Guía de Operaciones de OmniPGW

OmniPGW - Plano de Control de Puerta de Enlace de Paquetes (PGW-C)

por Omnitouch Network Services

Tabla de Contenidos

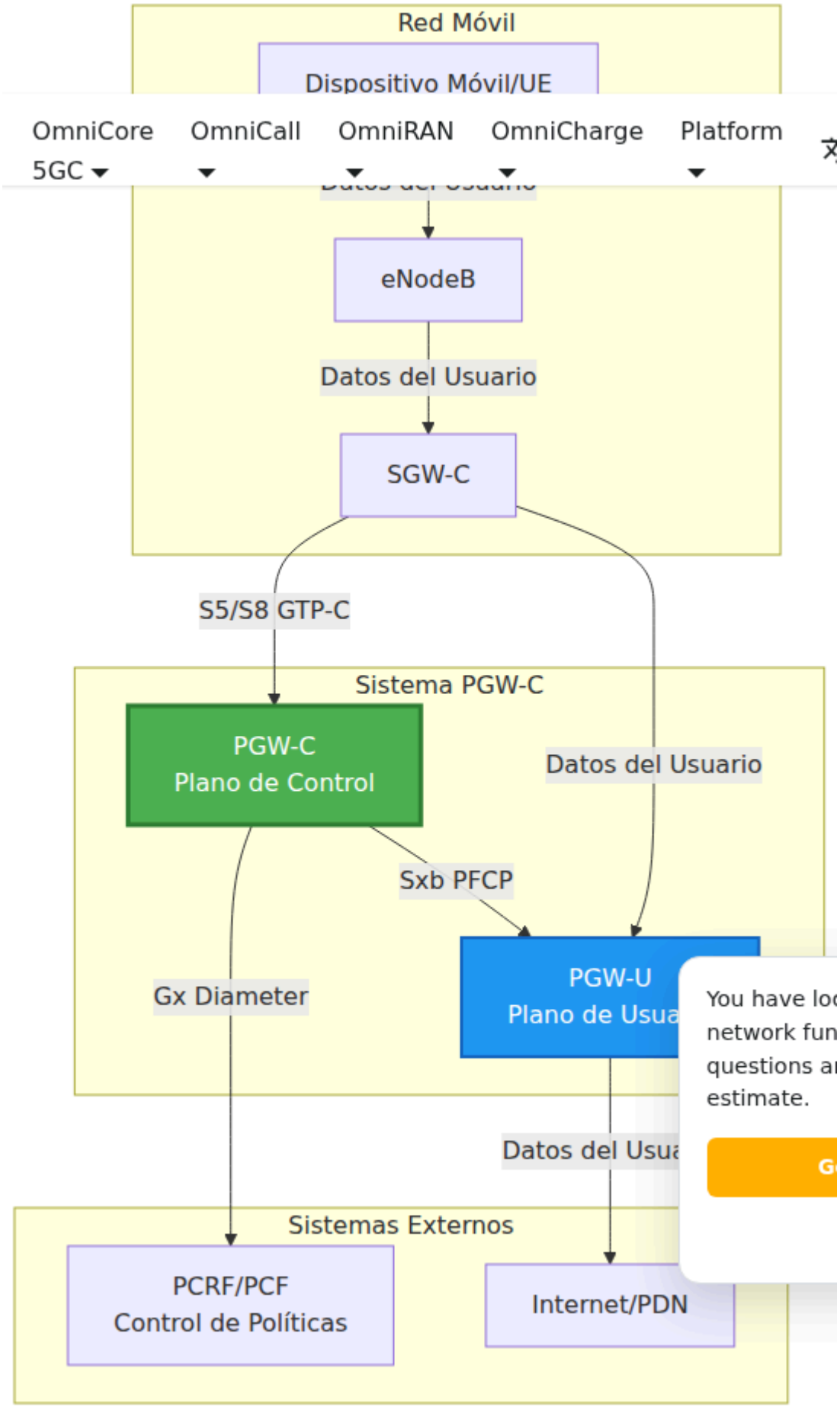
1. Descripción General
2. Arquitectura
3. Interfaces de Red
4. Conceptos Clave
5. Comenzando
6. Configuración
7. Monitoreo de Operaciones en Tiempo Real (API OAM)
8. Monitoreo y Métricas
9. Documentación Detallada
10. Recursos Adicionales

Descripción General

OmniPGW es una implementación de alto rendimiento del Plano de Control de Puerta de Enlace de Paquetes (PGW-C) para redes del Núcleo de Paquete Evolucionado (EPC) LTE de 3GPP, desarrollado por Omnitouch Network Services. Gestiona las funciones del plano de control para sesiones de datos, incluyendo:

- **Gestión de Sesiones** - Creación, modificación y terminación de sesiones de datos de UE (Equipo de Usuario)

- **Asignación de Direcciones IP** - Asignación de direcciones IP a dispositivos móviles desde grupos configurados
- **Control de Políticas y Cargos** - Interfaz con PCRF para la aplicación de políticas y cargos
- **Coordinación del Plano de Usuario** - Control del PGW-U (Plano de Usuario) para el reenvío de paquetes


Red Móvil
Dispositivo Móvil/UE
OmniCore
5GC
OmniCall
OmniRAN
OmniCharge
Platform
eNodeB
Datos del Usuario
SGW-C
S5/S8 GTP-C
Sistema PGW-C
PGW-C
Plano de Control
Datos del Usuario
Sxb PFCP
PGW-U
Plano de Usua
Gx Diameter
Datos del Usua
Sistemas Externos
PCRF/PCF
Control de Políticas
Internet/PDN

Lo que Hace PGW-C

- **Acepta solicitudes de sesión** de SGW-C a través de la interfaz S5/S8 (GTP-C)
- **Asigna direcciones IP a UE** desde grupos de subred configurados
- **Solicita decisiones de políticas** a PCRF a través de la interfaz Gx (Diameter)
- **Programa reglas de reenvío** en PGW-U a través de la interfaz Sxb (PFCP)
- **Gestiona la aplicación de QoS** a través de contextos de portadora y reglas de QoS
- **Rastrea información de cargos** para sistemas de facturación

---

Arquitectura

Descripción General de Componentes



Arquitectura de Procesos

PGW-C está construido sobre Elixir/OTP y utiliza una arquitectura de procesos supervisados:

- **Supervisor de Aplicación** - Supervisor de nivel superior que gestiona todos los componentes
- **Intermediarios de Protocolo** - Manejan mensajes de protocolo entrantes/salientes
- **Procesos de Sesión** - Un GenServer por cada conexión PDN activa
- **Registros** - Rastrea recursos asignados (IPs, TEIDs, SEIDs, etc.)
- **Gestor de Nodo PFCP** - Mantiene asociaciones PFCP con pares PGW-U

Cada componente es supervisado y se reiniciará automáticamente en caso de fallo, asegurando la fiabilidad del sistema.

Interfaces de Red

PGW-C implementa tres interfaces primarias de 3GPP:

Interfaz S5/S8 (GTP-C v2)

Propósito: Señalización del plano de control entre SGW-C y PGW-C

Protocolo: GTP-C Versión 2 sobre UDP

Mensajes Clave:

- Solicitud/Respuesta de Creación de Sesión
- Solicitud/Respuesta de Eliminación de Sesión
- Solicitud/Respuesta de Creación de Portadora
- Solicitud/Respuesta de Eliminación de Portadora

Configuración: Ver Configuración S5/S8

Interfaz Sxb (PFCP)

Propósito: Señalización del plano de control entre PGW-C y PGW-U

Protocolo: PFCP (Protocolo de Control de Reenvío de Paquetes) sobre UDP

Mensajes Clave:

- Solicitud/Respuesta de Configuración de Asociación
- Solicitud/Respuesta de Establecimiento de Sesión
- Solicitud/Respuesta de Modificación de Sesión
- Solicitud/Respuesta de Eliminación de Sesión
- Solicitud/Respuesta de Latido

Configuración: Ver Documentación de la Interfaz PFCP/Sxb

Interfaz Gx (Diameter)

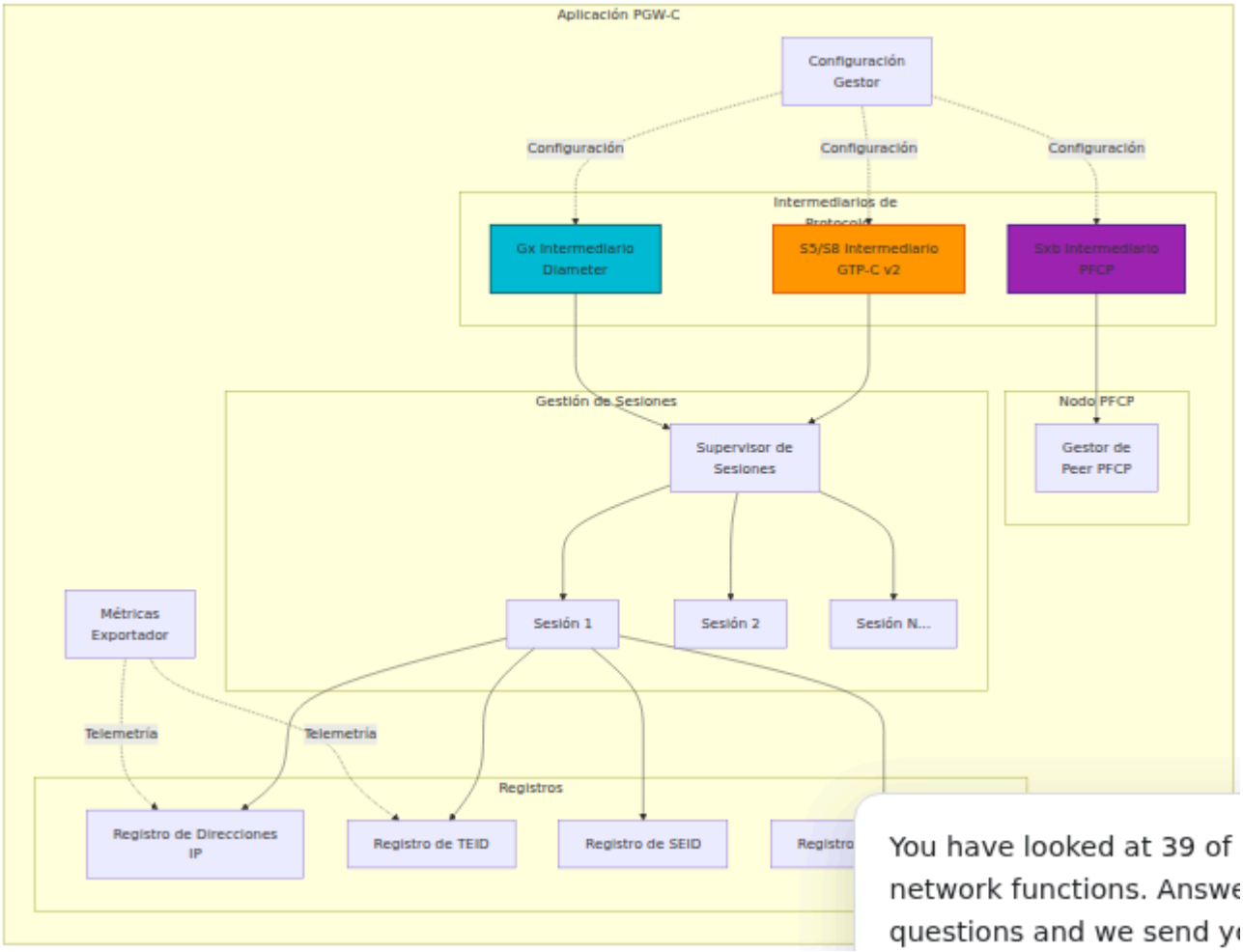
Propósito: Interfaz de Función de Reglas de Políticas y Cargos (PCRF)

Protocolo: Diameter (IETF RFC 6733)

Mensajes Clave:

- Solicitud/Respuesta Inicial de Control de Crédito (CCR-I/CCA-I)
- Solicitud/Respuesta de Terminación de Control de Crédito (CCR-T/CCA-T)

Configuración: Ver Documentación de la Interfaz Gx Diameter



Conceptos Clave

Sesión PDN

Una Sesión PDN (Red de Datos de Paquetes) representa la conexión de datos de un UE a una red externa (como Internet). Cada sesión tiene:

- **Dirección IP de UE** - Asignada desde un grupo de subred configurado
- **APN** (Nombre del Punto de Acceso) - Identifica la red externa
- **Contexto de Portadora** - Contiene parámetros de QoS e información de túnel
- **ID de Cargos** - Identificador único para facturación
- **TEID** (ID de Punto de Final de Túnel) - Identificador de túnel de la interfaz S5/S8
- **SEID** (ID de Punto de Final de Sesión) - Identificador de sesión de la interfaz Sxb

Contexto de Portadora

Una portadora representa un flujo de tráfico con características específicas de QoS:

- **Portadora Predeterminada** - Creada con cada sesión PDN
- **Portadoras Dedicadas** - Portadoras adicionales para necesidades específicas de QoS
- **EBI** (ID de Portadora EPS) - Identificador único para cada portadora
- **Parámetros de QoS** - QCI, ARP, tasas de bits (MBR, GBR)

Reglas PFCP

El PGW-C programa el PGW-U con reglas de procesamiento de paquetes:

- **PDR** (Regla de Detección de Paquetes) - Coincide con paquetes (uplink/downlink)
- **FAR** (Regla de Acción de Reenvío) - Especifica el comportamiento de reenvío

- **QER** (Regla de Aplicación de QoS) - Aplica límites de tasa de bits
- **BAR** (Regla de Acción de Buffer) - Controla el almacenamiento en búfer de paquetes

Ver Documentación de la Interfaz PFCP para más detalles.

Asignación de Direcciones IP

Las direcciones IP de UE se asignan desde grupos de subred configurados:

- **Selección basada en APN** - Diferentes APNs pueden usar diferentes subredes
- **Asignación dinámica** - Selección aleatoria de IP del rango disponible
- **Asignación estática** - Soporte para direcciones IP solicitadas por UE
- **Detección de colisiones** - Asegura la asignación única de IP

Ver Asignación de Grupos de IP de UE para configuración, y IPv6 / Doble Pila para operación PDN IPv6 e IPv4v6.

Comenzando

Requisitos Previos

- Elixir ~1.16
- Erlang/OTP 26+
- Conectividad de red a SGW-C, PGW-U y PCRF
- Comprensión de la arquitectura EPC LTE

Iniciando OmniPGW

1. **Configurar ajustes de tiempo de ejecución** en `config/runtime.exs`
2. **Compilar la aplicación:**

```
mix deps.get
mix compile
```

3. **Iniciar la aplicación:**

```
mix run --no-halt
```

Verificando la Operación

Verifique los registros para una inicialización exitosa:

```
[info] Iniciando OmniPGW...
[info] Iniciando Exportador de Métricas en 127.0.0.42:42069
[info] Iniciando Intermediario S5/S8 en 127.0.0.10
[info] Iniciando Intermediario Sxb en 127.0.0.20
[info] Iniciando Intermediario Gx
[info] Iniciando Gestor de Nodo PFCP
[info] OmniPGW iniciado con éxito
```

Acceda a las métricas en `http://127.0.0.42:42069/metrics` (dirección configurada).

Configuración

Toda la configuración de tiempo de ejecución se define en `config/runtime.exs`. Este archivo se evalúa al iniciar la aplicación. Un ejemplo completo sigue; cada sección se describe en la tabla de referencia a continuación y en la Referencia de Configuración.

```
# config/runtime.exs
import Config

# Configuración del registrador
config :logger, level: :info

config :pgw_c,
  # Métricas (Prometheus)
  metrics: %{
    enabled: true,
    ip_address: "10.0.0.20",  # Red de gestión
    port: 9090,
    registry_poll_period_ms: 5_000
  },

  # Diameter/Gx (interfaz PCRF)
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf-primary.epc.mnc001.mcc001.3gppnetwork.org",
        realm: "epc.mnc001.mcc001.3gppnetwork.org",
        ip: "10.0.1.30",
        initiate_connection: true
      },
      %{
        host: "pcrf-backup.epc.mnc001.mcc001.3gppnetwork.org",
        realm: "epc.mnc001.mcc001.3gppnetwork.org",
        ip: "10.0.2.30",
        initiate_connection: true
      }
    ]
  },

  # S5/S8 (interfaz SGW-C)
  s5s8: %{
    local_ipv4_address: "10.0.0.20"
  },

  # Sxb/PFCP (interfaz PGW-U)
  sxb: %{
```

```
    local_ip_address: "10.0.0.20"
  },

  # Selección de UPF
  upf_selection: %{
    rules: [
      %{
        name: "Internet Predeterminado",
        priority: 1,
        match_field: :apn,
        match_regex: ~r/^internet/,
        upf_pool: [
          %{remote_ip_address: "10.0.0.21", remote_port: 8805,
weight: 100},
          %{remote_ip_address: "10.0.0.22", remote_port: 8805,
weight: 0}  # Reserva
        ]
      }
    ],
    fallback_pool: [
      %{remote_ip_address: "10.0.0.21", remote_port: 8805, weight:
100}
    ]
  },

  # Grupos de IP de UE
  ue: %{
    subnet_map: %{
      "internet" => [
        "100.64.0.0/18"  # 16,382 IPs
      ],
      "ims" => [
        "100.64.64.0/22"  # 1,022 IPs
      ],
      "enterprise.corp" => [
        "10.100.0.0/16"  # 65,534 IPs
      ],
      default: [
        "100.64.127.0/24"  # 254 IPs
      ]
    }
  },

  # Opciones de Configuración de Protocolo
```

```
  pco: %{
    primary_dns_server_address: "8.8.8.8",
    secondary_dns_server_address: "8.8.4.4",
    p_cscf_ipv4_address_list: ["10.0.0.50", "10.0.0.51"],
    ipv4_link_mtu_size: 1400
  }
```

La configuración está estructurada en varias secciones:

Descripción General de la Configuración



Referencia Rápida de Configuración

Sección	Propósito	Documentación
metrics	Exportador de métricas Prometheus	Guía de Monitoreo
diameter	Interfaz Gx a PCRF	Configuración Gx Diameter
s5s8	Interfaz GTP-C a SGW-C	Configuración S5/S8
sxb	Interfaz PFCP a PGW-U	Configuración PFCP
ue	Grupos de direcciones IP de UE	Configuración de Grupos de IP
pco	Opciones de Configuración de Protocolo	Configuración PCO
CDR	Cargos fuera de línea e informes de uso	Formato CDR
charging	Modo de carga en línea/fuera de línea, anulación de emergencia	Anulación de Cargos

Vea la Guía de Configuración Completa para información detallada.

Monitoreo de Operaciones en Tiempo Real (API OAM)

OmniPGW expone una **API REST OAM** para el monitoreo y operaciones en tiempo real, proporcionando visibilidad instantánea del estado del sistema. Consulte estos puntos finales de lectura bajo demanda (o en un intervalo de sondeo / desde un script) para una vista operativa en vivo - no se requiere acceso a la línea de comandos al host o consultas de métricas en bruto.

Accediendo a la API OAM

La API se sirve a través de HTTPS/TLS. Todas las rutas se sirven bajo el prefijo `/api`.

```
https://<omnipgw-ip>:8443/
```

La documentación interactiva de la API (Swagger UI) está disponible en:

```
https://<omnipgw-ip>:8443/api/docs
```

Ejemplo de verificación de estado (use `-k` para un certificado de laboratorio autofirmado):

```
curl -k https://localhost:8443/api/status
{"result":"ok"}
```

Puntos Finales Disponibles:

Propósito	Punto Final	Reemplaza (página antigua)
Profundizar en un suscriptor específico (IMSI/MSISDN/IP)	`POST /api/ue_search`	Búsqueda de UE
Listar / buscar sesiones PDN activas	`GET /api/sessions[?search=<imsi|msisdn|ip>]`	Sesiones PGW
Una sesión por IMSI	`GET /api/sessions/<imsi>`	Sesiones PGW (detalle)
Historial de sesiones / eventos de auditoría	`GET /api/session_history[?type=&search=&page=&page_size=]`	Historial de Sesiones
Visión general de la topología de la red	`GET /api/topology`	Topología de Red
Utilización del grupo de direcciones IP de UE	`GET /api/ip_pools`, `GET /api/ip_pools/<name>`	Grupos de IP
Estado de pares UPF / PFCP	`GET /api/upf`, `GET /api/upf/<ip>`	Sesiones PFCP / Estado de UPF
Reglas de selección de UPF,	`GET /api/upf_selection`	Selección de UPF

Propósito	Punto Final	Reemplaza (página antigua)
estado, configuración PCO		
Conectividad de pares Diameter (Gx/Gy)	`GET /api/diameter[?status=connected|disconnected]`, `GET /api/diameter/<origin-host>`	Pares Diameter
Estado de carga en línea (Gy) por sesión	`GET /api/charging[?search=<imsi>]`, `GET /api/charging/<imsi>`	Estado Gy
Anulación de emergencia: deshabilitar el nodo de carga en línea en toda la red	`PUT /api/charging/override`, `GET /api/charging/override`, `DELETE /api/charging/override`	-
Estado de descubrimiento DNS de P-CSCF	`GET /api/pcscf_monitor`	Monitor de P-CSCF
Verificación de estado	`GET /api/status`	-

Para una vista estilo tablero en vivo, sondee los puntos finales de colección en un intervalo, por ejemplo:

```
watch -n 2 'curl -sk https://localhost:8443/api/sessions'
watch -n 1 'curl -sk https://localhost:8443/api/diameter?
status=disconnected'
```

> Nota: la antigua página **Registros** (transmisión de registros en vivo) y la página **Simulador Gy** no tienen un equivalente en la API OAM. Transmita registros desde el host / su agregador de registros, y use `GET /api/charging` para inspeccionar el estado en vivo de Gy/carga en línea.

Características Clave

Datos Bajo Demanda y Sondeados:

- Cada punto final devuelve el estado actual en vivo de los procesos de OmniPGW
- Sondee en un intervalo con `watch`/cron/un script para una vista de actualización automática
- Los campos de estado (por ejemplo, `connected`/`associated` de pares) se devuelven explícitamente en el JSON

Buscar y Filtrar:

- Busque sesiones por IMSI, IP, MSISDN o APN a través de `GET /api/sessions?search=...`
- Filtrar pares Diameter por `?status=connected|disconnected`
- Filtrar estado de carga por `?search=<imsi>`

Registros de Detalle Completo:

- Puntos finales por entidad (`/api/sessions/<imsi>`, `/api/upf/<ip>`, `/api/diameter/<origin-host>`, `/api/charging/<imsi>`) devuelven el estado completo como JSON
- Inspeccione la sesión completa, la configuración de pares y las capacidades

Control de Acceso:

- Servido a través de HTTPS/TLS en el puerto 8443
- Vincule solo a la IP de gestión y utilice sus controles de acceso
- Destinado para el equipo de NOC/operaciones y uso de automatización

Flujos de Trabajo Operativos

Solución de Problemas de Sesiones (Profundización):

```
1. El usuario informa un problema de conexión
2. POST /api/ue_search con un cuerpo JSON que contiene el IMSI,
MSISDN o IP
3. Revise los detalles completos de la sesión en la respuesta:
   a) Sesiones Activas - Verifique que la sesión exista con los
parámetros correctos
   b) Ubicación Actual - Verifique TAC, ID de Celda, red de
servicio
   c) Información de Portadora - Verifique portadoras
predeterminadas y dedicadas
      - QCI, MBR/GBR, Nombres de Reglas de Cargos
      - Límites APN-AMBR
   d) Información de Cargos - ID de sesión Gy, estado de cuota
(también GET /api/charging/<imsi>)
   e) Información de Políticas - Sesión Gx, reglas PCC instaladas
   f) Eventos Recientes - GET /api/session_history?search=<imsi>
4. Si no se encuentra la sesión → GET /api/diameter?
status=disconnected para conectividad PCRF
```

Búsqueda Rápida de Sesiones:

```
1. El usuario informa un problema
2. GET /api/sessions?search=<imsi|msisdn> (o GET
/api/sessions/<imsi>)
3. Verifique que la sesión exista con detalles básicos:
   - Dirección IP de UE asignada
   - Parámetros de QoS
   - Puntos finales de túnel establecidos
4. Para un análisis detallado → POST /api/ue_search
```

Verificación de Salud del Sistema:

```
1. GET /api/upf              → Verifique que todos los pares PGW-U
estén "Asociados"
2. GET /api/diameter?status=connected → Verifique que todos los
pares PCRF estén "Conectados"
3. GET /api/sessions         → Verifique el conteo de sesiones
activas frente a la capacidad
4. GET /api/status           → Verificación de salud general
({"result":"ok"})
```

Monitoreo de Capacidad:

- Cuente las entradas devueltas por `GET /api/sessions`
- Compare con la capacidad licenciada/esperada
- Identifique los momentos de uso máximo
- Monitoree la distribución entre APNs; use `GET /api/ip_pools` para la utilización por grupo

API vs. Métricas

Utilice la API OAM para:

- Solución de problemas de suscriptores en profundidad (`POST /api/ue_search`)
- Detalles y estado de sesiones individuales (`GET /api/sessions/<imsi>`)
- Estado de pares en tiempo real (`GET /api/upf`, `GET /api/diameter`)
- Verificaciones rápidas de salud en todas las interfaces (`GET /api/status`)
- Solución de problemas de usuarios específicos por IMSI/MSISDN/IP
- Análisis de QoS de portadoras (MBR, GBR, QCI)
- Inspección de reglas de políticas y cargos (`GET /api/charging`)
- Historial de sesiones y auditorías (`GET /api/session_history`)
- Monitoreo de capacidad de grupos IP (`GET /api/ip_pools`)
- Verificación de configuración y reglas (`GET /api/upf_selection`)

Utilice Métricas de Prometheus para:

- Tendencias históricas

- Alertas y notificaciones
- Gráficos de planificación de capacidad
- Análisis de rendimiento
- Monitoreo a largo plazo

Mejor Práctica: Utilice ambos juntos - la API OAM para operaciones inmediatas, Prometheus para tendencias y alertas.

Monitoreo y Métricas

Además de la API OAM, OmniPGW expone métricas compatibles con Prometheus para monitoreo:

Métricas Disponibles

- **Métricas de Sesiones**
  - `teid_registry_count` - Sesiones S5/S8 activas
  - `seid_registry_count` - Sesiones PFCP activas
  - `session_id_registry_count` - Sesiones Gx activas
  - `address_registry_count` - Direcciones IP de UE asignadas
  - `charging_id_registry_count` - IDs de cargos activos
- **Métricas de Mensajes**
  - `s5s8_inbound_messages_total` - Mensajes GTP-C recibidos
  - `sxb_inbound_messages_total` - Mensajes PFCP recibidos
  - `gx_inbound_messages_total` - Mensajes Diameter recibidos
  - Distribuciones de duración del manejo de mensajes
- **Métricas de Errores**
  - `s5s8_inbound_errors_total` - Errores de protocolo S5/S8
  - `sxb_inbound_errors_total` - Errores de protocolo PFCP
  - `gx_inbound_errors_total` - Errores de Diameter

- **Métricas del Ciclo de Vida de la Sesión**
  - `pgw_session_create_total{result,cause,pdn_type,rat_type}` - Intentos de creación de sesión PDN, desglosados por resultado (`success`/`failure`), la causa GTP devuelta, tipo de PDN (`ipv4`/`ipv6`/`ipv4v6`) y tipo de RAT
  - `pgw_session_delete_total{pdn_type}` - Eliminaciones de sesión PDN por tipo de PDN
  - `pgw_session_modify_total` - Solicitudes de Modificación de Bearer manejadas
- **Métricas del Pool de IP de UE**
  - `ue_pool_addresses_allocated{pool,ip_version}` - Direcciones de UE asignadas por pool (patrón APN) y versión de IP
  - `ue_pool_addresses_total{pool,ip_version}` - Capacidad total del pool
  - `ue_pool_addresses_utilization_ratio{pool,ip_version}` - Fracción asignada (0.0-1.0); útil para alertas de agotamiento del pool. Nota: los pools que comparten un rango de direcciones cuentan cada uno las asignaciones compartidas
  - `ue_ip_allocation_failures_total{ip_version,reason}` - Fallos de asignación (`pool_exhausted`, `already_registered`)
- **Métricas por Par UPF / PFCP**
  - `upf_peer_associated{peer_ip}` - Estado de asociación PFCP 1/0 por par
  - `upf_peer_healthy{peer_ip}` - Salud 1/0 por par
  - `upf_peer_missed_heartbeats{peer_ip}` - Latidos perdidos consecutivos por par
  - `upf_heartbeat_rtt` - Distribución del tiempo de ida y vuelta del latido PFCP, por `peer_ip`
- **Métricas de Bearer y QoS**
  - `pgw_bearer_create_total{type,qci}` - Bearers creados por tipo (`default`/`dedicated`) y QCI

    - `pgw_bearer_delete_total{type}` - Bearers eliminados por tipo

- **Métricas de Pares Diameter**
    - `diameter_peers_connected{application}` - Pares Diameter conectados por aplicación (`gx`/`gy`/`all`)

Accediendo a las Métricas

Las métricas se exponen a través de HTTP en el endpoint configurado:

```
curl http://127.0.0.42:42069/metrics
```

Ver Guía de Monitoreo y Métricas para la configuración del panel y alertas.

Documentación Detallada

Esta sección proporciona una visión general completa de toda la documentación de OmniPGW. Los documentos están organizados por tema y caso de uso.

Estructura de la Documentación

```
Documentación de OmniPGW
├── OPERATIONS.md (Esta Guía)
│
└── docs/
    ├── Configuración y Configuración
    │   ├── configuration.md          Referencia completa de
runtime.exs
    │   ├── ue-ip-allocation.md       Configuración del pool de IP
    │   └── pco-configuration.md      Configuración de DNS, P-
CSCF, MTU
    │
    ├── Interfaces de Red
    │   ├── pfcp-interface.md         Sxb/PFCP (comunicación PGW-
U)
    │   ├── diameter-gx.md            Gx (comunicación PCRF)
    │   ├── diameter-gy.md            Gy/Ro (comunicación OCS)
    │   └── s5s8-interface.md         S5/S8 (comunicación SGW-C)
    │
    └── Operaciones
        ├── session-management.md     Ciclo de vida de la sesión
PDN
        ├── charging-override.md      Anulación de carga en línea
        └── monitoring.md             Métricas de Prometheus y
alertas
```

Documentación por Tema

□ Comenzando

Documento	Descripción	Propósito
OPERATIONS.md	Guía principal de operaciones (este documento)	Visión general y inicio rápido

⚙ Configuración

Documento	Descripción	Líneas
configuration.md	Referencia completa de configuración de runtime.exs	1,600+
ue-ip-allocation.md	Gestión y asignación del pool de IP de UE	943
ipv6-dual-stack.md	Operación de PDN IPv6 / IPv4v6 a través de PGW-C y UPF	-
pco-configuration.md	Opciones de Configuración de Protocolo (DNS, P-CSCF, MTU)	344

□ Interfaces de Red

Documento	Descripción	Líneas
pfcp-interface.md	Interfaz PFCP/Sxb a PGW-U	1,355
diameter-gx.md	Interfaz Diameter Gx a PCRF (Control de Políticas)	941
diameter-gy.md	Interfaz Diameter Gy/Ro a OCS (Carga en Línea)	1,100+
charging-override.md	Anulación de carga en línea durante un incidente de OCS	-
s5s8-interface.md	Interfaz GTP-C S5/S8 a SGW-C	456

□ Operaciones y Monitoreo

Documento	Descripción	Líneas
session-management.md	Ciclo de vida y operaciones de la sesión PDN	435
monitoring.md	Métricas de Prometheus, paneles de Grafana, alertas	807
data-cdr-format.md	Formato de archivo CDR, configuración de URR, carga fuera de línea	847
qos-bearers.md	Gestión de QoS y bearers, control de políticas	448
troubleshooting.md	Procedimientos de resolución de problemas y problemas comunes	687

□ Características Avanzadas

Documento	Descripción	Líneas
pcscf-monitoring.md	Descubrimiento de P-CSCF y monitoreo de salud	894

Características de la Documentación

□ Diagramas Mermaid

Todos los documentos incluyen **gráficos Mermaid** para una comprensión visual:

- Diagramas de arquitectura
- Diagramas de secuencia (flujos de mensajes)
- Máquinas de estado
- Topología de red

□ Ejemplos Prácticos

Cada documento incluye:

- Ejemplos de configuración del mundo real
- Configuraciones listas para copiar y pegar
- Casos de uso comunes

□ Resolución de Problemas

Cada documento de interfaz incluye:

- Problemas comunes y soluciones
- Comandos de depuración
- Métricas para diagnóstico

□ Referencias Cruzadas

Los documentos están extensamente interconectados para facilitar la navegación.

Rutas de Lectura

Para Operadores de Red

1. OPERATIONS.md - Visión general (este documento)
2. configuration.md - Configuración
3. monitoring.md - Monitoreo
4. session-management.md - Operaciones diarias

Para Ingenieros de Red

1. OPERATIONS.md - Visión general de la arquitectura (este documento)
2. pfcp-interface.md - Control del plano de usuario
3. diameter-gx.md - Control de políticas
4. diameter-gy.md - Carga en línea
5. s5s8-interface.md - Gestión de sesiones
6. ue-ip-allocation.md - Gestión de IP

Para Configuración y Despliegue

1. configuration.md - Referencia completa
2. ue-ip-allocation.md - Pools de IP
3. pco-configuration.md - Parámetros de red
4. monitoring.md - Configurar monitoreo

Estadísticas del Documento

- **Total de Documentos:** 14
- **Total de Líneas:** ~10,900+
- **Tamaño Total:** ~265 KB
- **Diagramas Mermaid:** 75+
- **Ejemplos de Código:** 150+

Conceptos Clave Cubiertos

Arquitectura

- □ Separación del plano de control/usuario
- □ Arquitectura OTP/Elixir
- □ Supervisión de procesos
- □ Sesiones basadas en GenServer

Protocolos

- □ PFCP (Protocolo de Control de Reenvío de Paquetes)
- □ GTP-C v2 (Protocolo de Túneles GPRS)
- □ Diameter (RFC 6733)

Interfaces 3GPP

- □ Sxb (PGW-C ↔ PGW-U)
- □ Gx (PGW-C ↔ PCRF)
- □ Gy/Ro (PGW-C ↔ OCS)
- □ S5/S8 (SGW-C ↔ PGW-C)

Operaciones

- □ Gestión de sesiones
- □ Estrategias de asignación de IP
- □ Aplicación de QoS
- □ Integración de carga
- □ Monitoreo y alertas

Recursos Adicionales

Especificaciones 3GPP

Espec	Título
TS 29.274	GTP-C v2 (interfaz S5/S8)
TS 29.244	PFCP (interfaz Sxb)
TS 29.212	Interfaz Diameter Gx (Control de Políticas)
TS 32.299	Aplicaciones de Carga Diameter (Gy/Ro)
TS 32.251	Carga del dominio de Paquetes
TS 23.401	Arquitectura EPC

Documentación Relacionada

- Referencia de configuración: configuration.md - Referencia completa de `config/runtime.exs`

Anulación de Carga en Línea (Break-Glass)

La anulación de carga en línea es un interruptor a nivel de nodo. Saca la carga en línea (Gy/OCS) del camino de inmediato, sin necesidad de reinicio. Úselo durante un incidente de OCS, cuando el OCS no está saludable y los suscriptores se ven afectados.

Un reinicio no es una forma aceptable de desactivar la carga en línea. Un reinicio cierra cada sesión PDN activa en el nodo. La anulación cambia el comportamiento para las sesiones que ya están activas y para las sesiones que se conectan mientras está activa.

La carga fuera de línea no se ve afectada. El PGW-C continúa midiendo el uso y escribiendo CDRs mientras la anulación está activa. Consulte Formato de CDR.

Tabla de Contenidos

1. Cuándo Usarlo
2. Qué Hace la Anulación
3. Referencia de API
4. Procedimiento Operativo
5. Registro de Auditoría
6. Configuración
7. Métricas
8. Resolución de Problemas

Cuándo Usarlo

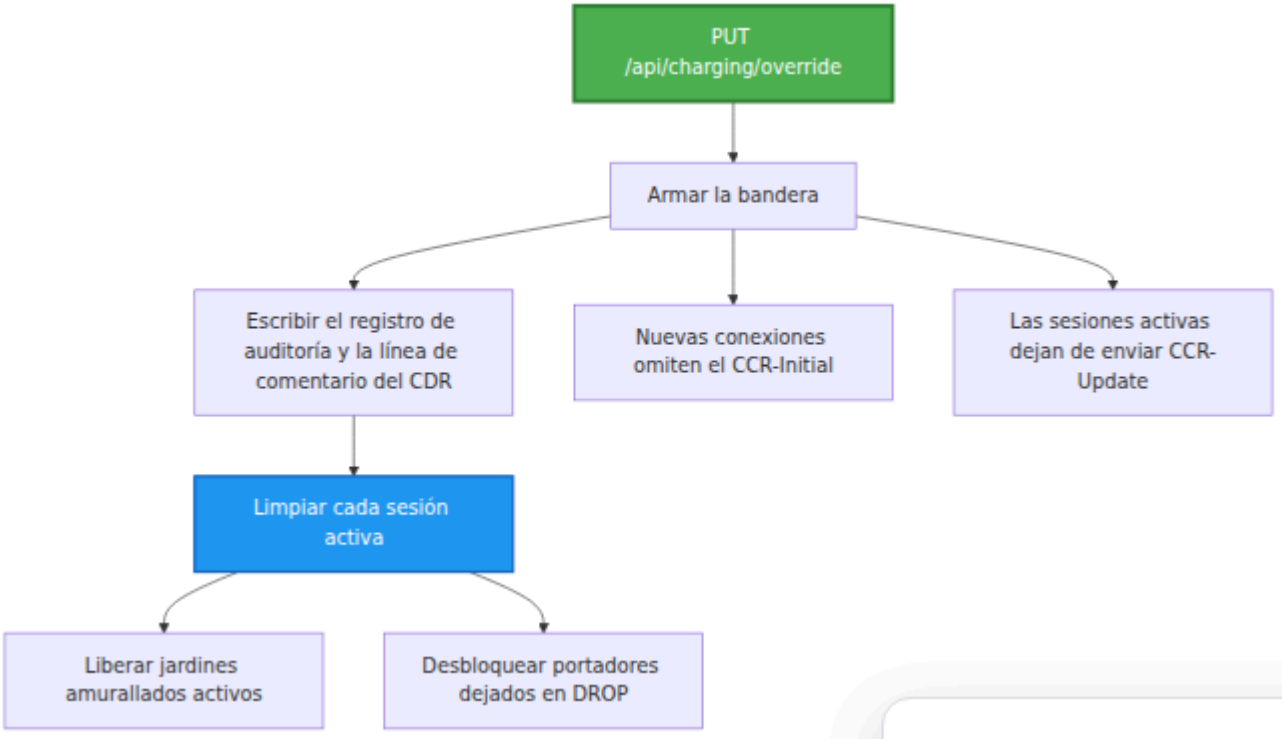
Utilice la anulación cuando el OCS cause un impacto en los suscriptores que no puede solucionar en el OCS. Tres modos de falla son comunes.

Modo de falla	Lo que ven los suscriptores	Lo que hace la anulación
El OCS rechaza o no responde al CCR-Initial	Nuevas conexiones se activan restringidas, o caen en el jardín amurallado	Nuevas conexiones no envían CCR-Initial y se activan con reenvío de tráfico
El OCS responde, pero su contabilidad es incorrecta	Los suscriptores son desconectados con saldo restante	Los jardines amurallados se liberan y los portadores bloqueados se desbloquean
El OCS deja reservas y drena paquetes	El saldo desaparece sin uso	No se envía más CCR-Update, por lo que la ventana no se informa y no se califica

No utilice la anulación para un solo suscriptor. Para mover una sesión dentro o fuera del jardín amurallado, use `PUT /api/charging/<imsi>`. Consulte Interfaz Diameter Gy.

El alcance de la anulación es un nodo. Si ejecuta más de un PGW-C, aplique la anulación a cada nodo. Una aplicación parcial es sobrevivible. Algunos suscriptores se recuperan, y el resto permanece como estaba.

Qué Hace la Anulación



Nuevas sesiones

Mientras la anulación está activa, el PGW-C trata la carga en línea como desactivada. Este es el mismo comportamiento que el valor de configuración `charging.online: :off`. El PGW-C no envía CCR-Initial. La conexión se completa y el portador por defecto reenvía tráfico.

La anulación tiene prioridad sobre la configuración local y el PCRF. Un Gx CCA que establece `Online` en habilitado no vuelve a habilitar la carga mientras la anulación está activa.

Sesiones existentes

Una bandera de configuración por sí sola ayuda solo a las sesiones que se conectan después de ella. Los suscriptores que ya están bloqueados son los que están sufriendo por el incidente. Cuando arma la anulación, el PGW-C limpia cada sesión activa y hace dos cosas.

1. **Liberar el jardín amurallado.** Si la sesión está en un jardín amurallado, el PGW-C envía una PFCP Modificación de Sesión que elimina la redirección.

Este es el mismo camino que se ejecuta cuando el OCS restaura el crédito.

2. **Desbloquear portadores bloqueados.** Si un portador tiene Reglas de Acción de Reenvío establecidas para aplicar-acción `DROP`, el PGW-C envía una Modificación de Sesión PFCP que los vuelve a establecer en `FORW`. Esto cubre las sesiones restringidas por la rama CCR-Initial `DIAMETER_USER_UNKNOWN`.

La limpieza es un esfuerzo máximo. Una sesión que no responde se cuenta como fallida y se nombra en el registro. La limpieza continúa con las sesiones restantes. El PGW-C ejecuta la limpieza en paralelo a través de las sesiones, por lo que el tiempo que toma está determinado por la respuesta más lenta del UPF, no por la suma de ellas.

Un caso no puede ser reparado. Si el OCS envió una Acción de Unidad Final de TERMINATE al conectarse, el PGW-C borró los parámetros de reenvío en esas reglas. El PGW-C no puede reconstruirlos a partir del estado de la sesión. El registro nombra cada regla que no pudo restaurar. El suscriptor debe volver a conectarse para recuperarse.

Sesiones que ya tienen una sesión Gy abierta

Mientras la anulación está activa, el PGW-C no envía CCR-Update para estas sesiones. El informe de uso es desechado en lugar de almacenarse en búfer. Esto es deliberado. La desactivación no debe facturar retroactivamente la ventana durante la cual la anulación estuvo activa.

Al desconectarse, el PGW-C no envía CCR-Terminate por defecto. Un CCR-Terminate libera la reserva en el OCS de manera limpia, pero uno por desconexión afecta a un OCS que ya está enfermo. El OCS recoge la reserva con su propio temporizador de sesión. Establezca `send_ccr_t` en `true` si desea que se envíe el CCR-Terminate de todos modos.

Desactivación

La desactivación devuelve el nodo a la carga normal de inmediato. No se necesita reinicio. El PGW-C no informa la ventana durante la cual la anulación estuvo activa. El uso en esa ventana se mide fuera de línea y se escribe en los CDRs, pero nunca llega al OCS.

Referencia de API

La anulación es un recurso singleton en la colección de carga. El identificador `override` está reservado. Ningún IMSI puede ser esa cadena.

Todas las rutas se sirven bajo el prefijo `/api` en la API OAM. Consulte Monitoreo de Operaciones en Tiempo Real.

Activar

```
PUT /api/charging/override
```

Cuerpo de la solicitud:

```
{
  "ttl_seconds": 3600,
  "reason": "Incidente OCS INC-1234",
  "actor": "noc@example.com",
  "send_ccr_t": false
}
```

Parámetro	Tipo	Requerido	Por defecto	Descripción
`ttl_seconds`	Entero	Sí	-	Segundos hasta que la anulación expire automáticamente. Mínimo `1`, máximo `86400` (24 horas).
`reason`	Cadena	Sí	-	Texto libre que dice por qué la anulación está activa. Aparece en el registro, el archivo CDR y `GET`.
`actor`	Cadena	No	IP del llamador	Quién activó la anulación. El PGW-C registra la dirección IP del llamador cuando omite esto.
`send_ccr_t`	Booleano	No	`false`	Establezca en `true` para aún enviar un Gy CCR-Terminate al desconectarse. Deje `false` para permanecer en silencio.

Respuesta:

```
{
  "online_charging": "off",
  "override": {
    "active": true,
    "reason": "Incidente OCS INC-1234",
    "actor": "noc@example.com",
    "ttl_seconds": 3600,
    "remaining_seconds": 3599,
    "activated_at": "2026-09-15T04:10:22.481Z",
    "expires_at": "2026-09-15T05:10:22.481Z",
    "send_ccr_t": false,
    "max_ttl_seconds": 86400
  },
  "relief": {
    "sessions_swept": 1842,
    "walled_gardens_released": 37,
    "bearers_ungated": 5,
    "failed": 0,
    "changed": [
      { "imsi": "313380000003530", "apn": "internet", "actions":
["walled_garden_released"] }
    ]
  }
}
```

Campo	Descripción
`online_charging`	`off` mientras la anulación está activa, `on` de lo contrario.
`override.active`	`true` mientras la anulación está armada y el TTL no ha expirado.
`override.remaining_seconds`	Segundos hasta la expiración automática. `null` cuando no hay anulación activa.
`relief.sessions_swept`	Cuántas sesiones activas el PGW-C pidió que eliminaran sus bloqueos de carga.
`relief.walled_gardens_released`	Cuántas sesiones salieron del jardín amurallado.
`relief.bearers_ungated`	Cuántas sesiones tuvieron portadores bloqueados restaurados a reenvío.
`relief.failed`	Cuántas sesiones no respondieron. Su estado no ha cambiado.
`relief.changed`	Las sesiones que realmente cambiaron, con la acción tomada en cada una.

El PGW-C rechaza la solicitud con `400 Bad Request` cuando `ttl_seconds` está ausente, fuera de rango o no es un entero, y cuando `reason` está ausente o en blanco.

Leer estado

```
GET /api/charging/override
```

La respuesta lleva los mismos campos `online_charging` y `override` que la respuesta de activación, con `remaining_seconds` contados desde el momento de la solicitud. No hay campo `relief`.

El punto final de lista `GET /api/charging` también lleva el estado de la anulación en un campo `charging_override`, junto al estado de carga por sesión.

Desactivar

```
DELETE /api/charging/override
```

Cuerpo de la solicitud (opcional):

```
{ "actor": "oncall@example.com" }
```

La respuesta lleva los mismos campos que `GET`, con `active` establecido en `false`.

Procedimiento Operativo

Siga estos pasos durante un incidente de OCS.

1. Confirme que el OCS es la causa. Verifique `GET /api/diameter?status=disconnected` para el estado del par Gy, y `GET /api/charging` para sesiones en el jardín amurallado.
2. Arme la anulación en el primer PGW-C. Dé un `reason` que nombre el ticket del incidente. Establezca `ttl_seconds` en un valor que cubra su tiempo de reparación esperado.
3. Lea el bloque `relief` en la respuesta. Confirme que `failed` es `0`. Si no lo es, consulte Resolución de Problemas.
4. Repita los pasos 2 y 3 en cada nodo PGW-C restante.
5. Confirme que la métrica `charging_override_active` lee `1` en cada nodo.
6. Repare el OCS.

7. Desactive la anulación en cada nodo con `DELETE /api/charging/override`.
8. Confirme que la métrica `charging_override_active` lee `0` en cada nodo, y que nuevas conexiones envían un CCR-Initial nuevamente.

Si no desactiva la anulación, esta expira automáticamente cuando el TTL vence. El PGW-C escribe una advertencia en el registro y una línea de comentario en el archivo CDR al expirar.

Registro de Auditoría

Una anulación que puede permanecer activa en silencio es una fuga de ingresos. El PGW-C registra cada cambio de estado en cuatro lugares.

Registro

El PGW-C escribe una `advertencia` en la activación, en la desactivación, en la expiración del TTL y en el re-armado después de un reinicio. Cada línea está precedida por `[CHARGING OVERRIDE]` y lleva el motivo, el actor y la fecha límite. La limpieza escribe una segunda `advertencia` con el conteo de sesiones cambiadas y fallidas.

Archivo CDR

El PGW-C escribe una línea de comentario en el archivo CDR que está abierto en ese momento. La escritura es asíncrona, por lo que un directorio de CDR en un montaje lento no puede detener o fallar la anulación en sí. Las líneas de comentario comienzan con `#`, el mismo marcador que usa el encabezado del archivo CDR, por lo que la mediación las omite. La línea permanece en el registro del archivo, que es lo que necesita cuando una ventana de tráfico no fue deliberadamente calificada.

```
# ANULACIÓN DE CARGA ACTIVADA en 2026-09-15T04:10:22.481Z: carga
en línea (Gy/OCS) desactivada a nivel de nodo; el uso en esta
ventana se mide fuera de línea pero NO se informa al OCS.
motivo=Incidente OCS INC-1234 actor=noc@example.com
ttl_seconds=3600 expires_at=2026-09-15T05:10:22.481Z
send_ccr_t=false
# ANULACIÓN DE CARGA DESACTIVADA en 2026-09-15T04:52:09.113Z:
carga en línea (Gy/OCS) reactivada a nivel de nodo. el uso entre
2026-09-15T04:10:22.481Z y 2026-09-15T04:52:09.113Z (2507s) no fue
informado al OCS. razón_original=Incidente OCS INC-1234
activado_por=noc@example.com desactivado_por=oncall@example.com
```

Los saltos de línea incrustados en el `reason` se aplanan a espacios. Un comentario nunca puede dividir un registro de CDR. Consulte Formato de CDR.

Métricas

Consulte Métricas. Alerta sobre `charging_override_active` para que un operador sea informado mientras la anulación esté activa.

Panel web

La página de Sesiones PGW muestra un banner mientras la anulación está activa. El banner lleva el motivo, el actor y el tiempo restante.

Configuración

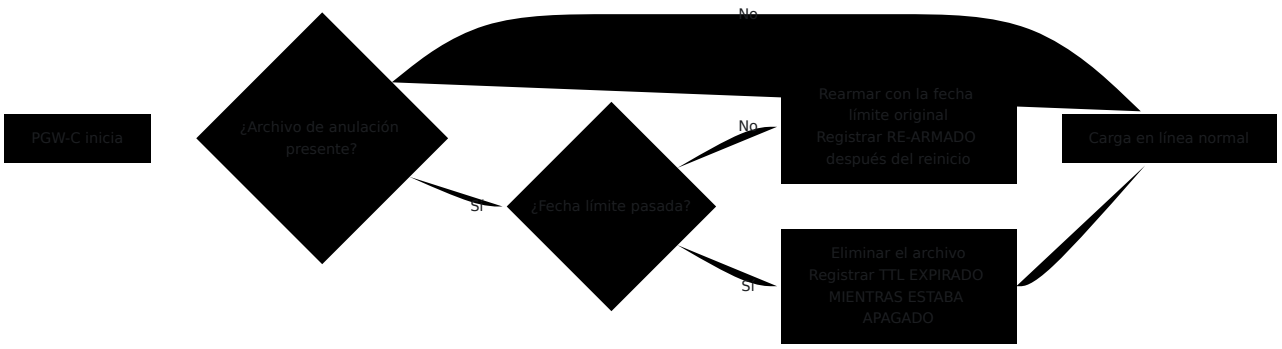
La anulación no necesita configuración para funcionar. Una clave opcional controla dónde se escribe el estado armado para que sobreviva a un reinicio.

```
config :pgw_c,
  # Donde se persiste la anulación armada a través de un reinicio
  charging_override_file: "/var/lib/pgw_c/charging_override.json"
```

Parámetro	Tipo	Requerido	Por defe
`charging_override_file`	Cadena	No	`/var/lib/pgw_c/chargi`

Comportamiento de reinicio

Un fallo durante un incidente no debe rearmar silenciosamente el corte para cada suscriptor. El PGW-C escribe la anulación armada en `charging_override_file` y la lee al inicio.



Un reinicio no extiende el TTL. El PGW-C mantiene el `expires_at` original.

Si el PGW-C no puede escribir el archivo, registra una advertencia y continúa. La anulación está en efecto en el nodo, pero no sobrevive a un reinicio. Verifique los permisos del sistema de archivos en el directorio.

Métricas

Métrica: `charging_override_active`
Tipo: Gauge
Descripción: `1` mientras la anulación a nivel de nodo desactiva la carga en línea, `0` de lo contrario.
Etiquetas: ninguna

Métrica: `charging_override_remaining_seconds`
Tipo: Gauge
Descripción: Segundos restantes antes de que la anulación expire automáticamente. `0` cuando no hay anulación activa.
Etiquetas: ninguna

Ambos medidores se actualizan en el intervalo de sondeo de métricas. Consulte Monitoreo y Métricas para el intervalo de sondeo y la configuración del exportador.

Consultas de ejemplo:

```
# Cualquier nodo con carga en línea omitida en este momento
max(charging_override_active)

# Nodos donde la anulación expira en menos de 10 minutos
charging_override_remaining_seconds > 0 and
charging_override_remaining_seconds < 600
```

Alerta de ejemplo:

```
- alert: OnlineChargingOverrideActive
  expr: charging_override_active == 1
  for: 5m
  labels:
    severity: critical
  annotations:
    summary: "La carga en línea está omitida en {{
$labels.instance }}"
    description: "El uso de suscriptores se mide para CDRs pero no
se califica en línea."
```

Resolución de Problemas

La solicitud de activación devuelve 400

Síntomas: El cuerpo de la respuesta menciona `ttl_seconds` o `reason`.

Posibles causas:

- `ttl_seconds` está ausente, `0`, negativo o mayor que `86400`
- `reason` está ausente o en blanco

Resolución:

1. Establezca `ttl_seconds` en un entero entre `1` y `86400`.
2. Establezca `reason` en texto que nombre el incidente.

La limpieza de alivio informa fallas

Síntomas: `relief.failed` es mayor que `0` en la respuesta de activación.

Posibles causas:

- Un proceso de sesión no respondió dentro del tiempo de espera de llamada
- El UPF no aceptó la Modificación de Sesión PFCP

Una sesión que se desconectó mientras se ejecutaba la limpieza no se cuenta como una falla. Ya no impone nada, por lo que no hay nada que liberar.

Resolución:

1. Busque en el registro `[CHARGING OVERRIDE] no se pudo liberar la aplicación de carga`.
2. Verifique la accesibilidad del UPF con `GET /api/upf`.
3. Ejecute `PUT /api/charging/override` nuevamente una vez que el UPF esté saludable. La limpieza es segura de repetir. Una sesión que no está bloqueada no se toca.

Un suscriptor sigue bloqueado después de la limpieza

Síntomas: `GET /api/charging/<imsi>` muestra que el jardín amurallado está liberado, pero el tráfico no fluye.

Posibles causas:

- El OCS envió una Acción de Unidad Final de TERMINATE al conectarse. Los parámetros de reenvío en ese portador fueron borrados y no pueden ser reconstruidos.

Resolución:

1. Busque en el registro `No se puede desbloquear FAR(s)` con ese IMSI.
2. Pida al suscriptor que se vuelva a conectar. Una nueva conexión se activa con reenvío de tráfico mientras la anulación está activa.

La anulación volvió después de un reinicio

Síntomas: El registro lleva `[CHARGING OVERRIDE] RE-ARMADO después del reinicio`.

Este es el comportamiento diseñado. La anulación todavía estaba dentro de su TTL cuando el nodo se reinició.

Resolución:

1. Ejecute `DELETE /api/charging/override` si ya no la desea.
2. De lo contrario, espere a que el TTL venza.

La carga en línea está desactivada y no hay anulación activa

Síntomas: No se envía CCR-Initial, y `GET /api/charging/override` informa `active: false`.

Posibles causas:

- `charging.online` está establecido en `:off` en la configuración en tiempo de ejecución
- `gy.enabled` es `false`
- El PCRF estableció el Gx CCA `Online` AVP en deshabilitado

Resolución:

1. Verifique los bloques `charging` y `gy`. Consulte Referencia de Configuración.
2. Verifique el Gx CCA con `GET /api/charging/<imsi>`. Consulte Interfaz Diameter Gx.

Documentación Relacionada

- Interfaz Diameter Gy - carga en línea, cuota y jardín amurallado
- Formato de CDR - carga fuera de línea y el archivo CDR

- Monitoreo y Métricas - exportador de métricas y paneles
- Resolución de Problemas - procedimientos generales de resolución de problemas
- Guía de Operaciones - punto de entrada

Guía de Configuración de OmniPGW

Referencia Completa para la Configuración de runtime.exs

por Omnitouch Network Services

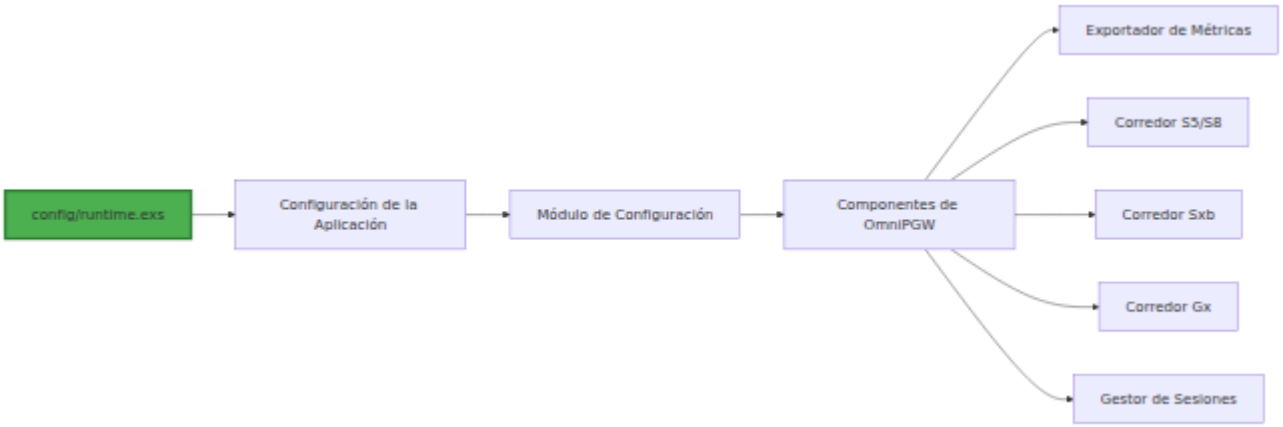
Tabla de Contenidos

1. Descripción General
2. Estructura del Archivo de Configuración
3. Configuración de Métricas
4. Configuración de Diameter/Gx
5. Configuración de S5/S8
6. Configuración de Gn/Gp (GGSN)
7. Configuración de Sxb/PFCP
    - Estrategias de Selección de UPF
    - Balanceo de Carga con Grupos de UPF
    - Selección Basada en DNS
    - Modo de Prueba
8. Configuración del Pool de IP de UE
9. Configuración de PCO
10. Configuración de API OAM
11. Ejemplo Completo
12. Validación de Configuración

Descripción General

OmniPGW utiliza **configuración en tiempo de ejecución** definida en `config/runtime.exs`. Este archivo se evalúa en el **inicio de la aplicación** y permite una configuración dinámica basada en variables de entorno o fuentes externas.

Filosofía de Configuración



Principios Clave:

- **Fuente Única de Verdad** - Toda la configuración en un solo archivo
- **Seguridad de Tipo** - Configuración validada al inicio
- **Flexibilidad de Entorno** - Soporte para desarrollo, pruebas, producción
- **Defaults Claros** - Defaults sensatos con sobrescrituras explícitas

---

Estructura del Archivo de Configuración

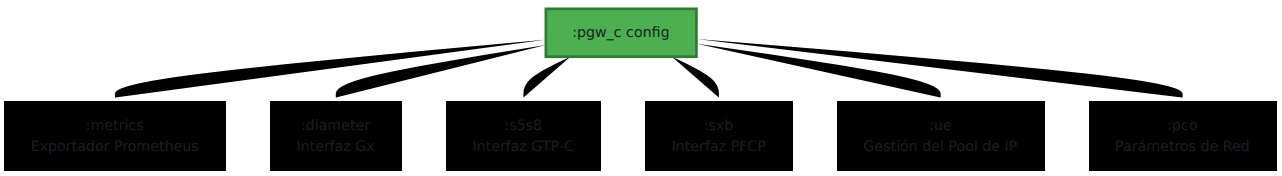
Ubicación del Archivo

```
pgw_c/
├── config/
│   ├── config.exs         # Configuración base (importa
runtime.exs)
│   ├── dev.exs            # Configuración específica de
desarrollo
│   ├── prod.exs           # Configuración específica de
producción
│   └── runtime.exs        # ← Archivo de configuración principal
```

Estructura de Nivel Superior

```
# config/runtime.exs
import Config

config :logger, level: :info

config :pgw_c,
  metrics: %{...},
  diameter: %{...},
  s5s8: %{...},
  sxb: %{...},
  ue: %{...},
  pco: %{...}
```

Secciones de Configuración



Configuración de Métricas

Propósito

Configurar el exportador de métricas Prometheus para monitorear OmniPGW.

Bloque de Configuración

```
config :pgw_c,
  metrics: %{
    # Habilitar/deshabilitar exportador de métricas
    enabled: true,

    # Dirección IP para enlazar el servidor HTTP
    ip_address: "0.0.0.0",

    # Puerto para el endpoint de métricas
    port: 9090,

    # Cada cuánto tiempo sondear registros (milisegundos)
    registry_poll_period_ms: 10_000
  }
```

Parámetros

Parámetro	Tipo	Predeterminado	Descripción
`enabled`	Booleano	`true`	Habilitar exportador de métricas
`ip_address`	Cadena (IP)	`"0.0.0.0"`	Dirección de enlace (0.0.0.0 = todas las interfaces)
`port`	Entero	`9090`	Puerto HTTP para el endpoint `/metrics`
`registry_poll_period_ms`	Entero	`10_000`	Intervalo de sondeo para conteos de registro

Ejemplos

Producción - Enlazar a IP específica:

```
metrics: %{
  enabled: true,
  ip_address: "10.0.0.20",  # Red de gestión
  port: 9090,
  registry_poll_period_ms: 5_000  # Sondear cada 5 segundos
}
```

Desarrollo - Solo localhost:

```
metrics: %{
  enabled: true,
  ip_address: "127.0.0.1",
  port: 42069,  # Puerto no estándar
  registry_poll_period_ms: 10_000
}
```

Deshabilitar métricas:

```
metrics: %{
  enabled: false
}
```

Accediendo a Métricas

```
# Endpoint predeterminado
curl http://<ip_address>:<port>/metrics

# Ejemplo
curl http://10.0.0.20:9090/metrics
```

Ver: Guía de Monitoreo y Métricas para documentación detallada de métricas.

Configuración de Diameter/Gx

Propósito

Configurar el protocolo Diameter para la interfaz Gx (comunicación PCRF).

Bloque de Configuración

```
config :pgw_c,
  diameter: %{
    # Dirección IP para escuchar conexiones Diameter
    listen_ip: "0.0.0.0",

    # Identidad Diameter de OmniPGW (Origin-Host)
    host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",

    # Dominio Diameter de OmniPGW (Origin-Realm)
    realm: "epc.mnc001.mcc001.3gppnetwork.org",

    # Lista de pares PCRF
    peer_list: [
      %{
        # Identidad Diameter PCRF
        host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",

        # Dominio PCRF
        realm: "epc.mnc001.mcc001.3gppnetwork.org",

        # Dirección IP PCRF
        ip: "10.0.0.30",

        # Iniciar conexión con PCRF
        initiate_connection: true
      }
    ]
  }
```

Parámetros

Parámetro	Tipo	Requerido	Descripción
`listen_ip`	Cadena (IP)	Sí	Dirección de escucha Diameter
`host`	Cadena (FQDN)	Sí	Origin-Host de OmniPGW (debe ser FQDN)
`realm`	Cadena (Dominio)	Sí	Origin-Realm de OmniPGW
`peer_list`	Lista	Sí	Configuraciones de pares PCRF

Configuración de Pares:

Parámetro	Tipo	Requerido	Descripción
`host`	Cadena (FQDN)	Sí	Identidad Diameter PCRF
`realm`	Cadena (Dominio)	Sí	Dominio PCRF
`ip`	Cadena (IP)	Sí	Dirección IP PCRF
`initiate_connection`	Booleano	Sí	Si OmniPGW se conecta al PCRF

Formato FQDN

Las identidades Diameter DEBEN ser FQDNs:

```
# CORRECTO
host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org"

# INCORRECTO
host: "omnipgw"              # No es un FQDN
host: "10.0.0.20"            # IP no permitida
```

Formato 3GPP:

```
<hostname>.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Ejemplos:
- omnipgw.epc.mnc001.mcc001.3gppnetwork.org  (MCC=001, MNC=001)
- pgw-c.epc.mnc260.mcc310.3gppnetwork.org   (MCC=310, MNC=260 - T-Mobile EE. UU.)
```

Ejemplos

Un solo PCRF:

```
diameter: %{
  listen_ip: "0.0.0.0",
  host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
  realm: "epc.mnc001.mcc001.3gppnetwork.org",
  peer_list: [
    %{
      host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.0.0.30",
      initiate_connection: true
    }
  ]
}
```

Múltiples PCRFs (Redundancia):

```
diameter: %{
  listen_ip: "0.0.0.0",
  host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
  realm: "epc.mnc001.mcc001.3gppnetwork.org",
  peer_list: [
    %{
      host: "pcrf-primary.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.0.1.30",
      initiate_connection: true
    },
    %{
      host: "pcrf-backup.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.0.2.30",
      initiate_connection: true
    }
  ]
}
```

Conexión Iniciada por PCRF:

```
diameter: %{
  listen_ip: "0.0.0.0",
  host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
  realm: "epc.mnc001.mcc001.3gppnetwork.org",
  peer_list: [
    %{
      host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.0.0.30",
      initiate_connection: false  # Esperar a que PCRF se conecte
    }
  ]
}
```

Ver: Documentación de la Interfaz Diameter Gx

Configuración de S5/S8

Propósito

Configurar la interfaz GTP-C para la comunicación con SGW-C.

Bloque de Configuración

```
config :pgw_c,
  s5s8: %{
    # Dirección IPv4 local para la interfaz S5/S8
    local_ipv4_address: "10.0.0.20",

    # Opcional: Dirección IPv6 local
    local_ipv6_address: nil,

    # Opcional: Sobrescribir el puerto GTP-C predeterminado (2123)
    local_port: 2123,

    # Tiempo de espera para solicitudes GTP-C en milisegundos
(predeterminado: 500ms)
    # Tiempo de espera por intento al esperar respuestas GTP-C
    request_timeout_ms: 500,

    # Número de intentos de reintento para solicitudes GTP-C
(predeterminado: 3)
    # Tiempo máximo total de espera = request_timeout_ms *
request_attempts
    request_attempts: 3
  }
```

Parámetros

Parámetro	Tipo	Predeterminado	Descripción
`local_ipv4_address`	Cadena (IPv4)	Requerido	Dirección IPv4 de la interfaz S5/S8
`local_ipv6_address`	Cadena (IPv6)	`nil`	Dirección IPv6 de la interfaz S5/S8 (opcional)
`local_port`	Entero	`2123`	Puerto UDP para GTP-C (puerto estándar 2123)
`request_timeout_ms`	Entero	`500`	Tiempo de espera por intento de reintento en milisegundos
`request_attempts`	Entero	`3`	Número de intentos de reintento antes de rendirse

Detalles del Protocolo

- **Protocolo:** GTP-C Versión 2
- **Transporte:** UDP
- **Puerto Estándar:** 2123
- **Dirección:** Recibe de SGW-C

Ejemplos

Solo IPv4 (Común):

```
s5s8: %{
  local_ipv4_address: "10.0.0.20"
}
```

IPv4 + IPv6 Doble Pila:

```
s5s8: %{
  local_ipv4_address: "10.0.0.20",
  local_ipv6_address: "2001:db8::20"
}
```

Puerto Personalizado (No Estándar):

```
s5s8: %{
  local_ipv4_address: "10.0.0.20",
  local_port: 2124  # Puerto personalizado
}
```

Red de Alta Latencia:

```
s5s8: %{
  local_ipv4_address: "10.0.0.20",
  request_timeout_ms: 1500,  # 1.5 segundos por intento
  request_attempts: 3         # Total: 4.5 segundos máximo
}
```

Configuración de Tiempo de Espera

La interfaz S5/S8 utiliza tiempos de espera configurables para transacciones de solicitud/respuesta GTP-C (Solicitud de Crear Bearer, Solicitud de Eliminar Bearer).

Cálculo del Tiempo Total de Espera:

```
Tiempo Máximo Total de Espera = request_timeout_ms × request_attempts
Predeterminado: 500ms × 3 = 1.5 segundos
```

Directrices de Ajuste:

Latencia de Red	Tiempo de Espera Recomendado	Tiempo Total de Espera
Baja latencia (<50ms)	200-300ms	600-900ms
Normal (50-150ms)	500ms (predeterminado)	1.5s
Alta latencia (>150ms)	1000-2000ms	3-6s
Satélite/inestable	2000-3000ms	6-9s

Cuándo Ajustar:

- **Aumentar el tiempo de espera** si se ven frecuentes errores de "Tiempo de espera de Solicitud de Crear Bearer" pero Wireshark muestra respuestas llegando
- **Disminuir el tiempo de espera** para una detección de fallos más rápida en entornos de baja latencia
- **Aumentar los intentos de reintento** para redes poco fiables con pérdida de paquetes

Comportamiento del Tiempo de Espera:

- En caso de tiempo de espera, se registra un error: `"Tiempo de espera de Solicitud de Crear Bearer"`
- Error de Diameter devuelto al PCRF: Código de Resultado 5012 (UNABLE_TO_COMPLY)
- El Bearer permanece en almacenamiento temprano para limpieza cuando llega Charging-Rule-Remove

Planificación de Red

Selección de Dirección IP:

- Utilizar una red de gestión/señalización dedicada
- Asegurar la alcanzabilidad desde todos los nodos SGW-C
- Considerar redundancia (VRRP/HSRP) para HA

Reglas de Firewall:

```
# Permitir GTP-C desde SGW-C
iptables -A INPUT -p udp --dport 2123 -s <sgw_c_network> -j ACCEPT
```

Configuración de Gn/Gp (GGSN)

Propósito

Configurar la interfaz GTP-C v1 para la comunicación con SGSNs, habilitando la funcionalidad GGSN para redes 2G/3G.

Bloque de Configuración

```
config :pgw_c,
  gn: %{
    # Dirección IPv4 local para la interfaz Gn
    local_ipv4_address: "10.0.0.20",

    # Opcional: Dirección IPv6 local (la mayoría de las redes
2G/3G son solo IPv4)
    local_ipv6_address: nil,

    # Puerto GTP-C (compartido con S5/S8)
    local_port: 2123
  },

  # Servidores DNS devueltos en PCO (compartidos con S5/S8)
  dns: %{
    primary_ipv4: {8, 8, 8, 8},
    secondary_ipv4: {8, 8, 4, 4}
  }
```

Parámetros

Parámetro	Tipo	Predeterminado	Descripción
`local_ipv4_address`	Cadena (IPv4)	Requerido	Dirección IPv4 de la interfaz Gn (dirección GGSN)
`local_ipv6_address`	Cadena (IPv6)	`nil`	Dirección IPv6 de la interfaz Gn (opcional, raramente utilizada)
`local_port`	Entero	`2123`	Puerto UDP para GTP-C v1 (compartido con S5/S8)

Parámetros DNS

Parámetro	Tipo	Predeterminado	Descripción
`primary_ipv4`	Tupla	`{8, 8, 8, 8}`	Servidor DNS primario para respuesta PCO
`secondary_ipv4`	Tupla	`{8, 8, 4, 4}`	Servidor DNS secundario para respuesta PCO

Detalles del Protocolo

- **Protocolo:** GTP-C Versión 1 (3GPP TS 29.060)
- **Transporte:** UDP
- **Puerto Estándar:** 2123 (compartido con GTP-C v2)
- **Dirección:** Recibe de SGSNs

Coexistencia con S5/S8

OmniPGW puede operar como PGW (4G) y GGSN (2G/3G) simultáneamente:

- Ambas interfaces comparten el puerto UDP 2123
- La versión GTP se detecta automáticamente a partir de los encabezados de mensaje
- La misma dirección IP puede servir tanto tráfico 4G como 2G/3G
- Infraestructura compartida: pools de IP, UPF/PFCP, carga en línea

Ver: Documentación de la Interfaz Gn/Gp

Configuración de Sxb/PFCP

Propósito

Configurar la interfaz PFCP para la comunicación con PGW-U (Plano de Usuario).

Bloque de Configuración

```
config :pgw_c,
  sxb: %{
    # Dirección IP local para la comunicación PFCP
    local_ip_address: "10.0.0.20",

    # Opcional: Sobrescribir el puerto PFCP predeterminado (8805)
    local_port: 8805
  }
```

Parámetros

Parámetro	Tipo	Predeterminado	Descripción
`local_ip_address`	Cadena (IP)	Requerido	Dirección de escucha PFCP
`local_port`	Entero	`8805`	Puerto UDP PFCP

> **Importante:**
>
> - **Todos los pares UPF se registran automáticamente** desde la configuración de `upf_selection` (reglas + pool de respaldo) al inicio
> - Los UPFs registrados automáticamente utilizan defaults sensatos:
>   - Nombre autogenerado: `"UPF-<ip>:<port>"`
>   - Asociación PFCP pasiva (esperar a que UPF inicie)
>   - Intervalo de latido de 5 segundos
> - Las reglas y pools de selección de UPF se configuran en la sección separada `upf_selection`. Ver Estrategias de Selección de UPF a continuación.
> - Se admite el registro dinámico de UPF para UPFs descubiertos por DNS que no están en la configuración

Ejemplos

Configuración Mínima:

```
sxb: %{
  local_ip_address: "10.0.0.20"
}

# Todos los UPFs en upf_selection se registrarán automáticamente
con:
# - Nombre autogenerado: "UPF-10.0.0.21:8805"
# - Asociación PFCP pasiva (esperar a que UPF se conecte)
# - Intervalo de latido de 5 segundos
```

Puerto PFCP Personalizado:

```
sxb: %{
  local_ip_address: "10.0.0.20",
  local_port: 8806  # Puerto PFCP no estándar
}
```

Ejemplo Completo con Selección de UPF:

```
sxb: %{
  local_ip_address: "10.0.0.20"
},
upf_selection: %{
  rules: [
    %{
      name: "Pool IMS",
      priority: 10,
      match_field: :apn,
      match_regex: ~r/^ims$/,
      upf_pool: [
        %{remote_ip_address: "10.0.1.21", remote_port: 8805,
weight: 100},
        %{remote_ip_address: "10.0.1.22", remote_port: 8805,
weight: 100}
      ]
    }
  ],
  fallback_pool: [
    %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight:
100}
  ]
}
# Todos los 3 UPFs (10.0.1.21, 10.0.1.22, 10.0.2.21) se registran
automáticamente
```

Selección Basada en DNS (Registro Dinámico):

```
sxb: %{
  local_ip_address: "10.0.0.20"
},
upf_selection: %{
  dns_enabled: true,
  dns_query_priority: [:ecgi, :tai],
  dns_suffix: "epc.3gppnetwork.org",
  fallback_pool: [
    %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight:
100}
  ]
}
# Los UPFs descubiertos por DNS se registrarán dinámicamente en el
primer uso
```

Estrategias de Selección de UPF

Importante: La configuración de selección de UPF se ha simplificado. Todos los pares UPF se registran automáticamente desde la configuración de `upf_selection`.

