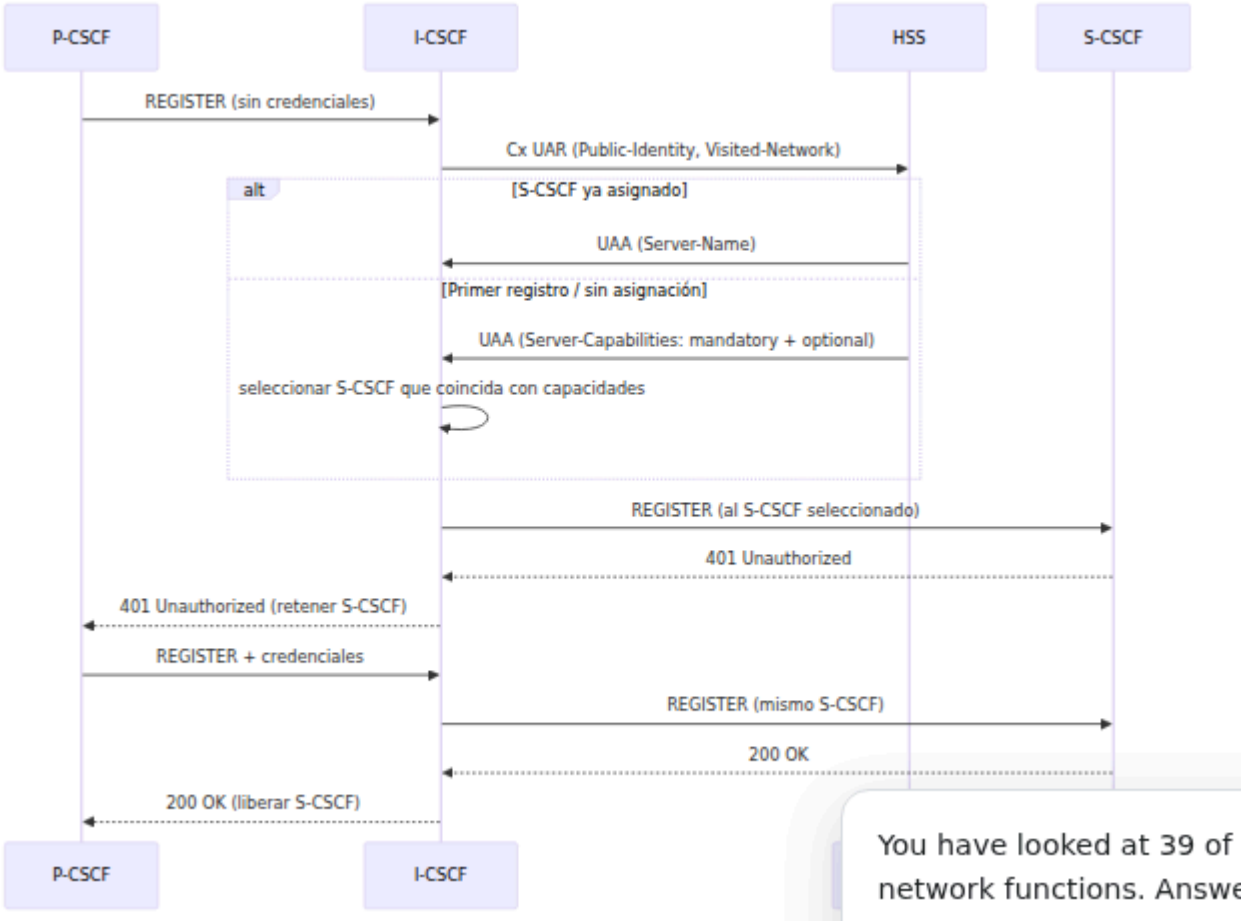
Enrutamiento de registro (Cx UAR)

Cuando llega un REGISTER, el I-CSCF consulta al HSS con un Cx **User-Authorization-Request (UAR)**. El I-CSCF envía esta consulta antes de reenviar el REGISTER. El UAR lleva la identidad pública y el identificador de la red visitada. Estos valores permiten que el HSS autorice al suscriptor a registrarse desde esa red. La respuesta (UAA) devuelve una de dos cosas:

- **Un nombre de S-CSCF ya asignado.** El I-CSCF utiliza este nombre directamente. Un re-registro regresa al mismo S-CSCF que mantiene la vinculación.
- **Capacidades de S-CSCF.** Estos son un conjunto de valores de capacidad obligatorios y opcionales que el S-CSCF seleccionado debe satisfacer. El HSS devuelve estos valores en el primer registro, o cuando no hay S-CSCF asignado actualmente. El I-CSCF luego realiza una selección basada en capacidades (a continuación).

El I-CSCF reenvía el REGISTER al S-CSCF elegido. El I-CSCF recuerda ese S-CSCF durante la duración del apretón de manos de registro. El re-REGISTER autenticado sigue el desafío 401. El I-CSCF enruta este re-REGISTER al **mismo** S-CSCF y no consulta nuevamente. El I-CSCF retiene el S-CSCF mientras un 401 está en vuelo. El I-CSCF descarta el S-CSCF cuando el registro se completa (2xx) o finalmente falla.

Un HSS que no está disponible o devuelve una respuesta malformada produce **503**. Un UAR puede autorizar pero no devolver ningún S-CSCF para seleccionar. En este caso, el I-CSCF vuelve a un URI de S-CSCF predeterminado configurado.



Enrutamiento de terminación (Cx LIR)

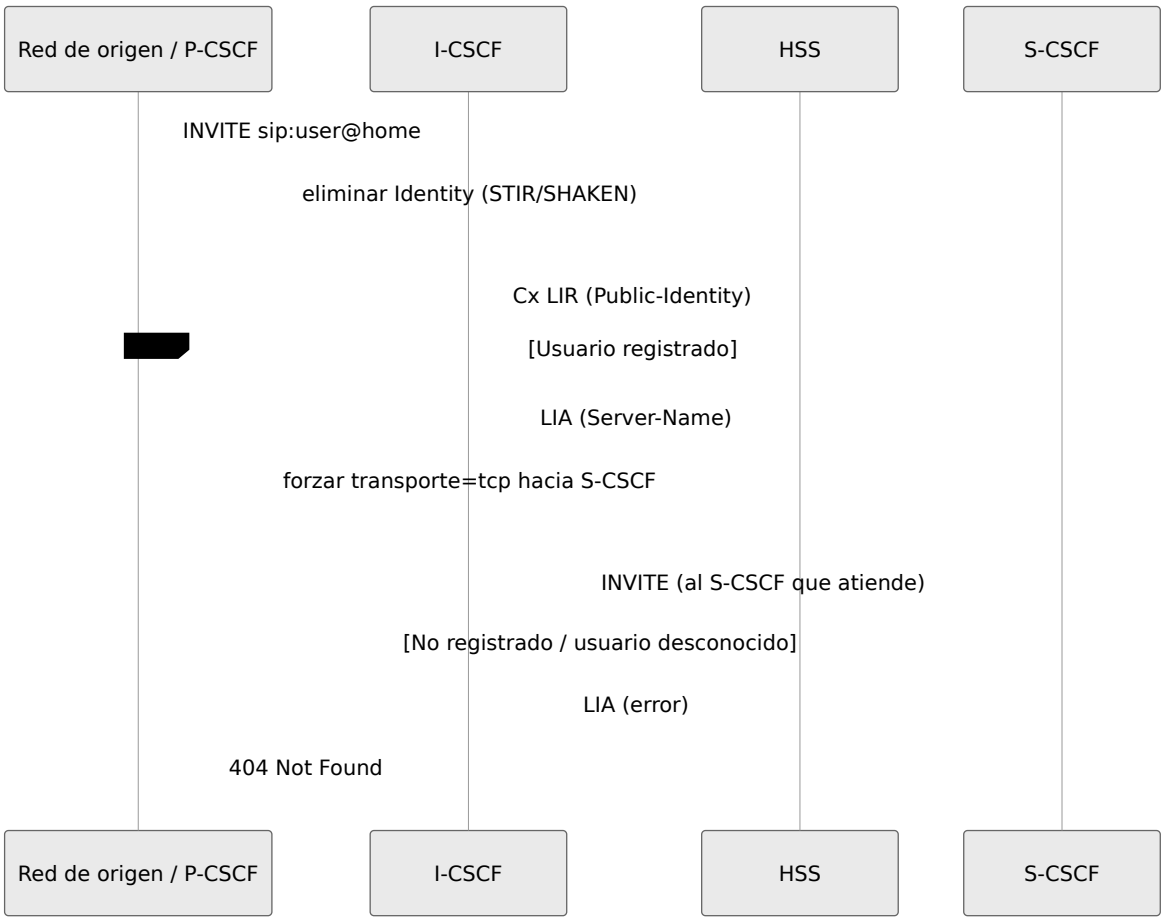
Una solicitud de terminación inicial es un INVITE, SUBSCRIBE, MESSAGE, INFO o PUBLISH. En tal solicitud, el I-CSCF consulta al HSS con un Cx **Location-Info-Request (LIR)** para la identidad del Request-URI. La respuesta (LIA) devuelve el nombre del S-CSCF que actualmente atiende al usuario. Para un usuario no registrado que tiene servicios provisionados, la LIA devuelve capacidades en su

lugar. El I-CSCF luego selecciona un S-CSCF de estas capacidades. El I-CSCF reenvía la solicitud a ese S-CSCF. Si el URI devuelto no especifica un transporte, el I-CSCF fuerza el transporte TCP hacia el S-CSCF. El I-CSCF elimina cualquier encabezado `Identity` STIR/SHAKEN entrante antes de reenviar la solicitud.

Manejo de resultados:

- **Éxito.** El I-CSCF selecciona el S-CSCF y retransmite la solicitud a él. Un fallo en la retransmisión devuelve **500**.
- **Usuario no encontrado / no registrado.** El I-CSCF devuelve **404 Not Found**.
- **HSS no disponible.** El I-CSCF devuelve **503**.

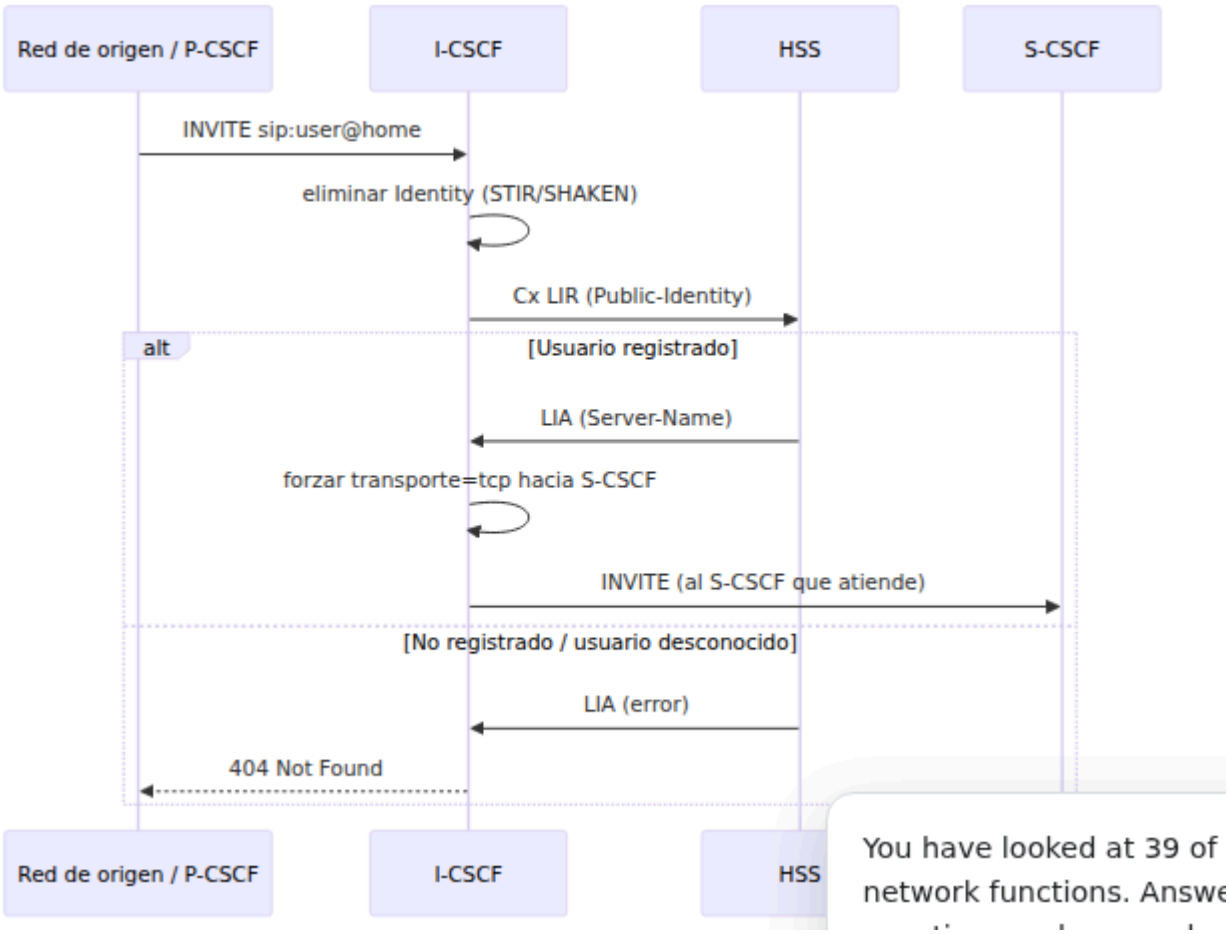
El I-CSCF no interroga CANCEL. El I-CSCF empareja CANCEL con su transacción existente y la retransmite. El I-CSCF rechaza cualquier otro método no inicial, no REGISTER con **406** y una lista `Allow`.



Selección de S-CSCF / coincidencia de capacidades

El HSS puede devolver capacidades en lugar de un nombre de S-CSCF asignado. En este caso, el I-CSCF selecciona un S-CSCF de su **conjunto de S-CSCF configurados**. Cada S-CSCF candidato tiene un URI SIP y un conjunto de valores de capacidad. La selección requiere que el S-CSCF satisfaga **todas las capacidades obligatorias**. Entre los candidatos que califican, el I-CSCF prefiere aquellos que coinciden con más de las **capacidades opcionales**. Varios candidatos pueden ser igualmente adecuados. Estos candidatos forman una lista de candidatos ordenada. Esta lista permite que el I-CSCF intente un alternativo en caso de fallo.

El I-CSCF mantiene la lista de candidatos en la memoria de transacción durante la vida de la solicitud. Esto preserva la posición de la lista a través de intentos. Un leg de REGISTER reenviado puede agotar el tiempo o recibir un 5xx/6xx. En este caso, el I-CSCF avanza al siguiente S-CSCF candidato y vuelve a intentar. Cuando la lista se agota, el I-CSCF se detiene. El I-CSCF retiene la lista a través de un desafío 401, porque el mismo S-CSCF debe manejar el reintento autenticado. El I-CSCF descarta la lista en una respuesta final de éxito o error del cliente. Si la selección no produce nada en absoluto, el I-CSCF vuelve al URI de S-CSCF predeterminado configurado.



Configuración de Despliegue (Inyectada por Ansible)

Ansible genera la configuración de tiempo de ejecución del I-CSCF (`icscf.cfg`) y su tabla de pares Diameter (`icscf.xml`) en el momento del despliegue. Los valores derivan de la identidad PLMN de la red (MCC/MNC) y el nombre de host del inventario del nodo. Los interruptores de características son banderas `#!define`. Una bandera definida habilita la característica. Una bandera comentada desactiva la característica.

Identidad / dominio

Nombre	Qué controla	Valor / de
`NETWORKNAME`	Dominio IMS local. Este es el dominio de destino Cx (`cxdx_dest_realm`). El I-CSCF verifica este dominio cuando enruta solicitudes de usuarios emparejados o desconocidos.	`ims.mnc<mnc>.mcc<mcc>.3gppnet`
`HOSTNAME`	FQDN (alias de host) de este nodo	`<inventory_hostname>.ims.mnc<`
`ICSCF_USER_AGENT`	El encabezado `User-Agent` que emite el nodo	`User-Agent: Omnitouch I-CSCF`
`ICSCF_SERVER`	El encabezado `Server` que emite el nodo	`Server: Omnitouch I-CSCF <inv`
`SCSCF_URI`	URI de S-CSCF predeterminado o de respaldo. El I-CSCF utiliza este URI cuando la selección basada en UAR no produce ningún S-CSCF.	`sip:scscf.ims.mnc<mnc>.mcc<mc`

Ansible plantilla los sockets de escucha SIP (UDP/TCP 5060, TLS 9090) desde la dirección del host de inventario y PLMN. Ansible también plantilla los alias de host (`ims.…`, `icscf.ims.…`, `<host>.ims.…`) a partir de estos valores.

`CAPTURE_NODE` es el objetivo de captura de Homer, `sip:<homer_host>:9060`. Ansible plantilla este valor solo cuando la captura de Homer está habilitada para el despliegue. La captura de Homer necesita `enable_homer` con un grupo de inventario `homer`. `CAPTURE_NODE` duplica la señalización SIP a Homer a través de HEP para rastreo.

Configuración de pares Diameter

La tabla de pares Diameter del I-CSCF (`icscf.xml`) publicita la aplicación **Cx** (`16777216`) hacia el HSS. Todos los CSCFs comparten la estructura del archivo y las variables de Ansible que lo llenan. Ver Diameter → Configuración de Pares (Despliegue).

Solución de Problemas

Los fallos de registro o los fallos de sesión de terminación se presentan en el I-CSCF. Estos fallos generalmente provienen de una de dos causas:

- **Selección / asignación de S-CSCF.** El HSS puede devolver capacidades en lugar de un nombre de S-CSCF asignado. La selección requiere que el S-CSCF satisfaga todas las capacidades obligatorias. Si ningún candidato califica, el I-CSCF vuelve al URI de S-CSCF predeterminado configurado. Si un REGISTER reenviado agota el tiempo o recibe un 5xx/6xx, el I-CSCF falla sobre el siguiente candidato hasta que la lista se agote. Confirme que el conjunto de S-CSCF configurado y sus valores de capacidad coincidan con lo que devuelve el HSS.
- **Conectividad Cx al HSS (UAR / LIR).** El I-CSCF no puede enrutar sin una respuesta al Cx UAR (en REGISTER) o LIR (en una solicitud de terminación). Una respuesta del HSS no disponible o malformada produce **503**. Un usuario que es desconocido o no registrado produce **404**. Verifique que el par Cx hacia el HSS esté activo. Ver Operaciones de Diameter.

Flujos de Llamadas

Los diagramas de secuencia aparecen con las funciones que documentan:

- Registro a través de I-CSCF → Enrutamiento de registro (Cx UAR)
- Sesión de terminación a través de I-CSCF → Enrutamiento de terminación (Cx LIR)
- Failover de S-CSCF → Selección de S-CSCF / coincidencia de capacidades

Documentación Relacionada

- Operaciones y Referencia de S-CSCF
- Operaciones
- Diameter
- Referencia de Métricas
- OmniWeb - lista de S-CSCF, sesiones activas y estado del par Diameter Cx: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Operaciones y Referencia de P-CSCF

El Proxy-CSCF es el punto de entrada SIP del IMS para el Equipo de Usuario. Cada REGISTER y cada sesión del UE llega aquí primero. El P-CSCF establece y hace cumplir la asociación de seguridad de acceso que protege la señalización del UE. El P-CSCF se inserta en la ruta de enrutamiento. Agrega un encabezado Path en el registro y un record-route en las sesiones. Todo el tráfico subsiguiente atraviesa este nodo. Este tráfico incluye solicitudes de terminación y mensajes en diálogo. El P-CSCF detecta la tecnología de acceso del UE para impulsar la política de portadora de medios. El P-CSCF también proporciona al punto de entrada de sesión de emergencia (E-CSCF) una identidad de línea de llamada utilizable según TS 23.167. El P-CSCF es solo un proxy de señalización. Los medios fluyen directamente entre el UE y el lado de terminación. Los medios nunca fluyen a través de este nodo.

Funciones del IMS

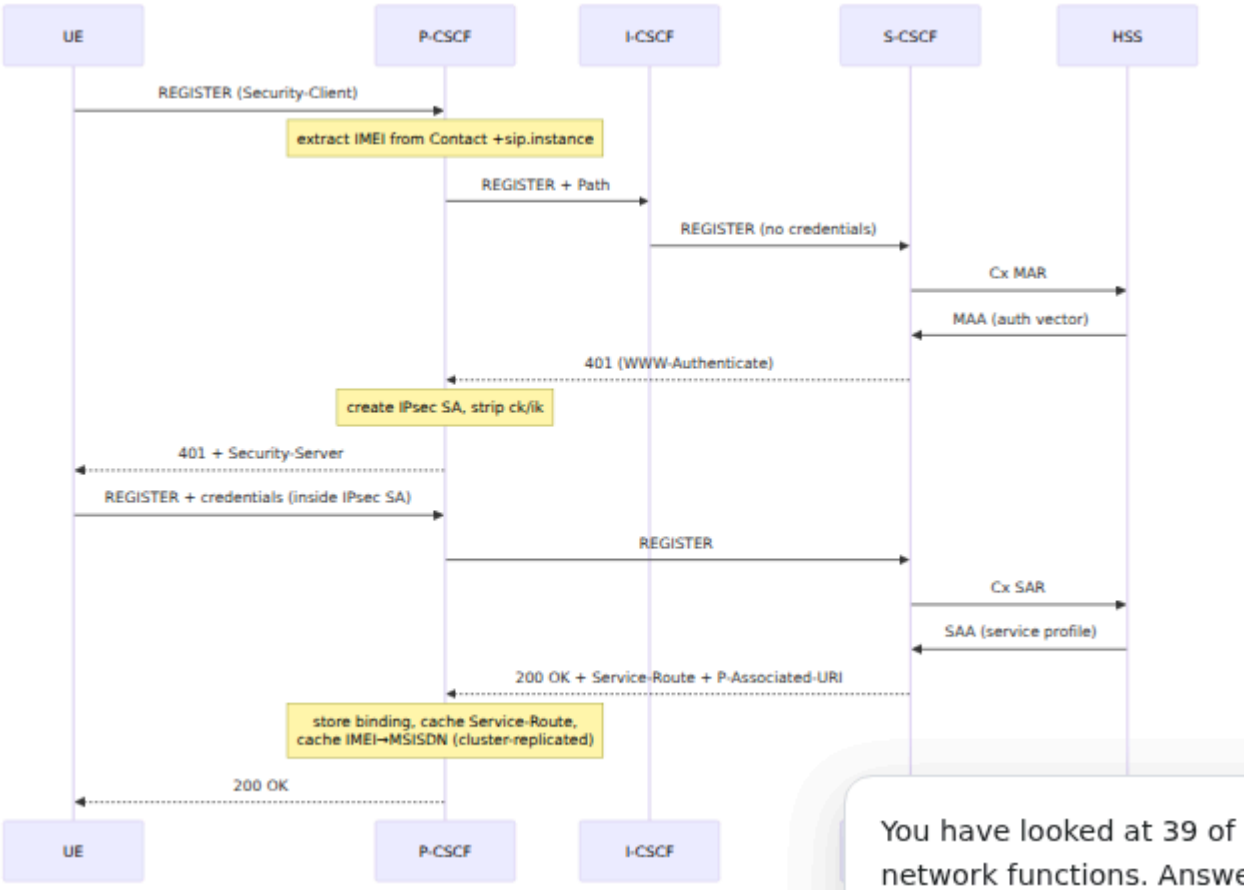
Proxy de registro y asociación de seguridad IPsec

El P-CSCF es el proxy que enfrenta al registrador del UE. El P-CSCF reenvía el REGISTER hacia la red de origen (I-CSCF/S-CSCF). En el intercambio de desafío/respuesta, el P-CSCF establece una asociación de seguridad IPsec ESP con el UE. Esto es parte del procedimiento IMS-AKA. Durante el registro, el UE y el P-CSCF negocian los parámetros de SA a través de los encabezados `Security-Client` / `Security-Server`. Desde el re-REGISTER autenticado en adelante, la SA transporta toda la señalización para ese UE.

En el REGISTER reenviado, el P-CSCF inserta un encabezado **Path**. Esto enruta las solicitudes de terminación de regreso a través de este mismo nodo. El P-CSCF fuerza la expiración del registro a un valor controlado por la red. El P-CSCF anuncia soporte para `path`. En el exitoso `200 OK`, el P-CSCF almacena el enlace de contacto. El P-CSCF almacena en caché el `Service-Route` y el `P-`

`Associated-URI` devueltos. Esto dirige las solicitudes subsiguientes a través de la ruta correcta de la red de origen.

Cada UE registrado utiliza **una** asociación de seguridad de un grupo de recursos por implementación. El P-CSCF libera la SA cuando el UE se desregistra (expiración 0) o su registro caduca. El P-CSCF rechaza un REGISTER cuyo Contacto marca un registro de emergencia (`;sos`). El P-CSCF maneja sesiones de emergencia directamente en el INVITE, no a través del registro de emergencia.