Estructura de Configuración

La selección de UPF se configura en la sección **`upf_selection`** que define:

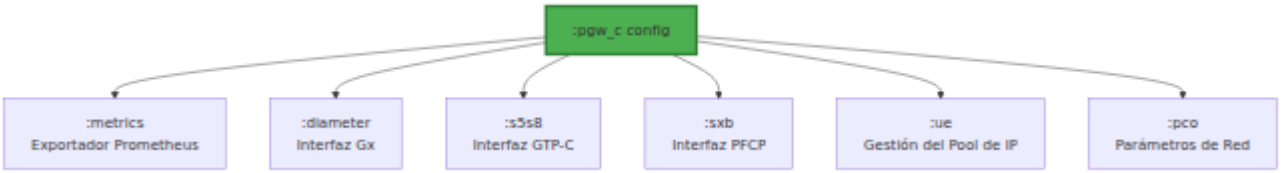
1. **Reglas Estáticas** - Enrutamiento basado en patrones con pools de balanceo de carga
2. **Configuraciones de DNS** - Descubrimiento dinámico de UPF basado en ubicación
3. **Pool de Respaldo** - Pool predeterminado cuando no coinciden reglas y DNS falla

Orden de Prioridad de Selección

1. **Reglas Estáticas** (Mayor Prioridad) - Enrutamiento basado en patrones con pools de balanceo de carga

2. **Selección Basada en DNS** (Menor Prioridad) - Descubrimiento dinámico de UPF basado en ubicación
3. **Pool de Respaldo** (Menor Prioridad) - Pool predeterminado cuando no coinciden reglas y DNS falla

Flujo de Decisión de Selección de UPF



Campos de Coincidencia Disponibles

Las reglas estáticas pueden coincidir en cualquiera de estos atributos de sesión:

Campo de Coincidencia	Descripción	Patrón de Ejemplo
`:imsi`	Identidad Internacional del Suscriptor Móvil	`^001001.*` (red de prueba)
`:apn`	Nombre del Punto de Acceso / DNN	`^internet\.` o `^ims\.`
`:serving_network_plmn_id`	Identificador de la red de servicio	`^001001$`
`:sgw_ip_address`	Dirección IP de SGW	`^10\.100\..*`
`:uli_tai_plmn_id`	ID de PLMN del Área de Seguimiento	`^313.*`
`:uli_ecgi_plmn_id`	ID de PLMN de la Celda E-UTRAN	`^313.*`

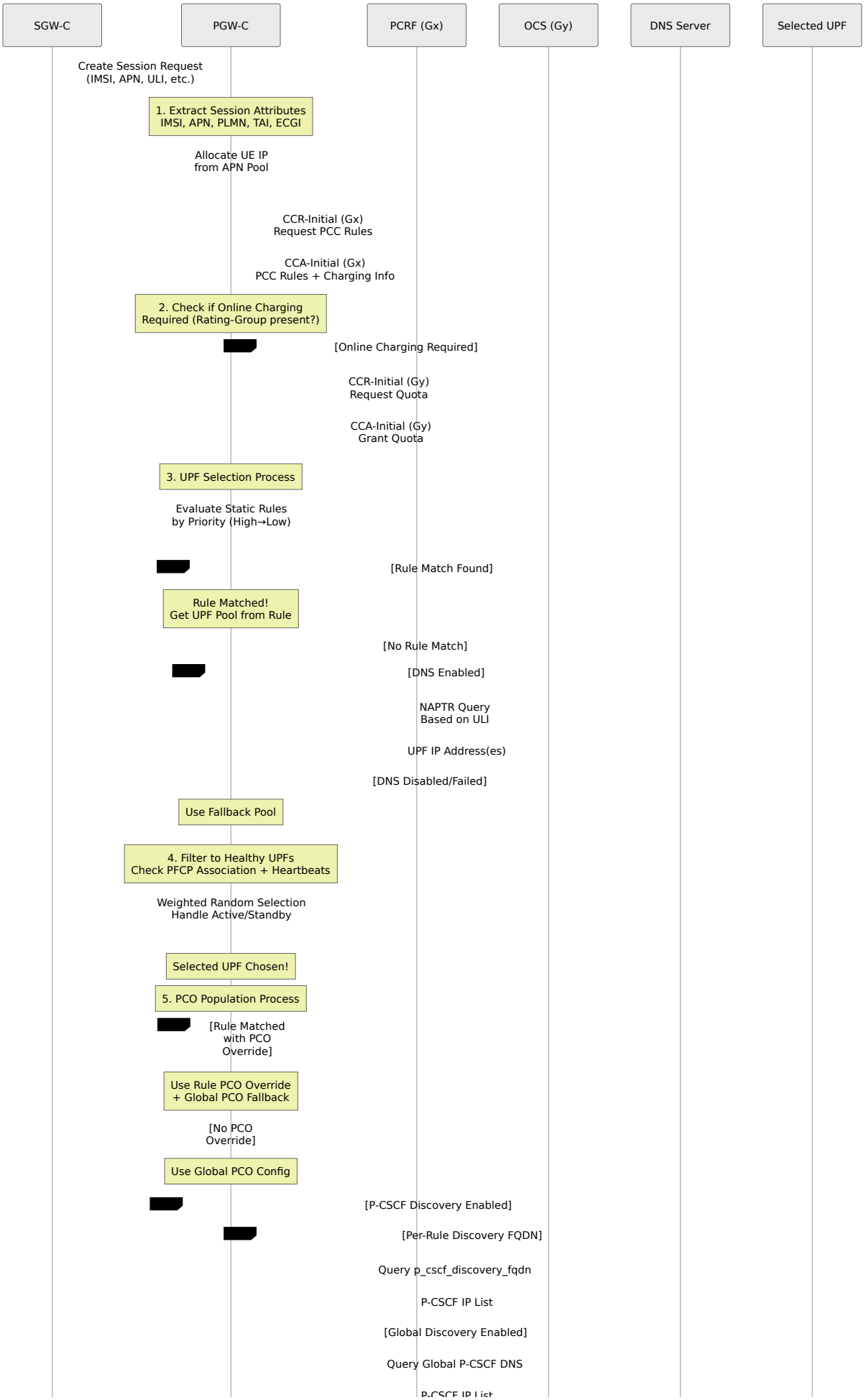
Comparación de Métodos de Selección

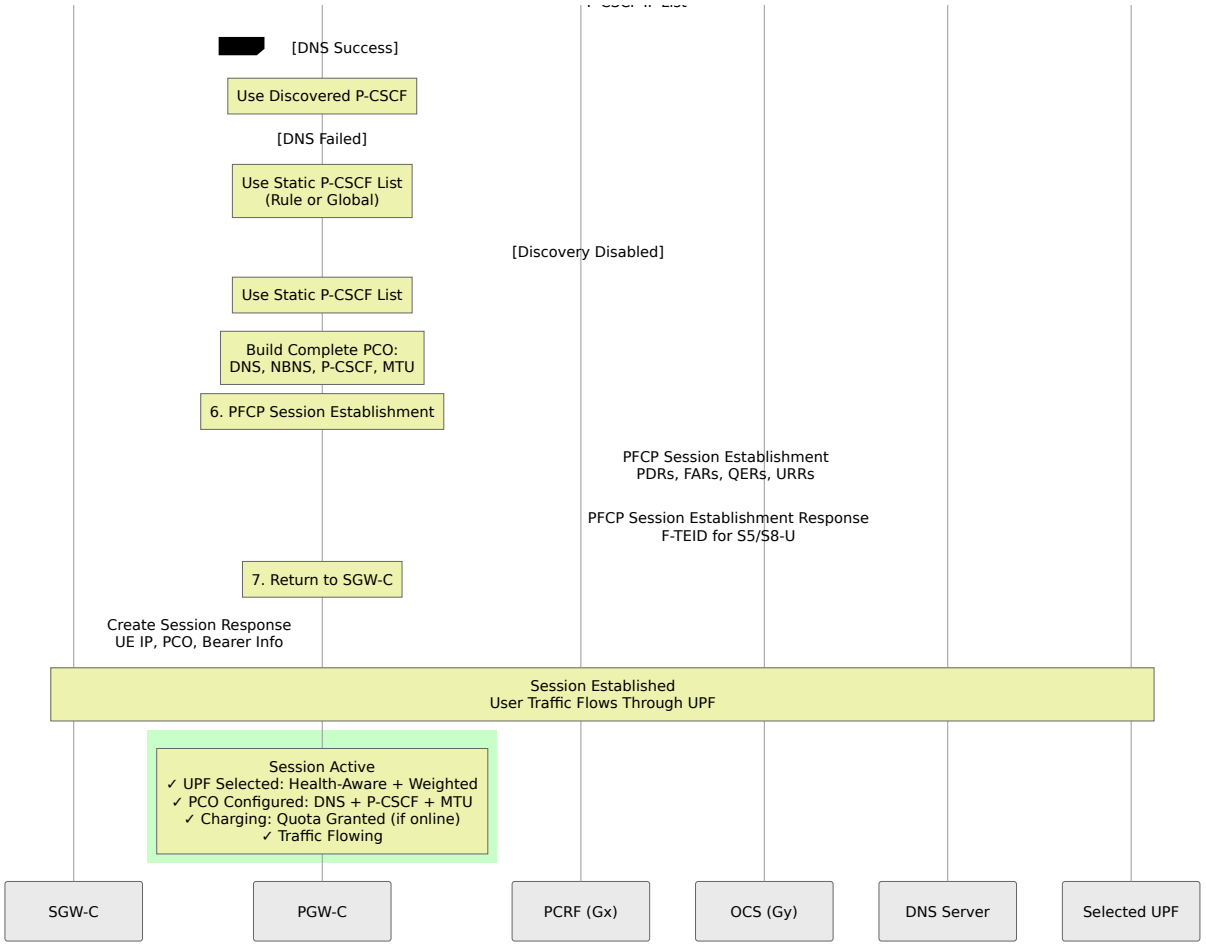
Método	Cuándo Usar	Pros	Contras
Pools de UPF	Despliegues de producción	Balanceo de carga, HA, pesos flexibles	Requiere múltiples UPFs
Basado en APN	Diferenciación de servicios	Enrutar IMS/Internet por separado	Configuración estática
Basado en IMSI	Escenarios de itinerancia	Enrutamiento geográfico	Complejidad de regex
Basado en DNS	MEC/Computación en el borde	Dinámico, consciente de la ubicación	Requiere infraestructura DNS
Pool de Respaldo	Red de seguridad	Siempre tener un UPF	Puede no ser óptimo
Modo de Prueba	Pruebas de configuraciones	Pruebas seguras	Sin tráfico real

---

Flujo Completo de Establecimiento de Sesión

Este diagrama muestra el flujo completo de establecimiento de sesión de extremo a extremo, incluyendo la selección de UPF y la población de PCO:


SGW-C
PGW-C
PCRF (Gx)
OCS (Gy)
DNS Server
Selected UPF
Create Session Request
(IMSI, APN, ULI, etc.)
1. Extract Session Attributes
IMSI, APN, PLMN, TAI, ECGI
Allocate UE IP
from APN Pool
CCR-Initial (Gx)
Request PCC Rules
CCA-Initial (Gx)
PCC Rules + Charging Info
2. Check if Online Charging
Required (Rating-Group present?)
[Online Charging Required]
CCR-Initial (Gy)
Request Quota
CCA-Initial (Gy)
Grant Quota
3. UPF Selection Process
Evaluate Static Rules
by Priority (High→Low)
[Rule Match Found]
Rule Matched!
Get UPF Pool from Rule
[No Rule Match]
[DNS Enabled]
NAPTR Query
Based on ULI
UPF IP Address(es)
[DNS Disabled/Failed]
Use Fallback Pool
4. Filter to Healthy UPFs
Check PFCP Association + Heartbeats
Weighted Random Selection
Handle Active/Standby
Selected UPF Chosen!
5. PCO Population Process
[Rule Matched
with PCO
Override]
Use Rule PCO Override
+ Global PCO Fallback
[No PCO
Override]
Use Global PCO Config
[P-CSCF Discovery Enabled]
[Per-Rule Discovery FQDN]
Query p_cscf_discovery_fqdn
P-CSCF IP List
[Global Discovery Enabled]
Query Global P-CSCF DNS
P-CSCF IP List



Puntos Clave de Decisión:

1. **Prioridad de Selección de UPF:**
   - Reglas Estáticas (Coincidencia de Patrón) → Descubrimiento DNS → Pool de Respaldo
   - Filtrado de salud aplicado en todas las etapas
   - Lógica Activa/Standby para alta disponibilidad
   - **Ver:** Interfaz PFCP para detalles de comunicación de UPF
2. **Prioridad de Población de PCO:**
   - Anulación de PCO de Regla → Descubrimiento DNS de P-CSCF → Configuración Global de PCO
   - Fusión por campo (la regla anula campos específicos, lo global proporciona valores predeterminados)
   - **Ver:** Configuración de PCO para parámetros detallados de PCO
3. **Prioridad de Descubrimiento de P-CSCF:**

- FQDN por Regla → Descubrimiento DNS Global → PCO de Regla Estática → PCO Estático Global
- **Ver:** Monitoreo de P-CSCF para métricas de descubrimiento y seguimiento de salud

4. **Integración de Cargos:**
   - PCRF determina si se requiere carga en línea (Rating-Group + Online=1)
   - OCS concede cuota antes del establecimiento de la sesión
   - PGW-C rastrea la cuota y solicita más a través de CCR-Update
   - **Ver:** Interfaz Diameter Gx y Interfaz Diameter Gy para detalles de carga

Ejemplo Completo de Configuración

Aquí hay un ejemplo completo que muestra la selección de UPF de múltiples pools con registro automático de pares:

```
config :pgw_c,
  # Interfaz PFCP - Todos los UPFs se registran automáticamente
desde upf_selection
  sxb: %{
    local_ip_address: "127.0.0.20"
  },

  # Lógica de Selección de UPF - Todos los UPFs definidos aquí se
registran automáticamente
  upf_selection: %{
    # Configuraciones de selección basadas en DNS
    dns_enabled: false,
    dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
    dns_suffix: "epc.3gppnetwork.org",
    dns_timeout_ms: 5000,

    # Reglas de selección estáticas (evaluadas en orden de
prioridad)
    rules: [
      # Regla 1: Tráfico IMS - Mayor Prioridad
      %{
        name: "IMS Traffic",
        priority: 20,
        match_field: :apn,
        match_regex: "^ims",
        upf_pool: [
          %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80},
          %{remote_ip_address: "10.100.2.22", remote_port: 8805,
weight: 20}
        ]
      },

      # Regla 2: APN Empresarial
      %{
        name: "Enterprise Traffic",
        priority: 15,
        match_field: :apn,
        match_regex: "^(enterprise|corporate)\.apn",
        upf_pool: [
          %{remote_ip_address: "10.100.3.21", remote_port: 8805,
weight: 100}
        ]
```

```
      },

      # Regla 3: Tráfico de Internet - Balanceado
      %{
        name: "Internet Traffic",
        priority: 5,
        match_field: :apn,
        match_regex: "^internet",
        upf_pool: [
          %{remote_ip_address: "10.100.1.21", remote_port: 8805,
weight: 33},
          %{remote_ip_address: "10.100.1.22", remote_port: 8805,
weight: 33},
          %{remote_ip_address: "10.100.1.23", remote_port: 8805,
weight: 34}
        ]
      }
    ],

    # Pool de respaldo - Usado cuando no hay coincidencias de
reglas y DNS falla
    fallback_pool: [
      %{remote_ip_address: "127.0.0.21", remote_port: 8805,
weight: 100}
    ]
  }
```

Características Clave

Formato Actual:

- **Registro Automático**: Todos los UPFs de `upf_selection` se registran automáticamente al inicio
- **Configuración Centralizada**: Toda la selección de UPF y configuración de pares en una sección
- **Pools Requeridos**: Todas las reglas utilizan el formato `upf_pool` (incluso para un solo UPF)
- **Respaldo Estructurado**: `fallback_pool` dedicado con distribución ponderada

- **Integración DNS**: Configuraciones de DNS junto a las reglas de selección
- **Registro Dinámico**: Los UPFs descubiertos por DNS se registran automáticamente en el primer uso
- **Monitoreo de Salud**: Todos los UPFs configurados son monitoreados con latidos de 5 segundos

Migración desde el Formato Anterior:

- Eliminado: campo `sxb.peer_list` (ya no es necesario)
- Eliminado: `selection_list` incrustado en configuraciones de pares
- Todas las definiciones de UPF ahora van en las reglas de `upf_selection` y el pool de respaldo

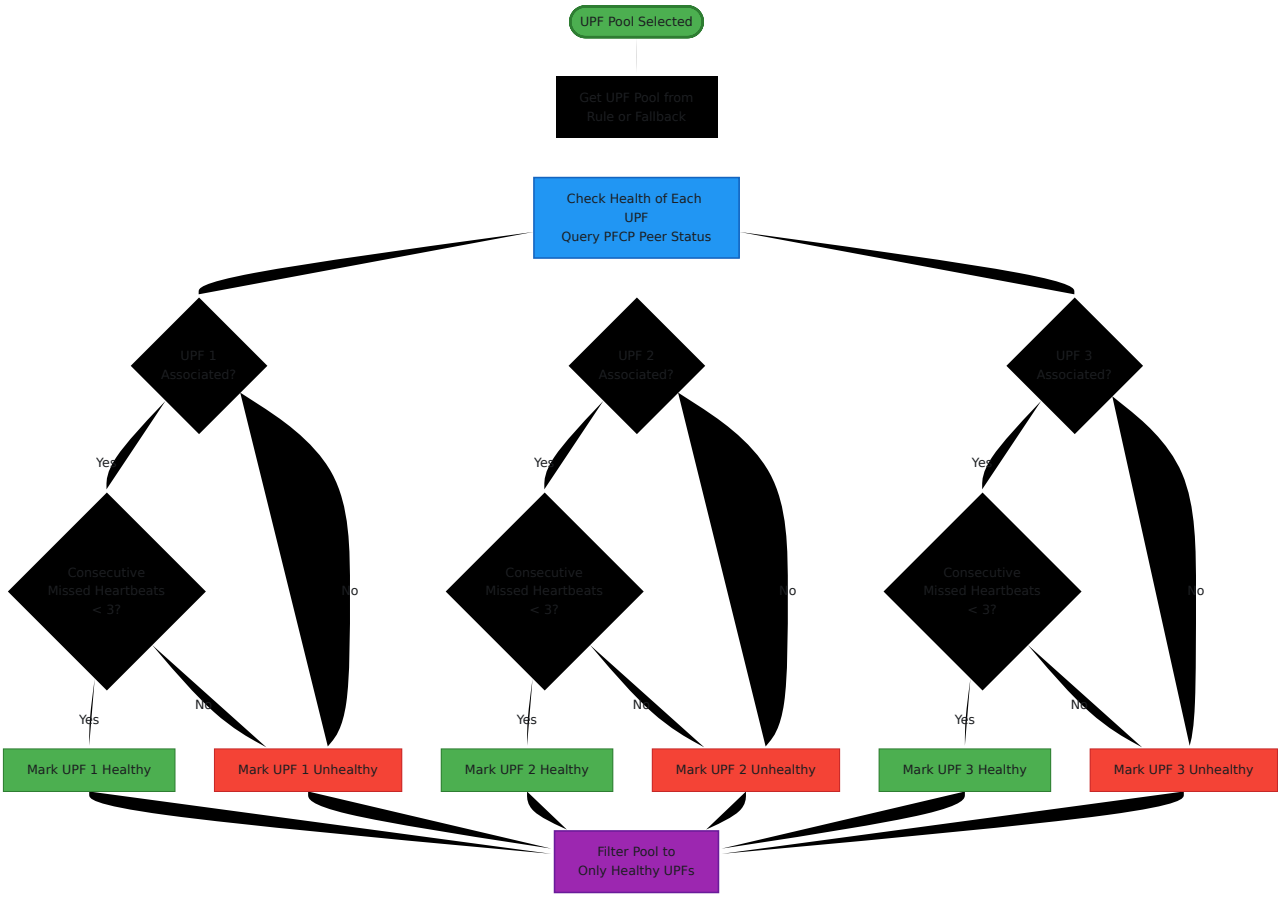
Cómo Funcionan los Pools de UPF:

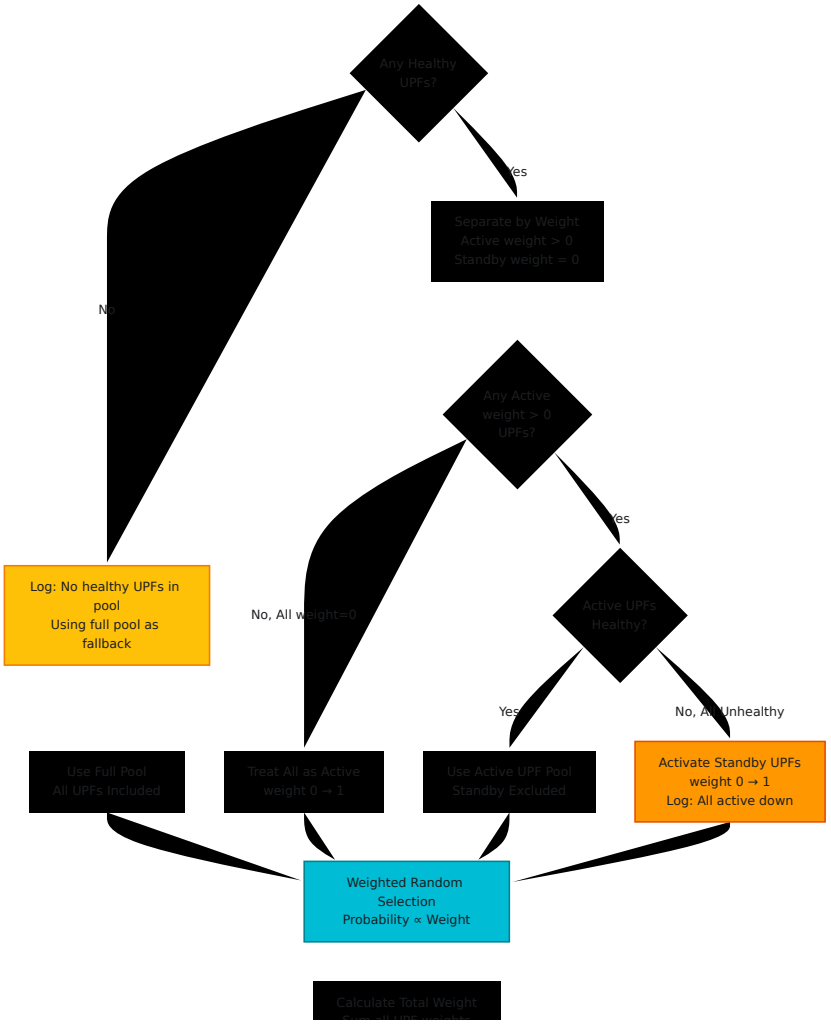
1. **Selección Consciente de Salud**: Solo los UPFs saludables reciben tráfico
    - Saludable = asociación PFCP activa + menos de 3 latidos perdidos consecutivos
    - Los UPFs no saludables se filtran automáticamente
    - Se vuelve a todos los UPFs si ninguno es saludable (fail-fast)
2. **Soporte Activo/Standby**: Use `weight: 0` para UPFs en espera
    - **UPFs Activos** (peso > 0): Reciben tráfico cuando son saludables
    - **UPFs en Espera** (peso == 0): Solo reciben tráfico cuando todos los UPFs activos están caídos
    - Los UPFs en espera se tratan como `weight: 1` cuando se activan
3. **Selección Aleatoria Ponderada**: Cada sesión se asigna aleatoriamente a un UPF saludable basado en pesos
    - En el ejemplo anterior: 70% va a .21, 20% a .22, 10% a .23
    - Mayor peso = más sesiones asignadas a ese UPF
    - Pesos iguales = distribución equitativa
4. **Registro Automático**: Todos los UPFs en los pools se registran automáticamente al inicio

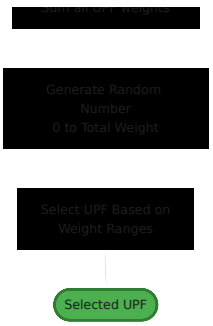
- Nombres generados automáticamente: `"UPF-<ip>:<port>"`
- Configuraciones predeterminadas: asociación PFCP pasiva, latidos de 5 segundos
- Seguimiento inmediato de salud para todos los UPFs configurados

Selección Consciente de Salud con

Activo/Standby


UPF Pool Selected
Get UPF Pool from Rule or Fallback
Check Health of Each UPF Query PFCP Peer Status
UPF 1 Associated?
UPF 2 Associated?
UPF 3 Associated?
Yes
No
Consecutive Missed Heartbeats < 3?
Mark UPF 1 Healthy
Mark UPF 1 Unhealthy
Mark UPF 2 Healthy
Mark UPF 2 Unhealthy
Mark UPF 3 Healthy
Mark UPF 3 Unhealthy
Filter Pool to Only Healthy UPFs


Any Healthy UPFs?
Yes
Separate by Weight Active weight > 0 Standby weight = 0
Any Active weight > 0 UPFs?
Log: No healthy UPFs in pool Using full pool as fallback
No, All weight=0
Active UPFs Healthy?
Use Full Pool All UPFs Included
Treat All as Active weight 0 → 1
Use Active UPF Pool Standby Excluded
Activate Standby UPFs weight 0 → 1 Log: All active down
Weighted Random Selection Probability ∝ Weight
Calculate Total Weight



Ejemplo de Selección Aleatoria Ponderada:

```
Pool: [
  UPF-A: weight 50, healthy ✓
  UPF-B: weight 30, healthy ✓
  UPF-C: weight 20, healthy ✓
]

Total Weight: 50 + 30 + 20 = 100

Weight Ranges:
  UPF-A: 0-49   (50%)
  UPF-B: 50-79  (30%)
  UPF-C: 80-99  (20%)

Random number: 63 → Selects UPF-B
Random number: 15 → Selects UPF-A
Random number: 91 → Selects UPF-C
```

Ejemplo de Failover Activo/Standby:

```
Initial Pool: [
  UPF-A: weight 100, healthy ✓   (Active)
  UPF-B: weight 0, healthy ✓     (Standby)
]

Scenario 1: UPF-A Healthy
→ Use Active Pool: [UPF-A: 100]
→ All traffic to UPF-A

Scenario 2: UPF-A Fails
→ No active UPFs healthy
→ Activate Standby: [UPF-B: 1]
→ All traffic fails over to UPF-B
→ Log: "All active UPFs down, activating standby UPFs"

Scenario 3: Both Unhealthy
→ No healthy UPFs
→ Use full pool: [UPF-A: 100, UPF-B: 0]
🔀 Select with weights (attempt connection, may fail)
→ Log: "No healthy UPFs in pool, using full pool as fallback"
```

Patrones de Peso Comunes:

```
# Distribución equitativa (25% cada uno)
upf_pool: [
  %{remote_ip_address: "10.0.1.1", remote_port: 8805, weight: 1},
  %{remote_ip_address: "10.0.1.2", remote_port: 8805, weight: 1},
  %{remote_ip_address: "10.0.1.3", remote_port: 8805, weight: 1},
  %{remote_ip_address: "10.0.1.4", remote_port: 8805, weight: 1}
]

# Carga balanceada primaria/respaldo (90% / 10%)
upf_pool: [
  %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight:
90},
  %{remote_ip_address: "10.0.1.22", remote_port: 8805, weight: 10}
]

# Activo/Standby (100% primario, 0% en espera hasta que falle el
primario)
upf_pool: [
  %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight:
100},  # Activo
  %{remote_ip_address: "10.0.1.22", remote_port: 8805, weight: 0}
# En espera (solo cuando el activo falla)
]

# Activo con múltiples en espera (carga balanceada cuando se
activa)
upf_pool: [
  %{remote_ip_address: "10.0.1.1", remote_port: 8805, weight:
100},   # Activo
  %{remote_ip_address: "10.0.1.2", remote_port: 8805, weight: 0},
# En espera 1
  %{remote_ip_address: "10.0.1.3", remote_port: 8805, weight: 0}
# En espera 2
]
# Resultado: Activo obtiene 100%. Si el activo falla, los en
espera obtienen 50/50%.

# Pruebas A/B (50% / 50%)
upf_pool: [
  %{remote_ip_address: "10.0.1.100", remote_port: 8805, weight:
50},  # Versión antigua
  %{remote_ip_address: "10.0.1.200", remote_port: 8805, weight:
```

```
50}   # Nueva versión
]
```

Casos de Uso:

- **Failover Activo/Standby**: Use `weight: 0` para UPFs en espera que solo se activan cuando los primarios fallan
- **HA Consciente de Salud**: Failover automático cuando los UPFs pierden la asociación PFCP o fallan en los latidos
- **Escalado Horizontal**: Distribuir la carga entre múltiples UPFs para aumentar la capacidad
- **Alta Disponibilidad**: La distribución automática previene la sobrecarga de un solo UPF
- **Despliegues Graduales**: Use pesos para implementaciones canarias (por ejemplo, 95% antiguo, 5% nuevo)
- **Optimización de Costos**: Dirigir más tráfico a UPFs de mayor capacidad
- **Distribución Geográfica**: Balancear sesiones entre UPFs de borde

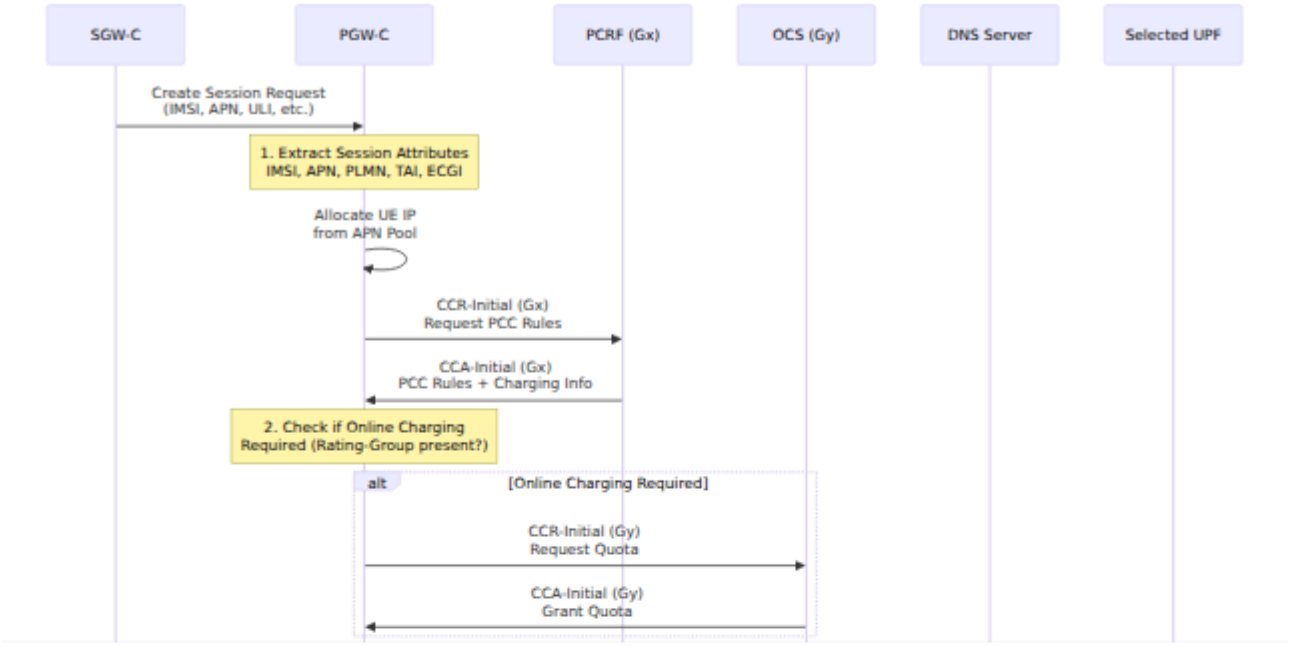
Anulaciones de PCO (Opciones de Configuración de Protocolo):

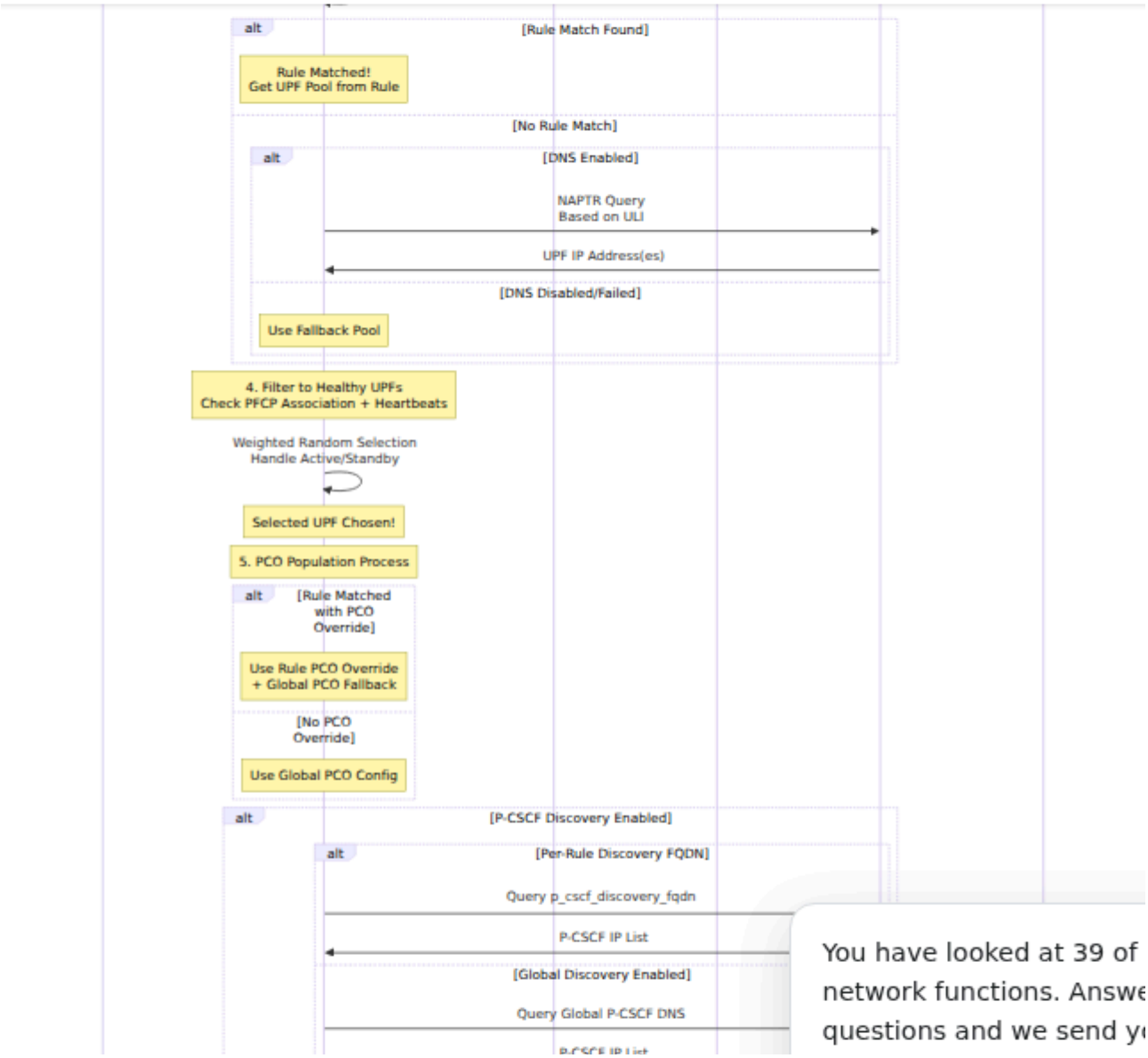
Cada regla de selección de UPF puede especificar opcionalmente valores de PCO personalizados que anulan la configuración de PCO predeterminada para sesiones coincidentes. Esto permite que diferentes APNs o tipos de tráfico reciban diferentes parámetros de red.

Cómo Funcionan las Anulaciones de PCO:

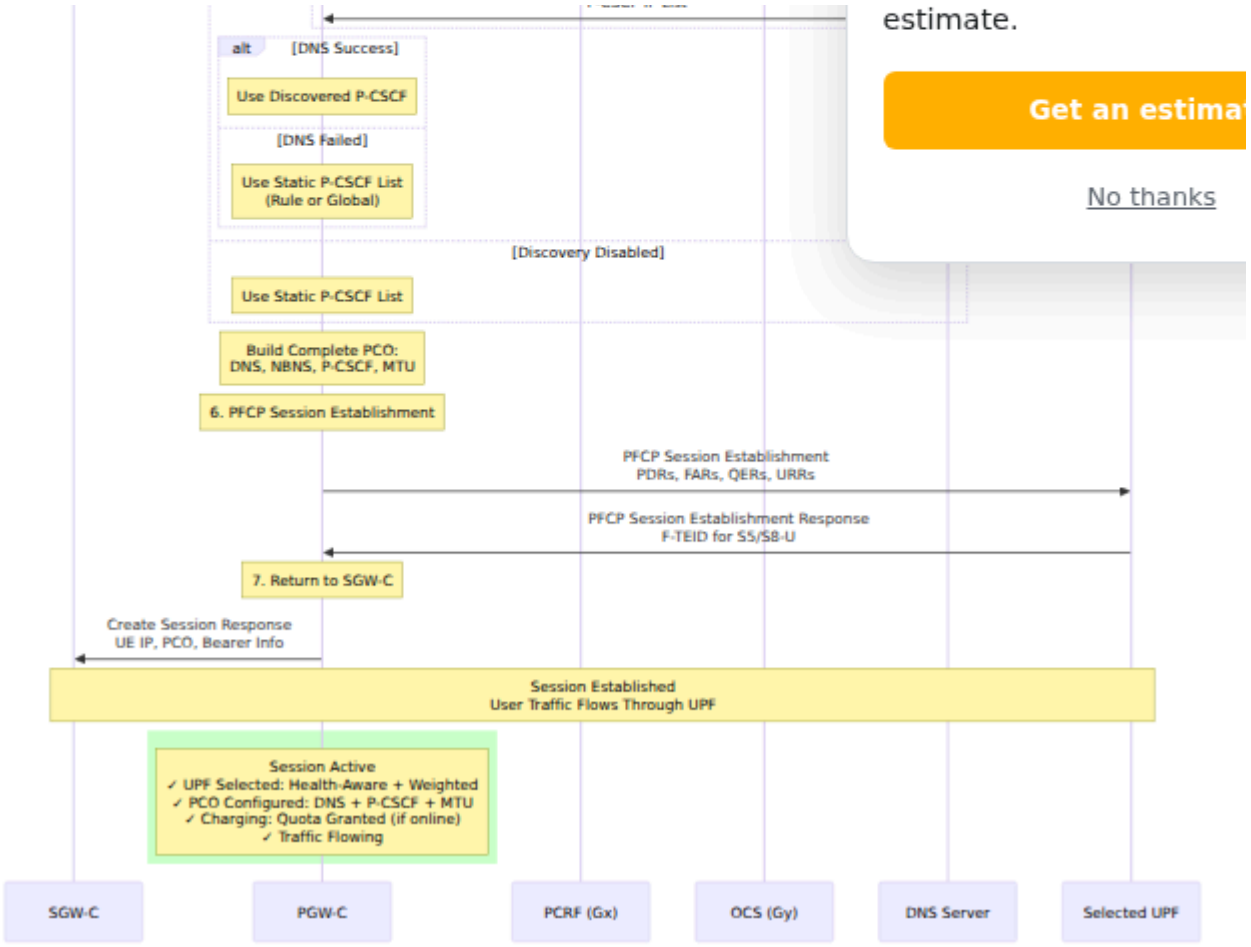
1. **Anulaciones Parciales**: Solo especifique los campos de PCO que desea anular
2. **Recaída Predeterminada**: Los campos no especificados utilizan valores de la configuración principal de `pco`
3. **Específico de Regla**: Cada regla puede tener diferentes anulaciones de PCO
4. **Fusión de Prioridad**: El PCO de la regla tiene prioridad sobre el PCO predeterminado

Jerarquía de Población de PCO





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



Orden de Prioridad para Cada Campo de PCO:

1. **Anulación de PCO de Regla** (Mayor Prioridad)
2. **Descubrimiento DNS de P-CSCF** (solo para direcciones de P-CSCF)
3. **Configuración Global de PCO** (Menor Prioridad / Recaída)

Ejemplo: La Regla IMS Anula DNS, La Regla Empresarial Anula Todo

```
Sesión IMS (coincidió con la regla "Tráfico IMS"):
├─ Servidores DNS: DE GLOBAL (no anulado en la regla)
├─ P-CSCF: DEL DESCUBRIMIENTO DNS (p_cscf_discovery_fqdn
establecido en la regla)
│  └─ Recaída: DE LA REGLA si DNS falla
└─ MTU: DE GLOBAL (no anulado en la regla)

Sesión Empresarial (coincidió con la regla "Tráfico Empresarial"):
├─ Servidores DNS: DE LA REGLA (192.168.1.10, 192.168.1.11)
├─ P-CSCF: DE GLOBAL (no anulado en la regla)
└─ MTU: DE LA REGLA (1500)

Sesión Predeterminada (sin regla coincidente):
├─ Servidores DNS: DE GLOBAL
├─ P-CSCF: DE GLOBAL o DNS si el descubrimiento global está
habilitado
└─ MTU: DE GLOBAL
```

Campos de Anulación de PCO Disponibles:

- `primary_dns_server_address` - Dirección IP del servidor DNS primario (IPv4)
- `secondary_dns_server_address` - Dirección IP del servidor DNS secundario (IPv4)
- `primary_dns_server_ipv6_address` - Dirección IP del servidor DNS primario (IPv6, contenedor 0x0003)
- `secondary_dns_server_ipv6_address` - Dirección IP del servidor DNS secundario (IPv6, contenedor 0x0003)
- `primary_nbns_server_address` - Dirección IP del servidor WINS primario
- `secondary_nbns_server_address` - Dirección IP del servidor WINS secundario
- `p_cscf_ipv4_address_list` - Lista de direcciones IP de servidores P-CSCF IPv4 (para IMS, contenedor 0x000C) - Ver Configuración de PCO y Monitoreo de P-CSCF para el descubrimiento dinámico de P-CSCF
- `p_cscf_ipv6_address_list` - Lista de direcciones IP de servidores P-CSCF IPv6 (para IMS, contenedor 0x0001)
- `ipv4_link_mtu_size` - Tamaño de MTU en bytes

Descubrimiento de P-CSCF por Regla:

Además de las anulaciones de PCO, las reglas de selección de UPF pueden especificar el descubrimiento dinámico de P-CSCF:

- `p_cscf_discovery_fqdn` - (Cadena) FQDN para el descubrimiento de P-CSCF basado en DNS (por ejemplo, `"pcscf.mnc001.mcc001.3gppnetwork.org"`)

Cuando este parámetro está configurado:

1. PGW-C realiza una búsqueda DNS para el FQDN especificado durante el establecimiento de la sesión.
2. El servidor DNS devuelve una lista de direcciones IP de P-CSCF.
3. Las direcciones P-CSCF descubiertas se envían a UE a través de PCO.
4. Si la búsqueda DNS falla, se retrocede a `p_cscf_ipv4_address_list` de la anulación de PCO (si se especifica) o la configuración global de PCO.
5. Consulte Monitoreo de P-CSCF para monitorear las tasas de éxito/fallo en el descubrimiento.

Esto es particularmente útil para:

- **APNs IMS** - Diferentes redes IMS con diferentes servidores P-CSCF.
- **Implementaciones multi-inquilino** - Diferentes empresas con infraestructura P-CSCF dedicada.
- **Enrutamiento geográfico** - DNS devuelve el P-CSCF más cercano según la ubicación del UE.
- **Alta disponibilidad** - DNS devuelve automáticamente solo servidores P-CSCF saludables.

Ejemplo: Tráfico IMS con P-CSCF Personalizado:

```
rules: [
  %{
    name: "IMS Traffic",
    priority: 20,
    match_field: :apn,
    match_regex: "^ims",
    upf_pool: [
      %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80},
      %{remote_ip_address: "10.100.2.22", remote_port: 8805,
weight: 20}
    ],
    # Descubrimiento de P-CSCF: Consultar dinámicamente DNS para
direcciones P-CSCF
    # La búsqueda DNS devuelve las IPs P-CSCF actuales basadas en
este FQDN
    p_cscf_discovery_fqdn: "pcscf.mnc001.mcc001.3gppnetwork.org",
    # Las sesiones IMS obtienen servidores P-CSCF personalizados
(se utilizan como respaldo si DNS falla)
    pco: %{
      p_cscf_ipv4_address_list: ["203.0.113.100", "203.0.113.101"]
      # DNS, NBNS, MTU utilizarán valores predeterminados de la
configuración principal de pco
    }
  }
]
```

Asignación de IP de UE por Regla:

Cada regla de selección de UPF elige **cómo se asigna la IP del UE**. Hay tres escenarios mutuamente consistentes:

Escenario	Configuración de regla	Quién asigna	Pool utilizado
1. Predeterminado	*(ningún campo)*	PGW-C (dirección enviada al UPF)	`ue.subnet_map` basado en APN, retrocediendo a `:default`
2. Pool nombrado	`ue_ip_pool: "name"`	PGW-C (dirección enviada al UPF)	el pool nombrado `ue.subnet_map` `"name"`
3. Delegado por UPF	`upf_assigns_ip: true`	UPF (PFCP CHV4)	un pool en el UPF

- `upf_assigns_ip` - (Booleano, predeterminado `false`) Cuando es `true`, el PGW-C envía el IE de UE-IP-Address con la bandera **CHV4** ("UP asigna") en lugar de una dirección explícita, y lee la dirección asignada de la PDR Creada del UPF en la Respuesta de Establecimiento de Sesión. **Qué** pool utiliza el UPF es completamente una preocupación del lado del UPF (el UPF puede basarlo en el APN / Instancia de Red PFCP si tiene varios pools) — nada sobre el pool se señala desde el PGW-C.
- `ue_ip_pool` - (Cadena, opcional) Nombre de un pool `ue.subnet_map` del **PGW-C** del que se asigna cuando se selecciona esta regla. Esto vincula un pool de PGW-C a un UPF a través de la regla de selección (por ejemplo, para que el UPF que posee/anuncia `100.64.20.0/24` solo reciba direcciones de ese pool). Un pool puede ser referenciado por una regla o muchas. `nil` → el comportamiento predeterminado basado en APN de `ue.subnet_map` (Escenario 1).

`upf_assigns_ip` y `ue_ip_pool` son **mutuamente excluyentes** — uno delega la asignación al UPF, el otro la mantiene en el PGW-C. Si una regla establece ambos, la carga de configuración registra una advertencia y `upf_assigns_ip` gana (`ue_ip_pool` se ignora).

Ya sea la asignación de PGW-C desde un pool vinculado a UPF (Escenario 2) *o* la delegación de UPF (Escenario 3) permite que cada UPF posea una subred y anuncie un único **agregado** OSPF (por ejemplo, `100.64.20.0/24`) en lugar de un `/32` por UE por conexión — el agregado está presente desde el inicio del UPF, por lo que el enlace descendente de un UE recién conectado es enrutado inmediatamente, eliminando la ventana de agujero negro de convergencia de rutas por UE.

> **Importante — alineación de pool/UPF:** el pool del que se asigna un UE debe caer dentro del agregado anunciado del UPF que lo transporta. Para el Escenario 2, vincule cada pool por UPF a una regla cuyo `upf_pool` sea ese único UPF. Para el Escenario 3, cada UPF de `upf_pool` debe configurarse con su propio `ueip_pool` no superpuesto (omniupf `feature_ueip: true`) anunciando ese agregado (`route_advertise_pools`). Si un UE aterriza en un UPF pero su dirección cae dentro del agregado de otro UPF, se producen agujeros negros en el enlace descendente.

Ejemplo — Escenario 2 (PGW-C asigna desde pools por UPF vinculados por la regla):

```
# ue.subnet_map define los pools nombrados:
ue: %{
  subnet_map: %{
    "ims_upf03" => ["100.64.20.0/24"],
    "ims_upf04" => ["100.64.21.0/24"],
    default:     ["100.64.16.0/24"]
  }
},
# cada regla fija un UPF y su pool:
upf_selection: %{
  rules: [
    %{name: "IMS→upf03", priority: 21, match_field: :apn,
match_regex: "^ims",
      upf_pool: [%{remote_ip_address: "10.179.1.42", remote_port:
8805, weight: 1}],
      ue_ip_pool: "ims_upf03"},
    %{name: "IMS→upf04", priority: 20, match_field: :apn,
match_regex: "^ims",
      upf_pool: [%{remote_ip_address: "10.179.1.45", remote_port:
8805, weight: 1}],
      ue_ip_pool: "ims_upf04"}
  ]
}
```

Ejemplo — Escenario 3 (UPF asigna la IP del UE a través de CHV4):

```
rules: [
  %{
    name: "IMS",
    priority: 20,
    match_field: :apn,
    match_regex: "^ims",
    upf_pool: [
      %{remote_ip_address: "10.179.1.42", remote_port: 8805,
weight: 50},
      %{remote_ip_address: "10.179.1.45", remote_port: 8805,
weight: 50}
    ],
    upf_assigns_ip: true   # UPF asigna la IP del UE (CHV4); el
pool es del lado del UPF
  }
]
```

Ejemplo: Tráfico Empresarial con DNS Personalizado:

```
rules: [
  %{
    name: "Enterprise Traffic",
    priority: 15,
    match_field: :apn,
    match_regex: "^(enterprise|corporate)\.apn",
    upf_pool: [
      %{remote_ip_address: "10.100.3.21", remote_port: 8805,
weight: 100}
    ],
    # Las sesiones empresariales obtienen DNS corporativo y MTU
personalizado
    pco: %{
      primary_dns_server_address: "192.168.1.10",
      secondary_dns_server_address: "192.168.1.11",
      ipv4_link_mtu_size: 1500
      # P-CSCF, NBNS utilizarán valores predeterminados de la
configuración principal de pco
    }
  }
]
```

Ejemplo: Anulación Completa (Todos los Campos de PCO):

```
rules: [
  %{
    name: "IoT APN - Totalmente Personalizado",
    priority: 10,
    match_field: :apn,
    match_regex: "^iot\.m2m",
    upf_pool: [
      %{remote_ip_address: "10.100.5.21", remote_port: 8805,
weight: 100}
    ],
    # Las sesiones IoT obtienen PCO completamente personalizado
    pco: %{
      primary_dns_server_address: "8.8.8.8",
      secondary_dns_server_address: "8.8.4.4",
      primary_nbns_server_address: "10.0.0.100",
      secondary_nbns_server_address: "10.0.0.101",
      p_cscf_ipv4_address_list: [],  # Sin P-CSCF para IoT
      ipv4_link_mtu_size: 1280       # MTU más pequeño para
dispositivos restringidos
    }
  }
]
```

Casos de Uso:

- **IMS/VoLTE**: Proporcionar servidores P-CSCF específicos del operador para servicios de voz.
- **APNs Empresariales**: Enrutar tráfico corporativo a través de servidores DNS de la empresa.
- **IoT/M2M**: Usar DNS público y MTU optimizado para dispositivos de bajo ancho de banda.
- **Roaming**: Proporcionar servidores DNS locales para suscriptores visitantes.
- **Diferenciación de Servicios**: Diferentes parámetros de red por tipo de servicio.

Selección de UPF Basada en DNS:

Habilitar la selección dinámica de UPF basada en la Información de Ubicación del Usuario (ULI) utilizando consultas DNS NAPTR. La configuración de DNS ahora se configura dentro de la sección `upf_selection`.

Nota: Esto proporciona selección de UPF basada en geografía o topología. Consulte Interfaz PFCP para la configuración de asociación PFCP con UPFs descubiertos dinámicamente y Gestión de Sesiones para flujos de establecimiento de sesiones.

```
upf_selection: %{
  # Habilitar selección basada en DNS
  dns_enabled: true,

  # Tipos de ubicación para consultar en orden de prioridad
  dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],

  # Sufijo DNS para consultas NAPTR de 3GPP
  dns_suffix: "epc.3gppnetwork.org",

  # Tiempo de espera de consulta DNS en milisegundos
  dns_timeout_ms: 5000,

  # ... reglas y fallback_pool ...
}
```

La selección basada en DNS funciona de la siguiente manera:

1. **Prioridad**: La selección DNS se utiliza solo cuando **NO coinciden reglas estáticas** (prioridad más baja).
2. **Generación de Consultas**: Construye consultas NAPTR DNS basadas en la ubicación del UE:
   - Consulta ECGI: `eci-<hex>.ecgi.epc.mnc<MNC>.mcc<MCC>.epc.3gppnetwork.org`
   - Consulta TAI: `tac-lb<hex>.tac-hb<hex>.tac.epc.mnc<MNC>.mcc<MCC>.epc.3gppnetwork.org`
   - Consultas RAI, SAI, CGI siguen un formato similar a 3GPP TS 23.003.
3. **Jerarquía de Respaldo**: Intenta cada tipo de ubicación en orden de prioridad hasta que se encuentra una coincidencia.

4. **Coincidencia de Pares**: Los resultados de DNS se filtran contra la lista de pares configurada.
5. **Selección**: Elige el par coincidente (actualmente la primera coincidencia, la selección basada en carga llegará pronto).

Ejemplo de Registros DNS (configurar en su servidor DNS):

```
; Registro NAPTR para TAC 100 en PLMN 001-001
tac-lb64.tac-hb00.tac.epc.mnc001.mcc001.epc.3gppnetwork.org IN
NAPTR 10 50 "a" "x-3gpp-upf:x-sxb" "" upf-edge-1.example.com.

; Registro A para el UPF
upf-edge-1.example.com IN A 10.100.1.21
```

Casos de Uso:

- **Computación de Borde de Múltiples Accesos (MEC)**: Enrutar sesiones a los UPFs de borde más cercanos geográficamente.
- **Descubrimiento Dinámico de UPF**: Agregar/quitar UPFs sin reconfigurar PGW-C.
- **Balanceo de Carga**: Distribuir la carga entre UPFs según la ubicación.
- **Segmentación de Red**: Enrutar diferentes segmentos a diferentes UPFs por ubicación.

Monitoreo de Salud de UPF

Selección Automática Consciente de la Salud: El PGW-C monitorea continuamente la salud de todos los UPFs y excluye automáticamente los UPFs no saludables de la selección.

Criterios de Verificación de Salud

Un UPF se considera **saludable** cuando se cumplen TODAS las siguientes condiciones:

1. **Asociación PFCP Activa**: El UPF tiene una asociación PFCP establecida.
2. **Responsividad del Latido**: Menos de 3 latidos consecutivos perdidos.
3. **Proceso Vivo**: El proceso GenServer del par UPF está en funcionamiento.

Un UPF se considera **no saludable** si ALGUNA de las siguientes es verdadera:

- La asociación PFCP no está establecida (`associated: false`).
- 3 o más timeouts consecutivos de latido.
- El proceso del par UPF se ha bloqueado o no responde.

Mecanismo de Monitoreo

Para UPFs Configurados (en `upf_selection`):

- El seguimiento de salud comienza inmediatamente al arrancar.
- La asociación PFCP se monitorea continuamente.
- Los latidos se envían cada 5 segundos.
- El contador `missed_heartbeats_consecutive` rastrea fallos consecutivos.
- Todos los UPFs de reglas y del pool de respaldo se registran automáticamente.

Para UPFs Descubiertos por DNS (registro dinámico):

- Se asume que son saludables hasta el primer intento de sesión.
- Se registran automáticamente en el primer uso.
- El seguimiento de salud comienza después del registro.

Comportamiento de Selección

Modo Activo/Standby (cuando se usa `weight: 0`):

1. Filtrar solo UPFs saludables.
2. Separar en **activos** (peso > 0) y **standby** (peso == 0).
3. Usar UPFs activos si alguno es saludable.
4. Activar UPFs de respaldo (tratar como peso 1) si todos los activos son no saludables.
5. Retroceder al pool completo si no existen UPFs saludables.

Modo Balanceado por Carga (todo peso > 0):

1. Filtrar solo UPFs saludables.
2. Realizar selección aleatoria ponderada entre UPFs saludables.

3. Retroceder al pool completo si no existen UPFs saludables.

Registro:

```
[debug] Usando pool de UPF activo (2/3 UPFs saludables, 1 standby)
[info] Todos los UPFs activos están caídos, activando UPFs de
respaldo (1 UPFs standby, tratando peso 0 como 1)
[warning] No hay UPFs saludables en el pool (3 en total), usando
el pool completo como respaldo
```

Verificación de Salud de UPF

Programáticamente:

```
# Verificar si un UPF específico es saludable
iex> PGW_C.PFCP_Node.is_peer_healthy?({10, 100, 1, 21})
true

# Obtener información detallada de salud
iex> PGW_C.PFCP_Node.get_peer_health({10, 100, 1, 21})
%{
  associated: true,
  missed_heartbeats: 0,
  healthy: true,
  registered: true
}
```

A través de la API OAM:

- Consultar el endpoint `/api/upf_selection`: `curl -k https://localhost:8443/api/upf_selection`
- Devuelve el estado de salud en tiempo real para todos los UPFs en cada pool.
- Valores de estado: Active-UP, Standby-Ready, Active-DOWN, Not Associated.
- Valores de rol: ACTIVE (peso > 0), STANDBY (peso == 0), DYNAMIC (descubierto por DNS, no en la configuración).
- Contador de fallos de latido reportado para UPFs asociados.

Mejores Prácticas de Monitoreo de Salud

1. **Configurar UPFs en upf_selection**: Todos los UPFs en reglas y pools de respaldo se monitorean automáticamente.

```
upf_selection: %{
  rules: [
    %{
      name: "Internet Traffic",
      priority: 10,
      match_field: :apn,
      match_regex: "^internet",
      upf_pool: [
        %{remote_ip_address: "10.100.1.21", remote_port: 8805,
weight: 100}
      ]
    }
  ],
  fallback_pool: [
    %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 100}
  ]
}
# Todos los UPFs obtienen automáticamente:
# - Latidos de 5 segundos
# - Monitoreo de salud desde el inicio
# - Nombres generados automáticamente
```

2. **Usar UPFs de respaldo**: Configurar reservas calientes con `weight: 0` para failover automático.

```
upf_pool: [
  %{remote_ip_address: "10.1.1.1", remote_port: 8805, weight:
100},  # Activo
  %{remote_ip_address: "10.1.1.2", remote_port: 8805, weight:
0}     # Standby
]
```

3. **Monitorear a través de la API OAM**: Consultar regularmente el endpoint `/api/upf_selection` para verificar el estado de salud de UPF.

4. **Monitoreo de latidos**: El sistema utiliza un umbral fijo de 3 latidos consecutivos perdidos para determinar la salud del par.

Registro Dinámico de UPF

Función: El PGW-C registra y monitorea automáticamente los UPFs descubiertos a través de DNS, incluso si no están en la configuración de `upf_selection`.

Cómo Funciona

Cuando cualquier método de selección (reglas estáticas, pools o DNS) devuelve un UPF que no está registrado, el sistema automáticamente:

1. **Crea un Par PFCP**: Genera una configuración de par predeterminada para el UPF desconocido.
2. **Inicia la Asociación PFCP**: Intenta establecer una asociación PFCP con el UPF.
3. **Registra en el Registro de Pares**: Agrega el UPF al sistema de seguimiento interno de pares.
4. **Inicia el Monitoreo de Latidos**: Comienza intercambios periódicos de latidos (intervalos de 10 segundos).
5. **Rastrea la Vitalidad**: Monitorea el UPF en busca de fallos y recuperaciones.

Configuración Predeterminada para UPFs Dinámicamente Registrados

Cuando un UPF se registra dinámicamente, recibe la siguiente configuración predeterminada:

```
%{
  name: "Dynamic-UPF-<IP>",              # por ejemplo, "Dynamic-
UPF-10-100-1-21"
  remote_ip_address: <discovered_ip>,     # IP de DNS o selección
  remote_port: 8805,                      # Puerto PFCP estándar
(sobrescribible)
  initiate_pfcp_association_setup: true,  # PGW-C inicia la
asociación
  heartbeat_period_ms: 10_000             # Intervalo de latido de
10 segundos
}
```

> **Nota**: Los UPFs dinámicos se registran únicamente para la gestión de asociaciones. Se utilizan como objetivos en las reglas de `upf_selection`, no como fuentes de lógica de selección.

Ejemplo: DNS Devuelve un UPF Desconocido

```
# La consulta DNS devuelve: upf-edge-2.example.com -> 10.200.5.99
# Este UPF NO está en su configuración de upf_selection.

# Flujo de registro dinámico:
# 1. El sistema detecta el UPF desconocido 10.200.5.99.
# 2. Registra: "UPF {10, 200, 5, 99} no preconfigurado, intentando
registro dinámico..."
# 3. Envía la Solicitud de Configuración de Asociación PFCP a
10.200.5.99:8805.
# 4. Si el UPF responde: Asociación establecida, la sesión
continúa normalmente.
# 5. Si el UPF no responde: La sesión falla de manera limpia con
un mensaje de error claro.
```

Beneficios

 Descubrimiento Dinámico Verdadero: La selección de UPF basada en DNS ahora funciona sin preconfiguración.
 Escalado Automático: Agregue UPFs a su red sin reiniciar PGW-C.
 Degradación Limpia: Si la asociación falla, las sesiones fallan de manera limpia (sin bloqueos).
 Compatible hacia Atrás: Los UPFs preconfigurados continúan funcionando

exactamente como antes.
 Monitoreo Completo: Los UPFs dinámicos obtienen el mismo monitoreo de latidos que los pares estáticos.

Manejo de Fallos

Si un UPF descubierto dinámicamente no responde a la Configuración de Asociación PFCP:

```
[error] Fallo en la Configuración de Asociación PFCP para el UPF
dinámico {10, 200, 5, 99}: :timeout
[error] Fallo al registrar dinámicamente el UPF {10, 200, 5, 99}:
:timeout.
        La creación de sesión fallará. Considere agregar este UPF
a la configuración de upf_selection.
```

La creación de la sesión fallará, pero el PGW-C permanece estable y continúa procesando otras sesiones.

Cuándo Preconfigurar vs. Registro Dinámico

Escenario	Recomendación
UPFs de Núcleo de Producción	Preconfigurar en `upf_selection` (configuración explícita, monitoreada desde el inicio)
UPFs de Borde Descubiertos por DNS	Usar registro dinámico (escalado automático con infraestructura)
UPFs de Prueba/Desarrollo	Cualquiera de los enfoques funciona (el dinámico es más conveniente)
UPFs Críticos para la Misión	Preconfigurar en `upf_selection` (asegura monitoreo desde el inicio)
UPFs Efímeros/Autoescalados	Usar registro dinámico (los UPFs van y vienen dinámicamente)

Monitoreo de UPFs Dinámicos

Los UPFs dinámicos aparecen en los registros con sus nombres generados automáticamente:

```
[info] Creando configuración de par PFCP dinámica para Dynamic-
UPF-10-200-5-99 ({10, 200, 5, 99}:8805)
[info] UPF dinámico Dynamic-UPF-10-200-5-99 registrado
exitosamente con PID #PID<0.1234.0>
```

Puede consultar el registro de pares para ver todos los pares registrados (tanto estáticos como dinámicos):

```
# Obtener todos los pares registrados
PGW_C.PFCP_Node.registered_peer_count()

# Verificar si un UPF específico está registrado
PGW_C.PFCP_Node.get_peer({10, 200, 5, 99})
# Devuelve: {:ok, #PID<0.1234.0>} si está registrado, :error de lo
contrario
```

Puerto Personalizado para UPFs Dinámicos

Si sus UPFs utilizan un puerto PFCP no estándar, puede activar manualmente el registro:

```
# Registrar UPF en puerto personalizado
PGW_C.PFCP_Node.register_dynamic_peer({10, 200, 5, 99}, 9999)
```

Sin embargo, la selección basada en DNS y el registro automático siempre utilizan el puerto 8805 (puerto PFCP estándar).

Modo de Prueba de Selección de UPF:

Pruebe y valide su configuración de selección de UPF sin afectar sesiones reales:

```
config :pgw_c,
  # Habilitar modo de prueba para pruebas (deshabilitado por
defecto)
  upf_selection_dry_run: true
```

Cuando el modo de prueba está habilitado:

1. **Sin Asignación Real**: Las sesiones no se asignan realmente a los UPFs.
2. **Registro Detallado**: Las decisiones de selección se registran con todos los detalles.
3. **Devolución de Error**: `assign_sxb_peer/1` devuelve `{:error, :dry_run_mode}`.
4. **Prevención de Sesiones**: Devolver un error impide la creación de sesiones.
5. **Ambos Métodos**: Funciona con reglas estáticas y selección basada en DNS.

Ejemplo de Salida de Registro:

```
[warning] ⚠  MODO DE PRUEBA DE SELECCIÓN DE UPF HABILITADO - No se
realizará ninguna asignación real.

[info] 🧪 PRUEBA: Regla estática coincidente
  Método: Regla Estática
  Campo de Coincidencia: :apn
  Expresión Regular de Coincidencia: ~r/^internet\./
  Prioridad: 10
  UPF Seleccionado: 10.0.1.21:8805

[warning] 🧪 PRUEBA: Se asignaría UPF pero se omite la asignación
real
  IMSI de la Sesión: 001001000000670
  APN de la Sesión: internet.apn
  Método de Selección: estático
  Se Enlazaría a: 10.0.1.21:8805
  ⚠  Devolviendo error para prevenir la creación de sesión
```

Pruebas a través de la Interfaz LiveView:

La página de LiveView de Selección de UPF (`/api/upf_selection`) incluye una interfaz de prueba interactiva:

1. Navegue a la página de Selección de UPF en el panel web.
2. Desplácese a la sección "Probar Selección de UPF".
3. Ingrese atributos de sesión de prueba:
   - IMSI (por ejemplo, `001001000000670`).
   - APN (por ejemplo, `internet.apn`).
   - ID de PLMN de la Red de Servicio (por ejemplo, `001001`).
4. Haga clic en "Probar Selección" para simular la selección.
5. Vea los resultados detallados que muestran:
   - Qué regla coincidió (o si se utilizaría DNS).
   - UPF seleccionado y nombre del par.
   - Detalles del campo de coincidencia y patrón.
   - Prioridad de la regla.

La interfaz de prueba LiveView simula la lógica de selección **sin requerir que el modo de prueba esté habilitado globalmente**, lo que hace que sea seguro probar en entornos de producción sin afectar el tráfico real.

Casos de Uso:

- **Pruebas de Configuración**: Validar reglas de enrutamiento antes de implementarlas en producción.
- **Resolución de Problemas**: Comprender por qué sesiones específicas se enrutan a UPFs específicos.
- **Capacitación**: Demostrar la lógica de selección de UPF a los equipos de operaciones.
- **Desarrollo**: Probar nuevas reglas de selección durante el desarrollo.

Campos de Coincidencia:

- `:imsi` - Identidad del Suscriptor Móvil Internacional.
- `:apn` - Nombre del Punto de Acceso (APN/DNN).
- `:serving_network_plmn_id` - ID de PLMN de la red de servicio.
- `:sgw_ip_address` - Dirección IP de SGW.
- `:uli_tai_plmn_id` - ID de PLMN del Área de Seguimiento.

- `:uli_ecgi_plmn_id` - ID de PLMN de la Celda E-UTRAN.

Ajuste de Latido:

```
# Agresivo (detectar fallos rápidamente)
heartbeat_period_ms: 2_000  # 2 segundos

# Estándar (recomendado)
heartbeat_period_ms: 5_000  # 5 segundos

# Relajado (redes de alta latencia)
heartbeat_period_ms: 10_000  # 10 segundos
```

Ver: Documentación de la Interfaz PFCP

Configuración del Pool de IP de UE

Propósito

Configurar pools de direcciones IP para la asignación de UE, organizados por APN.

Bloque de Configuración

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # Pools de APN "internet"
      "internet" => [
        "100.64.0.0/20"  # 4094 IPs utilizables
      ],

      # Pools de APN "ims"
      "ims" => [
        "100.64.16.0/22"  # 1022 IPs utilizables
      ],

      # Pool predeterminado para APNs desconocidos
      default: [
        "42.42.42.0/24"  # 254 IPs utilizables
      ]
    }
  }
```

Parámetros

Parámetro	Tipo	Requerido	Descripción
`subnet_map`	Mapa	Sí	Mapea nombres de APN a listas de subredes
`default`	Lista (Subredes)	Sí	Pool de respaldo para APNs desconocidos

Formato de Subred

Notación CIDR: `<network_address>/<prefix_length>`

Cálculo de IP Utilizables:

CIDR	Total de IPs	IPs Utilizables	Rango de Ejemplo
/24	256	254	100.64.1.1 - 100.64.1.254
/23	512	510	100.64.0.1 - 100.64.1.254
/22	1024	1022	100.64.0.1 - 100.64.3.254
/21	2048	2046	100.64.0.1 - 100.64.7.254
/20	4096	4094	100.64.0.1 - 100.64.15.254
/16	65536	65534	100.64.0.1 - 100.64.255.254

Ejemplos

Configuración Simple:

```
ue: %{
  subnet_map: %{
    "internet" => ["100.64.1.0/24"],
    default: ["42.42.42.0/24"]
  }
}
```

Configuración de Producción:

```
ue: %{
  subnet_map: %{
    # Internet general - pool grande
    "internet" => [
      "100.64.0.0/18"  # 16,382 IPs
    ],

    # IMS (VoLTE)
    "ims" => [
      "100.64.64.0/22"  # 1,022 IPs
    ],

    # APN Empresarial
    "enterprise.corp" => [
      "10.100.0.0/16"  # 65,534 IPs
    ],

    # Dispositivos IoT
    "iot.m2m" => [
      "100.64.72.0/20"  # 4,094 IPs
    ],

    # Respaldo predeterminado
    default: [
      "42.42.42.0/24"  # 254 IPs
    ]
  }
}
```

Balanceo de Carga (Múltiples Subredes por APN):

```
ue: %{
  subnet_map: %{
    "internet" => [
      "100.64.0.0/22",   # 1022 IPs
      "100.64.4.0/22",   # 1022 IPs
      "100.64.8.0/22",   # 1022 IPs
      "100.64.12.0/22"   # 1022 IPs
    ],
    # Total: 4088 IPs, distribuidos aleatoriamente
    default: ["42.42.42.0/24"]
  }
}
```

Coincidencia de Patrones Regex:

Para coincidencias de APN comodín, use claves que comiencen con `^` para indicar patrones regex:

```
ue: %{
  subnet_map: %{
    # Regex: APNs que comienzan con "ims" (coincide con "ims",
"ims.apn", "ims.something")
    "^ims" => [
      "100.64.10.0/24"
    ],

    # Regex: APNs que comienzan con "m2m." (coincide con
"m2m.test", "m2m.prod")
    "^m2m\." => [
      "100.64.20.0/24"
    ],

    # Coincidencia exacta solo
    "enterprise.corp" => [
      "10.100.0.0/16"
    ],

    default: ["42.42.42.0/24"]
  }
}
```

Reglas de Patrones:

- Las claves que comienzan con `^` son patrones regex
- Las claves sin `^` son coincidencias exactas (compatible hacia atrás)
- Los patrones regex se compilan en el momento del análisis de configuración
- El primer patrón coincidente gana
- Las barras invertidas deben ser escapadas (`\` por `\`)

Patrones Comunes:

- **Empieza con:** `"^ims"` coincide con `ims`, `ims.apn`, `ims.foo.bar`
- **Termina con:** `"^.*\.corp$"` coincide con `foo.corp`, `bar.corp`
- **Contiene:** `"^.*test.*"` coincide con `test`, `foo.test.bar`

Soporte IPv6:

```
ue: %{
  subnet_map: %{
    # Pools IPv4
    "internet" => [
      "100.64.0.0/20"
    ],

    # Pools IPv6 (delegación de prefijos)
    "internet.ipv6" => [
      "2001:db8:1::/48"
    ],

    default: [
      "42.42.42.0/24"
    ]
  }
}
```

Rangos de IP Recomendados

RFC 6598 (NAT de Grado de Transportista):

- **Rango:** `100.64.0.0/10`
- **Tamaño:** ~4 millones de IPs
- **Propósito:** Diseñado para NAT de proveedores de servicios

Rangos de IP Privadas (RFC 1918):

- `10.0.0.0/8` - 16 millones de IPs
- `172.16.0.0/12` - 1 millón de IPs
- `192.168.0.0/16` - 65,534 IPs

Ver: Documentación de Asignación de Pool de IP de UE

Configuración de PCO

Propósito

Configurar Opciones de Configuración de Protocolo (PCO) enviadas a UE.

Bloque de Configuración

```
config :pgw_c,
  pco: %{
    # Servidores DNS
    primary_dns_server_address: "8.8.8.8",
    secondary_dns_server_address: "8.8.4.4",

    # Servidores DNS IPv6 (opcional, contenedor 0x0003)
    primary_dns_server_ipv6_address: nil,
    secondary_dns_server_ipv6_address: nil,

    # Servidores NBNS (opcional, para dispositivos Windows)
    primary_nbns_server_address: nil,
    secondary_nbns_server_address: nil,

    # Direcciones P-CSCF para IMS
    p_cscf_ipv4_address_list: ["10.0.0.50", "10.0.0.51"],   #
contenedor 0x000C
    p_cscf_ipv6_address_list: [],                           #
contenedor 0x0001

    # Tamaño MTU IPv4
    ipv4_link_mtu_size: 1400
  }
```

Parámetros

Parámetro	Tipo	Predeterminado	Desc
`primary_dns_server_address`	Cadena (IPv4)	Requerido	Servi DNS prima
`secondary_dns_server_address`	Cadena (IPv4)	Opcional	Servi DNS secur
`primary_dns_server_ipv6_address`	Cadena (IPv6)	`nil`	Servi DNS prima (cont 0x00
`secondary_dns_server_ipv6_address`	Cadena (IPv6)	`nil`	Servi DNS secur (cont 0x00
`primary_nbns_server_address`	Cadena (IPv4)	`nil`	Servi NBNS (NetB prima
`secondary_nbns_server_address`	Cadena (IPv4)	`nil`	Servi NBNS secur
`p_cscf_ipv4_address_list`	Lista (IPv4)	`[]`	Direc P-CSC para

Parámetro	Tipo	Predeterminado	Desc
			(cont 0x00
`p_cscf_ipv6_address_list`	Lista (IPv6)	`[]`	Direc P-CSC para (cont 0x00
`ipv4_link_mtu_size`	Entero	`1400`	Tama la Un Trans Máxi

Ejemplos

DNS Público (Google):

```
pco: %{
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4",
  ipv4_link_mtu_size: 1400
}
```

DNS Privado:

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11",
  ipv4_link_mtu_size: 1400
}
```

Configuración IMS:

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11",

  # P-CSCF para IMS/VoLTE
  p_cscf_ipv4_address_list: [
    "10.0.0.50",  # P-CSCF primario
    "10.0.0.51"   # P-CSCF secundario
  ],

  ipv4_link_mtu_size: 1400
}
```

NBNS (Compatibilidad con Windows):

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11",
  primary_nbns_server_address: "10.0.0.20",
  secondary_nbns_server_address: "10.0.0.21",
  ipv4_link_mtu_size: 1400
}
```

Ajuste de MTU:

```
# Ethernet estándar
ipv4_link_mtu_size: 1500

# Reducido por sobrecarga de túneles
ipv4_link_mtu_size: 1400

# Tramas jumbo (si se admite)
ipv4_link_mtu_size: 9000
```

Ver: Documentación de Configuración de PCO

Configuración de la API OAM

Propósito

Configurar los puntos finales de la API REST de OAM para gestionar y monitorear OmniPGW. Todo el monitoreo y gestión se realiza a través de esta API.

> **Nota:** La configuración de la API solo está activa en entornos no de prueba. La configuración se omite automáticamente cuando `config_env()` es `:test`, `:test_mock`, o `:test_impl`.

Configuración de la API REST

```
config :api_ex,
  api: %{
    # Configuraciones de red
    port: 8443,
    listen_ip: "0.0.0.0",

    # Metadatos de la API
    product_name: "PGW-C",
    title: "API - PGW-C",
    hostname: "localhost",

    # Configuraciones TLS
    enable_tls: true,
    tls_cert_path: "priv/cert/omnitouch.crt",
    tls_key_path: "priv/cert/omnitouch.pem",

    # Definiciones de rutas
    routes: [
      %{
        path: "/status",
        module: ApiEx.Api.StatusController,
        actions: [:index]
      }
    ]
  }
```

Parámetros de la API

Parámetro	Tipo	Predeterminado	Descripción
`port`	Entero	`8443`	Puerto HTTPS para la API REST
`listen_ip`	Cadena (IP)	`"0.0.0.0"`	Dirección de escucha de la API (0.0.0.0 = todas las interfaces)
`product_name`	Cadena	`"PGW-C"`	Nombre del producto (para metadatos de la API)
`title`	Cadena	`"API - PGW-C"`	Título de la documentación de la API
`hostname`	Cadena	`"localhost"`	Nombre de host del servidor API
`enable_tls`	Booleano	`true`	Habilitar HTTPS para la API
`tls_cert_path`	Cadena (Ruta)	Requerido	Ruta al archivo de certificado SSL/TLS
`tls_key_path`	Cadena (Ruta)	Requerido	Ruta al archivo de clave privada SSL/TLS
`routes`	Lista (Mapas)	`[]`	Definiciones de rutas de la API

Formato de Definición de Ruta

Cada ruta en la lista `routes` es un mapa con:

Campo	Tipo	Descripción	Ejemplo
`path`	Cadena	Ruta URL para la ruta	`"/status"`
`module`	Módulo	Módulo del controlador que maneja las solicitudes	`ApiEx.Api.StatusController`
`actions`	Lista (Átomos)	Acciones permitidas del controlador	`[:index, :show]`

Ejemplos

Configuración Predeterminada (Desarrollo):

```
# API en localhost:8443
config :api_ex,
  api: %{
    port: 8443,
    listen_ip: "127.0.0.1",  # solo localhost
    hostname: "localhost",
    enable_tls: true,
    tls_cert_path: "priv/cert/dev-cert.crt",
    tls_key_path: "priv/cert/dev-key.pem",
    routes: [
      %{path: "/status", module: ApiEx.Api.StatusController,
actions: [:index]}
    ]
  }
```

Configuración de Producción:

```
# API en la interfaz de gestión
config :api_ex,
  api: %{
    port: 8443,
    listen_ip: "10.0.0.20",  # Red de gestión
    product_name: "OmniPGW-C",
    hostname: "pgw-c-api.example.com",
    enable_tls: true,
    tls_cert_path: "/etc/ssl/certs/pgw-c-api.crt",
    tls_key_path: "/etc/ssl/private/pgw-c-api.key",
    routes: [
      %{path: "/status", module: ApiEx.Api.StatusController,
actions: [:index]},
      %{path: "/sessions", module: ApiEx.Api.SessionController,
actions: [:index, :show]}
    ]
  }
```

Accediendo a la API

Consultar un punto final:

```
# Punto final de estado (certificado autofirmado, desarrollo)
curl -k https://localhost:8443/api/status

# Con un certificado de confianza (producción)
curl https://pgw-c-api.example.com:8443/api/status
```

Todas las rutas se sirven bajo el prefijo `/api`. Los puntos finales disponibles incluyen `/api/status`, `/api/sessions`, `/api/upf`, `/api/diameter`, `/api/charging`, `/api/ip_pools`, `/api/session_history`, `/api/topology`, `/api/ue_search` (POST), `/api/pcscf_monitor`, y `/api/upf_selection`.

Documentación interactiva de la API (Swagger UI):

```
https://localhost:8443/api/docs
```

Configuración del Certificado TLS

Generar Certificado Autofirmado (Desarrollo):

```
# Generar clave privada y certificado
openssl req -x509 -newkey rsa:4096 -keyout priv/cert/omnitouch.pem
\
  -out priv/cert/omnitouch.crt -days 365 -nodes \
  -subj "/CN=localhost"
```

Certificado de Producción:

Para producción, use certificados de una Autoridad de Certificación (CA) de confianza:

- Let's Encrypt (gratis, automatizado)
- CA comercial (DigiCert, GlobalSign, etc.)
- CA interna para implementaciones empresariales

Consideraciones de Seguridad

1. **Siempre use TLS en producción** - Establecer `enable_tls: true`
2. **Restringir listen_ip** - Usar direcciones IP específicas en producción (no 0.0.0.0)
3. **Usar certificados válidos** - Evitar certificados autofirmados en producción
4. **Protección de firewall** - Restringir el acceso al puerto de gestión (8443)
5. **Archivos de clave fuertes** - Usar RSA de 4096 bits o equivalente
6. **Actualizaciones regulares** - Rotar certificados antes de su expiración

Solución de Problemas

Problema: No se puede acceder a la API

```
# Verificar si el puerto está escuchando
netstat -tulpn | grep 8443

# Verificar que los archivos de certificado existan
ls -la priv/cert/

# Verificar registros en busca de errores de inicio
tail -f /var/log/pgw_c/application.log
```

Problema: Errores SSL/TLS

- Verificar que las rutas del certificado y la clave sean correctas
- Asegurarse de que el certificado coincida con el nombre de host
- Verificar la expiración del certificado: `openssl x509 -in cert.crt -text -noout`
- Verificar los permisos del archivo de clave (deben ser legibles por el proceso PGW-C)

Ver: Guía de Monitoreo para detalles sobre el uso de la API OAM

Ejemplo Completo

Configuración Lista para Producción

```
# config/runtime.exs
import Config

# Configuración del logger
config :logger, level: :info

config :pgw_c,
  # Métricas (Prometheus)
  metrics: %{
    enabled: true,
    ip_address: "10.0.0.20",  # Red de gestión
    port: 9090,
    registry_poll_period_ms: 5_000
  },

  # Diameter/Gx (interfaz PCRF)
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf-primary.epc.mnc001.mcc001.3gppnetwork.org",
        realm: "epc.mnc001.mcc001.3gppnetwork.org",
        ip: "10.0.1.30",
        initiate_connection: true
      },
      %{
        host: "pcrf-backup.epc.mnc001.mcc001.3gppnetwork.org",
        realm: "epc.mnc001.mcc001.3gppnetwork.org",
        ip: "10.0.2.30",
        initiate_connection: true
      }
    ]
  },

  # S5/S8 (interfaz SGW-C)
  s5s8: %{
```

```
    local_ipv4_address: "10.0.0.20"
  },

  # Sxb/PFCP (interfaz PGW-U)
  sxb: %{
    local_ip_address: "10.0.0.20"
  },

  # Selección de UPF
  upf_selection: %{
    rules: [
      %{
        name: "Internet Predeterminado",
        priority: 1,
        match_field: :apn,
        match_regex: ~r/^internet/,
        upf_pool: [
          %{remote_ip_address: "10.0.0.21", remote_port: 8805,
weight: 100},
          %{remote_ip_address: "10.0.0.22", remote_port: 8805,
weight: 0}  # Reserva
        ]
      }
    ],
    fallback_pool: [
      %{remote_ip_address: "10.0.0.21", remote_port: 8805, weight:
100}
    ]
  },

  # Pools de IP de UE
  ue: %{
    subnet_map: %{
      "internet" => [
        "100.64.0.0/18"  # 16,382 IPs
      ],
      "ims" => [
        "100.64.64.0/22"  # 1,022 IPs
      ],
      "enterprise.corp" => [
        "10.100.0.0/16"  # 65,534 IPs
      ],
      default: [
        "100.64.127.0/24"  # 254 IPs
```

```
      ]
    }
  },

  # Opciones de Configuración de Protocolo
  pco: %{
    primary_dns_server_address: "8.8.8.8",
    secondary_dns_server_address: "8.8.4.4",
    p_cscf_ipv4_address_list: ["10.0.0.50", "10.0.0.51"],
    ipv4_link_mtu_size: 1400
  }
```

Validación de Configuración

Validación al Inicio

OmniPGW valida la configuración al inicio. Verifique los registros:

```
[info] Cargando configuración desde runtime.exs
[info] Validando configuración...
[info] Configuración válida
[info] Iniciando OmniPGW...
```

Errores Comunes de Validación

Dirección IP Inválida:

```
[error] Dirección IP inválida en s5s8.local_ipv4_address: "10.0.0"
```

Campo Requerido Faltante:

```
[error] Falta la configuración requerida: sxb.local_ip_address
```

CIDR Inválido:

```
[error] Subred inválida en ue.subnet_map: "100.64.1.0/33"
```

Identidad Diameter Inválida:

```
[error] El host Diameter debe ser FQDN, no IP: "10.0.0.20"
```

Pruebas de Configuración

Probar configuración sin iniciar:

```
# Validar sintaxis
mix compile

# Verificar carga de configuración
iex -S mix
iex> Application.get_env(:pgw_c, :metrics)
```

Configuración Específica del

Entorno

Desarrollo

```
# config/dev.exs
import Config

config :logger, level: :debug

config :pgw_c,
  metrics: %{
    enabled: true,
    ip_address: "127.0.0.1",
    port: 42069,
    registry_poll_period_ms: 10_000
  },
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omnipgw-dev.local",
    realm: "local",
    peer_list: [
      %{
        host: "pcrf-dev.local",
        realm: "local",
        ip: "127.0.0.1",
        initiate_connection: true
      }
    ]
  },
  s5s8: %{
    local_ipv4_address: "127.0.0.10"
  },
  sxb: %{
    local_ip_address: "127.0.0.20"
  },
  upf_selection: %{
    fallback_pool: [
      %{remote_ip_address: "127.0.0.21", remote_port: 8805,
weight: 100}
    ]
  },
  ue: %{
```

```
    subnet_map: %{
      "internet" => ["100.64.1.0/24"],
      default: ["42.42.42.0/24"]
    }
  },
  pco: %{
    primary_dns_server_address: "8.8.8.8",
    secondary_dns_server_address: "8.8.4.4",
    ipv4_link_mtu_size: 1400
  }
```

Uso de Variables de Entorno

```
# config/runtime.exs
import Config

config :pgw_c,
  metrics: %{
    enabled: System.get_env("METRICS_ENABLED", "true") == "true",
    ip_address: System.get_env("METRICS_IP", "0.0.0.0"),
    port: String.to_integer(System.get_env("METRICS_PORT",
"9090")),
    registry_poll_period_ms: 10_000
  },
  diameter: %{
    listen_ip: System.get_env("DIAMETER_LISTEN_IP", "0.0.0.0"),
    host: System.get_env("DIAMETER_HOST") || raise("DIAMETER_HOST
requerido"),
    realm: System.get_env("DIAMETER_REALM") ||
raise("DIAMETER_REALM requerido"),
    peer_list: [
      %{
        host: System.get_env("PCRF_HOST") || raise("PCRF_HOST
requerido"),
        realm: System.get_env("PCRF_REALM") ||
System.get_env("DIAMETER_REALM"),
        ip: System.get_env("PCRF_IP") || raise("PCRF_IP
requerido"),
        initiate_connection: true
      }
    ]
  }
  # ... resto de la configuración
```

Uso:

```
export DIAMETER_HOST="omnipgw.epc.mnc001.mcc001.3gppnetwork.org"
export DIAMETER_REALM="epc.mnc001.mcc001.3gppnetwork.org"
export PCRF_HOST="pcrf.epc.mnc001.mcc001.3gppnetwork.org"
export PCRF_IP="10.0.0.30"

mix run --no-halt
```

Documentación Relacionada

Configuración de Interfaz

- **Interfaz PFCP** - Configuración de Sxb/PFCP, comunicación UPF, establecimiento de sesiones
- **Interfaz Diameter Gx** - Control de políticas PCRF, reglas PCC, gestión de QoS
- **Interfaz Diameter Gy** - Carga en línea OCS, gestión de cuotas, control de crédito
- **Interfaz S5/S8** - Configuración GTP-C v2, comunicación SGW-C (4G/LTE)
- **Interfaz Gn/Gp** - Configuración GTP-C v1, comunicación SGSN (2G/3G GGSN)

Configuración de Red

- **Asignación de IP de UE** - Gestión de pools de IP, asignación basada en APN, DHCP
- **Configuración de PCO** - Opciones de Configuración de Protocolo, DNS, P-CSCF, MTU
- **Monitoreo de P-CSCF** - Monitoreo de descubrimiento de P-CSCF, seguimiento de salud de IMS

Guías Operativas

- **Gestión de Sesiones** - Ciclo de vida de la sesión PDN, gestión de portadoras
- **Guía de Monitoreo** - Métricas de Prometheus, alertas, paneles
- **Formato de CDR de Datos** - Registros de carga offline, integración de facturación

---

Volver a la Guía de Operaciones

Guía de Configuración de OmniPGW - *por Omnitouch Network Services*

Formato del Registro de Datos de Carga (CDR)

Carga Offline para PGW-C

OmniPGW de Omnitouch Network Services

Tabla de Contenidos

1. Descripción General
2. Formato del Archivo CDR
3. Campos del CDR
4. Eventos del CDR
5. Estructura del Archivo
6. Configuración
7. Flujo de Generación del CDR
8. Detalles de los Campos
9. Ejemplos
10. Integración

Descripción General

El **formato del CDR de Datos (Registro de Datos de Carga)** proporciona capacidades de carga offline para el Plano de Control del Gateway de Paquetes (PGW-C). Se generan CDRs para registrar eventos de sesión de portadora, uso de datos e información del suscriptor para fines de facturación y análisis.

Este formato común es compatible con los CDRs de SGW-C, asegurando consistencia en los registros de carga a través de la infraestructura EPC.

Características Clave

- **Formato basado en CSV** - Valores separados por comas, simples y legibles para humanos
- **Grabación basada en eventos** - Captura eventos de inicio, actualización y finalización de portadoras
- **Medición de volumen** - Registra el uso de datos de enlace ascendente y descendente
- **Rotación automática** - Rotación de archivos configurable basada en intervalos de tiempo
- **Cumplimiento con 3GPP** - Sigue 3GPP TS 32.251 (carga del dominio PS) y TS 32.298 (codificación de CDR)

Casos de Uso

Caso de Uso	Descripción
Carga Offline	Generar CDRs para facturación postpaga
Análisis	Analizar patrones de uso de suscriptores
Rastro de Auditoría	Rastrear todos los eventos de sesión de portadora
Planificación de Capacidad	Monitorear la utilización de recursos de red
Resolución de Problemas	Depurar problemas de sesión y portadora

---

Formato del Archivo CDR

Convención de Nombres de Archivos

```
<epoch_timestamp>
```

Ejemplo:

```
1726598022
```

El nombre del archivo es la marca de tiempo de época Unix (en segundos) de cuando se creó el archivo.

Ubicación del Archivo

Directorio predeterminado:

- PGW-C: `/var/log/pgw_c/cdrs/`

Configurable a través del parámetro `cdr_directory` en config/runtime.exs.

Encabezado del Archivo

Cada archivo CDR comienza con un encabezado de varias líneas que contiene metadatos:

```
# Archivo CDR de Datos:
# Hora de Inicio del Archivo: HH:MM:SS (unix_timestamp)
# Hora de Fin del Archivo: HH:MM:SS (unix_timestamp)
# Nombre del Gateway: <gateway_name>
#
epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,eci
```

Campos del Encabezado:

- **Hora de Inicio del Archivo** - Cuando se creó el archivo CDR (legible para humanos y marca de tiempo Unix)
- **Hora de Fin del Archivo** - Cuando ocurrirá la rotación del archivo (legible para humanos y marca de tiempo Unix)
- **Nombre del Gateway** - Identificador para la instancia PGW-C (configurado a través del parámetro `pgw_name`)
- **Encabezados de Columna** - Nombres de campos CSV para los registros de datos

---

Campos del CDR

Resumen de Campos

Posición	Nombre del Campo	Tipo	Descripción
0	epoch	entero	Marca de tiempo del evento (segundos de época Unix)
1	imsi	cadena	Identidad Internacional de Suscriptor Móvil
2	event	cadena	Tipo de evento CDR (por ejemplo, "default_bearer_start")
3	charging_id	entero	Identificador de carga único para la portadora
4	msisdn	cadena	Número ISDN de la Estación Móvil (número de teléfono)
5	ue_imei	cadena	Identidad Internacional de Equipos Móviles
6	timezone_raw	cadena	Zona horaria del UE (reservado, actualmente vacío)
7	plmn	entero	Identificador de la Red Móvil Pública
8	tac	entero	Código de Área de Seguimiento
9	eci	entero	Identificador de Celda E-UTRAN

Posición	Nombre del Campo	Tipo	Descripción
10	sgw_ip	cadena	Dirección IP del plano de control S5/S8 de SGW-C
11	ue_ip	cadena	Dirección IP del UE (formato IPv4|IPv6)
12	pgw_ip	cadena	Dirección IP del plano de control S5/S8 de PGW-C
13	apn	cadena	Nombre del Punto de Acceso
14	qci	entero	Identificador de Clase de QoS
15	octets_in	entero	Volumen de datos de enlace descendente (bytes)
16	octets_out	entero	Volumen de datos de enlace ascendente (bytes)

Eventos del CDR

Tipos de Eventos

Se generan CDRs para tres tipos de eventos:

Tipo de Evento	Formato	Descripción	Cuándo se Genera
Inicio de Portadora	`<type>_bearer_start`	Establecimiento de portadora	Se envía la Respuesta de Creación de Se
Actualización de Portadora	`<type>_bearer_update`	Informe de uso durante la sesión	Informes de us periódicos desc plano de usuar
Fin de Portadora	`<type>_bearer_end`	Terminación de portadora	Solicitud/Respu de Eliminación Sesión

Tipos de Portadora:

- `default` - Portadora predeterminada (una por conexión PDN)
- `dedicated` - Portadora dedicada (cero o más por conexión PDN)

Ejemplos de Eventos

```
default_bearer_start      - Portadora predeterminada establecida
default_bearer_update     - Actualización de uso de portadora
predeterminada
default_bearer_end        - Portadora predeterminada terminada
dedicated_bearer_start    - Portadora dedicada establecida
dedicated_bearer_update   - Actualización de uso de portadora
dedicada
dedicated_bearer_end      - Portadora dedicada terminada
```

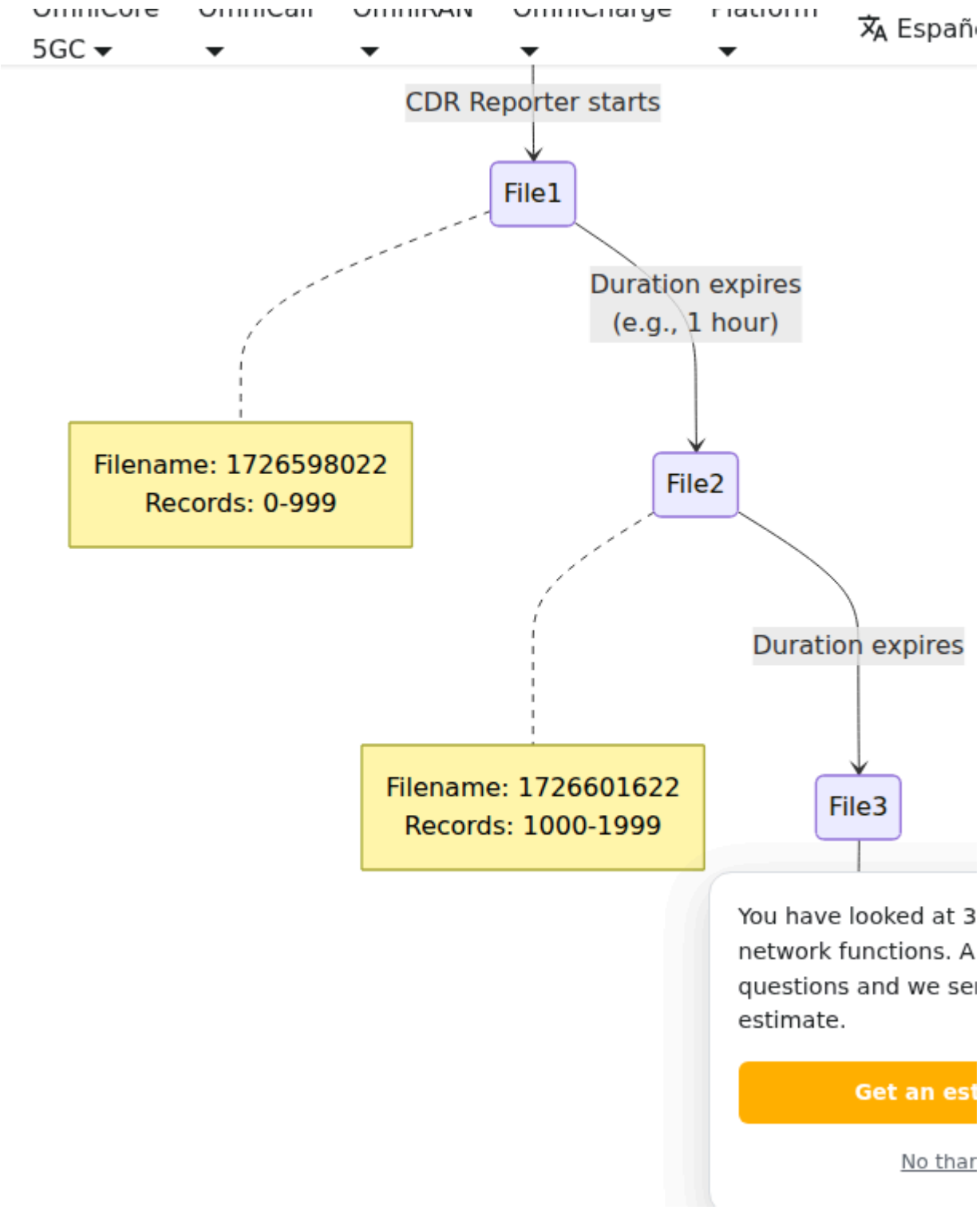
Estructura del Archivo

Ejemplo de Archivo CDR

```
# Archivo CDR de Datos:
# Hora de Inicio del Archivo: 18:53:42 (1726598022)
# Hora de Fin del Archivo: 19:53:42 (1726601622)
# Nombre del Gateway: sgw-c-prod-01
# epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,e
1726598022,310260123456789,default_bearer_start,12345,15551234567,123
1726598322,310260123456789,default_bearer_update,12345,15551234567,12
1726598622,310260123456789,default_bearer_update,12345,15551234567,12
1726598922,310260123456789,default_bearer_end,12345,15551234567,12345
```

Rotación de Archivos

Los archivos CDR se rotan automáticamente según la duración configurada:



Proceso de Rotación:

1. Cerrar el archivo CDR actual
2. Crear un nuevo archivo con la marca de tiempo actual
3. Escribir el encabezado en el nuevo archivo
4. Continuar grabando CDRs en el nuevo archivo

Configuración

Parámetros de Configuración

La generación de CDR para PGW-C se configura en `config/runtime.exs`:

Parámetro	Tipo	Descripción	Predeterminado	
`pgw_name`	cadena	Identificador de la instancia PGW (aparece en los encabezados de CDR)	"omni-pgw01"	Usa o Il
`cdr_file_duration`	entero	Intervalo de rotación del archivo (ms)	3600000	360
`cdr_directory`	cadena	Ruta del directorio de salida de CDR	"/tmp/pgw_c"	`/va`
`usage_report_interval`	entero	Intervalo de informe de URR (ms) - con qué frecuencia PGW-U envía informes de uso	60000	600

Ejemplos de Configuración

Configuración Mínima (config/runtime.exs):

```
config :pgw_c,
  # Configuración del archivo CDR
  pgw_name: "omni-pgw01",
  cdr_file_duration: 3_600_000,           # 1 hora
  cdr_directory: "/var/log/pgw_c/cdrs",

  # Configuración de URR (dispara informes de uso desde PGW-U)
  usage_report_interval: 60_000           # 60 segundos
```

Producción:

```
config :pgw_c,
  pgw_name: "pgw-c-prod-01",
  cdr_file_duration: 3_600_000,           # Rotación de 1 hora
  cdr_directory: "/var/log/pgw_c/cdrs",
  usage_report_interval: 60_000           # Actualizaciones de 1
minuto
```

Desarrollo:

```
config :pgw_c,
  pgw_name: "pgw-c-dev",
  cdr_file_duration: 300_000,             # Rotación de 5 minutos
para pruebas
  cdr_directory: "/tmp/pgw_c_cdrs",
  usage_report_interval: 30_000           # Actualizaciones de 30
segundos para pruebas más rápidas
```

Alto Volumen:

```
config :pgw_c,
  pgw_name: "pgw-c-prod-heavy",
  cdr_file_duration: 1_800_000,           # Rotación de 30 minutos
  cdr_directory: "/mnt/fast-storage/cdrs",
  usage_report_interval: 300_000          # Actualizaciones de 5
minutos (reducir sobrecarga)
```

URR (Reglas de Informe de Uso)

PGW-C utiliza **PFCP URRs (Reglas de Informe de Uso)** para activar informes de uso desde PGW-U. Cuando se alcanza un umbral de URR o expira el tiempo, PGW-U envía una Solicitud de Informe de Sesión que contiene datos de uso, lo que activa la generación de CDR.

Cómo Funciona la Configuración de URR:

1. `usage_report_interval` (en ms) se convierte a segundos para el umbral de tiempo PFCP
2. PGW-C crea URR con umbral de tiempo durante el establecimiento de la sesión
3. PGW-U envía informes de uso periódicos en el intervalo configurado
4. Cada informe de uso activa un evento CDR `bearer_update`
5. El informe de uso final (en la eliminación de la sesión) activa un evento CDR `bearer_end`

Ejemplo: `usage_report_interval: 60_000` significa:

- PGW-U informa el uso cada 60 segundos
- Eventos de actualización de CDR generados cada 60 segundos
- Seguimiento granular del uso para facturación

Definición del Tipo de URR:

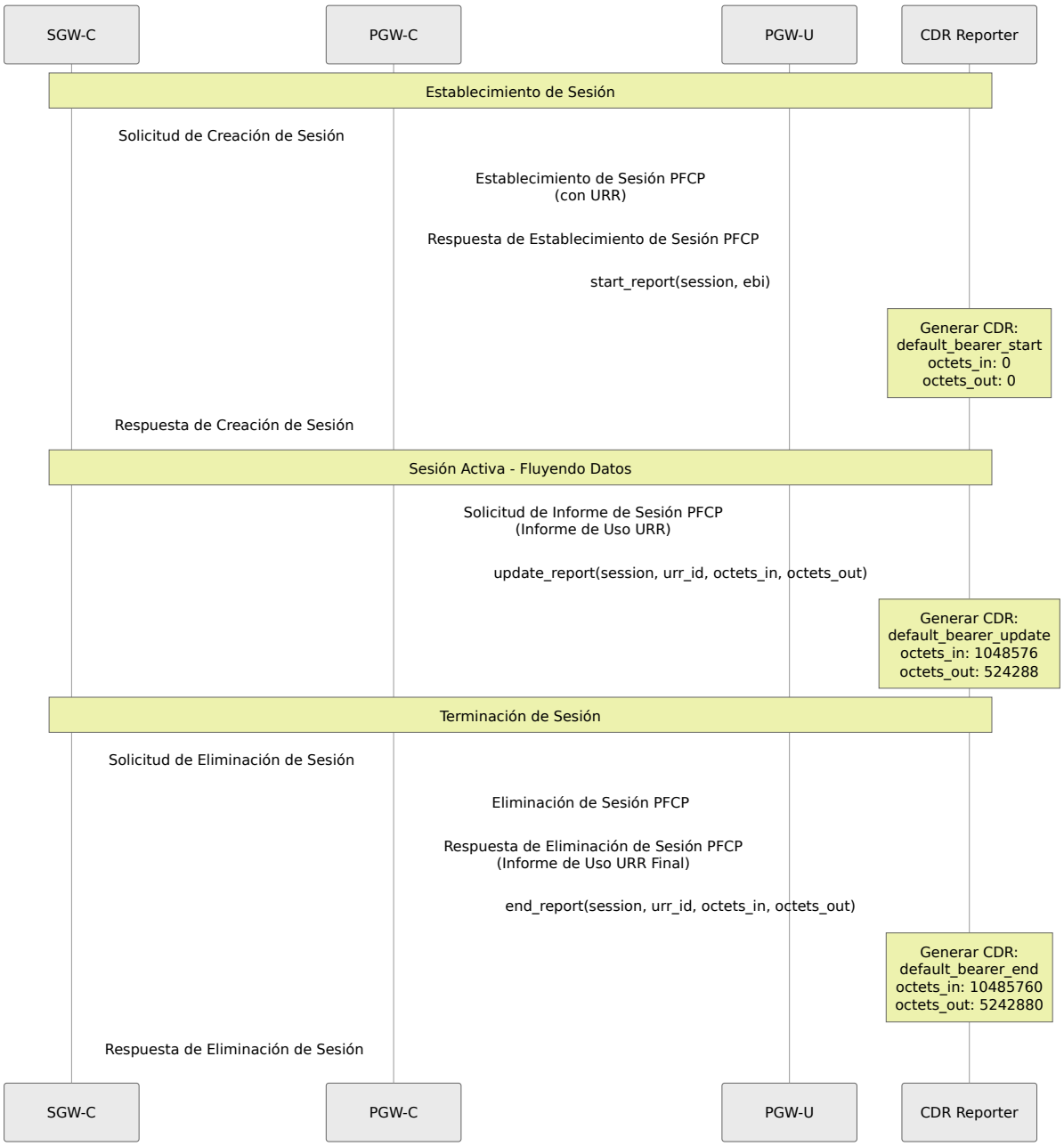
```
defmodule PGW_C.Session.Types.URR do
  typedstruct do
    field :urr_id, non_neg_integer()
    field :measurement_method, :duration | nil
    field :reporting_triggers, :time_threshold | nil
    field :time_threshold, non_neg_integer() | nil  # segundos
  end
end
```

Consulte la Documentación de la Interfaz PFCP para obtener detalles sobre URR PFCP, incluida la forma en que se crean los URRs durante el establecimiento de la sesión.

Flujo de Generación del CDR

Eventos de CDR del Ciclo de Vida de la Portadora

Generación de CDR de PGW-C:



Eventos de Generación de CDR

1. Inicio de Portadora:

- **Cuándo:** Se envía la Respuesta de Creación de Sesión
- **Propósito:** Registra el establecimiento de la portadora con uso cero
- **octets_in:** 0
- **octets_out:** 0

2. Actualización de Portadora:

- **Cuándo:** Se recibe la Solicitud de Informe de Sesión PFCP de PGW-U (informe de uso URR)
- **Propósito:** Registra el uso incremental de datos
- **octets_in:** Bytes acumulativos de enlace descendente desde el inicio de la portadora
- **octets_out:** Bytes acumulativos de enlace ascendente desde el inicio de la portadora
- **Disparador:** Expira el umbral de tiempo de URR (configurado a través de `usage_report_interval`)

3. Fin de Portadora:

- **Cuándo:** Se recibe la Respuesta de Eliminación de Sesión PFCP de PGW-U (con el informe de uso final)
- **Propósito:** Registra el uso final de datos antes de la terminación de la sesión
- **octets_in:** Total final de bytes de enlace descendente
- **octets_out:** Total final de bytes de enlace ascendente

Detalles de los Campos

1. epoch (Marca de Tiempo)

Tipo: Marca de tiempo de época Unix (segundos)

Descripción: El momento en que ocurrió el evento CDR

Ejemplo:

```
1726598022  → 2025-09-17 18:53:42 UTC
```

---

2. imsi (Identidad del Suscriptor)

Tipo: Cadena (hasta 15 dígitos)

Formato: MCCMNC + MSIN

Descripción: Identidad Internacional de Suscriptor Móvil que identifica de manera única al suscriptor

Ejemplo:

```
310260123456789
  └─┘ └─┘ └─────────┘
   MCC  MNC     MSIN
   (310)(260) (123456789)
```

Fuente: Contexto del UE, recibido en la Solicitud de Creación de Sesión

---

3. event (Tipo de Evento CDR)

Tipo: Cadena

Formato: `<bearer_type>_bearer_<event>`

Valores:

- `default_bearer_start`
- `default_bearer_update`
- `default_bearer_end`
- `dedicated_bearer_start`
- `dedicated_bearer_update`
- `dedicated_bearer_end`

Determinación:

- Si EBI (ID de Portadora EPS) es igual a LBI (ID de Portadora Vinculada): `default`

- Si EBI no es igual a LBI: `dedicated`

Fuente: Contexto de la portadora (comparación EBI vs LBI)

---

4. charging_id (Identificador de Carga)

Tipo: Entero sin signo de 32 bits

Descripción: Identificador único para la correlación de carga a través de elementos de red

Ejemplo:

```
12345
```

Fuente: Asignado por PGW-C, recibido en la Respuesta de Creación de Sesión

Uso:

- Correlaciona eventos de carga a través de SGW y PGW
- Utilizado en interfaces de carga Diameter Gy/Gz
- Único por portadora

---

5. msisdn (Número de Teléfono)

Tipo: Cadena (formato E.164)

Descripción: Número ISDN de la Estación Móvil (número de teléfono del suscriptor)

Formato: Código de país + número nacional

Ejemplo:

```
15551234567
 └┬┘└─────┬─────┘
  CC  Nacional
  (1) (5551234567)
```

Fuente: Contexto del UE, típicamente del HSS a través de MME

---

6. ue_imei (Identidad del Equipo)

Tipo: Cadena (15 dígitos)

Formato: TAC (8) + SNR (6) + Spare (1)

Descripción: Identidad Internacional de Equipos Móviles (identificador del dispositivo)

Ejemplo:

```
123456789012345
└──────┬──────┘└──┬──┘└
   TAC    SNR S
```

Fuente: Contexto del UE, recibido de MME

---

7. timezone_raw (Zona Horaria del UE)

Tipo: Cadena (actualmente reservado/vacío)

Descripción: Campo reservado para información de la zona horaria del UE

Estado Actual: No poblado (campo vacío en CSV)

Uso Futuro: Puede incluir el desplazamiento de la zona horaria y la bandera de horario de verano

Ejemplo:

```
,  (campo vacío)
```

---

8. plmn (Identificador de Red)

Tipo: Entero (formato legado)

Descripción: Identificador de la Red Móvil Pública codificado como hexadecimal little-endian

Proceso de Codificación:

```
MCC: 505, MNC: 57
  ↓
"50557"
  ↓
Intercambiar pares: "055570"
  ↓
Hex a decimal: 0x055570 = 349552
```

Ejemplo:

```
349552  → MCC: 505, MNC: 57
```

Fuente: Información de ubicación del UE de MME

Nota: Este es un formato de codificación legado para compatibilidad hacia atrás

---

9. tac (Código de Área de Seguimiento)

Tipo: Entero sin signo de 16 bits

Descripción: El Código de Área de Seguimiento identifica el área de seguimiento donde se encuentra el UE

Rango: 0 - 65535

Ejemplo:

```
1234
```

Fuente: Información de ubicación del UE, recibida de MME en la Solicitud de Creación de Sesión

Uso:

- Identifica el área de gestión de movilidad
- Utilizado para paginación y actualizaciones de ubicación
- Parte de TAI (Identidad del Área de Seguimiento)

---

10. eci (Identificador de Celda E-UTRAN)

Tipo: Entero sin signo de 28 bits

Descripción: El Identificador de Celda E-UTRAN identifica de manera única la celda que sirve al UE

Formato: ID de eNodeB (20 bits) + ID de Celda (8 bits)

Rango: 0 - 268,435,455

Ejemplo:

```
5678
```

Fuente: Información de ubicación del UE de MME

Uso:

- Identifica la torre de celda y sector específicos
- Utilizado para transferencia y gestión de movilidad

- Información de ubicación granular

---

11. sgw_ip (IP del Plano de Control SGW)

Tipo: Cadena (dirección IPv4 o IPv6)

Descripción: Dirección IP del plano de control S5/S8 de SGW-C (F-TEID)

Formato: Decimal con puntos (IPv4) o hexadecimal con dos puntos (IPv6)

Ejemplo:

```
10.0.0.15       (IPv4)
2001:db8::15    (IPv6)
```

Fuente: Configuración local, asignada a la interfaz S5/S8

---

12. ue_ip (Dirección IP del UE)

Tipo: Cadena (formato IPv4|IPv6)

Descripción: Dirección IP asignada al UE para la conexión PDN

Formato: `<ipv4>|<ipv6>`

Ejemplos:

```
172.16.1.100|                      (solo IPv4)
|2001:db8::1                       (solo IPv6)
172.16.1.100|2001:db8::1          (Dual-stack)
```

Fuente: Asignación de Dirección PDN (PAA) de PGW-C

Notas:

- IPv4 vacío: No se asignó dirección IPv4

- IPv6 vacío: No se asignó dirección IPv6
- Ambos presentes: Conexión PDN de doble pila

---

13. pgw_ip (IP del Plano de Control PGW)

Tipo: Cadena (dirección IPv4 o IPv6)

Descripción: Dirección IP del plano de control S5/S8 de PGW-C (F-TEID remoto)

Formato: Decimal con puntos (IPv4) o hexadecimal con dos puntos (IPv6)

Ejemplo:

```
10.0.0.20       (IPv4)
2001:db8::20    (IPv6)
```

Fuente: Recibido en la Respuesta de Creación de Sesión de PGW-C

---

14. apn (Nombre del Punto de Acceso)

Tipo: Cadena (hasta 100 caracteres)

Descripción: Nombre del Punto de Acceso que identifica la red externa (PDN)

Formato: Formato de etiqueta similar a DNS

Ejemplos:

```
internet
ims
mms
enterprise.corporate
```

Fuente: Recibido en la Solicitud de Creación de Sesión de MME

Uso:

- Determina a qué red externa conectarse
- Impulsa políticas y reglas de carga
- Puede determinar el grupo de direcciones IP

---

15. qci (Identificador de Clase de QoS)

Tipo: Entero sin signo de 8 bits

Descripción: El Identificador de Clase de QoS define la calidad de servicio de la portadora

Rango: 1 - 9 (estandarizados), 128-254 (específicos del operador)

Valores de QCI Estandarizados:

QCI	Tipo de Recurso	Prioridad	Retraso de Paquete	Pérdida de Paquete	Servicio de Ejemplo
1	GBR	2	100 ms	10^-2	Voz Conversacional
2	GBR	4	150 ms	10^-3	Video Conversacional
3	GBR	3	50 ms	10^-3	Juegos en Tiempo Real
4	GBR	5	300 ms	10^-6	Video No Conversacional
5	No-GBR	1	100 ms	10^-6	Señalización IMS
6	No-GBR	6	300 ms	10^-6	Video (en búfer)
7	No-GBR	7	100 ms	10^-3	Voz, Video, Juegos
8	No-GBR	8	300 ms	10^-6	Video (en búfer)
9	No-GBR	9	300 ms	10^-6	Portadora Predeterminada

Ejemplo:

```
9  → Portadora predeterminada (mejor esfuerzo)
```

Fuente: Parámetros de QoS de la portadora de PGW-C

---

16. octets_in (Volumen de Enlace Descendente)

Tipo: Entero sin signo de 64 bits

Descripción: Número de bytes transmitidos en la dirección de enlace descendente (red → UE)

Unidades: Bytes

Ejemplo:

```
1048576  → 1 MB de enlace descendente
```

Fuente: Medición de Volumen PFCP de PGW-U (a través de informes de uso URR)

Notas:

- Acumulativo para eventos `update`
- Total final para eventos `end`
- Siempre 0 para eventos `start`
- Informes activados por el umbral de tiempo de URR (configurado a través de `usage_report_interval`)

---

17. octets_out (Volumen de Enlace Ascendente)

Tipo: Entero sin signo de 64 bits

Descripción: Número de bytes transmitidos en la dirección de enlace ascendente (UE → red)

Unidades: Bytes

Ejemplo:

```
524288  → 512 KB de enlace ascendente
```

Fuente: Medición de Volumen PFCP de PGW-U (a través de informes de uso URR)

Notas:

- Acumulativo para eventos `update`
- Total final para eventos `end`
- Siempre 0 para eventos `start`
- Informes activados por el umbral de tiempo de URR (configurado a través de `usage_report_interval`)

Ejemplos

Ejemplo 1: Sesión Básica con Actualización Única

Cronología:

1. Portadora establecida
2. 5 minutos después: Actualización de uso (10 MB de bajada, 5 MB de subida)
3. Sesión terminada

Salida del CDR:

```
# Archivo CDR de Datos:
# Hora de Inicio del Archivo: 10:00:00 (1726570800)
# Hora de Fin del Archivo: 11:00:00 (1726574400)
# Nombre del Gateway: pgw-c-01
# epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,e
1726570800,310260111111111,default_bearer_start,10001,15551111111,111
1726571100,310260111111111,default_bearer_update,10001,15551111111,11
1726571400,310260111111111,default_bearer_end,10001,15551111111,11111
```

Ejemplo 2: Sesión de Doble Pila con Múltiples Actualizaciones

Cronología:

1. Portadora de doble pila establecida (IPv4 + IPv6)
2. Múltiples actualizaciones de uso
3. Sesión terminada

Salida del CDR:

```
1726570800,310260222222222,default_bearer_start,10002,15552222222,222
1726571100,310260222222222,default_bearer_update,10002,15552222222,22
1726571400,310260222222222,default_bearer_update,10002,15552222222,22
1726571700,310260222222222,default_bearer_update,10002,15552222222,22
1726572000,310260222222222,default_bearer_end,10002,15552222222,22222
```

Ejemplo 3: Sesión con Portadora Dedicada

Cronología:

1. Portadora predeterminada establecida (QCI 9)
2. Portadora dedicada creada para video (QCI 6)
3. Actualizaciones de uso para ambas portadoras
4. Portadora dedicada eliminada
5. Portadora predeterminada terminada

Salida del CDR:

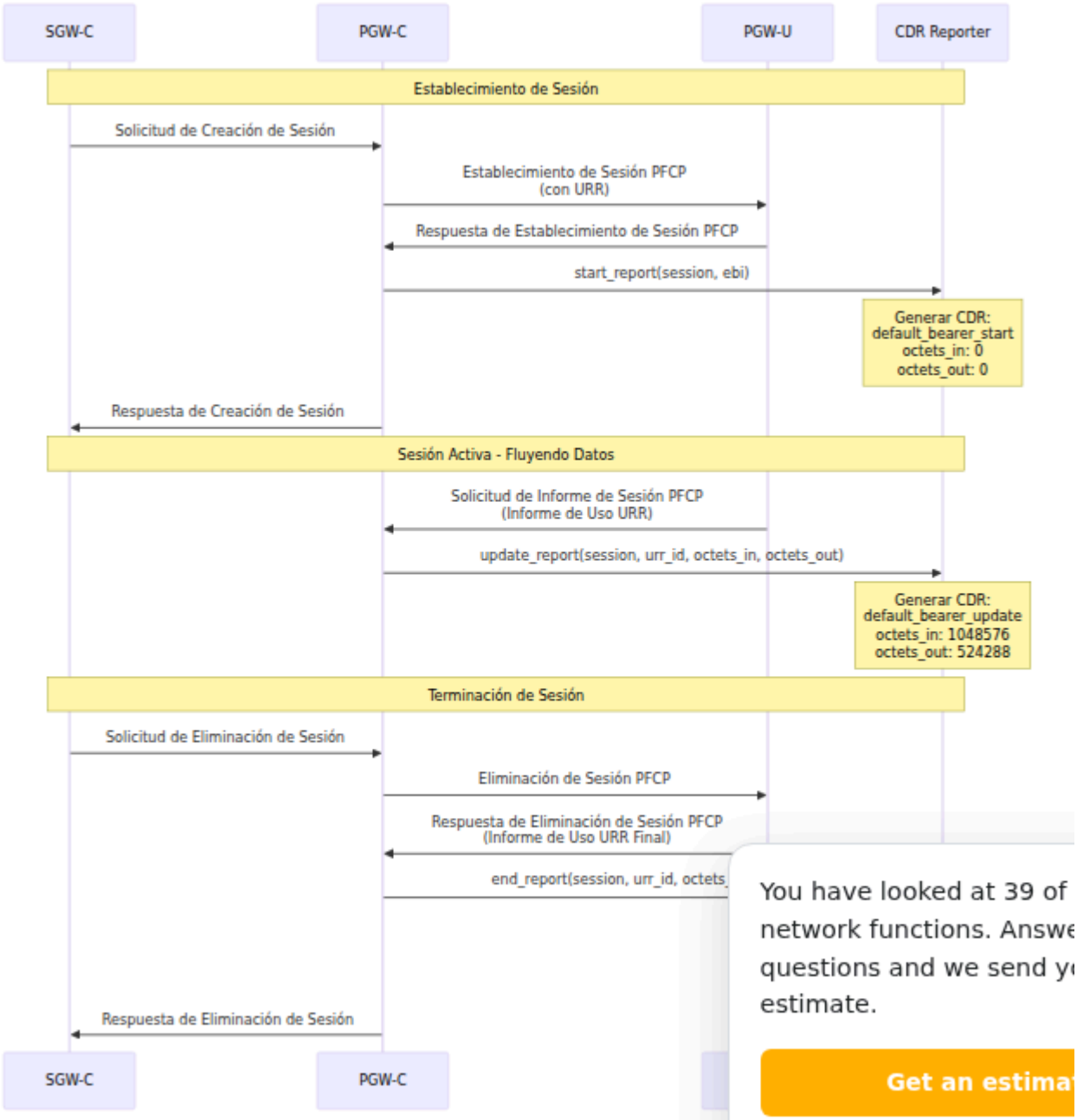
```
1726570800,310260333333333,default_bearer_start,10003,15553333333,333
1726571100,310260333333333,dedicated_bearer_start,10004,15553333333,3
1726571400,310260333333333,default_bearer_update,10003,15553333333,33
1726571400,310260333333333,dedicated_bearer_update,10004,15553333333,
1726571700,310260333333333,dedicated_bearer_end,10004,15553333333,333
1726572000,310260333333333,default_bearer_end,10003,15553333333,33333
```

Análisis:

- La portadora predeterminada (10003) transporta tráfico de fondo (10 MB de bajada, 4 MB de subida)
- La portadora dedicada (10004) transporta tráfico de video (200 MB de bajada, 2 MB de subida)
- Diferentes valores de QCI (9 vs 6) reflejan diferentes tratamientos de QoS

Integración

Pipeline de Procesamiento de CDR



Métodos de Recolección de CDR

1. Recolección Basada en Archivos:

```
# Monitorear el directorio CDR (PGW-C)
inotifywait -m /var/log/pgw_c/cdrs/ -e close_write | while read
path action file; do
    # Rotación de archivo completada, procesar CDR
    process_cdr "$path$file"
done
```

2. Transmisión en Tiempo Real:

```
# Seguir y transmitir al pipeline de procesamiento
tail -F /var/log/pgw_c/cdrs/* | process_cdr_stream
```

Documentación Relacionada

- Gestión de Sesiones - Ciclo de vida de la sesión y activadores de CDR
- Interfaz PFCP - Informe de uso desde PGW-U a través de URRs
- Guía de Monitoreo - Métricas de generación de CDR y alertas
- Guía de Configuración - Parámetros de configuración de CDR y URR
- Interfaz Diameter Gx - Control de políticas para valores de QCI en CDRs
- Interfaz Diameter Gy - Integración de carga en línea

Referencias 3GPP

- TS 32.251 - Carga del dominio de Paquetes (PS)
- TS 29.274 - Sistema de Paquetes Evolucionado 3GPP (EPS); protocolo GTP-C
- TS 29.244 - Interfaz entre nodos CP y UP (PFCP) - **Soporte URR**
- TS 32.298 - Codificación de CDR

Formato CDR - *Registros de Carga Offline para PGW-C*

Desarrollado por Omnitouch Network Services

Versión de Documentación: 1.0 **Última Actualización:** 2025-12-28

Documentación de la Interfaz Gx de Diameter

Interfaz de la Función de Reglas de Políticas y Cargos (PCRF)

Tabla de Contenidos

1. Descripción General
2. Conceptos Básicos de la Interfaz Gx
3. Protocolo Diameter
4. Mensajes de Control de Crédito
5. Reglas de Políticas y Cargos
6. Informe de Cambio de Ubicación
7. Configuración
8. Flujos de Mensajes
9. Manejo de Errores
10. Solución de Problemas

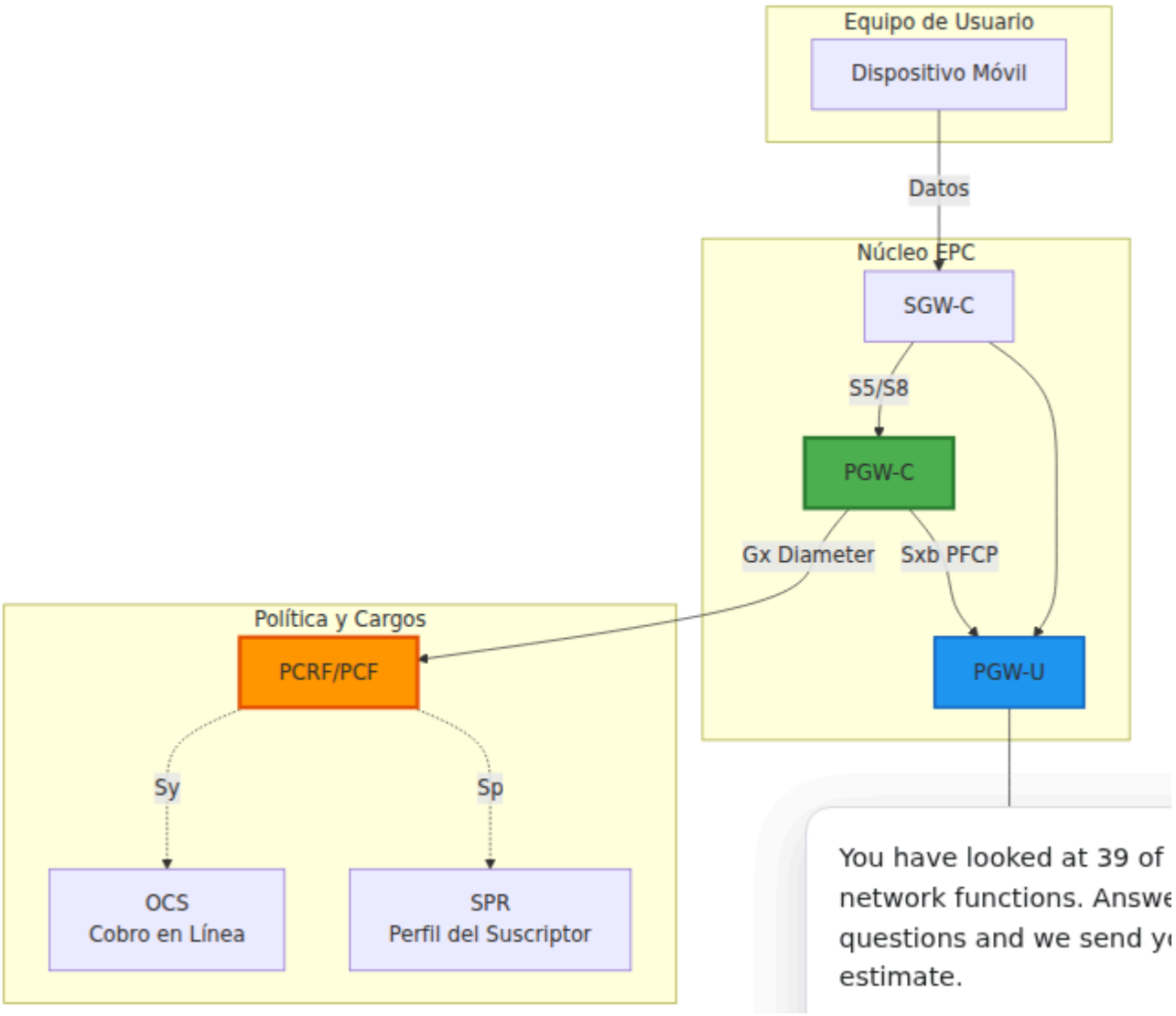
Descripción General

La **interfaz Gx** conecta PGW-C a la **PCRF (Función de Reglas de Políticas y Cargos)** o **PCF (Función de Control de Políticas)** en redes 5G. Esta interfaz permite:

- **Control Dinámico de Políticas** - Aplicación de QoS y políticas en tiempo real
- **Control de Cargos** - Autorización de crédito y seguimiento de uso

- **Conciencia del Servicio** - Diferenciación de tráfico a nivel de aplicación
- **Gestión del Perfil del Suscriptor** - Aplicación de políticas por usuario

Gx en la Arquitectura de la Red



Funciones Clave

Función	Descripción
Provisionamiento de Políticas	PCRF proporciona reglas PCC que definen cómo manejar el tráfico
Control de QoS	Ajuste dinámico de tasas de bits y parámetros de QoS
Control de Cargos	Autorización de crédito para escenarios prepagados/postpagados
Control de Gating	Habilitar/deshabilitar flujos de tráfico basados en políticas
Monitoreo de Uso	Seguimiento del consumo de datos por servicio

---

Conceptos Básicos de la Interfaz Gx

Referencia 3GPP

- **Especificación:** 3GPP TS 29.212
- **ID de Aplicación Diameter:** 16777238 (Gx)
- **Protocolo:** Protocolo Base de Diameter (RFC 6733)

Concepto de Sesión

Cada conexión PDN de UE tiene una **sesión Gx** correspondiente identificada por un **Session-ID**. Esta sesión:

- Se crea cuando el UE se conecta (CCR-Initial)

- Se actualiza durante la vida útil de la conexión (CCR-Update) - opcional, por ejemplo, cambios de política o informe de cambio de ubicación
- Se termina cuando el UE se desconecta (CCR-Termination)

Formato del ID de Sesión

```
Session-ID: <Origin-Host>;<high32>;<low32>[;<optional>]
Ejemplo: omni-
pgw_c.epc.mnc999.mcc999.3gppnetwork.org;1234567890;98765
```

Componentes:

- **Origin-Host:** Identidad Diameter de PGW-C
- **high32:** 32 bits altos del identificador único
- **low32:** 32 bits bajos del identificador único

Protocolo Diameter

Estructura del Mensaje

Los mensajes de Diameter están codificados en binario con la siguiente estructura:

```
Encabezado de Diameter (20 bytes)
├── Versión (1 byte) = 1
├── Longitud del Mensaje (3 bytes)
├── Banderas (1 byte)
│   ├── R: Solicitud (1) / Respuesta (0)
│   ├── P: Proxiable
│   ├── E: Error
│   └── T: Potencialmente retransmitido
├── Código de Comando (3 bytes)
├── ID de Aplicación (4 bytes) = 16777238 (Gx)
├── ID de Salto a Salto (4 bytes)
└── ID de Extremo a Extremo (4 bytes)

AVPs (Pares Atributo-Valor)
├── Encabezado de AVP
│   ├── Código de AVP
│   ├── Banderas (V, M, P)
│   ├── Longitud de AVP
│   └── ID de Vendedor (opcional)
└── Datos de AVP
```

Conceptos Clave de Diameter

AVP (Par Atributo-Valor):

- Unidad de datos básica en Diameter
- Contiene un código, banderas y valor
- Puede estar anidado (AVP Agrupado)

Comando:

- Par Solicitud/Respuesta
- CCR (Solicitud de Control de Crédito) / CCA (Respuesta de Control de Crédito)

Códigos de Resultado:

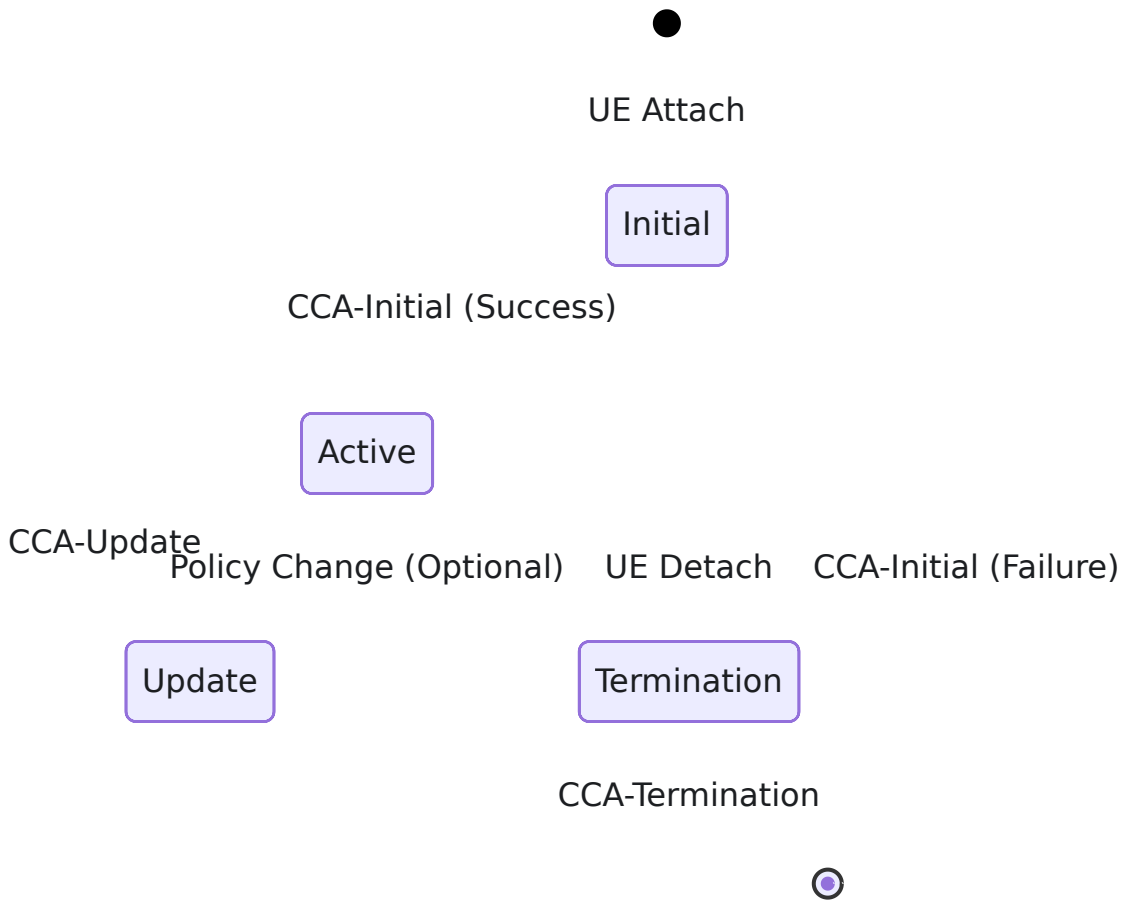
- `2001` - DIAMETER_SUCCESS
- `3xxx` - Errores de protocolo

- `4xxx` - Fallos transitorios
- `5xxx` - Fallos permanentes

Mensajes de Control de Crédito

PGW-C utiliza la **Aplicación de Control de Crédito Diameter** (RFC 4006) para Gx.

Tipos de Mensajes



CCR-Initial (Solicitud de Control de Crédito - Inicial)

Cuándo: UE crea una nueva conexión PDN

Propósito:

- Solicitar reglas iniciales de políticas y cargos
- Proporcionar contexto de UE y red a PCRF
- Obtener parámetros de QoS y autorización de cargos

AVPs Clave Enviados por PGW-C:

Nombre de AVP	Código de AVP	Tipo	Descripción
Session-Id	263	UTF8String	Identificador único de sesión Gx
Auth-Application-Id	258	Unsigned32	16777238 (Gx)
Origin-Host	264	DiamIdent	Identidad Diameter de PGW-C
Origin-Realm	296	DiamIdent	Reino Diameter de PGW-C
Destination-Realm	283	DiamIdent	Reino de PCRF
CC-Request-Type	416	Enumerated	1 = INITIAL_REQUEST
CC-Request-Number	415	Unsigned32	Número de secuencia (comienza en 0)
Subscription-Id	443	Grouped	Identificador de UE (IMSI/MSISDN)
Called-Station-Id	30	UTF8String	Nombre de APN
Framed-IP-Address	8	OctetString	Dirección IPv4 asignada a UE (PDNs IPv4 e IPv4v6)
Framed-IPv6-Prefix	97	OctetString	Prefijo IPv6 asignado a UE (PDNs solo IPv6)
3GPP-User-Location-Info	22	OctetString	ULI inicial del suscriptor (TS 29.061)

Nombre de AVP	Código de AVP	Tipo	Descripción
User-Equipment-Info	458	Grouped	Identidad de UE (por ejemplo, IMEISV), cuando esté disponible
IP-CAN-Type	1027	Enumerated	5 = 3GPP-EPS
RAT-Type	1032	Enumerated	Mapeado desde el tipo RAT de GTP (por ejemplo, 1004 = EUTRAN)
QoS-Information	1016	Grouped	QoS actual (APN-AMBR UL/DL)
Default-EPS-Bearer-QoS	1049	Grouped	QoS del portador por defecto QCI/ARP (QCI 5)
Network-Request-Support	1024	Enumerated	Procedimientos iniciados por la red
Supported-Features	628	Grouped	Lista de características Gx (Rel-8/9/10 Gx)

> El AVP de dirección enmarcada es seleccionado por la familia de direcciones de UE: `Framed-IP-Address` para IPv4 (y la IPv4 de un PDN IPv4v6), `Framed-IPv6-Prefix` para un IPv6 único PDN. Para IPv4v6, el prefijo IPv6 no se transporta en Gx. Ver IPv6 / Dual-Stack.

Ejemplo de Estructura CCR-I:

```
CCR (Código de Comando: 272, Solicitud)
├── Session-Id: "pgw_c.example.com;123;456"
├── Auth-Application-Id: 16777238
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: INITIAL_REQUEST (1)
├── CC-Request-Number: 0
├── Subscription-Id (Agrupado)
│   ├── Subscription-Id-Type: END_USER_IMSI (1)
│   └── Subscription-Id-Data: "310260123456789"
├── Called-Station-Id: "internet"
├── Framed-IP-Address: 100.64.1.42
├── IP-CAN-Type: 3GPP-EPS (5)
├── RAT-Type: EUTRAN (1004)
├── QoS-Information (Agrupado)
│   ├── APN-Aggregate-Max-Bitrate-UL: 100000000 (100 Mbps)
│   └── APN-Aggregate-Max-Bitrate-DL: 50000000 (50 Mbps)
├── Network-Request-Support: 1
└── Supported-Features: [...]
```

CCA-Initial (Respuesta de Control de Crédito - Inicial)

Enviado por: PCRF en respuesta a CCR-I

Propósito:

- Autorizar o rechazar la sesión
- Proporcionar reglas PCC para el manejo del tráfico
- Especificar parámetros de QoS

AVPs Clave Recibidos por PGW-C:

Nombre de AVP	Código de AVP	Descripción
Result-Code	268	Éxito (2001) o código de error
Experimental-Result	297	Códigos de resultado específicos del vendedor
QoS-Information	1016	QoS autorizada (puede diferir de la solicitud)
Charging-Rule-Install	1001	Reglas PCC a activar
Charging-Rule-Definition	1003	Definiciones de reglas en línea
Default-EPS-Bearer-QoS	1049	QoS para el portador por defecto

Ejemplo de Respuesta de Éxito:

```
CCA (Código de Comando: 272, Respuesta)
├── Session-Id: "pgw_c.example.com;123;456"
├── Result-Code: DIAMETER_SUCCESS (2001)
├── Origin-Host: "pcrf.example.com"
├── Origin-Realm: "example.com"
├── Auth-Application-Id: 16777238
├── CC-Request-Type: INITIAL_REQUEST (1)
├── CC-Request-Number: 0
├── QoS-Information (Agrupado)
│   ├── APN-Aggregate-Max-Bitrate-UL: 50000000 (50 Mbps -
reducido)
│   └── APN-Aggregate-Max-Bitrate-DL: 100000000 (100 Mbps -
incrementado)
├── Charging-Rule-Install (Agrupado)
│   ├── Charging-Rule-Name: "default_internet_rule"
│   └── Charging-Rule-Name: "video_streaming_rule"
└── Charging-Rule-Definition (Agrupado)
    ├── Charging-Rule-Name: "default_internet_rule"
    ├── QoS-Information: {...}
    └── Precedence: 1000
```

CCR-Termination (Solicitud de Control de Crédito - Terminación)

Cuándo: UE se desconecta o la conexión PDN se elimina

Propósito:

- Notificar a PCRF sobre la terminación de la sesión
- Registro final de contabilidad/cargos

Diferencias Clave con CCR-I:

- `CC-Request-Type: TERMINATION_REQUEST (3)`
- Puede incluir estadísticas de uso
- Conjunto de AVP simplificado

Ejemplo CCR-T:

```
CCR (Código de Comando: 272, Solicitud)
├── Session-Id: "pgw_c.example.com;123;456"
├── Auth-Application-Id: 16777238
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: TERMINATION_REQUEST (3)
├── CC-Request-Number: 1
└── Termination-Cause: DIAMETER_LOGOUT (1)
```

CCA-Termination

Enviado por: PCRF en respuesta a CCR-T

Propósito:

- Reconocer la terminación de la sesión
- No se devuelven reglas de políticas

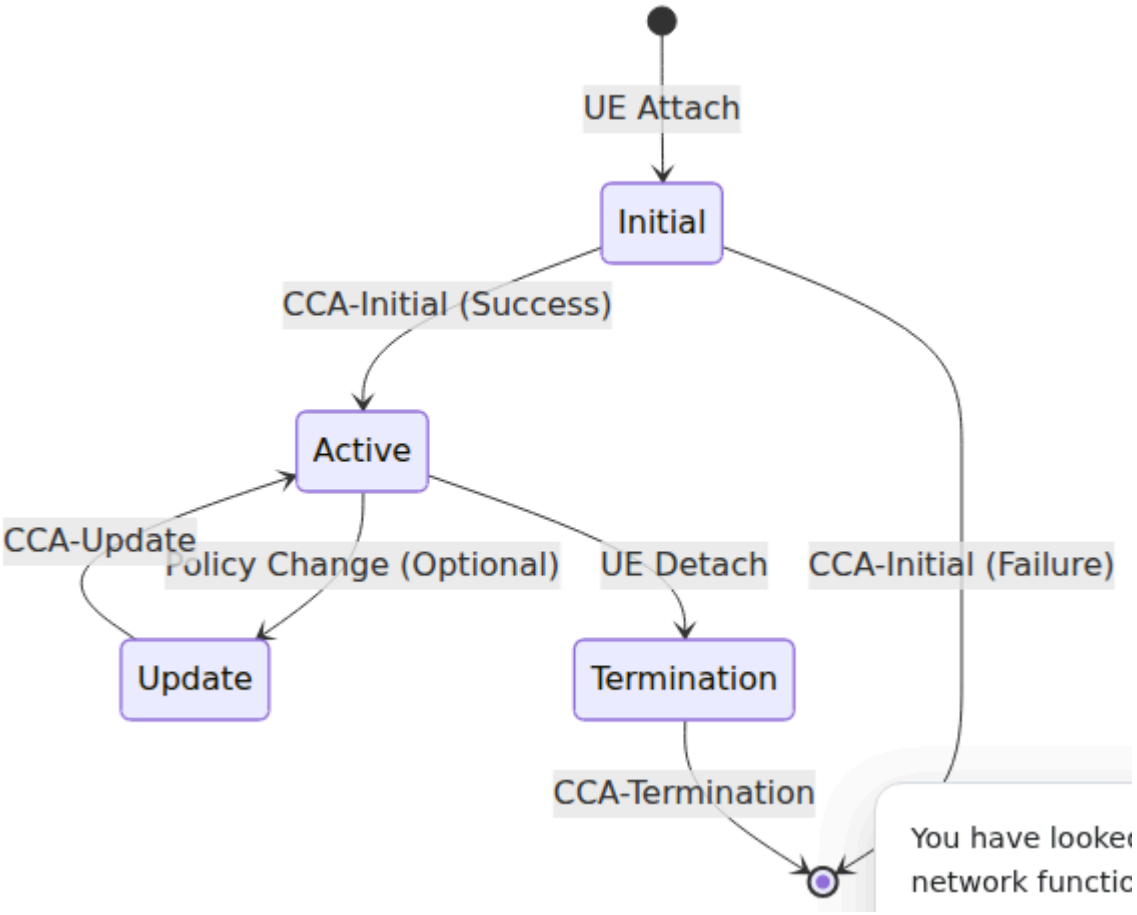
Ejemplo CCA-T:

```
CCA (Código de Comando: 272, Respuesta)
├── Session-Id: "pgw_c.example.com;123;456"
├── Result-Code: DIAMETER_SUCCESS (2001)
├── Origin-Host: "pcrf.example.com"
├── Origin-Realm: "example.com"
├── Auth-Application-Id: 16777238
├── CC-Request-Type: TERMINATION_REQUEST (3)
└── CC-Request-Number: 1
```

Reglas de Políticas y Cargos

Estructura de la Regla PCC

Una **Regla PCC (Control de Políticas y Cargos)** define cómo manejar flujos de tráfico específicos:



Componentes de la Regla

1. Nombre de la Regla:

- Identificador único para la regla
- Ejemplo: `"video_streaming_rule"`

2. Precedencia:

- Número más bajo = mayor prioridad
- Rango: 0-65535
- Se utiliza cuando múltiples reglas coinciden

3. Filtros de Flujo (TFT - Plantilla de Flujo de Tráfico):

- Define qué paquetes coinciden con esta regla
- Ejemplos:
  - Tupla IP 5: Protocolo, IP de origen/destino, Puerto de origen/destino

- `"permit out ip from any to 8.8.8.8 80"`

4. Información de QoS:

- **QCI (Identificador de Clase de QoS):** 1-9 (estandarizado), 128-254 (específico del operador)
  - QCI 1: Voz Conversacional
  - QCI 5: Señalización IMS
  - QCI 9: Internet por Defecto
- **ARP (Prioridad de Asignación y Retención):** Capacidad de preempción
- **MBR/GBR:** Tasas de Bits Máximas/Garantizadas

5. Información de Cargos:

- **Grupo de Calificación:** Identifica la categoría de cargos (utilizado por OCS - ver Interfaz Diameter Gy)
- **Método de Medición:** Basado en volumen, tiempo o evento
- **Cobro en Línea/Fuera de Línea:** OCS (prepago a través de Diameter Gy) vs. CDRs fuera de línea (postpago - ver Formato de CDR de Datos)

6. Estado de Gating:

- **ABIERTO:** Permitir tráfico
- **CERRADO:** Bloquear tráfico

Provisionamiento Dinámico de Reglas

PCRF puede proporcionar reglas de dos maneras:

1. Reglas Predefinidas (por nombre):

```
Charging-Rule-Install (Agrupado)
├── Charging-Rule-Name: "gold_subscriber_internet"
└── Charging-Rule-Name: "video_qos_boost"
```

2. Reglas Dinámicas (definición en línea):

```
Charging-Rule-Definition (Agrupado)
├── Charging-Rule-Name: "dynamic_rule_123"
├── Precedence: 100
├── Flow-Information (Agrupado)
│   ├── Flow-Description: "permit out ip from any to 192.0.2.0/24"
│   └── Flow-Direction: DOWNLINK
├── QoS-Information (Agrupado)
│   ├── QoS-Class-Identifier: 5
│   ├── Max-Requested-Bandwidth-UL: 10000000
│   └── Max-Requested-Bandwidth-DL: 50000000
└── Rating-Group: 1000
```

AVP de Información de QoS

APN-AMBR (Tasa de Bits Máxima Agregada):

Se aplica a todos los portadores no-GBR para este APN:

```
QoS-Information (Agrupado)
├── APN-Aggregate-Max-Bitrate-UL: 100000000  # 100 Mbps
└── APN-Aggregate-Max-Bitrate-DL: 200000000  # 200 Mbps
```

Respuesta de PGW-C:

- Actualiza el estado interno de AMBR
- Envía una Solicitud de Modificación de Sesión a PGW-U con QER actualizado

---

Informe de Cambio de Ubicación

PGW-C puede notificar a la PCRF cuando la **ubicación**, **tecnología de acceso radio (RAT)**, **PLMN de servicio** o **zona horaria de UE** de un suscriptor cambian durante la vida de una sesión. El cambio se transporta en un **CCR-Update** como el **3GPP-User-Location-Info** y AVPs relacionados.

El informe es opcional (controlado por PCRF)

Este informe es **condicional a que la PCRF lo solicite** — exactamente como se requiere en 3GPP TS 29.212 §4.5.7 / §5.3.7. La PCRF *arma* los eventos de los que quiere recibir información incluyendo uno o más AVPs **Event-Trigger** en un **CCA** (o en un **RAR**). PGW-C almacena el conjunto armado por sesión Gx y solo envía un CCR-Update cuando:

1. ocurre realmente la condición de un Event-Trigger armado, **y**
2. existe una sesión Gx para el suscriptor.

Si la PCRF no arma **ningún** Event-Trigger relacionado con la ubicación, PGW-C permanece en silencio sobre los cambios de ubicación — simplemente actualiza su estado interno y responde a la Solicitud de Modificación de Portador de GTP-C. Esto mantiene la interfaz silenciosa para PCRFs que no se preocupan por la movilidad, y conforme para aquellos que sí.

El conjunto armado puede cambiar en cualquier momento durante la sesión. PGW-C lo actualiza desde cada conjunto de AVP de Event-Trigger que la PCRF envía — en el CCA-Initial, en un CCA-Update, o en un **RAR** iniciado por PCRF. Un conjunto de Event-Trigger presente reemplaza el conjunto armado actual; un mensaje que no transporta AVP de Event-Trigger deja el conjunto armado sin cambios. Así, una PCRF puede iniciar una sesión sin informes de ubicación y luego activarlo (o desactivarlo) con un RAR, y viceversa.

Event-Triggers Soportados

Event-Trigger	Valor	Se activa cuando…	AVP Reportado
`RAT_CHANGE`	2	Cambios en RAT-Type (por ejemplo, EUTRAN → UTRAN)	`RAT-Type`
`PLMN_CHANGE`	4	Cambios en la red de servicio (MCC/MNC)	`3GPP-SGSN-MCC-MNC`
`USER_LOCATION_CHANGE`	13	Cualquier cambio en la Información de Ubicación del Usuario	`3GPP-User-Location-Info`
`UE_TIME_ZONE_CHANGE`	25	Cambios en la zona horaria de UE	`3GPP-MS-TimeZone`
`TAI_CHANGE`	26	Cambios en la Identidad del Área de Seguimiento	`3GPP-User-Location-Info`
`ECGI_CHANGE`	27	Cambios en la Identidad Global de Celda E-UTRAN	`3GPP-User-Location-Info`

Múltiples triggers pueden activarse a la vez (por ejemplo, moverse a una nueva celda en un nuevo área de seguimiento activa `USER_LOCATION_CHANGE`, `TAI_CHANGE` **y** `ECGI_CHANGE`); todos los triggers activados y armados se enumeran en los AVPs `Event-Trigger` del CCR-Update.

De dónde proviene la ubicación

- **CCR-Initial** ahora incluye la `3GPP-User-Location-Info` inicial del suscriptor, dando a la PCRF una línea base.

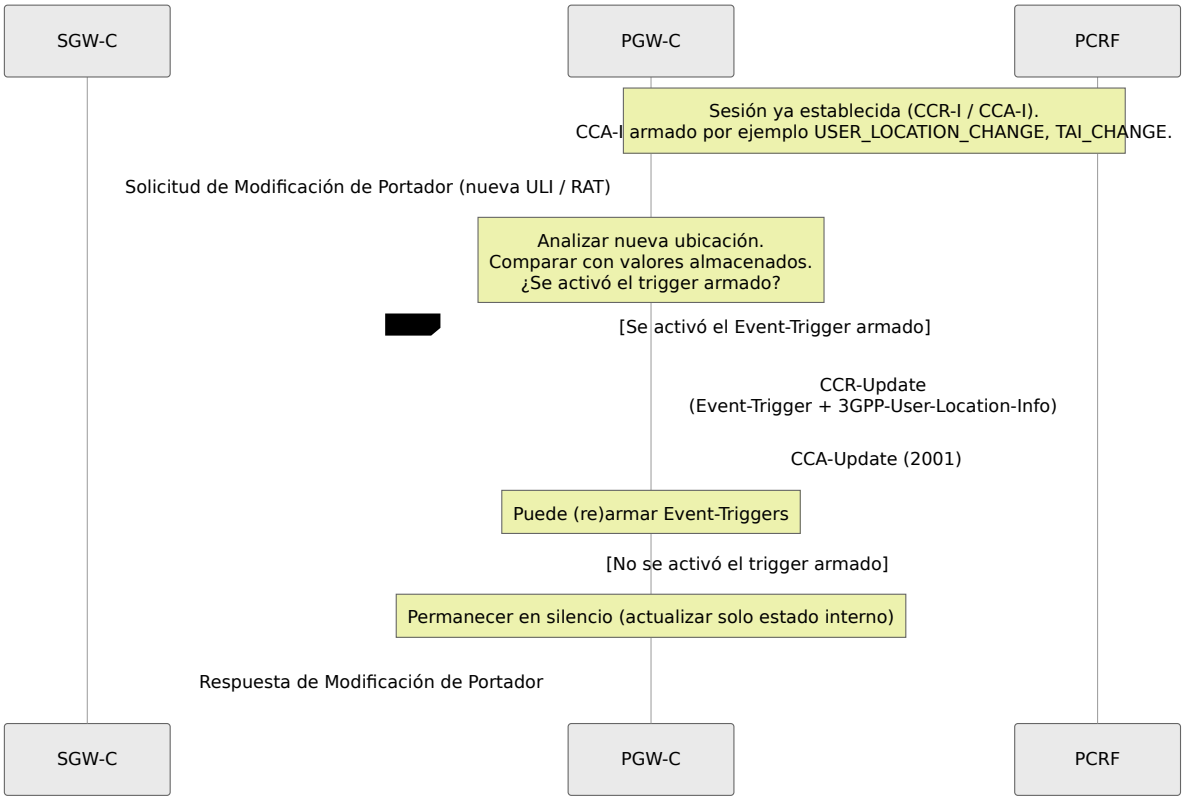
- Durante la sesión, una **Solicitud de Modificación de Portador de GTP-C** (S5/S8) transporta la Información de Ubicación del Usuario actualizada, RAT-Type, Red de Servicio y Zona Horaria de UE. PGW-C analiza estos, los compara con los valores almacenados y reporta cualquier cambio armado.
- IEs **ausentes** de una Solicitud de Modificación de Portador mantienen su valor anterior, por lo que una Solicitud de Modificación de Portador parcial nunca parece un cambio de ubicación espurio.

Codificación de 3GPP-User-Location-Info

El AVP se codifica según **3GPP TS 29.061 §16.4.7.2**: un tipo de *Ubicación Geográfica* de un octeto seguido de los campos de ubicación, con identidades PLMN codificadas según 3GPP TS 24.008 §10.5.1.3. Tipos soportados:

Tipo	Valor	Contenido
CGI	0	PLMN + LAC + CI (2G)
SAI	1	PLMN + LAC + SAC (3G)
RAI	2	PLMN + LAC + RAC
TAI	128	PLMN + TAC (LTE)
ECGI	129	PLMN + ECI (LTE)
TAI y ECGI	130	PLMN + TAC + PLMN + ECI (LTE, preferido)

Flujo de Mensajes



> **Robustez:** informar el cambio a la PCRF nunca bloquea la Respuesta de Modificación de Portador de GTP-C. Si el CCR-Update se agota o la PCRF devuelve un error, PGW-C lo registra y aún responde al SGW-C — la ruta de datos del suscriptor no se detiene por un fallo en el informe de políticas.

Inspeccionando los triggers armados a través de la API

La API de Sesiones (`GET /api/sessions` y `GET /api/sessions/:imsi`) devuelve un volcado completo, seguro para JSON de la sesión bajo la clave `state`, además de los campos de nivel superior curados. Los Event-Triggers armados por PCRF son visibles en `state.gx.requested_event_triggers`, junto con el resto del estado de la sesión Gx (`session_id`, `cc_request_number`, host/reino de destino) y el actual `state.uli`. Esto hace posible confirmar desde las herramientas de operaciones si un suscriptor está realmente suscrito a informes de ubicación.

Sobrescribiendo los triggers armados a través de la API

El conjunto armado también se puede cambiar directamente en una sesión activa con **`PATCH /api/sessions/:imsi`** (útil para probar la función sin una PCRF, o para forzar el informe encendido/apagado). El cuerpo se **fusiona profundamente en el estado de la sesión**, por lo que la ruta refleja la estructura devuelta por `GET` — los triggers armados viven bajo `gx`:

```
PATCH /api/sessions/310260000000001
Content-Type: application/json

{ "gx": { "requested_event_triggers": [13, 26, 27] } }
```

- El valor es una lista de códigos de Event-Trigger de Gx; reemplaza el conjunto armado (otros campos `gx` quedan intactos por la fusión).
- Una lista vacía (`[]`) desarma todos los informes de ubicación para la sesión.
- La respuesta refleja el estado de la sesión actualizado y saneado.

Este endpoint no tiene **guardrails**: el cuerpo se fusiona profundamente en la sesión activa, por lo que *cualquier* campo puede ser cambiado — incluyendo a un valor que rompa la sesión. Los cambios que tienen efectos posteriores se propagan al UPF. Actualizar el APN-AMBR o la QoS del portador por defecto recalcula el QER del portador por defecto (QCI / MBR / GBR) y lo empuja como un QER de Actualización en una Modificación de Sesión PFCP:

```
PATCH /api/sessions/310260000000001
Content-Type: application/json

{ "ambr": { "uplink": 200000, "downlink": 200000 } }
```

```
PATCH /api/sessions/310260000000001
Content-Type: application/json

{ "default_bearer_qos": { "qci": 5, "mbr_ul": 300000, "mbr_dl":
250000 } }
```

Cuando `default_bearer_qos` proporciona MBR/GBR explícitos (portadores GBR) esos impulsan los límites de tasa de QER; de lo contrario, se utiliza el APN-AMBR como el MBR del portador por defecto.

> Nota: sobrescribir los triggers armados cambia la vista local de PGW-C de lo que la PCRF armó. La PCRF aún puede rearmar el conjunto más tarde a través de un CCA o RAR, lo que sobrescribirá una anulación manual.

Configuración

Configuración Básica de Gx

Edita `config/runtime.exs`:

```
config :pgw_c,
  diameter: %{
    # Dirección IP para escuchar conexiones Diameter
    listen_ip: "0.0.0.0",

    # Identidad Diameter de PGW-C (Origin-Host)
    host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",

    # Reino Diameter de PGW-C (Origin-Realm)
    realm: "epc.mnc999.mcc999.3gppnetwork.org",

    # Lista de pares PCRF
    peer_list: [
      %{
        # Identidad Diameter de PCRF
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",

        # Reino de PCRF (generalmente el mismo que el reino de
PGW-C)
        realm: "epc.mnc999.mcc999.3gppnetwork.org",

        # Dirección IP de PCRF
        ip: "10.0.0.30",

        # Si PGW-C inicia la conexión a PCRF
        # true = PGW-C se conecta a PCRF
        # false = Espera a que PCRF se conecte
        initiate_connection: true
      }
    ]
  }
```

Múltiples Pares PCRF

Para redundancia o distribución geográfica:

```
config :pgw_c,
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf-primary.example.com",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.1.30",
        initiate_connection: true
      },
      %{
        host: "pcrf-backup.example.com",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.2.30",
        initiate_connection: true
      }
    ]
  }
```

Balanceo de Carga:

- El protocolo Diameter maneja la selección de pares
- Solicitudes distribuidas según disponibilidad
- Failover automático en caso de fallo de un par

Resolución de Nombres de Host

Las Identidades Diameter deben ser FQDNs (Nombres de Dominio Completamente Calificados):

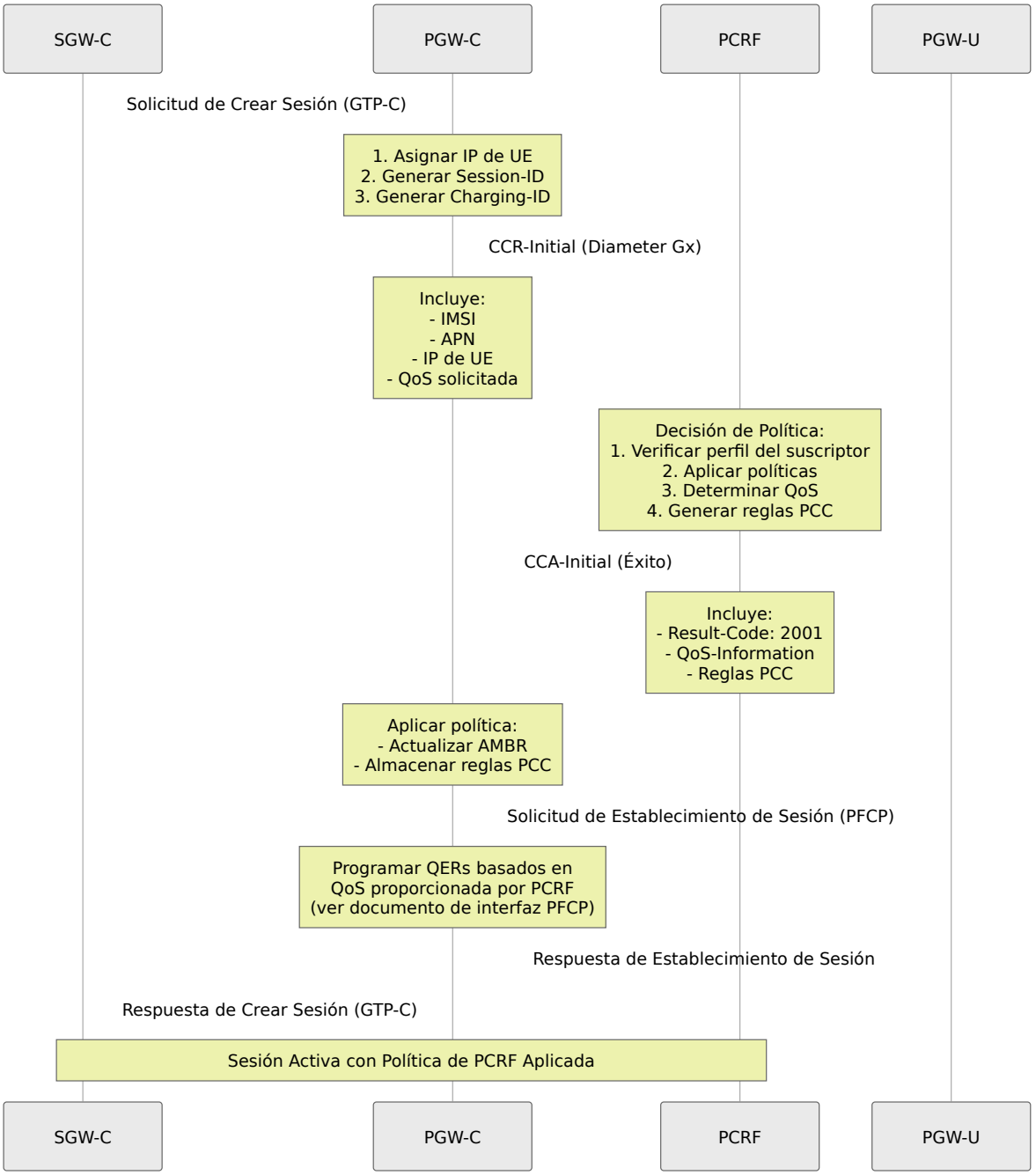
```
# CORRECTO - formato FQDN
host: "pgw_c.epc.mnc999.mcc999.3gppnetwork.org"

# INCORRECTO - No es una Identidad Diameter válida
host: "pgw_c"
host: "10.0.0.20"  # No se permiten direcciones IP
```

Formato de Reino:

- Debe ser un nombre de dominio válido
- Generalmente coincide con el formato PLMN de 3GPP: `epc.mncXXX.mccYYY.3gppnetwork.org`

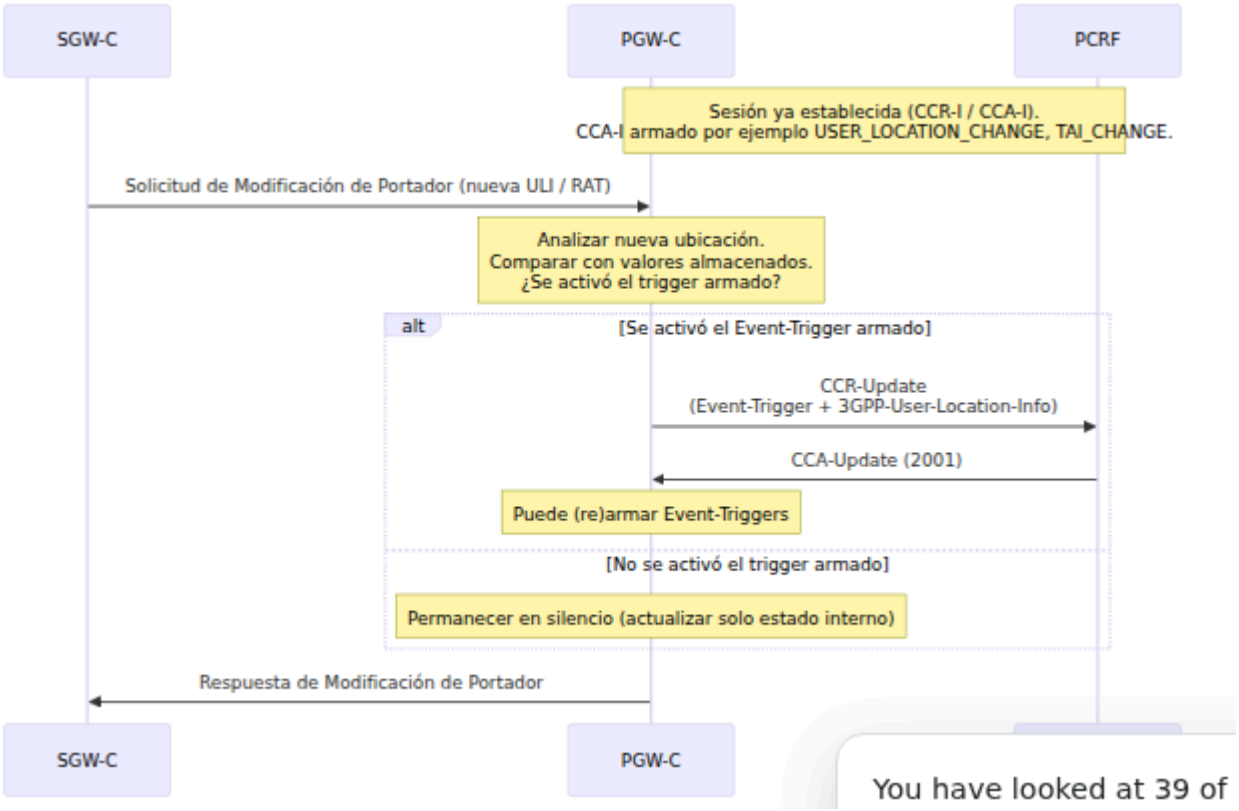
Flujos de Mensajes

Establecimiento Exitoso de Sesión

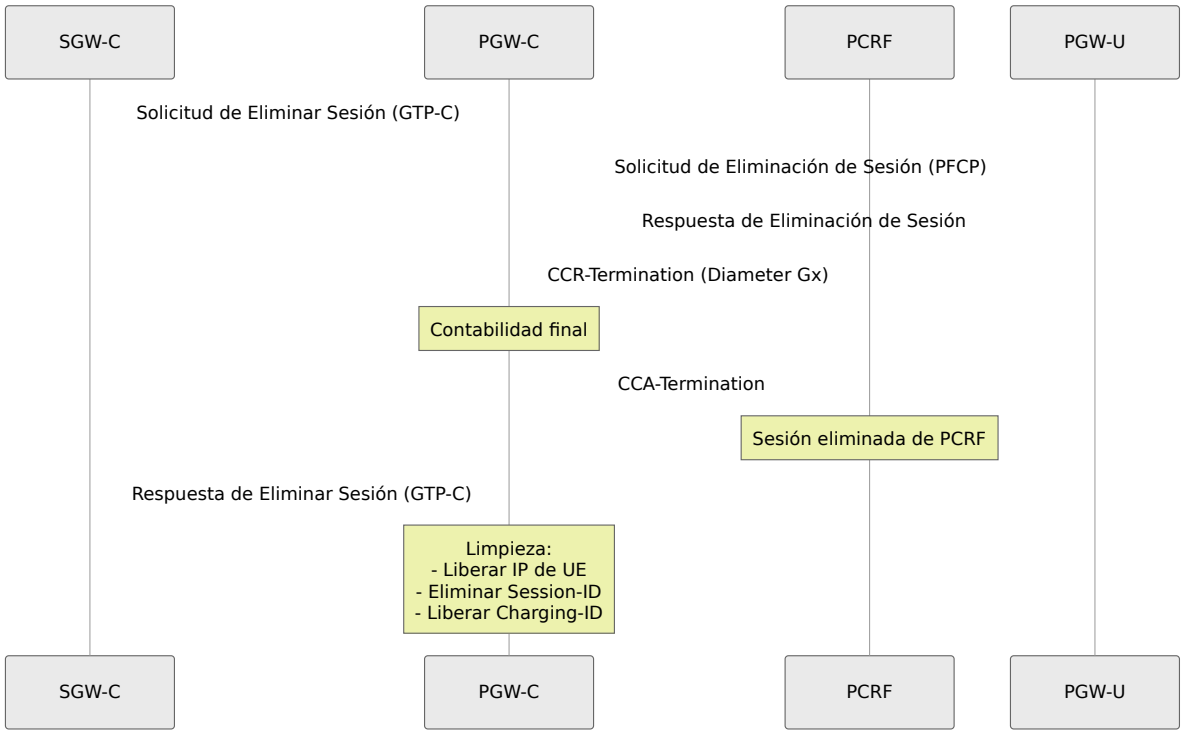


Nota: Los parámetros de QoS de PCRF se traducen en QERs (Reglas de Aplicación de QoS) y se programan en PGW-U a través de PFCP. Ver Interfaz PFCP para detalles de QER.