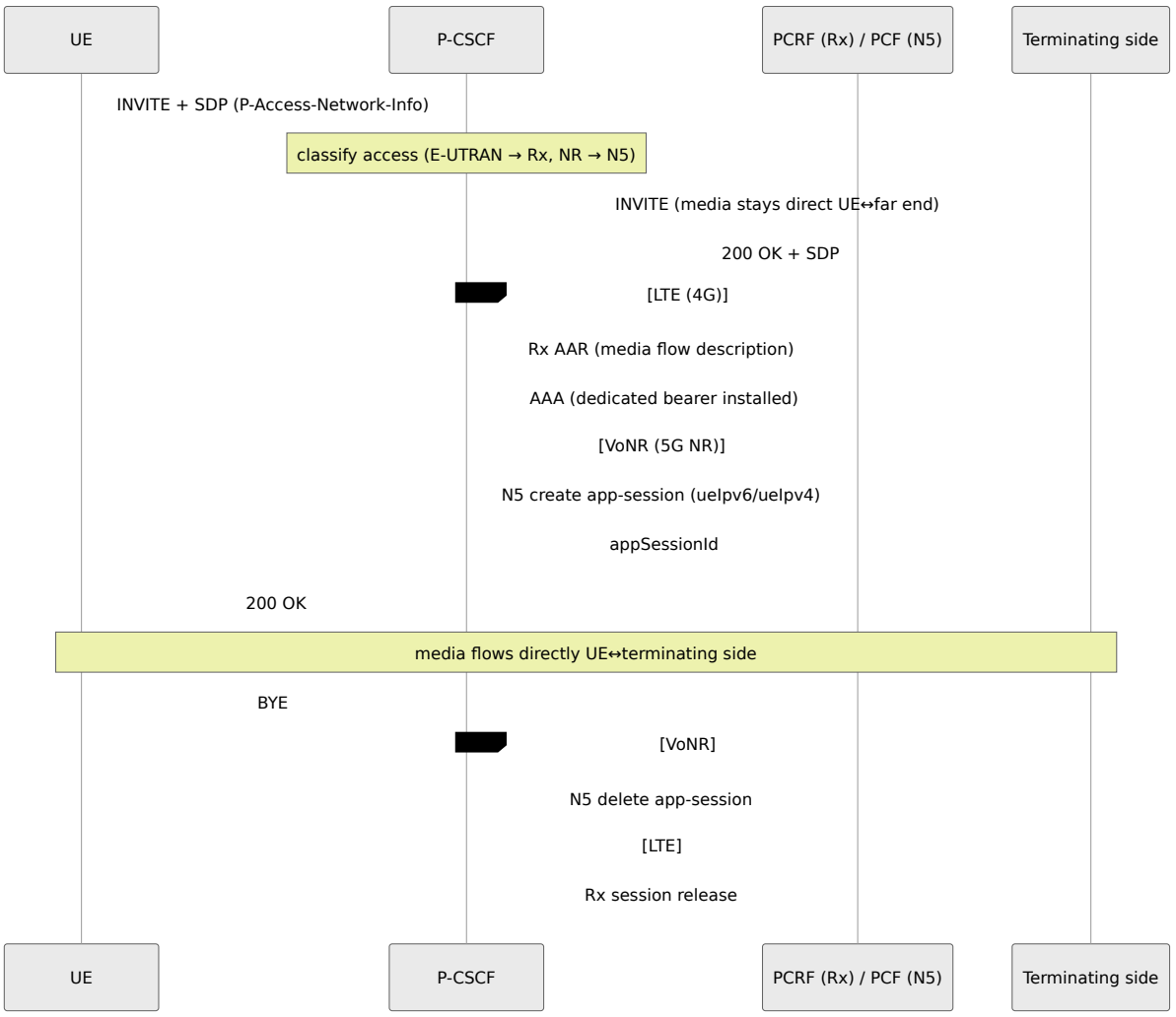
Detección de acceso y control de QoS / política

El P-CSCF nunca reenvía medios. Sin embargo, el P-CSCF autoriza la portadora de medios dedicada con el plano de políticas. El P-CSCF clasifica el acceso del UE a partir del encabezado `P-Access-Network-Info` (según TS 24.229 §5.2.6.3). LTE informa `3GPP-E-UTRAN`. 5G NR informa `3GPP-NR`. El acceso WiFi no tiene portadora dedicada. El P-CSCF excluye el acceso WiFi de QoS dinámica.

- **4G / LTE** - el P-CSCF autoriza la QoS de la portadora de medios a través de **Diameter Rx** hacia el PCRF. En la pierna de respuesta (el `200 OK` que lleva SDP), el P-CSCF emite una Solicitud de Autorización/Autenticación (AAR). La AAR describe el flujo de medios de audio y el flujo de medios de video donde esté presente. El PCRF luego instala la portadora dedicada correspondiente. El P-CSCF refresca la autorización en re-INVITEs en diálogo. El P-CSCF libera la autorización cuando el diálogo termina.
- **VoNR (5G NR)** - el P-CSCF autoriza la QoS de la portadora a través de la interfaz **N5** hacia el PCF. El P-CSCF utiliza el servicio `Npcf_PolicyAuthorization`. El P-CSCF actúa como una Función de Aplicación. Cuando el extremo lejano responde a los medios, el P-CSCF crea una sesión de aplicación en el PCF. Esta sesión utiliza afAppId `VoNR`, un componente de medios `AUDIO` con estado de flujo `ENABLED`, y un descriptor de flujo para los medios del UE. También incluye una URI de notificación AF para que el PCF llame de vuelta. El P-CSCF elimina esa sesión de aplicación cuando el diálogo termina.

La autorización de QoS se ejecuta tanto en las piernas de origen (MO) como de terminación (MT). Se basa en la dirección IP propia del UE. **Vinculación de dirección UE:** el P-CSCF codifica la dirección UE para que coincida con la vinculación de sesión PDU/portadora que tiene el nodo de políticas. El P-CSCF señala un UE IPv6 como `ueIpv6` y un UE IPv4 como `ueIpv4`. Una dirección v6 colocada en el campo v4 nunca coincide con la vinculación del PCF. El PCF entonces no instala ninguna portadora dedicada.

Para VoNR, el P-CSCF localiza el PCF de servicio a través del **descubrimiento NRF**. El P-CSCF se registra como un AF. Para cada sesión, el P-CSCF resuelve el PCF vinculado a la sesión PDU del UE a través de la cadena NRF→BSF. Este es el único camino de descubrimiento de PCF.



Llamadas de emergencia (E-CSCF) e identidad de línea de llamada - TS 23.167

El P-CSCF es el punto de entrada de emergencia. El P-CSCF detecta una sesión de emergencia por el URN del servicio de emergencia (`urn:service:sos`) en el INVITE. El P-CSCF lo enruta directamente al servidor de aplicaciones de emergencia. Esto elude la verificación normal del registro. Un INVITE de emergencia a menudo no lleva **MSISDN**. Por lo tanto, el P-CSCF proporciona una identidad de línea de llamada utilizable para el PSAP. Esto se aplica incluso a los llamantes que son desconocidos o anónimos. Esto cumple con el Anexo K de TS 23.167 y TS 29.214 §4.4.6a.

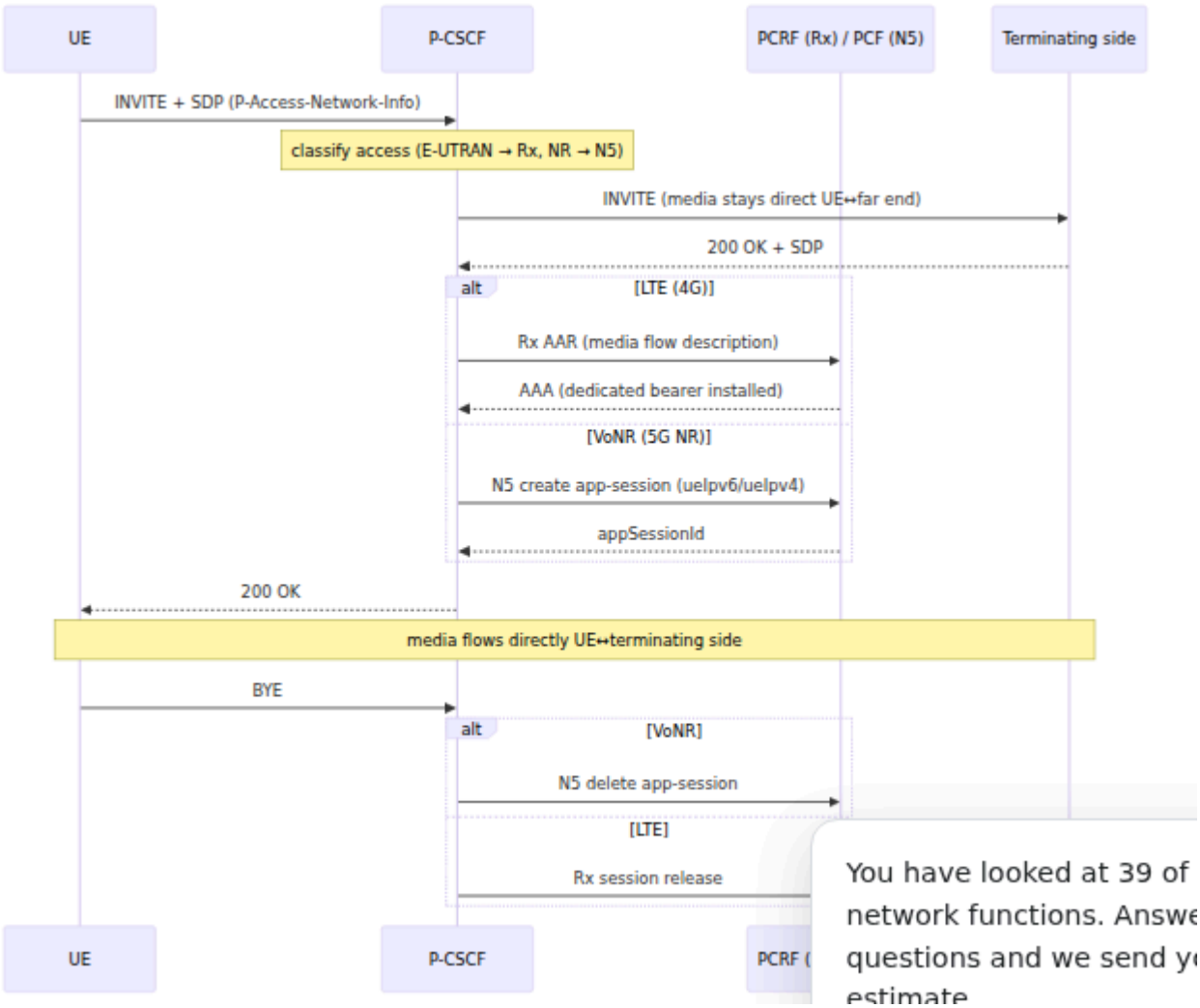
Dos mecanismos resuelven la identidad, en este orden:

1. **Consulta de suscripción asíncrona al PCRF (primaria).** El P-CSCF emite una consulta de suscripción asíncrona Rx al PCRF. La consulta se

basa en la dirección IP de origen del UE. El P-CSCF suspende el INVITE hasta que regrese la respuesta. El PCRF devuelve las identidades a nivel EPC de la sesión IP-CAN activa del UE. El P-CSCF elige una por precedencia **MSISDN → IMSI → IMEISV**. Esta identidad pertenece a la SIM en uso ahora, por lo que tiene prioridad.

2. **Vinculación IMEI→MSISDN en caché (fallback).** En cada REGISTER exitoso, el P-CSCF almacena en caché una vinculación. La vinculación mapea el IMEI del UE (del Contacto `+sip.instance`) al MSISDN (del `P-Associated-URI`). El P-CSCF **replica la vinculación en todos los nodos P-CSCF**. Cualquier nodo puede entonces resolver la identidad independientemente de dónde se registró el UE. El P-CSCF utiliza esta vinculación solo cuando el PCRF no devuelve ninguna identidad o la consulta Rx no puede ser enviada. La vinculación es por dispositivo, por lo que puede nombrar una SIM anterior utilizada en el mismo teléfono.

El P-CSCF afirma la identidad resuelta como el URI From del llamador y como un `P-Asserted-Identity` en el dominio `sos.apn`. El P-CSCF restaura la identidad de manera consistente en las respuestas y en las solicitudes en diálogo. El PSAP entonces ve una identidad de devolución de llamada utilizable incluso para un llamador originalmente anónimo. Cualquiera que sea el camino que resuelva la identidad, el INVITE de emergencia recibe el mismo tratamiento de medios/QoS y encabezados que cualquier otra solicitud de origen. El P-CSCF luego lo reenvía al servidor de aplicaciones de emergencia.



Seguridad / anti-inundación

El P-CSCF aplica protección contra inundaciones basada en la fuente. El P-CSCF limita la tasa de solicitudes por dirección IP de origen. El P-CSCF prohíbe una IP que excede el umbral de muestreo durante un período de espera. El P-CSCF rastrea la autenticación de registro fallida por dirección IP de origen en un contador de corta duración. El P-CSCF prohíbe una fuente que excede el umbral de intentos fallidos dentro de la ventana. Esto derrota los intentos de adivinanza de credenciales. El P-CSCF descarta solicitudes que un UE dirige al nodo mismo. El P-CSCF también descarta mensajes mal formados. Bajo presión de memoria, el nodo descarta nuevas solicitudes con `503`.

Replicación de clúster

El P-CSCF replica el estado relacionado con el registro y de emergencia entre nodos P-CSCF. En particular, el P-CSCF sincroniza la vinculación de emergencia

IMEI→MSISDN entre nodos. El P-CSCF realiza una sincronización completa al inicio. Cualquier nodo en el clúster puede entonces servir tráfico de terminación y resolver la identidad de llamada de emergencia. Esto funciona independientemente de qué nodo registró originalmente el UE. El P-CSCF no necesita aprovisionamiento por nodo.

Configuración de Implementación (Inyectada por Ansible)

Ansible genera la configuración de tiempo de ejecución del P-CSCF y su tabla de pares Diameter (`pcscf.xml`) en el momento de la implementación. La mayoría de los valores derivan de la identidad PLMN de la red (MCC/MNC) y el nombre de host del inventario del nodo. Ansible emite los bloques 5G SBI y PCF solo cuando el inventario de implementación contiene las funciones de red relevantes.

Identidad

Nombre	Qué controla	Valor / deri
`NETWORKNAME`	Dominio IMS de origen utilizado en `P-Visited-Network-ID` y reescrituras de identidad	`ims.mnc<mnc>.mcc<mcc>.3gppnetwo`
`HOSTNAME`	FQDN de este nodo (también su alias de host)	`<inventory_hostname>.ims.mnc<mn`
`URI`	La propia URI SIP del P-CSCF	`sip:<hostname>:5060`
`PCSCF_URL`	URI de origen utilizado para pings de keepalive NAT	`sip:<hostname>:5060`
`PCSCF_USER_AGENT`	Encabezado `User-Agent`	`User-Agent: Omnitouch Proxy-CSC`

Nombre	Qué controla	Valor / deri
	que emite el nodo	
`PCSCF_SERVER`	Encabezado `Server` que emite el nodo	`Server: Omnitouch Proxy-CSCF <i`
`DMQ_NOTIFICATION_ADDR`	Dirección de notificación del clúster para la replicación de estado entre nodos P-CSCF	`sip:pcscf.ims.mnc<mnc>.mcc<mcc>`

Ansible plantilla los sockets de escucha SIP (UDP/TCP 5060, más IPv6 5060 donde se define una dirección IPv6) y el socket HTTP de Prometheus (TCP 9090) desde la dirección del host del inventario. El P-CSCF atiende a los UEs en IPv6 donde está disponible. Los pares detrás de él permanecen en IPv4. Ansible también construye el `PATH_HEADER` y el `P_VISITED_NETWORK_ID_HEADER` a partir del nombre de host y PLMN.

Control de política / Rx (4G)

Nombre	Qué controla	Valor / derivaci
`RX_DEST_REALM`	Dominio de destino Diameter para Rx hacia el PCRF	`{{ diameter_realm }}`
`PCRF_REALM`	Dominio PCRF	`epc.mnc<mnc>.mcc<mcc>.3g`
`RX_AF_SIGNALING_IP`	IP de señalización AF transportada en el Rx AAR (este P-CSCF)	nodo `ansible_host` (sobres para doble-NAT)
`RX_IMS_REG_DIALOG_DIRECTION`	Modo de dirección de diálogo para el registro Rx	`3`

Los parámetros de medios Rx fijos incluyen autorización de video activada, un ancho de banda de audio predeterminado/mínimo de 64 kbit/s, inclusión de flujo RTCP y una duración máxima de sesión autorizada de 24 horas.

5G SBI / PCF (VoNR)

Emitido cuando el inventario de implementación contiene un PCF y un NRF. Sin un NRF, el P-CSCF no carga el módulo NRF en absoluto, y una sesión VoNR

avanza sin QoS dinámica.

Nombre	Qué controla	Valor / derivación
`VONR_AF_NOTIF_URI`	Punto final de notificación AF al que el PCF llama de vuelta	`http://<this host>:<pcscf_af_notif_port|9999`
`NRF_URI`	URI base NRF para el registro y descubrimiento de AF	`http://<nrf host>:<nrf_sbi_port|7777>`
`IMS_NRF_NF_IPV4`	Este P-CSCF's NF IPv4 para su registro AF	nodo `ansible_host`
`IMS_NRF_PLMN_MCC` / `IMS_NRF_PLMN_MNC`	PLMN anunciado en el registro/descubrimiento NRF	de `plmn_id`

Descubrimiento de PCF: el P-CSCF se registra con el NRF como un AF. Para cada sesión VoNR, el P-CSCF resuelve el PCF vinculado a esa sesión PDU del UE a través de la cadena NRF→BSF. Las sesiones de aplicación entonces siempre alcanzan el PCF correcto por suscriptor. Esto incluye núcleos 5G de múltiples PCF. Este es el único camino de descubrimiento admitido.

Dimensionamiento / transporte

Nombre	Qué controla	Valor
`CAPTURE_NODE`	Objetivo de captura SIP de Homer (plantillado solo cuando la captura de Homer está habilitada)	`sip:<homer host>:9060`

La configuración base ajusta el número de procesos de trabajo SIP (UDP) y el tamaño de la tabla hash del registrador para la escala de implementación. Los

UEs de iOS obtienen una duración de conexión TCP acortada para coincidir con su comportamiento de transporte.

Configuración de pares Diameter

La tabla de pares Diameter del P-CSCF (`pcscf.xml`) anuncia la aplicación **Rx** (`16777236`) hacia el PCRF. Todos los CSCFs comparten la estructura del archivo y las variables de Ansible que lo llenan. Ver Diameter → Configuración de Pares (Implementación). Rx solo está activo cuando se define `WITH_RX`.

Solución de Problemas

Registro / conectividad IPsec

Los usuarios que no pueden registrarse, o que tienen tiempos de espera de registro, a menudo apuntan a la seguridad de acceso del P-CSCF o la capa de descubrimiento en lugar de a la red de origen:

- **Establecimiento de SA IPsec** - los dispositivos móviles deben completar la negociación `Security-Client` / `Security-Server` de IMS-AKA. Si el re-REGISTER autenticado nunca llega dentro de la SA, verifique dos cosas. Confirme que el UE y el P-CSCF acordaron los parámetros de SA. Confirme que no hay un middlebox que elimine los encabezados de seguridad.
- **Travesía NAT** - para dispositivos detrás de NAT, verifique el manejo de NAT del extremo lejano. Verifique que los pings de opciones de keepalive lleguen al UE. El agujero para el tráfico de terminación entonces permanece abierto.
- **Descubrimiento de P-CSCF** - verifique que el UE descubra la dirección P-CSCF correcta (a través de DNS, DHCP o configuración estática). Verifique que los sockets de escucha SIP sean accesibles en la red de acceso.

Problemas de llamadas de emergencia

Síntomas: Llamadas de emergencia que no se enrutan al PSAP, o el PSAP no recibe ninguna identidad de línea de llamada (CLI) / número de devolución de llamada utilizable.

- **Detección de emergencia** - el P-CSCF enruta por el URN del servicio de emergencia (`urn:service:sos`), más los números de emergencia marcados. Confirme que el INVITE lleve la indicación de emergencia esperada. Confirme que el enrutamiento de emergencia eluda la verificación normal del registro.
- **Resolución de CLI para llamantes anónimos / desconocidos** - el P-CSCF primero envía una consulta de suscripción asíncrona Rx al PCRF. La consulta se basa en la dirección IP de origen del UE. El P-CSCF resuelve una identidad EPC por precedencia **MSISDN → IMSI → IMEISV** (Anexo K de TS 23.167). Si el PCRF no devuelve ninguna identidad, el P-CSCF recurre a la vinculación IMEI→MSISDN en caché (replicada en clúster, TTL de 4 horas). Si el PSAP ve un llamador anónimo, verifique que la consulta de suscripción Rx devolvió una identidad. De lo contrario, verifique que el P-CSCF haya almacenado en caché la vinculación en el registro. OmniWeb muestra el mapa de vinculación en caché.
- **Disponibilidad de ubicación** - verifique que la información de ubicación esté disponible para E911/E112. Verifique que la pierna de recuperación de ubicación (LRF) sea accesible.
- **Prueba de enrutamiento** - puede ejercitar el enrutamiento de llamadas de emergencia sin una conexión real al PSAP. Esto confirma la detección, la afirmación de identidad en el dominio `sos.apn` y el enrutamiento al servidor de aplicaciones de emergencia.

Las sesiones de emergencia tienen éxito incluso para usuarios no registrados, usuarios sin SIM o credenciales inválidas, y usuarios en roaming. Ver Llamadas de emergencia (E-CSCF) e identidad de línea de llamada - TS 23.167 para el mecanismo subyacente.

Flujos de Llamadas

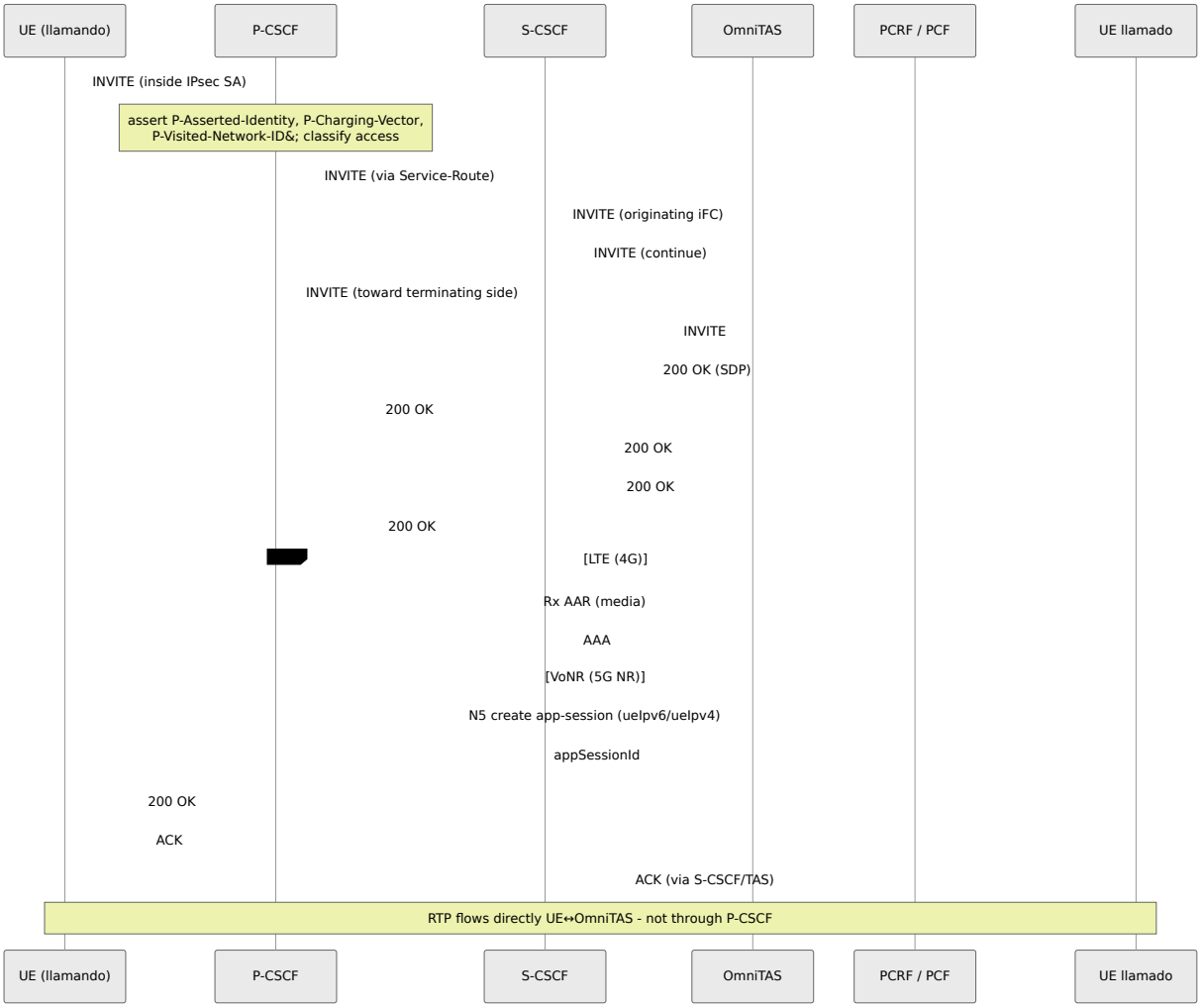
Los diagramas de secuencia aparecen con las funciones que documentan. Las escaleras de sesión completas aparecen a continuación:

- Registro y SA IPsec → Proxy de registro y asociación de seguridad IPsec
- QoS de medios / política (MO y MT) → Detección de acceso y control de QoS / política

- Sesión de emergencia → Llamadas de emergencia (E-CSCF) e identidad de línea de llamada - TS 23.167

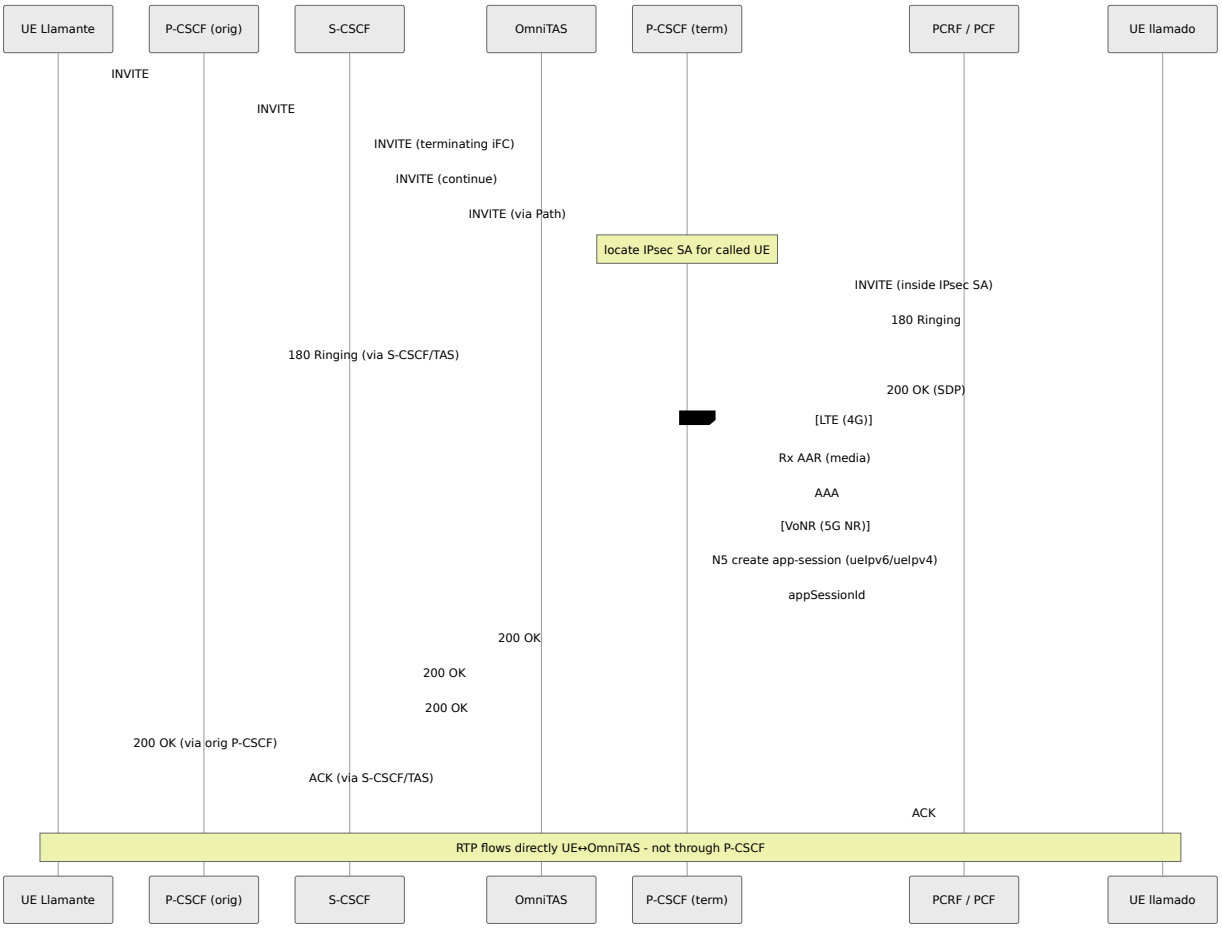
Llamada de origen móvil (MO)

El P-CSCF enruta las llamadas de origen a través del S-CSCF (a través del Service-Route en caché) al TAS para la lógica de servicio y el cobro. Los medios permanecen directos.