Actualización de Política (Iniciada por la Red)



Terminación de Sesión



Manejo de Errores

Códigos de Resultado

PGW-C maneja varios códigos de resultado de Diameter en mensajes CCA:

Códigos de Éxito:

Código	Nombre	Acción
2001	DIAMETER_SUCCESS	Continuar el establecimiento de la sesión

Fallos Permanentes (5xxx):

Código	Nombre	Acción de PGW-C
5002	DIAMETER_UNKNOWN_SESSION_ID	Registrar error, fallar sesión
5030	DIAMETER_USER_UNKNOWN	Rechazar sesión (Usuario Desconocido)
5140	DIAMETER_ERROR_INITIAL_PARAMETERS	Registrar error, reintentar o fallar
5003	DIAMETER_AUTHORIZATION_REJECTED	Rechazar sesión (No Autorizado)

Fallos Transitorios (4xxx):

Código	Nombre	Acción de PGW-C
4001	DIAMETER_AUTHENTICATION_REJECTED	Reintentar o fallar sesión
4010	DIAMETER_TOO_BUSY	Reintentar con retroceso
4012	DIAMETER_UNABLE_TO_COMPLY	Registrar error, puede reintentar

Códigos de Resultado Experimentales

Códigos de error específicos del vendedor:

```
Experimental-Result (Agrupado)
├── Vendor-Id: 10415 (3GPP)
└── Experimental-Result-Code: <código específico del vendedor>
```

Códigos Experimentales Comunes de 3GPP:

Código	Nombre	Significado
5065	IP_CAN_SESSION_NOT_AVAILABLE	PCRF no puede establecer sesión
5143	INVALID_SERVICE_INFORMATION	Datos de servicio inválidos

Manejo de Tiempos de Espera

Tiempo de Espera de CCR-I:

Si la PCRF no responde a CCR-Initial dentro del tiempo de espera:

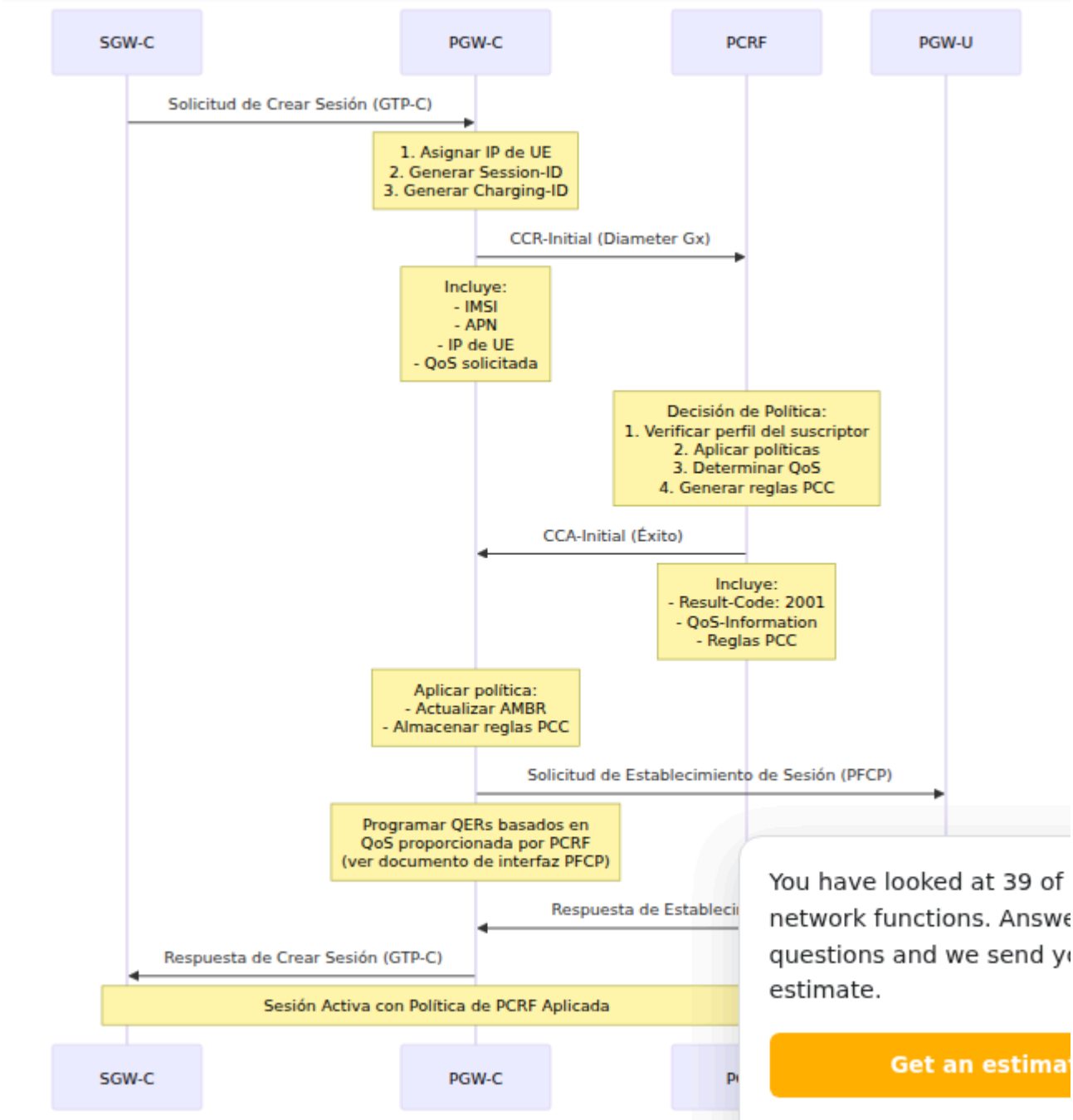
```
1. PGW-C espera el tiempo de espera configurado (por ejemplo, 5
segundos)
2. Si no se recibe CCA:
   - Registrar: "Tiempo de espera de CCR-Initial para Session-ID:
..."
   - Responder a SGW-C con causa de error
   - Limpiar recursos asignados
3. SGW-C recibe: Respuesta de Crear Sesión (Causa: Par Remoto No
Respondiendo)
```

Respuesta de Error a SGW-C:

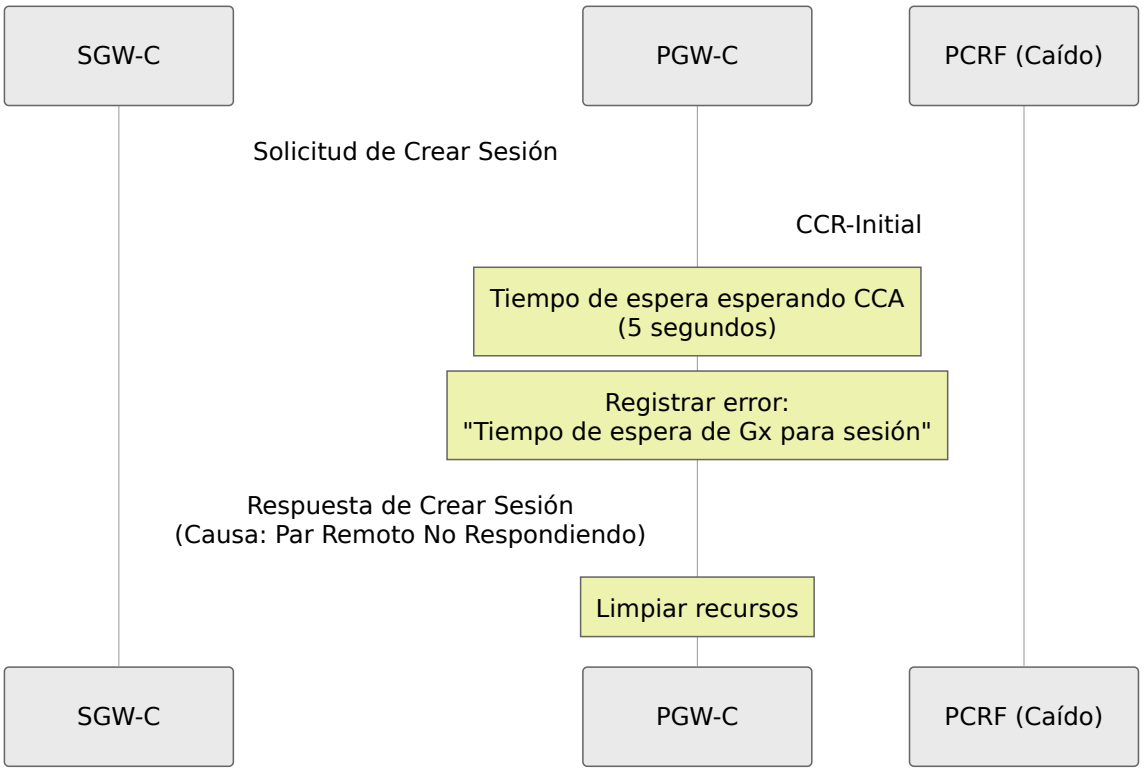
Cuando el CCR-Initial se agota, el PGW-C envía una Respuesta de Crear Sesión con el código de causa `:remote_peer_not_responding` al SGW-C.

Escenarios de Fallo

Escenario 1: PCRF Rechaza la Sesión (Usuario Desconocido)



Escenario 2: PCRF Temporalmente No Disponible



Solución de Problemas

Problemas Comunes

1. Falla de Conexión con el Par Diameter

Síntomas:

- Registro: "Par Diameter no conectado"
- No se envió CCR-Initial

Causas Posibles:

- PCRF no accesible
- IP de PCRF incorrecta en la configuración
- Cortafuegos bloqueando el puerto Diameter (3868)
- Identidades Diameter incorrectas (host/reino)

Resolución:

```
# Probar conectividad de red
ping <pcrf_ip>

# Probar puerto Diameter (TCP 3868)
telnet <pcrf_ip> 3868

# Verificar configuración de identidad Diameter
# Asegurarse de que host y reino sean FQDNs, no IPs
```

Verificar Configuración:

```
config :pgw_c,
  diameter: %{
    # Debe ser FQDN, no IP
    host: "pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.0.30"
      }
    ]
  }
```

2. Tiempos de Espera de CCR-Initial

Síntomas:

- Falla la Solicitud de Crear Sesión
- Registro: "Tiempo de espera de CCR-Initial"

Causas Posibles:

- PCRF sobrecargado
- Latencia de red
- PCRF no respondiendo a este Session-ID

Resolución:

1. Verificar registros de PCRF en busca de errores
2. Verificar que PCRF esté procesando solicitudes
3. Verificar latencia de red: `ping <pcrf_ip>`
4. Aumentar tiempo de espera si la latencia de red es alta

3. Sesiones Rechazadas por PCRF

Síntomas:

- CCA-Initial con Result-Code != 2001
- Falla la Respuesta de Crear Sesión

Códigos de Resultado Comunes:

Código de Resultado	Causa Probable	Resolución
5030	IMSI no en la base de datos de suscriptores	Provisionar suscriptor en HSS/SPR
5003	Autorización rechazada	Verificar permisos del suscriptor
4010	PCRF demasiado ocupado	Reintentar o aumentar capacidad de PCRF

Verificar Registros:

```
# Los registros de PGW-C muestran:
[error] Error Diameter Gx: Result-Code 5030
(DIAMETER_USER_UNKNOWN)
[error] IMSI 310260999999999 rechazado por PCRF
```

4. QoS No Aplicado

Síntomas:

- Sesión establecida pero QoS incorrecto

- Las tasas de bits no coinciden con los valores esperados

Pasos de Depuración:

1. **Verificar CCA-Initial:**
    - Verificar que el AVP `QoS-Information` esté presente
    - Verificar los valores de `APN-Aggregate-Max-Bitrate-UL/DL`
2. **Verificar Establecimiento de Sesión PFCP:**
    - Verificar que se haya creado QER con los valores correctos de MBR
    - Verificar registros de PGW-U para la instalación de QER
3. **Verificar Política de PCRF:**
    - Verificar configuración de PCRF
    - Verificar que el perfil del suscriptor incluya QoS correcta

5. Problemas de Enrutamiento Diameter

Síntomas:

- Mensajes Diameter no llegan a PCRF
- Registro: "No hay ruta al Destination-Realm"

Causa:

- Desajuste de reino entre configuración y mensajes

Resolución:

Asegurar consistencia:

```
# Todos deben coincidir
config :pgw_c,
  diameter: %{
    realm: "epc.mnc999.mcc999.3gppnetwork.org",  # Reino de PGW-C
    peer_list: [
      %{
        realm: "epc.mnc999.mcc999.3gppnetwork.org"  # Reino de
PCRF (generalmente el mismo)
      }
    ]
  }
```

En CCR-Initial:

```
Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
```

Monitoreo de la Salud de Gx

Métricas Clave:

```
# Tasas de mensajes Gx
rate(gx_inbound_messages_total{message_type="gx_CCA"}[5m])
rate(gx_outbound_messages_total{message_type="gx_CCR"}[5m])

# Tasas de errores Gx
rate(gx_inbound_errors_total[5m])

# Tasa de éxito de respuestas Gx (nueva métrica)
sum(rate(gx_outbound_responses_total{result_code_class="2xxx"}
[5m])) /
sum(rate(gx_outbound_responses_total[5m])) * 100

# Fallos de respuesta Gx por host de PCRF
rate(gx_outbound_responses_total{result_code_class!="2xxx"}[5m])
by (diameter_host)

# Contador de sesiones Gx
session_id_registry_count

# Duración del manejo de mensajes Gx
histogram_quantile(0.95,
rate(gx_inbound_handling_duration_bucket[5m]))
```

Métricas de Respuesta por Clase de Código de Resultado:

La métrica `gx_outbound_responses_total` proporciona visibilidad detallada sobre las respuestas Diameter enviadas a pares PCRF, categorizadas por:

- **`message_type`**: Tipo de mensaje de respuesta (`gx_RAA`, `gx_CCA`)
- **`result_code_class`**: Categoría de código de resultado (`2xxx`, `3xxx`, `4xxx`, `5xxx`)
- **`diameter_host`**: Par PCRF que recibe la respuesta

Ejemplos de Alertas:

```yaml
# Alerta sobre alta tasa de errores Gx
- alert: GxErrorRateHigh
  expr: rate(gx_inbound_errors_total[5m]) > 0.1
  for: 5m
  annotations:
    summary: "Alta tasa de errores Gx detectada"

# Alerta sobre alta tasa de fallos de respuesta Gx
- alert: GxResponseFailureRate
  expr: |

sum(rate(gx_outbound_responses_total{result_code_class!="2xxx"}
[5m])) /
    sum(rate(gx_outbound_responses_total[5m])) > 0.1
  for: 5m
  annotations:
    summary: "Alta tasa de fallos de respuesta Gx"
    description: "Más del 10% de las respuestas Gx son fallos"

# Alerta sobre rechazo de sesión
- alert: GxSessionRejection
  expr: rate(gx_inbound_errors_total{result_code="5030"}[5m]) >
0.01
  for: 5m
  annotations:
    summary: "PCRF rechazando sesiones (USER_UNKNOWN)"
```

Registro de Depuración

Habilitar registro detallado de Diameter:

```
# config/runtime.exs
config :logger, level: :debug

# O en tiempo de ejecución
iex> Logger.configure(level: :debug)
```

Buscar:

- `[debug] Enviando CCR-Initial para Session-ID: ...`

- `[debug] Recibido CCA-Initial: Result-Code 2001`
- `[error] Error Diameter: ...`

Monitoreo de Pares Diameter

La conectividad Diameter Gx con el PCRF se monitorea a través de la **API OAM REST**. La API se sirve a través de HTTPS/TLS en `https://<host>:8443` con todas las rutas bajo el prefijo `/api`. La documentación interactiva de la API (Swagger UI) está disponible en `https://<host>:8443/api/docs`.

Endpoints de Pares Diameter

```
GET /api/diameter                      # todos los pares
configurados + estado en vivo
GET /api/diameter?status=disconnected # filtrar por estado de
conexión
GET /api/diameter/<origin-host>       # un par por Origin-Host
```

Ejemplo:

```
curl -k https://localhost:8443/api/diameter
```

`GET /api/diameter` devuelve cada par Diameter configurado y su estado de conexión actual. Agregue `?status=connected` o `?status=disconnected` para filtrar por estado de conexión, o agregue el Origin-Host del par a `GET /api/diameter/<origin-host>` para obtener un solo par.

Para cada par se devuelven los siguientes campos:

Campo	Descripción
`host`	Identidad Diameter (Origin-Host) del par
`status`	Estado de conexión (por ejemplo, Conectado / Desconectado / Conectando)
`ip`	Dirección IP del par
`port`	Puerto del par
`transport`	TCP o SCTP
`connection_initiation`	Si OmniPGW inicia (saliente) o acepta (entrante) la conexión
`realm`	Reino Diameter reportado por el par en CEA
`product_name`	Cadena de producto del vendedor reportada por el par en CEA
`application_ids`	IDs de aplicación Diameter negociados en CEA (Gx = 16777238)

Un despliegue saludable muestra todos los pares PCRF configurados como **Conectados**. La pérdida de todos los pares Gx previene la instalación de políticas y bloquea la creación de nuevas sesiones.

Casos de Uso Operacionales

Monitorear Conectividad de PCRF:

```
curl -k https://localhost:8443/api/diameter
```

Verifique que todos los pares PCRF muestren `Conectado`, que `connection_initiation` coincida con la configuración, y que `application_ids`

incluya Gx (16777238).

Solucionar Fallos en la Creación de Sesiones (Problemas de Gx): Cuando las sesiones de usuario fallan con errores de "tiempo de espera de PCRF", consulte el par afectado:

```
curl -k https://localhost:8443/api/diameter/<origin-host>
```

- `status` es `Desconectado` → verifique la conectividad de red, asegúrese de que el PCRF esté en ejecución y confirme que las reglas del cortafuegos permitan TCP 3868.
- `status` es `Conectado` pero las sesiones aún fallan → el problema está a nivel de aplicación (verifique los registros); el PCRF puede estar rechazando suscriptores.

Verificar Configuración de Diameter: Después de configurar un nuevo par PCRF, confirme que aparezca y alcance `Conectado`:

```
curl -k https://localhost:8443/api/diameter/<origin-host>
```

Verifique que `realm` coincida con la configuración, que `application_ids` incluya Gx, y que `product_name` muestra el identificador esperado del PCRF.

Monitorear Failover: Cuando un PCRF primario falla, `GET /api/diameter?status=disconnected` lo lista como `Desconectado` mientras que el PCRF de respaldo permanece `Conectado`. Nuevas sesiones utilizan automáticamente el respaldo; cuando el primario se recupera su `status` vuelve a `Conectado`.

Detectar Problemas de Enrutamiento Diameter:

- El par muestra `Conectado` pero `realm` es incorrecto
- `application_ids` no incluye Gx (16777238)
- `product_name` no coincide con el esperado del PCRF

Identificar Desajustes de Configuración: Si `connection_initiation` informa que el par inicia mientras que la configuraci��n establece

`initiate_connection: true`, ambos extremos están intentando iniciar, lo que puede causar condiciones de carrera de conexión.

Integración con Métricas

La API OAM proporciona el estado de los pares en tiempo real; combínelo con Prometheus para:

- Tasas de errores históricos de Gx
- Contadores de mensajes CCR/CCA
- Tendencias de latencia

`GET /api/diameter` responde "¿Está funcionando ahora mismo?"; las métricas responden "¿Cómo ha estado funcionando a lo largo del tiempo?"

Documentación Relacionada

Configuración y Política

- **Guía de Configuración** - Configuración de Diameter, configuración de pares PCRF
- **Interfaz PFCP** - Aplicación de QoS a través de QERs de reglas PCC
- **Gestión de Sesiones** - Ciclo de vida de la sesión con integración de políticas
- **Gestión de QoS y Portadores** - Configuración detallada de QoS y configuración de portadores

Integración de Cargos

- **Interfaz Diameter Gy** - Cargos en línea activados por reglas PCC
- **Formato de CDR de Datos** - Registros de cargos fuera de línea con información de políticas
- **Configuración de PCO** - Entrega de P-CSCF para control de políticas IMS

Operaciones

- **Guía de Monitoreo** - Métricas de Gx, seguimiento de políticas, alertas de conectividad de PCRF
- **Interfaz S5/S8** - Integración de gestión de portadores con políticas

---

Volver a la Guía de Operaciones

Carga en Línea de Diámetro (Interfaz Gy/Ro)

Interfaz del Sistema de Carga en Línea (OCS)

Tabla de Contenidos

1. Descripción General
2. Arquitectura de Carga 3GPP
3. Fundamentos de la Interfaz Gy/Ro
4. Mensajes de Control de Crédito
5. Flujos de Carga en Línea
6. Control de Carga de Portadora
7. Control de Crédito para Múltiples Servicios
8. Configuración
9. Flujos de Mensajes
10. Manejo de Errores
11. Integración con Gx
12. Solución de Problemas

Descripción General

La **interfaz Gy** (también llamada **interfaz Ro** en contextos IMS) conecta PGW-C al **Sistema de Carga en Línea (OCS)** para el control de crédito en tiempo real. Esto permite:

- **Carga Prepagada** - Autorización y deducción de crédito en tiempo real

- **Control de Crédito en Tiempo Real** - Otorgar cuota antes de la entrega del servicio
- **Carga Basada en Servicios** - Diferente carga para voz, datos, SMS, etc.
- **Actualizaciones Inmediatas de Cuenta** - Actualizaciones del saldo de crédito en tiempo real
- **Negación de Servicio** - Bloquear el servicio cuando el crédito se agota

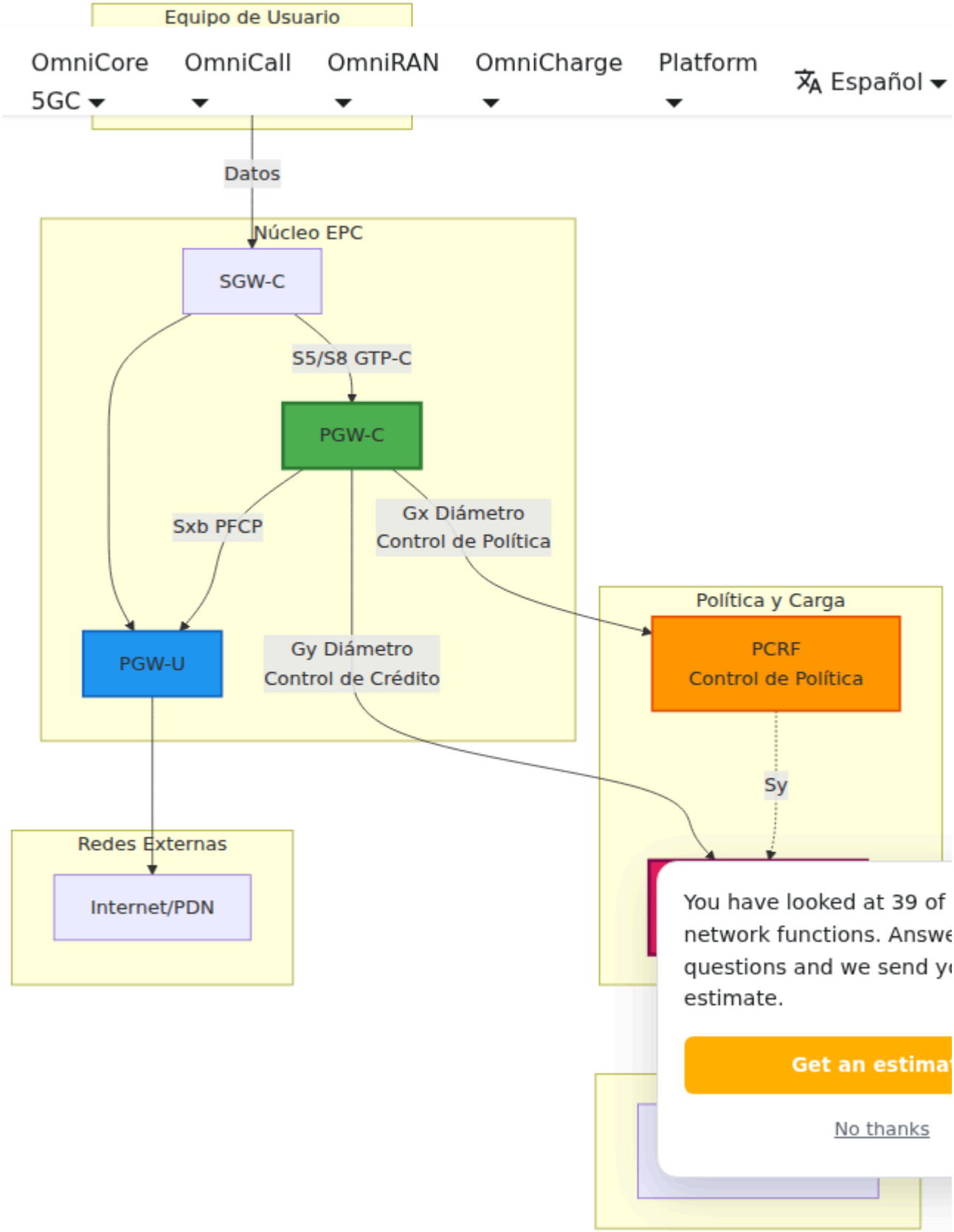
Carga en Línea vs. Carga Fuera de Línea

Aspecto	Carga en Línea (Gy/Ro)	Carga Fuera de Línea (Gz/Rf)
Tiempo	En tiempo real, antes del servicio	Después de la entrega del servicio
Caso de Uso	Suscriptores prepagados	Suscriptores postpagados
Verificación de Crédito	Sí, antes de otorgar el servicio	No, la factura se genera más tarde
Sistema	OCS (Sistema de Carga en Línea)	CGF/CDF (Función de Datos de Carga)
Riesgo	Sin pérdida de ingresos	Riesgo de facturas impagas
Complejidad	Alta (requisitos en tiempo real)	Menor (procesamiento por lotes)
Impacto en el Usuario	Servicio denegado si no hay crédito	Servicio siempre disponible

Véase también: Formato de CDR de Datos para registros de carga fuera de línea (facturación postpagada)

Véase también: Gestión de Sesiones para el ciclo de vida completo de la sesión PDN, incluida la integración de carga

Gy en la Arquitectura de la Red

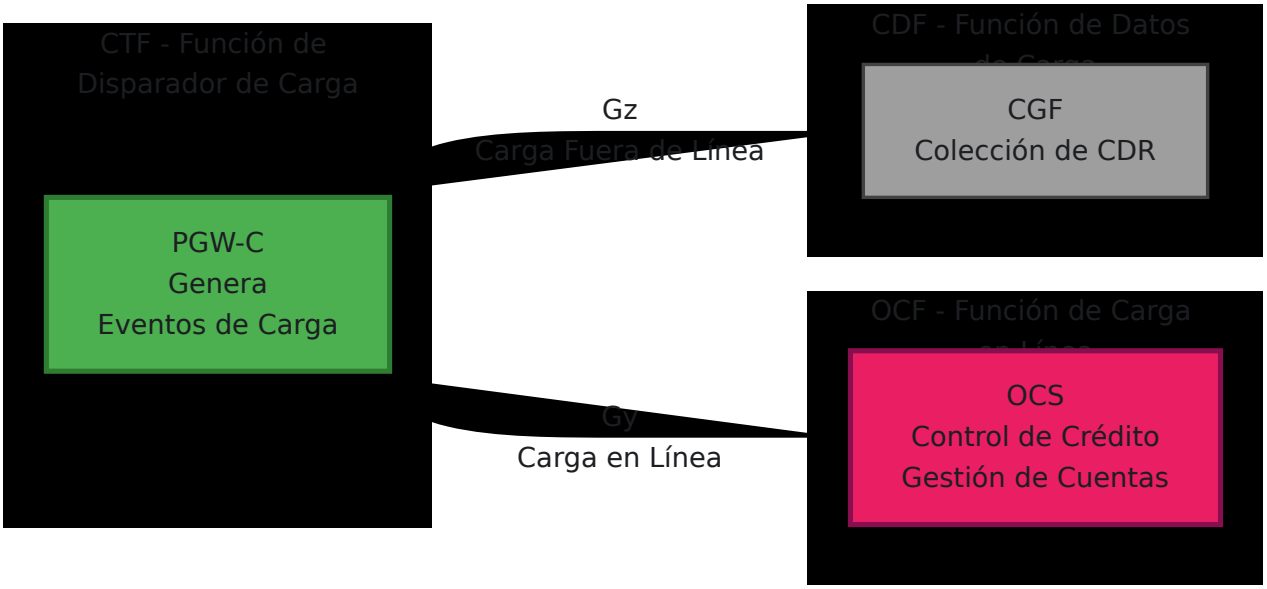


Funciones Clave

Función	Descripción
Autorización de Crédito	Solicitar cuota al OCS antes de permitir tráfico
Gestión de Cuota	Rastrear unidades otorgadas (bytes, tiempo, eventos)
Detección de Agotamiento de Crédito	Monitorear cuota restante
Re-autorización	Solicitar cuota adicional cuando se alcanza el umbral
Terminación de Servicio	Detener el servicio cuando el crédito se agota
Liquidación Final	Reportar uso real al finalizar la sesión

Arquitectura de Carga 3GPP

Puntos de Referencia de Carga



Función de Disparador de Carga (CTF)

PGW-C actúa como un **CTF (Función de Disparador de Carga)**, responsable de:

1. **Detectar eventos cobrables** - Inicio de sesión, uso de datos, fin de sesión
2. **Solicitar autorización de crédito** - Antes de permitir el servicio
3. **Rastrear el consumo de cuota** - Monitorear unidades otorgadas
4. **Generar eventos de carga** - Disparar solicitudes de crédito
5. **Hacer cumplir el control de crédito** - Bloquear tráfico cuando la cuota se agota

Función de Carga en Línea (OCF)

El OCS implementa la **OCF (Función de Carga en Línea)**:

1. **Gestión del saldo de cuenta** - Rastrear el crédito del suscriptor
2. **Tarificación** - Determinar el precio por unidad (por MB, por segundo, etc.)

3. **Reserva de crédito** - Reservar crédito para la cuota otorgada
4. **Deducción de crédito** - Deducir al informar el uso
5. **Decisiones de política** - Otorgar o denegar según el saldo

---

Fundamentos de la Interfaz Gy/Ro

Referencia 3GPP

- **Especificación:** 3GPP TS 32.299 (Arquitectura de carga)
- **Protocolo:** 3GPP TS 32.251 (Carga del dominio PS)
- **ID de Aplicación de Diámetro:** 4 (Gy/Ro - Aplicación de Control de Crédito)
- **Protocolo Base:** RFC 4006 (Aplicación de Control de Crédito de Diámetro)

Concepto de Sesión

Cada conexión PDN de UE que requiere carga en línea tiene una **sesión Gy/Ro** identificada por un **Session-ID**. Esta sesión:

- Se crea cuando la portadora requiere carga en línea (CCR-Initial)
- Se actualiza cuando se consume cuota (CCR-Update)
- Se termina cuando la sesión finaliza (CCR-Termination)

Formato del ID de Sesión

```
Session-ID: <Origin-Host>;<high32>;<low32>[;<optional>]
Ejemplo: omni-
pgw_c.epc.mnc999.mcc999.3gppnetwork.org;9876543210;12345;gy
```

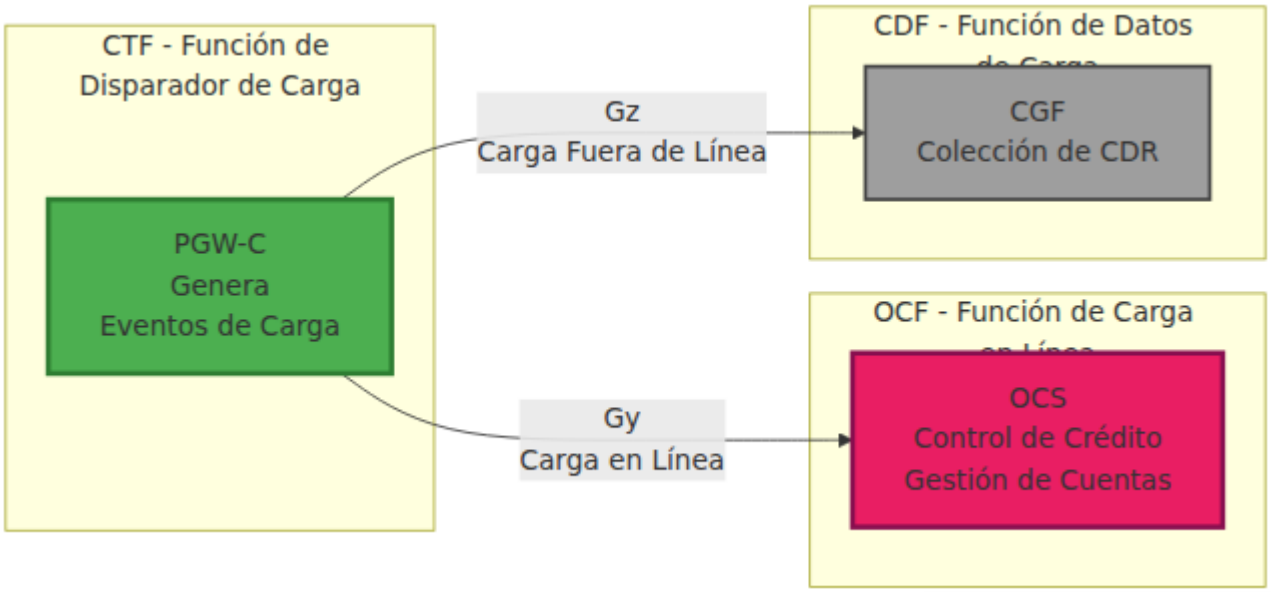
Componentes:

- **Origin-Host:** Identidad de Diámetro del PGW-C
- **high32:** 32 bits altos del identificador único

- **low32:** 32 bits bajos del identificador único
- **optional:** Identificador adicional (por ejemplo, "gy" para distinguir de Gx)

Mensajes de Control de Crédito

Tipos de Mensajes



CCR-Initial (Solicitud de Control de Crédito - Inicial)

Cuándo: UE crea una conexión PDN y la portadora requiere carga en línea

Propósito:

- Solicitar autorización de crédito inicial al OCS
- Reservar cuota para la entrega del servicio
- Establecer sesión Gy/Ro

AVPs Clave Enviados por PGW-C:

Nombre de AVP	Código de AVP	Tipo	Descripción
Session-Id	263	UTF8String	Identificador único de sesión Gy
Auth-Application-Id	258	Unsigned32	4 (Control de Crédito)
Origin-Host	264	DiamIdent	Identidad de Diámetro del PGW-C
Origin-Realm	296	DiamIdent	Reino de Diámetro del PGW-C
Destination-Realm	283	DiamIdent	Reino del OCS
CC-Request-Type	416	Enumerated	1 = INITIAL_REQUEST
CC-Request-Number	415	Unsigned32	Número de secuencia (comienza en 0)
Subscription-Id	443	Grouped	Identificador de UE (IMSI/MSISDN)
Service-Context-Id	461	UTF8String	Identificador del contexto de carga
Multiple-Services-Credit-Control	456	Grouped	Solicitudes de crédito específicas del servicio
Requested-Service-Unit	437	Grouped	Cuota solicitada (bytes, tiempo, etc.)
Used-Service-Unit	446	Grouped	Cuota utilizada (0 para inicial)

Nombre de AVP	Código de AVP	Tipo	Descripción
Service-Identifier	439	Unsigned32	Identificador del tipo de servicio
Rating-Group	432	Unsigned32	Identificador de la categoría de carga

Ejemplo de Estructura CCR-I:

```
CCR (Código de Comando: 272, Solicitud)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Auth-Application-Id: 4
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: INITIAL_REQUEST (1)
├── CC-Request-Number: 0
├── Subscription-Id (Grouped)
│   ├── Subscription-Id-Type: END_USER_IMSI (1)
│   └── Subscription-Id-Data: "310260123456789"
├── Subscription-Id (Grouped)
│   ├── Subscription-Id-Type: END_USER_E164 (0)
│   └── Subscription-Id-Data: "15551234567"
├── Service-Context-Id: "32251@3gpp.org"
├── Multiple-Services-Credit-Control (Grouped)
│   ├── Service-Identifier: 1
│   ├── Rating-Group: 100
│   └── Requested-Service-Unit (Grouped)
│       └── CC-Total-Octets: 10000000 (solicitud de 10 MB)
└── Used-Service-Unit (Grouped)
    └── CC-Total-Octets: 0 (sin uso aún)
```

CCA-Initial (Respuesta de Control de Crédito - Inicial)

Enviado por: OCS en respuesta a CCR-I

Propósito:

- Otorgar o denegar autorización de crédito
- Proporcionar cuota para la entrega del servicio
- Especificar parámetros de tarificación y carga

AVPs Clave Recibidos por PGW-C:

Nombre de AVP	Código de AVP	Descripción
Result-Code	268	Éxito (2001) o código de error
Multiple-Services-Credit-Control	456	Concesiones de crédito específicas del servicio
Granted-Service-Unit	431	Cuota otorgada (bytes, tiempo, etc.)
Validity-Time	448	Período de validez de la cuota (segundos)
Result-Code	268	Código de resultado por servicio
Final-Unit-Indication	430	Acción cuando la cuota se agota
Volume-Quota-Threshold	-	Umbral para re-autorización

Ejemplo de Respuesta de Éxito:

```
CCA (Código de Comando: 272, Respuesta)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Result-Code: DIAMETER_SUCCESS (2001)
├── Origin-Host: "ocs.example.com"
├── Origin-Realm: "example.com"
├── Auth-Application-Id: 4
├── CC-Request-Type: INITIAL_REQUEST (1)
├── CC-Request-Number: 0
└── Multiple-Services-Credit-Control (Grouped)
    ├── Result-Code: DIAMETER_SUCCESS (2001)
    ├── Service-Identifier: 1
    ├── Rating-Group: 100
    ├── Granted-Service-Unit (Grouped)
    │   └── CC-Total-Octets: 10000000 (otorgados 10 MB)
    ├── Validity-Time: 3600 (cuota válida por 1 hora)
    └── Volume-Quota-Threshold: 8000000 (re-autorización a 8 MB
usados, 80%)
```

CCR-Update (Solicitud de Control de Crédito - Actualización)

Cuándo:

- Se alcanza el umbral de cuota otorgada (por ejemplo, 80% consumido)
- Expira el tiempo de validez
- Un cambio de servicio requiere re-autorización
- Cambio de tiempo de tarifa

Propósito:

- Solicitar cuota adicional
- Informar uso de la cuota previamente otorgada
- Actualizar parámetros de carga

Diferencias Clave respecto a CCR-I:

- `CC-Request-Type: UPDATE_REQUEST (2)`
- `CC-Request-Number` incrementado

- `Used-Service-Unit` contiene el uso real
- `Requested-Service-Unit` para más cuota

Ejemplo de Estructura CCR-U:

```
CCR (Código de Comando: 272, Solicitud)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Auth-Application-Id: 4
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: UPDATE_REQUEST (2)
├── CC-Request-Number: 1
└── Multiple-Services-Credit-Control (Grouped)
    ├── Service-Identifier: 1
    ├── Rating-Group: 100
    ├── Used-Service-Unit (Grouped)
    │   └── CC-Total-Octets: 8000000 (8 MB usados hasta ahora)
    └── Requested-Service-Unit (Grouped)
        └── CC-Total-Octets: 10000000 (solicitud de otros 10 MB)
```

CCA-Update (Respuesta de Control de Crédito - Actualización)

Enviado por: OCS en respuesta a CCR-U

Propósito:

- Otorgar cuota adicional (si hay crédito disponible)
- Reconocer el uso
- Actualizar parámetros de carga

Resultados Posibles:

1. Más Cuota Otorgada:

```
CCA (Actualización)
└── Multiple-Services-Credit-Control
    ├── Result-Code: DIAMETER_SUCCESS (2001)
    ├── Granted-Service-Unit
    │   └── CC-Total-Octets: 10000000 (otros 10 MB)
    └── Validity-Time: 3600
```

2. Cuota Final (Crédito Agotado):

```
CCA (Actualización)
└── Multiple-Services-Credit-Control
    ├── Result-Code: DIAMETER_SUCCESS (2001)
    ├── Granted-Service-Unit
    │   └── CC-Total-Octets: 1000000 (solo 1 MB restante)
    └── Final-Unit-Indication
        └── Final-Unit-Action: TERMINATE (0)
```

3. Sin Crédito Disponible:

```
CCA (Actualización)
├── Result-Code: DIAMETER_CREDIT_LIMIT_REACHED (4012)
└── Multiple-Services-Credit-Control
    ├── Result-Code: DIAMETER_CREDIT_LIMIT_REACHED (4012)
    └── Final-Unit-Indication
        └── Final-Unit-Action: TERMINATE (0)
```

CCR-Termination (Solicitud de Control de Crédito - Terminación)

Cuándo:

- UE se desconecta
- Conexión PDN eliminada
- Sesión terminada por cualquier motivo

Propósito:

- Informe final de uso
- Cerrar sesión Gy/Ro
- Liquidación final

Diferencias Clave:

- `CC-Request-Type: TERMINATION_REQUEST (3)`
- `Used-Service-Unit` contiene el uso final
- No hay `Requested-Service-Unit` (no se necesita más cuota)
- Incluye `Termination-Cause`

Ejemplo de Estructura CCR-T:

```
CCR (Código de Comando: 272, Solicitud)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Auth-Application-Id: 4
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: TERMINATION_REQUEST (3)
├── CC-Request-Number: 5
├── Termination-Cause: DIAMETER_LOGOUT (1)
└── Multiple-Services-Credit-Control (Grouped)
    ├── Service-Identifier: 1
    ├── Rating-Group: 100
    └── Used-Service-Unit (Grouped)
        └── CC-Total-Octets: 18500000 (18.5 MB de uso total)
```

CCA-Termination (Respuesta de Control de Crédito - Terminación)

Enviado por: OCS en respuesta a CCR-T

Propósito:

- Reconocer la terminación de la sesión
- Completar la contabilidad
- Liberar el crédito reservado

Ejemplo de CCA-T:

```
CCA (Código de Comando: 272, Respuesta)
├─ Session-Id: "pgw_c.example.com;123;456;gy"
├── Result-Code: DIAMETER_SUCCESS (2001)
├── Origin-Host: "ocs.example.com"
├── Origin-Realm: "example.com"
├── Auth-Application-Id: 4
├── CC-Request-Type: TERMINATION_REQUEST (3)
└── CC-Request-Number: 5
```

Flujos de Carga en Línea

Tipos de Unidades de Servicio

El OCS puede otorgar cuota en diferentes unidades:

Tipo de Unidad	AVP	Descripción	Caso de Uso
Tiempo	CC-Time	Segundos	Llamadas de voz, duración de sesión
Volumen	CC-Total-Octets	Bytes (total sube+baja)	Servicios de datos
Volumen (separado)	CC-Input-Octets, CC-Output-Octets	Bytes (separados)	Carga asimétrica
Específico del Servicio	CC-Service-Specific-Units	Unidades personalizadas	SMS, MMS, llamadas API
Eventos	-	Eventos contados	Servicios de pago por uso

Gestión del Umbral de Cuota

Problema: ¿Cómo sabe PGW-C cuándo solicitar más cuota?

Solución: OCS proporciona un **Volume-Quota-Threshold** o **Time-Quota-Threshold**. PGW-C monitorea el uso a través de informes de sesión PFCP de PGW-U (ver Interfaz PFCP).

Ejemplo de Flujo:

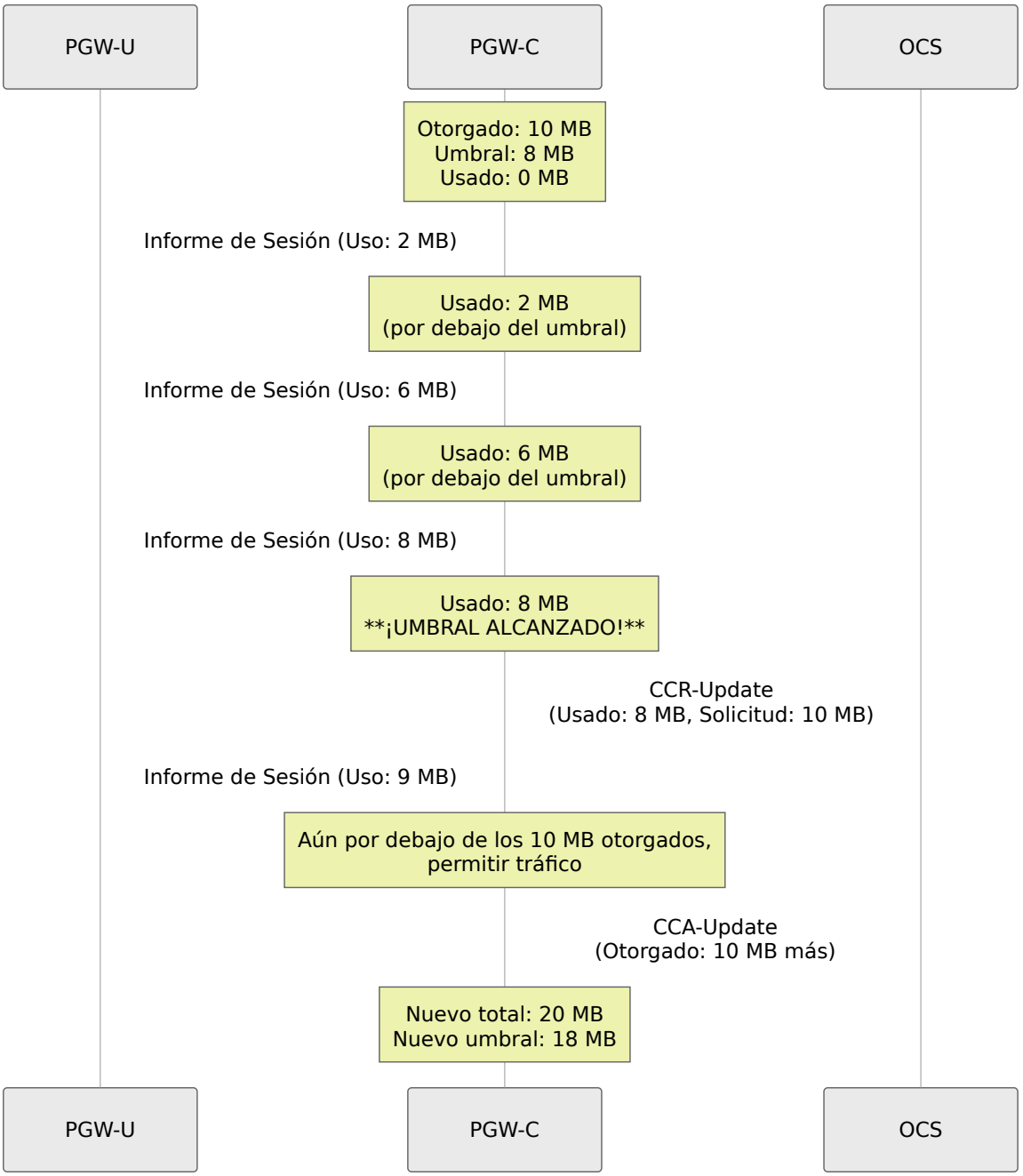
```
1. OCS otorga 10 MB de cuota con umbral del 80% (8 MB)
2. PGW-C monitorea el uso a través de informes de uso de PGW-U
(Informes de Sesión PFCP)
3. Cuando el uso alcanza 8 MB:
   → PGW-C envía CCR-Update
   → Continuar permitiendo tráfico (no esperar respuesta)
4. OCS responde con más cuota
5. Si la cuota se agota antes de enviar CCR-Update:
   → PGW-C debe bloquear el tráfico
```

Cálculo del Umbral:

```
Granted-Service-Unit: 10000000 bytes (10 MB)
Volume-Quota-Threshold: 8000000 bytes (8 MB)

Cuando se consumen 8 MB → Disparar CCR-Update
Buffer restante: 2 MB (permite tiempo para la respuesta de OCS)
```

Monitoreo de PGW-C:

PGW-C monitorea el uso a través de **Informes de Sesión PFCP** de PGW-U:



Indicación de Unidad Final

¿Qué sucede cuando el crédito se agota?

OCS incluye el AVP **Final-Unit-Indication** en CCA para especificar la acción:

Acción de Unidad Final	Valor	Comportamiento de PGW-C
TERMINAR	0	Bloquear todo el tráfico, iniciar la terminación de sesión
REDIRIGIR	1	Redirigir tráfico a portal (por ejemplo, página de recarga)
RESTRINGIR_ACCESO	2	Permitir acceso solo a servicios específicos (por ejemplo, servidor de recarga)

Ejemplo: Unidad Final con Redirección

```
CCA (Actualización)
└── Multiple-Services-Credit-Control
    ├── Result-Code: DIAMETER_SUCCESS (2001)
    ├── Granted-Service-Unit
    │   └── CC-Total-Octets: 1000000 (últimos 1 MB)
    └── Final-Unit-Indication
        ├── Final-Unit-Action: REDIRECT (1)
        └── Redirect-Server (Grouped)
            ├── Redirect-Address-Type: URL (2)
            └── Redirect-Server-Address:
"http://topup.example.com"
```

Acciones de PGW-C:

1. **TERMINAR:** Enviar CCR-T, eliminar portadora
2. **REDIRIGIR:** Instalar regla PFCP para redirigir HTTP a URL de recarga
3. **RESTRINGIR_ACCESO:** Instalar reglas PFCP que permiten solo IPs en lista blanca

---

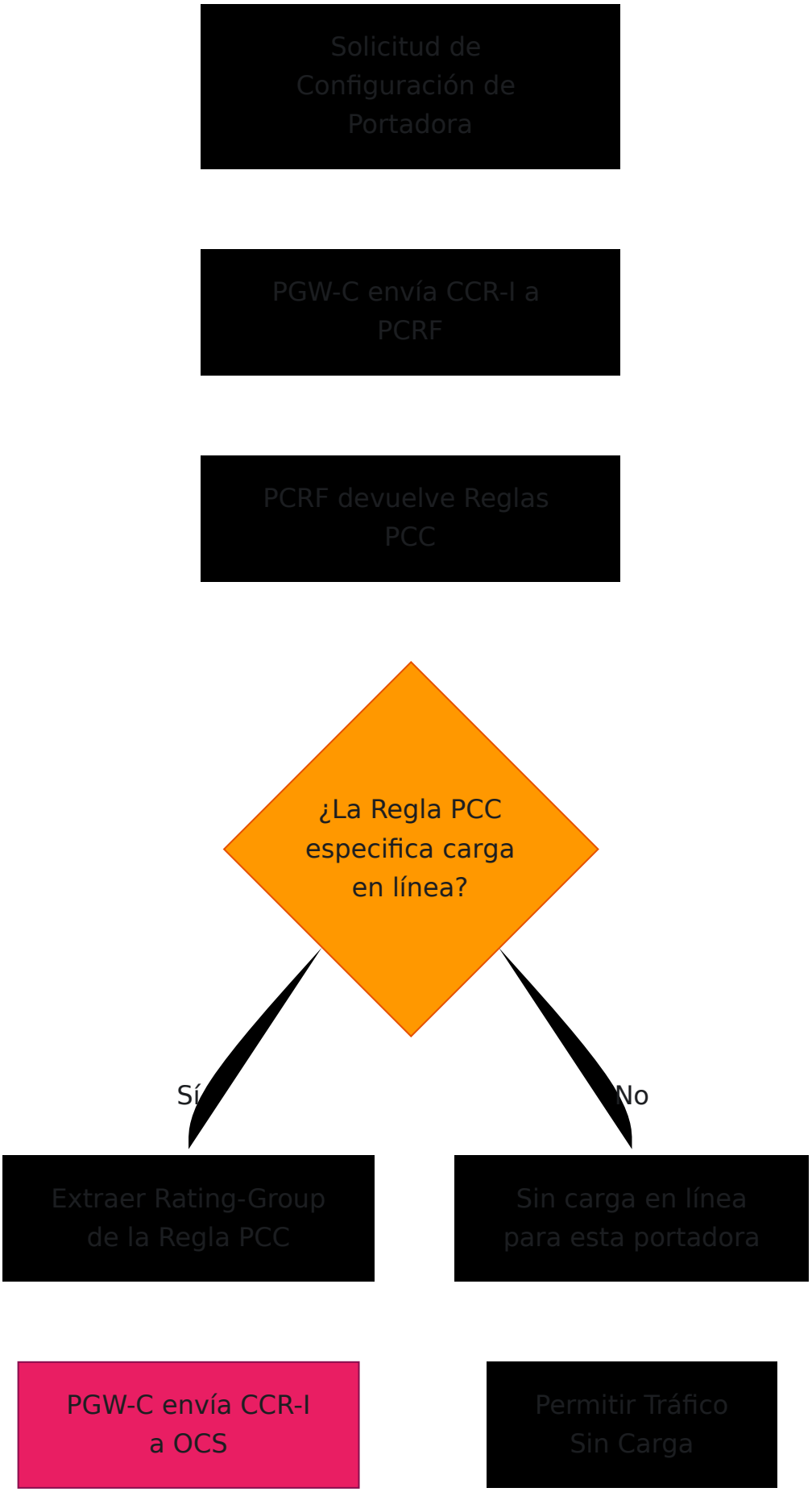
Control de Carga de Portadora

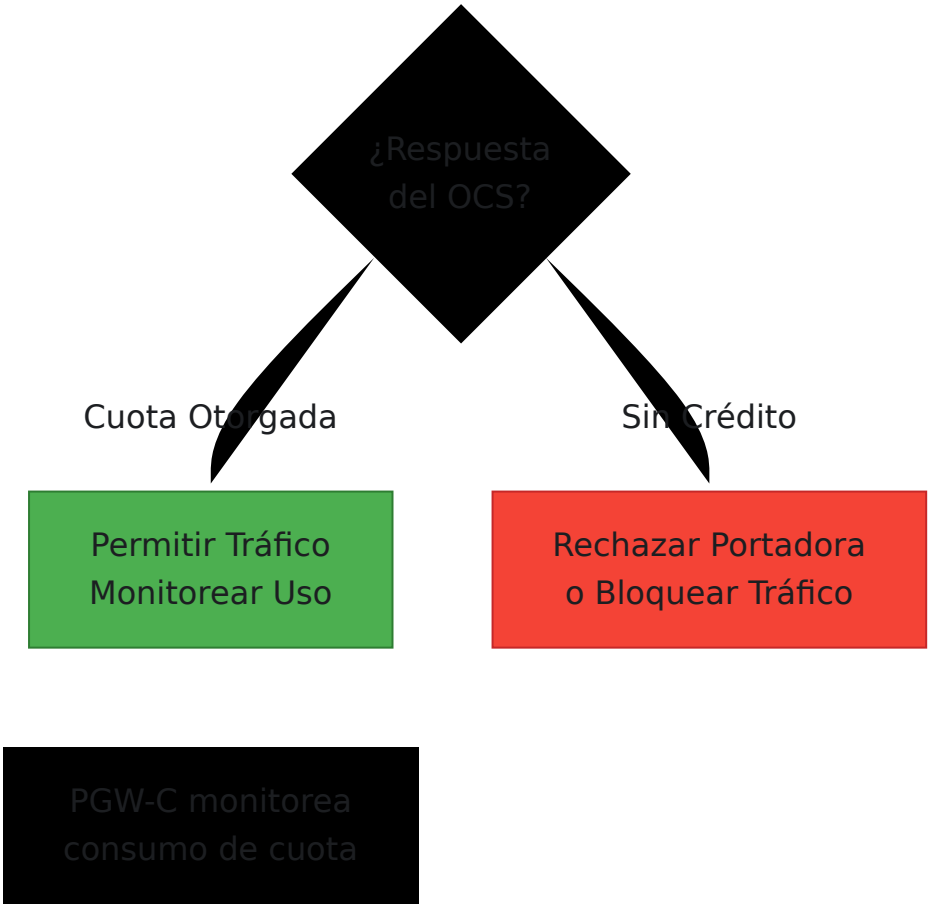
¿Qué Controla si una Portadora es Cobrada?

Especificación 3GPP: TS 23.203, TS 29.212, TS 32.251

La carga de portadora es controlada por **Reglas PCC** provistas por el PCRF a través de la interfaz Gx. Ver Interfaz Gx de Diámetro para la documentación completa de reglas PCC.

Flujo de Decisión de Carga:


Solicitud de Configuración de Portadora
PGW-C envía CCR-I a PCRF
PCRF devuelve Reglas PCC
¿La Regla PCC especifica carga en línea?
Sí
No
Extraer Rating-Group de la Regla PCC
Sin carga en línea para esta portadora
PGW-C envía CCR-I a OCS
Permitir Tráfico Sin Carga



Regla PCC con Información de Carga

Respuesta PCRF (CCA-I en Gx):

```
CCA (Interfaz Gx)
└── Charging-Rule-Definition (Grouped)
    ├── Charging-Rule-Name: "prepaid_data_rule"
    ├── Rating-Group: 100
    ├── Online: 1 (habilitar carga en línea)
    ├── Offline: 0 (deshabilitar carga fuera de línea)
    ├── Metering-Method: VOLUME (1)
    ├── Precedence: 100
    ├── Flow-Information: [...]
    └── QoS-Information: [...]
```

AVPs Clave de Carga en Reglas PCC:

Nombre de AVP	Código de AVP	Valores	Descripción
Rating-Group	432	Unsigned32	Categoría de carga (se mapea a tarifa en OCS)
Online	1009	0=Deshabilitar, 1=Habilitar	Habilitar carga en línea (Gy)
Offline	1008	0=Deshabilitar, 1=Habilitar	Habilitar carga fuera de línea (Gz)
Metering-Method	1007	0=Duración, 1=Volumen, 2=Ambos	Qué medir
Reporting-Level	1011	0=Servicio, 1=Grupo de Tarificación	Granularidad de los informes de uso

Matriz de Decisión de Carga de Portadora

En Línea	Fuera de Línea	Rating-Group	Comportamiento
1	0	Presente	Solo carga en línea (prepago)
0	1	Presente	Solo carga fuera de línea (postpago)
1	1	Presente	Carga tanto en línea como fuera de línea (convergente)
0	0	-	Sin carga (servicio gratuito)

Múltiples Grupos de Calificación

Una única conexión PDN puede tener **múltiples portadores con diferentes grupos de calificación**:

Escenario de Ejemplo:

```
Portador Predeterminado (Internet)
├── Grupo-de-Calificación: 100 (Datos Estándar)
└── En Línea: 1

Portador Dedicado 1 (Streaming de Video)
├── Grupo-de-Calificación: 200 (Servicio de Video)
└── En Línea: 1

Portador Dedicado 2 (Voz IMS)
├── Grupo-de-Calificación: 300 (Voz)
└── En Línea: 1
```

Comportamiento de PGW-C Gy:

- **Un solo CCR-I** con múltiples secciones MSCC (Control de Crédito de Múltiples Servicios):

```
CCR-Inicial
├── Session-Id: "..."
└── Control de Crédito de Múltiples Servicios
    ├── [Grupo-de-Calificación: 100] → Datos Estándar
    ├── [Grupo-de-Calificación: 200] → Servicio de Video
    └── [Grupo-de-Calificación: 300] → Voz
```

Respuesta de OCS:

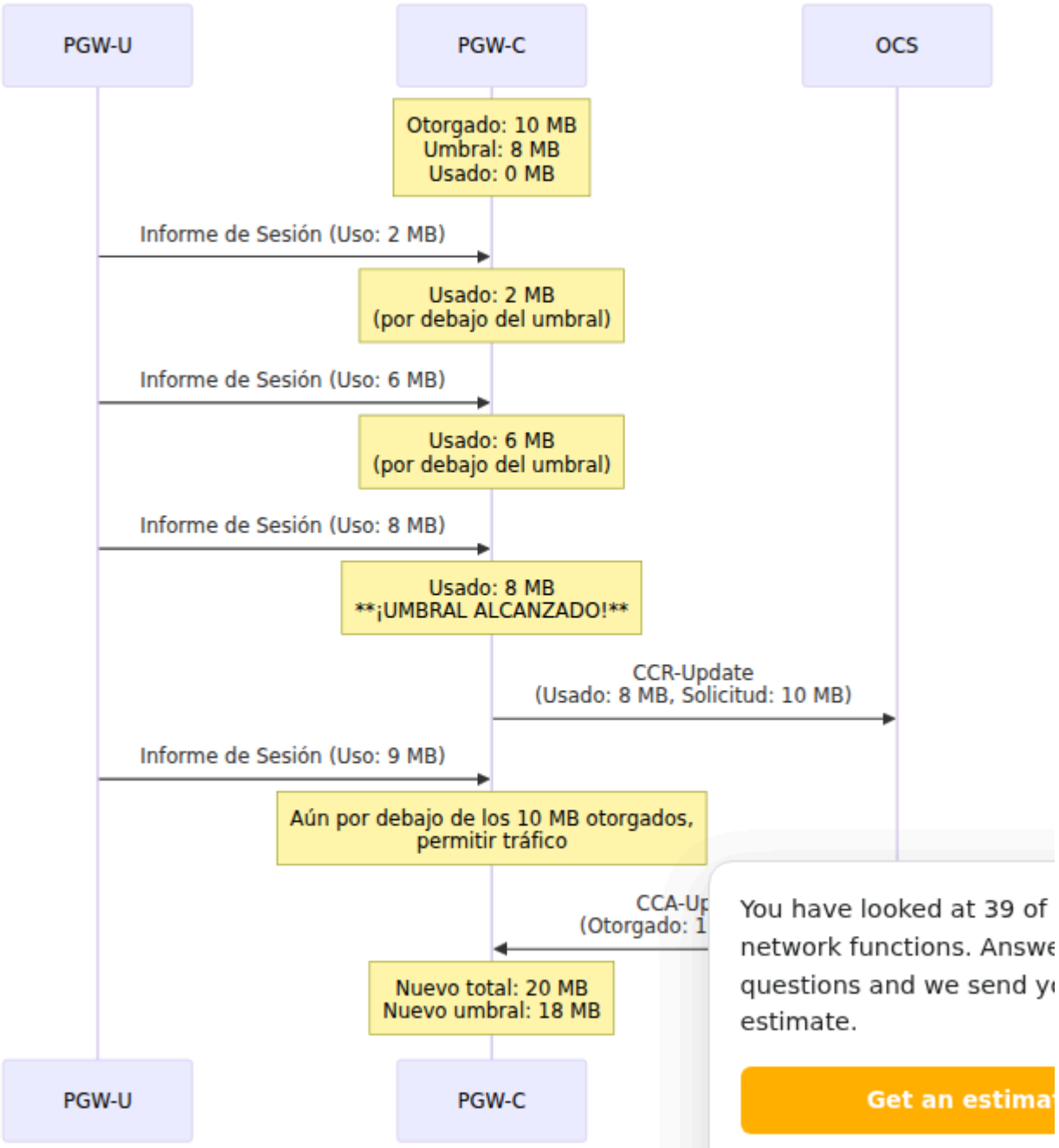
```
CCA-Inicial
└── Control de Crédito de Múltiples Servicios
    ├── [Grupo-de-Calificación: 100] → Concedido: 10 MB
    ├── [Grupo-de-Calificación: 200] → Concedido: 5 MB (video más
caro)
    └── [Grupo-de-Calificación: 300] → Concedido: 60 segundos
```

Aplicación de Cargos por Servicio

PGW-C rastrea la cuota por Grupo de Calificación:

```
# Pseudocódigo
state.charging_quotas = %{
  100 => %{granted: 10_000_000, used: 0, threshold: 8_000_000},
  200 => %{granted: 5_000_000, used: 0, threshold: 4_000_000},
  300 => %{granted: 60_000, used: 0, threshold: 48_000}  #
milisegundos
}
```

Monitoreo de Uso por Portador:



You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima

Control de Crédito de Múltiples Servicios

AVP de MSCC (Control de Crédito de Múltiples Servicios)

Propósito: Agrupar información de cargos para un servicio/grupo de calificación específico

Estructura:

```
Control de Crédito de Múltiples Servicios (Agrupado, AVP 456)
├── Identificador-de-Servicio (Unsigned32, AVP 439)
├── Grupo-de-Calificación (Unsigned32, AVP 432)
├── Unidad-de-Servicio-Solicitada (Agrupado, AVP 437)
│   ├── CC-Tiempo (Unsigned32, AVP 420)
│   ├── CC-Octetos-Totales (Unsigned64, AVP 421)
│   ├── CC-Octetos-Entrada (Unsigned64, AVP 412)
│   └── CC-Octetos-Salida (Unsigned64, AVP 414)
├── Unidad-de-Servicio-Usada (Agrupado, AVP 446)
│   └── [Misma estructura que Unidad-de-Servicio-Solicitada]
├── Unidad-de-Servicio-Concedida (Agrupado, AVP 431)
│   └── [Misma estructura que Unidad-de-Servicio-Solicitada]
├── Tiempo-de-Validez (Unsigned32, AVP 448)
├── Código-de-Resultado (Unsigned32, AVP 268)
└── Indicación-de-Unidad-Final (Agrupado, AVP 430)
    └── Acción-de-Unidad-Final (Enumerado, AVP 449)
```

Identificador-de-Servicio vs. Grupo-de-Calificación

Atributo	Identificador-de-Servicio	Grupo-de-Calificación
Propósito	Identifica el tipo de servicio	Identifica la categoría de cargos
Ejemplo	1=Datos, 2=Voz, 3=SMS	100=Regular, 200=Premium
Granularidad	Clasificación amplia	Tarifa específica
Requerido	Opcional	Requerido para el cobro
Mapeo	Puede mapear a múltiples RGs	Tarifa única en OCS

Ejemplo:

```
Identificador-de-Servicio: 1 (Servicio de Datos)
├── Grupo-de-Calificación: 100 (Datos Estándar - $0.01/MB)
└── Grupo-de-Calificación: 200 (Datos Premium - $0.05/MB)

Identificador-de-Servicio: 2 (Voz)
└── Grupo-de-Calificación: 300 (Llamadas de Voz - $0.10/min)
```

Configuración

Configuración Básica de Gy

Edita `config/runtime.exs`:

```
config :pgw_c,
  gy: %{
    # Habilitar o deshabilitar el cobro en línea globalmente
    enabled: true,

    # Tiempo de espera de conexión OCS (milisegundos)
    timeout_ms: 5000,

    # Solicitud de cuota predeterminada (bytes) si no es
especificada por PCRF
    default_requested_quota: 10_000_000,  # 10 MB

    # Porcentaje de umbral para re-autorización
    # (0.8 = activar CCR-Actualización al 80% de cuota consumida)
    quota_threshold_percentage: 0.8,

    # Acción cuando ocurre un tiempo de espera de OCS
    # Opciones: :block, :allow
    timeout_action: :block,

    # Acción cuando OCS no devuelve crédito
    # Opciones: :terminate, :redirect
    no_credit_action: :terminate,

    # URL de redirección para recarga (usada si no_credit_action:
:redirect)
    topup_redirect_url: "http://topup.example.com"
  },
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",

    # Configuración del par OCS
    peer_list: [
      # PCRF para control de políticas (Gx)
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.0.30",
        initiate_connection: true
      },
      # OCS para cobro en línea (Gy)
```

```
      %{
        host: "ocs.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.0.40",
        initiate_connection: true
      }
    ]
  }
```

Parámetros de Configuración Explicados

`enabled`

- `true`: Cobro en línea activo, mensajes CCR enviados a OCS
- `false`: Cobro en línea deshabilitado, no hay mensajes Gy

`timeout_ms`

- Tiempo de espera para la respuesta CCA de OCS
- Recomendado: 3000-5000 ms

`default_requested_quota`

- Cuota predeterminada a solicitar si PCRF no especifica
- Valores típicos: 1-100 MB

`quota_threshold_percentage`

- Activar CCR-Actualización cuando este % de cuota consumida
- Recomendado: 0.75-0.85 (75%-85%)
- Mayor = menos mensajes, pero riesgo de agotamiento de cuota
- Menor = más mensajes, pero más seguro

`timeout_action`

- **`:block`** - Bloquear tráfico si OCS no responde (más seguro, previene pérdida de ingresos)
- **`:allow`** - Permitir tráfico si OCS no responde (mejor UX, riesgo de ingresos)

`no_credit_action`

- `:terminate` - Eliminar portador cuando se agota el crédito
- `:redirect` - Redirigir a portal de recarga

Configuración Específica del Entorno

Producción (suscriptores de prepago):

```
config :pgw_c,
  gy: %{
    enabled: true,
    timeout_action: :block,
    no_credit_action: :terminate,
    quota_threshold_percentage: 0.8
  }
```

Prueba/Desarrollo:

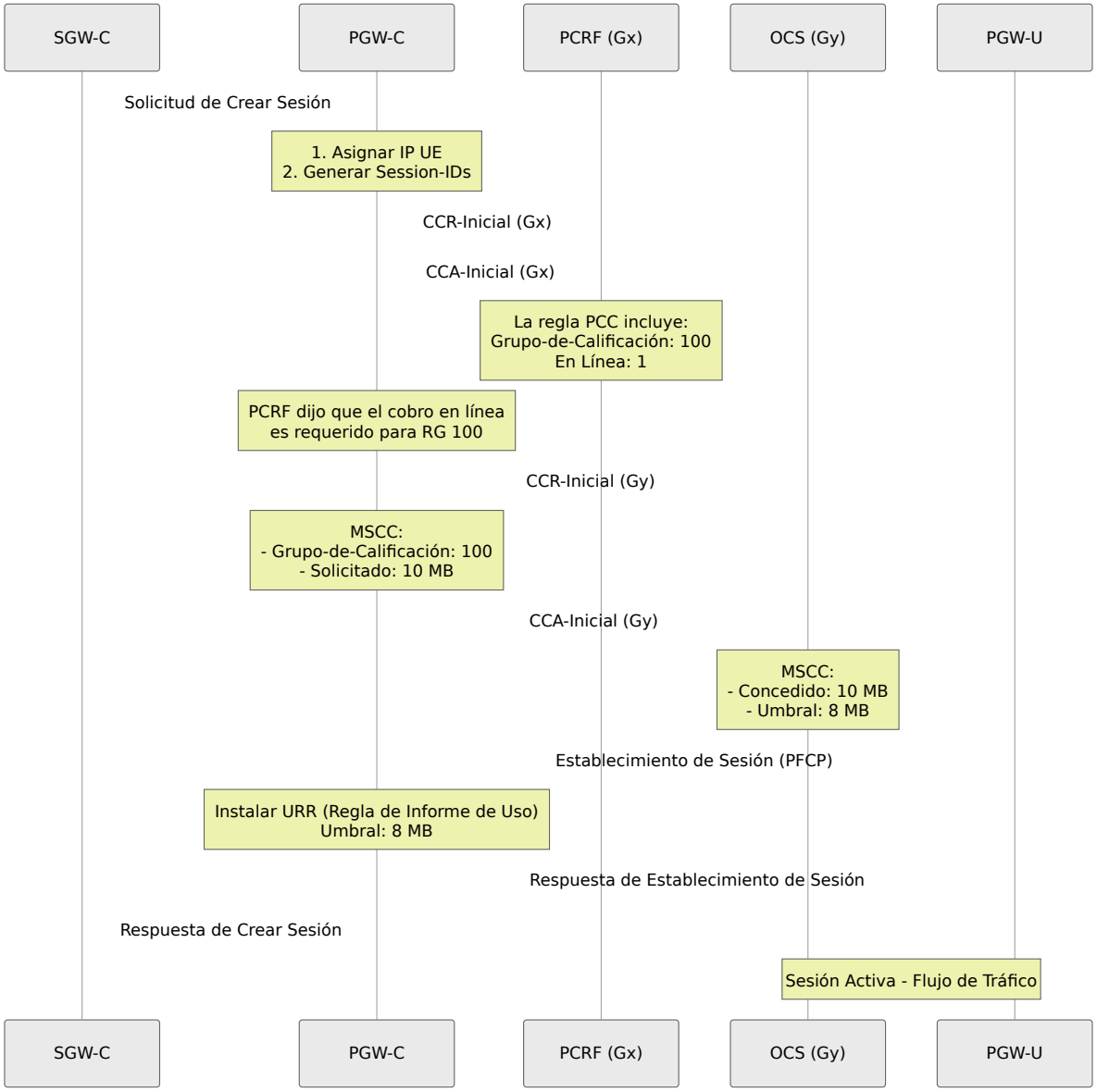
```
config :pgw_c,
  gy: %{
    enabled: false  # Deshabilitar para pruebas
  }
```

Híbrido (algunos prepago, algunos postpago):

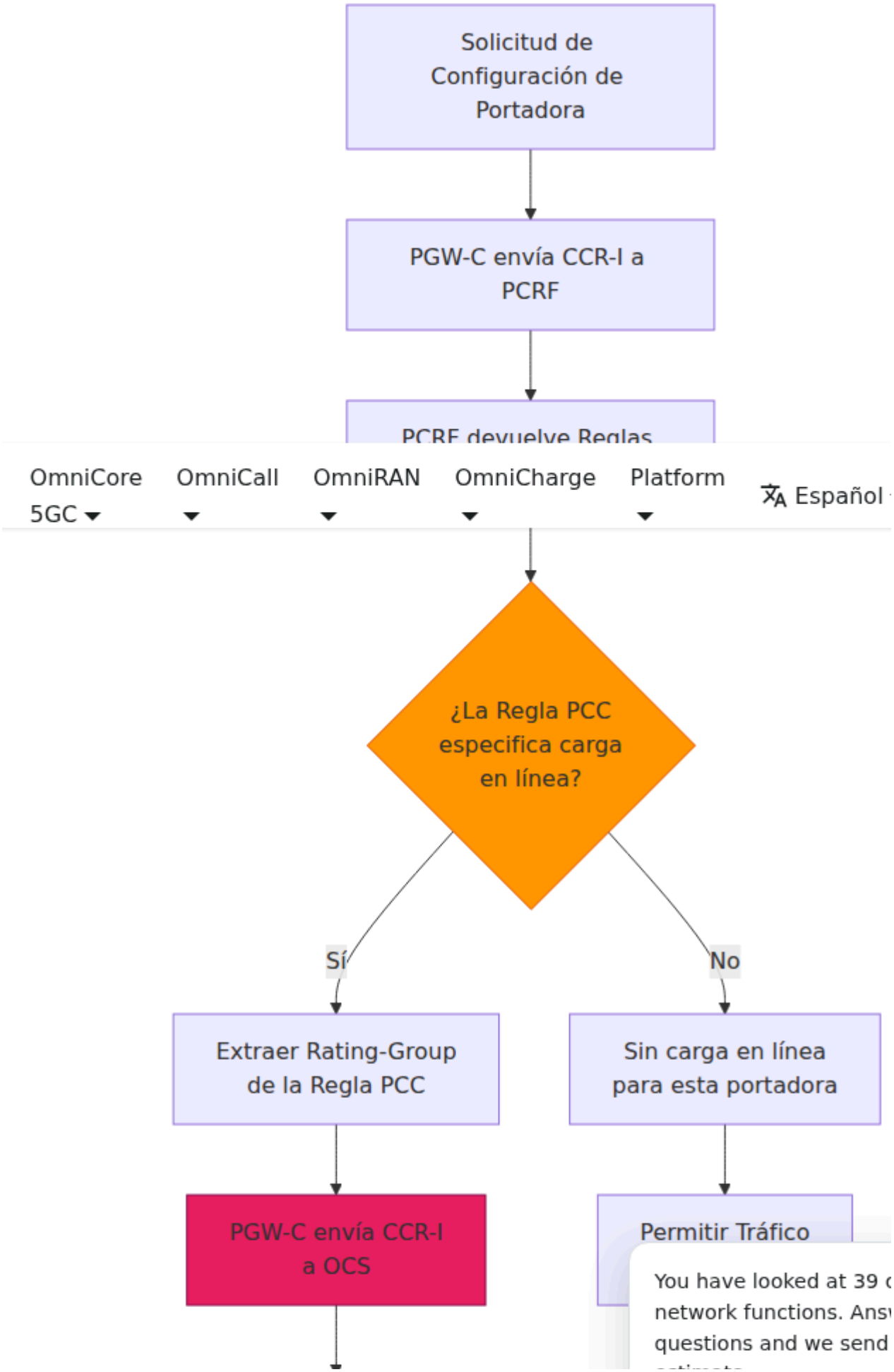
```
config :pgw_c,
  gy: %{
    enabled: true,  # Controlado por suscriptor por PCRF
    timeout_action: :allow,  # No bloquear postpago en fallo de
OCS
    no_credit_action: :terminate
  }
```

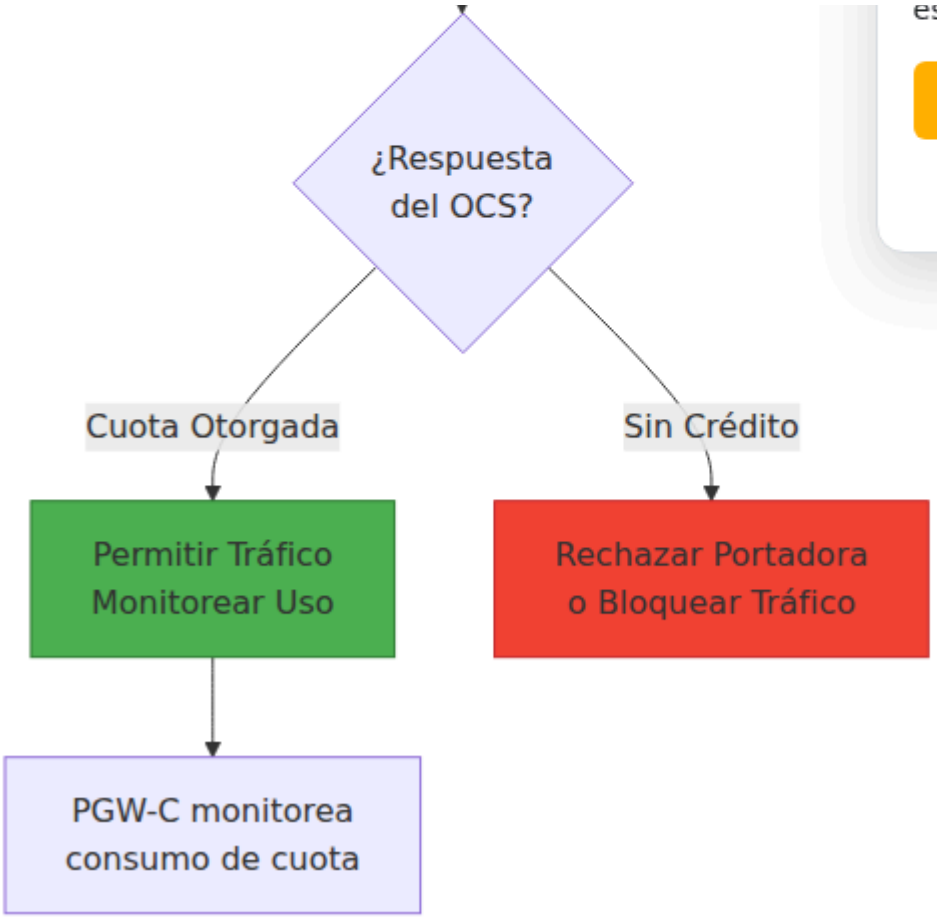
Flujos de Mensajes

Sesión Exitosa con Cobro en Línea

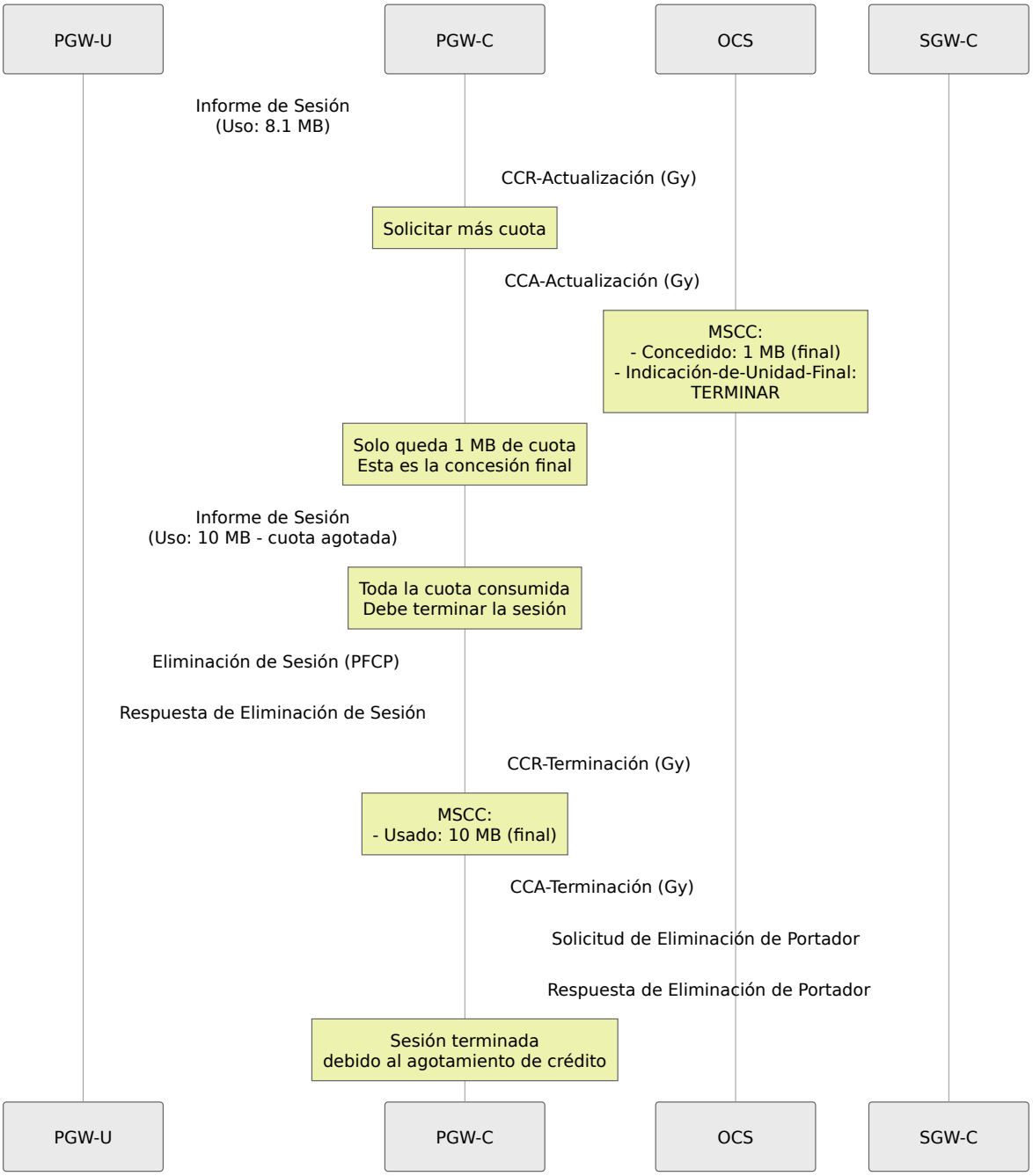


Re-autorización de Cuota (CCR-Actualización)

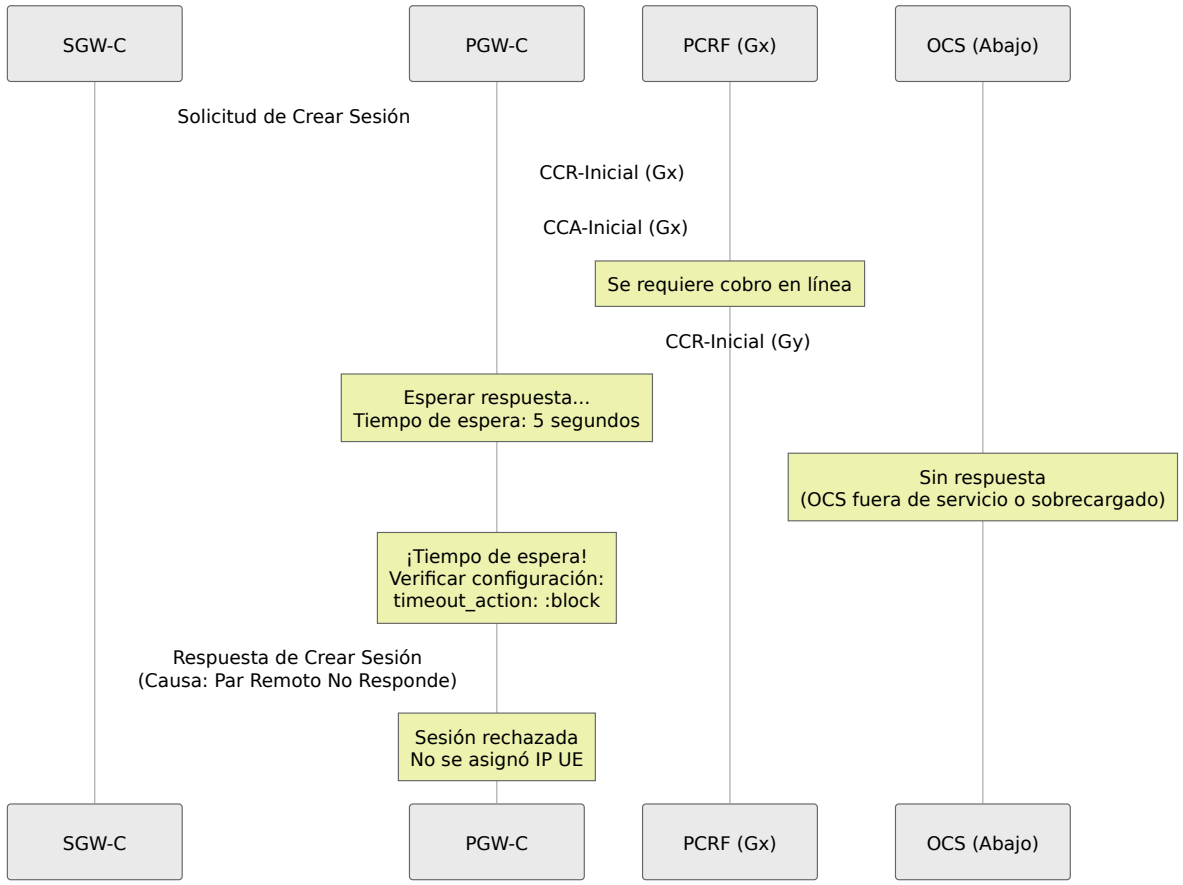

Solicitud de Configuración de Portadora
PGW-C envía CCR-I a PCRF
PCRF devuelve Reglas
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Español
¿La Regla PCC especifica carga en línea?
Sí
No
Extraer Rating-Group de la Regla PCC
Sin carga en línea para esta portadora
PGW-C envía CCR-I a OCS
Permitir Tráfico
You have looked at 39
network functions. Ans
questions and we send



Agotamiento de Crédito (Unidad Final)


PGW-U
PGW-C
OCS
SGW-C
Informe de Sesión
(Uso: 8.1 MB)
CCR-Actualización (Gy)
Solicitar más cuota
CCA-Actualización (Gy)
MSCC:
- Concedido: 1 MB (final)
- Indicación-de-Unidad-Final:
TERMINAR
Solo queda 1 MB de cuota
Esta es la concesión final
Informe de Sesión
(Uso: 10 MB - cuota agotada)
Toda la cuota consumida
Debe terminar la sesión
Eliminación de Sesión (PFCP)
Respuesta de Eliminación de Sesión
CCR-Terminación (Gy)
MSCC:
- Usado: 10 MB (final)
CCA-Terminación (Gy)
Solicitud de Eliminación de Portador
Respuesta de Eliminación de Portador
Sesión terminada
debido al agotamiento de crédito
PGW-U
PGW-C
OCS
SGW-C

Manejo de Tiempo de Espera de OCS



Manejo de Errores

Códigos de Resultado

Códigos de Éxito:

Código	Nombre	Acción
2001	DIAMETER_SUCCESS	Continuar con la cuota concedida

Fallos Transitorios (4xxx):

Código	Nombre	Acción de PGW-C
4010	DIAMETER_TOO_BUSY	Reintentar con retroceso
4011	DIAMETER_UNABLE_TO_COMPLY	Registrar error, puede reintentar
4012	DIAMETER_CREDIT_LIMIT_REACHED	Terminar o redirigir

Fallos Permanentes (5xxx):

Código	Nombre	Acción de PGW-C
5003	DIAMETER_AUTHORIZATION_REJECTED	Rechazar sesión
5031	DIAMETER_USER_UNKNOWN	Rechazar sesión (suscriptor inválido)

Códigos de Resultado por Servicio

Importante: El Código-de-Resultado puede aparecer en **dos niveles**:

1. **Nivel de mensaje** - Resultado general
2. **Nivel de MSCC** - Resultado por servicio

Ejemplo:

```
CCA-Inicial
├── Código-de-Resultado: DIAMETER_SUCCESS (2001)  ← Nivel de
mensaje: OK
└── Control de Crédito de Múltiples Servicios
    ├── [Grupo-de-Calificación: 100]
    │   └── Código-de-Resultado: DIAMETER_SUCCESS (2001)  ← RG
100: OK
    └── [Grupo-de-Calificación: 200]
        └── Código-de-Resultado: DIAMETER_CREDIT_LIMIT_REACHED
(4012)  ← RG 200: Sin crédito
```

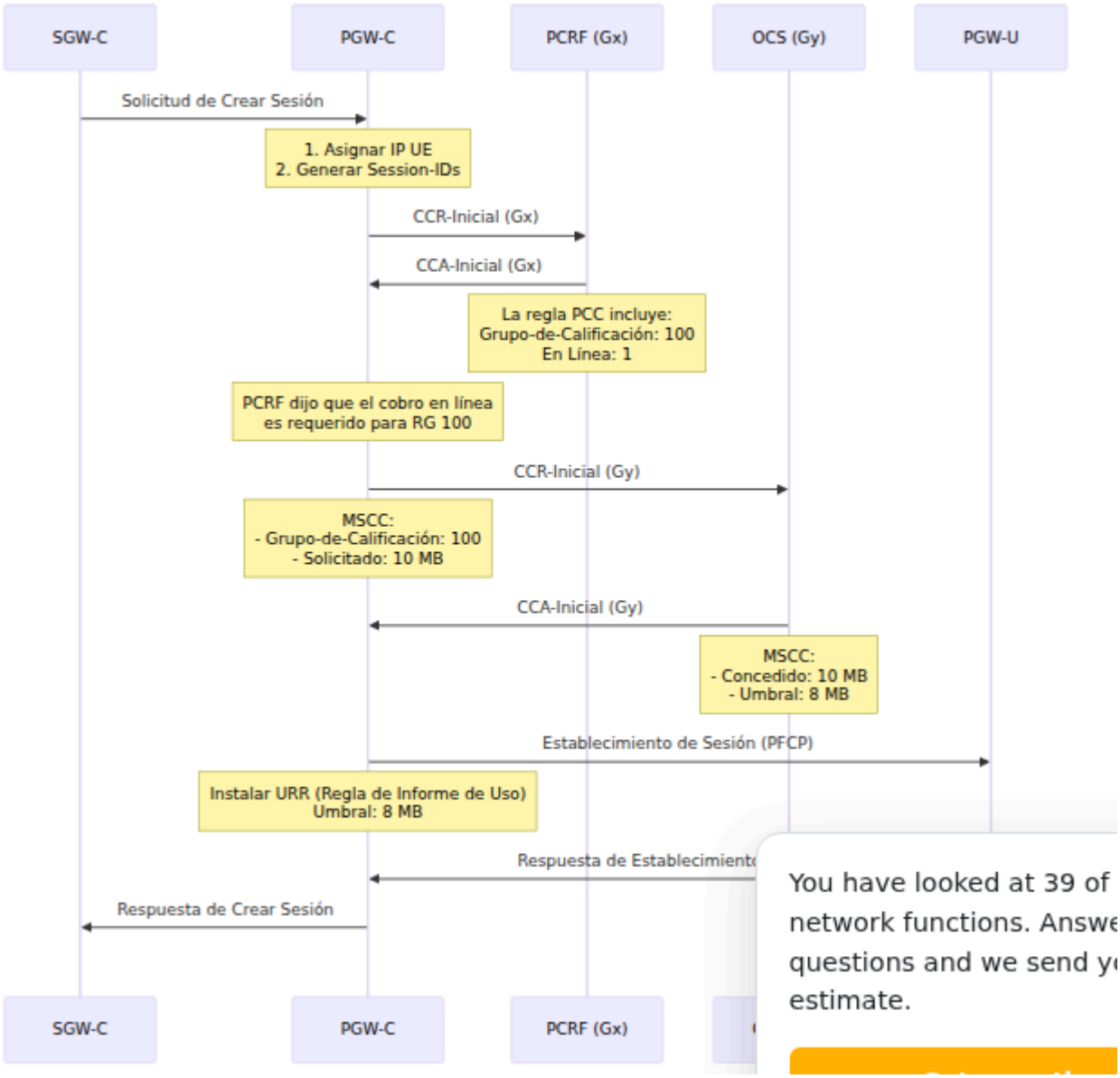
Comportamiento de PGW-C:

- Permitir tráfico para el Grupo-de-Calificación 100
- Bloquear tráfico para el Grupo-de-Calificación 200

Integración con Gx

La interfaz Gx (control de políticas PCRF) determina si se requiere cobro en línea y proporciona el Grupo-de-Calificación que impulsa el cobro Gy. Consulta Interfaz Diameter Gx para la documentación completa sobre control de políticas.

Relación entre Gx y Gy



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

Flujo de Integración

1. Configuración del Portador:

```
PGW-C recibe Solicitud de Crear Sesión
    ↓
Enviar CCR-I a PCRF (Gx)
    ↓
Recibir CCA-I con Reglas PCC
    ↓
Analizar Reglas PCC:
    - ¿La regla tiene Grupo-de-Calificación?
    - ¿Es En Línea = 1?
    ↓
Si SÍ:
    Enviar CCR-I a OCS (Gy) con Grupo-de-Calificación
    ↓
    Recibir CCA-I con cuota
    ↓
    Si cuota concedida: Proceder
    Si sin crédito: Rechazar portador
Si NO:
    Proceder sin cobro en línea
```

2. Actualización de Política Dinámica (RAR de PCRF):

```
PCRF envía RAR (Re-Auth-Request) en Gx
    ↓
Nueva Regla PCC añadida con En Línea=1, Grupo-de-Calificación=200
    ↓
PGW-C envía CCR-U a OCS (Gy)
    - Añadir MSCC para Grupo-de-Calificación 200
    ↓
OCS concede cuota para nuevo servicio
    ↓
Instalar portador dedicado con cobro en línea
```

Solución de Problemas

Problemas Comunes

1. Tiempos de Espera de CCR-Inicial a OCS

Síntomas:

- Las sesiones fallan con "tiempo de espera de OCS"
- Registro: "tiempo de espera de CCR-Inicial (Gy)"

Causas Posibles:

- OCS no accesible
- IP de OCS incorrecta en la configuración
- Cortafuegos bloqueando el puerto Diameter (3868)
- OCS sobrecargado

Resolución:

```
# Probar conectividad de red
ping <ocs_ip>

# Probar puerto Diameter (TCP 3868)
telnet <ocs_ip> 3868

# Verificar configuración
# Asegurarse de que el par OCS esté configurado en peer_list
```

2. Sesiones Rechazadas por OCS

Síntomas:

- CCA-I con Código-de-Resultado != 2001
- Fallo en la Respuesta de Crear Sesión

Códigos de Resultado Comunes:

Código de Resultado	Causa Probable	Resolución
4012	Límite de crédito alcanzado	El suscriptor necesita recargar
5003	Autorización rechazada	Verificar permisos del suscriptor
5031	Usuario desconocido	Provisionar suscriptor en OCS

Pasos de Depuración:

1. Verificar registros de OCS para la razón del rechazo
2. Verificar saldo del suscriptor en OCS
3. Comprobar que IMSI/MSISDN en CCR-I coincida con el registro del suscriptor

3. Agotamiento de Cuota No Detectado

Síntomas:

- El usuario continúa usando datos después de que se agota el saldo
- No se envió CCR-Actualización

Causas Posibles:

- URR (Regla de Informe de Uso) no instalada en PGW-U
- Umbral no configurado correctamente
- Informes de Sesión PFCP no recibidos

Pasos de Depuración:

1. Verificar URR en Establecimiento de Sesión PFCP:

```
Crear URR
├── URR-ID: 1
├── Método-de-Medición: VOLUMEN
├── Umbral-de-Volumen: 8000000 (8 MB)
└── Disparadores-de-Informe: VOLUME_THRESHOLD
```

2. Comprobar registros de PGW-U para informes de uso
3. Verificar `quota_threshold_percentage` en la configuración

4. Grupo-de-Calificación Incorrecto

Síntomas:

- OCS rechaza con "Grupo-de-Calificación Desconocido"
- Las sesiones fallan

Causa:

- Grupo-de-Calificación en CCR-I no coincide con la configuración de OCS
- PCRF provisionó un Grupo-de-Calificación inválido

Resolución:

1. Verificar Grupo-de-Calificación en la Regla PCC de PCRF
2. Comprobar configuración de OCS para Grupos-de-Calificación válidos
3. Asegurarse de que haya un mapeo entre Reglas PCC y tarifas de OCS

Monitoreo

Métricas Clave

La lista completa, con etiquetas, está en la Guía de Monitoreo.

```
# Tasas de mensajes Gy (message_type es ro_CCR, ro_CCA, ro_RAR o
ro_RAA)
rate(gy_outbound_messages_total{message_type="ro_CCR"}[5m])
rate(gy_inbound_messages_total{message_type="ro_CCA"}[5m])

# Resultados de CCA por tipo de solicitud (inicial, actualización,
terminación) y clase de código de resultado
sum by (cc_request_type, result_code_class)
(rate(gy_inbound_responses_total[5m]))

# Tasas de error de Gy
rate(gy_inbound_errors_total[5m])

# CCRs enviados sin CCA de vuelta (tiempos de espera de OCS o
respuestas perdidas)
sum(rate(gy_outbound_messages_total{message_type="ro_CCR"}[5m]))
  - sum(rate(gy_inbound_responses_total[5m]))

# Tiempo de ida y vuelta de OCS (CCR a CCA)
histogram_quantile(0.95, sum by (le)
(rate(gy_outbound_transaction_duration_bucket[5m])))

# Sesiones Gy abiertas
gy_session_id_registry_count
```

Alertas

```
# Alerta sobre una alta tasa de errores de Gy
- alert: GyErrorRateHigh
  expr: rate(gy_inbound_errors_total[5m]) > 0.1
  for: 5m
  annotations:
    summary: "Se detectó una alta tasa de errores de Gy"

# Alerta cuando el OCS no responde a CCRs (tiempos de espera o respue
- alert: OcsNotAnswering
  expr: |
    sum by (instance) (rate(gy_outbound_messages_total{message_type="
      - sum by (instance) (rate(gy_inbound_responses_total[5m])) > 0.
  for: 2m
  annotations:
    summary: "Los CCRs al OCS no están siendo respondidos"

# Alerta cuando el OCS rechaza nuevas sesiones
- alert: OcsRejectingCcrI
  expr:
sum(rate(gy_inbound_responses_total{cc_request_type="initial",result_
[5m])) > 0.1
  for: 5m
  annotations:
    summary: "El OCS está rechazando CCR-I (nuevas sesiones Gy)"
```

Control de Crédito Gy (API OAM)

El cobro en línea se inspecciona y se ejerce a través de la **API REST OAM**, servida sobre HTTPS/TLS en `https://<host>:8443`. La documentación interactiva de la API (Swagger UI) está disponible en `https://<host>:8443/api/docs`.

Estado del Cobro en Línea

```
GET /api/charging                # todas las sesiones de cobro en
línea + estado de crédito en vivo
GET /api/charging?search=<imsi>  # filtrar sesiones por IMSI
GET /api/charging/<imsi>         # estado de control de crédito de
una sesión por IMSI
```

Ejemplo:

```
curl -k https://localhost:8443/api/charging/310170123456789
```

`GET /api/charging` devuelve el estado de cobro en línea (cuota concedida vs. usada, validez, la Acción-de-Unidad-Final de OCS, y estado de redirección de jardín amurallado / sin crédito) para cada sesión activa. Agrega `?search=<imsi>` para reducir la lista, o agrega el IMSI a `GET /api/charging/<imsi>` para obtener el estado de control de crédito de un solo suscriptor.

Simulador de Control de Crédito Gy

```
POST /api/gy_simulator
```

Envía una Solicitud de Control de Crédito sintética al OCS configurado y devuelve la respuesta analizada — Código-de-Resultado a nivel de comando, cuota concedida, tiempo de validez, y cualquier Indicación-de-Unidad-Final — para que el cobro en línea pueda ejercerse **sin tráfico de suscriptor en vivo**. Este es el reemplazo de la API OAM para el antiguo simulador Gy basado en navegador. Requiere que Gy esté habilitado (`gy.enabled: true`); la solicitud se envía desde el propio host de origen Gy de PGW-C al dominio OCS configurado.

Cuerpo de la solicitud (`application/json`):

Campo	Tipo	Descripción
`imsi`	string	**Requerido.** IMSI del suscriptor.
`msisdn`	string	MSISDN opcional (E.164). Población de `User-Name` como `<msisdn>@<apn>`.
`apn`	string	APN opcional.
`requested_units`	integer	Cuota solicitada opcional en octetos (Unidad-de-Servicio-Solicitada → CC-Octetos-Totales).
`rating_group`	integer	Grupo-de-Calificación / clave de cobro opcional (predeterminado `1`).
`service_id`	integer	Identificador-de-Servicio opcional.
`cc_request_type`	string	`initial` (predeterminado), `update`, o `terminate` (o los numéricos `1`/`2`/`3`).

Ejemplo — solicitar 1 MB de cuota inicial para un suscriptor:

```
curl -k -X POST https://localhost:8443/api/gy_simulator \
  -H 'content-type: application/json' \
  -d
'{"imsi":"310170123456789","msisdn":"14155551234","apn":"internet","r
```

Ejemplo de respuesta (CCA-Inicial concediendo 1 MB, válido por 1 hora):

```
{
  "session_id": "omni-pgw_c.epc...;734825199;app_gy_sim",
  "cc_request_type": 1,
  "cc_request_type_name": "initial",
  "result_code": "diameter_success",
  "accepted": true,
  "ocs_host": "ocs.epc.example.org",
  "ocs_realm": "epc.example.org",
  "granted": { "total_octets": 1000000, "input_octets": null,
"output_octets": null, "time": null },
  "validity_time": 3600,
  "final_unit_action": null,
  "final_unit_redirect": null,
  "mscc_result_code": "diameter_success"
}
```


En caso de fallo, el punto final devuelve `422` (`imsi` faltante) o `503` (Gy deshabilitado, o el OCS no respondió — el campo `reason` lleva el error subyacente, por ejemplo, `:timeout`).

Casos de Uso Operativos

- **Inspeccionar la cuota de un suscriptor** — `GET /api/charging/<imsi>` devuelve la sesión actual cuota concedida y estado de crédito.
- **Probar la integración de OCS sin tráfico** — `POST /api/gy_simulator` para confirmar que el OCS concede la cuota esperada / Acción-de-Unidad-Final para un IMSI, grupo de calificación o servicio dado.
- **Solucionar problemas de cobro** — localizar un suscriptor afectado con `GET /api/charging?search=<imsi>` y revisar su estado de control de crédito en vivo.

Para tendencias históricas (tasas de mensajes, agotamiento de cuotas, tiempos de espera de OCS) utiliza las métricas de Prometheus descritas en Monitoreo arriba.

Documentación Relacionada

Carga y Políticas

- **Interfaz Diameter Gx** - Control de políticas PCRF, reglas PCC que activan la carga en línea
- **Formato de CDR de Datos** - Registros de carga fuera de línea para facturación postpaga
- **Guía de Configuración** - Parámetros completos de configuración de carga en línea

Gestión de Sesiones

- **Gestión de Sesiones** - Ciclo de vida de la sesión PDN, gestión de portadoras
- **Interfaz PFCP** - Informes de uso desde PGW-U a través de URRs
- **Interfaz S5/S8** - Configuración y desmantelamiento de portadoras GTP-C

Operaciones

- **Guía de Monitoreo** - Métricas Gy, seguimiento de cuotas, alertas de tiempo de espera de OCS
- **Asignación de IP de UE** - Configuración de pool de IP para sesiones con cargo

---

Volver a la Guía de Operaciones

Documentación de la Interfaz Gn/Gp

Comunicación GTP-C con SGSN (Redes 2G/3G)

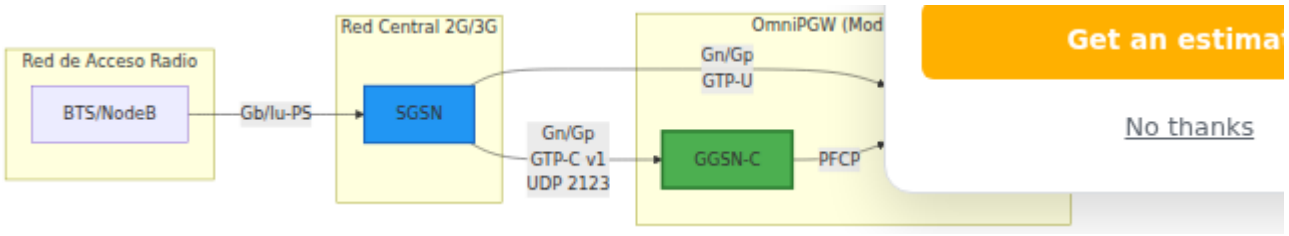
OmniPGW de Omnitouch Network Services

Descripción General

La **interfaz Gn/Gp** permite que OmniPGW funcione como un **GGSN** (Nodo de Soporte GPRS de Puerta de Enlace) para redes 2G/3G utilizando el protocolo **GTP-C v1**. Esta interfaz maneja la gestión del contexto PDP (Protocolo de Datos por Paquetes) entre el GGSN y los SGSNs.

- **Interfaz Gn**: Conecta a los SGSNs dentro del mismo PLMN (red doméstica)
- **Interfaz Gp**: Conecta a los SGSNs en otros PLMNs (escenarios de roaming)

Ambas interfaces utilizan protocolos idénticos; la distinción es puramente topológica.



Principales Diferencias con PGW (S5/S8)

Aspecto	GGSN (Gn/Gp)	PGW (S5/S8)
Versión del Protocolo	GTP-C v1	GTP-C v2
Especificación 3GPP	TS 29.060	TS 29.274
Concepto de Sesión	Contexto PDP	Sesión PDN + Portadoras
Identificador de Portadora	NSAPI (0-15)	EBI (5-15)
Interfaz de Políticas	Ninguna (política estática)	Gx (PCRF)
Modelo de QoS	Perfil QoS R99	QoS de Portadora EPS (QCI)
Puerto	2123 (compartido)	2123

Detalles del Protocolo

GTP-C Versión 1

- **Protocolo**: GTP-C v1 (3GPP TS 29.060)
- **Transporte**: UDP
- **Puerto**: 2123 (compartido con S5/S8 GTP-C v2)
- **Tipo de Interfaz**: Plano de Control

TEID (Identificador de Punto Final del Túnel)

Cada contexto PDP tiene TEIDs únicos para el plano de control y el plano de usuario:

- **TEID de Control GGSN**: Asignado por OmniPGW para mensajes de control entrantes
- **TEID de Datos GGSN**: Asignado por UPF para datos de usuario entrantes
- **TEID de Control SGSN**: Proporcionado por SGSN para mensajes de control salientes
- **TEID de Datos SGSN**: Proporcionado por SGSN para datos de usuario salientes

```
Flujo de Mensajes:
  SGSN → GGSN: TEID de destino = TEID de Control del GGSN
  GGSN → SGSN: TEID de destino = TEID de Control del SGSN
```

Soporte CUPS (Separación del Plano de Control y del Plano de Usuario)

OmniPGW soporta la arquitectura CUPS para 2G/3G:

- **Dirección GSN para Señalización**: IP del plano de control de OmniPGW (de `gn.local_ipv4_address`)
- **Dirección GSN para Tráfico de Usuario**: Dirección IP del UPF (de la Respuesta de Establecimiento de Sesión PFCP)

Esto permite que el GGSN-C y el PGW-U/UPF se ejecuten en nodos separados con diferentes direcciones IP, lo cual es estándar para implementaciones CUPS.

NSAPI (Identificador de Punto de Acceso al Servicio de Red)

El NSAPI identifica contextos PDP individuales dentro de una sesión de suscriptor:

- **Rango**: 5-15 (0-4 reservados)

- **Uso**: Múltiples contextos PDP por suscriptor posibles
- **Equivalente**: Similar al EBI en LTE/EPC

Configuración

Configuración Básica

```
# config/runtime.exs
config :pgw_c,
  # La interfaz Gn/Gp se habilita automáticamente cuando la
configuración gn está presente
  gn: %{
    # Dirección IPv4 local para la interfaz Gn
    local_ipv4_address: "10.0.0.20",

    # Opcional: Dirección IPv6 local
    local_ipv6_address: nil,

    # Puerto para GTP-C v1 (compartido con S5/S8)
    local_port: 2123
  },

  # Servidores DNS devueltos en PCO (compartido con PGW)
  dns: %{
    primary_ipv4: {8, 8, 8, 8},
    secondary_ipv4: {8, 8, 4, 4}
  }
```

Parámetros de la Interfaz Gn

Parámetro	Tipo	Requerido	Predeterminado	Descrip
`local_ipv4_address`	String	Sí	-	Direcció IPv4 a la se vincu interfaz Esta es direcció GGSN anuncia los SGS
`local_ipv6_address`	String	No	`nil`	Direcció IPv6 opciona mayoría las rede 2G/3G s solo IPv
`local_port`	Integer	No	2123	Puerto U para GT Puerto estánda según 3 TS 29.0 Compar con S5/S

Parámetros DNS

Parámetro	Tipo	Requerido	Predeterminado	Descripción
`primary_ipv4`	Tuple	No	`{8, 8, 8, 8}`	Dirección IPv4 del servidor DNS primario devuelta en PCO.
`secondary_ipv4`	Tuple	No	`{8, 8, 4, 4}`	Dirección IPv4 del servidor DNS secundario devuelta en PCO.
`primary_ipv6`	Tuple	No	`nil`	Dirección IPv6 del servidor DNS primario.
`secondary_ipv6`	Tuple	No	`nil`	Dirección IPv6 del servidor DNS secundario.

Requisitos de Red

Reglas de Firewall:

```
# Permitir GTP-C desde la red SGSN
iptables -A INPUT -p udp --dport 2123 -s <sgsn_network>/24 -j
ACCEPT

# Permitir GTP-C saliente a SGSN
iptables -A OUTPUT -p udp --dport 2123 -d <sgsn_network>/24 -j
ACCEPT
```

Tipos de Mensajes

Gestión del Contexto PDP

Solicitud de Creación de Contexto PDP

Dirección: SGSN → GGSN

Propósito: Establecer un nuevo contexto PDP para conectividad de datos

IEs Clave (Elementos de Información):

Nombre IE	Tipo	Descripción
IMSI	Identidad	Identidad Internacional de Suscriptor Móvil
NSAPI	Entero	Identificador de Punto de Acceso al Servicio de Red (5-15)
TEID Datos I	Entero	Punto final del túnel del plano de usuario del SGSN
TEID Control	Entero	Punto final del túnel del plano de control del SGSN
Dirección del Usuario Final	Dirección	Tipo de PDN solicitado y IP opcional
Nombre del Punto de Acceso	String	APN para la conexión
Dirección GSN (Señalización)	IP	Dirección del plano de señalización del SGSN
Dirección GSN (Usuario)	IP	Dirección del plano de usuario del SGSN
Perfil de QoS	Binario	Parámetros de QoS solicitados
MSISDN	Identidad	Número de teléfono móvil (opcional)
Modo de Selección	Enum	Modo de selección de APN
Opciones de Configuración del Protocolo	Opciones	Opciones de protocolo adicionales

Ejemplo:

```
Solicitud de Creación de Contexto PDP
├── IMSI: 310260123456789
├── NSAPI: 5
├── TEID Datos I: 0x12345678
├── TEID Control: 0x87654321
├── Dirección del Usuario Final: IPv4 (dinámica)
├── APN: internet
├── Dirección GSN (Señalización): 10.1.1.100
├── Dirección GSN (Usuario): 10.1.1.100
├── Perfil de QoS: [Parámetros QoS R99]
└── PCO: [Solicitud DNS, etc.]
```

Respuesta de Creación de Contexto PDP

Dirección: GGSN → SGSN

Propósito: Confirmar la creación del contexto PDP con recursos asignados

IEs Clave:

Nombre IE	Tipo	Descripción
Causa	Resultado	Código de éxito o error
Reordenamiento Requerido	Booleano	Si se necesita reordenamiento
Recuperación	Contador	Contador de reinicio del GGSN
TEID Datos I	Entero	Punto final del túnel del plano de usuario del GGSN
TEID Control	Entero	Punto final del túnel del plano de control del GGSN
NSAPI	Entero	NSAPI confirmado
ID de Carga	Binario	ID de correlación de carga
Dirección del Usuario Final	Dirección	Dirección IP asignada al UE
Dirección GSN (Señalización)	IP	Dirección del plano de señalización del GGSN
Dirección GSN (Usuario)	IP	Dirección del plano de usuario del GGSN
Perfil de QoS	Binario	Parámetros de QoS negociados
Opciones de Configuración del Protocolo	Opciones	Servidores DNS, etc.

Respuesta de Éxito:

```
Respuesta de Creación de Contexto PDP
├── Causa: Solicitud Aceptada (128)
├── TEID Datos I: 0xAABBCCDD
├── TEID Control: 0xDDCCBBAA
├── NSAPI: 5
├── ID de Carga: 0x11223344
├── Dirección del Usuario Final
│   └── IPv4: 100.64.1.42
├── Dirección GSN (Señalización): 10.0.0.20
├── Dirección GSN (Usuario): 10.0.0.20
├── Perfil de QoS: [QoS Negociado]
└── PCO
    ├── DNS Primario: 8.8.8.8
    └── DNS Secundario: 8.8.4.4
```

Solicitud de Actualización de Contexto PDP

Dirección: SGSN → GGSN

Propósito: Modificar un contexto PDP existente (por ejemplo, reubicación de SGSN, cambio de QoS)

Escenarios comunes:

- Transferencia inter-SGSN (actualización de área de enrutamiento)
- Renegociación de QoS
- Cambio de dirección SGSN

IEs Clave:

Nombre IE	Descripción
NSAPI	Identificador del contexto PDP
TEID Datos I	Nuevo TEID del plano de usuario del SGSN
Dirección GSN	Nuevas direcciones SGSN
Perfil de QoS	QoS actualizada (opcional)

Respuesta de Actualización de Contexto PDP

Dirección: GGSN → SGSN

Propósito: Confirmar la actualización del contexto PDP

IEs Clave:

Nombre IE	Descripción
Causa	Código de éxito o error
TEID Datos I	TEID del plano de usuario del GGSN
Dirección GSN	Direcciones GGSN
Perfil de QoS	QoS negociada

Solicitud de Eliminación de Contexto PDP

Dirección: SGSN → GGSN

Propósito: Terminar un contexto PDP

IEs Clave:

Nombre IE	Descripción
NSAPI	Contexto PDP a eliminar
Indicación de Desmontaje	Eliminar todos los contextos para este suscriptor

Respuesta de Eliminación de Contexto PDP

Dirección: GGSN → SGSN

Propósito: Confirmar la eliminación del contexto PDP

IEs Clave:

Nombre IE	Descripción
Causa	Código de éxito o error

Gestión de Rutas

Solicitud / Respuesta de Eco

Dirección: Bidireccional

Propósito: Mantenimiento de ruta y detección de reinicio

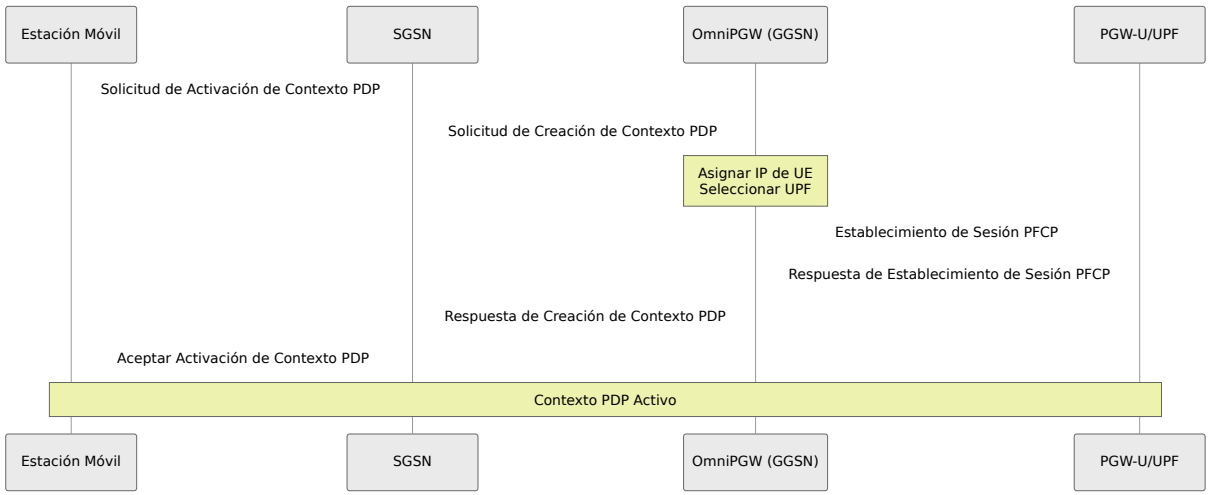
IEs Clave:

Nombre IE	Descripción
Recuperación	Contador de reinicio para detectar reinicios de nodos

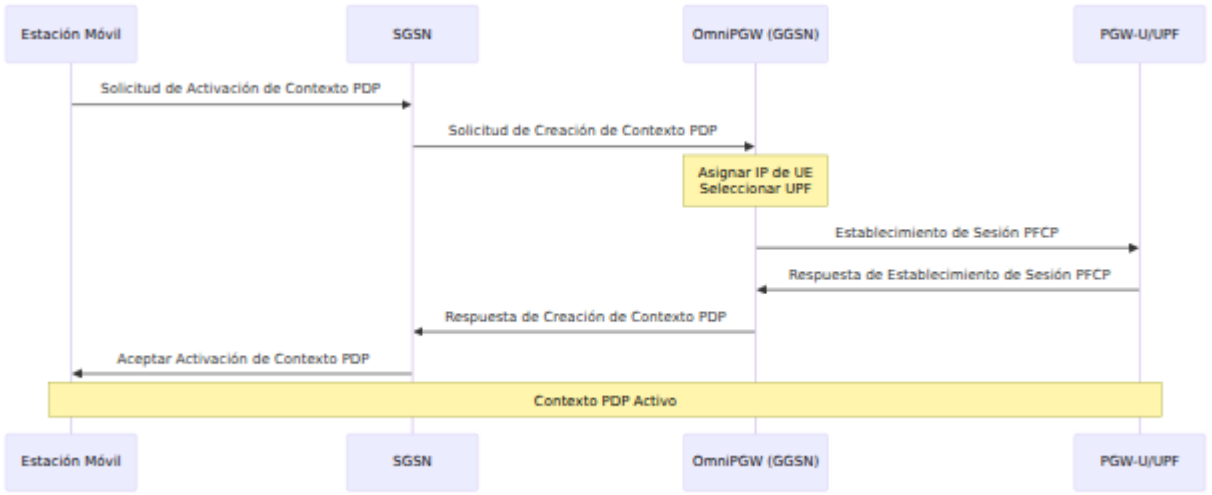
---

Flujos de Mensajes

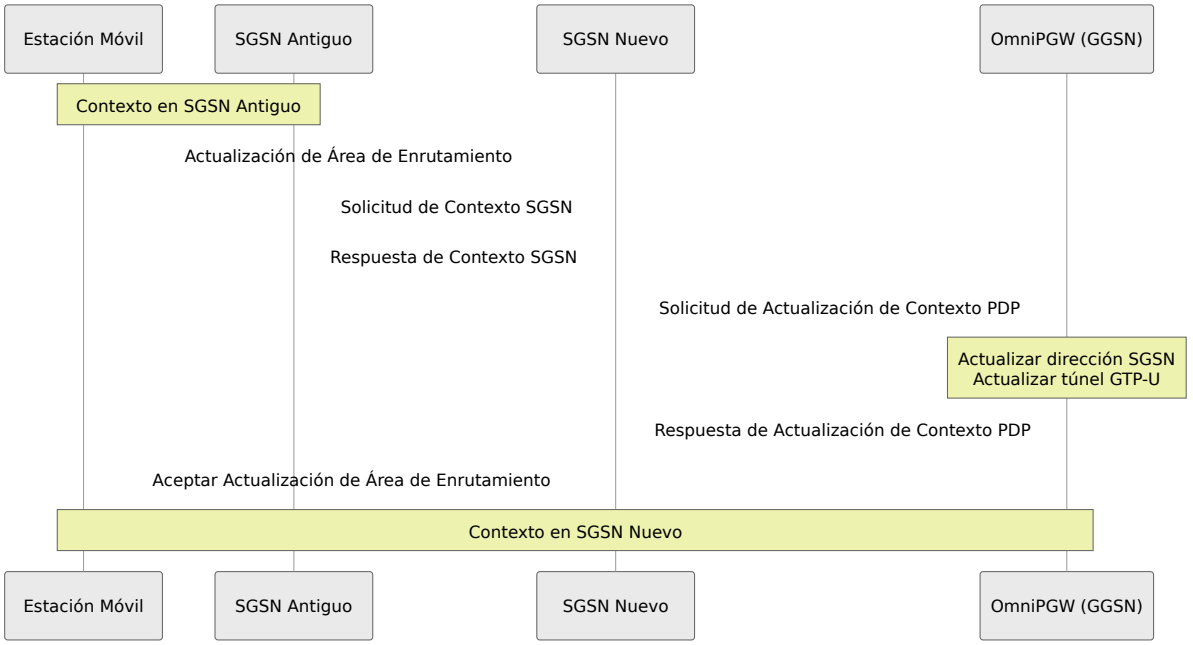
Activación del Contexto PDP



Desactivación del Contexto PDP



Transferencia Inter-SGSN



Infraestructura Compartida

La funcionalidad GGSN de OmniPGW comparte infraestructura con el modo PGW:

Asignación de Dirección IP de UE

Utiliza el mismo AddressRegistry y configuración de subred que PGW. Consulte Asignación de IP de UE para detalles de configuración.

Gestión de Sesiones UPF/PFCP

Utiliza el mismo establecimiento de sesión PFCP que PGW:

- Reglas PDR/FAR/QER creadas por contexto PDP
- Selección de UPF a través de la misma configuración de selección upf_selection
- Consulte Interfaz PFCP para más detalles

Carga en Línea (Gy)

Integración opcional de Diameter Gy disponible:

- Control de crédito para suscriptores prepagos
- La misma configuración de Gy que el modo PGW
- Consulte Interfaz Diameter Gy para configuración

Generación de CDR

Utiliza la misma generación de CDR que PGW. Consulte Formato de CDR de Datos para detalles.

Códigos de Causa

Éxito

Código	Nombre	Descripción
128	Solicitud Aceptada	Operación exitosa

Causas de Rechazo

Código	Nombre	Cuándo se Usa
192	No existente	Contexto PDP no encontrado
193	Formato de mensaje inválido	Mensaje GTP mal formado
194	IMSI no conocido	Suscriptor no encontrado
195	MS está Desconectado de GPRS	MS no adjunto
196	MS no está Respondiendo a GPRS	MS inalcanzable
197	MS Rechaza	MS rechazó la solicitud
198	Versión no soportada	Desajuste de versión GTP
199	No hay recursos disponibles	Agotamiento de recursos
200	Servicio no soportado	Servicio no soportado
201	IE obligatorio incorrecto	Validación de IE fallida
202	IE obligatorio faltante	IE requerido ausente
203	IE opcional incorrecto	IE opcional inválido
204	Fallo del sistema	Error interno
205	Restricción de roaming	Roaming no permitido
206	Desajuste de Firma P-TMSI	Fallo de seguridad
207	Conexión GPRS suspendida	Conexión suspendida

Código	Nombre	Cuándo se Usa
208	Fallo de autenticación	Fallo de autenticación
209	Fallo de autenticación de usuario	Fallo de autenticación de usuario

---

Monitoreo

Métricas de la Interfaz Gn

```
# Contadores de mensajes
gn_inbound_messages_total{message_type="create_pdp_context_request"}
gn_inbound_messages_total{message_type="update_pdp_context_request"}
gn_inbound_messages_total{message_type="delete_pdp_context_request"}

gn_outbound_messages_total{message_type="create_pdp_context_response"
gn_outbound_messages_total{message_type="update_pdp_context_response"
gn_outbound_messages_total{message_type="delete_pdp_context_response"

# Latencia de transacción
gn_outbound_transaction_duration_bucket
```

Consultas Útiles

Tasa de Creación de Contexto PDP:

```
rate(gn_inbound_messages_total{message_type="create_pdp_context_reque
[5m])
```

Tasa de Éxito:

```
sum(rate(gn_outbound_messages_total{message_type="create_pdp_context_
[5m]))
  /
sum(rate(gn_inbound_messages_total{message_type="create_pdp_context_r
[5m]))
```

Contextos PDP Activos:

```
gn_inbound_messages_total{message_type="create_pdp_context_request"}
  -
gn_inbound_messages_total{message_type="delete_pdp_context_request"}
```

Resolución de Problemas

Problema: Sin Respuesta a la Solicitud de Creación de Contexto PDP

Síntomas:

- SGSN envía Solicitud de Creación de Contexto PDP
- No se recibe respuesta
- Tiempo de espera en SGSN

Causas posibles:

1. Problema de conectividad de red
2. OmniPGW no escuchando en la IP configurada
3. Firewall bloqueando UDP 2123
4. Fallo en el establecimiento de UPF/PFCP

Depuración:

```
# Verificar que OmniPGW está escuchando
netstat -ulnp | grep 2123

# Verificar paquetes entrantes
tcpdump -i any -n port 2123

# Verificar configuración
grep "local_ipv4_address" config/runtime.exs

# Verificar conectividad PFCP
curl http://pgw:9090/metrics | grep pfcp
```

Problema: Creación de Contexto PDP Rechazada

Síntomas:

- Respuesta de Creación de Contexto PDP con causa de error
- Contexto PDP no establecido

Causas comunes:

```
Causa 199 (No hay recursos disponibles):
  → Pool de IP agotado
  → Verificar: curl http://pgw:9090/metrics | grep
address_registry_count
  → Ampliar pool de IP en ue.subnet_map

Causa 202 (IE obligatorio faltante):
  → SGSN no envía IEs requeridos
  → Verificar configuración del SGSN
  → Revisar mensaje en tcpdump

Causa 204 (Fallo del sistema):
  → Fallo de UPF/PFCP
  → Verificar estado de asociación PFCP
  → Revisar registros de OmniPGW
```

Problema: Fallo en la Actualización del Contexto PDP

Síntomas:

- Respuesta de Actualización de Contexto PDP con causa de error
- La transferencia falla

Causas posibles:

- Contexto PDP no encontrado (TEID diferente)
- Desajuste de NSAPI
- Sesión ya eliminada

Depuración:

```
# Verificar sesiones activas
curl http://pgw:9090/metrics | grep session_count

# Revisar registros para búsqueda de contexto
journalctl -u omnipgw | grep "PDP Context"
```

Mejores Prácticas

Diseño de Red

1. **Puerto Compartido con S5/S8**
    - Gn y S5/S8 comparten el puerto UDP 2123
    - OmniPGW detecta automáticamente la versión de GTP del mensaje
    - Una sola IP puede servir tanto para 2G/3G como para 4G
2. **Conectividad SGSN**
    - Asegurarse de que todos los SGSNs puedan alcanzar la IP del GGSN
    - Considerar VLAN dedicada para tráfico Gn

- Planificar para roaming (Gp) si es aplicable

3. **Planificación de Direcciones IP**
   - Los mismos pools de IP sirven tanto para modos PGW como GGSN
   - Considerar pools basados en APN separados para 2G/3G

Rendimiento

1. **Capacidad de Sesión**
   - Monitorear la métrica `session_count`
   - Planificar para el número esperado de suscriptores 2G/3G
   - Considerar que 2G/3G típicamente tiene menos sesiones concurrentes

2. **Tamaños de Buffer UDP**
   - Las mismas recomendaciones que S5/S8
   - Típico: 4-8 MB por socket

Consideraciones de Migración

Al migrar de un GGSN independiente a OmniPGW:

1. **Configuración de APN**
   - Asegurarse de que los APNs coincidan con la configuración existente del GGSN
   - Verificar configuraciones de servidores DNS en PCO

2. **Migración de Pool de IP**
   - Planificar cuidadosamente el corte del pool de IP
   - Considerar migración gradual por APN

3. **Mapeo de QoS**
   - Perfiles de QoS R99 aceptados tal como están
   - No se necesita traducción de QCI para 2G/3G

Documentación Relacionada

Funciones Principales

- **Guía de Configuración** - Referencia completa de configuración
- **Gestión de Sesiones** - Detalles del ciclo de vida de la sesión
- **Asignación de IP de UE** - Gestión de direcciones IP
- **Configuración de PCO** - Opciones de Configuración del Protocolo

Interfaces Relacionadas

- **Interfaz S5/S8** - Interfaz equivalente 4G/LTE
- **Interfaz PFCP** - Coordinación del plano de usuario
- **Interfaz Diameter Gy** - Carga en línea

Operaciones

- **Guía de Monitoreo** - Métricas y alertas
- **Resolución de Problemas** - Problemas comunes
- **Formato de CDR de Datos** - Generación de CDR

Referencias

- 3GPP TS 29.060 - Protocolo de Túnel GPRS (GTP) a través de la interfaz Gn y Gp
- 3GPP TS 23.060 - Servicio General de Paquetes de Radio (GPRS); Descripción del servicio
- 3GPP TS 24.008 - Especificación de la Capa 3 de la interfaz de radio móvil (perfiles de QoS)

Volver al Índice de Documentación

Interfaz Gn/Gp de OmniPGW - *por Omnitouch Network Services*

Soporte para PDN IPv6 / Dual-Stack (IPv4v6)

Guía completa para operar conexiones PDN compatibles con IPv6 a través del OmniPGW (plano de control) y OmniUPF (plano de usuario). Esta página cubre cómo se negocia y se señala el tipo de PDN, la configuración requerida en ambos nodos y cómo se logra la conectividad IPv6 del UE con enrutamiento dinámico.

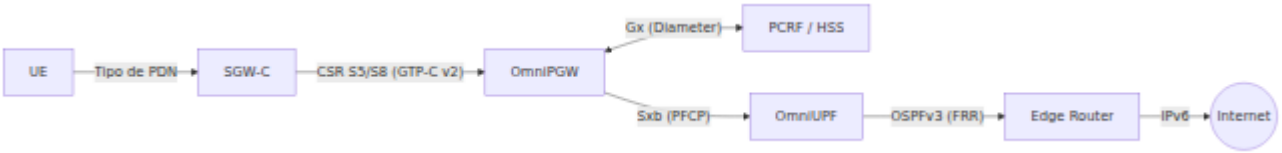
Para el modelo detallado de la piscina de direcciones del UE (coincidencia de APN, asignación, manejo de colisiones), consulte Asignación de IP del UE. Para las interfaces PFCP y Gx en general, consulte PFCP/Sxb y Diameter Gx.

Tabla de Contenidos

- Descripción General
- Tipos de PDN
- Flujo de Fin a Fin
- Configuración del PGW-C
- Plano de Usuario (OmniUPF)
- Tablas de Referencia
- Solución de Problemas

Descripción General

Una conexión PDN puede ser **IPv4**, **IPv6** o **IPv4v6** (dual-stack). El tipo de PDN es solicitado por el UE/SGW en la Solicitud de Creación de Sesión GTPv2 y confirmado por el PGW-C en la respuesta. Proporcionar un PDN IPv6 de extremo a extremo requiere un comportamiento coordinado a través de tres interfaces y ambos nodos:



Nodo / Interfaz	Responsabilidad por IPv6
OmniPGW — S5/S8	Negociar tipo de PDN; asignar dirección(es) del UE; devolver la Asignación de Dirección de PDN (PAA)
OmniPGW — Gx	Transmitir la dirección del UE al PCRF: `Framed-IP-Address` (IPv4) para PDNs IPv4/IPv4v6, `Framed-IPv6-Prefix` para PDNs solo IPv6
OmniPGW — Sxb	Señalar la dirección IPv6 del UE y el tipo de PDN al UPF a través de PFCP
OmniUPF — plano de datos	Programar la búsqueda de bajada de IPv6; reenviar/encapsular tráfico de usuario IPv6
OmniUPF — FRR	Anunciar cada ruta de host IPv6 `/128` del UE al enrutador de borde a través de OSPFv3

Referencias: 3GPP TS 29.274 (GTPv2-C), 3GPP TS 29.212 (Gx), 3GPP TS 29.244 (PFCP).

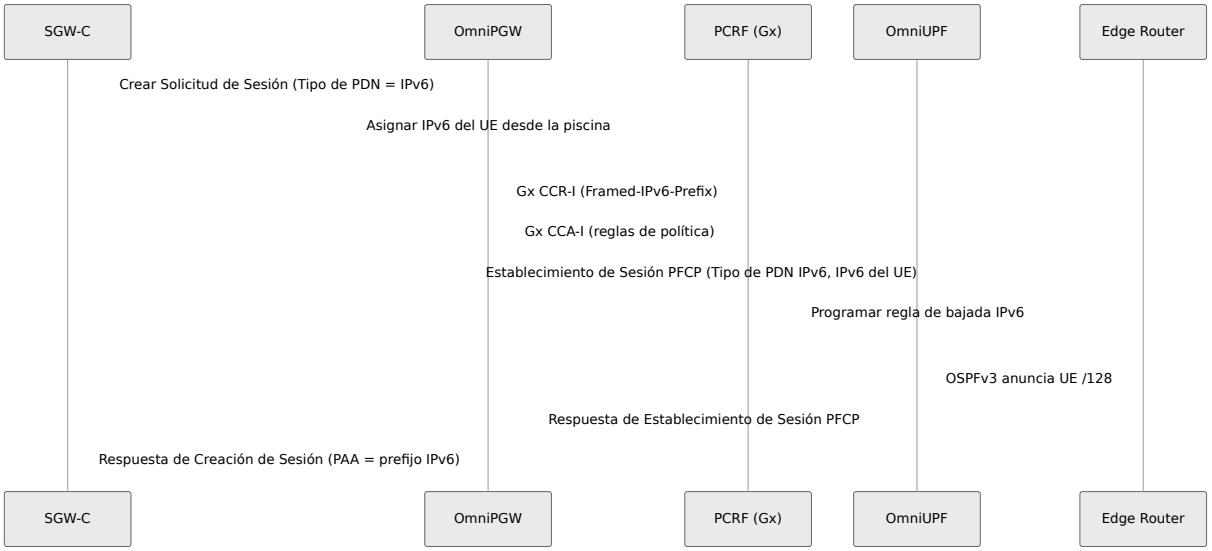
Tipos de PDN

Valor	Tipo de PDN	UE recibe	Contenido de PAA (TS 29.274 §8.14)
1	IPv4	Dirección IPv4	Dirección IPv4 de 4 bytes
2	IPv6	Prefijo IPv6 (/64)	octeto de longitud de prefijo + dirección de 16 bytes
3	IPv4v6	Dirección IPv4 + Prefijo IPv6	octeto de longitud de prefijo + 16 bytes IPv6 + 4 bytes IPv4

El PGW-C deriva el tipo de PDN efectivo del **IE Tipo de PDN**, retrocediendo al tipo del **IE PAA** si el IE Tipo de PDN está ausente. El mismo tipo negociado impulsa el PAA devuelto al SGW, el IE Tipo de PDN PFCP enviado al UPF, y qué familia/familias de direcciones son asignadas.

> **IPv4v6 sin piscina IPv6.** Si se solicita un PDN IPv4v6 pero el APN coincidente no tiene un rango IPv6 configurado, el PGW-C **no** falla; degrada el PDN a solo IPv4 o lo rechaza, dependiendo de si el APN es un APN de emergencia (SOS). Consulte Solicitud IPv4v6 cuando el APN no tiene piscina IPv6.

Flujo de Fin a Fin



Una Solicitud de Creación de Sesión retransmitida (mismo número de secuencia) se maneja de manera idempotente y produce la misma respuesta.

Configuración del PGW-C

Piscina de Direcciones IPv6 del UE

Las direcciones del UE se extraen de piscinas por APN bajo la clave `ue.subnet_map` en `runtime.exs`. Agregue un CIDR IPv6 junto al CIDR IPv4 para cualquier APN que deba ofrecer IPv6 o dual-stack. La piscina se analiza automáticamente por familia de direcciones.

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # Nombre del APN => lista de cadenas CIDR (IPv4 y/o IPv6)
      default: [
        "100.64.16.0/24",
        "2001:db8:6f85:70::/64"
      ]
    }
  }
```

Parámetro	Tipo	Requerido	Predeterminado	Descri
`ue.subnet_map`	Mapa	Sí	-	Mapea un nor (o `:default`) de cadenas C `:default` es respaldo cuar coincide ning específica de
(entradas de lista)	Cadena (CIDR)	Sí	-	Un prefijo IPv ejemplo, `100.64.16.0/` (por ejemplo, `2001:db8:6f8` La familia de se detecta a cadena. Las IPv6 del UE s dentro del pr configurado y un `/64` al UE.

> Para coincidencia de expresiones regulares de APN, múltiples subredes por APN, direcciones estáticas y el algoritmo de asignación, consulte Asignación de IP del UE.

Un APN con **tanto** un CIDR IPv4 como un CIDR IPv6 admite PDNs IPv4, IPv6 y IPv4v6; el PGW-C asigna de la familia/familias que el tipo de PDN negociado requiere (para IPv4v6, una dirección de cada uno).

Gx (Framed-IPv6-Prefix)

No se requiere configuración adicional para Gx. El PGW-C establece el AVP de dirección enmarcada Gx a partir de la dirección del UE por familia:

- **PDN solo IPv6** — el prefijo IPv6 del UE se transmite utilizando el **`Framed-IPv6-Prefix`** AVP (RFC 3162 §2.3), no `Framed-IP-Address` (que solo lleva IPv4).
- **PDNs IPv4 e IPv4v6** — la dirección IPv4 del UE se transmite en `Framed-IP-Address`. Para IPv4v6, el prefijo IPv6 **no** se lleva en Gx (los AVPs de dirección enmarcada del CCR se derivan de la dirección IPv4); el prefijo IPv6 todavía se señala al UPF a través de PFCP y al UE en el PAA.

Para un suscriptor solo IPv6, el PCRF debe estar provisionado y ser capaz de procesar `Framed-IPv6-Prefix`; de lo contrario, la Solicitud de Control de Crédito se descarta y la sesión falla — consulte Solución de Problemas.

Plano de Usuario (OmniUPF)

Para que un PDN IPv6 transporte tráfico, el OmniUPF debe estar habilitado para IPv6, programar la búsqueda de bajada de IPv6 desde la sesión PFCP que envía el PGW-C, y anunciar cada ruta de host IPv6 `/128` al enrutador de borde (a través de OSPFv3) para que el tráfico de bajada sea atraído al UPF.

Esas son preocupaciones del plano de usuario configuradas en el OmniUPF, no en el PGW-C. Consulte la **guía de IPv6 / Dual-Stack de OmniUPF** para configuraciones del kernel, la piscina de UE del UPF y la publicidad de rutas OSPFv3. Desde la perspectiva del PGW-C, el único requisito es que el UPF seleccionado soporte IPv6 — el PGW-C señala la dirección IPv6 del UE y el tipo de PDN a través de PFCP (consulte PFCP/Sxb).

Tablas de Referencia

Asignación de Dirección de PDN (PAA) — TS 29.274 §8.14

Tipo de PDN	Diseño del campo de dirección
IPv4	4 octetos: dirección IPv4
IPv6	1 octeto de longitud de prefijo + 16 octetos de prefijo/dirección IPv6
IPv4v6	1 octeto de longitud de prefijo + 16 octetos de IPv6 + 4 octetos de IPv4

AVPs de Dirección Enmarcada Gx

AVP	Código	Familia	Formato	Referencia
`Framed-IP-Address`	8	IPv4	dirección de 4 bytes	RFC 4005
`Framed-IPv6-Prefix`	97	IPv6	octeto reservado + longitud de prefijo + prefijo	RFC 3162 §2.3

IE Tipo de PDN PFCP — TS 29.244

Valor	Significado
1	IPv4
2	IPv6
3	IPv4v6

Solución de Problemas

El CCR de Gx se agota para sesiones IPv6

Síntomas: Las sesiones IPv4 para un suscriptor tienen éxito, pero las sesiones IPv6/IPv4v6 devuelven la causa `remote_peer_not_responding`; la Solicitud de Control de Crédito Gx se agota.

Causas posibles:

- El PCRF no puede procesar el AVP `Framed-IPv6-Prefix` y descarta silenciosamente la solicitud.
- El suscriptor no está provisionado para IPv6 en el PCRF/HSS.

Resolución:

1. Confirme que el suscriptor esté provisionado y habilitado en el PCRF/HSS.
2. Verifique que el PCRF acepte `Framed-IPv6-Prefix` para Gx CCR-I.
3. Compare con una sesión IPv4 para el mismo suscriptor para aislar el comportamiento específico de IPv6.

La sesión IPv6 es aceptada pero el tráfico de bajada no llega al UE

Síntomas: La Respuesta de Creación de Sesión lleva un PAA IPv6, el enlace ascendente funciona, pero el tráfico de la red al UE se pierde.

Esta es una preocupación del plano de usuario (OmniUPF) — el PGW-C ya ha asignado la dirección y la ha señalado a través de PFCP. La causa habitual es que la ruta de host `/128` del UE no está llegando al enrutador de borde (OSPFv3 no está en ejecución/adyacente en el UPF, o retraso de convergencia). Consulte la guía de IPv6 / Dual-Stack de OmniUPF para la configuración de publicidad de rutas y solución de problemas.

No se asigna ninguna dirección IPv6

Síntomas: Se rechaza una solicitud de PDN IPv6, o no se devuelve ningún PAA IPv6.

Causas posibles:

- El APN coincidente (o `:default`) no tiene un CIDR IPv6 en `ue.subnet_map`.
- La piscina IPv6 configurada está agotada.

Resolución:

1. Agregue un CIDR IPv6 a la entrada del APN en `ue.subnet_map` (consulte Configuración del PGW-C).
2. Confirme que la piscina tenga direcciones libres.

Solicitud IPv4v6 cuando el APN no tiene piscina IPv6

Síntomas: Un UE solicita un PDN **IPv4v6** contra un APN que solo tiene un CIDR IPv4 configurado en `ue.subnet_map` (sin rango IPv6). Dependiendo del APN, la sesión se establece como **solo IPv4** o es **rechazada**.

Comportamiento: El asignador de IPv6 informa que no hay piscina IPv6 cuando el APN coincidente tiene una lista IPv6 vacía, en lugar de hacer que el

proceso de sesión falle. El procedimiento de sesión luego elige por tipo de APN (según TS 29.274 / manejo de portadora de dirección única / degradación de tipo de PDN):

Tipo de APN	Resultado	Lo que ve el UE / PCRF / UPF
APN de Emergencia (SOS)	**Degradar a solo IPv4** — asignar la dirección IPv4, limpiar la dirección IPv6, establecer el tipo de PDN negociado a `IPv4`.	PAA, Tipo de PDN PFCP y IP del UE son solo IPv4; Gx lleva `Framed-IP-Address`. El **P-CSCF aún se devuelve en el PCO** para que el registro IMS de emergencia pueda proceder. Se registra una `advertencia`.
APN Regular	**Rechazar** — la sesión no se degrada silenciosamente; `{:error, :no_ipv6_pool}` se presenta para que la mala configuración (o solicitud genuinamente no soportada) sea visible. Se registra un `error`.	La creación de sesión falla con una causa no exitosa.

Un APN de emergencia se identifica por su nombre: el APN contiene `"sos"` (por ejemplo, `sos`, `sos.mnc410.mcc310.gprs`). Las solicitudes solo IPv6 contra un APN sin piscina IPv6 también son rechazadas.

> En la práctica, el MME normalmente degrada la solicitud IPv4v6 de un suscriptor regular a su IPv4 suscrito antes de que la solicitud llegue al PGW-C, por lo que la ruta de rechazo es un respaldo para una solicitud IPv4v6 que realmente llega sin una piscina IPv6. La ruta de degradación SOS mantiene las llamadas de emergencia (por ejemplo, 911/112) conectadas en un despliegue solo IPv4.

Resolución:

1. Para un APN regular que debería ofrecer dual-stack, agregue un CIDR IPv6 a la entrada del APN en `ue.subnet_map` (consulte Configuración del PGW-C).
2. Para un APN de emergencia (SOS) en un despliegue solo IPv4, no se requiere ninguna acción — la degradación a solo IPv4 es intencionada. Agregue un CIDR IPv6 solo si tiene la intención de que los PDNs SOS sean dual-stack.

Guía de Monitoreo y Métricas de OmniPGW

Integración de Prometheus y Monitoreo Operacional

por Omnitouch Network Services

Tabla de Contenidos

1. Descripción General
2. Endpoint de Métricas
3. Métricas Disponibles
4. Configuración de Prometheus
5. Dashboards de Grafana
6. Alertas
7. Monitoreo de Rendimiento
8. Solución de Problemas de Métricas

Descripción General

OmniPGW proporciona dos enfoques complementarios de monitoreo:

1. API REST OAM en Tiempo Real (cubierto brevemente aquí, detallado en los documentos de interfaz respectivos)

- Visor de sesiones en vivo (`GET /api/sessions`)
- Estado de pares PFCP (`GET /api/upf`)
- Conectividad de pares Diameter (`GET /api/diameter`)
- Inspección de sesiones individuales (`GET /api/sessions/<imsi>`)

2. Métricas de Prometheus (enfoque principal de este documento)

- Tendencias históricas y análisis
- Alertas y notificaciones
- Métricas de rendimiento
- Planificación de capacidad

Este documento se centra en **métricas de Prometheus**. Para la API REST OAM (servida sobre HTTPS en el puerto `8443`, bajo el prefijo `/api`), consulte:

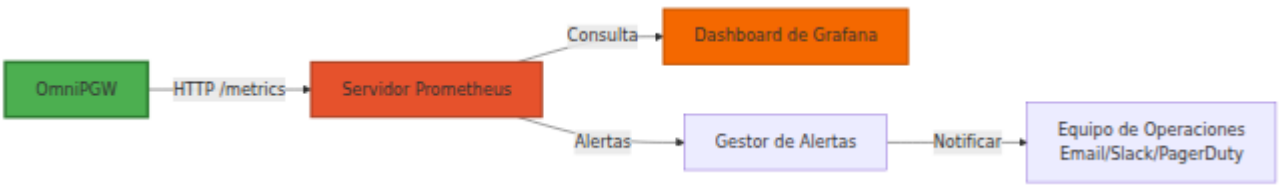
- Gestión de Sesiones - API de Sesiones
- Interfaz PFCP - API de Monitoreo
- Diameter Gx - API de Monitoreo de Pares

Descripción General de las Métricas de Prometheus

OmniPGW expone **métricas compatibles con Prometheus** para un monitoreo integral de la salud del sistema, rendimiento y capacidad. Esto permite a los equipos de operaciones:

- **Monitorear la Salud del Sistema** - Rastrear sesiones activas, asignaciones y errores
- **Planificación de Capacidad** - Comprender las tendencias de utilización de recursos
- **Análisis de Rendimiento** - Medir la latencia en el manejo de mensajes
- **Alertas** - Notificación proactiva de problemas
- **Depuración** - Identificar las causas raíz de los problemas

Arquitectura de Monitoreo



Endpoint de Métricas

Configuración

Habilite las métricas en `config/runtime.exs`:

```
config :pgw_c,
  metrics: %{
    enabled: true,
    ip_address: "127.0.0.42",       # Dirección de enlace
predeterminada (use "0.0.0.0" para exponer en todas las
interfaces)
    port: 9090,                      # Puerto HTTP predeterminado
    registry_poll_period_ms: 10_000  # Intervalo de sondeo para
medidores sondeados (predeterminado 10s)
  }
```

> **Nota:** Los valores predeterminados enviados enlazan el endpoint de métricas a `127.0.0.42:9090`. Para rasparlo desde un Prometheus remoto, establezca `ip_address` en una dirección accesible (por ejemplo, `"0.0.0.0"`).

Accediendo a las Métricas

Endpoint HTTP:

```
http://<omnipgw_ip>:<port>/metrics
```

Ejemplo:

```
curl http://10.0.0.20:9090/metrics
```

Formato de Salida

Las métricas se exponen en **formato de texto de Prometheus**:

```
# HELP teid_registry_count El número de TEID registrados en
sesiones
# TYPE teid_registry_count gauge
teid_registry_count 150

# HELP address_registry_count El número de direcciones registradas
en sesiones
# TYPE address_registry_count gauge
address_registry_count 150

# HELP s5s8_inbound_messages_total El número total de mensajes
recibidos de pares S5/S8
# TYPE s5s8_inbound_messages_total counter
s5s8_inbound_messages_total{message_type="create_session_request"}
1523
s5s8_inbound_messages_total{message_type="delete_session_request"}
1487
```

Métricas Disponibles

OmniPGW expone las siguientes categorías de métricas:

Métricas de Sesión

Conteos de Sesiones Activas:

Nombre de Métrica	Tipo	Descripción
`teid_registry_count`	Gauge	Sesiones S5/S8 activas (conteo de TEID)
`seid_registry_count`	Gauge	Sesiones PFCP activas (conteo de SEID)
`gx_session_id_registry_count`	Gauge	Sesiones Gx activas (conteo de Diameter Session-ID)
`gy_session_id_registry_count`	Gauge	Sesiones Gy activas (conteo de Diameter Session-ID)
`session_registry_count`	Gauge	Sesiones activas (pares IMSI, EBI)
`address_registry_count`	Gauge	Direcciones IP de UE asignadas
`charging_id_registry_count`	Gauge	IDs de carga activos (ver Formato de CDR de Datos para registros de facturación CDR)
`sxb_sequence_number_registry_count`	Gauge	Respuestas PFCP pendientes (esperando respuesta)
`s5s8_sequence_number_registry_count`	Gauge	Respuestas S5/S8 pendientes (esperando respuesta)
`sxb_peer_registry_count`	Gauge	Número de procesos de pares PFCP

Nombre de Métrica	Tipo	Descripción
		registrados

Uso:

```
# Sesiones activas actuales
teid_registry_count

# Tasa de creación de sesiones (por segundo)
rate(teid_registry_count[5m])

# Sesiones máximas en la última hora
max_over_time(teid_registry_count[1h])
```

Ciclo de Vida de Sesiones y Bearers:

Contadores incrementados a medida que se crean, modifican y destruyen sesiones y bearers PDN.

Nombre de Métrica	Tipo	Etiquetas	Descripción
`pgw_session_create_total`	Counter	`result`, `cause`, `pdn_type`, `rat_type`	Creaciones de sesione PDN, por resultado (éxito/fallo), causa GTF tipo de PDN y tipo de F
`pgw_session_delete_total`	Counter	`pdn_type`	Eliminaciones de sesio PDN, por tipo de PDN
`pgw_session_modify_total`	Counter	-	Solicitudes de Modifica de Bearer manejadas c éxito
`pgw_bearer_create_total`	Counter	`type`, `qci`	Bearers creados, por ti (predeterminado/dedic y QCI
`pgw_bearer_delete_total`	Counter	`type`	Bearers eliminados, po tipo (predeterminado/dedic

Uso:

```
# Tasa de éxito de configuración de sesiones (últimos 5m)
sum(rate(pgw_session_create_total{result="success"}[5m])) /
sum(rate(pgw_session_create_total[5m]))

# Fallos en configuraciones de sesiones por causa
sum(rate(pgw_session_create_total{result="failure"}[5m])) by
(cause)
```

Pool de Direcciones IP de UE

Los medidores de utilización del pool se sondean periódicamente; los fallos de asignación se cuentan a medida que ocurren. Vea Asignación de IP de UE.

Nombre de Métrica	Tipo	Etiquetas	Descrip
`ue_pool_addresses_allocated`	Gauge	`pool`, `ip_version`	Direccio IP de UE actualm asignad desde u pool
`ue_pool_addresses_total`	Gauge	`pool`, `ip_version`	Total de direccio IP de UE disponib en un po
`ue_pool_addresses_utilization_ratio`	Gauge	`pool`, `ip_version`	Fracción (0.0–1.0 un pool actualm asignad
`ue_ip_allocation_failures_total`	Counter	`ip_version`, `reason`	Fallos en asignaci de IP de (por ejemplo agotami del pool colisión estática

Uso:

```
# Pools por encima del 80% de utilización
ue_pool_addresses_utilization_ratio > 0.8

# Tasa de fallos de asignación por razón
sum(rate(ue_ip_allocation_failures_total[5m])) by (reason)
```

Contadores de Mensajes

Mensajes S5/S8 (GTP-C):

Nombre de Métrica	Tipo	Etiquetas	Descripción
`s5s8_inbound_messages_total`	Counter	`message_type`	Total de mensajes S5/S8 entrantes
`s5s8_outbound_messages_total`	Counter	`message_type`	Total de mensajes S5/S8 salientes
`s5s8_inbound_errors_total`	Counter	`message_type`	Errores de procesamiento S5/S8 entrantes
`s5s8_outbound_errors_total`	Counter	`message_type`	Errores de procesamiento S5/S8 salientes

Tipos de Mensajes:

- `create_session_request`
- `create_session_response`

- `delete_session_request`
- `delete_session_response`
- `create_bearer_request`
- `delete_bearer_request`

Mensajes Sxb (PFCP):

Nombre de Métrica	Tipo	Etiquetas	Descrip
`sxb_inbound_messages_total`	Counter	`message_type`	Total de mensajes PFCP entrantes
`sxb_outbound_messages_total`	Counter	`message_type`	Total de mensajes PFCP sali
`sxb_inbound_errors_total`	Counter	`message_type`	Errores d procesam PFCP entrantes
`sxb_outbound_errors_total`	Counter	`message_type`	Errores d procesam PFCP sali
`sxb_outbound_responses_total`	Counter	`message_type`, `cause_code_class`, `peer_ip`	Respuest PFCP enviadas categoriz por clase código de causa PF par UPF

Tipos de Mensajes:

- `association_setup_request`
- `association_setup_response`
- `heartbeat_request`
- `heartbeat_response`
- `session_establishment_request`
- `session_establishment_response`
- `session_modification_request`
- `session_deletion_request`

Mensajes Gx (Diameter):

Nombre de Métrica	Tipo	Etiquetas	Descrip
`gx_inbound_messages_total`	Counter	`message_type`	Total de mensajes Diameter entrantes
`gx_outbound_messages_total`	Counter	`message_type`	Total de mensajes Diameter salientes
`gx_inbound_errors_total`	Counter	`message_type`	Errores d procesam Diameter entrantes
`gx_outbound_errors_total`	Counter	`message_type`	Errores d procesam Diameter salientes
`gx_outbound_responses_total`	Counter	`message_type`, `result_code_class`, `diameter_host`	Respuest Diameter enviadas categoriz por clase código de resultado host par

Tipos de Mensajes:

- `gx_CCA` (Respuesta de Control de Crédito)
- `gx_CCR` (Solicitud de Control de Crédito)
- `gx_RAA` (Respuesta de Reautenticación)
- `gx_RAR` (Solicitud de Reautenticación)

Clases de Códigos de Resultado (para `gx_outbound_responses_total`):

- `2xxx` - Respuestas de éxito (por ejemplo, 2001 DIAMETER_SUCCESS)
- `3xxx` - Errores de protocolo (por ejemplo, 3001 DIAMETER_COMMAND_UNSUPPORTED)
- `4xxx` - Fallos transitorios (por ejemplo, 4001 DIAMETER_AUTHENTICATION_REJECTED)
- `5xxx` - Fallos permanentes (por ejemplo, 5012 DIAMETER_UNABLE_TO_COMPLY)

Ejemplos de Uso:

```
# Monitorear la tasa de éxito de respuestas Gx
sum(rate(gx_outbound_responses_total{result_code_class="2xxx"}[5m]))
sum(rate(gx_outbound_responses_total[5m])) * 100

# Rastrear fallos por host PCRF
rate(gx_outbound_responses_total{result_code_class!="2xxx"}[5m]) by (

# Contar el total de mensajes exitosos de Reautenticación
gx_outbound_responses_total{message_type="gx_RAA",result_code_class="