Llamada de terminación móvil (MT)

Las llamadas de terminación llegan de regreso a través del P-CSCF registrado en el Path en el registro. El P-CSCF autoriza QoS cuando el UE llamado responde.



Documentación Relacionada

- Operaciones
- Diameter
- Interfaz Basada en Servicios (SBI)
- Referencia de Métricas
- OmniWeb - contactos registrados, tablas hash (incluido el mapa de emergencia IMEI→MSISDN), descubrimiento NRF/PCF y estado de pares Rx: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Guía de Operaciones del SBI 5G

Tabla de Contenidos

1. Descripción General
2. SBI en la Arquitectura IMS
3. N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)
4. Nnrf - Gestión y Descubrimiento de NF (P-CSCF ↔ NRF)
5. Cuándo se Usa SBI vs Diameter
6. Configuración
7. Gestión a través de OmniWeb
8. Problemas Comunes
9. Documentación Relacionada

Descripción General

El núcleo 5G es **basado en servicios**. Las funciones de red exponen APIs REST JSON sobre HTTP/2 entre sí a través de la Interfaz Basada en Servicios (SBI). El SBI reemplaza a Diameter. Para VoNR (Voz sobre Nueva Radio), el P-CSCF actúa como una **Función de Aplicación (AF)** 5G. El P-CSCF utiliza SBI para autorizar la QoS de medios. El P-CSCF también utiliza SBI para descubrir las funciones de red que necesita.

El SBI reemplaza la ruta Diameter Rx utilizada para VoLTE. Consulte Operaciones de Diameter para el lado 4G/LTE.

¿Qué es SBI?

La Interfaz Basada en Servicios (3GPP TS 29.500) difiere de Diameter en estos aspectos:

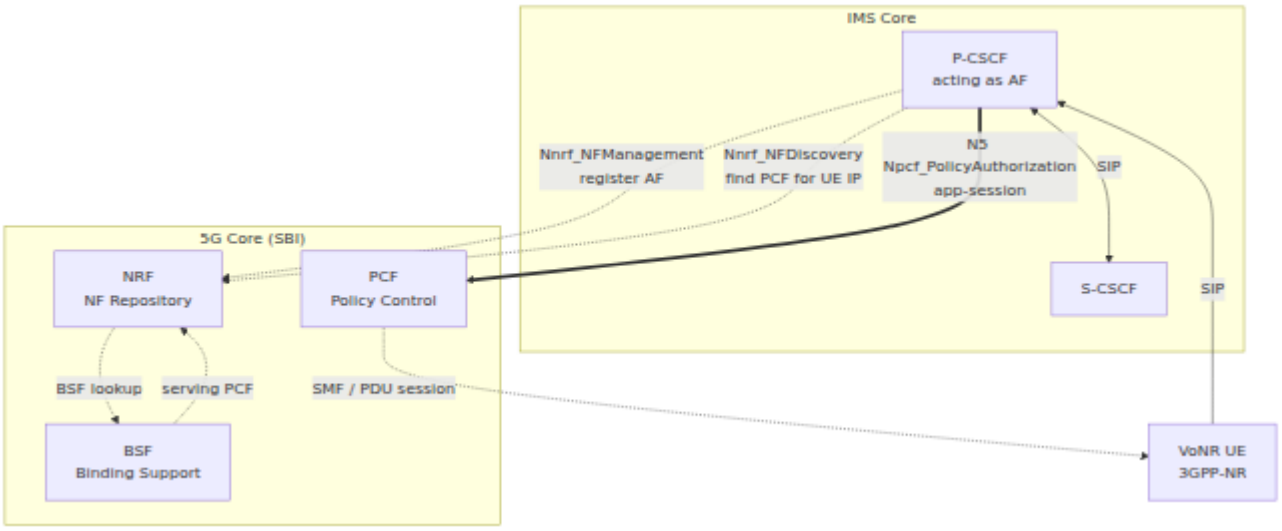
- **Transporte**: HTTP/2 sobre TCP. Diameter utiliza TCP o SCTP.
- **Codificación**: cargas útiles JSON descritas por OpenAPI. Diameter utiliza AVPs.
- **Modelo**: recursos RESTful. Se crea, modifica o elimina un recurso de *app-session*. Diameter utiliza pares de comandos de solicitud y respuesta.
- **Descubrimiento**: el **NRF** encuentra productores dinámicamente. Diameter utiliza pares configurados estáticamente.
- **Nomenclatura**: los servicios utilizan el nombre `Nxxx` (por ejemplo `Npcf_PolicyAuthorization`, `Nnrf_NFDiscovery`)

SBI en el CSCF

El P-CSCF es el único componente CSCF que utiliza SBI. Como una Función de Aplicación (AF) 5G, el P-CSCF autoriza la QoS de medios VoNR a través de N5 al PCF. Cuando se habilita el descubrimiento NRF, el P-CSCF se registra con el NRF y consulta al NRF.

Rol	Servicio	Transporte	Conectado a	Propósito
AF	Npcf_PolicyAuthorization (N5)	HTTP/2	PCF	Autorizar medios VoNR y QoS. Crear una app-session.
NF (AF)	Nnrf_NFManagement	HTTP/2	NRF	Registrar el P-CSCF como una instancia AF (opcional)
NF (AF)	Nnrf_NFDiscovery	HTTP/2	NRF → BSF	Descubrir el PCF vinculado a una sesión PDU de UE (opcional)

SBI en la Arquitectura IMS



Para VoNR, el P-CSCF detecta el acceso 5G. El P-CSCF descubre el PCF que sirve a través de la cadena NRF→BSF. Luego, el P-CSCF envía un POST de una app-session de autorización de política a ese PCF. Esta app-session reserva la QoS del portador de voz.

N5 - Npcf_PolicyAuthorization (P-CSCF → PCF)

El punto de referencia **N5** lleva el servicio `Npcf_PolicyAuthorization`. En una llamada VoNR, el P-CSCF crea un recurso de *app-session* en el PCF. La app-session describe los medios que la sesión necesita. El PCF luego instala la QoS correcta en la sesión PDU 5G del UE.

Solicitud de app-session

El P-CSCF envía un objeto `ascReqData` a la colección de app-sessions del PCF. La colección predeterminada es `http://<pcf>/npcf-policyauthorization/v1/app-sessions`. El objeto contiene estos campos:

Campo	Valor	Notas
`notifUri`	URI de notificación AF	La dirección donde el PCF envía notificaciones de eventos de app-session. Este es el endpoint de notificación AF configurado.
`suppFeat`	`3f`	Mapa de características soportadas
`ueIpv4` / `ueIpv6`	IP de origen del UE	**Debe coincidir con la familia de direcciones** que el PCF vinculó a la sesión PDU del SMF
`afAppId`	`VoNR`	Identificador de aplicación
`medComponents`	componente de medios de audio	`mediaType: AUDIO`, `fStatus: ENABLED`, con una descripción de flujo (`permit out 17 from <ue-ip> to any`)

> **Problema operativo - familia de direcciones.** El PCF vincula la app-session a la sesión PDU del SMF por la dirección IP del UE. Debe codificar un UE en una sesión PDU IPv6 como `ueIpv6`. Una dirección v6 en `ueIpv4` nunca coincide. Una dirección v4 en `ueIpv6` nunca coincide. En estos casos, el PCF rechaza la autorización o descarta la autorización silenciosamente. El P-CSCF selecciona `ueIpv6` o `ueIpv4` de la dirección de origen SIP automáticamente.

Ciclo de Vida

- **Crear** - el P-CSCF envía un POST de la app-session cuando procesa la INVITE VoNR o medios tempranos.
- **Notificar** - el PCF llama de vuelta a `notifUri` para eventos de sesión.
- **Eliminar** - el P-CSCF desmantela la app-session cuando el diálogo termina. Esto libera la QoS reservada.

Diameter Rx utiliza `Rx_AAR` y `Rx_STR`. N5 no tiene conexión de pares persistente. Cada app-session es una transacción HTTP/2 independiente al PCF descubierto para ese UE.

Nnrf - Gestión y Descubrimiento de NF (P-CSCF ↔ NRF)

El P-CSCF utiliza el descubrimiento NRF para encontrar el PCF para cada sesión VoNR. El descubrimiento NRF es la única ruta de descubrimiento del PCF.

Registro de NF (Nnrf_NFManagement)

El P-CSCF se registra como una instancia AF con el NRF. El P-CSCF utiliza una identidad de instancia estable por host. Un reinicio reutiliza un registro. Esto evita que el NRF acumule registros AF obsoletos.

Descubrimiento del PCF (Nnrf_NFDiscovery)

Para una sesión VoNR, el P-CSCF consulta al NRF con la IP de origen del UE. Esta consulta descubre el PCF que sirve a esa sesión PDU del UE. La cadena **NRF → BSF** resuelve la consulta. El BSF mantiene la vinculación UE-IP a PCF que sirve. El endpoint descubierto se convierte en el objetivo N5. Si el P-CSCF no encuentra ninguna vinculación, omite la QoS dinámica para esa llamada. La sesión luego continúa sin una reserva de portador dedicada.

Cuándo se Usa SBI vs Diameter

El P-CSCF deriva el tipo de acceso del encabezado `P-Access-Network-Info` (según TS 24.229 §5.2.6.3). LTE informa `3GPP-E-UTRAN`. 5G NR informa `3GPP-NR`. El P-CSCF excluye WiFi (`3GPP-IEEE-802.11`) porque WiFi no tiene portadores dedicados.

Acceso	`P-Access-Network-Info`	Ruta QoS	Par
5G NR (VoNR)	`3GPP-NR`	**N5 SBI** (`Npcf_PolicyAuthorization`)	PCF
LTE (VoLTE)	`3GPP-E-UTRAN`	**Diameter Rx**	PCRF
WiFi	`3GPP-IEEE-802.11`	ninguno (sin portador dedicado)	-

El P-CSCF descubre el PCF para la ruta N5 por sesión. Utiliza la cadena NRF → BSF → PCF que sirve.

Configuración

Las herramientas de implementación provisionan el comportamiento del SBI por implementación. No edite el comportamiento del SBI manualmente. Los ajustes relevantes son:

Ajuste	Propósito
Endpoint de notificación AF	La URL de callback que el P-CSCF anuncia al PCF para notificaciones de eventos de app-session
Endpoint del NRF	La dirección del NRF para el registro de AF y descubrimiento del PCF
Identidad del PLMN local (MCC / MNC)	La identidad de la red local que el P-CSCF presenta al NRF
Identidad de instancia AF	Una identidad estable por host para el registro en el NRF. Un reinicio reutiliza un único registro.

OmniWeb muestra el estado de registro NRF en vivo. OmniWeb también muestra las vinculaciones del PCF descubiertas por sesión. Vea a continuación.

Gestión a través de OmniWeb

Omnitouch eliminó el panel de control web integrado. La pestaña **NRF** de la página OmniWeb P-CSCF muestra el estado de registro NRF, las vinculaciones del PCF descubiertas y el estado 5G/N5. Consulte la documentación de OmniWeb.

Problemas Comunes

Síntoma	Causa probable	Acción
No se encontró vinculación PCF para el UE (registrado al configurar la llamada)	El NRF o BSF no tiene vinculación para la sesión PDU del UE aún. O la IP del UE difiere del ancla de sesión.	Confirme que la sesión PDU del UE esté establecida. Confirme que el BSF tenga la vinculación. La llamada continúa sin QoS dinámica.
El PCF rechaza o ignora la app-session	La IP del UE está codificada en la familia incorrecta (`ueIpv4` vs `ueIpv6`)	Verifique que la familia de dirección de origen SIP coincida con la sesión PDU. Consulte el problema de familia de direcciones anterior.
Se acumulan registros AF obsoletos en el NRF	La identidad de instancia AF no es estable entre reinicios	Haga que la identidad de instancia AF por host sea estable
No hay tráfico N5 en absoluto para una llamada 5G	El P-CSCF no detecta el acceso como `3GPP-NR`. O el NRF no es accesible, por lo que el P-CSCF no descubre ningún PCF.	Verifique `P-Access-Network-Info`. Verifique que el endpoint del NRF sea accesible.
La llamada VoNR se establece pero no hay portador dedicado	El P-CSCF no creó la app-session porque el descubrimiento falló. O el P-CSCF desmanteló la app-session prematuramente.	Correlacione el POST N5 del P-CSCF con el PCF. Verifique la conectividad HTTP/2 y los tiempos de espera.

Documentación Relacionada

- Operaciones de Diameter - las interfaces Diameter Rx, Cx y Ro utilizadas para VoLTE (4G/LTE)
- Operaciones del P-CSCF - Detección de acceso VoNR, QoS N5 y descubrimiento NRF en contexto
- Referencia de Métricas - métricas del P-CSCF
- Documentación de OmniWeb - estado del NRF y 5G en el portal de gestión

Operaciones y Referencia del S-CSCF

El Serving-CSCF es el registrador SIP de la red local y el punto de control de sesión del IMS. Autentica a los suscriptores contra el HSS a través de Cx (MAR/SAR). Almacena el enlace de registro. Descarga el perfil de servicio del suscriptor (Criterios de Filtro Inicial). Se sitúa en la ruta de señalización para cada sesión de origen y terminación. Desde esta posición, activa los Servidores de Aplicaciones a través de la interfaz ISC, afirma la identidad del llamante y enruta la sesión hacia el lado de terminación, un Servidor de Aplicaciones o la PSTN. El HSS registra el nombre de este S-CSCF para el suscriptor. Por lo tanto, todo el tráfico subsiguiente para ese usuario atraviesa este nodo.

Funciones del IMS

Registro y autenticación

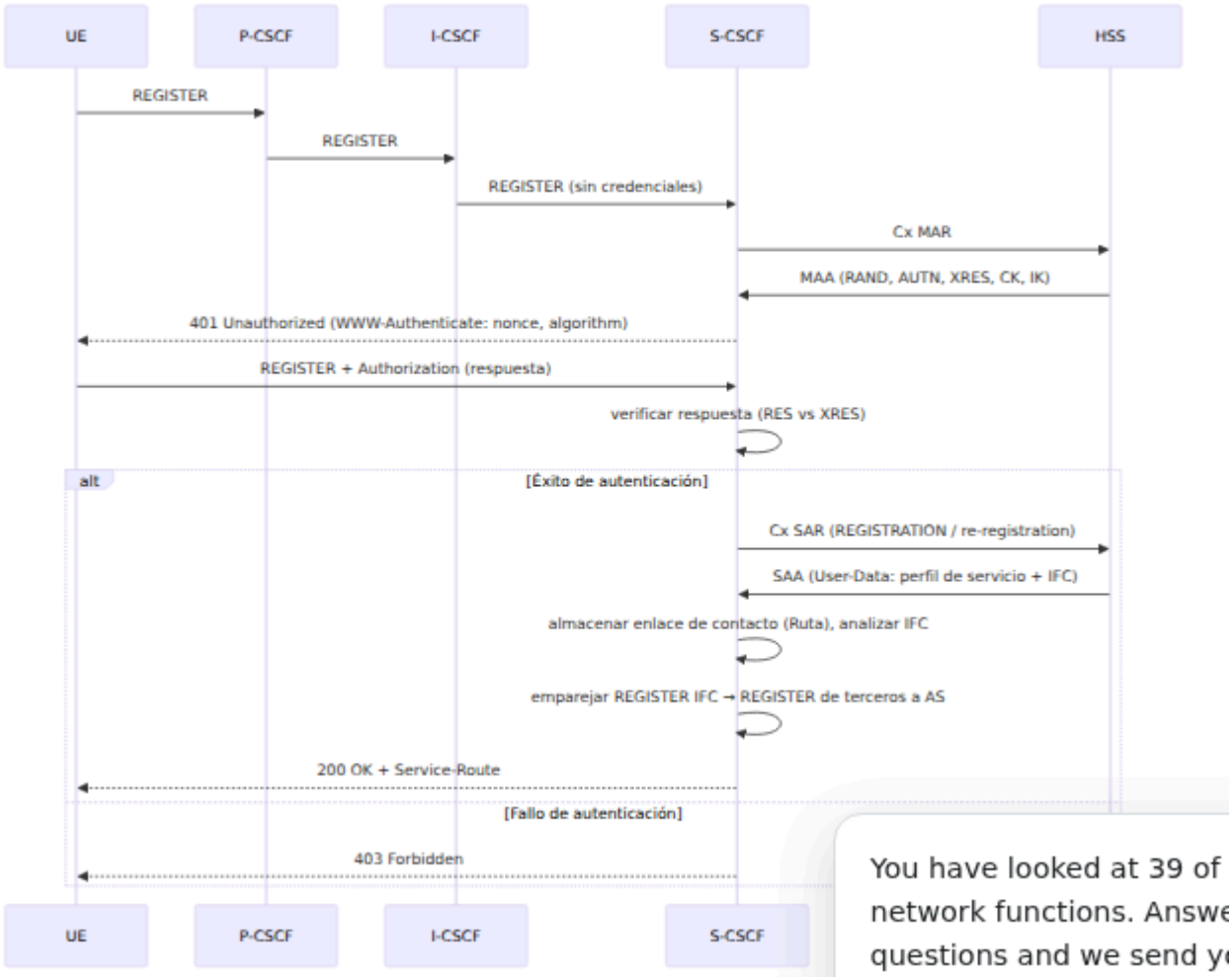
El S-CSCF es el registrador autoritativo. Desafía al UE. Valida la respuesta contra un vector de autenticación Cx del HSS. Con éxito, registra el enlace de contacto y descarga el perfil de servicio del suscriptor.

El registro se lleva a cabo de la siguiente manera:

1. **Selección de algoritmo.** El S-CSCF desafía con el algoritmo que el UE ofrece en su encabezado de Autorización. Si el UE no ofrece ningún algoritmo, el S-CSCF predetermina a SIP Digest (MD5). SIP Digest acomoda a los softphones no IMS. Por defecto, el S-CSCF autentica cada REGISTER.
2. **Desafío (MAR).** El S-CSCF recibe un REGISTER sin credenciales. Solicita un vector de autenticación al HSS con un Cx Multimedia-Auth-Request. El HSS devuelve el vector en la respuesta (para AKA: RAND, AUTN, XRES, CK, IK). El S-CSCF responde **401 Unauthorized** con un encabezado `WWW-Authenticate`. Este encabezado lleva el nonce (derivado de RAND) y el algoritmo seleccionado. Si el HSS rechaza la identidad, el registro falla **403**.

Si el HSS no está disponible o devuelve una respuesta malformada, el registro falla **503**.

3. **Verificación.** El UE reenvía REGISTER con su respuesta calculada. El S-CSCF verifica la respuesta contra el vector almacenado. Coincide con la identidad pública.
4. **Re-sincronización.** Si el UE informa un desajuste de número de secuencia (SQN), el S-CSCF reenvía el token AUTS al HSS para re-sincronizar. Luego, el S-CSCF vuelve a desafiar con nuevos vectores.
5. **Asignación de servidor (SAR).** Después de una autenticación exitosa, el S-CSCF envía un Cx Server-Assignment-Request. El tipo de asignación es REGISTRATION en el primer registro, o re-registro en una actualización. La respuesta devuelve los User-Data del suscriptor (perfil de servicio e IFC). El S-CSCF mantiene los User-Data en memoria. Una asignación rechazada, o un suscriptor sin perfil de servicio IMS, falla **403**. Un tiempo de espera del HSS falla **503**.
6. **Vinculación y Service-Route.** El S-CSCF almacena el enlace de contacto junto con la Ruta P-CSCF. La Ruta permite que las solicitudes de terminación se enruten de regreso a través del mismo P-CSCF. El 200 OK lleva un Service-Route, por lo que el UE envía solicitudes subsiguientes a través de este S-CSCF. El S-CSCF mantiene hasta `maxcontact` contactos por identidad pública (ver los parámetros usrloc en la configuración del S-CSCF). Un número compartido por varios dispositivos en SIMs separadas (por ejemplo, un teléfono y un reloj inteligente) mantiene un contacto por dispositivo: cada dispositivo se registra con su propia identidad privada (IMPI, derivada de su IMSI) bajo la identidad pública compartida, y los contactos se emparejan por URI de contacto. Una llamada de terminación puede bifurcarse a cada dispositivo (ver Manejo de llamadas de terminación). La expiración es de 599 segundos fijos.
7. **Registro de terceros / reg-event.** El S-CSCF también evalúa el registro contra los Criterios de Filtro Inicial activados por REGISTER. Esta evaluación activa los REGISTER de terceros a cualquier Servidor de Aplicaciones coincidente. El paquete de evento de registro notifica a las entidades suscritas sobre el estado del registro. El S-CSCF desmantela la suscripción en la desregistración.



Múltiples dispositivos en un número (número compartido)

Para servir un número en varios dispositivos en SIMs separadas (un teléfono y un reloj inteligente, por ejemplo), el S-CSCF debe mantener un contacto por dispositivo bajo la identidad pública compartida y bifurcar una llamada de terminación a todos ellos. Los parámetros relevantes de usrloc / registrador son:

Parámetro	Valor	Propósito
`ims_usrloc_scscf maxcontact`	`10`	Máximo de contactos por identidad pública. Era `1` (contacto único, el segundo dispositivo sobrescribió el primero).
`ims_usrloc_scscf maxcontact_3gpp`	`10`	Mismo límite para contactos 3GPP.
`ims_registrar_scscf max_contacts`	`10`	Límite de contacto del lado del registrador, mantenido consistente con usrloc.
`ims_usrloc_scscf maxcontact_behaviour`	`2`	Sobrescribir solo el contacto más antiguo cuando se excede el límite.
`ims_registrar_scscf append_branches`	`1`	En una `lookup("location")` de terminación, agregar cada contacto registrado como una rama paralela, de modo que la llamada se bifurque a todos los dispositivos.

Notas:

- `maxcontact` se cuenta **por identidad pública**, no por dispositivo. Los contactos se emparejan por URI de contacto, por lo que cada dispositivo (cada identidad privada / IMSI) mantiene su propio contacto bajo la identidad pública compartida.
- El número debe estar provisionado como una identidad pública compartida en el HSS (una suscripción IMS cuyos miembros comparten el número). Ver la documentación del HSS "Identidad de Usuario Pública Compartida".
- Aumentar `maxcontact` se aplica a todos los números. Un número con un solo dispositivo no se ve afectado (sigue teniendo un contacto). Un dispositivo que vuelve a registrarse desde un nuevo contacto sin desregistrar el antiguo deja el contacto antiguo hasta que expire; la

bifurcación de terminación prueba ambos y la rama obsoleta falla rápidamente.

Activación de servicios a través de IFC (ISC)

El S-CSCF evalúa cada solicitud inicial contra los **Criterios de Filtro Inicial** descargados del suscriptor. Cada IFC tiene un Punto de Activación priorizado, una dirección de Servidor de Aplicaciones y un valor de Manejo Predeterminado. El Punto de Activación es una combinación booleana de Puntos de Activación de Servicio (método, Request-URI, encabezado SIP, Caso de Sesión, SDP). El valor de Manejo Predeterminado es sesión-continuada o sesión-terminada en caso de fallo del AS. El Punto de Activación utiliza forma normal conjuntiva o disyuntiva. Puedes agrupar y negar los disparadores individuales.

El S-CSCF recorre el perfil en orden de prioridad para el caso de sesión relevante. Al coincidir, reenvía la solicitud al Servidor de Aplicaciones a través de ISC. El S-CSCF marca la solicitud con un **Identificador de Diálogo Original (ODI)**. También inserta un encabezado **P-Served-User** (RFC 5502) que identifica al suscriptor servido y al caso de sesión. Estas marcas permiten que el AS devuelva la solicitud al punto en la cadena donde se quedó. Cuando el AS enruta la solicitud de vuelta, el S-CSCF reconoce el ODI. Luego, reanuda la evaluación de IFC después del último criterio coincidente en lugar de reiniciar.

El Manejo Predeterminado gobierna el comportamiento en caso de fallo del AS. El Servidor de Aplicaciones devuelve un 408 o 5xx. El S-CSCF entonces continúa al siguiente criterio (sesión-continuada) o abandona la rama, según lo especifique el IFC.

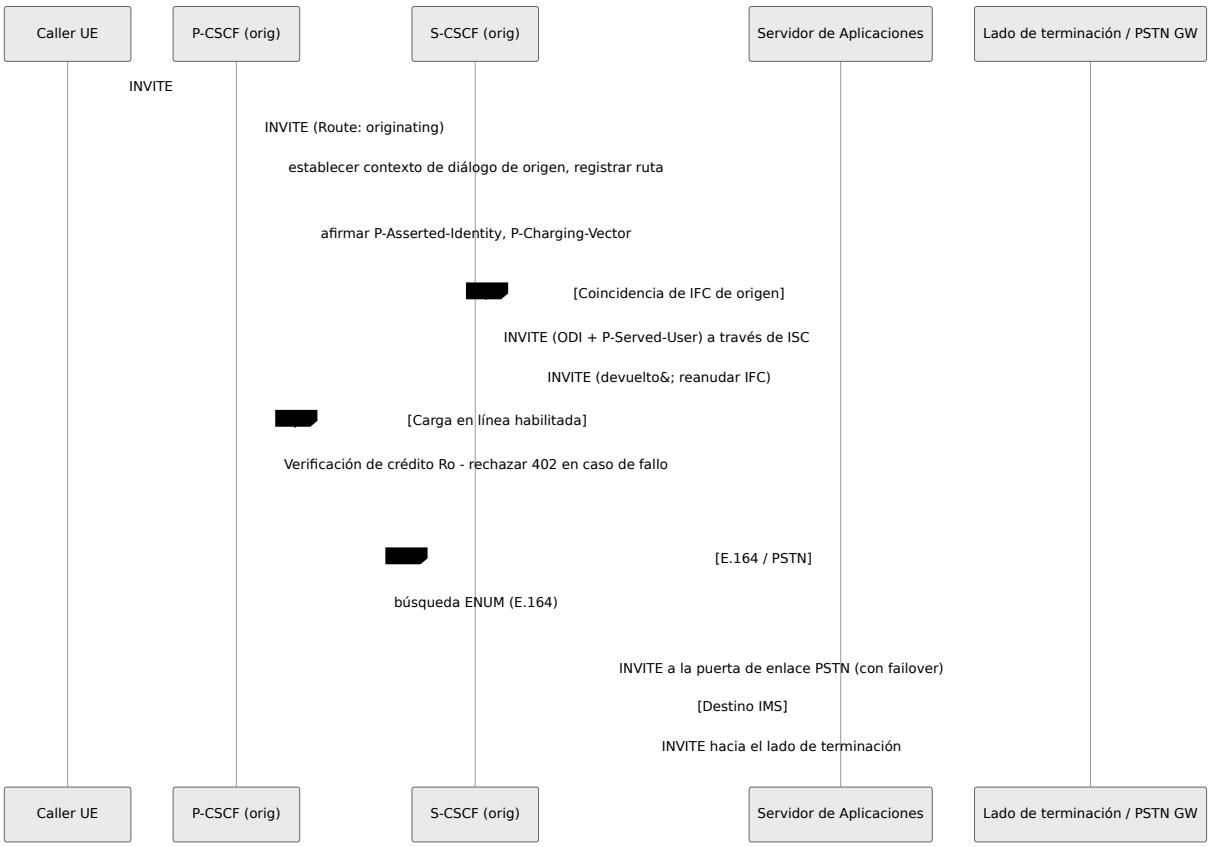
Manejo de llamadas de origen

Una solicitud es **de origen** cuando llega con el indicador de origen en su encabezado Route superior, o cuando regresa de un Servidor de Aplicaciones de origen. El S-CSCF entonces:

- Asigna el contexto de diálogo de origen y registra las rutas, por lo que reconoce las solicitudes en diálogo como la rama de origen.

- **Afirma la identidad.** La solicitud no regresa de un AS. El S-CSCF elimina cualquier `P-Asserted-Identity` proporcionado por el cliente. Reemplaza la identidad con la identidad que autenticó en el registro. Esta es la identidad de línea de llamada autenticada para la rama.
- Evalúa el IFC de origen y reenvía las coincidencias al Servidor de Aplicaciones a través de ISC.
- **Normalización de números.** Un Request-URI lleva un `phone-context`. El S-CSCF reescribe el Request-URI a un URI `tel:` en el contexto telefónico de la red local antes de enrutar.
- **PSTN / ENUM.** Para destinos E.164, el S-CSCF resuelve el número mediante ENUM. En un fallo de ENUM, el S-CSCF envía la llamada a las puertas de enlace de salida de PSTN, con failover a través del conjunto de puertas de enlace. Si la solicitud lleva una indicación de Transit-and-Roaming Function en roaming (`Feature-Caps: +g.3gpp.trf`), el S-CSCF la enruta a ese TRF en su lugar.
- **Vector de carga.** Las llamadas de origen llevan un `P-Charging-Vector` para la correlación de carga interoperadora.
- Si la carga en línea está habilitada, el S-CSCF envía una solicitud de control de crédito antes de que la llamada continúe (ver Carga).

El S-CSCF reenvía destinos no PSTN hacia el lado de terminación. Si este mismo S-CSCF atiende al usuario de terminación, el manejo de terminación continúa localmente.



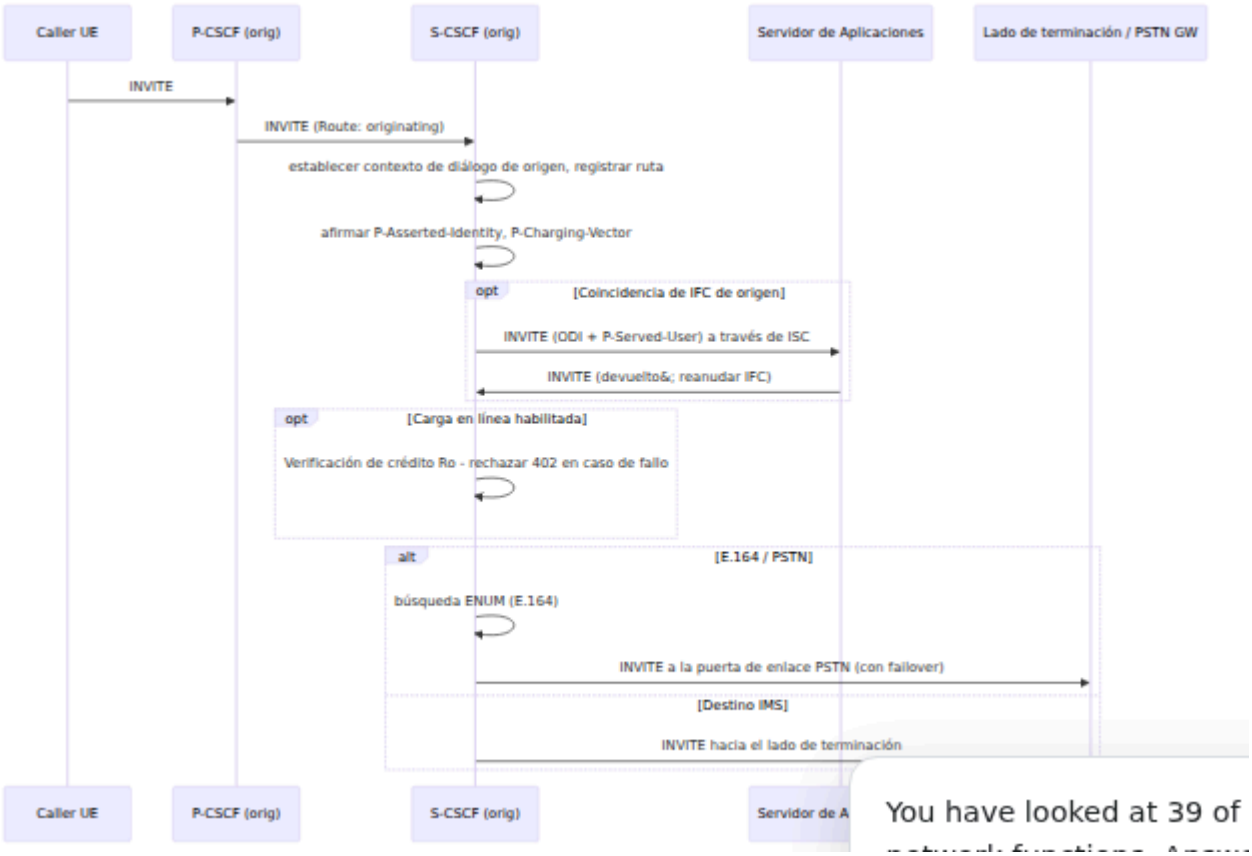
Manejo de llamadas de terminación

Una solicitud es **de terminación** cuando su Request-URI es una identidad servida localmente. El S-CSCF entonces:

1. Asigna el contexto de diálogo de terminación y registra las rutas, por lo que reconoce las solicitudes en diálogo como la rama de terminación.
2. Restaura el Request-URI original. Para métodos no INVITE, evalúa el IFC de terminación y reenvía las coincidencias al Servidor de Aplicaciones a través de ISC. Para INVITEs, el reenvío de IFC sigue el ciclo de retorno del AS.
3. Si la carga en línea de terminación está habilitada, el S-CSCF envía una solicitud de control de crédito del lado de terminación antes de continuar.
4. **Resolución de ubicación.** El S-CSCF recupera el contacto(s) registrado del usuario servido. Reenvía la solicitud a cada contacto a través del P-CSCF registrado en la Ruta al momento del registro. Cuando varios dispositivos comparten la identidad pública (un número compartido), `append_branches` bifurca la solicitud a cada contacto registrado en paralelo, de modo que todos los dispositivos suenen. Si el usuario no tiene un enlace, el S-CSCF devuelve un **404 Not Found**.

5. El S-CSCF recibe un INVITE a una identidad que **no está actualmente registrada**. Primero, obtiene el perfil de servicio no registrado del HSS con un Cx Server-Assignment-Request de tipo UNREGISTERED_USER. Esto permite que los servicios no registrados de terminación se ejecuten (por ejemplo, correo de voz). Un tiempo de espera del HSS falla **503**. Un perfil faltante falla **403**.

El S-CSCF aplica privacidad en la salida. Si la solicitud afirma `Privacy: id`, el S-CSCF elimina el `P-Asserted-Identity` antes de que el mensaje salga del S-CSCF.



Carga (opcional)

La carga en línea a través de Diameter **Ro** a un OCS es opcional. Se habilita por implementación (ver las banderas de carga a continuación). Cuando está habilitada, el S-CSCF envía una solicitud de control de crédito antes de permitir un INVITE. El S-CSCF mapea la respuesta a respuestas SIP (por ejemplo, fondos insuficientes → 402, límite de crédito alcanzado → 486, suscriptor de carga desconocido → 403). El Service-Context-Id identifica el servicio cargado. El S-

CSCF ensambla este identificador a partir de los parámetros de carga enumerados en la referencia de configuración.

En producción, esto normalmente está **deshabilitado**. El TAS realiza la carga en su lugar. El TAS contabiliza correctamente los servicios suplementarios (desvío, transferencia, piernas de roaming) que el S-CSCF no puede observar de extremo a extremo. Trata la carga Ro del S-CSCF como una capacidad opcional, no como un valor predeterminado.

Presencia / reg-event

El S-CSCF no actúa como un servidor de presencia general. El S-CSCF acepta solicitudes de `SUBSCRIBE` de evento de registro (`Event: reg`) (200 OK). El S-CSCF no sirve suscripciones de presencia general. El S-CSCF acepta un `PUBLISH` de evento de registro solo de un usuario registrado. Tal `PUBLISH` actualiza el estado de registro publicado. De lo contrario, el S-CSCF lo rechaza **403**. Esta configuración no tiene manejo de presencia de disponibilidad de usuario (PIDF).

Configuración de Implementación (Inyectada por Ansible)

Ansible renderiza la configuración de tiempo de ejecución del S-CSCF y su tabla de pares Diameter (`scscf.xml`) en el momento de la implementación. Los valores a continuación derivan de la identidad PLMN de la red (MCC/MNC) y el nombre de host del inventario del nodo.

Identidad / reino

Nombre	Qué controla	Valor / derivac
`NETWORKNAME`	Dominio IMS local. Es el reino de destino Cx y el `phone-context` utilizado en la normalización de números	`ims.mnc<mnc>.mcc<mcc>.3gppnetwork.`
`HOSTNAME`	FQDN de este nodo (alias de host y origin-host de Diameter cuando Ro está habilitado)	`<inventory_hostname>.ims.mnc<mnc>.`
`URI`	El propio URI SIP del S-CSCF. Es la identidad de registrador y autenticación	`sip:<hostname>:5060`
`SCSCF_USER_AGENT`	El encabezado `User-Agent` que emite el nodo	`User-Agent: Omnitouch S-CSCF <inve`

Nombre	Qué controla	Valor / derivac
`ISC_MY_URI`	Token de host que identifica las propias rutas ODI de este S-CSCF cuando un AS devuelve una solicitud	`<inventory_hostname>`
`ENUM_SUFFIX`	Sufijo de dominio ENUM para la resolución de URI de números de PSTN de origen E.164→URI	`mnc<mnc>.mcc<mcc>.3gppnetwork.org.`

Ansible plantilla los sockets de escucha SIP (UDP/TCP 5060, TLS 9090) y alias de host a partir de la dirección del host del inventario y PLMN.

Autenticación - `REG_AUTH_DEFAULT_ALG`

El algoritmo de autenticación predeterminado que aplica el S-CSCF cuando debe elegir uno, en lugar de repetir el algoritmo que solicita el UE. Opciones:

Valor	Significado / cuándo usar
`AKAv1-MD5`	3GPP IMS-AKA (TS 33.203). Estándar para USIM/ISIM VoLTE/VoNR con SAs IPsec. Usar para suscriptores móviles normales.
`AKAv2-MD5`	Variante mejorada de IMS-AKA. Usar solo donde los UEs y el HSS negocian específicamente AKAv2.
`MD5`	SIP HTTP Digest simple (sin AKA, sin IPsec). Usar para clientes no IMS / softphone que no pueden hacer AKA.
`CableLabs-Digest`	Perfil de digest de PacketCable/CableLabs. Implementaciones de red por cable.
`3GPP-Digest`	3GPP SIP Digest (TS 33.203 Anexo N). Basado en contraseña, sin ISIM. Suscriptores de línea fija / no UICC.
`TISPAN-HTTP_DIGEST_MD5`	Perfil de digest de ETSI TISPAN NASS/HTTP-Digest. Suscriptores de banda ancha fija TISPAN.
`HSS-Selected`	**Predeterminado.** El S-CSCF no impone ningún algoritmo. El HSS devuelve el esquema por suscriptor en la respuesta de autenticación. Usar esto para que el S-CSCF desafíe a cada suscriptor con lo que el HSS provisionó (AKA para móviles, Digest para fijos, etc.).

El algoritmo no cambia los siguientes valores predeterminados. El S-CSCF autentica cada REGISTER por defecto (ver `WITH_AUTH`). El reino de destino Cx es el dominio de la red local (`NETWORKNAME`). El S-CSCF empareja los vectores de autenticación en la identidad pública. Los vectores expiran después de 599 s.

Carga (Ro) - banderas y par

Nombre	Qué controla	Valores
`WITH_RO`	Habilitar el control de crédito Diameter Ro de origen antes de un INVITE saliente	definir / indefinir (predeterminado: indefinir)
`WITH_RO_TERM`	Habilitar el control de crédito Diameter Ro del lado de terminación	definir / indefinir (predeterminado: indefinir)
`RO_DESTINATION`	Host de destino Diameter OCS (el reino de destino es el dominio de la red local)	FQDN de OCS, p. ej. `hssocs.voiceblue.com`
`RO_FORCED_PEER`	Fijar el enrutamiento de control de crédito a un par Diameter específico. Esto evita el enrutamiento por reino	id de par (p. ej. `32260@3gpp.org`); desactivado por defecto
`RO_ROOT`	Raíz del Service-Context-Id	`32260@3gpp.org`
`RO_EXT`	Extensión del Service-Context-Id	`ext`
`RO_MNC`	Componente MNC del Service-Context-Id	p. ej. `07`
`RO_MCC`	Componente MCC del Service-Context-Id	p. ej. `262`

Nombre	Qué controla	Valores
`RO_RELEASE`	Versión 3GPP para Service-Context-Id	p. ej. `8`

Banderas de características (`WITH_*`)

Bandera	Efecto cuando está definida
`WITH_AUTH`	Autenticar cada REGISTER (no solo clientes Digest/MD5). Habilitado por defecto en la plantilla.
`WITH_RO`	Habilitar carga en línea de origen a través de Diameter Ro.
`WITH_RO_TERM`	Habilitar carga en línea de terminación a través de Diameter Ro.

Ansible plantilla `CAPTURE_NODE` (el objetivo de captura de Homer) solo cuando la captura de Homer está habilitada para la implementación. `CAPTURE_NODE` duplica la señalización SIP a Homer para el rastreo.

Configuración de pares Diameter

La tabla de pares Diameter del S-CSCF (`scscf.xml`) anuncia la aplicación **Cx** (`16777216`) hacia el HSS más la contabilidad base. La estructura del archivo y las variables de Ansible que lo llenan se comparten entre todos los CSCFs. Ver Diameter → Configuración de Pares (Implementación). Cuando la carga Ro está habilitada, `RO_DESTINATION` se dirige al par OCS en lugar del XML.

Solución de Problemas

Fallos de registro

Síntomas: Usuarios incapaces de registrarse, tiempos de espera de registro, 4xx/5xx en REGISTER.

- **Conectividad HSS (Cx)** - el S-CSCF depende del HSS para responder al Cx MAR (vector de autenticación) y SAR (perfil de servicio). Si MAR/SAR se agotan o devuelven respuestas malformadas, el registro falla **503**. Verifica que el par Cx al HSS esté activo y responda. Ver Operaciones Diameter.
- **Fallas de autenticación** - confirma que las credenciales del suscriptor estén provisionadas en el HSS y que el HSS haya generado el vector de autenticación (MAR/MAA). Verifica que el algoritmo de desafío sea uno que el UE soporte (AKA/Milenage para USIM/ISIM, Digest para clientes no IMS). Una identidad rechazada falla **403**.
- **Asignación S-CSCF / capacidad** - un suscriptor sin perfil de servicio IMS, o una asignación de servidor rechazada (SAR), falla **403**. Confirma que las capacidades del S-CSCF coincidan con lo que seleccionó el I-CSCF. También confirma que el nodo tenga capacidad de registro.

Fallos en la configuración de llamadas

Síntomas: Las llamadas no se establecen, errores SIP 4xx/5xx.

- **Usuario no registrado** - verifica que tanto las identidades de origen como de terminación estén registradas en IMS. Un INVITE de terminación a una identidad sin enlace de contacto devuelve **404**. Para una identidad de terminación no registrada con servicios provisionados, el S-CSCF obtiene el perfil no registrado (Cx SAR UNREGISTERED_USER). Un tiempo de espera del HSS aquí falla **503**.
- **IFC / activación de servicios** - verifica que el S-CSCF haya descargado el IFC del HSS (SAR/SAA) y que los puntos de activación coincidan con el caso de sesión. Verifica que cualquier Servidor de Aplicaciones invocado a través de ISC (OmniTAS, OmniMessage) sea accesible. El Manejo Predeterminado gobierna si un fallo del AS continúa la rama o la abandona.

- **QoS** - el P-CSCF autoriza QoS de medios para la llamada (Rx al PCRF para VoLTE, N5 al PCF para VoNR). Si las llamadas se conectan pero no tienen ruta de medios, verifica la rama de política en el P-CSCF.
- **Enrutamiento** - para destinos E.164 verifica la resolución ENUM y el failover de puerta de enlace PSTN. Verifica el enrutamiento de roaming/red externa para llamadas que salen de la red local.

Problemas de entrega de SMS

Síntomas: SMS no entregados a través de IMS, o retrocediendo al SMSC heredado.

- **Activación de IFC de OmniMessage** - verifique que el IFC del suscriptor active OmniMessage en el método SIP MESSAGE y que su prioridad sea lo suficientemente alta como para activarse. Pruebe la coincidencia de IFC con un SMS simulado.
- **Integración de SMSC** - verifique la conectividad de OmniMessage con el SMSC (MAP/SMPP) y que la conversión de SIP MESSAGE ↔ SMS PDU esté intacta.
- **Tipo de contenido** - verifique que el SIP MESSAGE lleve `Content-Type: application/vnd.3gpp.sms` y la codificación de conjunto de caracteres correcta (GSM-7, UCS-2).

Flujos de Llamadas

Los diagramas de secuencia están incrustados con las funciones que documentan:

- Registro y autenticación → Registro y autenticación
- Sesión de origen → Manejo de llamada de origen
- Sesión de terminación → Manejo de llamada de terminación

Documentación Relacionada

- Operaciones

- Diámetro
- Interfaz Basada en Servicios (SBI)
- Referencia de Métricas
- OmniWeb - registros, diálogos y estado de pares de Diámetro: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>

Documentación de Cumplimiento de Intercepción ANSSI R226

Propósito del Documento: Este documento proporciona las especificaciones técnicas requeridas para la autorización ANSSI R226. Estas especificaciones se aplican bajo los Artículos R226-3 y R226-7 del Código Penal Francés. Cubren la Red Central IMS OmniCSCF (Funciones de Control de Sesiones de Llamadas).

Clasificación: Documentación de Cumplimiento Regulatorio

Autoridad Objetivo: Agence nationale de la sécurité des systèmes d'information (ANSSI)

Regulación: R226 - Protección de la Privacidad de la Correspondencia y la Intercepción Legal

---

1. ESPECIFICACIONES TÉCNICAS DETALLADAS

1.1 Identificación del Sistema

Nombre del Producto: OmniCSCF IMS Core Network
Tipo de Producto: Red Central del Subsistema Multimedia IP (IMS)
Función Principal: Control de sesiones de llamadas VoIP/VoLTE y entrega de servicios multimedia
Modelo de Implementación: Infraestructura de telecomunicaciones local

Componentes de la Red:

- P-CSCF (Función de Control de Sesiones de Llamadas Proxy)
- E-CSCF (Función de Control de Sesiones de Llamadas de Emergencia)
- I-CSCF (Función de Control de Sesiones de Llamadas de Interrogación)
- S-CSCF (Función de Control de Sesiones de Llamadas de Servicio)

Este sistema maneja el registro, la autenticación, el enrutamiento de sesiones y el control de llamadas para redes del Subsistema Multimedia IP (IMS). Las secciones a continuación describen las capacidades de intercepción y las características de cifrado.

1.2 Capacidades de Intercepción

1.2.1 Captura de Registro y Adquisición de Sesiones

Captura de Registro SIP:

El sistema CSCF procesa todos los registros SIP. Mantiene el estado completo del registro:

- **Identificadores de Usuario:**
  - IMPU (Identidad Pública Multimedia IP) - URI SIP (por ejemplo, sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org)
  - IMPI (Identidad Privada Multimedia IP) - Nombre de usuario de autenticación (por ejemplo, user@ims.mnc001.mcc001.3gppnetwork.org)
  - IMSI (Identidad Internacional de Suscriptor Móvil) - De los encabezados P o HSS
  - MSISDN (Número de teléfono móvil) - De IMPU o perfil de usuario HSS
- **Metadatos de Registro:**
  - URI de contacto (dirección de red actual del UE)
  - Encabezado de ruta (ruta de regreso a través de P-CSCF)
  - Encabezado de Service-Route (ruta a S-CSCF)
  - Cadena User-Agent (identificación del tipo de dispositivo)
  - Marca de tiempo de expiración del registro

    - Dirección IP y puerto de origen
    - Protocolo de transporte (TCP/UDP/TLS)
    - Vectores de autenticación (RAND, AUTN, XRES, CK, IK de HSS)

- **Información de Ubicación de la Red:**

    - Encabezado P-Access-Network-Info (torre de celular, área de ubicación)
    - P-Visited-Network-ID (identificación de la red de roaming)
    - Dirección IP recibida (fuente actual)
    - Dirección P-CSCF (punto de entrada a la red)

Captura de Sesión de Llamadas:

El S-CSCF mantiene el estado completo del diálogo SIP para todas las llamadas activas:

- **Identificadores de Sesión:**

    - Call-ID (identificador de sesión único)
    - URIs y etiquetas From/To
    - Conjuntos de rutas para ambas partes
    - Original-Dialog-ID (para seguimiento de interacción con el Servidor de Aplicaciones)

- **Metadatos de Sesión:**

    - Identidad del llamante (encabezado From, P-Asserted-Identity)
    - Parte llamada (encabezado To, Request-URI)
    - Marca de tiempo de establecimiento de la sesión
    - Marca de tiempo de terminación de la sesión
    - Estado del diálogo (Temprano/Confirmado/Eliminado)
    - Números CSeq (secuenciación de transacciones)

- **Información de Medios:**

    - SDP (Protocolo de Descripción de Sesiones) en los cuerpos de mensajes SIP
    - Direcciones de servidores de medios (OmniTAS)

- Información de códec (formatos de audio/video)
- Puntos finales de flujo de medios
- Asignaciones de puertos RTP/RTCP

Identificación de Llamadas de Emergencia:

El componente E-CSCF identifica llamadas de emergencia y las enruta:

- Detección de números de emergencia (112, 911, etc.)
- Captura de IMEI (Identidad Internacional de Equipos Móviles)
- Mapeo de IMEI a MSISDN (para devolución de llamada)
- Información de ubicación del UE o de la red
- Soporte del protocolo HELD (HTTP-Enabled Location Delivery)
- Destino de enrutamiento de emergencia (PSAP/AS de emergencia)

Determinación de Identidad del Llamante (según 3GPP TS 23.167):

El sistema establece la identidad de línea de llamada autenticada presentada en la parte de emergencia de la siguiente manera:

- **Llamante conocido (registrado):** El sistema toma la identidad del IMPU registrado. Cuando sea aplicable, también utiliza el mapeo IMEI→MSISDN en caché mantenido por el P-CSCF.
- **Llamante desconocido / anónimo (emergencia no autenticada, sin identidad registrada):** El P-CSCF resuelve la identidad a nivel EPC desde el PCRF a través de la interfaz Diameter Rx. Utiliza un `Rx_AAR_Subscription` asíncrono, vinculado por la dirección IP de origen del UE. El sistema selecciona la identidad por precedencia **MSISDN → IMSI → IMEISV**. Asegura el valor resuelto como el **P-Asserted-Identity** en el dominio `sos.apn`.