# Alertar sobre alta tasa de fallos a un PCRF específico
rate(gx_outbound_responses_total{result_code_class=~"4xxx|5xxx",diame
[5m]) > 0.1
```

Mensajes Gy (Diameter):

Contadores de mensajes de carga en línea Gy (OCS). Vea Diameter Gy para la interfaz.

Nombre de Métrica	Tipo	Etiquetas	Descrip
`gy_inbound_messages_total`	Counter	`message_type`	Total de mensajes entrantes
`gy_outbound_messages_total`	Counter	`message_type`	Total de mensajes salientes
`gy_inbound_errors_total`	Counter	`message_type`	Errores d procesam Gy entran
`gy_outbound_errors_total`	Counter	`message_type`	Errores d procesam Gy salien
`gy_inbound_responses_total`	Counter	`cc_request_type`, `result_code_class`, `diameter_host`	Respuest Control d Crédito recibidas OCS, por solicitud responde clase de de resulta host OCS
`gy_outbound_responses_total`	Counter	`message_type`, `result_code_class`, `diameter_host`	Respuest enviadas OCS (Res de Reautent a un RAR OCS), por de código

Nombre de Métrica	Tipo	Etiquetas	Descrip
			resultado host OCS
`gy_usage_clamped_total`	Counter	-	CCR-Ts cu Uso-Serv Unit fue limitado a porque el reportad más que medido. U valor dist de cero significa OCS está facturad

Tipos de Mensajes (`message_type`):

- `ro_CCR` (Solicitud de Control de Crédito)
- `ro_CCA` (Respuesta de Control de Crédito)
- `ro_RAR` (Solicitud de Reautenticación)
- `ro_RAA` (Respuesta de Reautenticación)

Tipos de Solicitudes de CC (`cc_request_type`, para `gy_inbound_responses_total`):

- `initial` - respuesta a un CCR-I (inicio de sesión, primera concesión de cuota)
- `update` - respuesta a un CCR-U (informe de uso, siguiente concesión de cuota)
- `termination` - respuesta a un CCR-T (fin de sesión, uso final)
- `event` - respuesta a un CCR basado en eventos

Clases de Códigos de Resultado (para `gy_inbound_responses_total` y `gy_outbound_responses_total`): las mismas clases que para Gx (`2xxx`, `3xxx`, `4xxx`, `5xxx`, `other`). En Gy, `4012` DIAMETER_CREDIT_LIMIT_REACHED es un `4xxx` y `5030` DIAMETER_USER_UNKNOWN es un `5xxx`.

La `result_code_class` es el Código de Resultado de nivel superior del CCA. Un OCS puede responder `2001` en el nivel superior y aún así negar o redirigir un único servicio en su Control de Crédito de Múltiples Servicios.

Ejemplos de Uso:

```
# Tasa de éxito de CCA por tipo de solicitud
sum by (cc_request_type) (rate(gy_inbound_responses_total{result_code
[5m]))
  / sum by (cc_request_type) (rate(gy_inbound_responses_total[5m])) *

# Fallos en CCR-Is (nuevas sesiones que el OCS rechazó), por host OCS
sum by (diameter_host)
(rate(gy_inbound_responses_total{cc_request_type="initial",result_cod
[5m]))

# CCRs enviados sin CCA de vuelta (timeouts del OCS o respuestas perd
sum by (instance) (rate(gy_outbound_messages_total{message_type="ro_C
  - sum by (instance) (rate(gy_inbound_responses_total[5m]))

# Respuestas de Reautenticación enviadas al OCS que no fueron exitosa
rate(gy_outbound_responses_total{message_type="ro_RAA",result_code_cl
[5m])
```

Mensajes Gn/Gp (GTPv1-C):

Contadores de mensajes de control de Gn/Gp GGSN (interoperabilidad SGSN 2G/3G). Vea Interfaz Gn.

Nombre de Métrica	Tipo	Etiquetas	Descripción
`gn_inbound_messages_total`	Counter	`message_type`	Total de mensajes Gn/Gp entrantes (desde SGSN)
`gn_outbound_messages_total`	Counter	`message_type`	Total de mensajes Gn/Gp salientes (hacia SGSN)
`gn_inbound_errors_total`	Counter	`message_type`	Errores de procesamiento Gn/Gp entrantes
`gn_outbound_errors_total`	Counter	`message_type`	Respuestas de error Gn/Gp enviadas al SGSN

Manejo de Errores:

Nombre de Métrica	Tipo	Etiquetas	Descripción
`rescues_total`	Counter	`module`, `function`	Total de bloques de rescate alcanzados (manejo de excepciones)

Métricas de Latencia

Duración del Procesamiento de Mensajes Entrantes:

Nombre de Métrica	Tipo	Etiquetas	
`s5s8_inbound_handling_duration`	Histogram	`request_message_type`	
`gn_inbound_handling_duration`	Histogram	`request_message_type`	
`sxb_inbound_handling_duration`	Histogram	`request_message_type`	
`gx_inbound_handling_duration`	Histogram	`request_message_type`	

Nombre de Métrica	Tipo	Etiquetas	
			e r
`gy_inbound_handling_duration`	Histogram	`request_message_type`	T r r ((c c e r

Duración de Transacciones Salientes:

Nombre de Métrica	Tipo	Etiquetas
`s5s8_outbound_transaction_duration`	Histogram	`request_message_type`
`gn_outbound_transaction_duration`	Histogram	`request_message_type`
`sxb_outbound_transaction_duration`	Histogram	`request_message_type`
`gx_outbound_transaction_duration`	Histogram	`request_message_type`
`gy_outbound_transaction_duration`	Histogram	`request_message_type`

Buckets (segundos):

- Valores: 0.0001, 0.0005, 0.001, 0.005, 0.01, 0.05, 0.1, 0.5, 1.0, 5.0
- (100µs, 500µs, 1ms, 5ms, 10ms, 50ms, 100ms, 500ms, 1s, 5s)

Uso:

```
# Latencia del percentil 95 S5/S8
histogram_quantile(0.95,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)

# Latencia promedio de PFCP
rate(sxb_inbound_handling_duration_sum[5m]) /
rate(sxb_inbound_handling_duration_count[5m])
```

Monitoreo de Salud de UPF

Métricas de Pares UPF:

Nombre de Métrica	Tipo	Etiquetas	Descripción
`upf_peers_total`	Gauge	-	Total de pares UPF registrados
`upf_peers_healthy`	Gauge	-	Número de pares UPF saludables (asociados + latidos OK)
`upf_peers_unhealthy`	Gauge	-	Número de pares UPF no saludables
`upf_peers_associated`	Gauge	-	N��mero de pares UPF con asociación PFCP activa
`upf_peers_unassociated`	Gauge	-	Número de pares UPF sin asociación PFCP
`upf_peer_associated`	Gauge	`peer_ip`	Si un UPF específico tiene una asociación PFCP activa (1/0)
`upf_peer_healthy`	Gauge	`peer_ip`	Estado de salud de un UPF específico (1=saludable, 0=no saludable)
`upf_peer_missed_heartbeats`	Gauge	`peer_ip`	Latidos perdidos consecutivos para un UPF específico

Nombre de Métrica	Tipo	Etiquetas	Descripción
`upf_heartbeat_rtt`	Histogram	`peer_ip`	Tiempo de ida y vuelta de solicitud/respuesta de latido PFCP (segundos)

Uso:

```
# Monitorear la salud del pool de UPF
upf_peers_healthy / upf_peers_total

# Alertar sobre UPFs no saludables
upf_peers_unhealthy > 0

# Rastrear la salud de un UPF específico
upf_peer_healthy{peer_ip="10.98.0.20"}

# Identificar UPFs con problemas de latido
upf_peer_missed_heartbeats > 2
```

Ejemplos de Alertas:

```yaml
# Alertar cuando un UPF se cae
- alert: UPF_Peer_Down
  expr: upf_peer_healthy == 0
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "El UPF {{ $labels.peer_ip }} está caído"
    description: "El par UPF no responde a los latidos PFCP"

# Alertar cuando múltiples UPFs están caídos
- alert: UPF_Pool_Degraded
  expr: (upf_peers_healthy / upf_peers_total) < 0.5
  for: 2m
  labels:
    severity: critical
  annotations:
    summary: "Pool de UPF degradado"
    description: "Solo {{ $value | humanizePercentage }} de los
UPFs son saludables"

# Advertencia sobre latidos perdidos
- alert: UPF_Heartbeat_Issues
  expr: upf_peer_missed_heartbeats > 2
  for: 30s
  labels:
    severity: warning
  annotations:
    summary: "UPF {{ $labels.peer_ip }} problemas de latido"
    description: "{{ $value }} latidos perdidos consecutivos"
```

Monitoreo de Salud de P-CSCF

Métricas del Servidor P-CSCF:

Nombre de Métrica	Tipo	Etiquetas	Descripción
`pcscf_fqdns_total`	Gauge	-	Total de FQDNs de P-CSCF que se están monitoreando
`pcscf_fqdns_resolved`	Gauge	-	FQDNs de P-CSCF resueltos con éxito a través de DNS
`pcscf_fqdns_failed`	Gauge	-	FQDNs de P-CSCF que fallaron en la resolución DNS
`pcscf_servers_total`	Gauge	-	Total de servidores P-CSCF descubiertos
`pcscf_servers_healthy`	Gauge	`fqdn`	Servidores P-CSCF saludables por FQDN
`pcscf_servers_unhealthy`	Gauge	`fqdn`	Servidores P-CSCF no saludables por FQDN

Vea: Guía de Monitoreo de P-CSCF para un seguimiento detallado de la salud de IMS.

Conectividad de Pares Diameter

Sondeado periódicamente desde la pila Diameter.

Nombre de Métrica	Tipo	Etiquetas	Descripción
`diameter_peers_connected`	Gauge	`application`	Número de pares Diameter actualmente conectados, por aplicación (`gx`/`gy`/`all`)

Uso:

```
# Alertar cuando no hay pares Gx (PCRF) conectados
diameter_peers_connected{application="gx"} == 0
```

Métricas de Licencia

Estado de la Licencia:

Nombre de Métrica	Tipo	Descripción
`license_status`	Gauge	Estado actual de la licencia (1 = válido, 0 = inválido)

Uso:

```
# Verificar si la licencia es válida
license_status == 1

# Alertar sobre licencia inválida
license_status == 0
```

Ejemplo de Alerta:

```
- alert: PGW_C_License_Invalid
  expr: license_status == 0
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "Licencia PGW-C inválida o expirada"
    description: "El estado de la licencia es inválido - se están
bloqueando las solicitudes de creación de sesión"
```

Impacto de Licencia Inválida:

Cuando la licencia es inválida o el servidor de licencias no es accesible, **las solicitudes de creación de sesión serán rechazadas** con el código de causa GTP-C **"No hay recursos disponibles" (73)**. Esto es visible en las capturas de paquetes como se muestra a continuación:

Captura de Wireshark mostrando la respuesta de creación de sesión con el código de causa "No hay recursos disponibles" cuando la licencia es inválida

Notas:

- Nombre del producto registrado con el servidor de licencias: `omnipgwc`
- La URL del servidor de licencias está configurada en `config/runtime.exs` bajo `:license_client`

- Cuando la licencia es inválida (`license_status == 0`), las solicitudes de creación de sesión están bloqueadas con el código de causa GTP-C 73 (No hay recursos disponibles)
- La interfaz de usuario y la monitorización siguen siendo accesibles independientemente del estado de la licencia
- Los pares de Diameter, GTP-C y PFCP continúan manteniendo conexiones
- Las sesiones existentes no se ven afectadas; solo se bloquea la creación de nuevas sesiones

Métricas del Sistema

Métricas de la VM de Erlang:

Nombre de Métrica	Tipo	Descripción
`vm_memory_total`	Gauge	Memoria total de la VM (bytes)
`vm_memory_processes`	Gauge	Memoria utilizada por los procesos
`vm_memory_system`	Gauge	Memoria utilizada por el sistema
`vm_system_process_count`	Gauge	Total de procesos de Erlang
`vm_system_port_count`	Gauge	Total de puertos abiertos

Configuración de Prometheus

Configuración de Scrape

Agrega OmniPGW a `prometheus.yml`:

```yaml
# prometheus.yml
global:
  scrape_interval: 15s
  evaluation_interval: 15s

scrape_configs:
  - job_name: 'omnipgw'
    static_configs:
      - targets: ['10.0.0.20:9090']
        labels:
          instance: 'omnipgw-01'
          environment: 'production'
          site: 'datacenter-1'
```

Múltiples Instancias de OmniPGW

```yaml
scrape_configs:
  - job_name: 'omnipgw'
    static_configs:
      - targets:
          - '10.0.0.20:9090'
          - '10.0.0.21:9090'
          - '10.0.0.22:9090'
        labels:
          environment: 'production'
```

Descubrimiento de Servicios

Kubernetes:

```yaml
scrape_configs:
  - job_name: 'omnipgw'
    kubernetes_sd_configs:
      - role: pod
    relabel_configs:
      - source_labels: [__meta_kubernetes_pod_label_app]
        action: keep
        regex: omnipgw
      - source_labels: [__meta_kubernetes_pod_ip]
        target_label: __address__
        replacement: '${1}:9090'
```

Verificación

Prueba de scrape:

```
# Verificar objetivos de Prometheus
curl http://prometheus:9090/api/v1/targets

# Consultar una métrica
curl 'http://prometheus:9090/api/v1/query?
query=teid_registry_count'
```

Dashboards de Grafana

Configuración del Dashboard

1. Agregar Fuente de Datos de Prometheus:

```
Configuración → Fuentes de Datos → Agregar fuente de datos →
Prometheus
URL: http://prometheus:9090
```

2. Importar Dashboard:

Crea un nuevo dashboard o importa desde JSON.

Paneles Clave

Panel 1: Sesiones Activas

```
# Consulta
teid_registry_count

# Tipo de Panel: Gauge
# Umbrales:
#   Verde: < 5000
#   Amarillo: 5000-8000
#   Rojo: > 8000
```

Panel 2: Tasa de Sesiones

```
# Consulta
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m])

# Tipo de Panel: Gráfico
# Unidad: solicitudes/seg
```

Panel 3: Utilización del Pool de IP

```
# Consulta (para subred /24 con 254 IPs)
(address_registry_count / 254) * 100

# Tipo de Panel: Gauge
# Unidad: porcentaje (0-100)
# Umbrales:
#   Verde: < 70%
#   Amarillo: 70-85%
#   Rojo: > 85%
```

Panel 4: Latencia de Mensajes (Percentil 95)

```
# Consulta
histogram_quantile(0.95,

rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m])
)

# Tipo de Panel: Gráfico
# Unidad: milisegundos
```

Panel 5: Tasa de Errores

```
# Consulta
rate(s5s8_inbound_errors_total[5m])

# Tipo de Panel: Gráfico
# Unidad: errores/seg
# Umbral de Alerta: > 0.1
```

Panel 6: Tasa de Éxito de Respuestas Gx

```
# Consulta: Calcular el porcentaje de respuestas Gx exitosas
sum(rate(gx_outbound_responses_total{result_code_class="2xxx"}
[5m])) /
sum(rate(gx_outbound_responses_total[5m])) * 100

# Tipo de Panel: Gauge
# Unidad: porcentaje (0-100)
# Umbrales:
#   Verde: > 95%
#   Amarillo: 90-95%
#   Rojo: < 90%
```

Alternativa - Desglose por Clase de Código de Resultado:

```
# Consulta: Mostrar conteos de respuestas por clase de código de
resultado
sum(rate(gx_outbound_responses_total[5m])) by (result_code_class)

# Tipo de Panel: Gráfico de Pastel o Gráfico de Barras
# Leyenda: {{ result_code_class }}
```

Alternativa - Estado de Respuesta por PCRF:

```
# Consulta: Mostrar respuestas por host PCRF
sum(rate(gx_outbound_responses_total[5m])) by (diameter_host,
result_code_class)

# Tipo de Panel: Gráfico de Barras Apiladas
# Leyenda: {{ diameter_host }} - {{ result_code_class }}
```

Panel 7: Estado de Salud del UPF

```
# Consulta: Porcentaje de salud general del pool
(upf_peers_healthy / upf_peers_total) * 100

# Tipo de Panel: Gauge
# Unidad: porcentaje (0-100)
# Umbrales:
#   Verde: 100%
#   Amarillo: 50-99%
#   Rojo: < 50%
```

Alternativa - Estado por UPF:

```
# Consulta: Salud individual del UPF
upf_peer_healthy

# Tipo de Panel: Estado
# Mapeos:
#   1 = "UP" (Verde)
#   0 = "DOWN" (Rojo)
```

Ejemplo Completo de Dashboard

```
{
  "dashboard": {
    "title": "OmniPGW - Dashboard de Operaciones",
    "panels": [
      {
        "title": "Sesiones Activas",
        "targets": [
          {
            "expr": "teid_registry_count",
            "legendFormat": "Sesiones Activas"
          }
        ],
        "type": "graph"
      },
      {
        "title": "Tasa de Creación de Sesiones",
        "targets": [
          {
            "expr":
"rate(s5s8_inbound_messages_total{message_type=\"create_session_reque
[5m])",
            "legendFormat": "Sesiones/seg"
          }
        ],
        "type": "graph"
      },
      {
        "title": "Utilización del Pool de IP",
        "targets": [
          {
            "expr": "(address_registry_count / 254) * 100",
            "legendFormat": "Uso del Pool %"
          }
        ],
        "type": "gauge"
      },
      {
        "title": "Latencia de Mensajes (p95)",
        "targets": [
          {
            "expr": "histogram_quantile(0.95,
```

```
rate(s5s8_inbound_handling_duration_bucket[5m]))",
            "legendFormat": "S5/S8 p95"
          },
          {
            "expr": "histogram_quantile(0.95,
rate(sxb_inbound_handling_duration_bucket[5m]))",
            "legendFormat": "PFCP p95"
          }
        ],
        "type": "graph"
      }
    ]
  }
}
```

Alertas

Reglas de Alerta

Crea `omnipgw_alerts.yml`:

```yaml
groups:
  - name: omnipgw
    interval: 30s
    rules:
      # Alertas de Conteo de Sesiones
      - alert: OmniPGW_HighSessionCount
        expr: teid_registry_count > 8000
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Conteo alto de sesiones en OmniPGW"
          description: "{{ $value }} sesiones activas (umbral:
8000)"

      - alert: OmniPGW_SessionCountCritical
        expr: teid_registry_count > 9500
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Conteo crítico de sesiones en OmniPGW"
          description: "{{ $value }} sesiones activas acercándose
a la capacidad"

      # Alertas de Pool de IP
      - alert: OmniPGW_IPPoolUtilizationHigh
        expr: (address_registry_count / 254) * 100 > 80
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Utilización alta del pool de IP en OmniPGW"
          description: "Pool de IP {{ $value }}% utilizado"

      - alert: OmniPGW_IPPoolExhausted
        expr: address_registry_count >= 254
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "Pool de IP agotado en OmniPGW"
          description: "No hay IPs disponibles para asignación"
```

```
      # Alertas de Tasa de Errores
      - alert: OmniPGW_HighErrorRate
        expr: rate(s5s8_inbound_errors_total[5m]) > 0.1
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Tasa de errores alta en OmniPGW"
          description: "{{ $value }} errores/seg en la interfaz
S5/S8"

      - alert: OmniPGW_GxErrorRate
        expr: rate(gx_inbound_errors_total[5m]) > 0.05
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Errores Gx en OmniPGW"
          description: "{{ $value }} errores de Diameter/seg"

      # Alertas de Respuestas Gx
      - alert: OmniPGW_GxResponseFailureRate
        expr: |

sum(rate(gx_outbound_responses_total{result_code_class!="2xxx"}
[5m])) /
          sum(rate(gx_outbound_responses_total[5m])) > 0.1
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Tasa alta de fallos en respuestas Gx de
OmniPGW"
          description: "{{ $value | humanizePercentage }} de las
respuestas Gx son fallos (códigos de resultado no-2xxx)"

      - alert: OmniPGW_GxPCRFFailures
        expr:
rate(gx_outbound_responses_total{result_code_class=~"4xxx|5xxx"}
[5m]) by (diameter_host) > 0.05
        for: 3m
        labels:
          severity: warning
```

```
        annotations:
          summary: "PCRF {{ $labels.diameter_host }} recibiendo
respuestas de fallo"
          description: "{{ $value }} respuestas de fallo/seg al
PCRF {{ $labels.diameter_host }}"

      # Alertas de Salud del UPF
      - alert: OmniPGW_UPF_PeerDown
        expr: upf_peer_healthy == 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "El par UPF {{ $labels.peer_ip }} está caído"
          description: "UPF no responde a los latidos de PFCP"

      - alert: OmniPGW_UPF_PoolDegraded
        expr: (upf_peers_healthy / upf_peers_total) < 0.5
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Pool de UPF degradado"
          description: "{{ $value | humanizePercentage }} de los
UPFs están sanos (< 50%)"

      - alert: OmniPGW_UPF_HeartbeatFailures
        expr: upf_peer_missed_heartbeats > 2
        for: 30s
        labels:
          severity: warning
        annotations:
          summary: "Fallos de latidos en UPF {{ $labels.peer_ip
}}"
          description: "{{ $value }} latidos consecutivos
perdidos"

      - alert: OmniPGW_UPF_AllDown
        expr: upf_peers_healthy == 0 and upf_peers_total > 0
        for: 30s
        labels:
          severity: critical
        annotations:
          summary: "Todos los pares UPF están caídos"
```

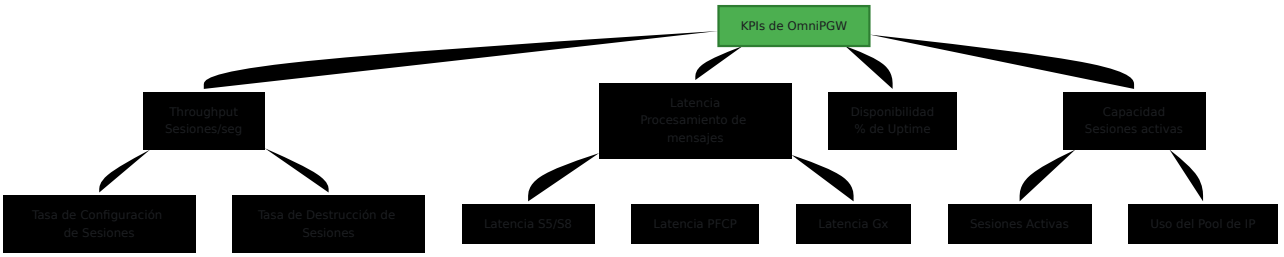
```
          description: "No hay UPFs sanos disponibles para la
creación de sesiones"

      # Alertas de Latencia
      - alert: OmniPGW_HighLatency
        expr: |
          histogram_quantile(0.95,
            rate(s5s8_inbound_handling_duration_bucket[5m])
          ) > 100000
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Alta latencia de mensajes en OmniPGW"
          description: "latencia p95 {{ $value }}µs (> 100ms)"

      # Alertas del Sistema
      - alert: OmniPGW_HighMemoryUsage
        expr: vm_memory_total > 2000000000
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Alto uso de memoria en OmniPGW"
          description: "VM utilizando {{ $value | humanize }}B de
memoria"

      - alert: OmniPGW_HighProcessCount
        expr: vm_system_process_count > 100000
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Alto conteo de procesos en OmniPGW"
          description: "{{ $value }} procesos de Erlang (posible
fuga)"
```

Configuración de AlertManager

```yaml
# alertmanager.yml
global:
  resolve_timeout: 5m

route:
  receiver: 'ops-team'
  group_by: ['alertname', 'instance']
  group_wait: 10s
  group_interval: 10s
  repeat_interval: 12h

  routes:
    - match:
        severity: critical
      receiver: 'pagerduty'

    - match:
        severity: warning
      receiver: 'slack'

receivers:
  - name: 'ops-team'
    email_configs:
      - to: 'ops@example.com'

  - name: 'slack'
    slack_configs:
      - api_url:
'https://hooks.slack.com/services/YOUR/SLACK/WEBHOOK'
        channel: '#omnipgw-alerts'
        title: 'Alerta OmniPGW: {{ .GroupLabels.alertname }}'
        text: '{{ range .Alerts }}{{ .Annotations.description }}{{
end }}'

  - name: 'pagerduty'
    pagerduty_configs:
      - service_key: 'YOUR_PAGERDUTY_KEY'
```

Monitoreo de Rendimiento

Indicadores Clave de Rendimiento (KPI)



Consultas de Throughput

Tasa de Configuración de Sesiones:

```
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m])
```

Tasa de Destrucción de Sesiones:

```
rate(s5s8_inbound_messages_total{message_type="delete_session_request
[5m])
```

Crecimiento Neto de Sesiones:

```
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m]) -
rate(s5s8_inbound_messages_total{message_type="delete_session_request
[5m])
```

Análisis de Latencia

Latencia de Procesamiento de Mensajes (Percentiles):

```
# p50 (Mediana)
histogram_quantile(0.50,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)

# p95
histogram_quantile(0.95,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)

# p99
histogram_quantile(0.99,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)
```

Desglose de Latencia por Tipo de Mensaje:

```
histogram_quantile(0.95,
  rate(s5s8_inbound_handling_duration_bucket[5m])
) by (request_message_type)
```

Tendencia de Capacidad

Tendencia de Crecimiento de Sesiones (24h):

```
teid_registry_count -
teid_registry_count offset 24h
```

Capacidad Restante:

```
# Para capacidad máxima de 10,000 sesiones
10000 - teid_registry_count
```

Tiempo hasta el Agotamiento de la Capacidad:

```
# Días hasta que se agote la capacidad (basado en la tasa de
crecimiento de 1h)
(10000 - teid_registry_count) /
(rate(teid_registry_count[1h]) * 86400)
```

Solución de Problemas de Métricas

Identificación de Problemas

Problema: Alta Tasa de Rechazo de Sesiones

Consulta:

```
rate(s5s8_inbound_errors_total[5m]) by (message_type)
```

Acción:

- Verificar registros de errores
- Verificar conectividad PCRF (errores Gx)
- Comprobar agotamiento del pool de IP

Problema: Configuración Lenta de Sesiones

Consulta:

```
histogram_quantile(0.95,

rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m])
)
```

Acción:

- Verificar latencia Gx (tiempo de respuesta del PCRF)
- Verificar latencia PFCP (tiempo de respuesta del PGW-U)

- Revisar uso de recursos del sistema

Problema: Fallos de Políticas del PCRF

Consultas:

```
# Tasa general de fallos de respuesta Gx
sum(rate(gx_outbound_responses_total{result_code_class!="2xxx"}
[5m])) /
sum(rate(gx_outbound_responses_total[5m])) * 100

# Desglose por host PCRF
sum(rate(gx_outbound_responses_total[5m])) by (diameter_host,
result_code_class)

# Clases específicas de códigos de resultado
rate(gx_outbound_responses_total{result_code_class="5xxx"}[5m]) by
(diameter_host)
```

Acción:

- Verificar conectividad y salud del PCRF
- Revisar perfiles de suscriptores en el PCRF (errores 5xxx a menudo indican problemas de política)
- Verificar configuración de pares de Diameter
- Revisar registros del PCRF para errores correspondientes
- Para 5012 (DIAMETER_UNABLE_TO_COMPLY), revisar el manejo de Re-Auth-Request

Problema: Sospecha de Fuga de Memoria

Consultas:

```
# Tendencia de memoria total
rate(vm_memory_total[1h])

# Tendencia de memoria de procesos
rate(vm_memory_processes[1h])

# Tendencia de conteo de procesos
rate(vm_system_process_count[1h])
```

Acción:

- Verificar sesiones obsoletas
- Revisar conteos de registro
- Reiniciar si se confirma fuga

Consultas de Depuración

Encontrar Hora de Máximo de Sesiones:

```
max_over_time(teid_registry_count[24h])
```

Comparar Actual vs. Histórico:

```
teid_registry_count /
avg_over_time(teid_registry_count[7d])
```

Identificar Anomalías:

```
abs(
  teid_registry_count -
  avg_over_time(teid_registry_count[1h])
) > 100
```

Mejores Prácticas

Recolección de Métricas

1. **Intervalo de Scrape:** 15-30 segundos (equilibrar granularidad vs. carga)
2. **Retención:** 15+ días para análisis histórico
3. **Etiquetas:** Usar etiquetado consistente (instancia, entorno, sitio)

Diseño de Dashboard

1. **Dashboard de Visión General** - KPIs de alto nivel para NOC
2. **Dashboards Detallados** - Profundización por interfaz
3. **Dashboard de Solución de Problemas** - Métricas de errores y registros

Diseño de Alertas

1. **Evitar Fatiga de Alertas** - Solo alertar sobre problemas accionables
2. **Escalación** - Advertencia → Crítico con severidad creciente
3. **Contexto** - Incluir enlaces a runbooks en descripciones de alertas

---

Documentación Relacionada

Configuración y Configuración

- **Guía de Configuración** - Configuración de métricas de Prometheus, configuración de API REST de OAM
- **Guía de Solución de Problemas** - Uso de métricas para depuración

Métricas de Interfaz

- **Interfaz PFCP** - Métricas de sesión PFCP, monitoreo de salud del UPF
- **Interfaz Diameter Gx** - Métricas de políticas Gx, seguimiento de interacción con PCRF

- **Interfaz Diameter Gy** - Métricas de carga Gy, seguimiento de cuotas, tiempos de espera de OCS
- **Interfaz S5/S8** - Métricas de mensajes GTP-C, comunicación SGW-C

Monitoreo Especializado

- **Monitoreo P-CSCF** - Métricas de descubrimiento P-CSCF, salud IMS
- **Gestión de Sesiones** - Sesiones activas, métricas del ciclo de vida de sesiones
- **Asignación de IP UE** - Métricas de utilización del pool de IP

Volver a la Guía de Operaciones

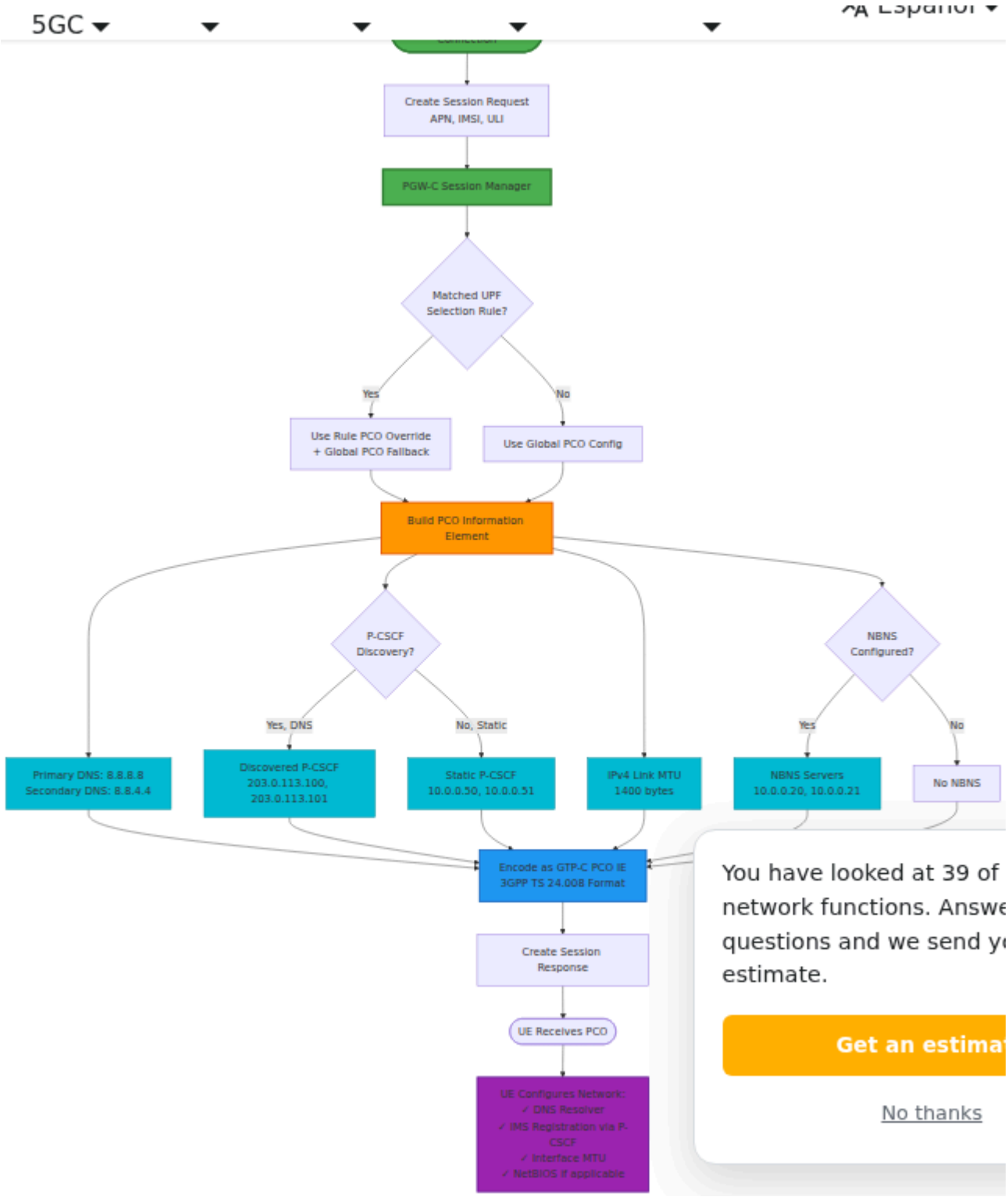
Opciones de Configuración de Protocolo (PCO)

Parámetros de Red Entregados al UE

OmniPGW de Omnitouch Network Services

Descripción General

PCO (Opciones de Configuración de Protocolo) son parámetros de red enviados al UE (dispositivo móvil) durante el establecimiento de la conexión PDN. Estos parámetros permiten al UE acceder a servicios de red como DNS, IMS y configurar ajustes de red.



You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima
No thanks

Contenedores PCO que emite OmniPGW (red → MS):

Nombre IE	ID de Contenedor	Descripción	Requerido
Dirección IPv4 del Servidor DNS	0x000D	DNS Primario	Sí
Dirección IPv4 del Servidor DNS	0x000D	DNS Secundario	Opcional
Dirección IPv6 del Servidor DNS	0x0003	DNS Primario/Secundario (IPv6)	Opcional
Dirección IPv4 del P-CSCF	0x000C	P-CSCF para IMS (un contenedor por dirección)	Opcional (IMS)
Dirección IPv6 del P-CSCF	0x0001	P-CSCF para IMS (un contenedor por dirección)	Opcional (IMS)
MTU de Enlace IPv4	0x0010	Unidad máxima de transmisión	Recomendado

> **DNS/NBNS a través de IPCP.** Cuando el UE solicita servidores DNS (y NBNS/WINS) utilizando un **IPCP** (Protocolo de Control de Internet, contenedor `0x8021`) Configure-Request en lugar de un contenedor DNS simple, OmniPGW responde dentro de un IPCP **Configure-Nak** llevando las direcciones configuradas como las opciones IPCP `ms_dns1`/`ms_dns2` y `ms_wins1`/`ms_wins2` (RFC 1877). NBNS/WINS se entrega **solo** a través de esta ruta IPCP — no se emite un contenedor PCO NBNS independiente (`0x0011`). Se utiliza un Configure-Nak (no un Ack) porque el PGW proporciona direcciones que difieren de los marcadores de posición `0.0.0.0` del UE, y la respuesta refleja el Identificador IPCP de la solicitud (RFC 1661 §5).

> **P-CSCF IPv4 e IPv6 / DNS; sin E-CSCF.** OmniPGW responde tanto a solicitudes de dirección P-CSCF IPv4 como IPv6, enroutando cada dirección descubierta o configurada al contenedor que coincide con su familia: las direcciones IPv4 van en `0x000C`, las direcciones IPv6 van en `0x0001`. Una solicitud de P-CSCF IPv6 (`p_cscf_ipv6_address_request`) se sirve desde `p_cscf_ipv6_address_list` (o las direcciones IPv6 devueltas por DNS/AAAA discovery), y una solicitud de DNS IPv6 (`dns_server_ipv6_address_request`) se sirve en el contenedor `0x0003` desde `primary_dns_server_ipv6_address` / `secondary_dns_server_ipv6_address`. Las familias de direcciones nunca se mezclan entre contenedores. No hay manejo de contenedor E-CSCF. Todo lo anterior se aplica igualmente a APCO (PCO Adicional).

Configuración

Configuración Básica

```
# config/runtime.exs
config :pgw_c,
  pco: %{
    # Servidores DNS (requerido)
    primary_dns_server_address: "8.8.8.8",
    secondary_dns_server_address: "8.8.4.4",

    # Servidores DNS IPv6 (opcional, contenedor 0x0003)
    primary_dns_server_ipv6_address: nil,
    secondary_dns_server_ipv6_address: nil,

    # Servidores NBNS (opcional, para dispositivos Windows)
    primary_nbns_server_address: nil,
    secondary_nbns_server_address: nil,

    # Direcciones P-CSCF para IMS/VoLTE (opcional)
    p_cscf_ipv4_address_list: [],   # contenedor 0x000C
    p_cscf_ipv6_address_list: [],   # contenedor 0x0001

    # Descubrimiento Dinámico de P-CSCF (opcional; resuelve
registros A y AAAA)
    p_cscf_discovery_enabled: false,
    p_cscf_discovery_dns_server: nil,
    p_cscf_discovery_timeout_ms: 5000,

    # Tamaño MTU IPv4 (bytes)
    ipv4_link_mtu_size: 1400
  }
```

Parámetros PCO

Direcciones de Servidor DNS

DNS Primario y Secundario:

```
pco: %{
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4"
}
```

Proveedores de DNS Comunes:

Proveedor	Primario	Secundario
Google	8.8.8.8	8.8.4.4
Cloudflare	1.1.1.1	1.0.0.1
Quad9	9.9.9.9	149.112.112.112
OpenDNS	208.67.222.222	208.67.220.220

DNS Privado:

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11"
}
```

Direcciones P-CSCF (IMS)

Para Servicios IMS/VoLTE:

```
pco: %{
  p_cscf_ipv4_address_list: [
    "10.0.0.50",  # P-CSCF Primario (IPv4, contenedor 0x000C)
    "10.0.0.51"   # P-CSCF Secundario
  ],
  # Direcciones P-CSCF IPv6 (contenedor 0x0001) para PDNs IMS
IPv6/IPv4v6
  p_cscf_ipv6_address_list: [
    "2001:db8::50",
    "2001:db8::51"
  ]
}
```

Cada dirección se emite solo en el contenedor que coincide con su familia, y solo cuando el UE solicita esa familia — una solicitud de P-CSCF IPv4 recibe los contenedores `0x000C`, una solicitud de P-CSCF IPv6 recibe los contenedores `0x0001`. Los PDNs IMS de doble pila típicamente solicitan ambos.

P-CSCF (Función de Control de Sesión de Llamadas Proxy):

- Punto de entrada para la señalización IMS
- Requerido para VoLTE, VoWiFi, RCS
- El UE utiliza SIP a través de este servidor

Descubrimiento Dinámico de P-CSCF

Descubrimiento de P-CSCF Basado en DNS:

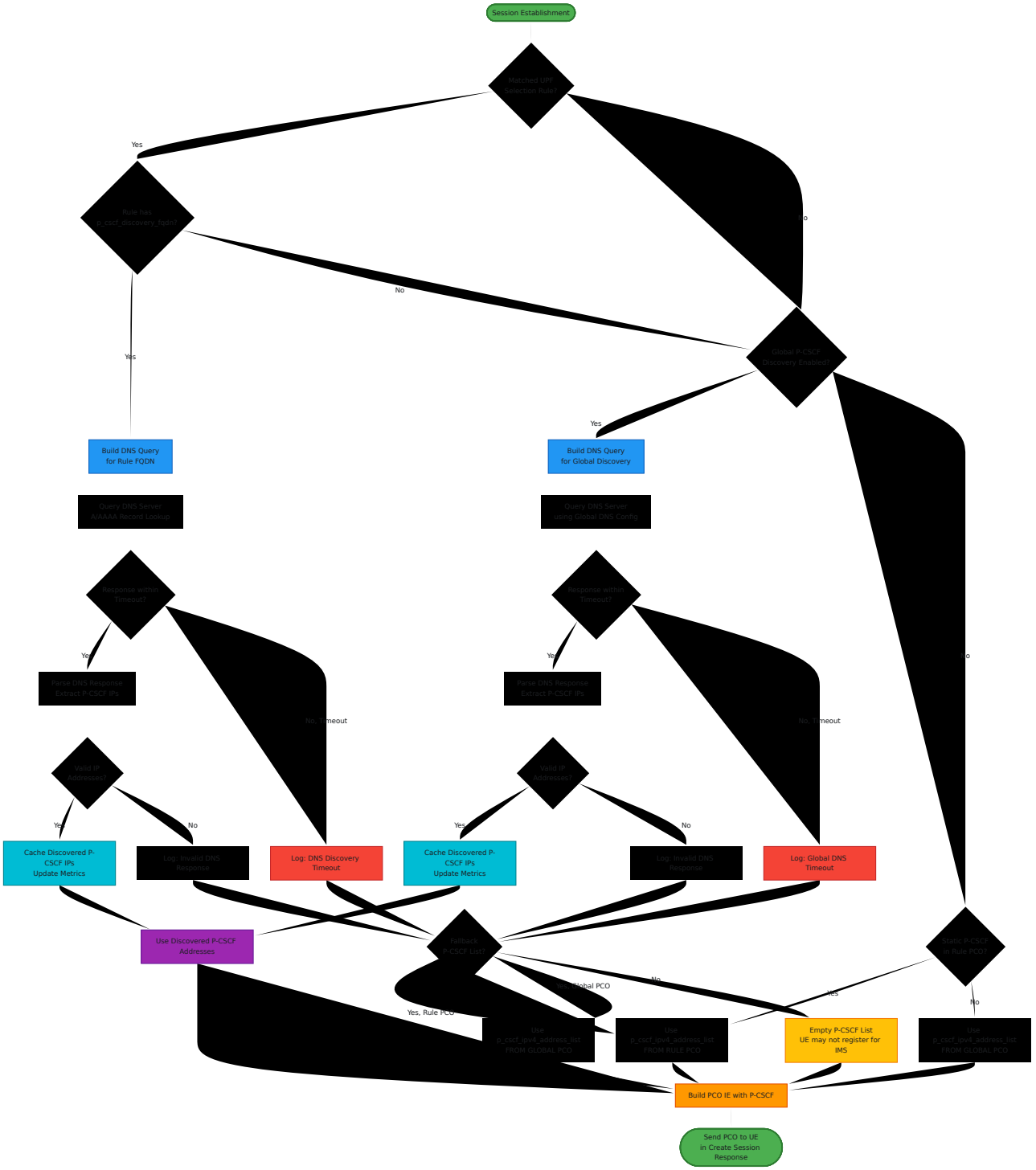
OmniPGW admite el descubrimiento dinámico de P-CSCF a través de consultas DNS como se define en 3GPP TS 23.003 y TS 24.229. Cuando está habilitado, PGW-C puede consultar DNS para direcciones P-CSCF en lugar de usar una configuración estática.

```
pco: %{
  # Habilitar descubrimiento dinámico de P-CSCF
  p_cscf_discovery_enabled: true,

  # Servidor DNS para consultas P-CSCF (como tupla)
  p_cscf_discovery_dns_server: {10, 179, 2, 177},

  # Tiempo de espera para consultas DNS (milisegundos)
  p_cscf_discovery_timeout_ms: 5000,

  # Lista estática de P-CSCF (usada como respaldo si DNS falla)
  p_cscf_ipv4_address_list: ["10.0.0.50"]
}
```

Cómo Funciona:

1. Cuando `p_cscf_discovery_enabled: true`, PGW-C realiza consultas DNS para direcciones P-CSCF
2. La consulta DNS se envía al `p_cscf_discovery_dns_server` configurado
3. Si la consulta DNS tiene éxito, las direcciones P-CSCF descubiertas se envían al UE a través de PCO
4. Si la consulta DNS falla o se agota el tiempo, se vuelve a la lista estática `p_cscf_ipv4_address_list`
5. Consulte Monitoreo de P-CSCF para un monitoreo y métricas detalladas

Flujo de Descubrimiento de P-CSCF



Prioridad de Descubrimiento:

1. **Descubrimiento FQDN por Regla** (Mayor Prioridad) - `p_cscf_discovery_fqdn` en la regla de selección UPF
2. **Descubrimiento DNS Global** - `p_cscf_discovery_enabled: true` en la configuración global de PCO

3. **Lista Estática de PCO por Regla** - `p_cscf_ipv4_address_list` en la anulación de PCO de la regla
4. **Lista Estática de PCO Global** (Respaldo) - `p_cscf_ipv4_address_list` en la configuración global de PCO

Monitoreo:

Todos los intentos de descubrimiento de P-CSCF se registran y se rastrean con métricas:

- Tasas de éxito/fallo de consultas DNS
- Latencia de descubrimiento
- Estadísticas de uso de respaldo
- Métricas de descubrimiento por regla y globales

Consulte Monitoreo de P-CSCF para obtener detalles completos de monitoreo.

Opciones de Configuración:

Parámetro	Tipo	Predeterminado	Descripc
`p_cscf_discovery_enabled`	Booleano	`false`	Habilitar descubrim dinámico d CSCF basa en DNS
`p_cscf_discovery_dns_server`	Tupla (IP)	`nil`	Dirección I servidor D como tupl 4 (por ejer `{10, 179, 177}`)
`p_cscf_discovery_timeout_ms`	Entero	`5000`	Tiempo de espera par consultas en milisegun

Casos de Uso:

- **Despliegues IMS dinámicos** - Las direcciones P-CSCF cambian según la configuración de DNS
- **Balanceo de carga geográfico** - DNS devuelve los servidores P-CSCF más cercanos
- **Alta disponibilidad** - DNS devuelve automáticamente los servidores P-CSCF disponibles
- **Entornos multi-inquilinos** - Diferentes suscriptores obtienen diferentes servidores P-CSCF

Ejemplo: IMS en Producción con Descubrimiento DNS

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11",

  # Habilitar descubrimiento dinámico de P-CSCF
  p_cscf_discovery_enabled: true,
  p_cscf_discovery_dns_server: {10, 179, 2, 177},  # Servidor DNS
de IMS
  p_cscf_discovery_timeout_ms: 3000,

  # Direcciones P-CSCF de respaldo (si DNS falla)
  p_cscf_ipv4_address_list: [
    "10.0.0.50",  # Respaldo primario
    "10.0.0.51"   # Respaldo secundario
  ],

  ipv4_link_mtu_size: 1400
}
```

Descubrimiento P-CSCF por Regla:

El descubrimiento de P-CSCF también se puede configurar por regla de selección UPF. Esto permite que diferentes APNs utilicen diferentes servidores DNS para el descubrimiento de P-CSCF:

```
# En la configuración de selección upf
rules: [
  %{
    name: "IMS Traffic",
    priority: 20,
    match_field: :apn,
    match_regex: "^ims",
    upf_pool: [...],

    # Descubrimiento de P-CSCF por regla
    p_cscf_discovery_fqdn: "pcscf.mnc001.mcc001.3gppnetwork.org"
  }
]
```

Consulte Configuración de Selección UPF para obtener detalles sobre el descubrimiento de P-CSCF por regla.

Véase también: Monitoreo de P-CSCF para monitorear el descubrimiento y la salud de P-CSCF

Servidores NBNS (NetBIOS)

Para Compatibilidad con Dispositivos Windows:

```
pco: %{
  primary_nbns_server_address: "10.0.0.20",
  secondary_nbns_server_address: "10.0.0.21"
}
```

Cuándo Usar:

- Redes empresariales con dispositivos Windows
- Soporte para aplicaciones heredadas
- Resolución de nombres NetBIOS requerida

Tamaño MTU de Enlace

Unidad Máxima de Transmisión:

```
pco: %{
  ipv4_link_mtu_size: 1400  # bytes
}
```

Valores MTU Comunes:

MTU	Caso de Uso
1500	Ethernet estándar (sin túneles)
1400	Sobrecarga de túneles GTP contabilizada
1420	Sobrecarga reducida
1280	MTU mínima de IPv6
1360	Entornos VPN/túnel

Recomendación: Use **1400** para LTE para tener en cuenta la sobrecarga de GTP-U.

Ejemplos de Configuración

APN de Internet

```
pco: %{
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4",
  ipv4_link_mtu_size: 1400
}
```

APN de IMS

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11",
  p_cscf_ipv4_address_list: [
    "10.0.0.50",
    "10.0.0.51"
  ],
  ipv4_link_mtu_size: 1400
}
```

Véase: Monitoreo de P-CSCF para monitorear las tasas de éxito de registro IMS y la salud de P-CSCF

APN Empresarial

```
pco: %{
  primary_dns_server_address: "10.100.0.10",
  secondary_dns_server_address: "10.100.0.11",
  primary_nbns_server_address: "10.100.0.20",
  secondary_nbns_server_address: "10.100.0.21",
  ipv4_link_mtu_size: 1400
}
```

PCO en Mensajes GTP-C

Respuesta a la Creación de Sesión

OmniPGW incluye PCO en el mensaje **Respuesta a la Creación de Sesión**:

```
Create Session Response
├── Cause: Request accepted
├── UE IP Address: 100.64.1.42
├── PCO (Protocol Configuration Options)
│   ├── DNS Server IPv4 Address: 8.8.8.8
│   ├── DNS Server IPv4 Address: 8.8.4.4
│   ├── P-CSCF IPv4 Address: 10.0.0.50
│   ├── P-CSCF IPv4 Address: 10.0.0.51
│   └── IPv4 Link MTU: 1400
```

Procesamiento del UE

El UE recibe PCO y:

1. Configura el resolutor DNS con los servidores proporcionados
2. Se registra con P-CSCF para servicios IMS
3. Establece el MTU de la interfaz al valor especificado

Solución de Problemas

Problema: UE No Puede Resolver DNS

Síntomas:

- UE tiene dirección IP pero no puede acceder a internet
- Las búsquedas DNS fallan

Causas Posibles:

1. Direcciones de servidor DNS incorrectas en la configuración de PCO
2. Servidores DNS no accesibles desde el grupo de IP del UE
3. Firewall bloqueando el tráfico DNS

Resolución:

```
# Probar la accesibilidad del servidor DNS
ping 8.8.8.8

# Probar la resolución DNS desde la red del UE
nslookup google.com 8.8.8.8

# Verificar la configuración de PCO
grep "primary_dns_server_address" config/runtime.exs
```

Problema: Falla el Registro IMS

Síntomas:

- Las llamadas VoLTE fallan
- El UE muestra "No hay registro IMS"

Causas Posibles:

1. Configuración de P-CSCF faltante
2. Direcciones IP de P-CSCF incorrectas
3. P-CSCF no accesible

Resolución:

```
# Verificar la configuración de P-CSCF
pco: %{
  p_cscf_ipv4_address_list: ["10.0.0.50"]  # Asegúrese de que no
esté vacío
}
```

Problema: Problemas de MTU

Síntomas:

- Algunos sitios web cargan, otros no
- Las transferencias de archivos grandes fallan
- Problemas de fragmentación

Causas Posibles:

- MTU demasiado grande para la sobrecarga de túneles
- MTU demasiado pequeña causando fragmentación excesiva

Resolución:

```
# Recomendado: 1400 para túneles GTP
pco: %{
  ipv4_link_mtu_size: 1400
}

# Si aún tiene problemas, intente un valor más bajo
pco: %{
  ipv4_link_mtu_size: 1360
}
```

Mejores Prácticas

Configuración de DNS

1. **Usar Servidores DNS Confiables**
    - Públicos: Google (8.8.8.8), Cloudflare (1.1.1.1)
    - Privados: DNS interno para empresas
2. **Siempre Configurar Secundario**
    - Proporciona redundancia
    - Mejora la confiabilidad
3. **Considerar la Seguridad DNS**
    - Resolutores compatibles con DNSSEC
    - Filtrado DNS para seguridad

Configuración de IMS

1. **Proporcionar Múltiples P-CSCF**
    - Al menos 2 para redundancia
    - Distribución geográfica si es posible
2. **Asegurar Accesibilidad**
    - P-CSCF debe ser accesible desde el grupo de IP del UE
    - Probar conectividad SIP

Optimización de MTU

1. **Tener en Cuenta la Sobrecarga**
    - GTP-U: 36 bytes (IPv4)
    - IPsec: Variable (50-100 bytes)
2. **MTU Estándar para LTE**
    - Recomendado: **1400 bytes**
    - Equilibra el rendimiento y la compatibilidad
3. **Probar de Extremo a Extremo**
    - Descubrimiento de MTU de ruta
    - Probar con paquetes grandes

Documentación Relacionada

Guías de Configuración

- **Guía de Configuración** - Referencia completa de runtime.exs, selección de UPF con anulaciones de PCO
- **Asignación de IP del UE** - Gestión de grupos de IP, asignación basada en APN

- **Monitoreo de P-CSCF** - Monitoreo del descubrimiento de P-CSCF, seguimiento de salud, métricas

Gestión de Sesiones e Interfaces

- **Gestión de Sesiones** - Ciclo de vida de la sesión PDN, establecimiento de portadores
- **Interfaz S5/S8** - Protocolo GTP-C, codificación y entrega de PCO
- **Interfaz PFCP** - Establecimiento de sesión de plano de usuario

IMS y VoLTE

- **Interfaz Diameter Gx** - Control de políticas para portadores IMS
- **Guía de Monitoreo** - Métricas y paneles relacionados con PCO

Volver a la Guía de Operaciones

Descubrimiento y Monitoreo de P-CSCF

Descubrimiento Dinámico del Servidor P-CSCF con Monitoreo en Tiempo Real

OmniPGW de Omnitouch Network Services

Descripción General

Descubrimiento y Monitoreo de P-CSCF (Función de Control de Sesión de Llamadas Proxy) proporciona un descubrimiento dinámico de servidores IMS P-CSCF utilizando consultas DNS SRV con verificación de salud SIP OPTIONS en tiempo real. Esta característica permite:

- **Descubrimiento de P-CSCF por Regla**: Diferentes servidores P-CSCF para diferentes tipos de tráfico
- **Monitoreo Automático**: Proceso en segundo plano que monitorea continuamente la resolución DNS (cada 60 segundos)
- **Verificaciones de Salud SIP OPTIONS**: Verifica que los servidores P-CSCF estén activos a través de pings SIP OPTIONS
  - **TCP Primero**: Intenta SIP OPTIONS a través de TCP (preferido por su fiabilidad)
  - **Recaída a UDP**: Recae a UDP si TCP falla
  - **Seguimiento de Estado**: Marca cada servidor como :up o :down según la respuesta
- **Seguimiento de Salud en Tiempo Real**: La API OAM expone el estado de resolución, las IPs descubiertas y el estado de salud
- **Recaída Elegante**: Estrategia de recaída de tres niveles para máxima fiabilidad
- **Métricas de Prometheus**: Observabilidad completa a través de métricas de Prometheus

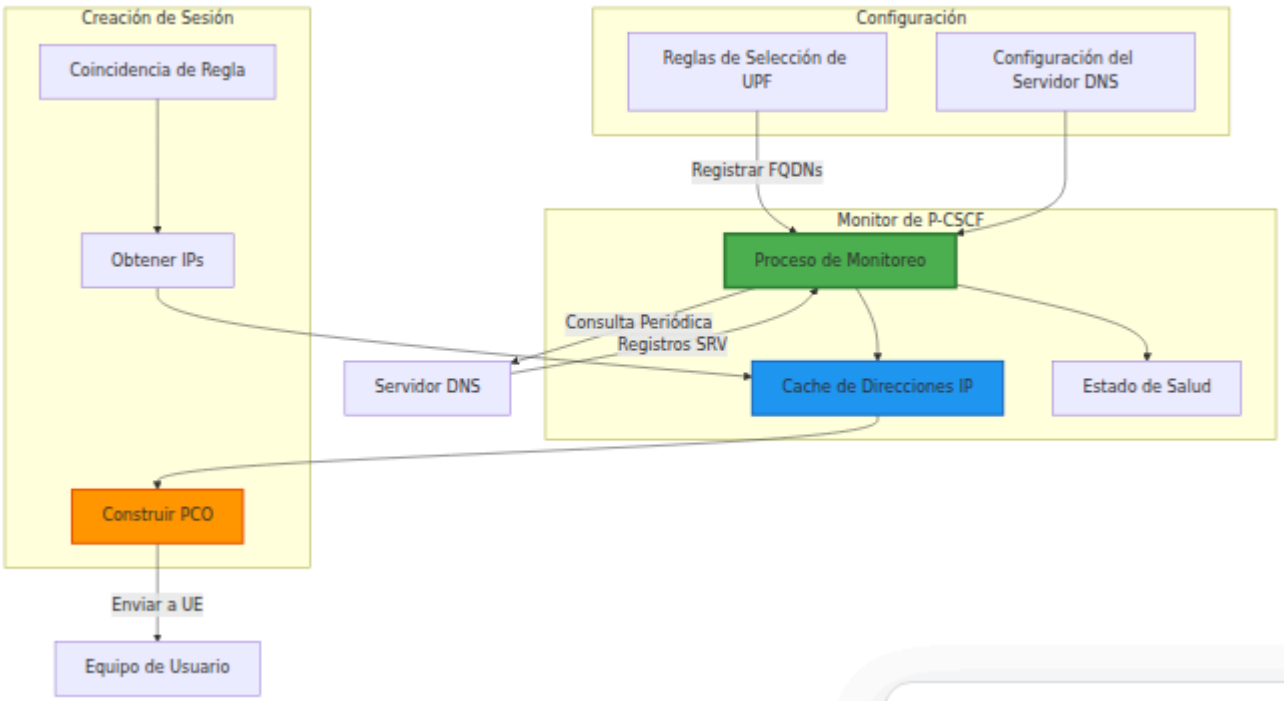


Tabla de Contenidos

1. Inicio Rápido
2. Configuración
3. Cómo Funciona
4. Monitoreo de la API OAM
5. Métricas y Observabilidad
6. Estrategia de Recaída
7. Configuración de DNS
8. Solución de Problemas
9. Mejores Prácticas

Inicio Rápido

Configuración Básica

```
# config/runtime.exs

# Configuración global de PCO (servidor DNS para descubrimiento de
P-CSCF)
config :pgw_c,
  pco: %{
    p_cscf_discovery_dns_server: "192.0.2.177",
    p_cscf_discovery_enabled: true,
    p_cscf_discovery_timeout_ms: 5000
  },

  upf_selection: %{
    rules: [
      # Tráfico IMS - Descubrimiento dinámico de P-CSCF
      %{
        name: "Tráfico IMS",
        priority: 20,
        match_field: :apn,
        match_regex: "^ims",
        upf_pool: [
          %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80}
        ],
        # FQDN de Descubrimiento de P-CSCF (ver Guía de
Configuración para más reglas de selección de UPF)
        p_cscf_discovery_fqdn:
"pcscf.mnc001.mcc001.3gppnetwork.org",
        # Recaída estática (ver Guía de Configuración de PCO)
        pco: %{
          p_cscf_ipv4_address_list: ["203.0.113.100",
"203.0.113.101"]
        }
      }
    ]
  }
```

Consulta la Guía de Configuración para la configuración completa de reglas de selección de UPF y Configuración de PCO para opciones de recaída estática de P-CSCF.

Monitoreo de Acceso

1. Inicia OmniPGW
2. Consulta la API OAM: `curl -k https://localhost:8443/api/pcscf_monitor`
3. Inspecciona el estado de resolución devuelto y las IPs descubiertas (vuelve a ejecutar la solicitud para el estado actual)

Configuración

Configuración Global de Descubrimiento de P-CSCF

Configura el servidor DNS utilizado para el descubrimiento de P-CSCF en la sección PCO:

```
pco: %{
  # Servidor DNS para el descubrimiento de P-CSCF (separado del
DNS dado a UE)
  p_cscf_discovery_dns_server: "192.0.2.177",

  # Habilitar la función de descubrimiento DNS de P-CSCF
  p_cscf_discovery_enabled: true,

  # Tiempo de espera para consultas DNS SRV (milisegundos)
  p_cscf_discovery_timeout_ms: 5000,

  # Direcciones P-CSCF estáticas (recaída global)
  p_cscf_ipv4_address_list: ["203.0.113.146"]
}
```

FQDNs de P-CSCF por Regla

Cada regla de selección de UPF puede especificar su propio FQDN de descubrimiento de P-CSCF:

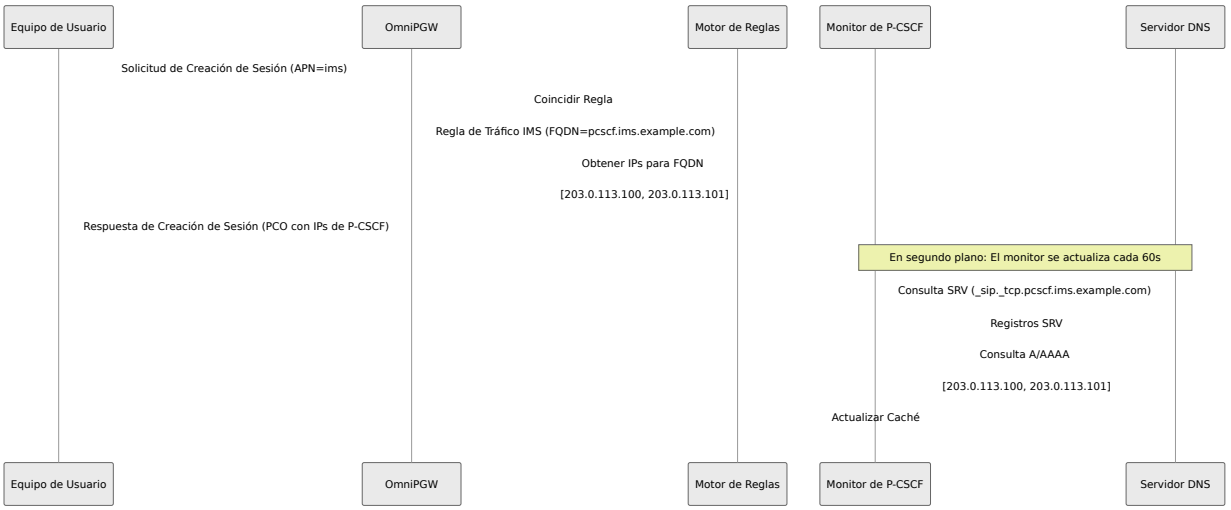
```
upf_selection: %{
  rules: [
    # Tráfico IMS - P-CSCF específico de IMS
    %{
      name: "Tráfico IMS",
      match_field: :apn,
      match_regex: "^ims",
      upf_pool: [...],
      p_cscf_discovery_fqdn:
"pcscf.ims.mnc001.mcc001.3gppnetwork.org",
      pco: %{
        p_cscf_ipv4_address_list: ["203.0.113.100"]  # Recaída
      }
    },

    # Empresa - P-CSCF específico de la empresa
    %{
      name: "Tráfico Empresarial",
      match_field: :apn,
      match_regex: "^enterprise",
      upf_pool: [...],
      p_cscf_discovery_fqdn: "pcscf.enterprise.example.com",
      pco: %{
        p_cscf_ipv4_address_list: ["192.168.1.50"]  # Recaída
      }
    },

    # Internet - Sin descubrimiento de P-CSCF (utiliza la
configuración global)
    %{
      name: "Tráfico de Internet",
      match_field: :apn,
      match_regex: "^internet",
      upf_pool: [...]
      # Sin p_cscf_discovery_fqdn - utiliza la configuración
global de PCO
    }
  ]
}
```

Cómo Funciona

Proceso de Inicio

1. **La Aplicación Inicia**
    - Se inicializa el GenServer del Monitor de P-CSCF
    - El analizador de configuración extrae todos los FQDNs únicos de P-CSCF de las reglas de selección de UPF
2. **Registro de FQDN**
    - Cada FQDN único se registra con el monitor
    - El monitor realiza una consulta inicial de DNS SRV para cada FQDN
    - **Verificación de Salud SIP OPTIONS** (en paralelo para todos los servidores descubiertos):
        - Intenta TCP primero (`SIP/2.0/TCP` en el puerto 5060)
        - Si TCP falla, recae a UDP (`SIP/2.0/UDP` en el puerto 5060)
        - Marca cada servidor como `:up` (responde) o `:down` (sin respuesta/tiempo de espera)
    - Los resultados (IPs, estado de salud o errores) se almacenan en caché con marcas de tiempo
3. **Monitoreo Periódico** (Cada 60 segundos)
    - El monitor actualiza todos los FQDNs
    - Las consultas DNS se ejecutan en segundo plano sin bloquear
    - Para cada servidor descubierto:
        - Envía SIP OPTIONS a través de TCP (tiempo de espera: 5 segundos)
        - Si TCP falla, intenta UDP (tiempo de espera: 5 segundos)
        - Actualiza el estado de salud según la respuesta
    - La caché se actualiza con los últimos resultados DNS y el estado de salud

Flujo de Creación de Sesión



Proceso de Consulta DNS

El monitor utiliza **registros SRV de DNS** para el descubrimiento directo de P-CSCF:

1. **Consulta SRV**: Consulta registros SRV en `_sip._tcp.{fqdn}`
2. **Ordenamiento por Prioridad**: Ordena por prioridad y peso
3. **Extracción de Objetivos**: Extrae nombres de host de los registros SRV
4. **Resolución de Nombres de Host**: Resuelve nombres de host a direcciones IP (registros A/AAAA)
5. **Caché**: Almacena en caché las IPs resueltas con estado y marca de tiempo

Precedencia de Selección de Direcciones P-CSCF

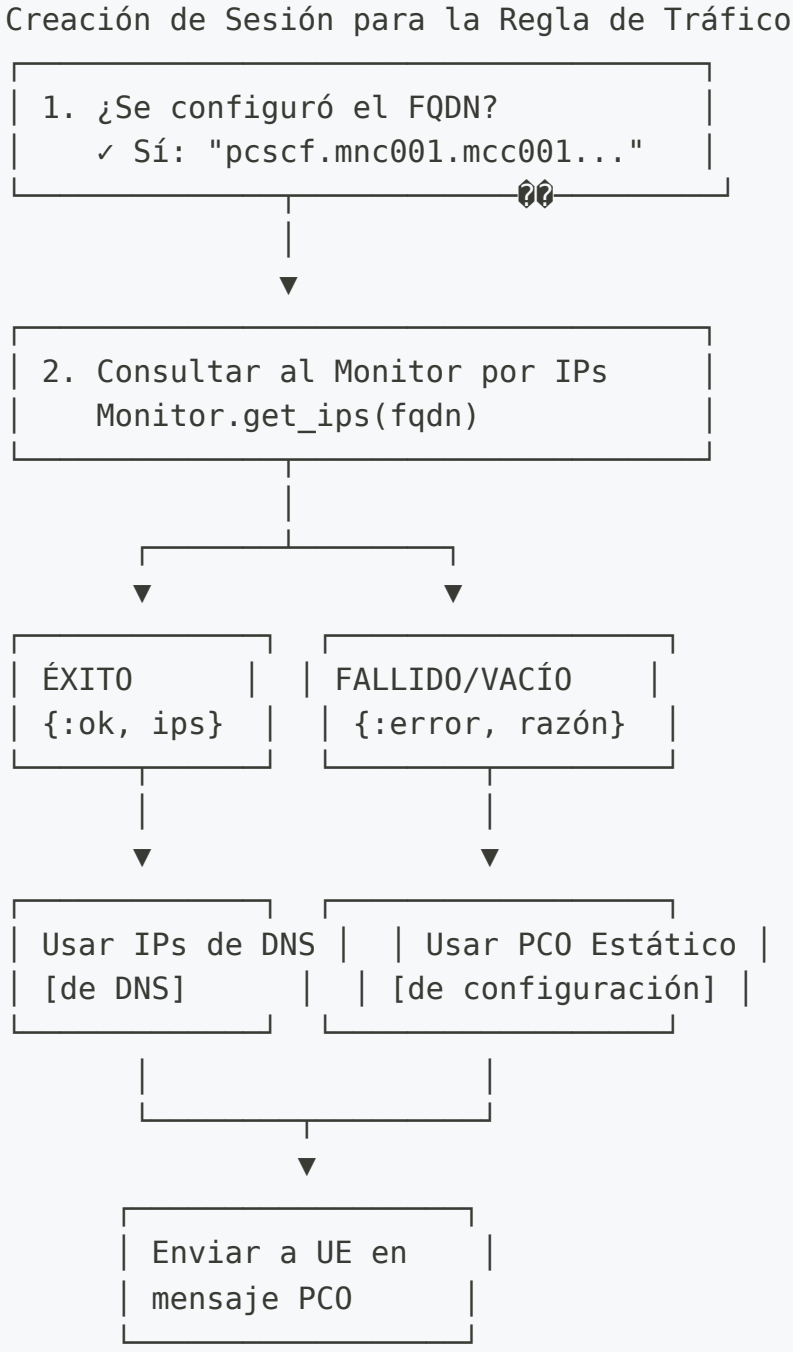
Cuando tanto el FQDN como el PCO estático están configurados en una regla, el FQDN tiene prioridad:

```
%{
  name: "Tráfico IMS",
  p_cscf_discovery_fqdn: "pcscf.mnc001.mcc001.3gppnetwork.org",  #
← Intentado PRIMERO
  pco: %{
    p_cscf_ipv4_address_list: ["203.0.113.100", "203.0.113.101"]
# ← Recaída
  }
}
```

Lógica de Selección:

Condición	Fuente de P-CSCF	IPs Usadas	Me R
FQDN se resuelve con éxito	Descubrimiento DNS (Monitor)	IPs descubiertas de DNS	`"Usand direcci del FQ pcscf.e`
FQDN falla al resolverse	Anulación de PCO de Regla	IPs estáticas de `pco.p_cscf_ipv4_address_list`	`"Fallo IPs de FQDN... a la co estátic`
FQDN devuelve lista vacía	Anulación de PCO de Regla	IPs estáticas de `pco.p_cscf_ipv4_address_list`	Recaída
Monitor no disponible	Anulación de PCO de Regla	IPs estáticas de `pco.p_cscf_ipv4_address_list`	Error ac recaída
No FQDN configurado	Anulación de PCO de Regla o Global	IPs estáticas de la regla o configuración global	Usa la c estática directar

Flujo de Ejemplo:



Escenarios del Mundo Real:

Escenario 1: Descubrimiento DNS Funciona

```
Configuración:
  p_cscf_discovery_fqdn: "pcscf.ims.example.com"
  pco.p_cscf_ipv4_address_list: ["203.0.113.100"]

Resultado DNS: [203.0.113.150, 203.0.113.151]
UE Recibe: [203.0.113.150, 203.0.113.151] ← Desde DNS
Nota: PCO estático se ignora cuando DNS tiene éxito
```

Escenario 2: DNS Falla, Recaída Elegante ⚠

```
Configuración:
  p_cscf_discovery_fqdn: "pcscf.ims.example.com"
  pco.p_cscf_ipv4_address_list: ["203.0.113.100"]

Resultado DNS: ERROR :no_naptr_records
UE Recibe: [203.0.113.100] ← Desde PCO estático
Nota: La sesión tiene éxito a pesar de la falla de DNS
```

Escenario 3: No FQDN Configurado

```
Configuración:
  # Sin p_cscf_discovery_fqdn
  pco.p_cscf_ipv4_address_list: ["192.168.1.50"]

UE Recibe: [192.168.1.50] ← Desde PCO estático
Nota: No se intenta el descubrimiento DNS
```

¿Por qué este diseño?

1. **Preferir Dinámico**: DNS proporciona flexibilidad, balanceo de carga y enrutamiento consciente de la ubicación
2. **Asegurar Fiabilidad**: La recaída estática asegura que las sesiones nunca fallen debido a problemas de DNS
3. **Cero Intervención Manual**: Conmutación automática sin intervención del operador
4. **Seguro para Producción**: Lo mejor de ambos mundos - agilidad con estabilidad

Recomendación: Siempre configura tanto el FQDN como el PCO estático para implementaciones en producción:

```
# ✓ RECOMENDADO: Dinámico con recaída
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com",  # Preferido
  pco: %{
    p_cscf_ipv4_address_list: ["203.0.113.100"]     # Red de
seguridad
  }
}

# ⚠ RIESGOSO: Solo dinámico (recae en PCO global)
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com"
  # ¡Sin recaída específica de regla!
}

# ✓ VÁLIDO: Solo estático (sin sobrecarga de DNS)
%{
  pco: %{
    p_cscf_ipv4_address_list: ["192.168.1.50"]
  }
}
```

Monitoreo de la API OAM

Endpoint del Monitor de P-CSCF

El monitoreo se expone a través de la API REST OAM (HTTPS/TLS en el puerto `8443`). Todas las rutas se sirven bajo el prefijo `/api`. Consulta el monitor de descubrimiento de P-CSCF con:

```
GET /api/pcscf_monitor
```

```
curl -k https://localhost:8443/api/pcscf_monitor
```

El endpoint no toma parámetros de ruta o consulta y devuelve el estado actual de descubrimiento en cada llamada. La documentación interactiva de la API (Swagger UI) está disponible en `https://localhost:8443/api/docs`.

Contenido de la respuesta:

- **Estadísticas Generales**
  - Total de FQDNs monitoreados
  - FQDNs resueltos con éxito
  - Resoluciones fallidas
  - Total de IPs de P-CSCF descubiertas
- **Detalles por FQDN**
  - FQDN que se está monitoreando
  - Estado de resolución (Resuelto / Fallido / Pendiente)
  - Número de IPs descubiertas
  - Lista de direcciones IP resueltas (con detalles por servidor)
  - Marca de tiempo de la última actualización
  - **Estado de Salud**: Cada servidor descubierto informa:
    - Dirección IP y puerto
    - Nombre de host (del objetivo DNS SRV)
    - Indicador de salud (Activo / Inactivo)
- **Métricas de Monitoreo**
  - **Total de FQDNs**: Número de FQDNs únicos registrados para monitoreo
  - **Resueltos con Éxito**: FQDNs que se resolvieron con éxito a través de DNS
  - **Resoluciones DNS Fallidas**: FQDNs que no se resolvieron
  - **Total de Servidores P-CSCF**: Número total de servidores descubiertos en todos los FQDNs

- **Saludables (SIP OPTIONS ACTIVOS)**: Servidores que responden a las verificaciones de salud SIP OPTIONS
- **No Saludables (SIP OPTIONS INACTIVOS)**: Servidores que no responden a SIP OPTIONS
- **Tasa de Éxito de DNS**: Porcentaje de resoluciones DNS exitosas
- **Intervalo de Verificación de Salud**: Frecuencia de las verificaciones de salud SIP OPTIONS (60s, tiempo de espera de 5s)

La respuesta proporciona visibilidad actual tanto sobre la salud de la resolución DNS como sobre la disponibilidad del servidor P-CSCF a través de SIP OPTIONS. Para actualizar, simplemente vuelve a ejecutar `GET /api/pcscf_monitor` — cada llamada devuelve el estado más reciente.

Estado de Selección de UPF

El endpoint de estado de selección de UPF (`GET /api/upf_selection`) informa el estado de descubrimiento de P-CSCF para cada regla:

```
 Tráfico IMS (Prioridad 20)
   Coincidencia: Coincidencia de APN ^ims
   Pool: UPF-IMS-Primario (10.100.2.21:8805)

    Descubrimiento de P-CSCF
      FQDN: pcscf.mnc001.mcc001.3gppnetwork.org
      Estado: ✓ Resuelto (2 IPs)
      IPs Resueltas: 203.0.113.100, 203.0.113.101

   ⚙ Anulaciones de PCO
      DNS Primario: 198.51.100.195
      P-CSCF (recaída estática): 203.0.113.100, 203.0.113.101
```

Métricas y Observabilidad

Métricas de Prometheus

El sistema de monitoreo de P-CSCF expone métricas a través de Prometheus (puerto 42069 por defecto):

Métricas de Medición

```
# Métricas a nivel de FQDN
pcscf_fqdns_total                    # Número total de FQDNs
monitoreados
pcscf_fqdns_resolved                 # FQDNs resueltos con éxito
(DNS tuvo éxito)
pcscf_fqdns_failed                   # Resoluciones de FQDN
fallidas (DNS falló)

# Métricas a nivel de servidor (agregadas)
pcscf_servers_total                  # Total de servidores P-
CSCF descubiertos a través de DNS SRV
pcscf_servers_healthy                # Servidores que responden
a SIP OPTIONS (agregados)
pcscf_servers_unhealthy              # Servidores que no
responden a SIP OPTIONS (agregados)

# Métricas a nivel de servidor (por FQDN con etiqueta)
pcscf_servers_healthy{fqdn="..."}    # Servidores saludables
para un FQDN específico
pcscf_servers_unhealthy{fqdn="..."}  # Servidores no saludables
para un FQDN específico
```

Detalles de Verificación de Salud:

- `healthy`: El servidor respondió al ping SIP OPTIONS (TCP o UDP)
- `unhealthy`: El servidor no respondió a SIP OPTIONS (tiempo de espera de 5s por transporte)

Ejemplos de Métricas

Métricas de Resolución DNS:

```
# Consultar FQDNs resueltos con éxito
pcscf_fqdns_resolved

# Calcular tasa de éxito de DNS
(pcscf_fqdns_resolved / pcscf_fqdns_total) * 100

# Total de servidores descubiertos
pcscf_servers_total
```

Métricas de Salud SIP OPTIONS:

```
# Total de servidores saludables en todos los FQDNs
pcscf_servers_healthy

# Total de servidores no saludables
pcscf_servers_unhealthy

# Calcular tasa de éxito de verificación de salud
(pcscf_servers_healthy / pcscf_servers_total) * 100

# Servidores saludables para un FQDN específico
pcscf_servers_healthy{fqdn="pcscf.mnc001.mcc001.3gppnetwork.org"}

# Alerta sobre todos los servidores inactivos
pcscf_servers_healthy == 0 AND pcscf_servers_total > 0
```

Ejemplos de Alertas de Prometheus:

```yaml
# Alerta cuando todos los servidores P-CSCF están inactivos
- alert: AllPCSCFServersDown
  expr: pcscf_servers_healthy == 0 AND pcscf_servers_total > 0
  for: 5m
  labels:
    severity: critical
  annotations:
    summary: "Todos los servidores P-CSCF están no saludables"
    description: "{{ $value }} servidores saludables (0) - todas
las verificaciones SIP OPTIONS fallaron"

# Alerta cuando más del 50% de los servidores están inactivos
- alert: MajorityPCSCFServersDown
  expr: (pcscf_servers_healthy / pcscf_servers_total) < 0.5
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "La mayoría de los servidores P-CSCF están no
saludables"
    description: "Solo {{ $value }}% de los servidores están
respondiendo a SIP OPTIONS"

# Alerta sobre fallas en la resolución DNS
- alert: PCSCFDNSResolutionFailed
  expr: pcscf_fqdns_failed > 0
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Fallas en la resolución DNS de P-CSCF"
    description: "{{ $value }} FQDN(s) fallando en resolverse"
```

Registro

El monitor registra eventos clave:

```
[info] Monitor de P-CSCF iniciado
[info] Registrando 2 FQDNs únicos de P-CSCF para monitoreo:
["pcscf.ims.example.com", "pcscf.enterprise.example.com"]
[info] Monitor de P-CSCF: Registrando FQDN pcscf.ims.example.com
[debug] Monitor de P-CSCF: Resuelto con éxito
pcscf.ims.example.com a 2 IPs
[warning] Monitor de P-CSCF: Fallo al resolver
pcscf.enterprise.example.com: :nxdomain
[debug] Usando direcciones P-CSCF del FQDN pcscf.ims.example.com:
[{10, 101, 2, 100}, {10, 101, 2, 101}]
```

Estrategia de Recaída

El sistema utiliza una **estrategia de recaída de tres niveles** para máxima fiabilidad:

Nivel 1: Descubrimiento DNS (Preferido)

```
p_cscf_discovery_fqdn: "pcscf.ims.example.com"
```

- El monitor consulta DNS y almacena en caché las IPs resueltas
- La sesión utiliza las IPs en caché si están disponibles
- **Ventaja**: Dinámico, balanceado, consciente de la ubicación

Nivel 2: PCO Estático Específico de Regla (Recaída)

```
pco: %{
  p_cscf_ipv4_address_list: ["203.0.113.100", "203.0.113.101"]
}
```

- Usado si el descubrimiento DNS falla o no devuelve IPs
- Configuración estática específica de la regla

- **Ventaja**: Recaída específica de la regla, predecible

Nivel 3: Configuración Global de PCO (Último Recurso)

```
# Configuración global de pco
pco: %{
  p_cscf_ipv4_address_list: ["203.0.113.146"]
}
```

- Usado si no hay configuración específica de regla y DNS falla
- Direcciones P-CSCF globales por defecto
- **Ventaja**: Siempre disponible, previene fallos en la sesión

Ejemplo de Lógica de Recaída

```
La sesión coincide con la regla "Tráfico IMS":

1. Intentar descubrimiento DNS para "pcscf.ims.example.com"
   ├─ Éxito → Usar [203.0.113.100, 203.0.113.101] ✓
   └─ Fallido → Intentar siguiente nivel

2. Intentar anulación de PCO de la regla
   ├─ Configurado → Usar [203.0.113.100, 203.0.113.101] ✓
   └─ No configurado → Intentar siguiente nivel

3. Usar configuración global de PCO
   └─ Usar [203.0.113.146] ✓ (Siempre tiene éxito)
```

Configuración de DNS

Configuración del Servidor DNS

Configura el servidor DNS con registros SRV y A/AAAA para el descubrimiento de P-CSCF:

```
; Registros SRV para P-CSCF (el prefijo _sip._tcp se consulta
automáticamente)
_sip._tcp.pcscf.mnc001.mcc001.3gppnetwork.org. IN SRV 10 50 5060
pcscf1.example.com.
_sip._tcp.pcscf.mnc001.mcc001.3gppnetwork.org. IN SRV 20 50 5060
pcscf2.example.com.

; Registros A
pcscf1.example.com. IN A 203.0.113.100
pcscf2.example.com. IN A 203.0.113.101
```

Importante: OmniPGW automáticamente antepone `_sip._tcp.` al FQDN configurado. Si configuras `p_cscf_discovery_fqdn: "pcscf.mnc001.mcc001.3gppnetwork.org"`, el sistema consultará `_sip._tcp.pcscf.mnc001.mcc001.3gppnetwork.org`.