En ambos casos, el P-Asserted-Identity resultante es la identidad de línea de llamada autenticada presentada al PSAP y en las interfaces LI. Es una identidad afirmada por la red, no una mera aproximación.

1.2.2 Almacenamiento y Procesamiento de Datos

IMPORTANTE: Solo Estado en Memoria

Los componentes CSCF (P-CSCF, E-CSCF, I-CSCF, S-CSCF) mantienen **todos los datos de estado solo en memoria**. No hay **almacenamiento de base de datos persistente** de datos de registro o sesión de llamadas. El sistema almacena todos los enlaces de registro, el estado del diálogo y las asociaciones de seguridad IPsec en memoria. El sistema pierde estos datos al reiniciar.

Datos de Registro Activo (En Memoria):

El sistema CSCF mantiene solo el estado en tiempo real:

Estado de Registro P-CSCF:

- Datos de Asociación de Seguridad IPsec (pares SPI, puertos, parámetros de cifrado)
- Vínculos de contacto del UE y direcciones de red
- Puntos finales y estado del túnel IPsec
- Períodos de validez del registro

Estado de Registro S-CSCF:

- Identidades públicas (IMPU) y estado de registro actual
- Vínculos de contacto con encabezados de ruta, User-Agent, direcciones recibidas
- Mapeos de identidad privada (IMPI) a identidad pública
- Perfiles de usuario de HSS (en caché durante el registro)

Estado de Sesión Activa (En Memoria):

El S-CSCF mantiene solo el estado de llamadas activas:

- Identificadores de llamada (Call-ID), identidades de participantes (etiquetas From/To)
- Conjuntos de rutas y direcciones de contacto
- Estado de la sesión (Temprano/Confirmado/Terminado)
- Información de tiempo de la sesión

Sin CDR ni Seguimiento Histórico:

Los componentes CSCF **no** generan ni almacenan:

- Registros de Detalles de Llamadas (CDRs)
- Registros históricos de llamadas
- Registros históricos de registro
- Seguimiento de eventos a largo plazo

Generación de CDR y Seguimiento Histórico: El **TAS (Servidor de Aplicaciones de Telefonía - OmniTAS)** maneja todos los registros de detalles de llamadas, datos de facturación y seguimiento de llamadas históricas. Los componentes CSCF no los manejan.

Registro de Mensajes SIP/Diameter:

Los CSCF pueden generar registros de eventos en tiempo real para uso operativo:

- **Registro de Mensajes SIP:** Registro opcional de mensajes SIP (INVITE, REGISTER, etc.)
- **Registro de Mensajes Diameter:** Registro opcional de transacciones Diameter (Cx, Rx, Ro)
- **Eventos del Sistema:** Cambios de configuración, errores, fallos

Estos registros son registros operativos transitorios, no registros de llamadas persistentes. Puedes configurar la retención de registros. La retención es típicamente a corto plazo (horas a días) solo para depuración.

1.2.3 Capacidades de Análisis

Monitoreo en Tiempo Real:

El portal de gestión OmniWeb (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>) proporciona:

- **Monitoreo de Registro:**
  - Ver todos los usuarios registrados con paginación
  - Buscar por IMPU, contacto, IMPI
  - Detalles del registro (contacto, ruta, user-agent, expiración)
  - Capacidad de desregistro forzado

- **Monitoreo de Diálogo:**
  - Vista de sesiones de llamadas activas
  - Call-ID, URIs From/To, estado, duración
  - Capacidad de terminación de llamada (enviar BYE)
  - Auto-refresco cada 5 segundos
- **Estado del Sistema:**
  - Estado de pares Diameter (HSS, PCRF, conectividad OCS)
  - Estado de la puerta de enlace frontal
  - Métricas de capacidad del sistema
  - Capacidad del túnel IPsec (P-CSCF)

Nota sobre Datos Históricos:

Los componentes CSCF no mantienen datos históricos. **OmniTAS (Servidor de Aplicaciones de Telefonía)** maneja toda la generación de CDR y el seguimiento de llamadas a largo plazo. Para registros de llamadas históricos, CDRs y análisis de patrones de comunicación, las autoridades de intercepción legal deben coordinarse con OmniTAS.

Visibilidad de Activación de Servicios en Tiempo Real:

El S-CSCF procesa Criterios de Filtro Inicial (iFC) en tiempo real:

- La evaluación de iFC determina qué Servidores de Aplicaciones se activan para cada llamada
- Visibilidad en tiempo real de qué servicios se invocan
- Decisiones de enrutamiento del Servidor de Aplicaciones visibles en el flujo de mensajes SIP

Estado de la Red:

- Estado de conectividad HSS (interfaz Diameter Cx)
- Distribución de selección S-CSCF (I-CSCF)
- Patrones de enrutamiento de llamadas
- Tiempos de respuesta del Servidor de Aplicaciones

- Rendimiento de transacciones Diameter

1.3 Capacidades de Contramedidas

1.3.1 Mecanismos de Protección de la Privacidad

Confidencialidad de la Comunicación:

- **Túneles IPsec:** Túneles ESP (Encapsulating Security Payload) entre UE y P-CSCF
    - Cifrado: AES-CBC, AES-GCM
    - Autenticación: HMAC-SHA1, HMAC-SHA256
    - Derivación de claves de IMS AKA (CK/IK de HSS)
    - Asociaciones de seguridad por UE
- **Soporte TLS/TLS:**
    - Soporte de SIP sobre TLS (SIPS)
    - Diameter sobre TLS (conexiones HSS, PCRF, OCS)
    - Autenticación basada en certificados
    - Perfect Forward Secrecy (PFS) a través de ECDHE/DHE
- **Encabezados de Privacidad SIP:**
    - P-Asserted-Identity (ID de llamada autenticada)
    - Encabezado de privacidad (solicitud de supresión de ID de llamada)
    - Soporte de sesión anónima

Control de Acceso:

- Autenticación de OmniWeb y control de acceso basado en roles
- Interfaz de gestión BINRPC (puerto 2046)
- Controles de acceso al registro y separación de roles
- Autenticación SIP (AKA a través de HSS)
- Autenticación de pares Diameter

Registro de Auditoría:

- Registro completo de mensajes SIP y Diameter
- Eventos de registro/desregistro
- Eventos de establecimiento y terminación de llamadas
- Acciones administrativas a través de OmniWeb
- Cambios de configuración
- Éxito/fallo de autenticación

1.3.2 Características de Protección de Datos

Seguridad de Acceso:

- Control de acceso basado en roles (RBAC)
- Cuentas de monitoreo de solo lectura
- Controles de autenticación y autorización

Fortalecimiento del Sistema:

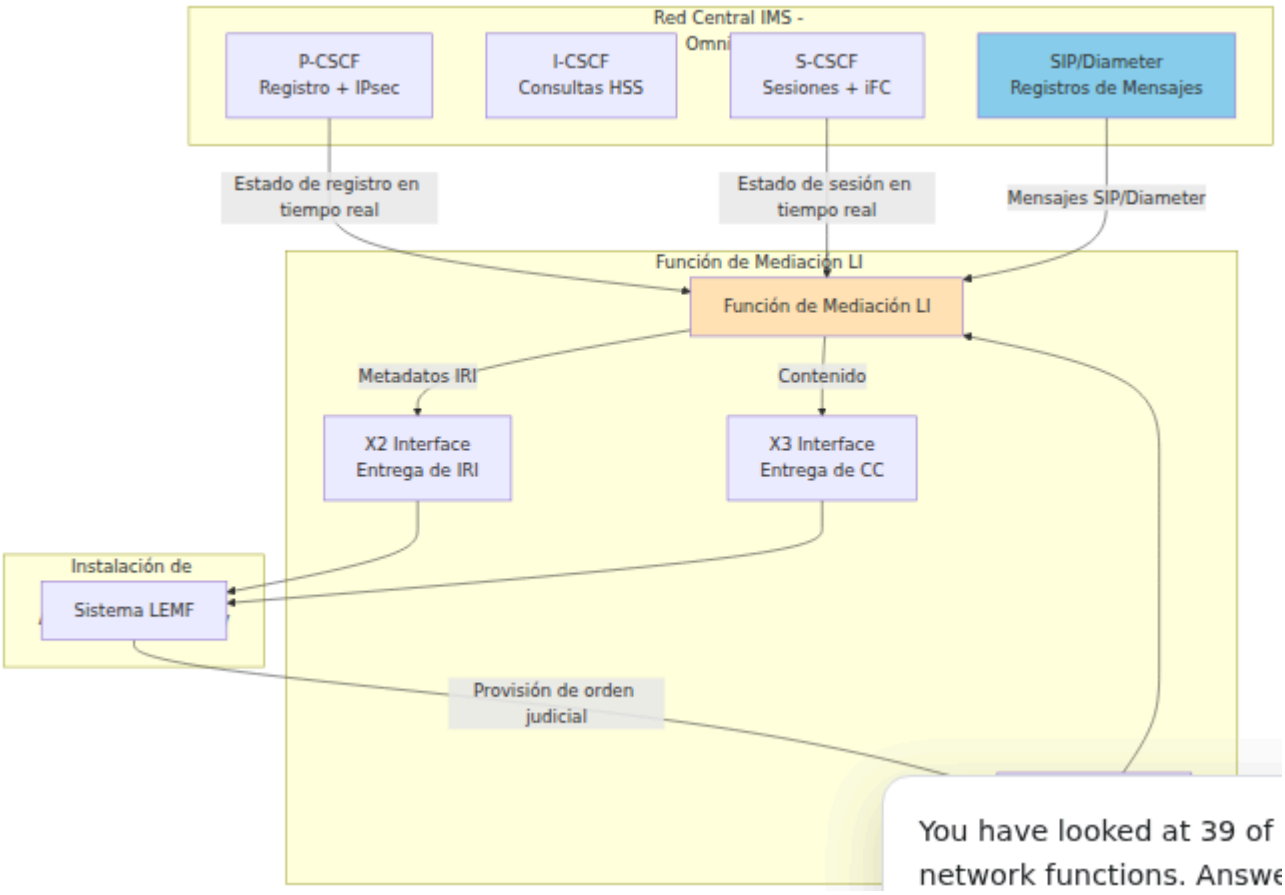
- Puertos de red expuestos mínimos (5060 SIP, 3868 Diameter, 2046 gestión BINRPC)
- Verificación de cordura de mensajes SIP
- Prevención de bucles Max-Forwards
- Limitación de tasa y protección contra inundaciones
- Límites de tamaño de mensajes
- Aislamiento de procesos de trabajo

1.4 Puntos de Integración de Intercepción Legal

1.5.1 Arquitectura de Intercepción Legal ETSI

El sistema CSCF proporciona una base para la intercepción legal conforme a ETSI. El sistema no incorpora interfaces nativas X1/X2/X3. Todos los puntos de acceso de datos necesarios existen para la integración con sistemas externos de Función de Mediación de Intercepción Legal (LIMF).

Interfaces LI Estándar ETSI:



Interfaz X1 - Función de Administración:

- **Propósito:** Provisión de órdenes y objetivos de la aplicación de la ley
- **Dirección:** LEMF → LIMF (bidireccional)
- **Funciones:**
  - Activar/desactivar intercepción para objetivos (IMPUs, IMSIs, MSISDNs)
  - Establecer duración de la intercepción y período de validez
  - Configurar criterios de filtrado (identidades, ventanas de tiempo)
  - Recuperar estado de intercepción
- **Integración con CSCF:**
  - LIMF mantiene la base de datos de órdenes (lista de objetivos, externa al CSCF)
  - LIMF monitorea el estado en tiempo real del CSCF y los registros de mensajes para sesiones coincidentes
  - LIMF filtra según los criterios provistos por X1

Interfaz X2 - Entrega de IRI (Información Relacionada con la Intercepción):

- **Propósito:** Entregar metadatos de sesión a la aplicación de la ley
- **Dirección:** LIMF → LEMF (unidireccional)
- **Formato de Datos:** XML/ASN.1 conforme a ETSI TS 102 232
- **Contenido del CSCF:**
  - Identificadores de sesión (Call-ID, etiquetas de diálogo)
  - Parte llamante (URI From, P-Asserted-Identity, IMPU, IMSI, MSISDN)
  - Parte llamada (URI To, Request-URI, IMPU, IMSI, MSISDN)
  - Marcas de tiempo de registro
  - Marcas de tiempo de configuración/desmantelamiento de la sesión
  - Ubicación de la red (P-Access-Network-Info, torre de celular, área de ubicación)
  - Direcciones P-CSCF/S-CSCF (identificación del elemento de red)
  - User-Agent (tipo de dispositivo)
  - Información de roaming (P-Visited-Network-ID)

Interfaz X3 - Entrega de CC (Contenido de la Comunicación):

- **Propósito:** Entregar el contenido real de la comunicación
- **Dirección:** LIMF → LEMF (unidireccional)
- **Formato de Datos:** Conforme a ETSI TS 102 232
- **Contenido del CSCF:**
  - Cuerpos de mensajes SIP (descripciones de sesiones SDP)
  - Direcciones de servidores de medios (para intercepción RTP)
  - Información de códec
  - Mensajes instantáneos SIP MESSAGE (contenido del cuerpo)
  - Datos de aplicación (si se enrutan a través del CSCF)

Nota: Para flujos RTP de voz/video, el LIMF también debe integrarse con servidores de medios (OmniTAS). Esta integración captura el contenido real de los medios. El CSCF proporciona información de configuración de sesiones (SDP). Esta información muestra dónde fluyen los medios.

1.5.2 Fuentes de Datos CSCF para Intercepción Legal

1. Acceso a Datos de Registro:

Datos de Registro P-CSCF:

- IMPU (identidad pública)
- URI de contacto (dirección de red UE)
- IP y puerto recibidos
- Encabezado de ruta
- Expiración del registro
- Información de SPI y puerto IPsec
- Cadena User-Agent

Datos de Registro S-CSCF:

- Identidades públicas (IMPU), estado de bloqueo, estado de registro
- Vínculos de contacto con encabezados de ruta, User-Agent, direcciones recibidas
- Mapeos de identidad privada (IMPI) a identidad pública
- Perfiles de usuario de HSS (formato XML que incluye detalles del suscriptor)

Métodos de Acceso:

- Interfaces de acceso a datos de solo lectura
- Interfaz de monitoreo OmniWeb
- Capacidades de registro de eventos en tiempo real

2. Datos de Sesión Activa:

Datos de Diálogo S-CSCF:

- Call-ID (identificador de sesión único)
- URIs y etiquetas From/To
- Números CSeq del llamante y del llamado
- Conjuntos de rutas para ambas partes
- Direcciones de contacto
- Estado del diálogo (Temprano, Confirmado, Eliminado)
- Marca de tiempo de inicio
- Valores de tiempo de espera

Métodos de Acceso:

- Monitoreo del estado del diálogo en tiempo real
- Consulta por identificadores de sesión o identificadores de partes
- Capacidades de exportación para análisis forense

3. Registro de Mensajes SIP:

Captura de Registro:

- Todos los mensajes SIP pueden ser registrados (REGISTER, INVITE, MESSAGE, etc.)
- Niveles de registro configurables
- Registro estructurado con marcas de tiempo
- Registro basado en syslog o archivos

Análisis de Registros:

- Analizar encabezados SIP para extracción de identidad
- Extraer SDP para información de medios
- Rastrear secuencias de mensajes (CSeq)
- Correlacionar solicitudes y respuestas

Ejemplo de Entrada de Registro:

```
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 Mensajes Diameter:

Mensajes Cx (Comunicación HSS):

- UAR/UAA: Autorización de usuario (contiene IMPU, IMPI)
- LIR/LIA: Información de ubicación (contiene IMPU, S-CSCF que sirve)
- MAR/MAA: Autenticación (contiene IMPI, vectores de autenticación)
- SAR/SAA: Asignación de servidor (contiene IMPU, IMPI, perfil de usuario XML)

Datos Diameter Disponibles:

- IMSI (del perfil de usuario)
- MSISDN (del perfil de usuario)
- IMPUs asociados (múltiples identidades por suscriptor)
- Perfil de usuario (servicios, estado de bloqueo, estado de roaming)

Ejemplo de Registro:

```
Diameter Cx SAA recibido del 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 (Éxito)
User-Data: <XML perfil de usuario con IMSI, MSISDN, iFC>
```

5. Datos de Llamadas de Emergencia (E-CSCF):

Mapeo de IMEI a MSISDN:

- El P-CSCF crea el mapeo cuando un UE se registra con un IMEI (tabla `emergency_imei_msisdn_map`)
- TTL de 4 horas (14400s autoexpira)
- Utilizado para devolución de llamada de emergencia
- Replicado a través de nodos del clúster P-CSCF

Retención de Datos:

- Mapeos de IMEI a MSISDN retenidos durante 4 horas (14400s)
- Disponibles para correlación de devolución de llamada de emergencia
- Accesibles a través de interfaces de monitoreo

Registros de Llamadas de Emergencia:

- Detección de números de emergencia (112, 911, etc.)
- Extracción de IMEI de contacto o encabezados P
- Información de ubicación (de HELD o P-Access-Network-Info)
- Enrutamiento PSAP (Punto de Respuesta de Seguridad Pública)
- Enrutamiento E-CSCF a AS de emergencia

1.5.3 Capacidades de Integración para LIMF

El sistema proporciona varios métodos de integración para sistemas de Función de Mediación de Intercepción Legal (LIMF):

1. **Acceso a Datos de Registro y Sesión:**

- Acceso en tiempo real a datos de registro (identidades, ubicaciones, información del dispositivo)
- Monitoreo de sesiones activas (estado de llamada, participantes, tiempos)
- Capacidades de consulta histórica

2. **Registro de Eventos:**

   - Registro de mensajes SIP con niveles de detalle configurables
   - Registro de mensajes Diameter para interacciones HSS
   - Registros de eventos estructurados con marcas de tiempo

3. **Monitoreo en Tiempo Real:**

   - Monitoreo del estado de registro en vivo
   - Seguimiento de sesiones de llamadas activas
   - Detección de llamadas de emergencia y información de enrutamiento

Los métodos de integración admiten arquitecturas basadas en sondeos y en eventos para la conectividad LIMF.

1.5.4 Mapeo de Datos CSCF a Interfaces LI

Mapeo de Datos CSCF a IRI (X2):

Fuente de Datos CSCF	Campo IRI	Ejemplo de Datos
IMPU (encabezados SIP/estado en memoria)	Parte A	sip:+33612345678@ims.mnc001.mcc001.3
IMPI (encabezados SIP/estado en memoria)	ID de Autenticación	user@ims.mnc001.mcc001.3gppnetwork.org
IMSI (perfil de usuario HSS)	ID de Suscriptor	208011234567890
MSISDN (perfil de usuario HSS)	Número de Teléfono	+33612345678
Call-ID (encabezados SIP/estado de diálogo)	ID de Sesión	f81d4fae-7dec-11d0-a765-00a0c91e6bf6@..
From/To (encabezados SIP)	Parte A/Parte B	sip:+33612345678@... / sip:+33687654321
Marca de tiempo de registro (en memoria)	Tiempo del Evento	2025-11-29T10:30:00Z
P-Access-Network-Info	Ubicación	3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=2080

Fuente de Datos CSCF	Campo IRI	Ejemplo de Datos
(encabezado SIP)		
IP Recibida (contacto SIP)	Dirección IP UE	10.20.30.40:5060
Dirección P-CSCF (enrutamiento SIP)	Elemento de Red	10.4.12.165:5060
Dirección S-CSCF (enrutamiento SIP)	Elemento de Red	10.4.11.45:5060

Mapeo de Datos CSCF a CC (X3):

Fuente de Datos CSCF	Campo CC	Ejemplo de Datos
Cuerpo de SIP MESSAGE	Contenido del Mensaje Instantáneo	"Hola, ¿cómo estás?"
SDP en INVITE	Información de Sesión de Medios	Puntos finales RTP, códecs
Dirección del servidor de medios	Objetivo de Intercepción RTP	10.50.60.70:49170

Nota: Para el contenido real de voz/video (RTP), el LIMF debe coordinarse con servidores de medios (OmniTAS) para capturar flujos RTP. El CSCF proporciona solo información de configuración de sesiones.

Nota sobre la identidad de llamada de emergencia (Parte A): Para una llamada normal (registrada), el sistema deriva la Parte A del IMPU registrado / P-Asserted-Identity. Para una **llamada de emergencia desconocida/anónima**, el P-CSCF resuelve la Parte A del PCRF a través de Diameter Rx (`Rx_AAR_Subscription`, vinculado por la IP de origen del UE, precedencia MSISDN → IMSI → IMEISV). El P-CSCF asegura esta identidad como P-Asserted-Identity en el dominio `sos.apn`, según 3GPP TS 23.167. Esta es la identidad de línea de llamada autenticada que se transporta en la interfaz X2/IRI para tales llamadas.

1.5 Interfaz de Monitoreo Basada en Web

OmniWeb proporciona acceso de monitoreo y administrativo. OmniWeb es el portal de gestión unificado (<https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>). Ofrece monitoreo en tiempo real y acceso administrativo a los componentes CSCF:

Capacidades de Monitoreo:

- Monitoreo en tiempo real de registros y sesiones (suscriptores activos, ubicaciones, información del dispositivo, estado de llamada, tiempos)
- Búsqueda de identidad por IMPU, IMPI, IMSI o MSISDN
- Estado y monitoreo de capacidad del túnel IPsec
- Capacidades de exportación para análisis forense

Seguridad:

- Acceso cifrado HTTPS/TLS
- Autenticación requerida
- Control de acceso basado en roles (RBAC), incluidos modos de acceso de solo lectura para personal de monitoreo
- Registro de auditoría de todas las acciones administrativas

---

2. CAPACIDADES DE CIFRADO Y CRIPTOANÁLISIS

2.1 Visión General de Capacidades Criptográficas

El OmniCSCF implementa varias capas de protección criptográfica para la señalización y los datos de suscriptores. Esta sección documenta todas las capacidades criptográficas, según lo requerido por ANSSI.

2.2 Cifrado de Túneles IPsec ESP (UE a P-CSCF)

2.2.1 Implementación del Protocolo IPsec

Modo IPsec Soportado:

- ESP (Encapsulating Security Payload) - Protocolo IP 50
- Modo de transporte (no modo túnel)
- Protege la señalización SIP entre UE y P-CSCF

Algoritmos de Cifrado Soportados:

El sistema con IPsec del kernel soporta:

- **AES-CBC (Estándar de Cifrado Avanzado - Cadena de Bloques de Cifrado):**
  - AES-128-CBC (clave de 128 bits)
  - AES-192-CBC (clave de 192 bits)
  - AES-256-CBC (clave de 256 bits) - Recomendado
- **AES-GCM (Estándar de Cifrado Avanzado - Modo Galois/Contador):**
  - AES-128-GCM (clave de 128 bits con AEAD)
  - AES-256-GCM (clave de 256 bits con AEAD) - Recomendado
- **3DES-CBC (Triple DES - Cadena de Bloques de Cifrado):**

    - Clave efectiva de 168 bits (obsoleto, compatibilidad heredada)
- **Cifrado NULL:**
    - Sin confidencialidad (solo autenticación)
    - Usado solo para depuración o escenarios de cumplimiento específicos

Algoritmos de Autenticación Soportados:

- **HMAC-SHA1 (Código de Autenticación de Mensajes Basado en Hash - SHA-1):**
    - Salida de 160 bits
    - Compatibilidad heredada
- **HMAC-SHA256 (HMAC - SHA-256):**
    - Salida de 256 bits
    - Recomendado
- **HMAC-SHA384 (HMAC - SHA-384):**
    - Salida de 384 bits
- **HMAC-SHA512 (HMAC - SHA-512):**
    - Salida de 512 bits
- **HMAC-MD5:**
    - Salida de 128 bits
    - Obsoleto, solo para compatibilidad heredada

Derivación de Claves:

El sistema deriva claves IPsec (CK - Clave de Cifrado, IK - Clave de Integridad) de la autenticación IMS AKA:

1. UE realiza autenticación AKA con S-CSCF/HSS
2. HSS genera CK (128 bits) e IK (128 bits)
3. S-CSCF entrega CK/IK a P-CSCF a través de la interfaz interna

4. P-CSCF utiliza CK/IK para establecer asociaciones de seguridad IPsec con UE
5. CK utilizado para cifrado ESP
6. IK utilizado para autenticación ESP

Parámetros de Asociación de Seguridad:

- **Vida Útil:** Vinculada a la expiración del registro SIP (típicamente 599 segundos)
- **Protección contra Repetición:** Habilitada (ventana anti-repetición)
- **Números de Secuencia:** 32 bits o 64 bits (ESN - Números de Secuencia Extendidos)
- **Perfect Forward Secrecy:** No aplicable (claves de AKA, no Diffie-Hellman)

Implementación:

La capacidad IPsec de P-CSCF:

- Interactúa con la pila IPsec del kernel de Linux (marco XFRM)
- Configura políticas de seguridad y asociaciones a través de la API del kernel
- Asignación y gestión de SPI (Índice de Parámetro de Seguridad)
- Asignación de puertos para tráfico protegido

2.2.2 Capacidades de Configuración IPsec

Selección de Conjuntos de Cifrado:

Puedes configurar el P-CSCF para preferir conjuntos de cifrado específicos:

Preferidos (seguridad fuerte):

- ESP con AES-256-GCM y HMAC-SHA256
- ESP con AES-256-CBC y HMAC-SHA256

Soportados (compatibilidad):

- ESP con AES-128-CBC y HMAC-SHA1
- ESP con 3DES-CBC y HMAC-SHA1 (heredado)

Gestión de Claves:

- IKE (Intercambio de Claves de Internet) NO se utiliza
- Claves proporcionadas a través de IMS AKA (CK/IK de HSS)
- Configuración manual de asociación de seguridad a través de XFRM del kernel
- Destrucción automática de SA al expirar el registro

Ciclo de Vida del Túnel:

1. UE se registra → autenticación AKA → CK/IK generados
2. P-CSCF recibe CK/IK de S-CSCF
3. P-CSCF asigna par de SPI (SPI del cliente, SPI del servidor)
4. P-CSCF asigna par de puertos (puerto del cliente, puerto del servidor)
5. P-CSCF configura SAs IPsec del kernel utilizando CK/IK
6. P-CSCF envía parámetros IPsec a UE en 200 OK (encabezado Security-Server)
7. UE configura SAs IPsec con los mismos parámetros
8. Todo el tráfico SIP subsiguiente fluye a través de túneles ESP
9. Al expirar el registro o al desregistro: SAs eliminadas, recursos liberados

2.3 Cifrado TLS (SIP y Diameter)

2.3.1 TLS para SIP (SIPS)

Versiones TLS Soportadas:

- **TLS 1.2** (RFC 5246) - Soportado
- **TLS 1.3** (RFC 8446) - Soportado (si hay soporte del kernel/biblioteca)
- **TLS 1.0/1.1** - Obsoleto (deshabilitado por defecto)
- **SSL 2.0/3.0** - NO SOPORTADO (vulnerabilidades conocidas)

Implementación de TLS:

El sistema utiliza OpenSSL o LibreSSL:

- Bibliotecas TLS estándar de la industria

- Implementaciones criptográficamente validadas
- Actualizaciones de seguridad regulares

Conjuntos de Cifrado Soportados:

TLS 1.3 (Preferido):

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (Soportado):

- ECDHE-RSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- ECDHE-RSA-AES128-GCM-SHA256 (Perfect Forward Secrecy)
- ECDHE-ECDSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- DHE-RSA-AES256-GCM-SHA384 (Perfect Forward Secrecy)
- DHE-RSA-AES128-GCM-SHA256 (Perfect Forward Secrecy)

Cifrados débiles deshabilitados:

- Sin RC4
- Sin MD5
- Sin cifrado NULL
- Sin cifrados de grado EXPORT
- Sin DES/3DES (obsoleto)

Soporte de Certificados:

- **Certificados X.509** (formato estándar)
- **Claves RSA:** mínimo de 2048 bits, recomendado 4096 bits
- **Claves ECDSA:** curvas P-256, P-384, P-521 soportadas
- **Validación de cadena de certificados**
- **Verificación de CRL (Lista de Revocación de Certificados)** (opcional)
- **OCSP (Protocolo de Estado de Certificado en Línea)** (opcional)

Características de TLS:

- **Perfect Forward Secrecy (PFS):** A través de intercambio de claves ECDHE/DHE
- **Indicación de Nombre del Servidor (SNI):** Soportado
- **Reanudación de Sesión TLS:** Soportada (optimización de rendimiento)
- **Autenticación de Certificado del Cliente:** Soportada (TLS mutuo)

SIP sobre TLS (SIPS):

- Transporte: TCP con cifrado TLS
- Puerto: 5061 (puerto estándar SIPS)
- Utilizado para comunicación inter-CSCF (opcional)
- Utilizado para conexiones de red de confianza

2.3.2 TLS para Diameter

Capacidades Diameter:

El sistema soporta lo siguiente:

- **Diameter sobre SCTP** (preferido por fiabilidad)
- **Diameter sobre TCP con TLS**
- **Puerto:** 3868 (puerto estándar Diameter)

Casos de Uso:

- **Interfaz Cx:** S-CSCF/I-CSCF a HSS (datos de suscriptor, autenticación)
- **Interfaz Rx:** P-CSCF a PCRF (política de QoS)
- **Interfaz Ro:** S-CSCF a OCS (cobro en línea - si está habilitado)

Configuración TLS para Diameter:

Los mismos conjuntos de cifrado que SIP

- TLS 1.2/1.3
- Intercambio de claves ECDHE/DHE (PFS)
- Cifrado AES-GCM
- Autenticación SHA256/SHA384

Autenticación Basada en Certificados:

- Los pares Diameter se autentican a través de certificados TLS
- TLS mutuo (certificados tanto del cliente como del servidor)
- Validación de FQDN (Nombre de Dominio Totalmente Calificado) en certificados
- Validación de cadena CA de confianza

2.4 Criptografía de Autenticación

2.4.1 Funciones Criptográficas IMS AKA

Algoritmo 3GPP AKA (MILENAGE):

Utilizado para generar vectores de autenticación (RAND, AUTN, XRES, CK, IK):

Funciones Criptográficas:

- **f1:** Función de autenticación de mensajes (calcular MAC-A y MAC-S)
- **f2:** Función de respuesta (calcular RES a partir de RAND y K)
- **f3:** Derivación de clave de cifrado (calcular CK)
- **f4:** Derivación de clave de integridad (calcular IK)
- **f5:** Función de clave de anonimato (calcular AK para privacidad de IMSI)

Material de Clave:

- **K:** Clave permanente de suscriptor de 128 bits (almacenada en ISIM y HSS)
- **OPc:** Clave variante del operador (derivada de K y OP)
- **RAND:** Desafío aleatorio de 128 bits
- **SQN:** Número de secuencia de 48 bits (protección contra repetición)

Secuencia AKA:

1. HSS genera RAND (aleatorio criptográficamente)
2. HSS calcula MAC-A = f1(K, RAND, SQN, AMF)
3. HSS calcula AUTN = (SQN ⊕ AK) || AMF || MAC-A
4. HSS calcula XRES = f2(K, RAND)

5. HSS calcula CK = f3(K, RAND)
6. HSS calcula IK = f4(K, RAND)
7. HSS envía {RAND, AUTN, XRES, CK, IK} a S-CSCF
8. S-CSCF desafía a UE con RAND y AUTN
9. UE calcula RES = f2(K, RAND) usando ISIM
10. UE envía RES a S-CSCF
11. S-CSCF compara RES con XRES (validación de autenticación)

Propiedades de Seguridad:

- **Autenticación Mutua:** UE verifica HSS a través de AUTN, HSS verifica UE a través de RES
- **Frescura de Clave:** RAND es aleatorio, SQN previene repetición
- **Derivación de Clave:** CK e IK derivadas de la clave compartida K

2.4.2 Autenticación Digest HTTP

Para autenticación no IMS (si se utiliza):

Algoritmo: MD5 (RFC 2617)

- **Función Hash:** MD5 (salida de 128 bits)
- **Desafío-Respuesta:** Basado en nonce
- **Protección contra Repetición:** Nonce con marca de tiempo

Nota: HTTP Digest con MD5 se considera débil. IMS AKA es fuertemente preferido.

2.5 Hashing e Integridad

2.5.1 Funciones Hash Disponibles

El sistema puede usar las siguientes funciones hash (a través de OpenSSL/crypto del kernel):

- **SHA-256:** salida de 256 bits, recomendado
- **SHA-384:** salida de 384 bits
- **SHA-512:** salida de 512 bits

- **SHA-1:** salida de 160 bits, obsoleto para uso de seguridad
- **MD5:** salida de 128 bits, obsoleto para uso de seguridad

Uso:

- Construcciones HMAC para IPsec/TLS
- Verificación de integridad de datos
- Generación de nonce
- Detección de duplicados (hashing de Call-ID)

2.5.2 Integridad del Mensaje

Integridad del Mensaje SIP:

- **IPsec ESP:** HMAC-SHA256 para SIP autenticado sobre IPsec
- **TLS:** Autenticación de mensajes a través de TLS MAC
- **Digest SIP:** Integridad del encabezado de autenticación

Integridad del Mensaje Diameter:

- **TLS:** Diameter sobre TLS proporciona autenticación de mensajes
- **HMAC:** Los mensajes Diameter pueden incluir AVPs HMAC para integridad

2.6 Generación de Números Aleatorios

Generación de Números Aleatorios Criptográficamente Segura:

El sistema se basa en lo siguiente:

- **Linux kernel /dev/urandom:** PRNG seguro criptográficamente
- **OpenSSL RAND_bytes():** CSPRNG (Generador de Números Pseudo-Aleatorios Criptográficamente Seguro)

Uso:

- Asignación de SPI (valor inicial aleatorio)
- Generación de Call-ID
- Generación de par��metros de rama

- Generación de nonce para autenticación
- Generación de ID de sesión

2.7 Gestión de Claves

2.7.1 Gestión de Certificados TLS

Almacenamiento de Certificados:

- Almacenamiento en el sistema de archivos con permisos restringidos (0600)
- Ubicado en: `/etc/system/tls/`
- Formato PEM para certificados y claves

Generación de Certificados:

```
# Generar clave privada RSA de 4096 bits
openssl genrsa -out system-key.pem 4096

# Generar CSR (Solicitud de Firma de Certificado)
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

# Certificado autofirmado (desarrollo/pruebas)
openssl x509 -req -days 365 -in system.csr \
  -signkey system-key.pem -out system-cert.pem

# Producción: Enviar CSR a CA de confianza
```

Rotación de Certificados:

- Se recomienda la renovación anual de certificados
- Reinicio del servicio de manera controlada para cargar nuevos certificados
- No se requiere tiempo de inactividad

2.7.2 Gestión de Claves IPsec

Derivación de Claves:

- CK (Clave de Cifrado) e IK (Clave de Integridad) de IMS AKA
- Claves de 128 bits de HSS
- Entregadas de manera segura a través de Diameter Cx (sobre TLS)

Vida Útil de la Clave:

- Vinculada a la expiración del registro SIP (típicamente 599 segundos)
- Re-keying en la actualización del registro
- Destrucción automática de claves al desregistrarse

Almacenamiento de Claves:

- Efímero (solo en memoria durante el registro activo)
- Instaladas en la pila IPsec del kernel
- Sin almacenamiento persistente de claves
- Claves descartadas cuando se elimina SA

2.8 Resistencia al Criptoanálisis

2.8.1 Selección de Algoritmos

Defensa Contra Criptoanálisis:

- **Sin algoritmos personalizados:** Solo algoritmos estándar de la industria, revisados por pares
- **Tamaños de clave fuertes:** AES-256, RSA-4096, SHA-256
- **Cifrado autenticado:** AES-GCM (AEAD - Cifrado Autenticado con Datos Asociados)
- **Perfect Forward Secrecy:** ECDHE/DHE en TLS
- **Actualizaciones regulares:** Parches de seguridad de OpenSSL/LibreSSL aplicados

Algoritmos Obsoletos Deshabilitados:

- MD5 (colisiones de hash)
- RC4 (debilidades del cifrado de flujo)
- DES/3DES (tamaño de bloque pequeño, longitud de clave)

- SSL 2.0/3.0 (vulnerabilidades del protocolo)
- TLS 1.0/1.1 (ataques BEAST, POODLE)

2.8.2 Mitigación de Ataques de Canal Lateral

Resistencia a Ataques de Tiempo:

- Comparación en tiempo constante para respuestas de autenticación
- Sin filtraciones de tiempo en operaciones criptográficas (a través de OpenSSL)

Protección de Memoria:

- Aislamiento de la pila IPsec del kernel
- Aislamiento de memoria de procesos
- Sin intercambio para datos sensibles (si está configurado)

2.9 Cumplimiento y Normas

Cumplimiento de Normas Criptográficas:

- **NIST SP 800-52:** Directrices TLS
- **NIST SP 800-131A:** Transiciones de algoritmos criptográficos
- **RFC 7525:** Recomendaciones TLS
- **ETSI TS 133 203:** Seguridad de acceso 3GPP (IMS AKA)
- **ETSI TS 133 210:** Seguridad de la capa de red IP (IPsec)
- **3GPP TS 33.203:** Seguridad de acceso para IMS
- **3GPP TS 33.210:** Seguridad del dominio de la red

Regulaciones Francesas sobre Criptografía:

- Sin criptografía restringida para exportación (todos los algoritmos estándar)
- Medios criptográficos estándar (sin puertas traseras gubernamentales)
- Certificación de productos criptográficos ANSSI (si es necesario)

Referencia de Métricas IMS CSCF

Este documento es la referencia para todas las métricas que exportan los componentes P-CSCF, I-CSCF y S-CSCF.

Acceso a Métricas

Todos los componentes CSCF exponen métricas de Prometheus en el puerto 9090:

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

Cada host CSCF (P-CSCF, I-CSCF, S-CSCF) exporta sus propias métricas. Para obtener una cobertura de monitoreo completa, configure su servidor Prometheus para raspar todos los hosts.

Ejemplo de Configuración de 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 obtener orientación sobre monitoreo y alertas, consulte:

- Monitoreo a través de OmniWeb y Grafana

Monitoreo a través de OmniWeb y Grafana

Vea el estado operativo en **OmniWeb**, el portal de gestión unificado: <https://docs.omnitouch.com.au/docs/repos/Platform/OmniWeb/>. El estado operativo incluye registros, diálogos y estado de pares de Diameter. OmniWeb integra paneles de Grafana para visibilidad en tiempo real e histórica. Estos paneles incluyen vistas de registro de S-CSCF y ubicación de usuarios. Las métricas `ims_usrloc_scscf_active_impus` y `ims_usrloc_scscf_active_contacts` respaldan estas vistas. Los paneles también muestran el estado de los pares de Diameter y la profundidad de la cola. La métrica `cdp_queuelength` y las métricas de interfaz `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_registrar_scscf_sar_*` y `ims_qos_*` respaldan estas vistas.

Las métricas de Prometheus en esta referencia respaldan esos paneles de Grafana. También respaldan cualquier alerta personalizada que configure.

Métricas P-CSCF

Métricas CDP (Diameter)

Nombre de Métrica	Significado
`cdp_average_response_time`	Tiempo promedio de respuesta para solicitudes de Diameter en milisegundos (calculado como replies_response_time / replies_received)
`cdp_queuelength`	Longitud actual de la cola de tareas del trabajador de Diameter
`cdp_replies_received`	Número total de respuestas de Diameter recibidas
`cdp_replies_response_time`	Tiempo total gastado esperando respuestas de Diameter en milisegundos
`cdp_timeout`	Número de eventos de tiempo de espera en solicitudes de Diameter

Estadísticas SIP del Núcleo

Contadores de Solicitudes

Nombre de Métrica	Significado
`core_rcv_requests`	Número total de solicitudes SIP recibidas
`core_rcv_requests_ack`	Número de solicitudes ACK recibidas
`core_rcv_requests_bye`	Número de solicitudes BYE recibidas
`core_rcv_requests_cancel`	Número de solicitudes CANCEL recibidas
`core_rcv_requests_info`	Número de solicitudes INFO recibidas
`core_rcv_requests_invite`	Número de solicitudes INVITE recibidas
`core_rcv_requests_message`	Número de solicitudes MESSAGE recibidas
`core_rcv_requests_notify`	Número de solicitudes NOTIFY recibidas
`core_rcv_requests_options`	Número de solicitudes OPTIONS recibidas
`core_rcv_requests_prack`	Número de solicitudes PRACK recibidas
`core_rcv_requests_publish`	Número de solicitudes PUBLISH recibidas
`core_rcv_requests_refer`	Número de solicitudes REFER recibidas
`core_rcv_requests_register`	Número de solicitudes REGISTER recibidas
`core_rcv_requests_subscribe`	Número de solicitudes SUBSCRIBE recibidas
`core_rcv_requests_update`	Número de solicitudes UPDATE recibidas

Contadores de Respuestas (General)

Nombre de Métrica	Significado
`core_rcv_replies`	Número total de respuestas SIP recibidas
`core_rcv_replies_18x`	Número de respuestas provisionales 180/181/183/186/187/189 recibidas
`core_rcv_replies_1xx`	Número de respuestas 1xx (provisionales) recibidas
`core_rcv_replies_2xx`	Número de respuestas 2xx (éxito) recibidas
`core_rcv_replies_3xx`	Número de respuestas 3xx (redirección) recibidas
`core_rcv_replies_4xx`	Número de respuestas 4xx (error del cliente) recibidas
`core_rcv_replies_5xx`	Número de respuestas 5xx (error del servidor) recibidas
`core_rcv_replies_6xx`	Número de respuestas 6xx (fallo global) recibidas

Contadores de Respuestas por Método (1xx)

Nombre de Métrica	Significado
`core_rcv_replies_1xx_bye`	Número de respuestas 1xx a solicitudes BYE
`core_rcv_replies_1xx_cancel`	Número de respuestas 1xx a solicitudes CANCEL
`core_rcv_replies_1xx_invite`	Número de respuestas 1xx a solicitudes INVITE
`core_rcv_replies_1xx_message`	Número de respuestas 1xx a solicitudes MESSAGE
`core_rcv_replies_1xx_prack`	Número de respuestas 1xx a solicitudes PRACK
`core_rcv_replies_1xx_refer`	Número de respuestas 1xx a solicitudes REFER
`core_rcv_replies_1xx_reg`	Número de respuestas 1xx a solicitudes REGISTER
`core_rcv_replies_1xx_update`	Número de respuestas 1xx a solicitudes UPDATE

Contadores de Respuestas por Método (2xx)

Nombre de Métrica	Significado
`core_rcv_replies_2xx_bye`	Número de respuestas 2xx (éxito) a solicitudes BYE
`core_rcv_replies_2xx_cancel`	Número de respuestas 2xx (éxito) a solicitudes CANCEL
`core_rcv_replies_2xx_invite`	Número de respuestas 2xx (éxito) a solicitudes INVITE
`core_rcv_replies_2xx_message`	Número de respuestas 2xx (éxito) a solicitudes MESSAGE
`core_rcv_replies_2xx_prack`	Número de respuestas 2xx (éxito) a solicitudes PRACK
`core_rcv_replies_2xx_refer`	Número de respuestas 2xx (éxito) a solicitudes REFER
`core_rcv_replies_2xx_reg`	Número de respuestas 2xx (éxito) a solicitudes REGISTER
`core_rcv_replies_2xx_update`	Número de respuestas 2xx (éxito) a solicitudes UPDATE

Contadores de Respuestas por Método (3xx)

Nombre de Métrica	Significado
`core_rcv_replies_3xx_bye`	Número de respuestas 3xx (redirección) a solicitudes BYE
`core_rcv_replies_3xx_cancel`	Número de respuestas 3xx (redirección) a solicitudes CANCEL
`core_rcv_replies_3xx_invite`	Número de respuestas 3xx (redirección) a solicitudes INVITE
`core_rcv_replies_3xx_message`	Número de respuestas 3xx (redirección) a solicitudes MESSAGE
`core_rcv_replies_3xx_prack`	Número de respuestas 3xx (redirección) a solicitudes PRACK
`core_rcv_replies_3xx_refer`	Número de respuestas 3xx (redirección) a solicitudes REFER
`core_rcv_replies_3xx_reg`	Número de respuestas 3xx (redirección) a solicitudes REGISTER
`core_rcv_replies_3xx_update`	Número de respuestas 3xx (redirección) a solicitudes UPDATE

Contadores de Respuestas por Método (4xx)

Nombre de Métrica	Significado
`core_rcv_replies_4xx_bye`	Número de respuestas 4xx (error del cliente) a solicitudes BYE
`core_rcv_replies_4xx_cancel`	Número de respuestas 4xx (error del cliente) a solicitudes CANCEL
`core_rcv_replies_4xx_invite`	Número de respuestas 4xx (error del cliente) a solicitudes INVITE
`core_rcv_replies_4xx_message`	Número de respuestas 4xx (error del cliente) a solicitudes MESSAGE
`core_rcv_replies_4xx_prack`	Número de respuestas 4xx (error del cliente) a solicitudes PRACK
`core_rcv_replies_4xx_refer`	Número de respuestas 4xx (error del cliente) a solicitudes REFER
`core_rcv_replies_4xx_reg`	Número de respuestas 4xx (error del cliente) a solicitudes REGISTER
`core_rcv_replies_4xx_update`	Número de respuestas 4xx (error del cliente) a solicitudes UPDATE

Contadores de Respuestas por Método (5xx)

Nombre de Métrica	Significado
`core_rcv_replies_5xx_bye`	Número de respuestas 5xx (error del servidor) a solicitudes BYE
`core_rcv_replies_5xx_cancel`	Número de respuestas 5xx (error del servidor) a solicitudes CANCEL
`core_rcv_replies_5xx_invite`	Número de respuestas 5xx (error del servidor) a solicitudes INVITE
`core_rcv_replies_5xx_message`	Número de respuestas 5xx (error del servidor) a solicitudes MESSAGE
`core_rcv_replies_5xx_prack`	Número de respuestas 5xx (error del servidor) a solicitudes PRACK
`core_rcv_replies_5xx_refer`	Número de respuestas 5xx (error del servidor) a solicitudes REFER
`core_rcv_replies_5xx_reg`	Número de respuestas 5xx (error del servidor) a solicitudes REGISTER
`core_rcv_replies_5xx_update`	Número de respuestas 5xx (error del servidor) a solicitudes UPDATE

Contadores de Respuestas por Método (6xx)

Nombre de Métrica	Significado
`core_rcv_replies_6xx_bye`	Número de respuestas 6xx (fallo global) a solicitudes BYE
`core_rcv_replies_6xx_cancel`	Número de respuestas 6xx (fallo global) a solicitudes CANCEL
`core_rcv_replies_6xx_invite`	Número de respuestas 6xx (fallo global) a solicitudes INVITE
`core_rcv_replies_6xx_message`	Número de respuestas 6xx (fallo global) a solicitudes MESSAGE
`core_rcv_replies_6xx_prack`	Número de respuestas 6xx (fallo global) a solicitudes PRACK
`core_rcv_replies_6xx_refer`	Número de respuestas 6xx (fallo global) a solicitudes REFER
`core_rcv_replies_6xx_reg`	Número de respuestas 6xx (fallo global) a solicitudes REGISTER
`core_rcv_replies_6xx_update`	Número de respuestas 6xx (fallo global) a solicitudes UPDATE

Contadores de Códigos de Estado Específicos

Nombre de Métrica	Significado
`core_rcv_replies_400`	Número de respuestas 400 Bad Request recibidas
`core_rcv_replies_401`	Número de respuestas 401 Unauthorized recibidas
`core_rcv_replies_402`	Número de respuestas 402 Payment Required recibidas
`core_rcv_replies_403`	Número de respuestas 403 Forbidden recibidas
`core_rcv_replies_404`	Número de respuestas 404 Not Found recibidas
`core_rcv_replies_405`	Número de respuestas 405 Method Not Allowed recibidas
`core_rcv_replies_406`	Número de respuestas 406 Not Acceptable recibidas
`core_rcv_replies_407`	Número de respuestas 407 Proxy Authentication Required recibidas
`core_rcv_replies_408`	Número de respuestas 408 Request Timeout recibidas
`core_rcv_replies_409`	Número de respuestas 409 Conflict recibidas
`core_rcv_replies_410`	Número de respuestas 410 Gone recibidas
`core_rcv_replies_411`	Número de respuestas 411 Length Required recibidas
`core_rcv_replies_413`	Número de respuestas 413 Request Entity Too Large recibidas

Nombre de Métrica	Significado
`core_rcv_replies_414`	Número de respuestas 414 Request-URI Too Long recibidas
`core_rcv_replies_415`	Número de respuestas 415 Unsupported Media Type recibidas
`core_rcv_replies_420`	Número de respuestas 420 Bad Extension recibidas
`core_rcv_replies_480`	Número de respuestas 480 Temporarily Unavailable recibidas
`core_rcv_replies_481`	Número de respuestas 481 Call/Transaction Does Not Exist recibidas
`core_rcv_replies_482`	Número de respuestas 482 Loop Detected recibidas
`core_rcv_replies_483`	Número de respuestas 483 Too Many Hops recibidas
`core_rcv_replies_484`	Número de respuestas 484 Address Incomplete recibidas
`core_rcv_replies_485`	Número de respuestas 485 Ambiguous recibidas
`core_rcv_replies_486`	Número de respuestas 486 Busy Here recibidas
`core_rcv_replies_487`	Número de respuestas 487 Request Terminated recibidas
`core_rcv_replies_488`	Número de respuestas 488 Not Acceptable Here recibidas
`core_rcv_replies_489`	Número de respuestas 489 Bad Event recibidas

Nombre de Métrica	Significado
`core_rcv_replies_491`	Número de respuestas 491 Request Pending recibidas
`core_rcv_replies_493`	Número de respuestas 493 Undecipherable recibidas

Estadísticas de Reenvío y Error

Nombre de Métrica	Significado
`core_fwd_replies`	Número de respuestas SIP reenviadas
`core_fwd_requests`	Número de solicitudes SIP reenviadas
`core_drop_replies`	Número de respuestas SIP descartadas
`core_drop_requests`	Número de solicitudes SIP descartadas
`core_err_replies`	Número de respuestas de error
`core_err_requests`	Número de solicitudes de error
`core_bad_URIs_rcvd`	Número de mensajes con URIs malformados recibidos
`core_bad_msg_hdr`	Número de mensajes con encabezados malos/malformados
`core_unsupported_methods`	Número de solicitudes con métodos SIP no soportados

Seguimiento de Diálogos

Nombre de Métrica	Significado
`dialog_ng_active`	Número de diálogos actualmente activos (respondidos/confirmados)
`dialog_ng_early`	Número de diálogos tempranos (sonando/estado provisional)
`dialog_ng_expired`	Número de diálogos que han expirado o sido terminados forzosamente
`dialog_ng_processed`	Número total de diálogos procesados desde el inicio

Estadísticas de DNS

Nombre de Métrica	Significado
`dns_failed_dns_request`	Número de consultas DNS fallidas
`dns_slow_dns_request`	Número de consultas DNS lentas (excediendo el umbral)

IMS IPSec P-CSCF

Nombre de Métrica	Significado
`ims_ipsec_pcscf_spi_free`	Número de valores SPI (Índice de Parámetro de Seguridad) libres disponibles para asignación
`ims_ipsec_pcscf_spi_total`	Capacidad total de SPI configurada para el sistema
`ims_ipsec_pcscf_spi_used`	Número de valores SPI actualmente asignados/usados
`ims_ipsec_pcscf_spi_utilization_pct`	Porcentaje de utilización del grupo de SPI
`ims_ipsec_pcscf_worker_cache_size`	Tamaño de la caché IPSec del proceso trabajador

IMS QoS (Interfaz Rx)

Métricas de Registro AAR

Nombre de Métrica	Significado
`ims_qos_active_registration_rx_sessions`	Número de sesiones de registro Rx actualmente activas
`ims_qos_registration_aars`	Número total de mensajes AAR (Solicitud de Autorización-Autenticación) de registro enviados
`ims_qos_successful_registration_aars`	Número de transacciones AAR de registro exitosas
`ims_qos_failed_registration_aars`	Número de transacciones AAR de registro fallidas
`ims_qos_registration_aar_avg_response_time`	Tiempo promedio de respuesta para mensajes AAR de registro en milisegundos
`ims_qos_registration_aar_response_time`	Tiempo total de respuesta para todos los mensajes AAR de registro en milisegundos
`ims_qos_registration_aar_replies_received`	Número total de respuestas AAR de registro recibidas
`ims_qos_registration_aar_timeouts`	Número de tiempos de espera de solicitudes AAR de registro

Métricas de AAR de Medios

Nombre de Métrica	Significado
`ims_qos_active_media_rx_sessions`	Número de sesiones de medios Rx actualmente activas
`ims_qos_media_rx_sessions`	Número total de sesiones de medios Rx creadas
`ims_qos_media_aars`	Número total de mensajes AAR de medios enviados
`ims_qos_successful_media_aars`	Número de transacciones AAR de medios exitosas
`ims_qos_failed_media_aars`	Número de transacciones AAR de medios fallidas
`ims_qos_media_aar_avg_response_time`	Tiempo promedio de respuesta para mensajes AAR de medios en milisegundos
`ims_qos_media_aar_response_time`	Tiempo total de respuesta para todos los mensajes AAR de medios en milisegundos
`ims_qos_media_aar_replies_received`	Número total de respuestas AAR de medios recibidas
`ims_qos_media_aar_timeouts`	Número de tiempos de espera de solicitudes AAR de medios

Métricas ASR

Nombre de Métrica	Significado
`ims_qos_asrs`	Número total de mensajes ASR (Solicitud de Abort-Session) recibidos del PCRF

Ubicación de Usuario P-CSCF

Nombre de Métrica	Significado
`ims_usrloc_pcscf_expired_contacts`	Número de enlaces de contacto expirados
`ims_usrloc_pcscf_registered_contacts`	Número de enlaces de contacto actualmente registrados
`ims_usrloc_pcscf_registered_impus`	Número de IMPUs (Identidades de Usuario Público IMS) actualmente registrados

Base de Datos MySQL

Nombre de Métrica	Significado
`mysql_driver_errors`	Número de errores de conexión/controlador de MySQL

Anti-Flood (Bloqueo de IP)

Nombre de Métrica	Significado
`pike_blocked_ips`	Número de direcciones IP actualmente bloqueadas (detección de inundación)

Módulo Registrador

Nombre de Métrica	Significado
`registrar_accepted_regs`	Número de solicitudes REGISTER aceptadas
`registrar_rejected_regs`	Número de solicitudes REGISTER rechazadas
`registrar_default_expire`	Tiempo de expiración predeterminado para registros en segundos
`registrar_default_expires_range`	Configuración del rango de expiración predeterminado
`registrar_expires_range`	Rango de expiración configurado
`registrar_max_contacts`	Número máximo de contactos permitidos por AOR
`registrar_max_expires`	Tiempo máximo de expiración permitido en segundos

Estadísticas de Script

Nombre de Métrica	Significado
`script_register_failed`	Número de intentos de registro que fallaron en la lógica del script de enrutamiento
`script_register_success`	Número de registros exitosos procesados por el script de enrutamiento
`script_register_time`	Tiempo total gastado procesando registros en el script de enrutamiento (milisegundos)

Transporte SCTP

Nombre de Métrica	Significado
`sctp_assoc_shutdown`	Número de apagados de asociación SCTP iniciados localmente
`sctp_comm_lost`	Número de asociaciones SCTP perdidas debido a fallos de comunicación
`sctp_connect_failed`	Número de intentos de asociación SCTP salientes fallidos
`sctp_current_opened_connections`	Número de asociaciones SCTP actualmente abiertas
`sctp_current_tracked_connections`	Número de asociaciones SCTP actualmente rastreadas
`sctp_established`	Número total de asociaciones SCTP establecidas
`sctp_local_reject`	Número de asociaciones SCTP entrantes rechazadas localmente
`sctp_remote_shutdown`	Número de apagados de asociación SCTP iniciados por pares
`sctp_send_failed`	Número de operaciones de envío SCTP que fallaron
`sctp_send_force_retry`	Número de reintentos forzados en envíos SCTP fallidos
`sctp_sendq_full`	Número de intentos de envío que fallaron debido a la cola de envío

Nombre de Métrica	Significado
	llena

Memoria Compartida

Nombre de Métrica	Significado
`shmem_fragments`	Número de fragmentos en el grupo de memoria compartida (indica fragmentación)
`shmem_free_size`	Cantidad de memoria compartida libre en bytes
`shmem_max_used_size`	Máxima memoria compartida utilizada desde el inicio en bytes
`shmem_real_used_size`	Memoria compartida realmente utilizada incluyendo sobrecarga del asignador en bytes
`shmem_total_size`	Tamaño total del grupo de memoria compartida en bytes
`shmem_used_size`	Memoria compartida actualmente utilizada (solo datos de usuario) en bytes

Módulo SL (Sin Estado)

Contadores de Respuestas Sin Estado por Clase

Nombre de Métrica	Significado
`sl_1xx_replies`	Número de respuestas sin estado 1xx enviadas
`sl_2xx_replies`	Número de respuestas sin estado 2xx enviadas
`sl_3xx_replies`	Número de respuestas sin estado 3xx enviadas
`sl_4xx_replies`	Número de respuestas sin estado 4xx enviadas
`sl_5xx_replies`	Número de respuestas sin estado 5xx enviadas
`sl_6xx_replies`	Número de respuestas sin estado 6xx enviadas
`sl_xxx_replies`	Número de otras respuestas sin estado enviadas

Contadores de Respuestas Sin Estado Específicos

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

Nombre de Métrica	Significado
`sl_500_replies`	Número de respuestas sin estado 500 Server Internal Error enviadas

Estadísticas Generales Sin Estado

Nombre de Métrica	Significado
`sl_sent_replies`	Número total de respuestas sin estado enviadas
`sl_sent_err_replies`	Número de respuestas de error sin estado enviadas
`sl_received_ACKs`	Número de mensajes ACK recibidos para transacciones sin estado
`sl_failures`	Número de fallos en el envío de respuestas sin estado

Transporte TCP

Nombre de Métrica	Significado
`tcp_con_reset`	Número de conexiones TCP reiniciadas (RST recibido en conexión establecida)
`tcp_con_timeout`	Número de conexiones TCP cerradas debido a tiempo de inactividad
`tcp_connect_failed`	Número de intentos de conexión TCP salientes fallidos
`tcp_connect_success`	Número de conexiones TCP salientes exitosas
`tcp_current_opened_connections`	Número de conexiones TCP actualmente abiertas
`tcp_current_write_queue_size`	Tamaño total actual de las colas de escritura TCP en todas las conexiones
`tcp_established`	Número total de conexiones TCP establecidas (tanto entrantes como salientes)
`tcp_local_reject`	Número de conexiones TCP entrantes rechazadas localmente
`tcp_passive_open`	Número de conexiones TCP entrantes aceptadas
`tcp_send_timeout`	Número de operaciones de envío TCP que se agotaron (modo asíncrono)
`tcp_sendq_full`	Número de intentos de envío que fallaron porque la cola de envío estaba

Nombre de Métrica	Significado
	llena

Módulo TM/TMX (Transacción)

Contadores de Tipos de Transacción

Nombre de Métrica	Significado
`tmx_UAC_transactions`	Número de transacciones UAC (cliente) creadas
`tmx_UAS_transactions`	Número de transacciones UAS (servidor) creadas
`tmx_active_transactions`	Número de transacciones actualmente activas
`tmx_inuse_transactions`	Número de transacciones actualmente en uso

Finalización de Transacciones por Estado

Nombre de Métrica	Significado
`tmx_2xx_transactions`	Número de transacciones completadas con respuesta 2xx
`tmx_3xx_transactions`	Número de transacciones completadas con respuesta 3xx
`tmx_4xx_transactions`	Número de transacciones completadas con respuesta 4xx
`tmx_5xx_transactions`	Número de transacciones completadas con respuesta 5xx
`tmx_6xx_transactions`	Número de transacciones completadas con respuesta 6xx

Estadísticas de Respuestas de Transacción

Nombre de Métrica	Significado
`tmx_rpl_absorbed`	Número de respuestas absorbidas por la capa de transacción (duplicados)
`tmx_rpl_generated`	Número de respuestas generadas localmente por el módulo de transacción
`tmx_rpl_received`	Número de respuestas recibidas para transacciones
`tmx_rpl_relayed`	Número de respuestas retransmitidas por el módulo de transacción
`tmx_rpl_sent`	Número de respuestas enviadas por el módulo de transacción

Ubicación de Usuario

Nombre de Métrica	Significado
`usrloc_location_contacts`	Número de contactos en el dominio 'location' (módulo usrloc estándar)
`usrloc_location_expires`	Número de contactos expirados en el dominio 'location'
`usrloc_registered_users`	Número de usuarios/AORs (Dirección de Registros) registrados

---

Métricas I-CSCF

El I-CSCF comparte la mayoría de las estadísticas SIP del núcleo con el P-CSCF. Consulte la sección de Estadísticas SIP del Núcleo del P-CSCF anterior. Las métricas a continuación son específicas del I-CSCF.

Contexto Operativo I-CSCF

El I-CSCF mantiene una lista de instancias S-CSCF disponibles para balanceo de carga. Para un nuevo registro, el I-CSCF consulta el HSS para seleccionar la instancia S-CSCF correcta. Las métricas UAR y LIR a continuación rastrean el éxito de estas operaciones.

IMS I-CSCF (Interfaz Cx - Comunicación HSS)

El I-CSCF utiliza la interfaz Diameter Cx para comunicarse con el HSS (Servidor de Suscriptor Local). Envía consultas de ubicación de usuario y autorización.

Métricas UAR (Solicitud de Autorización de Usuario)

Nombre de Métrica	Significado
`ims_icscf_uar_avg_response_time`	Tiempo promedio de respuesta para mensajes UAR en milisegundos (calculado como uar_replies_response_time / uar_replies_received)