Formato del Registro SRV

Los registros SRV siguen este formato:

```
_servicio._proto.dominio. IN SRV prioridad peso puerto objetivo.
```

- **Prioridad**: Valores más bajos tienen mayor prioridad (10 antes de 20)
- **Peso**: Para balanceo de carga entre la misma prioridad (mayor = más tráfico)
- **Puerto**: Puerto SIP (típicamente 5060 para TCP, 5060 para UDP)
- **Objetivo**: Nombre de host a resolver a dirección IP

Prueba de Configuración DNS

```
# Consultar registros SRV (nota el prefijo _sip._tcp)
dig SRV _sip._tcp.pcscf.mnc001.mcc001.3gppnetwork.org @192.0.2.177

# Salida esperada:
# _sip._tcp.pcscf.mnc001.mcc001.3gppnetwork.org. 300 IN SRV 10 50
5060 pcscf1.example.com.

# Resolver nombre de P-CSCF a IP
dig A pcscf1.example.com @192.0.2.177

# Salida esperada:
# pcscf1.example.com. 300 IN A 203.0.113.100
```

Solución de Problemas

Problema: FQDN Muestra Estado "Fallido"

Síntomas:

- `GET /api/pcscf_monitor` informa estado Fallido
- Error: `:nxdomain`, `:timeout`, o `:no_naptr_records`

Causas Posibles:

1. Servidor DNS no accesible
2. FQDN no existe en DNS
3. No se configuraron registros NAPTR
4. Tiempo de espera del servidor DNS

Resolución:

```
# 1. Probar conectividad al servidor DNS
ping 192.0.2.177

# 2. Probar consulta NAPTR manualmente
dig NAPTR pcscf.mnc001.mcc001.3gppnetwork.org @192.0.2.177

# 3. Verificar registros de OmniPGW
grep "P-CSCF" /var/log/pgw_c.log

# 4. Verificar configuración
grep "p_cscf_discovery_dns_server" config/runtime.exs

# 5. Volver a consultar la API OAM para el estado actual
curl -k https://localhost:8443/api/pcscf_monitor
```

Problema: No se Devuelven IPs

Síntomas:

- `GET /api/pcscf_monitor` informa "0 IPs"
- El estado puede ser Resuelto o Fallido

Causas Posibles:

1. Existen registros NAPTR pero los FQDNs de reemplazo no se resuelven
2. El campo de servicio no coincide con el patrón IMS/SIP
3. Faltan registros A/AAAA

Resolución:

```
# Verificar el campo de servicio del registro NAPTR
dig NAPTR pcscf.example.com @192.0.2.177

# Asegurarse de que el servicio contenga "SIP" o "IMS":
# CORRECTO: "SIP+D2U", "x-3gpp-ims:sip"
# INCORRECTO: "HTTP", "FTP"

# Verificar que existan registros A/AAAA
dig pcscf1.example.com A @192.0.2.177
```

Problema: Sesiones Usan P-CSCF Incorrecto

Síntomas:

- UE recibe direcciones P-CSCF inesperadas
- Se utiliza la recaída estática en lugar de las IPs descubiertas

Causas Posibles:

1. El descubrimiento DNS falló pero la recaída está funcionando
2. Coincidencia de regla incorrecta
3. FQDN no registrado

Resolución:

```
# 1. Verificar la página del Monitor de P-CSCF
# Verificar que el FQDN esté registrado y resuelto

# 2. Verificar registros de sesión
grep "Usando direcciones P-CSCF del FQDN" /var/log/pgw_c.log

# 3. Verificar la página de Selección de UPF
# Verificar que la regla muestre el FQDN y estado correctos

# 4. Probar coincidencia de regla
# Crear sesión con APN específico y verificar qué regla coincide
```

Problema: Alta Latencia en Consultas DNS

Síntomas:

- Creación de sesión lenta
- Métricas muestran alta `pcscf_discovery_query_duration_seconds`

Causas Posibles:

1. Problemas de rendimiento del servidor DNS
2. Latencia de red hacia el servidor DNS
3. Tiempo de espera demasiado alto

Resolución:

```
# Reducir tiempo de espera de consulta
pco: %{
  p_cscf_discovery_timeout_ms: 2000  # Reducir de 5000ms
}

# Considerar usar un servidor DNS más cercano
pco: %{
  p_cscf_discovery_dns_server: "10.0.0.10"  # DNS local
}
```

Mejores Prácticas

1. Selección del Servidor DNS

Usar Servidor DNS Dedicado

```
pco: %{
  # DNS dedicado para el descubrimiento de P-CSCF (no el mismo que
el DNS de UE)
  p_cscf_discovery_dns_server: "192.0.2.177",

  # Servidores DNS de UE (dados a dispositivos móviles)
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4"
}
```

¿Por qué?

- Separar preocupaciones: DNS de UE vs. DNS interno de IMS
- Diferentes políticas de acceso y seguridad
- Escalabilidad y fiabilidad independientes

2. Siempre Configurar Recaída Estática

```
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com",  # Preferido
  pco: %{
    p_cscf_ipv4_address_list: ["203.0.113.100"]  # Requerido como
recaída
  }
}
```

¿Por qué?

- Asegura que las sesiones tengan éxito incluso si DNS falla
- Degradación elegante
- Cumple con los requisitos de SLA

3. Usar FQDNs Específicos por Tipo de Tráfico

```
rules: [
  # IMS
  %{
    name: "IMS",
    match_regex: "^ims",
    p_cscf_discovery_fqdn:
"pcscf.ims.mnc001.mcc001.3gppnetwork.org"
  },

  # Empresa
  %{
    name: "Empresa",
    match_regex: "^enterprise",
    p_cscf_discovery_fqdn: "pcscf.enterprise.example.com"
  }
]
```

¿Por qué?

- Diferentes grupos de P-CSCF por servicio
- Mejor distribución de carga

- Enrutamiento específico de servicio

4. Monitorear el Rendimiento de Consultas DNS

```
# Alerta sobre alta latencia en consultas de P-CSCF
alert: HighPCSCFQueryLatency
expr: histogram_quantile(0.95,
pcscf_discovery_query_duration_seconds_bucket) > 2
for: 5m
labels:
  severity: warning
annotations:
  summary: "Las consultas DNS de P-CSCF son lentas (p95 > 2s)"
```

5. Verificaciones de Salud DNS Regulares

- **API OAM**: Consultar `GET /api/pcscf_monitor` diariamente
- **Métricas**: Monitorear la métrica `pcscf_monitor_fqdns_failed`
- **Registros**: Vigilar errores de DNS
- **Pruebas**: Verificar periódicamente que existan registros DNS

6. Configurar un Tiempo de Espera Apropiado

```
# Producción: Equilibrar fiabilidad vs. latencia
pco: %{
  p_cscf_discovery_timeout_ms: 5000  # 5 segundos
}

# Alto rendimiento: Favorecer velocidad, confiar en la recaída
pco: %{
  p_cscf_discovery_timeout_ms: 2000  # 2 segundos
}
```

7. Usar Redundancia DNS

Configurar DNS primario y secundario:

```
# DNS Primario de P-CSCF
pcscf.mnc001.mcc001.3gppnetwork.org. IN NAPTR 10 50 "s" "SIP+D2U"
"" _sip._udp.pcscf1.example.com.

# DNS Secundario de P-CSCF
pcscf.mnc001.mcc001.3gppnetwork.org. IN NAPTR 20 50 "s" "SIP+D2U"
"" _sip._udp.pcscf2.example.com.
```

Documentación Relacionada

- **Configuración de PCO** - Opciones de Configuración de Protocolo, configuración de DNS y P-CSCF
- **Guía de Configuración** - Referencia completa de configuración de OmniPGW
- **Monitoreo** - Métricas, registro y observabilidad
- **Gestión de Sesiones** - Ciclo de vida de la sesión y entrega de PCO
- **Interfaz PFCP** - Comunicación de la Función de Plano de Usuario

---

Volver a la Documentación Principal

Documentación de la Interfaz PFCP/Sxb

Protocolo de Control de Reenvío de Paquetes - Comunicación de PGW-C a PGW-U

Tabla de Contenidos

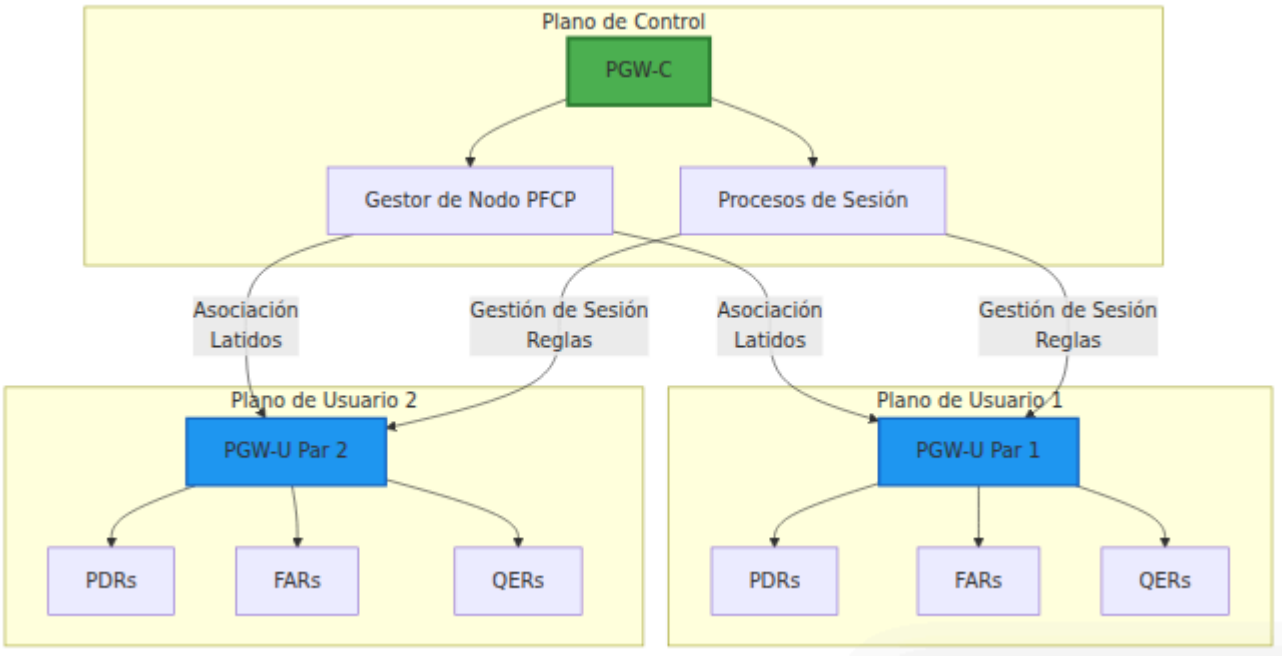
1. Descripción General
2. Fundamentos del Protocolo
3. Gestión de Asociaciones PFCP
4. Gestión de Sesiones PFCP
5. Reglas de Procesamiento de Paquetes
6. Configuración
7. Selección de UPF Basada en DNS
8. Flujos de Mensajes
9. Resolución de Problemas
10. Monitoreo de PFCP
11. Documentación Relacionada

Descripción General

La **interfaz Sxb** utiliza el **PFCP (Protocolo de Control de Reenvío de Paquetes)** para la comunicación entre el PGW-C (plano de control) y el PGW-U (plano de usuario). Esta separación permite:

- **Plano de Control (PGW-C)** - Maneja la señalización, gestión de sesiones, decisiones de políticas
- **Plano de Usuario (PGW-U)** - Maneja el reenvío real de paquetes a alta velocidad

Arquitectura PFCP



Fundamentos del Protocolo

Versión PFCP

PGW-C implementa **PFCP Versión 1** (3GPP TS 29.244).

Transporte

- **Protocolo:** UDP
- **Puerto Predeterminado:** 8805
- **Formato de Mensaje:** Codificado en binario utilizando la especificación PFCP

Tipos de ID de Nodo

Los pares PFCP se identifican por ID de Nodo, que puede ser:

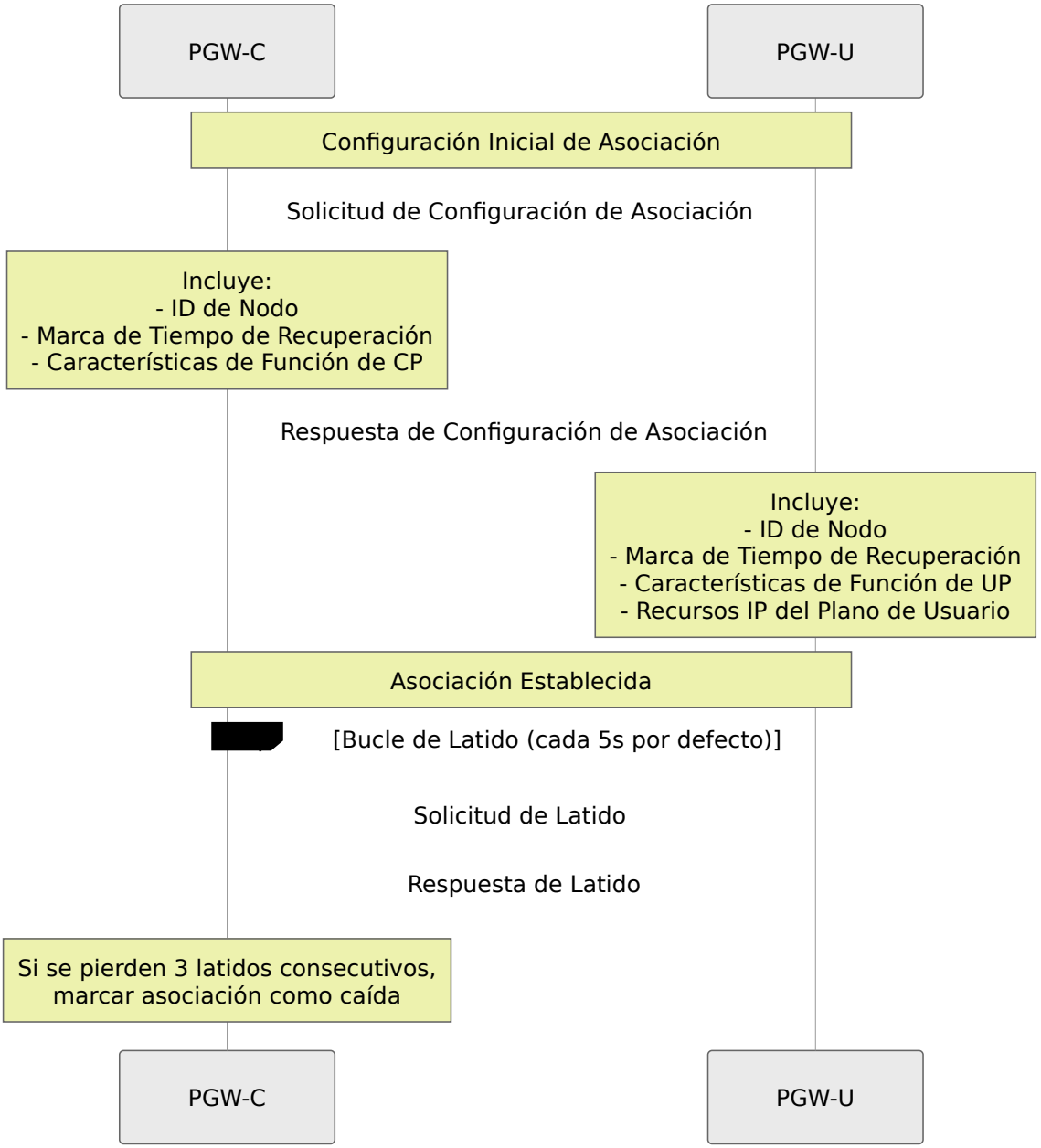
- **Dirección IPv4** - Más común
- **Dirección IPv6**

- **FQDN** (Nombre de Dominio Totalmente Calificado)

Gestión de Asociaciones PFCP

Antes de que se pueda llevar a cabo la gestión de sesiones, se debe establecer una **asociación** PFCP entre PGW-C y PGW-U.

Flujo de Configuración de Asociación



Gestión del Estado del Par

Cada par PFCP mantiene el estado:

Campo	Descripción
`is_associated`	Booleano que indica el estado de asociación
`remote_node_id`	ID de Nodo del par (IP o FQDN)
`remote_ip_address`	Dirección IP para la comunicación
`remote_port`	Puerto UDP (predeterminado 8805)
`heartbeat_period_ms`	Intervalo de latido en milisegundos
`missed_heartbeats_consecutive`	Conteo de latidos perdidos
`up_function_features`	Características del plano de usuario soportadas
`up_recovery_time_stamp`	Marca de tiempo de recuperación del par

Mecanismo de Latido

Propósito: Detectar fallos en el par y mantener la vitalidad de la asociación

Configuración:

```
# En config/runtime.exs
sxb: %{
  local_ip_address: "10.0.0.20"
},
upf_selection: %{
  fallback_pool: [
    %{remote_ip_address: "10.0.0.21", remote_port: 8805, weight:
100}
  ]
}
# Todos los UPFs se registran automáticamente con latidos de 5
segundos
```

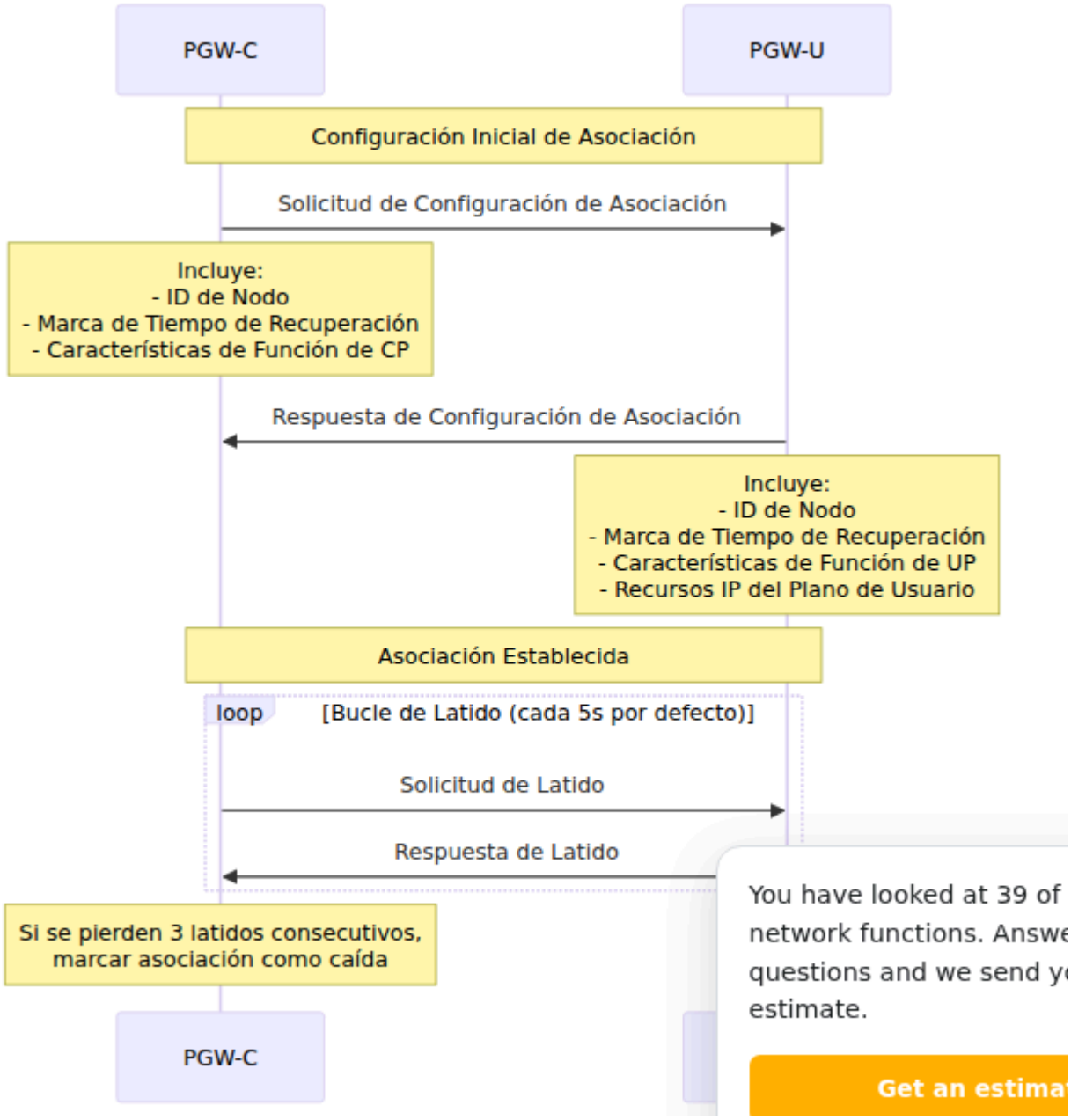
Detección de Fallos:

- Cada latido perdido incrementa `missed_heartbeats_consecutive`
- Típicamente configurado para fallar después de 3 pérdidas consecutivas
- La asociación fallida impide nuevas sesiones a ese par

Gestión de Sesiones PFCP

Las sesiones PFCP se crean para cada conexión PDN de UE para programar reglas de reenvío en el plano de usuario.

Ciclo de Vida de la Sesión



Establecimiento de Sesión

Cuándo: El UE se conecta y crea una conexión PDN

PGW-C envía a PGW-U:

Solicitud de Establecimiento de Sesión que contiene:

- **SEID** (ID de Punto Final de Sesión) - Identificador único de sesión
- **ID de Nodo** - ID de Nodo de PGW-C

- **F-SEID** - SEID Totalmente Calificado (incluye IP + SEID)
- **PDRs** - Reglas de Detección de Paquetes (típicamente 2: uplink + downlink)
- **FARs** - Reglas de Acción de Reenvío (típicamente 2: uplink + downlink)
- **QERs** - Reglas de Aplicación de QoS (límites de bitrate)
- **BAR** - Regla de Acción de Buffering (para buffering de downlink)

PGW-U responde:

Respuesta de Establecimiento de Sesión que contiene:

- **Causa** - Razón de éxito o fallo
- **F-SEID** - Punto final de sesión de PGW-U
- **PDRs Creados** - Reconocimiento de reglas creadas
- **F-TEID** - TEID Totalmente Calificado para la interfaz S5/S8

Modificación de Sesión

Cuándo: Ocurren cambios en QoS, actualizaciones de políticas o modificaciones de portadores

La modificación puede incluir:

- Agregar nuevos PDRs, FARs, QERs
- Eliminar reglas existentes
- Actualizar parámetros de regla

Eliminación de Sesión

Cuándo: El UE se desconecta o se termina la conexión PDN

Proceso:

1. PGW-C envía Solicitud de Eliminación de Sesión con SEID
2. PGW-U elimina todas las reglas y libera recursos
3. PGW-U responde con Respuesta de Eliminación de Sesión

Asignación de F-TEID

F-TEID (Identificador de Punto Final de Túnel Totalmente Calificado) identifica los puntos finales de túnel GTP-U para el tráfico del plano de usuario. Al establecer una sesión PFCP, alguien debe asignar el F-TEID que identifica dónde el UPF debe enviar el tráfico de uplink. Hay dos enfoques:

Entendiendo la Asignación de F-TEID

Qué se está asignando: El F-TEID consiste en:

- **TEID** (Identificador de Punto Final de Túnel) - Número de 32 bits que identifica el túnel
- **Dirección IP** - Dónde enviar paquetes GTP-U (la dirección IP del UPF)

La Pregunta: ¿Quién asigna el valor TEID?

Opción 1: UPF Asigna (Predeterminado Recomendado)

- PGW-C dice "por favor asigna un TEID para mí" (bandera CHOOSE)
- UPF elige un TEID de su grupo local y responde con el valor

Opción 2: PGW-C Asigna (Modo de Compatibilidad)

- PGW-C elige un TEID y le dice al UPF "usa este TEID específico"
- UPF utiliza el TEID proporcionado sin asignación

Asignación de UPF (Predeterminado - Recomendado)

Configuración:

```
sxb: %{
  allocate_uplink_f_teid: false  # Predeterminado
}
```

Cómo Funciona:

1. PGW-C construye Solicitud de Establecimiento de Sesión PFCP con la bandera F-TEID CHOOSE

2. UPF recibe la solicitud, asigna TEID de su grupo interno
3. UPF responde con F-TEID asignado (TEID + dirección IP)
4. PGW-C almacena el F-TEID asignado durante la vida de la sesión

Por qué esto es mejor (normalmente):

□ Separación de Preocupaciones

- UPF posee el plano de usuario = UPF gestiona los identificadores del plano de usuario
- No es necesario que PGW-C rastree qué TEIDs tiene disponibles el UPF
- Cada componente gestiona su propio grupo de recursos

□ Escalabilidad Multi-PGW-C

- Múltiples instancias de PGW-C pueden comunicarse con el mismo UPF sin coordinación
- Sin riesgo de colisiones de TEID entre diferentes instancias de PGW-C
- UPF asegura unicidad entre todos los pares del plano de control

□ Comportamiento Estándar de 3GPP

- La bandera CHOOSE está definida en 3GPP TS 29.244 para este propósito
- Las implementaciones modernas de UPF lo soportan
- Sigue el principio de "dejar que el propietario asigne"

□ Failover Más Simple

- Si PGW-C se reinicia, UPF aún posee el espacio de nombres de TEID
- No es necesario sincronizar el estado de asignación de TEID
- UPF puede continuar utilizando TEIDs existentes

Cuándo Usar:

- □ Implementaciones de producción con UPFs modernos (predeterminado)
- □ Implementaciones Multi-PGW-C compartiendo grupos de UPF
- □ Arquitecturas nativas de la nube con planos de control sin estado
- □ Quieres un comportamiento estándar PFCP de 3GPP

Problemas Potenciales:

- ⚠ Algunas implementaciones de UPF heredadas o propietarias no soportan la bandera CHOOSE
- ⚠ Si el establecimiento de sesión falla con "IE obligatoria faltante" o similar, el UPF puede no soportar CHOOSE

Asignación de PGW-C (Compatibilidad Legada)

Configuración:

```
sxb: %{
  allocate_uplink_f_teid: true
}
```

Cómo Funciona:

1. PGW-C asigna TEID de su grupo local durante la creación de la sesión
2. PGW-C construye Solicitud de Establecimiento de Sesión PFCP con un valor TEID explícito
3. UPF recibe la solicitud, utiliza el TEID proporcionado sin asignación
4. Tanto PGW-C como UPF rastrean el mismo valor TEID

Por qué podrías necesitar esto:

□ UPF No Soporta CHOOSE

- Algunas implementaciones de UPF (especialmente heredadas/propietarias) no soportan asignación dinámica
- UPF espera un TEID explícito en la Solicitud de Establecimiento de Sesión PFCP
- Única solución para compatibilidad

□ Gestión Centralizada de TEID

- Si necesitas que PGW-C tenga visibilidad total sobre todos los TEIDs asignados

- Útil para depurar problemas del plano de usuario (PGW-C conoce los valores exactos de TEID)
- Puede correlacionar TEID en capturas de paquetes con el estado de la sesión

□ Asignación Determinista

- Si necesitas patrones de asignación de TEID predecibles
- Algunos entornos de prueba pueden requerir rangos de TEID específicos

Compensaciones:

⚠ Coordinación Requerida para Multi-PGW-C

- Múltiples instancias de PGW-C compartiendo un UPF deben evitar colisiones de TEID
- Requiere:
  - Rangos de TEID particionados por PGW-C (configuración compleja)
  - Servicio de asignación de TEID compartido (infraestructura adicional)
  - Aceptar riesgo de colisión con asignación aleatoria (baja probabilidad)

⚠ Sincronización de Estado

- PGW-C debe rastrear los TEIDs asignados para evitar reutilización
- Estado del grupo de TEID perdido en el reinicio de PGW-C (debe reconstruirse a partir de sesiones)
- Escenarios de failover más complejos

⚠ Comportamiento No Estándar

- No es el patrón de diseño PFCP previsto
- Puede no funcionar con todas las implementaciones de UPF que esperan CHOOSE

Cuándo Usar:

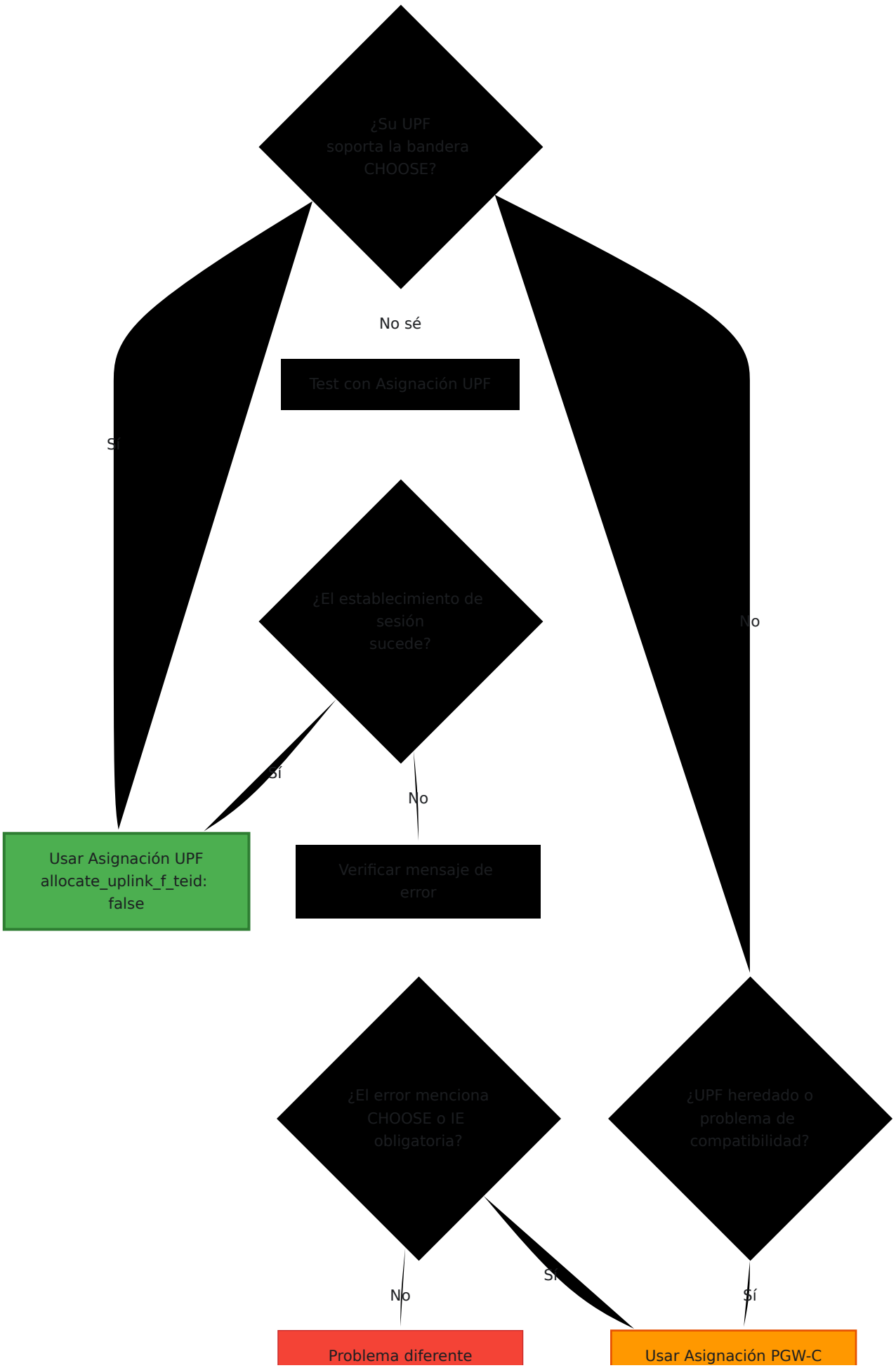
- **⚠ Solo cuando el UPF no soporte la bandera CHOOSE**
- ⚠ Implementaciones de UPF heredadas (por ejemplo, algunos hardware propietarios)

- ⚠ Requisitos específicos de compatibilidad
- ⚠ Escenarios de depuración que requieren visibilidad de TEID en PGW-C

Manejo de Colisiones de TEID: PGW-C utiliza asignación aleatoria con detección de colisiones:

- Rango de TEID: 1 a 0xFFFFFFFF (4.2 mil millones de valores)
- Probabilidad de colisión: ~0.023% a 1 millón de sesiones
- Reintento automático en caso de colisión (transparente para el llamador)
- TEIDs liberados automáticamente cuando la sesión termina

Cómo Elegir


¿Su UPF soporta la bandera CHOOSE?
No sé
Test con Asignación UPF
Sí
¿El establecimiento de sesión sucede?
No
Sí
No
Usar Asignación UPF allocate_uplink_f_teid: false
Verificar mensaje de error
¿El error menciona CHOOSE o IE obligatoria?
¿UPF heredado o problema de compatibilidad?
No
Sí
Sí
Problema diferente
Usar Asignación PGW-C



Resolución de Problemas

Síntoma: El establecimiento de sesión falla inmediatamente

Verifique los registros de PFCP:

```
# Busque errores relacionados con CHOOSE
grep -i "choose\|mandatory.*missing" /var/log/pgw_c.log

# Verifique los códigos de causa de Respuesta de Establecimiento
de Sesión PFCP
grep "Session Establishment Response" /var/log/pgw_c.log
```

Si el UPF rechaza la bandera CHOOSE:

- El error puede decir "IE obligatoria faltante" o "IE inválida"
- UPF espera un F-TEID explícito pero recibió CHOOSE
- **Solución:** Establecer `allocate_uplink_f_teid: true`

Si la asignación de PGW-C causa problemas:

- Muy raro - el espacio de TEID es enorme (4 mil millones de valores)
- Verifique si hay agotamiento de TEID (poco probable por debajo de millones de sesiones):

```
# Verifique el conteo del registro
grep "registered_teid_count" /var/log/pgw_c.log
```

Cambio entre Modos:

```
# Editar config/runtime.exs
sxb: %{
  local_ip_address: "10.0.0.20",
  allocate_uplink_f_teid: false  # Cambiar a true si el UPF no
soporta CHOOSE
}
```

Luego reinicie PGW-C:

```
systemctl restart pgw_c
```

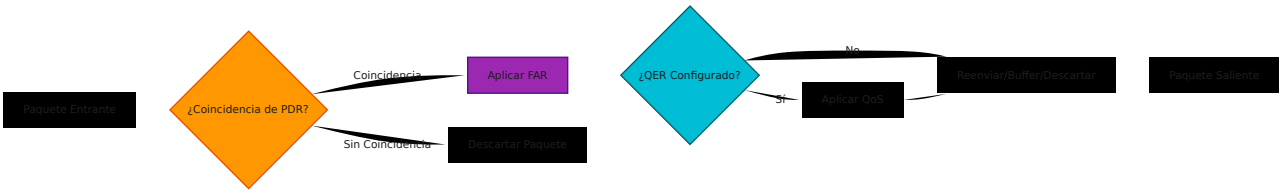
Verificando qué Modo está Activo: Verifique las capturas de paquetes PFCP:

```
# Capturar tráfico PFCP
tcpdump -i any -n port 8805 -w pfcp.pcap

# Abrir en Wireshark y mirar la Solicitud de Establecimiento de
Sesión
# Si F-TEID muestra "banderas CHOOSE": modo de asignación UPF
# Si F-TEID muestra valor TEID explícito: modo de asignación PGW-C
```

Reglas de Procesamiento de Paquetes

PFCP utiliza un conjunto de reglas para definir cómo el plano de usuario procesa paquetes.

Arquitectura de Reglas



PDR (Regla de Detección de Paquetes)

Propósito: Identificar a qué paquetes se aplica esta regla

Configuración Típica de PGW-C:

PDR #1 - Downlink:

```
ID de PDR: 1
Precedencia: 100
PDI (Información de Detección de Paquetes):
  - Interfaz de Origen: CORE (lado de Internet)
  - Dirección IP de UE: 100.64.1.42/32
ID de FAR: 1 (regla de reenvío asociada)
```

PDR #2 - Uplink:

```
ID de PDR: 2
Precedencia: 100
PDI (Información de Detección de Paquetes):
  - Interfaz de Origen: ACCESS (lado de SGW)
  - F-TEID: <punto final de túnel S5/S8>
ID de FAR: 2 (regla de reenvío asociada)
ID de QER: 1 (aplicación de QoS)
```

Campos Clave de PDR:

- **ID de PDR** - Identificador único de regla (por sesión)
- **Precedencia** - Prioridad de coincidencia de regla (más alto = más específico)
- **PDI** - Criterios de coincidencia (interfaz, IP, TEID, etc.)
- **Eliminación de Encabezado Externo** - Quitar encabezado GTP-U en ingreso
- **ID de FAR** - Acción de reenvío asociada
- **ID de QER** - Aplicación de QoS asociada (opcional)

FAR (Regla de Acción de Reenvío)

Propósito: Definir qué hacer con los paquetes coincidentes

FAR #1 - Downlink (Internet → UE):

```
ID de FAR: 1
Aplicar Acción: REENVIAR
Parámetros de Reenvío:
  - Interfaz de Destino: ACCESS (a SGW)
  - Creación de Encabezado Externo: GTP-U/UDP/IPv4
  - F-TEID Remoto: <punto final de túnel SGW S5/S8>
```

FAR #2 - Uplink (UE → Internet):

```
ID de FAR: 2
Aplicar Acción: REENVIAR
Parámetros de Reenvío:
  - Interfaz de Destino: CORE (a Internet)
  - (Sin encabezado externo - reenvío IP simple)
```

Campos Clave de FAR:

- **ID de FAR** - Identificador único de regla
- **Aplicar Acción** - REENVIAR, DESCARTAR, BUFFER, NOTIFICAR
- **Parámetros de Reenvío:**
  - Interfaz de destino (ACCESS/CORE)
  - Creación de Encabezado Externo (agregar túnel GTP-U)
  - Instancia de Red (VRF/tablas de enrutamiento)

QER (Regla de Aplicación de QoS)

Propósito: Aplicar límites de bitrate y parámetros de QoS. Los QERs también pueden rastrear el uso para la gestión de cuotas de carga en línea (ver Interfaz Diameter Gy para control de crédito).

Ejemplo de QER:

```
ID de QER: 1
Estado de Puerta: ABIERTO
Bitrate Máximo:
  - Uplink: 100 Mbps
  - Downlink: 50 Mbps
Bitrate Garantizado: (opcional, para portadores GBR)
  - Uplink: 10 Mbps
  - Downlink: 10 Mbps
```

Campos Clave de QER:

- **ID de QER** - Identificador único de regla
- **Estado de Puerta** - ABIERTO (permitir) o CERRADO (bloquear)
- **MBR** - Bitrate Máximo (uplink/downlink)
- **GBR** - Bitrate Garantizado (para portadores dedicados)
- **QCI** - Identificador de Clase de QoS (afecta la programación)

BAR (Regla de Acción de Buffering)

Propósito: Controlar el buffering de paquetes de downlink cuando el UE está inactivo

Ejemplo de BAR:

```
ID de BAR: 1
Retraso de Notificación de Datos de Downlink: 100ms
Conteo Sugerido de Paquetes en Buffer: 10
```

Usado para: Optimización de DRX (Recepción Discontinua) en modo inactivo

---

Configuración

Configuración Básica de Sxb

Edita `config/runtime.exs`:

```
config :pgw_c,
  sxb: %{
    # Dirección IP local para comunicación PFCP
    local_ip_address: "10.0.0.20",

    # Opcional: Sobrescribir puerto predeterminado (8805)
    local_port: 8805,

    # Tiempo de espera de solicitud PFCP en milisegundos
(predeterminado: 500ms)
    # Tiempo de espera para la respuesta del UPF antes de
retransmitir
    # Debe ser >= tiempo de procesamiento esperado del UPF para
evitar sesiones duplicadas
    request_timeout_ms: 500,

    # Número de intentos de retransmisión para solicitudes PFCP
(predeterminado: 3)
    # Tiempo total máximo de espera = request_timeout_ms *
request_attempts
    request_attempts: 3,

    # Opcional: Control de asignación de F-TEID para el plano de
usuario
    # Cuando es falso (predeterminado): UPF asigna F-TEID (bandera
CHOOSE)
    # Cuando es verdadero: PGW-C pre-asigna F-TEID y proporciona
un valor explícito
    # Nota: Algunos UPFs pueden no soportar la bandera CHOOSE y
requerir asignación explícita
    allocate_uplink_f_teid: false
  },

  # Selección de UPF - Todos los UPFs definidos aquí se registran
automáticamente
  upf_selection: %{
    fallback_pool: [
      %{
        # Dirección IP de PGW-U
        remote_ip_address: "10.0.0.21",

        # Puerto PFCP (predeterminado: 8805)
        remote_port: 8805,
```

```
        # Peso para balanceo de carga (100 = normal, 0 = en
espera)
        weight: 100
      }
    ]
  }
```

Configuración de Tiempo de Espera de Solicitud

La interfaz PFCP utiliza tiempos de espera configurables para las solicitudes de Establecimiento, Modificación y Eliminación de Sesiones al UPF.

Parámetros:

Parámetro	Tipo	Predeterminado	Descripción
`request_timeout_ms`	Entero	500	Tiempo en milisegundos para esperar la respuesta del UPF antes de retransmitir
`request_attempts`	Entero	3	Número máximo de intentos de transmisión antes de fallar la solicitud

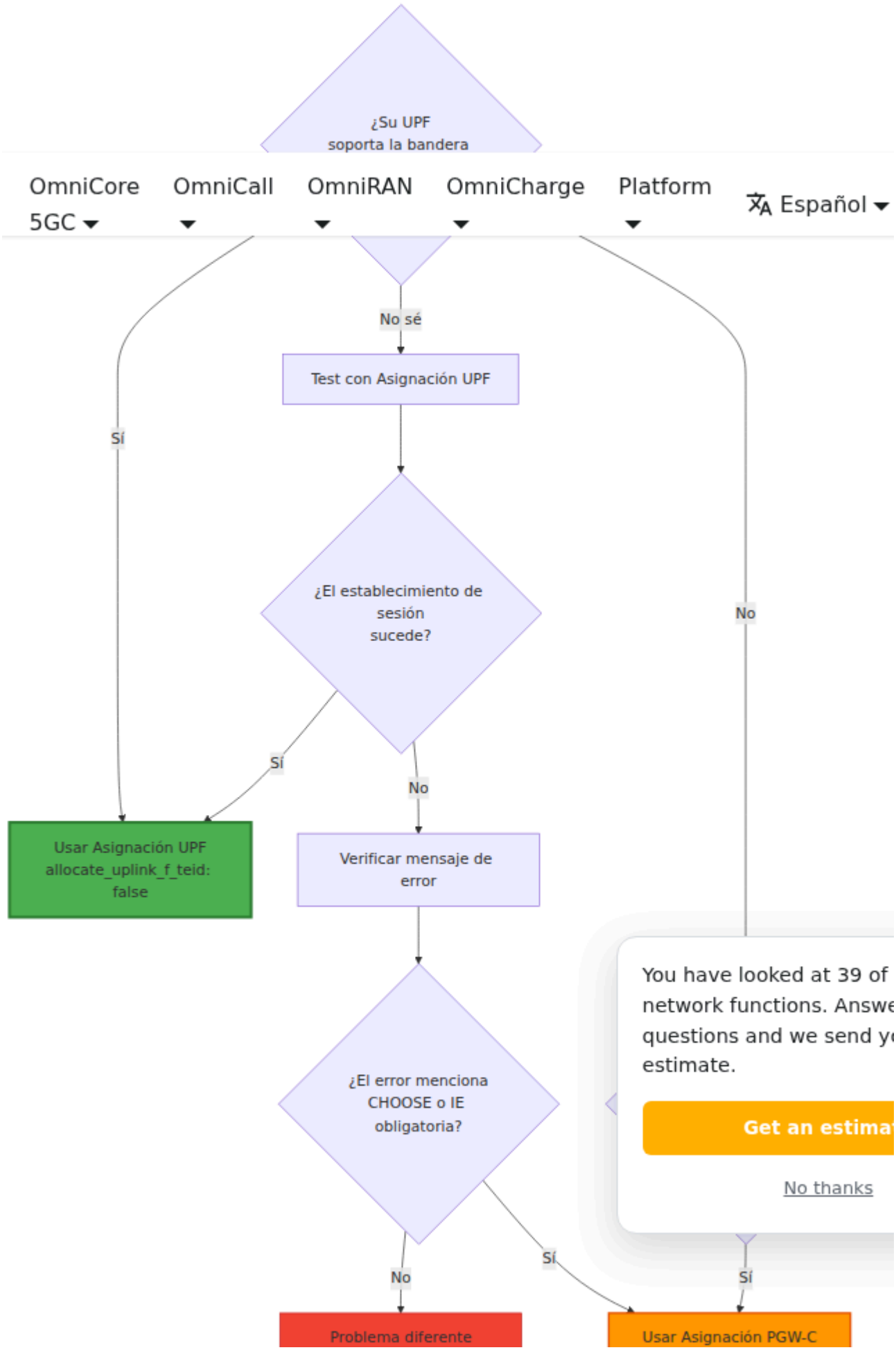
Tiempo Total de Espera: `request_timeout_ms × request_attempts`

Comportamiento predeterminado: 500ms × 3 intentos = **1.5 segundos de espera máxima total**

Por qué importa la configuración de tiempo de espera

Si `request_timeout_ms` se establece demasiado bajo en relación con el tiempo de procesamiento del UPF:

1. PGW-C envía Solicitud de Establecimiento de Sesión
2. El tiempo de espera expira antes de que el UPF responda
3. PGW-C retransmite con el mismo número de secuencia
4. UPF procesa ambas solicitudes y crea **sesiones PFCP duplicadas**
5. PGW-C recibe la primera respuesta y almacena un ID de sesión
6. La segunda sesión se convierte en **huérfana** en el UPF


¿Su UPF
soporta la bandera
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Español
No sé
Test con Asignación UPF
Sí
¿El establecimiento de sesión sucede?
No
Sí
No
Usar Asignación UPF allocate_uplink_f_teid: false
Verificar mensaje de error
¿El error menciona CHOOSE o IE obligatoria?
No
Sí
Problema diferente
Usar Asignación PGW-C
Sí
You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima
No thanks



Directrices de Ajuste

Tiempo de Respuesta del UPF	`request_timeout_ms` Recomendado	Tiempo Total de Espera
Rápido (<100ms)	200-300ms	600-900ms (3 intentos)
Normal (100-300ms)	500ms (predeterminado)	1.5s (3 intentos)
Lento (300-500ms)	750-1000ms	2.25-3s (3 intentos)
Muy lento (>500ms)	1500-2000ms	4.5-6s (3 intentos)

Recomendación: Establecer `request_timeout_ms` al menos **2× el tiempo de respuesta esperado del UPF** para evitar sesiones huérfanas inducidas por retransmisiones.

Ejemplo - UPF Lento

```
sxb: %{
  local_ip_address: "10.0.0.20",
  request_timeout_ms: 1000,  # 1 segundo por intento
  request_attempts: 3         # Total: 3 segundos como máximo
}
```

Diagnóstico de Problemas de Tiempo de Espera

Síntomas de tiempo de espera demasiado bajo:

- El UPF informa más sesiones PFCP de las esperadas
- Las sesiones huérfanas se acumulan en el UPF con el tiempo

- Mensajes de registro: `"Session Establishment Request timed out"` seguidos de sesión exitosa

Cómo diagnosticar:

1. Verifique el conteo de sesiones del UPF a través de la API o interfaz de gestión del UPF
2. Compare con el conteo de sesiones activas de PGW-C
3. Si el UPF tiene más sesiones, existen huérfanas de retransmisiones

Resolución:

1. Aumente `request_timeout_ms` para superar el tiempo de respuesta del UPF
2. Reinicie PGW-C para aplicar la nueva configuración
3. Limpie las sesiones huérfanas del UPF (limpieza manual o reinicio del UPF)

Múltiples Pares PGW-U

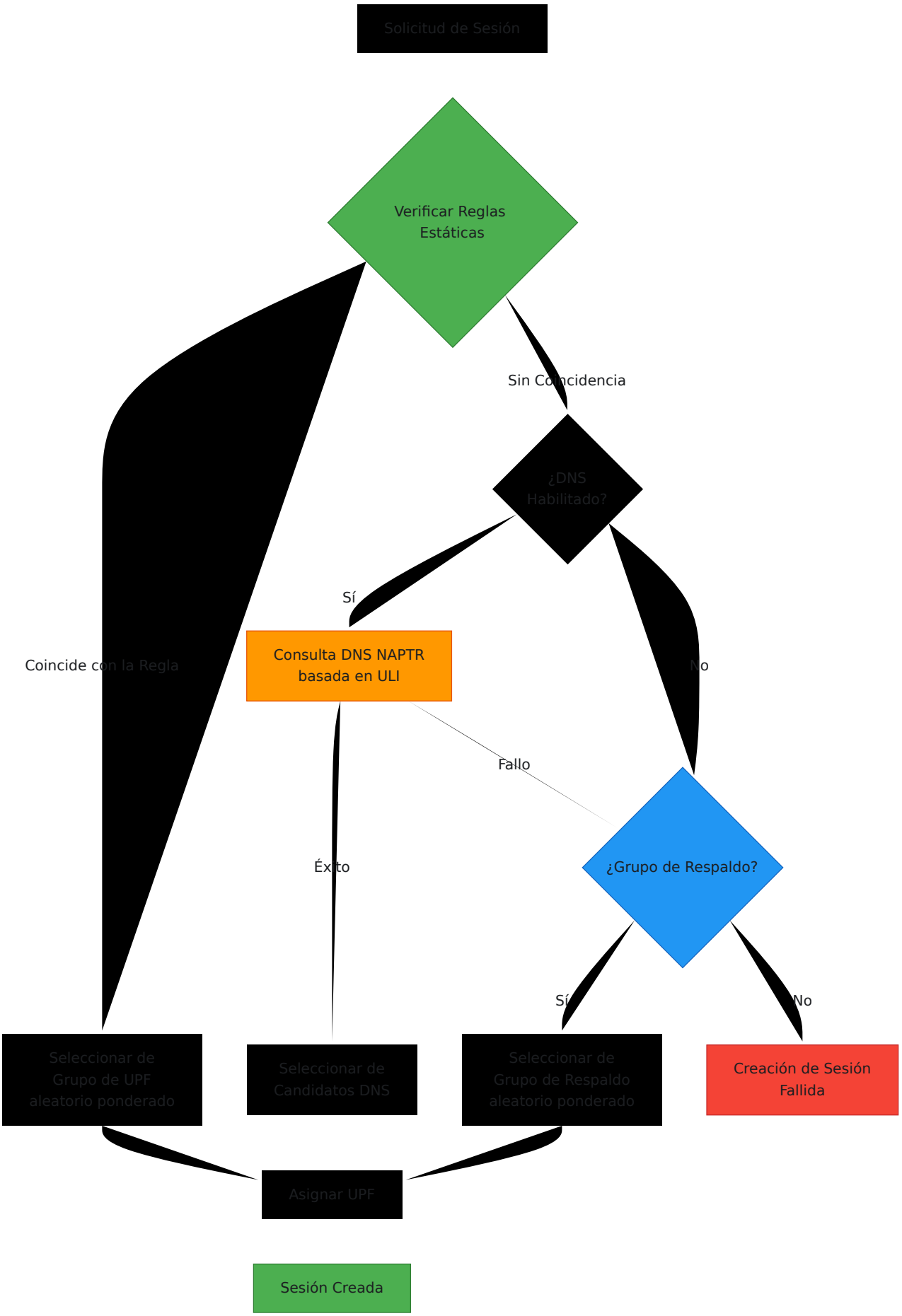
Para balanceo de carga o redundancia:

```
config :pgw_c,
  sxb: %{
    local_ip_address: "10.0.0.20"
  },
  upf_selection: %{
    fallback_pool: [
      %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight:
50},  # 50% tráfico
      %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight:
50}   # 50% tráfico
    ]
  }
# Ambos UPFs se registran automáticamente con latidos de 5
segundos
```

Configuración de Selección de UPF

PGW-C utiliza un **sistema de selección de UPF de tres niveles** con reglas basadas en prioridades:

1. **Reglas Estáticas** (Mayor Prioridad) - Coinciden según los atributos de la sesión
2. **Selección Basada en DNS** (Prioridad Media) - Enrutamiento consciente de la ubicación a través de consultas DNS NAPTR
3. **Grupo de Respaldo** (Menor Prioridad) - Grupo de UPF predeterminado cuando no coinciden reglas


Solicitud de Sesión
Verificar Reglas Estáticas
Coincide con la Regla
Sin Coincidencia
¿DNS Habilitado?
Sí
No
Consulta DNS NAPTR basada en ULI
Éxito
Fallo
¿Grupo de Respaldo?
Sí
No
Seleccionar de Grupo de UPF aleatorio ponderado
Seleccionar de Candidatos DNS
Seleccionar de Grupo de Respaldo aleatorio ponderado
Creación de Sesión Fallida
Asignar UPF
Sesión Creada

Ejemplo Completo de Selección de UPF

```
config :pgw_c,
  # Interfaz PFCP
  sxb: %{
    local_ip_address: "10.0.0.20"
  },

  # Selección de UPF: Todos los UPFs definidos aquí se registran
automáticamente
  upf_selection: %{
    #
==========================================================================
    # Selección Basada en DNS (Enrutamiento Consciente de la
Ubicación)
    #
==========================================================================
    # Consulta DNS utilizando Información de Ubicación del Usuario
(ULI)
    # Proporciona selección dinámica de UPF basada en la ubicación de
la celda
    dns_enabled: false,
    dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
    dns_suffix: "epc.3gppnetwork.org",
    dns_timeout_ms: 5000,

    #
==========================================================================
    # Reglas de Selección Estática (Evaluadas por Prioridad)
    #
==========================================================================
    # Las reglas se verifican de mayor a menor prioridad
    # La primera regla que coincida determina el grupo de UPF
    rules: [
      # Regla 1: Tráfico IMS - Mayor Prioridad
      %{
        name: "Tráfico IMS",
        priority: 20,
        match_field: :apn,
        match_regex: "^ims",
        upf_pool: [
          %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80},
          %{remote_ip_address: "10.100.2.22", remote_port: 8805,
weight: 20}
```

```
        ],
        # Opcional: Sobrescribir PCO para esta regla
        pco: %{
          p_cscf_ipv4_address_list: ["203.0.113.100",
"203.0.113.101"]
        }
      },

      # Regla 2: APN Empresarial - Alta Prioridad
      %{
        name: "Tráfico Empresarial",
        priority: 15,
        match_field: :apn,
        match_regex: "^(enterprise|corporate)\.apn",
        upf_pool: [
          %{remote_ip_address: "10.100.3.21", remote_port: 8805,
weight: 100}
        ],
        pco: %{
          primary_dns_server_address: "192.168.1.10",
          secondary_dns_server_address: "192.168.1.11",
          ipv4_link_mtu_size: 1500
        }
      },

      # Regla 3: Suscriptores en Roaming - Prioridad Media
      %{
        name: "Suscriptores en Roaming",
        priority: 10,
        match_field: :serving_network_plmn_id,
        match_regex: "^(310|311|312|313)",  # Redes de EE. UU.
        upf_pool: [
          %{remote_ip_address: "10.100.4.21", remote_port: 8805,
weight: 100}
        ]
      },

      # Regla 4: Tráfico de Internet - Baja Prioridad
      %{
        name: "Tráfico de Internet",
        priority: 5,
        match_field: :apn,
        match_regex: "^internet",
        upf_pool: [
```

```
          %{remote_ip_address: "10.100.1.21", remote_port: 8805,
weight: 33},
          %{remote_ip_address: "10.100.1.22", remote_port: 8805,
weight: 33},
          %{remote_ip_address: "10.100.1.23", remote_port: 8805,
weight: 34}
        ]
      }
    ],

    #
================================================================
    # Grupo de Respaldo (Último Recurso)
    #
================================================================
    # Utilizado cuando no coinciden reglas y la selección DNS falla o
está deshabilitada
    fallback_pool: [
      %{remote_ip_address: "127.0.0.21", remote_port: 8805, weight:
100}
    ]
  }
```

Campos de Coincidencia Soportados

Campo de Coincidencia	Descripción	Valor de Ejemplo
`:imsi`	Identidad Internacional del Suscriptor Móvil	`"310260123456789"`
`:apn`	Nombre del Punto de Acceso	`"internet"`, `"ims"`
`:serving_network_plmn_id`	PLMN de red de servicio (MCC+MNC)	`"310260"` (red de prueba)
`:sgw_ip_address`	Dirección IP de SGW (formato de cadena)	`"10.0.1.50"`
`:uli_tai_plmn_id`	ID de PLMN del Área de Seguimiento	`"310260"`
`:uli_ecgi_plmn_id`	ID de PLMN de la Celda E-UTRAN	`"310260"`

Grupo de UPF y Balanceo de Carga

Cada regla puede especificar un **grupo de UPF** con selección aleatoria ponderada:

```
upf_pool: [
  %{remote_ip_address: "10.100.1.21", remote_port: 8805, weight:
50},
  %{remote_ip_address: "10.100.1.22", remote_port: 8805, weight:
30},
  %{remote_ip_address: "10.100.1.23", remote_port: 8805, weight:
20}
]
```

Cómo Funciona la Selección Ponderada:

1. Calcular peso total: 50 + 30 + 20 = 100

2. Generar número aleatorio: 0.0 a 100.0
3. Seleccionar UPF según los rangos de peso acumulativos:
    - 0-50: UPF-1 (50% de probabilidad)
    - 50-80: UPF-2 (30% de probabilidad)
    - 80-100: UPF-3 (20% de probabilidad)

Casos de Uso:

- **Distribución equitativa:** Todos los pesos iguales (33, 33, 34)
- **Primario/respaldo:** Primario de alto peso (80), respaldo de bajo peso (20)
- **Basado en capacidad:** Peso proporcional a la capacidad del UPF

Sobrescrituras de PCO

Las reglas pueden sobrescribir valores de PCO (Opciones de Configuración de Protocolo):

```
%{
  name: "Tráfico IMS",
  match_field: :apn,
  match_regex: "^ims",
  upf_pool: [...],
  pco: %{
    # Sobrescribir solo campos específicos
    p_cscf_ipv4_address_list: ["203.0.113.100", "203.0.113.101"],
    # Otros campos utilizan valores predeterminados de la
configuración principal de pco
  }
}
```

Campos de Sobrescritura de PCO Disponibles:

- `primary_dns_server_address`
- `secondary_dns_server_address`
- `primary_nbns_server_address`
- `secondary_nbns_server_address`
- `p_cscf_ipv4_address_list`
- `ipv4_link_mtu_size`

Selección Basada en DNS

Cuando está habilitada, PGW-C realiza consultas DNS NAPTR basadas en la Información de Ubicación del Usuario:

```
upf_selection: %{
  dns_enabled: true,
  dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
  dns_suffix: "epc.3gppnetwork.org",
  dns_timeout_ms: 5000
}
```

Prioridad de Consulta:

1. **ECGI** (Identificador Global de Celda E-UTRAN) - Más específico
2. **TAI** (Identidad del Área de Seguimiento) - Área de celda
3. **RAI** (Identidad del Área de Enrutamiento) - Área 3G/2G
4. **SAI** (Identidad del Área de Servicio) - Área de servicio 3G
5. **CGI** (Identidad Global de Celda) - Celda 2G

Ejemplo de Consulta DNS:

```
# Para consulta ECGI:
eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org

# Para consulta TAI:
tac-lb64.tac-hb00.tac.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Proceso de Selección DNS:

1. Intentar consultas en orden de prioridad (ECGI primero, luego TAI, etc.)
2. Si DNS devuelve candidatos, usar el primer resultado (registrado dinámicamente si es necesario)
3. Seleccionar el UPF devuelto
4. Si no hay coincidencia DNS o DNS deshabilitado, pasar al grupo de respaldo

Ver Selección de UPF Basada en DNS para información detallada.

Selección de UPF Basada en DNS

Descripción General

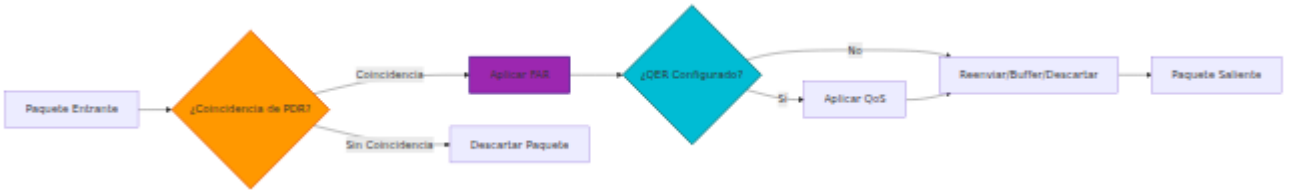
La selección de UPF basada en DNS proporciona **enrutamiento consciente de la ubicación** realizando consultas DNS NAPTR utilizando la Información de Ubicación del Usuario (ULI) de la celda actual del UE.

Referencia 3GPP: TS 23.003 - Procedimientos DNS para el descubrimiento de UPF

Beneficios:

- Selección automática de UPF basada en la ubicación geográfica
- Sin configuración manual de reglas por celda
- Adaptación dinámica a cambios en la topología de la red
- Reduce el backhaul al enrutarse al UPF más cercano

Cómo Funciona



Configuración

```
config :pgw_c,
  upf_selection: %{
    # Habilitar selección basada en DNS
    dns_enabled: true,

    # Prioridad de consulta: intentar ECGI primero, luego TAI,
luego RAI, etc.
    dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],

    # Sufijo DNS para consultas
    dns_suffix: "epc.3gppnetwork.org",

    # Tiempo de espera de consulta DNS
    dns_timeout_ms: 5000,

    # Las reglas estáticas aún tienen prioridad sobre DNS
    rules: [...],

    # Respaldo si DNS falla
    fallback_pool: [...]
  }
```

Formatos de Consulta DNS

Las consultas DNS se construyen utilizando la Información de Ubicación del Usuario (ULI) del mensaje GTP-C:

1. ECGI (Identificador Global de Celda E-UTRAN)

Más específico - Enrutamiento a nivel de celda LTE

Formato:

```
eci-<HEX-ECI>.ecgi.epc.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Ejemplo:

```
# ID de Celda: 0x1A2B3C (1,715,004 decimal)
# PLMN: MCC=999, MNC=999
eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Cuándo se Usa: Redes LTE (4G)

2. TAI (Identidad del Área de Seguimiento)

Área de celda - Múltiples celdas en la misma área de seguimiento

Formato:

```
tac-lb<LB>.tac-hb<HB>.tac.epc.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Ejemplo:

```
# TAC: 0x0064 (100 decimal)
# Byte bajo: 0x64, Byte alto: 0x00
tac-lb64.tac-hb00.tac.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Cuándo se Usa: Áreas de seguimiento LTE (4G)

3. RAI (Identidad del Área de Enrutamiento)

Área de enrutamiento 3G/2G

Formato:

```
rac<RAC>.lac-lb<LB>.lac-hb<HB>.lac.rai.mnc<MNC>.mcc<MCC>.
<dns_suffix>
```

Ejemplo:

```
# RAC: 0x0A (10 decimal)
# LAC: 0x1234 (4660 decimal)
rac0a.lac-lb34.lac-hb12.lac.rai.mnc999.mcc999.epc.3gppnetwork.org
```

Cuándo se Usa: Redes UMTS/GPRS 3G/2G

4. SAI (Identidad del Área de Servicio)

Área de servicio 3G

Formato:

```
sac<SAC>.lac-lb<LB>.lac-hb<HB>.lac.sai.mnc<MNC>.mcc<MCC>.
<dns_suffix>
```

Ejemplo:

```
# SAC: 0x0001
# LAC: 0x1234
sac0001.lac-lb34.lac-
hb12.lac.sai.mnc999.mcc999.epc.3gppnetwork.org
```

Cuándo se Usa: Áreas de servicio UMTS 3G

5. CGI (Identidad Global de Celda)

Nivel de celda 2G

Formato:

```
ci<CI>.lac-lb<LB>.lac-hb<HB>.lac.cgi.mnc<MNC>.mcc<MCC>.
<dns_suffix>
```

Ejemplo:

```
# CI: 0x5678
# LAC: 0x1234
ci5678.lac-lb34.lac-hb12.lac.cgi.mnc999.mcc999.epc.3gppnetwork.org
```

Cuándo se Usa: Celdas GSM 2G

Procesamiento de Respuestas DNS

Formato de Registro NAPTR:

DNS devuelve registros NAPTR que apuntan a direcciones IP de UPF:

```
eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org.
  IN NAPTR 10 50 "a" "x-3gpp-upf:x-s5-gtp:x-s8-gtp" ""
upf1.epc.mnc999.mcc999.3gppnetwork.org.

upf1.epc.mnc999.mcc999.3gppnetwork.org.
  IN A 10.100.1.21
```

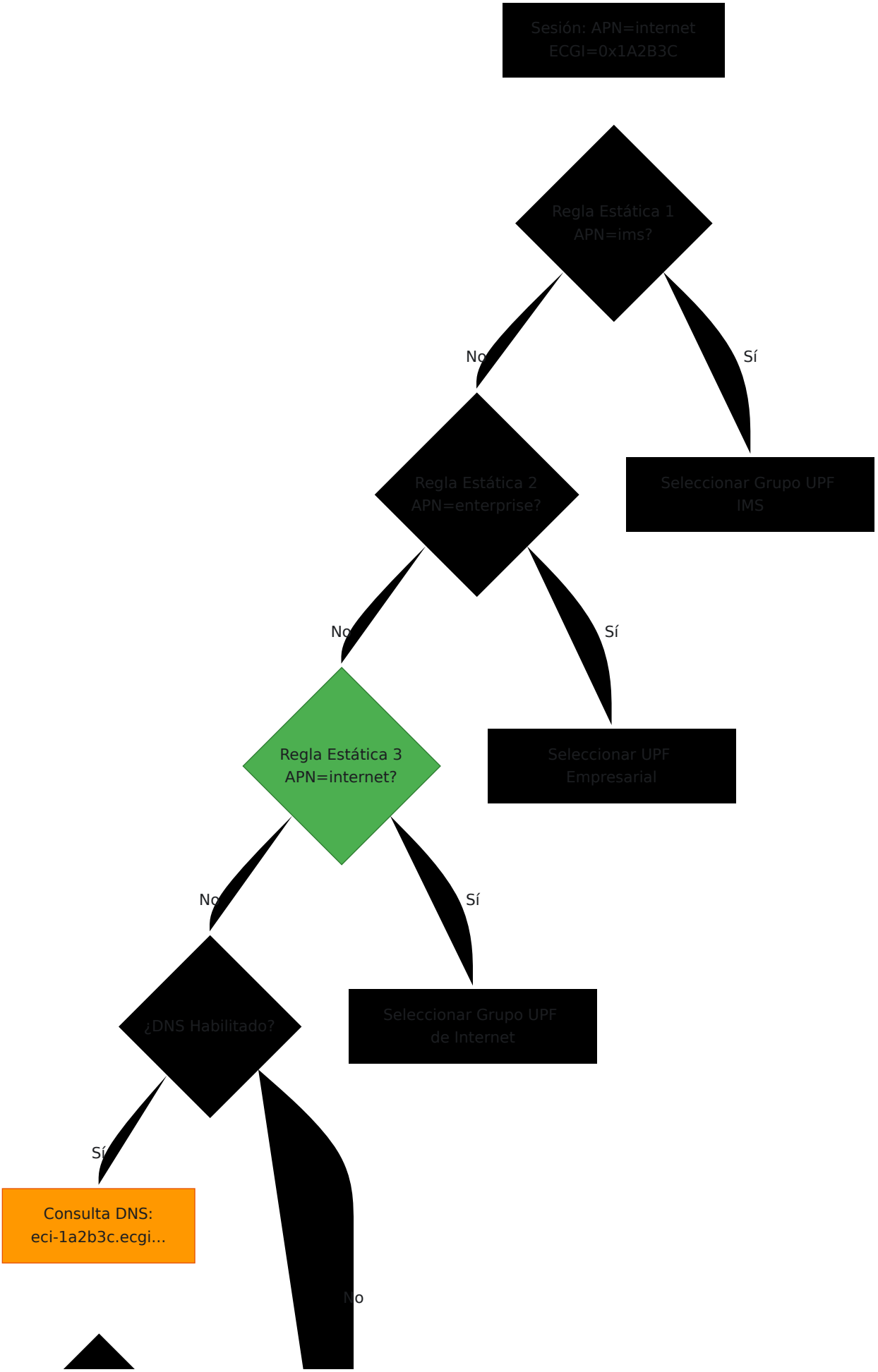
Procesamiento de PGW-C:

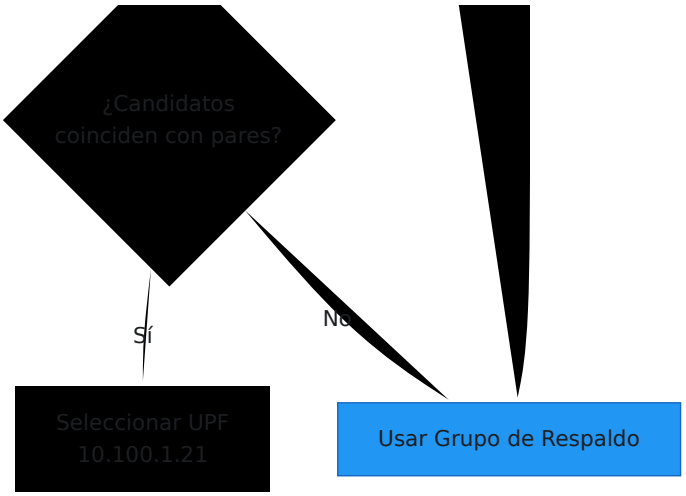
1. Analizar registros NAPTR para extraer direcciones IP de UPF
2. Seleccionar el primer candidato de la respuesta DNS
3. Registrar dinámicamente si no está ya configurado (o implementar selección basada en carga)

Ejemplo:

```
DNS devuelve: [10.100.1.21, 10.100.5.99, 10.200.3.50]

Seleccionado:    10.100.1.21 (primer candidato)
Acción:         Registrar dinámicamente si no está en
upf_selection
```

Ejemplo de Prioridad de Selección


Sesión: APN=internet
ECGI=0x1A2B3C
Regla Estática 1
APN=ims?
No
Sí
Seleccionar Grupo UPF
IMS
Regla Estática 2
APN=enterprise?
No
Sí
Seleccionar UPF
Empresarial
Regla Estática 3
APN=internet?
No
Sí
Seleccionar Grupo UPF
de Internet
¿DNS Habilitado?
Sí
Consulta DNS:
eci-1a2b3c.ecgi...
No



Casos de Uso

1. Balanceo de Carga Geográfico

Escenario: El operador tiene UPFs en múltiples ciudades

Configuración DNS:

```
# Celda de Chicago
eci-aaa.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-Chicago
(10.1.1.21)

# Celda de Nueva York
eci-bbb.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-NewYork
(10.2.1.21)

# Celda de Los Ángeles
eci-ccc.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-
LosAngeles (10.3.1.21)
```

Beneficio: Los usuarios se enrutan automáticamente al UPF más cercano, reduciendo la latencia y el backhaul

2. Computación en el Borde

Escenario: UPFs de MEC (Computación de Acceso Múltiple) desplegados en sitios de celdas

Configuración DNS:

```
# Cada celda apunta al UPF de borde local
eci-*.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF de Borde Local
```

Beneficio: Latencia ultra-baja para aplicaciones en el borde

3. Topología de Red Dinámica

Escenario: Las direcciones de UPF cambian debido a actualizaciones o mantenimiento

Beneficio: Actualizar registros DNS sin cambiar la configuración de PGW-C

Resolución de Problemas de Selección DNS

Fallos en Consultas DNS

Síntomas:

- Registro: "La selección de UPF por DNS falló: :nxdomain"
- Las sesiones caen en el grupo de respaldo

Causas Posibles:

1. Servidor DNS no configurado correctamente
2. Zona DNS no poblada para IDs de celda
3. ULI no presente en el mensaje GTP-C

Resolución:

```
# Probar consulta DNS manualmente
dig eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org NAPTR

# Verificar registros de PGW-C para consultas DNS
grep "DNS UPF selection: querying" /var/log/pgw_c.log

# Verificar que ULI esté presente en la sesión
# Verificar el campo "uli" en el estado de la sesión
```

DNS Devuelve UPF Desconocido

Comportamiento:

- DNS devuelve un UPF candidato que no está en `upf_selection`
- El sistema intenta registrar dinámicamente
- Si la asociación PFCP tiene éxito, se utiliza para la sesión
- Si la asociación PFCP falla, se pasa al grupo de respaldo

Ejemplo:

```
DNS devuelve: [10.99.1.50]
upf_selection: [10.100.1.21, 10.100.1.22]

Acción: Registrar dinámicamente 10.99.1.50
  - Enviar Configuración de Asociación PFCP
  - Si tiene éxito: Usar para la sesión
  - Si hay tiempo de espera: Pasar al grupo de respaldo
```

Opciones de Resolución:

1. Preconfigurar en `upf_selection` para monitoreo inmediato:

```
upf_selection: %{
  fallback_pool: [
    %{remote_ip_address: "10.99.1.50", remote_port: 8805, weight:
100}
  ]
}
```

2. Actualizar DNS para devolver IPs de UPF preconfigurados

3. Permitir registro dinámico (recomendado para escenarios de MEC/borde)

Tiempo de Espera de Consulta

Síntomas:

- Registro: "Selección de UPF DNS: tiempo de espera de consulta"

- Las sesiones tardan más en establecerse

Resolución:

```
upf_selection: %{
  dns_timeout_ms: 10000  # Aumentar tiempo de espera a 10 segundos
}
```

Monitoreo de Selección DNS

Métricas:

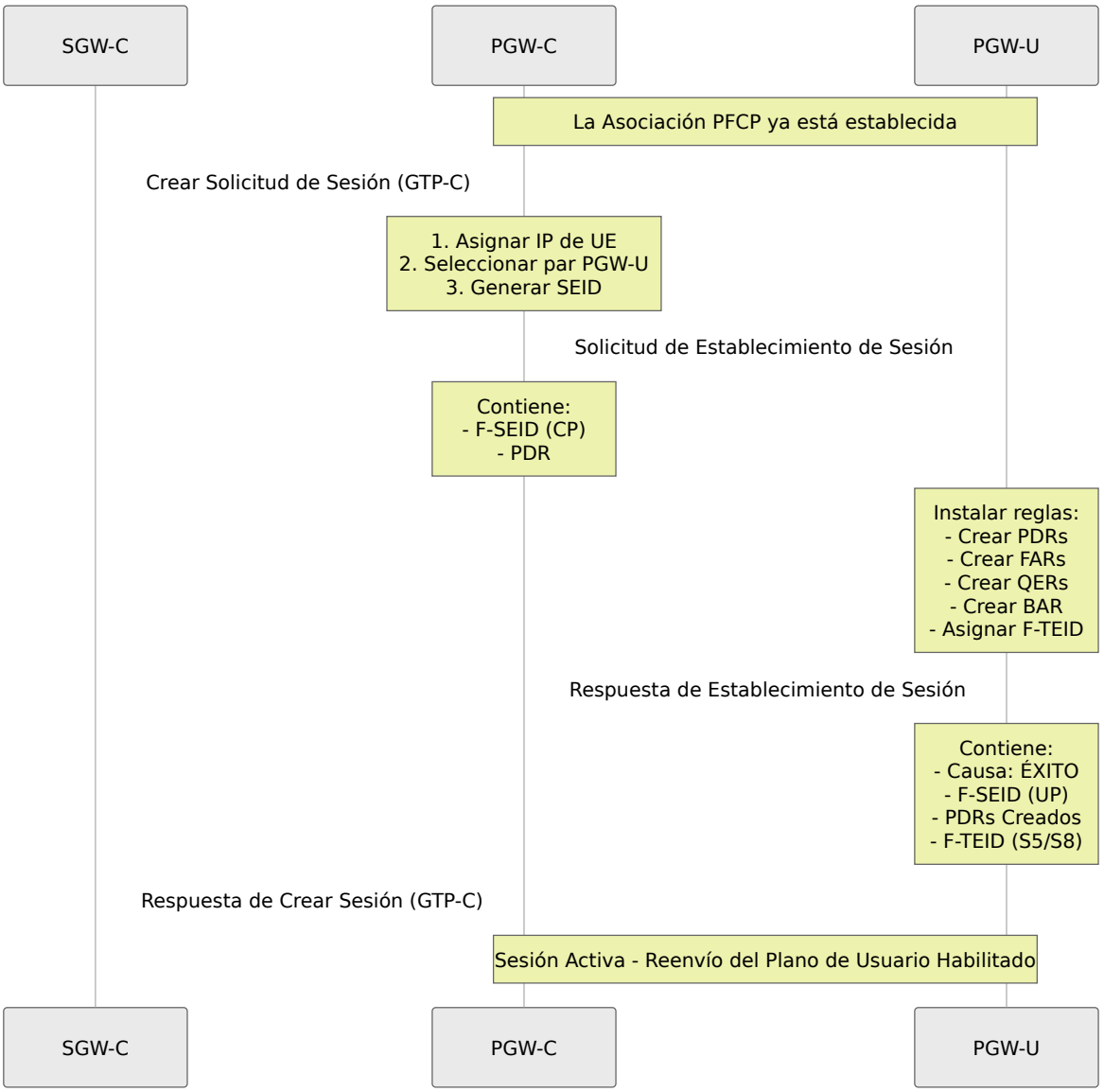
```
# Tasa de éxito de consultas DNS
rate(upf_selection_dns_success_total[5m]) /
rate(upf_selection_dns_attempts_total[5m])