`ims_icscf_uar_replies_received`	Número total de respuestas UAA (Respuesta de Autorización de Usuario) recibidas del HSS
`ims_icscf_uar_replies_response_time`	Tiempo total de respuesta para todos los mensajes UAR en milisegundos
`ims_icscf_uar_timeouts`	Número de tiempos de espera de solicitudes UAR

Métricas LIR (Solicitud de Información de Ubicación)

Nombre de Métrica	Significado
`ims_icscf_lir_avg_response_time`	Tiempo promedio de respuesta para mensajes LIR en milisegundos (calculado como lir_replies_response_time / lir_replies_received)
`ims_icscf_lir_replies_received`	Número total de respuestas LIA (Respuesta de Información de Ubicación) recibidas del HSS
`ims_icscf_lir_replies_response_time`	Tiempo total de respuesta para todos los mensajes LIR en milisegundos
`ims_icscf_lir_timeouts`	Número de tiempos de espera de solicitudes LIR

Métricas Comunes

El I-CSCF también exporta las métricas comunes a continuación. La sección P-CSCF anterior documenta estas métricas.

- **Métricas CDP (Diameter)** - Estadísticas del protocolo Diameter
- **Estadísticas SIP del Núcleo** - Contadores de solicitudes/respuestas por método y código de estado
- **Estadísticas de DNS** - Métricas de consultas DNS
- **Base de Datos MySQL** - Errores de conexión a la base de datos
- **Anti-Flood** - Estadísticas de bloqueo de IP
- **Memoria Compartida** - Estadísticas de uso de memoria
- **Módulo SL (Sin Estado)** - Contadores de respuestas sin estado
- **Transporte TCP** - Estadísticas de conexión TCP
- **Módulo TM/TMX (Transacción)** - Seguimiento del estado de transacciones

Métricas S-CSCF

El S-CSCF comparte la mayoría de las estadísticas SIP del núcleo con el P-CSCF y el I-CSCF. Consulte la sección de Estadísticas SIP del Núcleo del P-CSCF anterior. Las métricas a continuación son específicas del S-CSCF.

Contexto Operativo S-CSCF

El S-CSCF proporciona información detallada sobre la ubicación del usuario. También gestiona IFC (Criterios de Filtro Inicial).

Una búsqueda de ubicación de usuario muestra IMPUs registrados con enlaces de contacto y perfiles de servicio. Las métricas `ims_usrloc_scscf_active_contacts` y `ims_usrloc_scscf_active_impus` rastrean el número de contactos y IMPUs activos.

IFC (Criterios de Filtro Inicial) determina qué Servidores de Aplicaciones procesan sesiones SIP. El rendimiento de la evaluación de IFC puede cambiar los tiempos de configuración de llamadas. Las métricas de transacción (`tmx_*`) rastrean estos tiempos.

IMS ISC (Control de Servicio IMS)

El módulo IMS ISC evalúa los Criterios de Filtro Inicial (iFC). Determina qué Servidores de Aplicaciones deben procesar sesiones SIP. Estas métricas rastrean el rendimiento y el efecto de las operaciones de coincidencia de iFC.

Nombre de Métrica	Significado
`ims_isc_ifc_match_attempts`	Número total de intentos de coincidencia de iFC realizados
`ims_isc_ifc_match_time_total`	Tiempo acumulado gastado realizando operaciones de coincidencia de iFC en milisegundos
`ims_isc_ifc_nomatch_count`	Número de intentos de coincidencia de iFC en los que no coincidió ningún criterio de activación

Monitoreo de Rendimiento: Calcule el tiempo promedio de coincidencia de iFC como `ifc_match_time_total / ifc_match_attempts`. Un tiempo promedio alto puede mostrar criterios de filtro complejos. También puede mostrar un límite de rendimiento en la selección del Servidor de Aplicaciones. Una alta proporción de `ifc_nomatch_count` a `ifc_match_attempts` puede mostrar puntos de activación incorrectos. También puede mostrar patrones de tráfico inesperados.

Autenticación IMS (Interfaz Cx - MAR)

El S-CSCF utiliza la interfaz Diameter Cx para autenticar usuarios con el HSS. Envía un MAR (Solicitud de Autenticación Multimedia).

Nombre de Métrica	Significado
`ims_auth_mar_avg_response_time`	Tiempo promedio de respuesta para mensajes MAR en milisegundos (calculado como mar_replies_response_time / mar_replies_received)
`ims_auth_mar_replies_received`	Número total de respuestas MAA (Respuesta de Autenticación Multimedia) recibidas del HSS
`ims_auth_mar_replies_response_time`	Tiempo total de respuesta para todos los mensajes MAR en milisegundos
`ims_auth_mar_timeouts`	Número de tiempos de espera de solicitudes MAR

Registrador IMS S-CSCF

Estadísticas de Registro

Nombre de Métrica	Significado
`ims_registrar_scscf_accepted_regs`	Número de solicitudes REGISTER aceptadas con éxito
`ims_registrar_scscf_rejected_regs`	Número de solicitudes REGISTER rechazadas
`ims_registrar_scscf_default_expire`	Tiempo de expiración predeterminado para registros en segundos
`ims_registrar_scscf_default_expires_range`	Configuración del rango de expiración predeterminado
`ims_registrar_scscf_max_contacts`	Número máximo de contactos permitidos por registro
`ims_registrar_scscf_max_expires`	Tiempo máximo de expiración permitido en segundos
`ims_registrar_scscf_notifies_in_q`	Número de mensajes NOTIFY pendientes en la cola

Métricas SAR (Solicitud de Asignación de Servidor)

Nombre de Métrica	Significado
`ims_registrar_scscf_sar_avg_response_time`	Tiempo promedio de respuesta para mensaje SAR en milisegundos (calculado como sar_replies_response_ti / sar_replies_received)
`ims_registrar_scscf_sar_replies_received`	Número total de respuestas SAA (Respuesta de Asignaci de Servidor) recibidas d HSS
`ims_registrar_scscf_sar_replies_response_time`	Tiempo total de respues para todos los mensajes SAR en milisegundos
`ims_registrar_scscf_sar_timeouts`	Número de tiempos de espera de solicitudes SA

Ubicación de Usuario S-CSCF

Nombre de Métrica	Significado
`ims_usrloc_scscf_active_contacts`	Número de enlaces de contacto registrados actualmente activos
`ims_usrloc_scscf_active_impus`	Número de IMPUs (Identidades de Usuario Público IMS) registrados actualmente activos
`ims_usrloc_scscf_active_subscriptions`	Número de suscripciones actualmente activas
`ims_usrloc_scscf_contact_collisions`	Número de colisiones de hash en la tabla hash de contactos
`ims_usrloc_scscf_impu_collisions`	Número de colisiones de hash en la tabla hash de IMPU
`ims_usrloc_scscf_subscription_collisions`	Número de colisiones de hash en la tabla hash de suscripciones

Seguimiento de Diálogos

El S-CSCF rastrea el estado del diálogo para llamadas activas:

Nombre de Métrica	Significado
`dialog_ng_active`	Número de diálogos actualmente activos (respondidos/confirmados)
`dialog_ng_early`	Número de diálogos tempranos (sonando/estado provisional)
`dialog_ng_expired`	Número de diálogos que han expirado o sido terminados forzosamente
`dialog_ng_processed`	Número total de diálogos procesados desde el inicio

Métricas Comunes

El S-CSCF también exporta las métricas comunes a continuación. La sección P-CSCF anterior documenta estas métricas.

- **Métricas CDP (Diameter)** - Estadísticas del protocolo Diameter
- **Estadísticas SIP del Núcleo** - Contadores de solicitudes/respuestas por método y código de estado (nota: el S-CSCF enruta entre puntos finales. Generalmente tiene más fwd_requests y fwd_replies.)
- **Estadísticas de DNS** - Métricas de consultas DNS
- **Base de Datos MySQL** - Errores de conexión a la base de datos
- **Anti-Flood** - Estadísticas de bloqueo de IP
- **Memoria Compartida** - Estadísticas de uso de memoria
- **Módulo SL (Sin Estado)** - Contadores de respuestas sin estado
- **Transporte TCP** - Estadísticas de conexión TCP
- **Módulo TM/TMX (Transacción)** - Seguimiento del estado de transacciones (nota: el S-CSCF actúa como cliente y servidor. Generalmente tiene transacciones tanto UAC como UAS.)

Escenarios de Múltiples Identidades (Números Compartidos y Multi-MSISDN)

Esta guía explica cómo OmniCSCF maneja los dos modelos de "un suscriptor, muchas identidades" que IMS soporta. Cubre el registro, la bifurcación de llamadas terminantes, el comportamiento de rechazo de bifurcación y la selección de identidad de llamada de origen. Documenta lo que cada elemento de la red ve.

Los dos modelos son independientes. Un suscriptor puede usar uno, ambos o ninguno.

- **Identidad de Usuario Pública Compartida (un número, varios dispositivos).** Un número es servido por varios dispositivos en SIMs separadas. Un teléfono y un reloj inteligente son el ejemplo común. Cada dispositivo tiene su propio IMSI (identidad privada, IMPI). Los dispositivos comparten una identidad pública (IMPU, el número).
- **Multi-MSISDN (un dispositivo, varios números).** Un suscriptor (un IMSI) tiene varios números. Un número personal y un número de negocio en el mismo dispositivo son el ejemplo común. El dispositivo registra todos sus números como identidades públicas.

Tabla de Contenidos

1. Modelo de Identidad
2. Registro
3. Llamadas Terminantes a un Número Compartido
4. Comportamiento de Rechazo de Bifurcación
5. Lo que Ve el Servidor de Aplicaciones

6. Llamadas Terminantes a un Suscriptor Multi-MSISDN
7. Llamadas de Origen e Identidad de Línea de Llamada
8. Referencia

Modelo de Identidad

3GPP TS 23.228 define el modelo de identidad IMS. Una identidad privada (IMPI) identifica una suscripción para autenticación. Una identidad pública (IMPU) es un número o un URI SIP que otros usuarios llaman. Una suscripción puede tener varias identidades públicas. Varias identidades privadas pueden compartir una identidad pública.



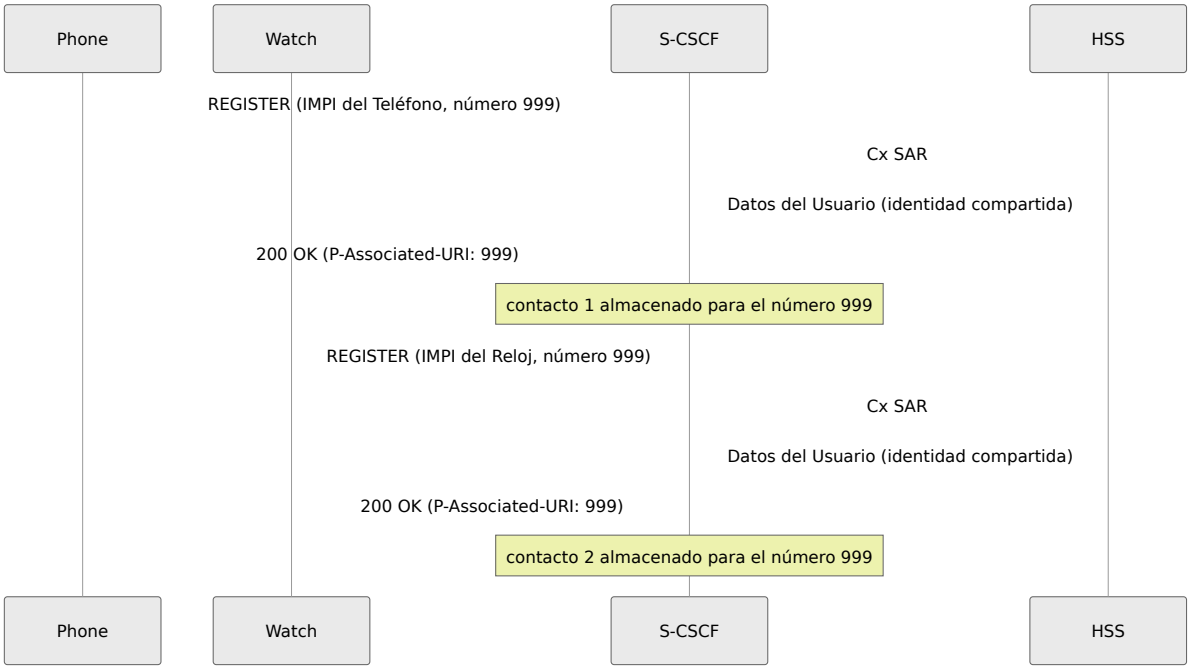
El HSS sostiene el modelo. El S-CSCF lo descarga en los Datos del Usuario durante el registro (Cx Server-Assignment, TS 29.228). El conjunto de identidades públicas que se registran juntas es el conjunto de registro implícito (TS 23.228).

Registro

Cada dispositivo se autentica con su propia identidad privada. El S-CSCF desafía cada REGISTER y valida la respuesta contra un vector de autenticación Cx (ver la guía de S-CSCF). Con éxito, el S-CSCF almacena un enlace de contacto por dispositivo.

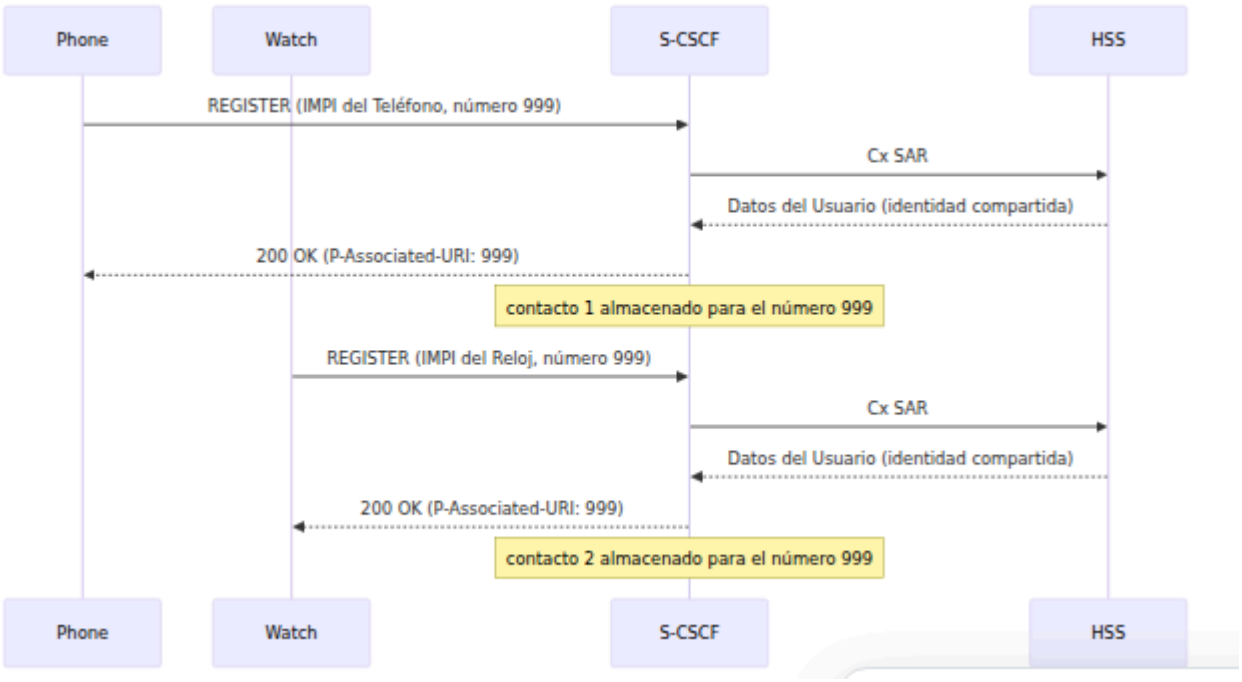
El 200 OK al REGISTER lleva un encabezado **P-Associated-URI**. Este encabezado lista cada identidad pública en el conjunto de registro implícito del suscriptor. El dispositivo aprende sus números de este encabezado.

- **Número compartido.** Cada dispositivo se registra con su propia identidad privada bajo la misma identidad pública. El S-CSCF mantiene un contacto por dispositivo. El S-CSCF empareja contactos por URI de contacto, por lo que los dispositivos no se sobrescriben entre sí. El S-CSCF mantiene hasta `maxcontact` contactos por identidad pública. Establezca `maxcontact` al número máximo de dispositivos que comparten un número.
- **Multi-MSISDN.** El dispositivo se registra con su única identidad privada. El 200 OK P-Associated-URI lista todos los números del suscriptor. Una llamada terminante a cualquiera de los números llega al dispositivo.



Llamadas Terminantes a un Número Compartido

Una llamada a un número compartido debe sonar en cada dispositivo. El S-CSCF realiza la bifurcación. Cuando el S-CSCF resuelve la ubicación de terminación con `lookup("location")`, el parámetro `append_branches` agrega cada contacto registrado como una rama paralela. El S-CSCF envía el INVITE a todos los dispositivos al mismo tiempo (una bifurcación paralela, TS 24.229 y RFC 3261 sección 16).



El primer dispositivo en responder gana. El S-CSCF reenvía el 200 OK de ese dispositivo al llamante. El S-CSCF envía un CANCEL a cada otra rama. Los otros dispositivos dejan de sonar.

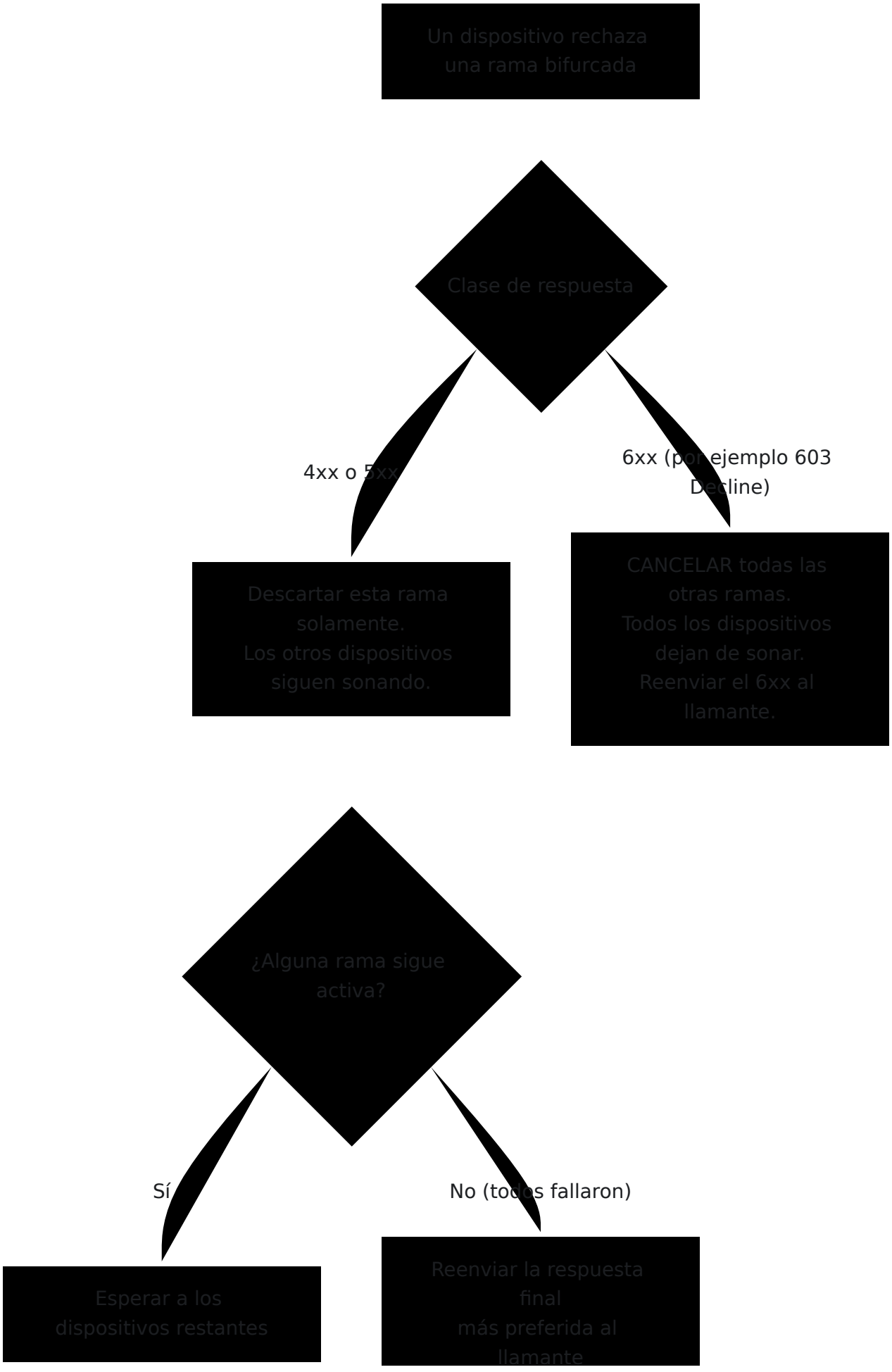
La guía de S-CSCF documenta los parámetros `append_branches` y `maxcontact`.

Comportamiento de Rechazo de Bifurcación

Un dispositivo puede rechazar una llamada bifurcada en lugar de responderla. El código de respuesta decide si los otros dispositivos siguen sonando. Esto sigue las reglas de respuesta de bifurcación paralela en la sección 16.7 del RFC 3261. La capa de transacción del S-CSCF aplica estas reglas.

Un dispositivo responde con	Significado	Efecto en los otros dispositivos	Resultado para el llamante
200 OK	El dispositivo respondió	El S-CSCF envía CANCEL a los demás. Dejan de sonar.	La llamada se conecta al primer dispositivo que respondió.
4xx (por ejemplo **486 Busy Here**, **480 Temporarily Unavailable**)	Este dispositivo no puede atender la llamada	Los otros **siguen sonando**. Esa rama se descarta.	El llamante ve un fallo solo después de que cada dispositivo falle. El S-CSCF luego reenvía la respuesta final más preferida.
5xx (por ejemplo **500 Server Internal Error**)	Un error de servidor en esa rama	Los otros **siguen sonando**. Esa rama se descarta.	Igual que 4xx: un fallo llega al llamante solo después de que cada rama falle.
6xx (por ejemplo **603 Decline**, **600 Busy Everywhere**)	Un rechazo para toda la identidad, no solo un dispositivo	El S-CSCF envía CANCEL a los demás. Ellos **dejan de sonar**.	El llamante recibe el 6xx.
Sin respuesta (timeout)	El dispositivo es inalcanzable	Los otros **siguen sonando**. La rama se agota (`fr_inv_timer`).	Igual que 4xx: un fallo llega al llamante solo después de que cada rama falle.

La distinción clave es 6xx contra 4xx/5xx. Un 4xx o 5xx es un fallo de una sola rama, por lo que la bifurcación continúa. Un 6xx es un rechazo global para la identidad, por lo que el S-CSCF cancela toda la bifurcación. Para rechazar una llamada en todos los dispositivos de un suscriptor a la vez, un dispositivo debe enviar un 6xx. Para rechazar en un dispositivo mientras los otros siguen sonando, un dispositivo debe enviar un 4xx.


Un dispositivo rechaza una rama bifurcada
Clase de respuesta
4xx o 5xx
6xx (por ejemplo 603 Decline)
Descartar esta rama solamente.
Los otros dispositivos siguen sonando.
CANCELAR todas las otras ramas.
Todos los dispositivos dejan de sonar.
Reenviar el 6xx al llamante.
¿Alguna rama sigue activa?
Sí
No (todos fallaron)
Esperar a los dispositivos restantes
Reenviar la respuesta final
más preferida al llamante

Lo que Ve el Servidor de Aplicaciones

El Servidor de Aplicaciones MMTel (el TAS) se encuentra en la ruta de terminación antes de la bifurcación. El S-CSCF activa el TAS con los Criterios de Filtro Iniciales de terminación. El TAS aplica sus servicios. Luego, el TAS devuelve la sesión al S-CSCF. El S-CSCF resuelve los contactos y bifurca.

Por lo tanto, el TAS maneja **una** sesión de terminación hacia la identidad compartida. El TAS no ve las ramas de dispositivos individuales. La bifurcación es transparente para él. El TAS ve el resultado consolidado:

- una indicación de timbre,
- luego el único 200 OK ganador, o
- el fallo final agregado, o
- el rechazo 6xx.

El TAS controla **si** el S-CSCF bifurca. Para una identidad compartida, el TAS permite la bifurcación, por lo que el S-CSCF suena en cada dispositivo. Para una identidad de un solo dispositivo, el TAS establece `Request-Disposition: no-fork`, por lo que el S-CSCF envía la llamada a un contacto. El TAS toma esta decisión según el número de miembros en la identidad compartida, que lee del HSS a través de Sh. El manejo de respuestas por dispositivo permanece dentro del S-CSCF.

Rechazo y la decisión de correo de voz

Una pregunta común es si el TAS ve a un dispositivo rechazar la llamada, mientras que los otros dispositivos siguen sonando, para que el TAS pueda reenviar al llamante al correo de voz. **No lo hace.** El TAS ve solo el resultado final de toda la bifurcación. La bifurcación está dentro del S-CSCF, aguas abajo del TAS.

- Un dispositivo que envía **486 Busy Here** no llega, por sí solo, al TAS. Los otros dispositivos siguen sonando. El S-CSCF mantiene la transacción abierta. El TAS no es notificado.

- El TAS recibe una respuesta final solo cuando la bifurcación se resuelve. La bifurcación se resuelve cuando un dispositivo responde (200), cuando cada dispositivo ha fallado, o cuando un dispositivo envía un 6xx.
- Cuando cada dispositivo falla, el S-CSCF selecciona una respuesta final para toda la bifurcación. Selecciona la respuesta más preferida entre las ramas (RFC 3261 sección 16.7). El S-CSCF devuelve ese código al TAS. El TAS no ve los códigos separados por dispositivo.
- El TAS luego aplica su lógica de Reenvío de Comunicación a ese único código final. El TAS reenvía al llamante al correo de voz bajo las condiciones para las que está configurado (por ejemplo, Reenvío de Comunicación en Ocupado para 486, o en No Respuesta para un timeout). Por lo tanto, el correo de voz se alcanza cuando toda la **bifurcación** falla, no cuando un dispositivo rechaza.

Un **6xx** (por ejemplo 603 Decline) es diferente. Un dispositivo que envía un 6xx cancela toda la bifurcación. El S-CSCF devuelve el 6xx al TAS. El TAS trata esto como un rechazo explícito para la identidad. Si el TAS luego reenvía al correo de voz depende de las reglas de Reenvío de Comunicación configuradas para una llamada rechazada.

En resumen: un comportamiento "este dispositivo rechazó, así que envía a ese llamante al correo de voz mientras los otros dispositivos siguen sonando" por dispositivo no es posible con una bifurcación de red. El correo de voz es una propiedad de toda la identidad compartida. El llamante solo llega a ella cuando toda la bifurcación falla.

Ejemplo trabajado: cada dispositivo devuelve 480

Dos dispositivos comparten un número. Una llamada se bifurca a ambos. Ambos rechazan con 480 Temporarily Unavailable unos milisegundos de diferencia. Esto es lo que sucede en la red:

1. El S-CSCF recibe ambas respuestas 480. Cada respuesta lleva los encabezados de su propio dispositivo (su propio `User-Agent`, su propia etiqueta `To`, y cualquier encabezado extra que el dispositivo agregó). Ambos comparten el Call-ID bifurcado y CSeq.
2. El S-CSCF selecciona **una** de las dos respuestas 480 y la reenvía aguas arriba. **Reenvía la respuesta real de esa rama** (procesamiento estándar

de proxy: elimina su propio `Via` y deja el resto). El 480 reenviado conserva el `User-Agent` del dispositivo seleccionado, su encabezado `Reason` (por ejemplo `Reason: Q.850;cause=18`), y **cualquier encabezado extra** que ese dispositivo estableció. Es una respuesta real de un solo dispositivo, no una combinada.

3. La respuesta seleccionada **no** es "el último dispositivo en rechazar". El S-CSCF selecciona la rama según sus propias reglas de transacción. Cuando cada rama devuelve el mismo código, la selección sigue el orden de las ramas, no el orden de respuesta. No dependa de qué dispositivo provino el 480 reenviado (y su `User-Agent`). Solo el código de respuesta es confiable.
4. El Servidor de Aplicaciones ve ese 480, aplica Reenvío de Comunicación para un suscriptor no alcanzable (480 se mapea a CFNRc), y reenvía al llamante al correo de voz. El llamante se conecta al correo de voz con un 200 OK.

Si los dispositivos devuelven códigos de rechazo diferentes, el S-CSCF selecciona el más preferido según la sección 16.7 del RFC 3261, y el Servidor de Aplicaciones actúa sobre ese único código.

Ejemplo trabajado: un dispositivo rechaza, otro responde

Dos dispositivos comparten un número. Una llamada se bifurca a ambos. Un dispositivo rechaza con 480. El otro dispositivo suena y luego responde. Esto es lo que sucede en la red:

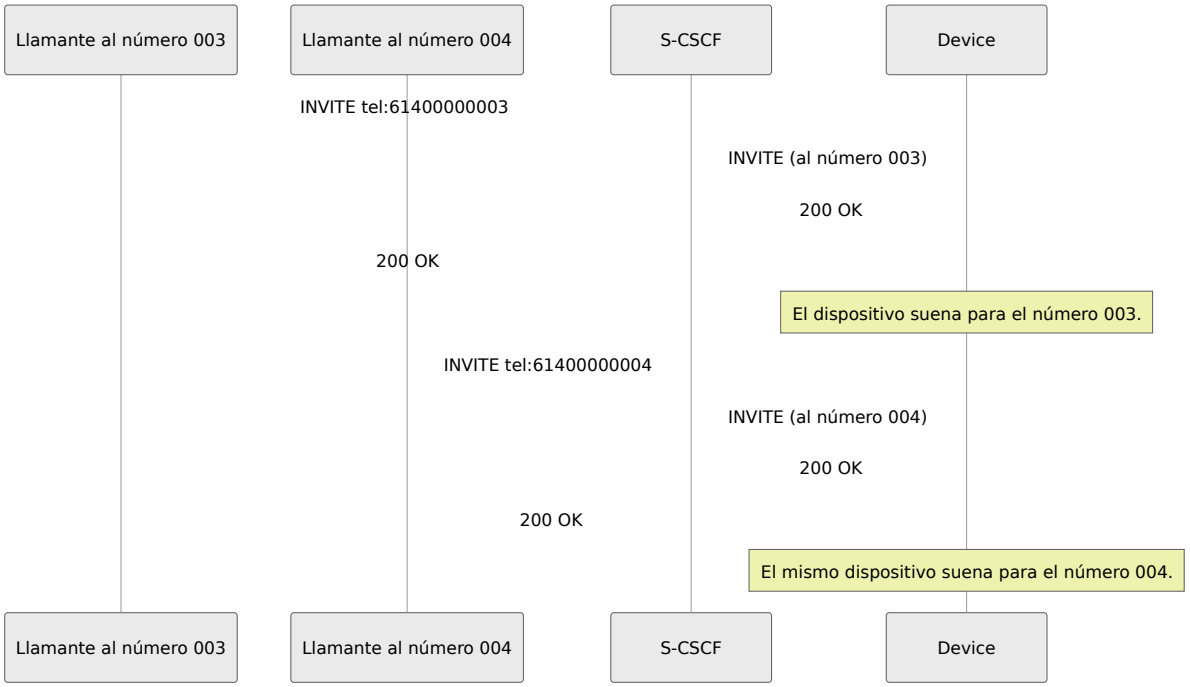
1. El 480 del primer dispositivo llega, **incluso antes de que suene el segundo dispositivo**. El S-CSCF **no** termina la bifurcación en este 480. Un 4xx termina solo esa rama. El S-CSCF sigue esperando al segundo dispositivo.
2. El segundo dispositivo envía 180 Ringing, luego 200 OK.
3. El 200 OK gana. El S-CSCF reenvía el 200 al llamante. El llamante se conecta al dispositivo que respondió.
4. El anterior 480 se descarta. Es una rama perdedora. El llamante nunca lo ve, y la llamada **no** va al correo de voz.

Esto confirma la regla central: un dispositivo que rechaza con un 4xx no puede bloquear a un dispositivo diferente de responder. Solo un 6xx (o que todas las ramas fallen) impide que la llamada se conecte.

Llamadas Terminantes a un Suscriptor Multi-MSISDN

Un suscriptor multi-MSISDN tiene un dispositivo y varios números. Una llamada a **cualquiera** de los números llega al único dispositivo. El número que el llamante marcó permanece en el Request-URI, por lo que el dispositivo puede mostrar el número marcado al usuario (por ejemplo, para separar una llamada de negocio de una llamada personal).

Todos los números pertenecen a un único conjunto de registro implícito. Por lo tanto, cada número se resuelve al mismo contacto del dispositivo. El S-CSCF resuelve la ubicación de terminación de la misma manera que cualquier otra llamada. No hay bifurcación, porque hay un solo dispositivo.



Para provisionar un suscriptor multi-MSISDN, agregue cada número como una identidad pública a la única suscripción IMS en el HSS. El 200 OK al REGISTER luego lista cada número en el P-Associated-URI. Consulte la documentación multi-MSISDN del HSS.

Mensajería a un Número Compartido

SMS sobre IMS utiliza una solicitud SIP MESSAGE (TS 24.341). Un mensaje a un número compartido llega a cada dispositivo, de la misma manera que una llamada se bifurca a cada dispositivo. El S-CSCF resuelve los contactos registrados y entrega el mensaje a cada uno. Cada dispositivo en el número compartido recibe el mensaje.

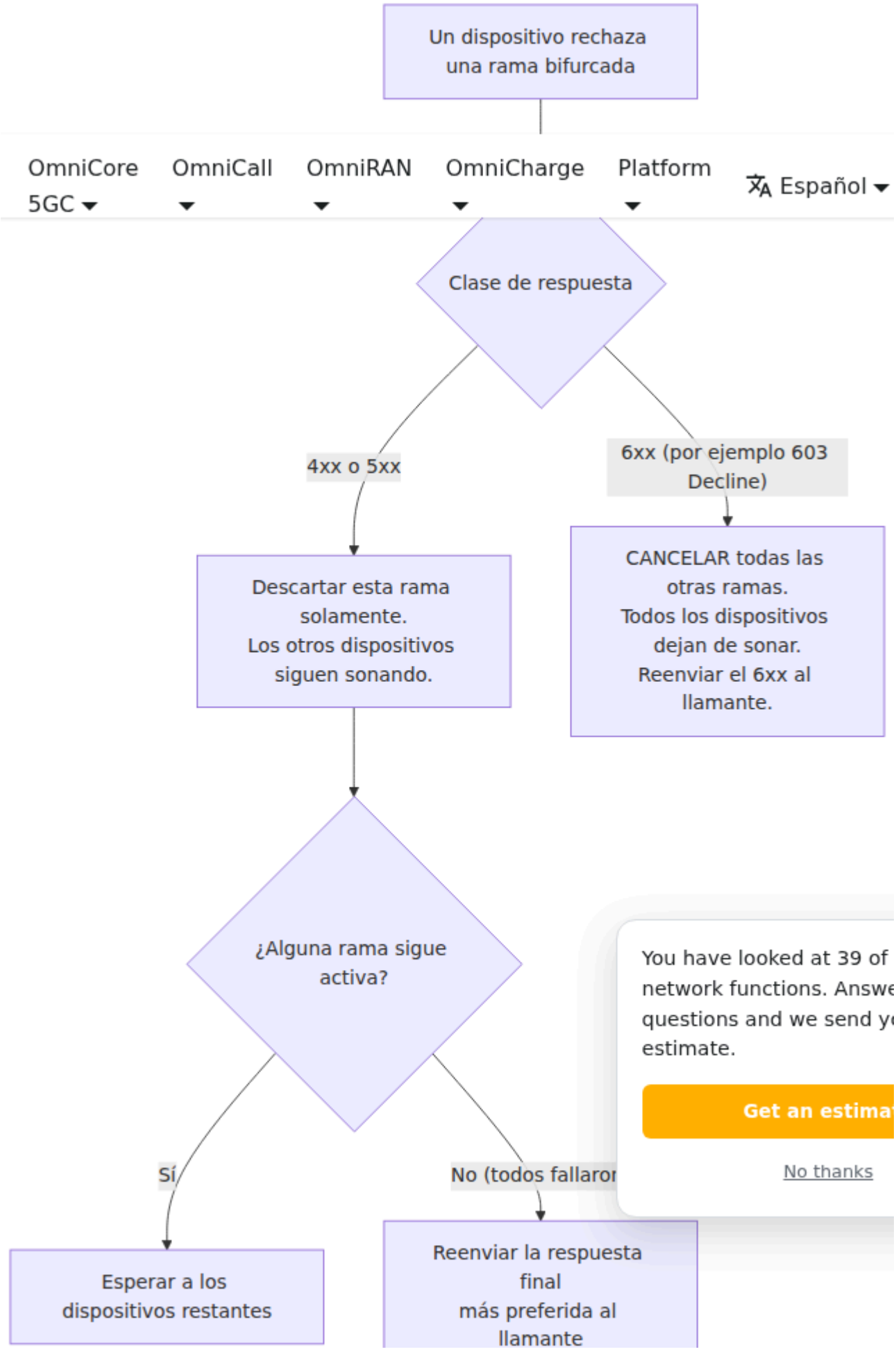
Un mensaje a un número multi-MSISDN llega al único dispositivo, de la misma manera que una llamada a cualquiera de sus números llega al único dispositivo.

Llamadas de Origen e Identidad de Línea de Llamada

Un suscriptor presenta una identidad de línea de llamada (CLI) en una llamada de origen. Un suscriptor multi-MSISDN puede presentar **cualquiera** de sus propios números. Por ejemplo, el suscriptor presenta el número de negocio para una llamada de negocio y el número personal para una llamada personal. El dispositivo elige el número en el encabezado P-Preferred-Identity (TS 24.229).

El P-CSCF afirma la identidad. El dispositivo no. El P-CSCF aplica estas reglas en cada solicitud de origen:

1. El P-CSCF elimina cualquier P-Asserted-Identity que el dispositivo envíe. El dispositivo no es confiable para afirmar su propia identidad.
2. Si el dispositivo envía un P-Preferred-Identity, el P-CSCF lo verifica contra las identidades registradas del suscriptor. Si es una de ellas, el P-CSCF la afirma en un encabezado P-Asserted-Identity.
3. Si el dispositivo no envía ningún P-Preferred-Identity, o una identidad que no está registrada al suscriptor, el P-CSCF afirma la identidad pública predeterminada (primaria) del suscriptor.



OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Español
You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima
No thanks

La identidad que el usuario del extremo lejano finalmente ve también depende de la política del Servidor de Aplicaciones. El Servidor de Aplicaciones MMTel puede anular la identidad afirmada (por ejemplo, una red puede normalizar cada llamada al número primario del suscriptor, o aplicar una Restricción de Identificación de Línea de Llamada). Para presentar un número no primario al extremo lejano, el Servidor de Aplicaciones debe mantener la identidad afirmada por el P-CSCF. Consulte la documentación del Servidor de Aplicaciones para la política de CLI.

Consulte la guía de P-CSCF para la configuración de afirmación de identidad.

Referencia

Códigos de Respuesta en una Bifurcación

Código	Nombre	Clase	Efecto de bifurcación
180	Ringing	1xx	Progreso. La rama sigue activa.
200	OK	2xx	Respuesta. Gana la bifurcación. Cancela las demás.
486	Busy Here	4xx	Esta rama falla. Las otras siguen sonando.
480	Temporarily Unavailable	4xx	Esta rama falla. Las otras siguen sonando.
408	Request Timeout	4xx	Esta rama falla. Las otras siguen sonando.
600	Busy Everywhere	6xx	Rechazo global. Cancela toda la bifurcación.
603	Decline	6xx	Rechazo global. Cancela toda la bifurcación.

Parámetros Relacionados de S-CSCF

Parámetro	Propósito
`ims_usrloc_scscf` `maxcontact`	Máximo de contactos mantenidos por identidad pública. Establezca en el número máximo de dispositivos que comparten un número.
`ims_registrar_scscf` `append_branches`	Cuando se establece en `1`, un `lookup("location")` de terminación bifurca a cada contacto registrado en paralelo.
`tm` `fr_inv_timer`	El tiempo de espera de la rama INVITE. Un dispositivo que nunca responde falla cuando este temporizador expira.

Consulte la guía de S-CSCF para la referencia completa de parámetros.

Referencias de 3GPP e IETF

Especificación	Relevancia
3GPP TS 23.228	Arquitectura IMS, identidades públicas y privadas, conjunto de registro implícito
3GPP TS 24.229	Perfil SIP de IMS, manejo de identidad de origen y terminación
3GPP TS 29.228	Interfaz Cx, Datos del Usuario, identidades públicas compartidas
RFC 3261 sección 16.7	Procesamiento de respuesta de proxy y manejo de rechazo de bifurcación paralela