# Latencia de consultas DNS
histogram_quantile(0.95,
rate(upf_selection_dns_duration_seconds_bucket[5m]))

# Uso de respaldo (indica problemas de DNS)
rate(upf_selection_fallback_used_total[5m])
```

Ejemplos de Registros:

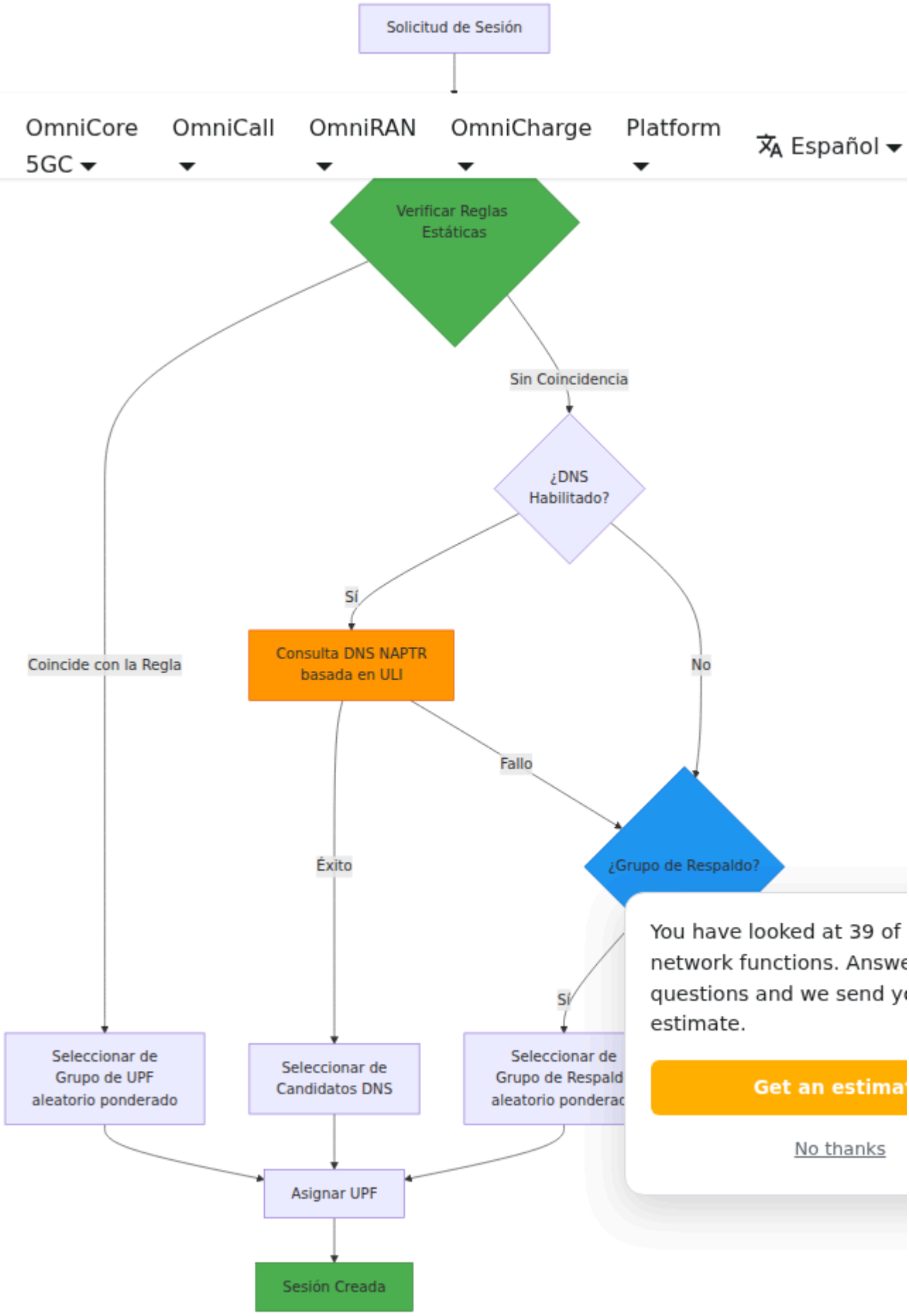
```
[debug] Selección de UPF DNS: consultando eci-
1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org
[debug] Selección de UPF DNS: obtuvo 2 candidatos de DNS
[info]  Selección de UPF DNS: seleccionado 10.100.1.21
```

Flujos de Mensajes

Flujo Completo de Establecimiento de Sesión

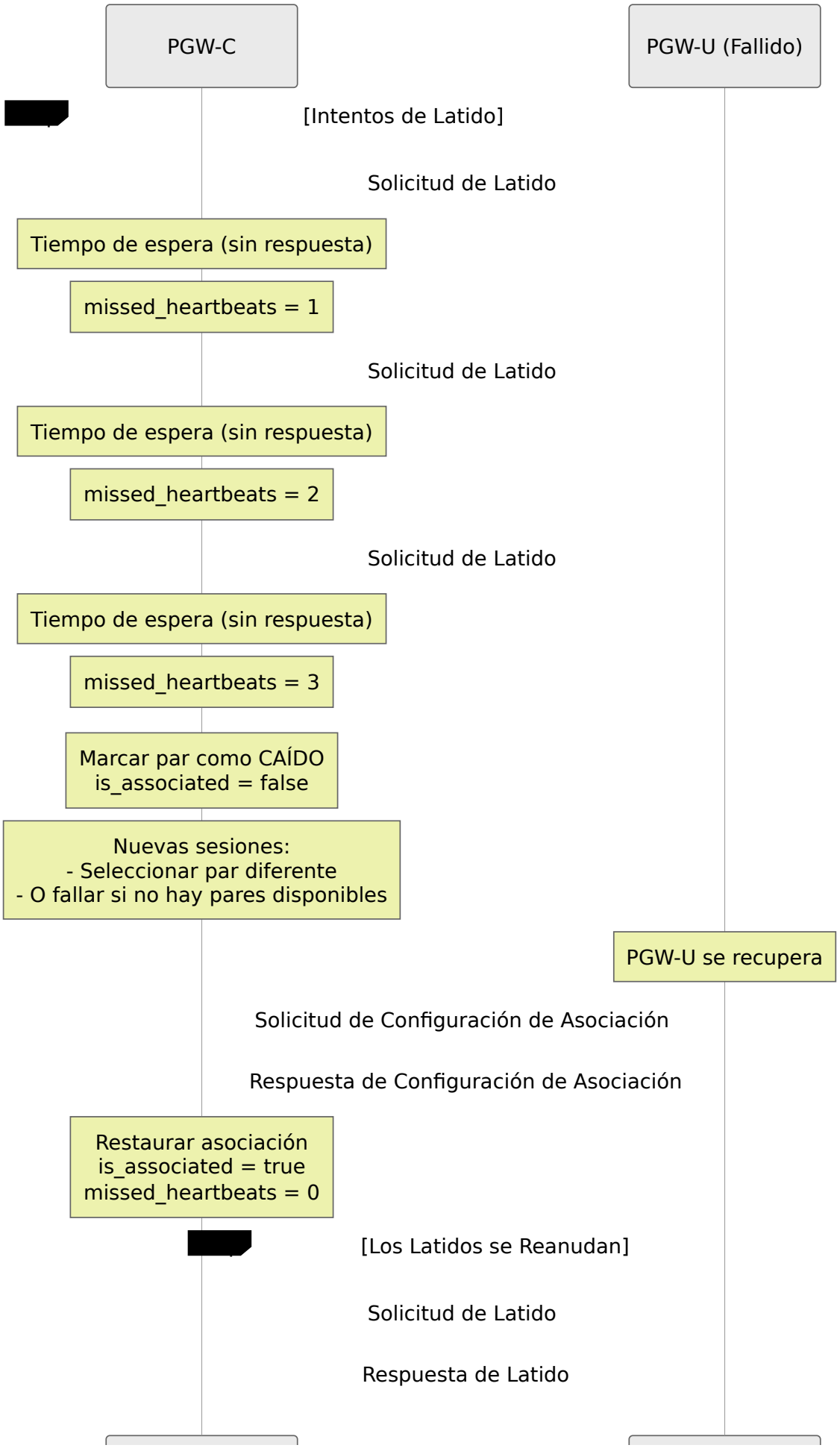


Flujo de Modificación de Sesión



You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima
No thanks

Recuperación de Fallos de Latido


PGW-C
PGW-U (Fallido)
[Intentos de Latido]
Solicitud de Latido
Tiempo de espera (sin respuesta)
missed_heartbeats = 1
Solicitud de Latido
Tiempo de espera (sin respuesta)
missed_heartbeats = 2
Solicitud de Latido
Tiempo de espera (sin respuesta)
missed_heartbeats = 3
Marcar par como CAÍDO
is_associated = false
Nuevas sesiones:
- Seleccionar par diferente
- O fallar si no hay pares disponibles
PGW-U se recupera
Solicitud de Configuración de Asociación
Respuesta de Configuración de Asociación
Restaurar asociación
is_associated = true
missed_heartbeats = 0
[Los Latidos se Reanudan]
Solicitud de Latido
Respuesta de Latido

PGW-C

PGW-U (Fallido)

Resolución de Problemas

Problemas Comunes

1. La Configuración de Asociación Falla

Síntomas:

- Mensaje de registro: "La Configuración de Asociación PFCP falló"
- Sin respuesta a la Solicitud de Configuración de Asociación

Causas Posibles:

- PGW-U no es accesible (problema de red)
- PGW-U no está en funcionamiento
- Firewall bloqueando el puerto UDP 8805
- ID de `remote_ip_address` incorrecto en la configuración

Resolución:

```
# Probar conectividad
ping <pgw_u_ip_address>

# Probar puerto UDP
nc -u -v <pgw_u_ip_address> 8805

# Verificar firewall
iptables -L -n | grep 8805
```

2. Fallos en los Latidos

Síntomas:

- Registro: "Fallos consecutivos de latido: 3"

- Asociación marcada como caída

Causas Posibles:

- Latencia de red o pérdida de paquetes
- PGW-U sobrecargado
- Intervalo de latido demasiado agresivo

Resolución:

El período de latido está fijado en 5 segundos con un umbral de fallo de 3 latidos perdidos consecutivos.

3. El Establecimiento de Sesión Falla

Síntomas:

- Respuesta de Crear Sesión con código de error
- Registro: "El Establecimiento de Sesión PFCP falló"

Causas Posibles:

- No hay pares PGW-U disponibles
- Agotamiento de recursos del PGW-U
- Configuración de regla inválida

Verificar:

1. Verifique que al menos un par tenga `is_associated = true`
2. Verifique los registros de PGW-U para errores
3. Verifique la unicidad de SEID

4. Errores de SEID Duplicados

Síntomas:

- Respuesta de Establecimiento de Sesión: Causa "Contexto de sesión no encontrado"

Causa:

- Colisión de SEID (muy raro)
- Reinicio de PGW-U sin conocimiento de PGW-C

Resolución:

- Reinicie la asociación PFCP (dispara una nueva marca de tiempo de recuperación)
- PGW-C detectará el reinicio de PGW-U y limpiará sesiones antiguas

Monitoreo de la Salud de PFCP

Métricas a Monitorear:

```
# Estado de asociación del par PFCP
pfcp_peer_associated{peer="PGW-U Primario"} 1

# Sesiones PFCP activas
seid_registry_count 150

# Tasas de mensajes PFCP
rate(sxb_inbound_messages_total[5m])

# Errores PFCP
rate(sxb_inbound_errors_total[5m])

# Fallos de latido
pfcp_consecutive_heartbeat_failures{peer="PGW-U Primario"} 0
```

Ejemplos de Alertas:

```
# Alerta sobre asociación caída
- alert: PFCPAssociationDown
  expr: pfcp_peer_associated == 0
  for: 1m
  annotations:
    summary: "El par PFCP {{ $labels.peer }} está caído"

# Alerta sobre altas tasas de fallos en el establecimiento de sesione
- alert: PFCPSessionEstablishmentFailureHigh
  expr:
rate(sxb_inbound_errors_total{message_type="session_establishment_res
[5m]) > 0.1
  for: 5m
  annotations:
    summary: "Alta tasa de fallos en el establecimiento de sesiones F
```

Monitoreo de PFCP

El estado de la asociación PFCP/Sxb y de los pares UPF se monitorea a través de la API REST OAM. La API se sirve a través de HTTPS/TLS en el puerto `8443` con todas las rutas bajo el prefijo `/api` documentación interactiva (Swagger UI) está disponible en `https://<omnipgw-ip>:8443/api/docs`.

Estado de UPF / Par PFCP

```
GET /api/upf            # todos los pares UPF / PFCP + estado
GET /api/upf/<ip>       # un UPF por IP
```

Propósito: Monitorear el estado de asociación PFCP con todos los pares PGW-U configurados.

Ejemplo:

```
curl -k https://<omnipgw-ip>:8443/api/upf
curl -k https://<omnipgw-ip>:8443/api/upf/10.0.0.1
```

Información por Par devuelta para cada par PGW-U configurado:

Campo	Descripción
Nombre del Par	Nombre amigable de la configuración
Dirección IP	IP remota de PGW-U
Estado de Asociación	Asociado o No Asociado
ID de Nodo	Identificador de Nodo PFCP
Marca de Tiempo de Recuperación	Última hora de reinicio del par
Período de Latido	Intervalo de latido configurado
Latidos Perdidos Consecutivos	Conteo actual de fallos
Características de Función UP	Capacidades publicitadas por PGW-U

`GET /api/upf/<ip>` devuelve el estado completo para un solo par, incluyendo el mapa de características de función UP y las marcas de tiempo de asociación.

Inspección de Sesiones PFCP

Las sesiones PFCP activas son visibles a través del detalle de sesión por suscriptor:

```
GET /api/sessions/<imsi>
```

El detalle de la sesión incluye el par PGW-U asociado y las reglas de reenvío programadas (PDRs, FARs, QERs, BARs) y F-SEIDs para la sesión.

Casos de Uso Operacionales

Monitorear la Salud de la Asociación PFCP:

```
1. GET /api/upf
2. Verificar que todos los pares muestren "Asociado"
3. Verificar que el conteo de latidos perdidos = 0
4. Si un par muestra "No Asociado":
   - Verificar la accesibilidad de la IP del par
   - Verificar que el par esté en funcionamiento
   - Verificar el firewall (UDP 8805)
```

Resolver Fallos en el Establecimiento de Sesiones:

```
1. La sesión del usuario falla al establecerse
2. GET /api/sessions/<imsi> - ¿existe la sesión?
3. Inspeccionar el estado PFCP de la sesión - ¿sesión PFCP creada?
4. Si no hay sesión PFCP:
   - GET /api/upf - ¿hay algún par asociado?
   - Verificar registros para errores PFCP
5. Si existe sesión PFCP:
   - Inspeccionar PDRs/FARs para verificar reglas programadas
   - El problema es probablemente aguas abajo (PGW-U o red)
```

Verificar Distribución de Carga del Par:

```
1. Con múltiples pares PGW-U configurados
2. GET /api/upf para revisar el estado de cada par
3. Verificar que las sesiones estén distribuidas entre los pares
4. Identificar si un par tiene carga desproporcionada
```

Detectar Fallos en el Par:

- `GET /api/upf` informa el estado "No Asociado" por par
- El contador de latidos perdidos muestra degradación antes del fallo total
- Configurar alertas de monitoreo basadas en los datos de la API OAM

Ventajas:

- **Monitoreo programable** - Consultar `GET /api/upf` desde herramientas o alertas
- **Estado explícito** - Asociado / no asociado por par

- **Tendencias de salud del par** - El conteo de latidos perdidos muestra advertencias tempranas
- **Inspección a nivel de sesión** - Ver exactamente PDRs/FARs/QERs programados

---

Documentación Relacionada

Configuración

- **Guía de Configuración** - Selección de UPF, monitoreo de salud, configuración de PFCP
- **Gestión de Sesiones** - Ciclo de vida de la sesión PDN, establecimiento de portadores

Carga y Monitoreo

- **Interfaz Diameter Gx** - Reglas PCC que impulsan la aplicación de QoS de PFCP
- **Interfaz Diameter Gy** - Gestión de cuotas de carga en línea a través de URRs
- **Formato de CDR de Datos** - Generación de CDR a partir de informes de uso de PFCP
- **Guía de Monitoreo** - Métricas de PFCP, seguimiento de sesiones, alertas de salud de UPF

Interfaces de Red

- **Interfaz S5/S8** - Gestión de portadores del plano de control
- **Asignación de IP de UE** - Asignación de direcciones de UE a través de PFCP

Volver a la Guía de Operaciones

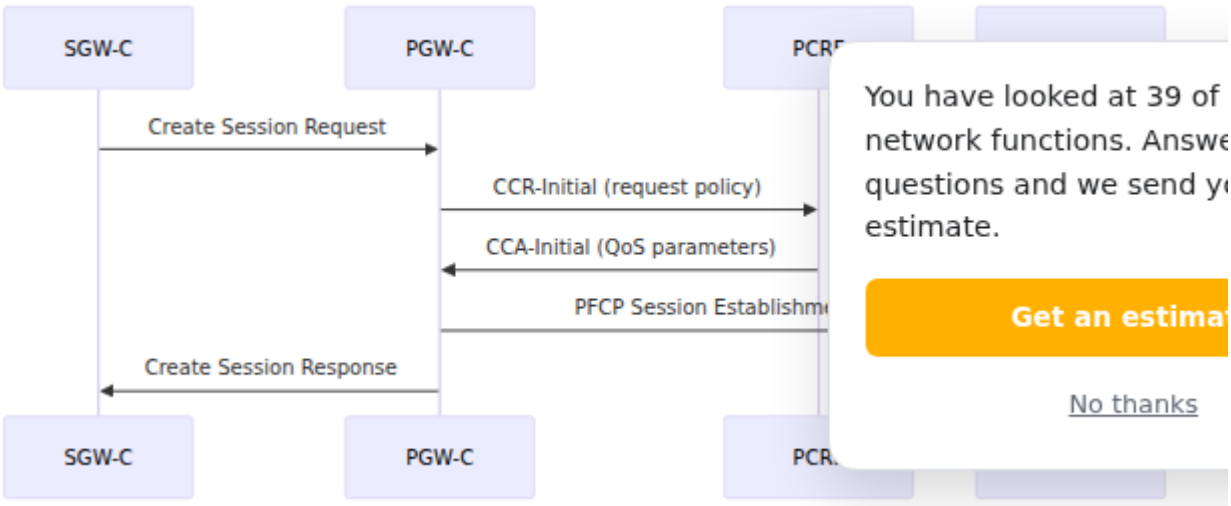
QoS y Gestión de Bearer

Visión General

El PGW-C implementa un sistema de gestión de bearer y QoS basado en políticas que coordina tres interfaces clave:

- **Gx (Diameter)** - Recibe decisiones de políticas y parámetros de QoS del PCRF
- **S5/S8 (GTP-C)** - Gestiona contextos de bearer con SGW-C
- **Sxb (PFCP)** - Programa reglas de aplicación de QoS en PGW-U

Flujo de Arquitectura



Conceptos Clave

- **Sesión**: Contiene información del UE, mapa de bearer, mapas de PDR/FAR/QER/BAR, y AMBR
- **Contexto de Bearer**: Vincula EBI (EPS Bearer ID) a PDRs, FARs y QERs específicos

- **QER (Regla de Aplicación de QoS)**: Aplica l��mites de MBR/GBR y estado de puerta en el plano de usuario
- **Bearer por Defecto**: Siempre creado con la sesión PDN, proporciona conectividad básica
- **Bearer Dedicado**: Creado dinámicamente basado en la política del PCRF, proporciona garantías de QoS específicas

Configuración

Importante: Política de QoS Dinámica

Todos los parámetros de QoS se reciben dinámicamente del PCRF a través de la interfaz Diameter Gx y se definen en el PCRF (Consulte OmniHSS para más información).

Los operadores configuran la **conexión PCRF** en `config/runtime.exs`:

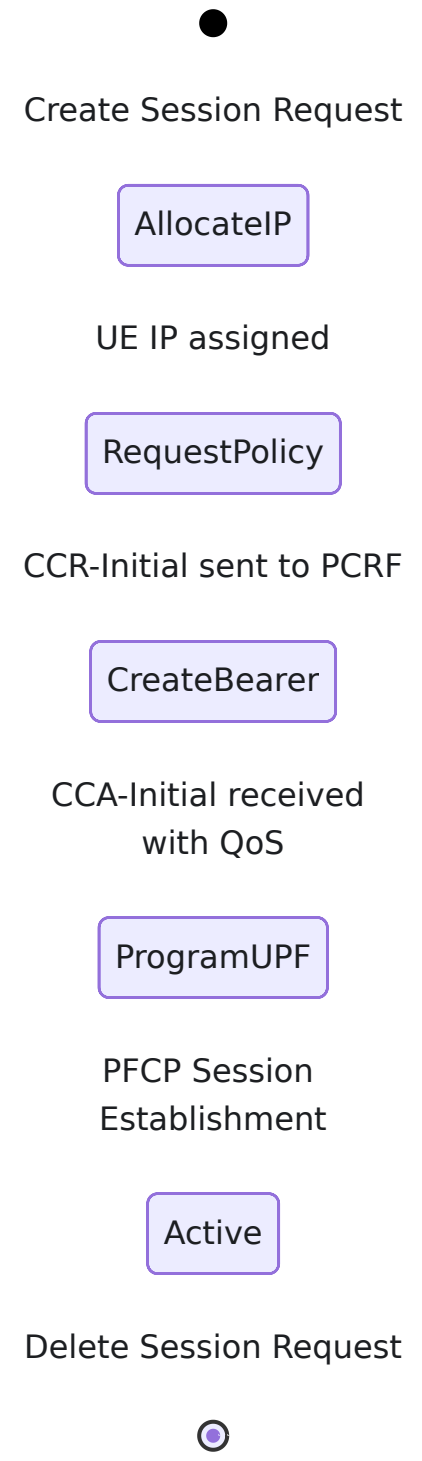
```
config :pgw_c,
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "192.168.1.100",
        initiate_connection: true
      }
    ]
  }
```

Las políticas de QoS, reglas de facturación y límites de ancho de banda se configuran en el PCRF, no en los archivos de configuración de PGW-C.

Ciclo de Vida del Bearer

Creación del Bearer por Defecto

El bearer por defecto se crea durante el establecimiento de la sesión PDN:



Flujo de trabajo:

1. SGW-C envía Create Session Request
2. PGW-C asigna dirección IP del UE desde el grupo configurado
3. PGW-C envía CCR-Initial al PCRF con IMSI, APN, dirección IP
4. PCRF responde con CCA-Initial que contiene parámetros de QoS:
    - Default-EPS-Bearer-QoS (QCI, ARP)
    - QoS-Information (ajustes de AMBR)
5. PGW-C crea contexto de bearer con:
    - IDs fijos: Downlink PDR=1, Uplink PDR=2, Downlink FAR=1, Uplink FAR=2, QER=1, BAR=1
    - QER programado con MBR de QoS de bearer
6. PGW-C envía PFCP Session Establishment Request a PGW-U
7. PGW-C envía Create Session Response a SGW-C

Características del bearer por defecto:

- Siempre existe durante la vida de la sesión PDN
- Típicamente utiliza QCI 5 o QCI 9 (no-GBR)
- EBI rastreado en el estado de la sesión
- No se puede eliminar de forma independiente (eliminarlo termina la sesión)

Creación del Bearer Dedicado

Los bearers dedicados se crean dinámicamente en función de la política del PCRF:

Disparador: Re-Auth Request (RAR) del PCRF con Charging-Rule-Install

Flujo de trabajo:

1. PCRF envía RAR con Charging-Rule-Definition que contiene:
    - Charging-Rule-Name (identificador de regla de política)
    - Flow-Information (filtros de paquetes)
    - QoS-Information (QCI, MBR, GBR, ARP)
    - Precedence (prioridad de coincidencia de regla)
2. PGW-C traduce la regla dinámica a entidades PFCP:
    - Cada entrada de Flow-Information → nuevo PDR con SDF Filter

    - QoS-Information → nuevo QER con aplicación de MBR/GBR
    - Flow-Description → reglas de coincidencia de IP 5-tuple
3. PGW-C envía PFCP Session Modification Request para agregar PDRs/FARs/QERs
4. PGW-C inicia Create Bearer Request a SGW-C
5. SGW-C responde con Create Bearer Response confirmando el establecimiento

Ejemplo de Charging-Rule-Definition:

```
Charging-Rule-Name: "video_streaming"
Flow-Information:
  - Flow-Description: "permit in ip from any to 10.0.0.1 5000-
6000"
    Flow-Direction: 1 (downlink)
QoS-Information:
  QoS-Class-Identifier: 7
  Max-Requested-Bandwidth-UL: 5000000 (5 Mbps)
  Max-Requested-Bandwidth-DL: 10000000 (10 Mbps)
  Guaranteed-Bitrate-UL: 1000000 (1 Mbps)
  Guaranteed-Bitrate-DL: 2000000 (2 Mbps)
Precedence: 100
Flow-Status: 2 (ENABLED)
```

Reglas Vinculadas al Bearer por Defecto

Una regla dinámica cuyo QCI y ARP coinciden con el bearer por defecto se vincula al bearer por defecto (TS 29.212 §4.5.2). No se crea ningún bearer dedicado.

Cuando la regla coincide con todo el tráfico (cada Flow-Description es `permit out ip from any to any`), su MBR limita el APN-AMBR en el propio QER del bearer por defecto:

- Al instalar (CCA-Initial o RAR), el MBR del QER por defecto se convierte en el menor de APN-AMBR y el MBR de la regla, por dirección. Una regla del CCA-Initial ya está en el QER que lleva el Establishment de la Sesión.
- En Charging-Rule-Remove, el QER vuelve al APN-AMBR.

- Un cambio posterior de APN-AMBR del PCRF mantiene el límite mientras la regla esté instalada.

Así es como funciona un límite de uso justo con Sy: el PCRF instala una regla como `throttle` (QCI 9, MBR 1 Mbit/s) cuando se agota el límite, y la elimina después de una recarga.

Una regla de bearer por defecto que coincide solo con parte del tráfico, o que limita una dirección con Flow-Status, necesitaría PDRs propios y no es compatible. Un RAR que lleve uno se responde con DIAMETER_UNABLE_TO_COMPLY (5012). En CCA-Initial se registra y no se aplica.

Modificación del Bearer

La QoS del bearer se puede modificar a través de:

- **Gx RAR** con Charging-Rule-Definition actualizada
- **PFCP Session Modification** para actualizar QERs existentes (cambiar tasas de bits), FARs (cambiar reenvío), o PDRs (cambiar filtros de paquetes)

Eliminación del Bearer

Disparadores:

- **Delete Session Request** (iniciado por SGW) - Elimina el bearer por defecto y termina la sesión
- **Re-Auth Request con Charging-Rule-Remove** (iniciado por PCRF) - Elimina el bearer dedicado

Flujo de trabajo:

1. Eliminar bearer del estado de la sesión
2. Eliminar PDRs/FARs/QERs asociados
3. Enviar Delete Bearer Request a SGW-C (si es iniciado por PCRF)
4. Enviar PFCP Session Modification (eliminar reglas) o Session Deletion (si es bearer por defecto)

Parámetros de QoS

QCI (Identificador de Clase de QoS)

Fuente: PCRF a través de Gx `QoS-Class-Identifier` AVP

Valores Estándar:

- **QCI 1**: Voz Conversacional (GBR, 100ms de presupuesto de retraso)
- **QCI 2**: Video Conversacional (GBR, 150ms de presupuesto de retraso)
- **QCI 3**: Juegos en Tiempo Real (GBR, 50ms de presupuesto de retraso)
- **QCI 4**: Video No Conversacional (GBR, 300ms de presupuesto de retraso)
- **QCI 5**: Señalización IMS (no-GBR, 100ms de presupuesto de retraso) - **Por Defecto para bearer por defecto**
- **QCI 6**: Video (basado en TCP), Transmisión en Vivo (no-GBR, 300ms de presupuesto de retraso)
- **QCI 7**: Voz, Juegos Interactivos (no-GBR, 100ms de presupuesto de retraso)
- **QCI 8**: Video (basado en TCP), por ejemplo, YouTube (no-GBR, 300ms de presupuesto de retraso)
- **QCI 9**: Internet por Defecto (no-GBR, 300ms de presupuesto de retraso)

Nota del Operador:

- El QCI se recibe del PCRF y se señala a SGW-C en Bearer-Level-QoS IE
- PGW-C no aplica directamente el comportamiento del QCI - la aplicación real es a través de MBR/GBR en QERs
- Los valores de QCI más bajos generalmente indican mayor prioridad
- El QCI determina el tratamiento de reenvío de paquetes y la prioridad de programación

ARP (Prioridad de Asignación y Retención)

Fuente: PCRF a través de `Allocation-Retention-Priority` grouped AVP

Componentes:

- **Priority-Level**: 1 (máxima prioridad) a 15 (mínima prioridad)
- **Pre-emption-Capability**: ¿Puede este bearer preemptar bearers de menor prioridad?
  - 0 = HABILITADO (puede preemptar a otros)
  - 1 = DESHABILITADO (no puede preemptar)
- **Pre-emption-Vulnerability**: ¿Puede este bearer ser preemptado por bearers de mayor prioridad?
  - 0 = HABILITADO (puede ser preemptado)
  - 1 = DESHABILITADO (no puede ser preemptado)

Valores por Defecto:

- Priority-Level: 1
- Pre-emption-Capability: HABILITADO (0)
- Pre-emption-Vulnerability: DESHABILITADO (1)

Nota del Operador:

- El ARP se señala a SGW-C y, en última instancia, a eNodeB
- **No es aplicado por PGW-C** - la aplicación se realiza típicamente en eNodeB durante el control de admisión de radio
- Se utiliza durante la congestión de la red para determinar qué bearers admitir o eliminar
- Crítico para servicios de emergencia (nivel de prioridad 1) y servicios de alto valor

MBR (Tasa de Bits Máxima)

Fuente: PCRF a través de `Max-Requested-Bandwidth-UL` y `Max-Requested-Bandwidth-DL` AVPs

Formato: Bytes por segundo (convertido a kbps internamente: `bytes / 1000`)

Aplicado a: Todos los bearers (por defecto y dedicados)

Cómo funciona:

- PGW-C crea QER con `mbr: %Bitrate{ul: kbps_ul, dl: kbps_dl}`

- QER enviado a PGW-U a través de PFCP
- **PGW-U aplica limitación de tasa** (policía de tráfico)
- El tráfico excesivo por encima de MBR es descartado

Ejemplo:

```
Max-Requested-Bandwidth-UL: 5000000 (5 Mbps)
Max-Requested-Bandwidth-DL: 10000000 (10 Mbps)

→ QER creado con mbr: {ul: 5000, dl: 10000} kbps
→ PGW-U descarta paquetes de uplink que exceden 5 Mbps
→ PGW-U descarta paquetes de downlink que exceden 10 Mbps
```

GBR (Tasa de Bits Garantizada)

Fuente: PCRF a través de `Guaranteed-Bitrate-UL` y `Guaranteed-Bitrate-DL` AVPs

Formato: Bytes por segundo (convertido a kbps)

Aplicado a: Bearers dedicados solamente (bearers GBR)

Cómo funciona:

- Si se especifica GBR en Charging-Rule-Definition, el bearer es **tipo GBR**
- PGW-U aplica la garantía de tasa de bits mínima a través de QER
- Requiere programación adecuada en eNodeB para reservar recursos de radio
- Los bearers GBR tienen control de admisión - pueden ser rechazados si no hay recursos disponibles

Ejemplo:

```
Guaranteed-Bitrate-UL: 1000000 (1 Mbps)
Guaranteed-Bitrate-DL: 2000000 (2 Mbps)

→ QER creado con gbr: {ul: 1000, dl: 2000} kbps
→ La red garantiza al menos 1 Mbps de uplink y 2 Mbps de downlink
→ Utilizado para VoIP, videollamadas, transmisión en vivo
```

Nota del Operador:

- GBR requiere una planificación de capacidad de red suficiente
- Sobresuscribir recursos GBR lleva a fallos de admisión
- Monitorear el uso de GBR a través de conteos de sesión y métricas de bearer

AMBR (Tasa de Bits Máxima Agregada)

Fuente: PCRF a través de `APN-Aggregate-Max-Bitrate-UL` y `APN-Aggregate-Max-Bitrate-DL` AVPs

Alcance: Se aplica a **todos los bearers no-GBR** para el APN (no por bearer)

Cómo funciona:

- AMBR es un límite agregado en todos los bearers no-GBR en una sesión
- Enviado a SGW-C en Create Session Response
- La aplicación se realiza típicamente en eNodeB/SGW
- PGW-C almacena AMBR en el estado de la sesión y lo señala a SGW-C

Ejemplo:

```
APN-Aggregate-Max-Bitrate-UL: 50000000 (50 Mbps)
APN-Aggregate-Max-Bitrate-DL: 100000000 (100 Mbps)

→ Todos los bearers no-GBR combinados no pueden exceder 50 Mbps de
uplink / 100 Mbps de downlink
→ Los bearers individuales están limitados por su propio MBR
→ AMBR proporciona un límite adicional general por UE/APN
```

Nota del Operador:

- Establecido a través del perfil del suscriptor en HSS/PCRF
- Utilizado para hacer cumplir niveles de suscripción (por ejemplo, plan de 10 Mbps vs plan de 100 Mbps)
- No afecta a los bearers GBR

Estado del Flujo y Control de Puertas

Mapeo del Estado del Flujo (Gx) al Estado de la Puerta (PFCP)

El PCRF controla si se permite el tráfico a través del AVP `Flow-Status` en Charging-Rule-Definition:

Flow-Status (Gx)	Gate-Status (PFCP QER)	Significado
0 = ENABLED-UPLINK	ul: OPEN, dl: CLOSED	Solo se permite tráfico de uplink
1 = ENABLED-DOWNLINK	ul: CLOSED, dl: OPEN	Solo se permite tráfico de downlink
2 = ENABLED	ul: OPEN, dl: OPEN	Se permiten ambas direcciones
3 = DISABLED	ul: CLOSED, dl: CLOSED	No se permite tráfico
4 = REMOVED	ul: CLOSED, dl: CLOSED	Bearer siendo eliminado

Casos de uso:

- **DISABLED**: Utilizado para servicios aparcados o agotamiento de crédito (paquetes descartados pero bearer retenido)
- **ENABLED-UPLINK**: Inusual, pero podría ser utilizado para servicios solo de carga
- **ENABLED-DOWNLINK**: Servicios solo de descarga o escenarios limitados por crédito
- **ENABLED**: Operación normal

Monitoreo y Observabilidad

Métricas de Prometheus

Métricas a nivel de sesión:

```
session_registry_count        # Bearers activos (pares IMSI, EBI)
address_registry_count        # IPs de UE asignadas
charging_id_registry_count    # Sesiones de facturación activas
```

Métricas de la interfaz Gx:

```
gx_inbound_messages_total{message_type="gx_RAR"}     #
Actualizaciones de políticas del PCRF
gx_outbound_messages_total{message_type="gx_CCR"}    # Solicitudes
de políticas al PCRF
gx_outbound_transaction_duration_bucket              # Latencia al
PCRF
```

Métricas de la interfaz PFCP:

```
sxb_outbound_messages_total{message_type="pfcp_session_establishment_
sxb_outbound_messages_total{message_type="pfcp_session_modification_r
sxb_outbound_transaction_duration_bucket
```

Métricas de creación de bearers:

```
s5s8_inbound_messages_total{message_type="create_session_request"}
# Bearers por defecto
s5s8_outbound_messages_total{message_type="create_bearer_request"}
# Bearers dedicados
```

Monitoreo a través de la API OAM

El estado del bearer y QoS se inspecciona a través de la API REST OAM (HTTPS/TLS en el puerto `8443`, rutas bajo el prefijo `/api`). La documentación interactiva (Swagger UI) está disponible en `https://<omnipgw-ip>:8443/api/docs`.

La información del bearer y QoS se expone a través del detalle de sesión por suscriptor:

```
GET /api/sessions/<imsi>       # detalle de sesión incl. bearers,
QCI/5QI, reglas de facturación
```

Ejemplo:

```
curl -k https://<omnipgw-ip>:8443/api/sessions/999000123456789
```

El detalle de la sesión incluye los bearers activos para la sesión, sus parámetros de QoS (QCI/5QI, MBR, GBR, AMBR), las reglas de facturación instaladas y el mapa de QER programado (estado de la puerta y tasas de bits). No hay un endpoint de bearers dedicados; el estado del bearer siempre se lee de la sesión a la que pertenece.

Mensajes de Registro Clave

```
[debug] Sending Credit Control Request: ...          # CCR al PCRF
[debug] Handling Credit Control Answer: ...          # CCA del
PCRF (contiene QoS)
[debug] Handling Re-Auth Request                     # RAR del
PCRF (cambio de política)
[debug] Sending Session Establishment Request        # PFCP a PGW-
U (programar QERs)
[debug] Sending Session Modification Request         # PFCP a PGW-
U (actualizar QERs)
```

Tareas Operativas

Verificar QoS Aplicada a la Sesión

1. `GET /api/sessions/<imsi>` (por ejemplo, `curl -k https://<omnipgw-ip>:8443/api/sessions/999000123456789`)
2. Localizar la sesión para el suscriptor en la respuesta
3. Inspeccionar el detalle de la sesión
4. Verificar la sección **qer_map**:

   ```
   qer_id: 1
   gate_status: {ul: OPEN, dl: OPEN}
   mbr: {ul: 50000, dl: 100000}  # kbps
   gbr: {ul: 10000, dl: 20000}   # kbps (o nil para no-GBR)
   ```

5. Verificar que los valores coincidan con la política esperada del PCRF

Solucionar Problemas de QoS Faltante

Síntoma: Sesión creada pero QoS no aplicada

Pasos:

1. **Verificar conectividad PCRF:**

- Verificar estado del par PCRF = "conectado" (ver las métricas de Diameter/Gx y el estado del par)
- Si está desconectado, verificar conectividad de red y configuración de Diameter

2. **Verificar el intercambio CCR/CCA:**

   - Buscar en los registros de OmniPGW "Credit Control Answer"
   - Verificar que el AVP `QoS-Information` esté presente en el registro de CCA
   - Comprobar si hay errores en CCA (Result-Code debería ser 2001 = ÉXITO)

3. **Verificar programación PFCP:**

   - Buscar en los registros "PFCP Session Establishment Request"
   - Verificar que QER esté incluido en el mensaje
   - Comprobar registros de PGW-U para errores de procesamiento PFCP

4. **Verificar configuración de política PCRF:**

   - Verificar perfil del suscriptor en PCRF
   - Confirmar que existan reglas de política específicas para el APN
   - Comprobar registros de PCRF para errores de evaluación de políticas

Monitorear Tasa de Creación de Bearers

Consultas de Prometheus:

```
# Tasa de creación de bearers por defecto (sesiones/segundo)
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m])

# Tasa de creación de bearers dedicados
rate(s5s8_outbound_messages_total{message_type="create_bearer_request
[5m])

# Tasa de actualización de políticas del PCRF
rate(gx_inbound_messages_total{message_type="gx_RAR"}[5m])
```

Planificación de Capacidad

Métricas clave a monitorear:

```
# Utilización de direcciones IP de UE (porcentaje)
(address_registry_count / <configured_pool_size>) * 100

# Conteo de bearers activos
session_registry_count

# Latencia de consulta PCRF (P95)
histogram_quantile(0.95, gx_outbound_transaction_duration_bucket)
```

Límites de capacidad:

- Tamaño del grupo de direcciones: configurado en `config/runtime.exs` bajo `ue.subnet_map`
- Espacio TEID: 32 bits (4 mil millones de identificadores únicos, gestionados automáticamente)
- Sesiones concurrentes: típicamente limitadas por el tamaño del grupo de direcciones

Directrices de planificación:

- Monitorear la utilización de direcciones IP - escalar el grupo antes de exceder el 80%

- Monitorear la latencia del PCRF - alta latencia impacta el tiempo de configuración de la sesión
- Monitorear la tasa de creación de bearers dedicados - indica la complejidad de la política

Documentación Relacionada

- Gestión de Sesiones - Ciclo de vida de la sesión PDN
- Interfaz Diameter Gx - Detalles del protocolo de política PCRF
- Interfaz PFCP - Programación del plano de usuario
- Guía de Configuración - Configuración del sistema
- Guía de Monitoreo - Métricas y observabilidad

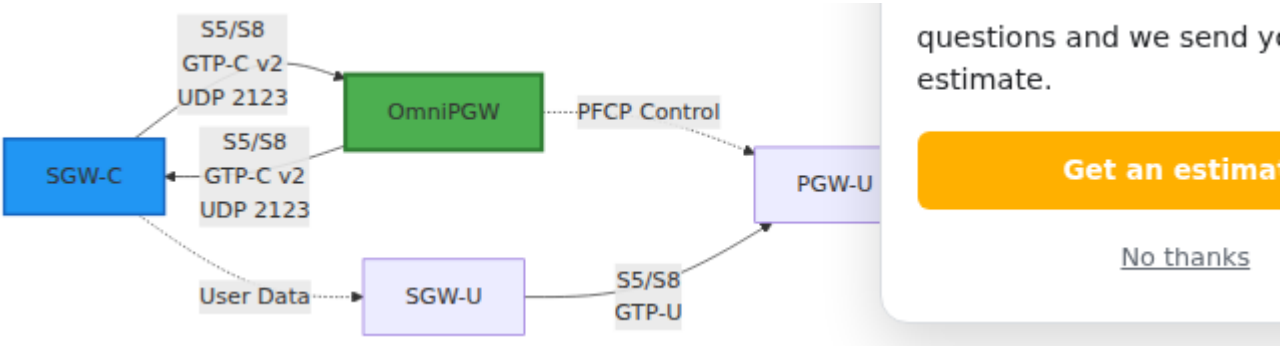
Documentación de la Interfaz S5/S8

Comunicación GTP-C con SGW-C

OmniPGW de Omnitouch Network Services

Descripción General

La **interfaz S5/S8** conecta OmniPGW al SGW-C (plano de control del Gateway de Servicio) utilizando el protocolo **GTP-C v2** (Protocolo de Túnel GPRS - Plano de Control). Esta interfaz maneja la señalización de gestión de sesiones entre los gateways.



Detalles del Protocolo

GTP-C Versión 2

- **Protocolo:** GTP-C v2 (3GPP TS 29.274)
- **Transporte:** UDP
- **Puerto:** 2123 (estándar)
- **Tipo de Interfaz:** Plano de Control

TEID (Identificador de Punto de Final de Túnel)

Cada sesión tiene un **TEID** único para el enrutamiento de mensajes:

- **TEID Local** - Asignado por OmniPGW para mensajes entrantes
- **TEID Remoto** - Asignado por SGW-C para mensajes salientes

```
Flujo de Mensajes:
  SGW-C → OmniPGW: TEID de destino = TEID local de OmniPGW
  OmniPGW → SGW-C: TEID de destino = TEID remoto de SGW-C
```

Configuración

Configuración Básica

```
# config/runtime.exs
config :pgw_c,
  s5s8: %{
    # Dirección IPv4 local para la interfaz S5/S8
    local_ipv4_address: "10.0.0.20",

    # Opcional: Dirección IPv6 local
    local_ipv6_address: nil,

    # Opcional: Sobrescribir puerto por defecto
    local_port: 2123,

    # Tiempo de espera de solicitud GTP-C en milisegundos (por
defecto: 500ms)
    # Tiempo de espera por intento al esperar respuestas GTP-C
(Crear Bearer, Eliminar Bearer, etc.)
    request_timeout_ms: 500,

    # Número de intentos de reintento para solicitudes GTP-C (por
defecto: 3)
    # Tiempo máximo total de espera = request_timeout_ms *
request_attempts
    # Ejemplo: 500ms * 3 intentos = 1500ms (1.5 segundos) en total
    request_attempts: 3
  }
```

Configuración de Tiempo de Espera

La interfaz S5/S8 utiliza tiempos de espera configurables para transacciones de solicitud/respuesta GTP-C.

Parámetros:

- **`request_timeout_ms`** - Tiempo de espera en milisegundos por intento de reintento (por defecto: 500ms)

- **`request_attempts`** - Número de intentos de reintento antes de rendirse (por defecto: 3)

Tiempo Total de Espera: `request_timeout_ms × request_attempts`

Comportamiento por defecto: 500ms × 3 intentos = **1.5 segundos de espera máxima total**

Directrices de Ajuste:

Latencia de Red	**`request_timeout_ms`** recomendado	Tiempo Total de Espera
Baja latencia (<50ms)	200-300ms	600-900ms (3 intentos)
Normal (50-150ms)	500ms (por defecto)	1.5s (3 intentos)
Alta latencia (>150ms)	1000-2000ms	3-6s (3 intentos)
Inestable/satélite	2000-3000ms	6-9s (3 intentos)

Ejemplo - Red de Alta Latencia:

```
s5s8: %{
  local_ipv4_address: "10.0.0.20",
  request_timeout_ms: 1500,  # 1.5 segundos por intento
  request_attempts: 3         # Total: 4.5 segundos máximo
}
```

Cuando ocurre un tiempo de espera:

- OmniPGW registra el error: `"Se agotó el tiempo de espera de la solicitud de creación de bearer"`
- Devuelve error al PCRF (Código de Resultado de Diámetro: 5012 UNABLE_TO_COMPLY)

- El bearer permanece en almacenamiento temprano para limpieza a través de Charging-Rule-Remove

Requisitos de Red

Reglas de Firewall:

```
# Permitir GTP-C desde la red SGW-C
iptables -A INPUT -p udp --dport 2123 -s <sgw_network>/24 -j
ACCEPT

# Permitir GTP-C saliente a SGW-C
iptables -A OUTPUT -p udp --dport 2123 -d <sgw_network>/24 -j
ACCEPT
```

Enrutamiento:

```
# Asegurar ruta a la red SGW-C
ip route add <sgw_network>/24 via <gateway_ip> dev eth0
```

Tipos de Mensajes

La interfaz S5/S8 maneja la señalización GTP-C para la gestión de sesiones PDN. Para un ciclo de vida de sesión detallado y gestión de estado, consulte la Guía de Gestión de Sesiones.

Gestión de Sesiones

Solicitud de Creación de Sesión

Dirección: SGW-C → OmniPGW

Propósito: Establecer una nueva conexión PDN

IEs Clave (Elementos de Información):

Nombre de IE	Tipo	Descripción
IMSI	Identidad	Identidad Internacional del Suscriptor Móvil
MSISDN	Identidad	Número de teléfono móvil
APN	Cadena	Nombre del Punto de Acceso (por ejemplo, "internet")
Tipo de RAT	Enum	Tecnología de Acceso Radio (EUTRAN)
Contexto de Bearer	Agrupado	Información del bearer por defecto
Zona Horaria del UE	Marca de Tiempo	Zona horaria del UE
ULI	Agrupado	Información de Localización del Usuario (TAI, ECGI)
Red de Servicio	PLMN	MCC/MNC de la red de servicio

Ejemplo:

```
Solicitud de Creación de Sesión
├── IMSI: 310260123456789
├── MSISDN: 14155551234
├── APN: internet
├── Tipo de RAT: EUTRAN (6)
├── Contexto de Bearer
│   ├── EBI: 5
│   ├── QoS de Bearer (QCI 9, ARP, tasas de bits)
│   └── S5/S8 F-TEID (punto final de túnel SGW-U)
└── ULI
    ├── TAI: MCC 310, MNC 260, TAC 12345
    └── ECGI: MCC 310, MNC 260, ECI 67890
```

Respuesta de Creación de Sesión

Dirección: OmniPGW → SGW-C

Propósito: Reconocer la creación de la sesión

IEs Clave:

Nombre de IE	Tipo	Descripción
Causa	Resultado	Código de éxito o error
Contexto de Bearer	Agrupado	Información del bearer
Asignación de Dirección PDN	IP	Dirección IP asignada al UE (ver Asignación de IP del UE)
Restricción de APN	Enum	Restricciones de uso de APN
PCO	Opciones	Opciones de Configuración de Protocolo (ver Configuración de PCO)

Respuesta de Éxito:

```
Respuesta de Creación de Sesión
├── Causa: Solicitud aceptada (16)
├── Asignación de Dirección PDN
│   └── IPv4: 100.64.1.42
├── Contexto de Bearer
│   ├── EBI: 5
│   ├── Causa: Solicitud aceptada
│   └── S5/S8 F-TEID (punto final de túnel PGW-U desde PFCP)
├── Restricción de APN: Público-1 (1)
└── PCO
    ├── Servidor DNS: 8.8.8.8
    ├── Servidor DNS: 8.8.4.4
    └── MTU de Enlace: 1400
```

> La disposición de la Asignación de Dirección PDN sigue el tipo de PDN negociado (TS 29.274 §8.14): una dirección IPv4 de 4 bytes; un octeto de longitud de prefijo más un prefijo IPv6 de 16 bytes; o para IPv4v6 un octeto de longitud de prefijo más un prefijo IPv6 de 16 bytes más una IPv4 de 4 bytes. Si se solicita un PDN IPv4v6 para un APN de emergencia (SOS) que no tiene un grupo IPv6, el PGW-C degrada a un PAA solo IPv4 (los APNs regulares son rechazados) — consulte Solicitud IPv4v6 cuando el APN no tiene grupo IPv6.

Solicitud de Eliminación de Sesión

Dirección: SGW-C → OmniPGW

Propósito: Terminar la conexión PDN

IEs Clave:

Nombre de IE	Descripción
EBI	ID de Bearer EPS a eliminar
EBI Vinculado	Bearer relacionado (opcional)

Respuesta de Eliminación de Sesión

Dirección: OmniPGW → SGW-C

Propósito: Reconocer la eliminación de la sesión

IEs Clave:

Nombre de IE	Descripción
Causa	Código de éxito o error

Gestión de Bearer

Solicitud de Creación de Bearer

Dirección: OmniPGW → SGW-C

Propósito: Crear un bearer dedicado (iniciado por la política del PCRF)

Activado por:

- PCRF envía una nueva regla PCC que requiere un bearer dedicado
- OmniPGW solicita a SGW-C establecer el bearer

Solicitud de Eliminación de Bearer

Dirección: OmniPGW → SGW-C o SGW-C → OmniPGW

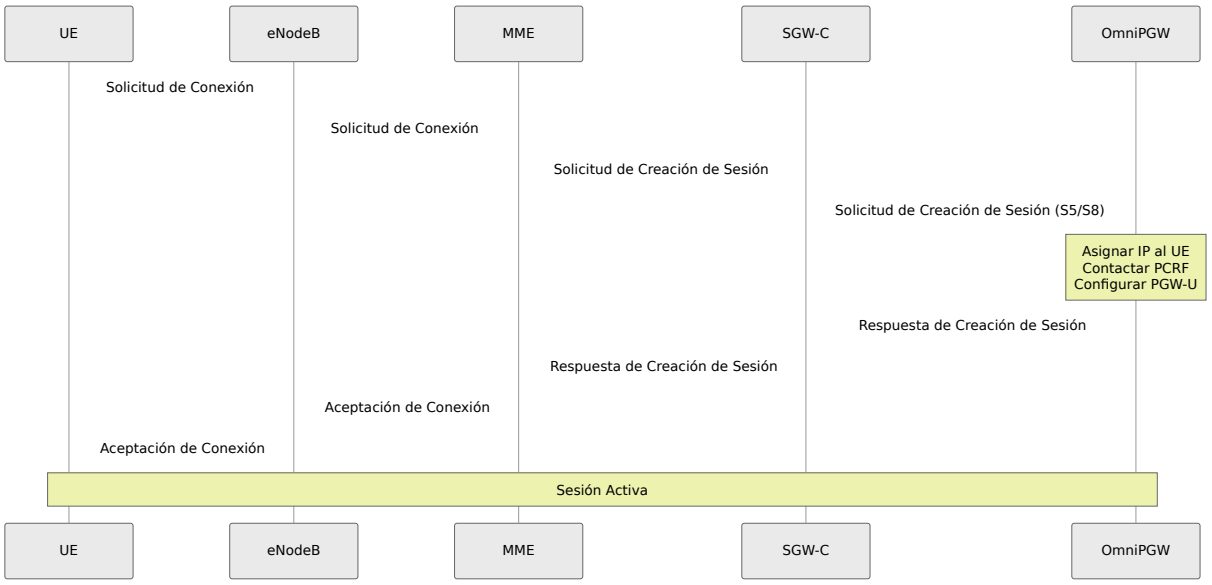
Propósito: Eliminar el bearer dedicado

Escenarios:

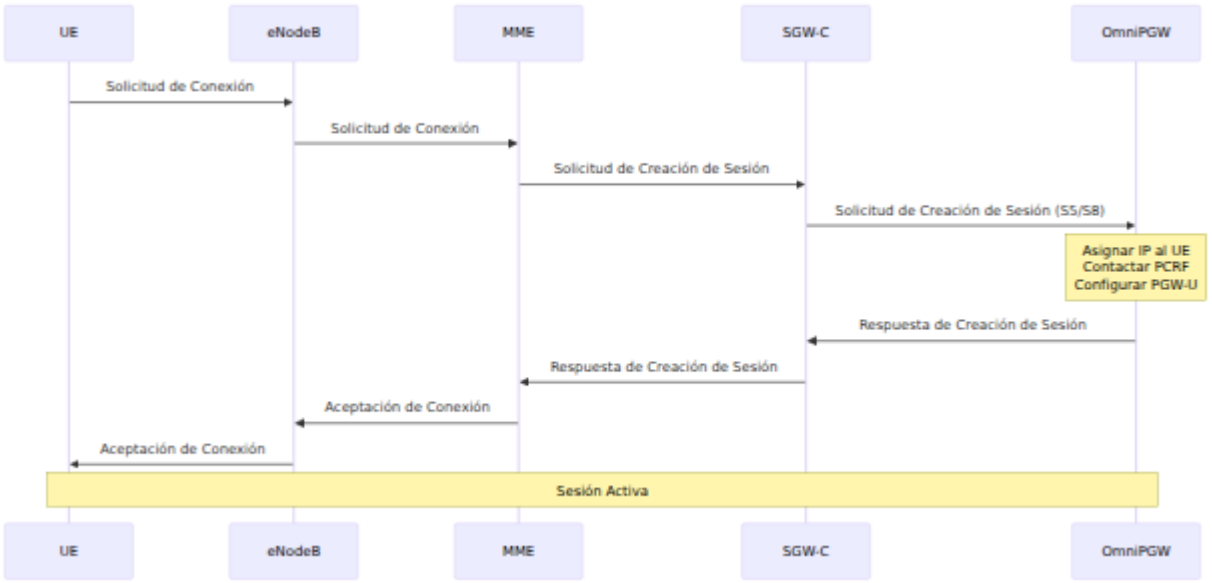
- **Iniciado por PGW:** Cambio de política del PCRF elimina el bearer dedicado
- **Iniciado por SGW:** Liberación de recursos de radio

Flujos de Mensajes

Establecimiento de Sesión



Terminación de Sesión



Códigos de Causa

Éxito

Código	Nombre	Descripción
16	Solicitud aceptada	Operación exitosa

Errores (Fallos Permanentes)

Código	Nombre	Cuándo se Usa
65	Usuario Desconocido	PCRF rechazado (IMSI no encontrado)
66	No hay recursos disponibles	Grupo de IP agotado
93	Servicio no soportado	APN inválido
94	Error semántico en TFT	Plantilla de flujo de tráfico inválida

Errores (Fallos Transitorios)

Código	Nombre	Cuándo se Usa
72	Par de remoto no responde	Tiempo de espera del PCRF/PGW-U
73	Colisión con solicitud iniciada por la red	Operaciones simultáneas

---

Monitoreo

Métricas S5/S8

```
# Contadores de mensajes
s5s8_inbound_messages_total{message_type="create_session_request"}
s5s8_inbound_messages_total{message_type="delete_session_request"}

# Contadores de errores
s5s8_inbound_errors_total

# Latencia de manejo de mensajes
s5s8_inbound_handling_duration_bucket

# TEIDs activos
teid_registry_count
```

Consultas Útiles

Tasa de Creación de Sesiones:

```
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m])
```

Tasa de Errores:

```
rate(s5s8_inbound_errors_total[5m])
```

Latencia (p95):

```
histogram_quantile(0.95,

rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m])
)
```

Solución de Problemas

Problema: Sin Respuesta de OmniPGW

Síntomas:

- SGW-C envía Solicitud de Creación de Sesión
- No se recibe respuesta
- Tiempo de espera en SGW-C

Causas:

1. Problema de conectividad de red
2. OmniPGW no está escuchando en la IP configurada
3. Firewall bloqueando UDP 2123
4. TEID incorrecto en la solicitud

Depuración:

```
# Verificar que OmniPGW está escuchando
netstat -ulnp | grep 2123

# Verificar paquetes entrantes
tcpdump -i any -n port 2123

# Verificar configuración
grep "local_ipv4_address" config/runtime.exs

# Verificar firewall
iptables -L -n | grep 2123
```

Problema: Fallo en la Creación de Sesión

Síntomas:

- Respuesta de Creación de Sesión con causa de error
- Sesión no establecida

Causas Comunes:

```
Causa 65 (Usuario Desconocido):
  → PCRF rechazó al suscriptor
  → Verificar IMSI en HSS/SPR

Causa 66 (No hay recursos):
  → Grupo de IP agotado
  → Verificar: curl http://pgw:9090/metrics | grep
address_registry_count
  → Expandir grupo de IP

Causa 72 (Par remoto no responde):
  → Tiempo de espera del PCRF o PGW-U caído
  → Verificar conectividad Gx
  → Verificar asociación PFCP
```

Problema: Colisión de TEID

Síntomas:

- Mensaje enrutado a la sesión incorrecta
- Comportamiento inesperado

Causa:

- TEID reutilizado antes de la limpieza
- Error en la asignación de TEID

Resolución:

- Asegurar asignación única de TEID
- Verificar registro de TEID en busca de fugas

Mejores Prácticas

Diseño de Red

1. **Interfaz de Red Dedicada**
    - Usar VLAN separada para S5/S8
    - Aislar del tráfico de gestión
2. **Optimización de MTU**
    - Asegurar que el MTU soporte encabezados GTP
    - MTU mínima: 1500 bytes (1464 carga útil + 36 GTP)
3. **Redundancia**
    - Múltiples instancias de OmniPGW
    - Balanceo de carga basado en DNS desde SGW-C

Rendimiento

1. **Tamaños de Buffer UDP**
    - Aumentar buffers de socket para alta carga
    - Típico: 4-8 MB por socket
2. **Límites de Conexión**
    - Planificar para el número esperado de sesiones
    - Monitorear el conteo del registro de TEID

Seguridad

1. **Filtrado de IP**
    - Permitir solo GTP-C desde IPs conocidas de SGW-C
    - Usar iptables o ACLs de red

2. **Validación de Mensajes**
    - OmniPGW valida todos los mensajes entrantes
    - Rechaza paquetes GTP-C mal formados

Documentación Relacionada

Funciones Básicas

- **Guía de Configuración** - Configuración de la interfaz S5/S8, configuración de IP local
- **Gestión de Sesiones** - Ciclo de vida de la sesión PDN, establecimiento de bearer
- **Asignación de IP del UE** - Entrega de dirección IP a través de la Respuesta de Creación de Sesión
- **Configuración de PCO** - Parámetros de PCO en mensajes GTP-C

Interfaces Relacionadas

- **Interfaz Gn/Gp** - GTP-C v1 para funcionalidad GGSN 2G/3G
- **Interfaz PFCP** - Coordinación del plano de usuario con el plano de control S5/S8
- **Interfaz Diameter Gx** - Integración de políticas con el establecimiento de bearer
- **Interfaz Diameter Gy** - Integración de carga con la gestión de bearer

Operaciones

- **Guía de Monitoreo** - Métricas GTP-C S5/S8, seguimiento de mensajes
- **Formato de CDR de Datos** - Generación de CDR a partir de sesiones GTP-C

Volver a la Guía de Operaciones

Interfaz S5/S8 de OmniPGW - *por Omnitouch Network Services*

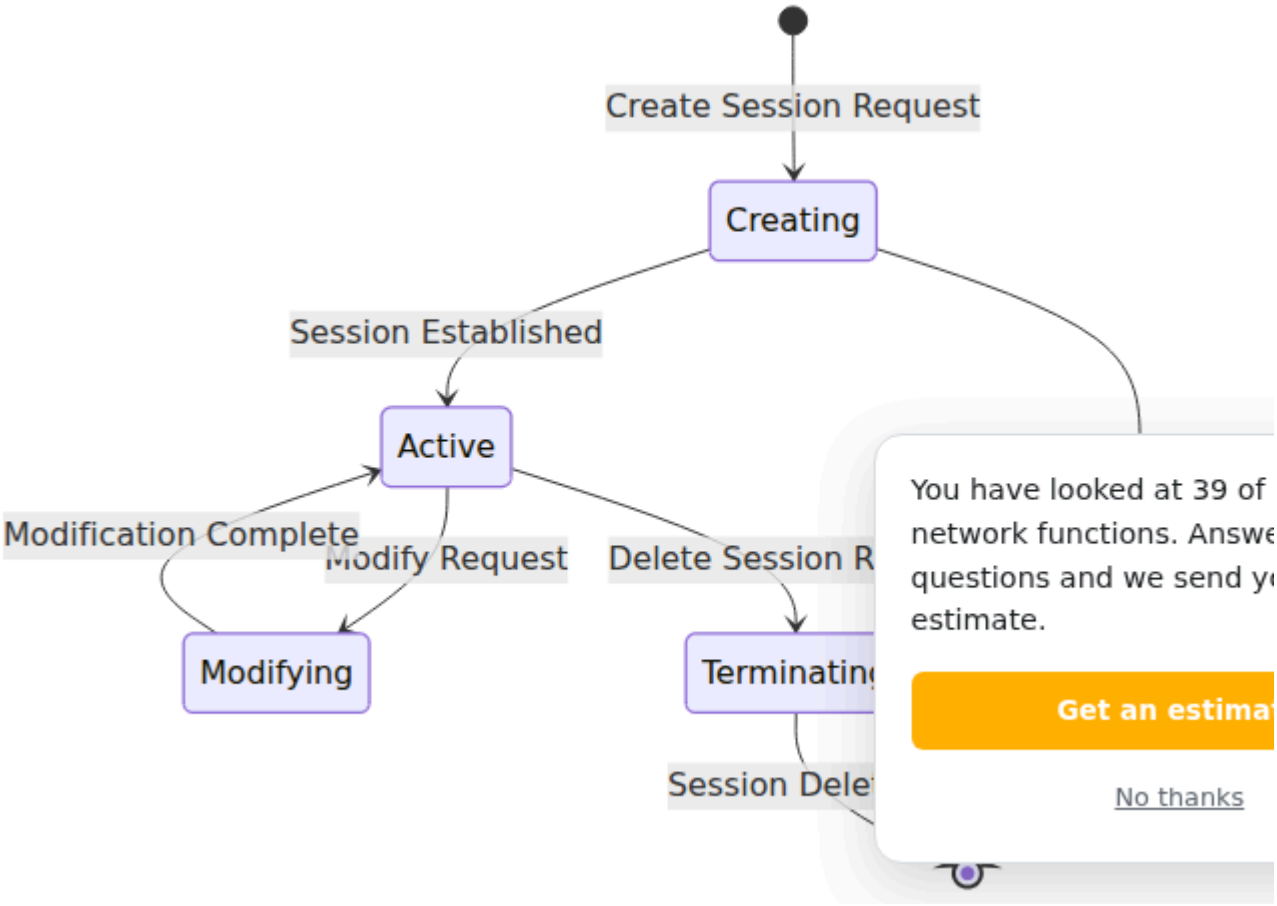
Guía de Gestión de Sesiones

Ciclo de Vida y Operaciones de Conexión PDN

OmniPGW de Omnitouch Network Services

Visión General

Una **Sesión PDN (Packet Data Network)** representa la conexión de datos de un UE a través de OmniPGW. Cada sesión coordina múltiples interfaces y recursos para habilitar la conectividad de datos.



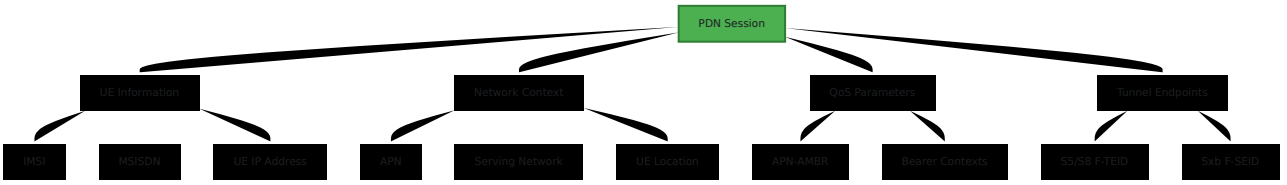
Componentes de la Sesión

Identificadores de Sesión

Cada sesión tiene múltiples identificadores para diferentes interfaces:

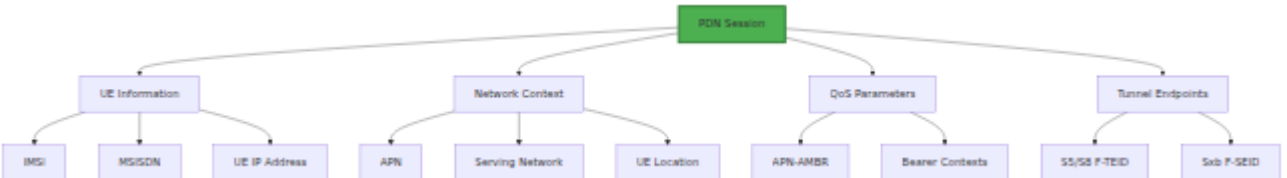
Identificador	Interfaz	Propósito
TEID	S5/S8 (GTP-C)	ID de Punto de Túnel para comunicación SGW-C
SEID	Sxb (PFCP)	ID de Punto de Sesión para comunicación PGW-U
Session-ID	Gx (Diameter)	Sesión Diameter para comunicación PCRF
Charging-ID	Contabilidad	ID único para facturación/cobro

Datos de la Sesión



Creación de Sesiones

Flujo de Llamadas



Pasos

1. Recibir Solicitud de Creación de Sesión (S5/S8)

La creación de la sesión se inicia a través de señalización GTP-C en la interfaz S5/S8. Consulte Interfaz S5/S8 para obtener detalles completos del protocolo GTP-C y formatos de mensajes.

Entrada:

- IMSI, MSISDN, IMEI
- APN (por ejemplo, "internet")
- Tipo de RAT (EUTRAN)
- Ubicación UE (TAI, ECGI)
- Contexto de Portadora (QoS, F-TEID)

2. Asignación de Recursos

```
- Asignar IP UE del grupo de APN
- Generar ID de Cobro
- Generar ID de Sesión Gx
- Asignar TEID S5/S8
- Seleccionar par PGW-U
```

3. Solicitud de Política (Gx)

Solicitar política al PCRF:

- Enviar CCR-Initial
- Recibir CCA-Initial con QoS y reglas PCC

4. Configuración del Plano de Usuario (PFCP)

Programar PGW-U con reglas de reenvío:

- Enviar Solicitud de Establecimiento de Sesión
- Incluir PDRs, FARs, QERs, BAR
- Recibir F-TEID para túnel S5/S8

5. Respuesta a SGW-C

Enviar Respuesta de Creación de Sesión:

- Dirección IP UE
- F-TEID S5/S8 (de PGW-U)
- PCO (DNS, P-CSCF, MTU)
- Contexto de Portadora

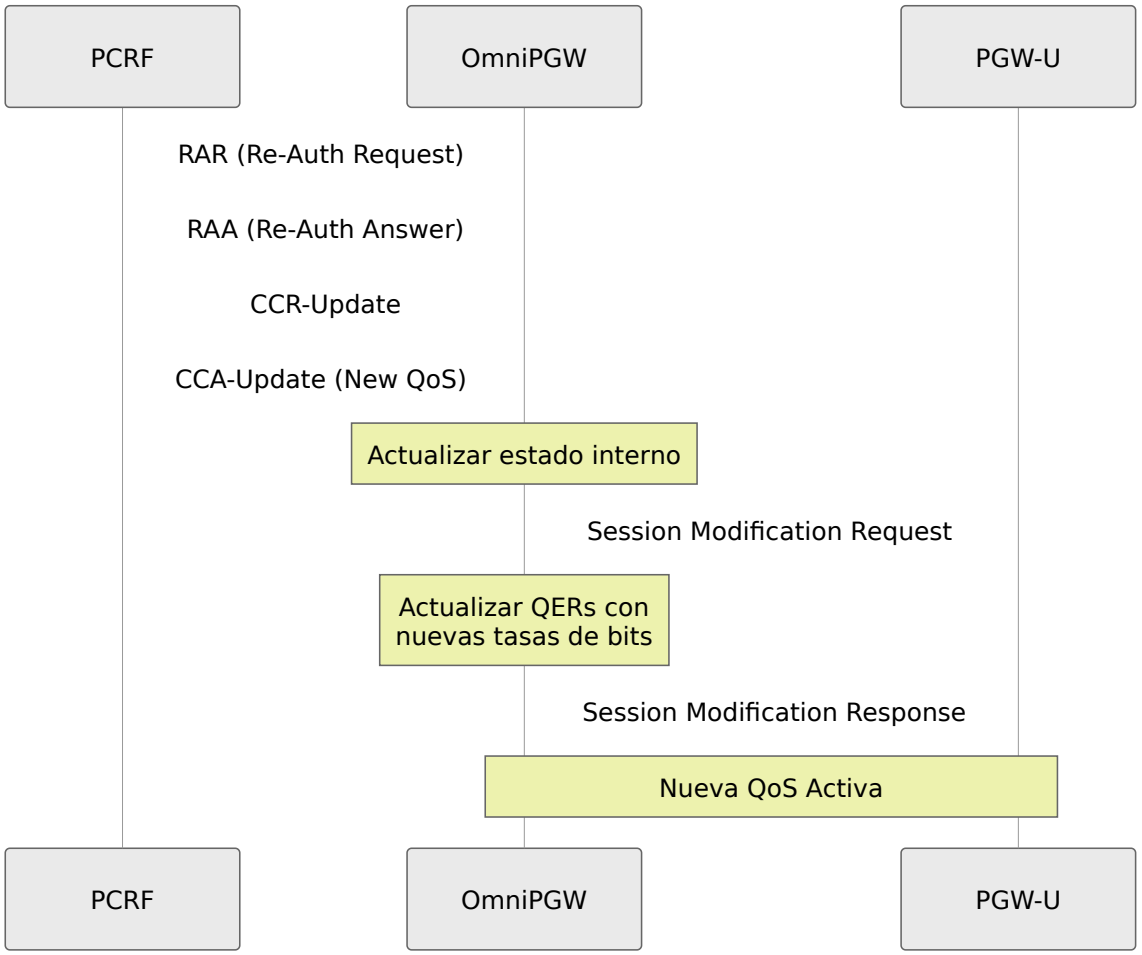
Modificación de Sesiones

Disparadores

Las sesiones pueden ser modificadas debido a:

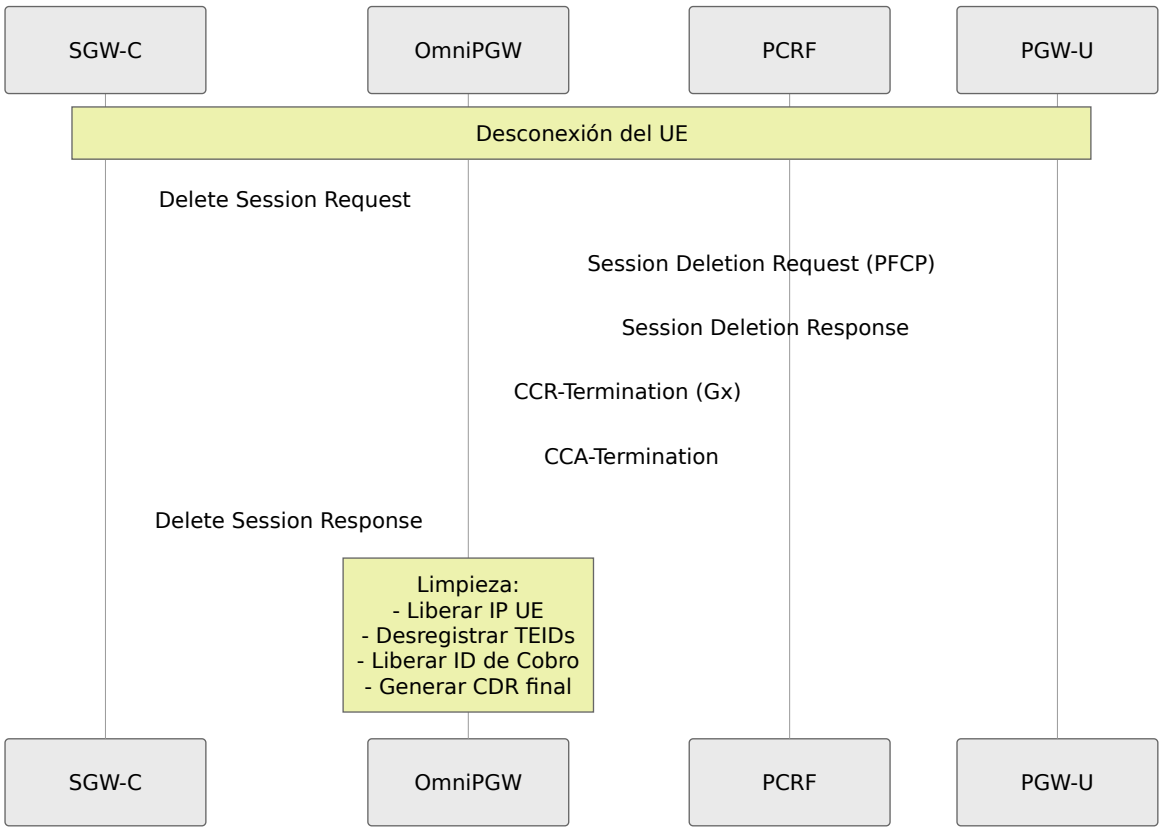
- **Cambios de QoS** - Actualizaciones de PCRF sobre tasas de bits
- **Operaciones de Portadora** - Agregar/eliminar portadoras dedicadas
- **Transferencia** - Cambio de SGW
- **Actualizaciones de Política** - Nuevas reglas PCC del PCRF

Flujo de Modificación de QoS



Eliminación de Sesiones

Flujo de Llamadas



Proceso de Limpieza

Recursos Liberados:

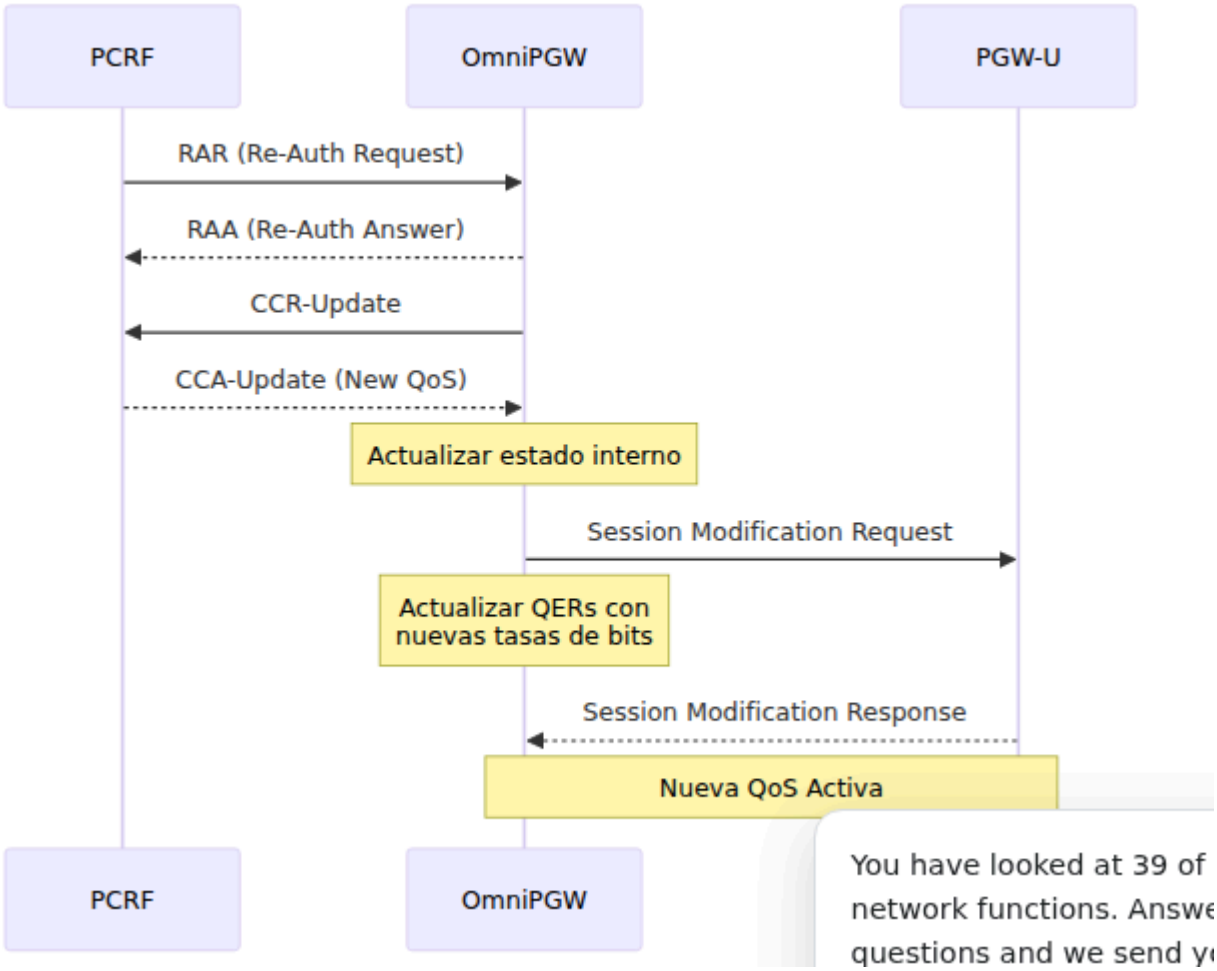
1. Dirección IP UE → de vuelta al grupo
2. TEID → eliminado del registro
3. SEID → eliminado del registro
4. Session-ID → eliminado del registro
5. Charging-ID → liberado
6. Proceso de sesión terminado

Registros de Facturación Generados:

- CDR final (Registro de Datos de Cobro) escrito para facturación offline - Consulte Formato de CDR de Datos

Estado de la Sesión

Máquina de Estados



Seguimiento de Sesiones

Búsquedas en el Registro:

```
Por TEID (S5/S8):
  TEID 0x12345678 → PID de Sesión

Por SEID (Sxb):
  SEID 0xABCDEF → PID de Sesión

Por Session-ID (Gx):
  "pgw.example.com;123;456" → PID de Sesión

Por IP UE:
  100.64.1.42 → PID de Sesión

Por IMSI + EBI:
  "310260123456789" + EBI 5 → PID de Sesión
```

Monitoreo de Sesiones

Conteo de Sesiones Activas

```
# Total de sesiones activas
teid_registry_count

# Sesiones PFCP
seid_registry_count

# Sesiones Gx
session_id_registry_count
```

Métricas de Sesiones

```
# Tasa de creación de sesiones
rate(s5s8_inbound_messages_total{message_type="create_session_request

# Tasa de eliminación de sesiones
rate(s5s8_inbound_messages_total{message_type="delete_session_request

# Latencia de creación de sesiones (p95)
histogram_quantile(0.95,

rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m])
)
```

Problemas Comunes

Fallas en la Creación de Sesiones

Causas:

1. **Grupo de IP Agotado** - No hay IPs disponibles
2. **PCRF Inalcanzable** - Tiempo de espera Gx
3. **PGW-U Caído** - No hay par PFCP disponible
4. **Rechazo del PCRF** - Usuario desconocido, no autorizado

Depuración:

```
# Verificar grupo de IP
curl http://pgw:9090/metrics | grep address_registry_count

# Verificar conectividad PCRF
# Comprobar errores Gx en los registros

# Verificar asociación PGW-U
# Verificar estado del par PFCP
```

Sesión Atascada/Obsoleta

Síntomas:

- Sesión no eliminada correctamente
- Recursos no liberados
- Registros muestran un conteo más alto de lo esperado

Causas:

1. Solicitud de Eliminación de Sesión no recibida
2. Proceso de sesión falló sin limpieza
3. Fuga en el registro

Resolución:

```
# Reiniciar OmniPGW (libera todas las sesiones)
# Implementar mecanismo de tiempo de espera para sesiones
obsoletas
```

UE No Puede Establecer Sesión

Síntomas:

- Fallo en la conexión del UE
- Respuesta de Creación de Sesión con causa de error

Causas y Respuestas Comunes:

Valor de Causa	Significado	Acción
Usuario Desconocido	PCRF rechazó (IMSI no en la base de datos)	Provisionar suscriptor
No Hay Recursos Disponibles	Grupo de IP agotado	Ampliar grupo de IP
Par Remoto No Responde	Tiempo de espera PCRF/PGW-U	Verificar conectividad
Servicio No Soportado	APN inválido	Configurar grupo de APN

Mejores Prácticas

Límites de Sesión

Configurar capacidad apropiada:

```
Usuarios concurrentes esperados: 10,000
Sobrecarga de sesión por usuario: ~10KB RAM
RAM total para sesiones: ~100MB

Configuraciones de Erlang VM:
  - Máx. procesos: 262,144 (predeterminado)
  - Tamaño de heap de procesos: Ajustar según carga
```

Limpieza de Sesiones

Asegurar limpieza adecuada:

1. Siempre responder a Solicitudes de Eliminación de Sesiones
2. Implementar tiempo de espera para sesiones obsoletas

3. Monitorear conteos de registro para fugas

Alta Disponibilidad

Redundancia de Sesiones:

- Usar diseño sin estado (sesiones vinculadas a la instancia)
- Implementar base de datos de sesiones para HA (futuro)
- DNS/balancer de carga para conmutación por error

Elementos de Datos de Sesión

¿Qué Información Almacena una Sesión?

Cada sesión PDN activa mantiene la siguiente información:

Identificación del UE:

- IMSI: "310260123456789" (identidad del suscriptor)
- MSISDN: "14155551234" (número de teléfono)
- MEI/IMEI: Identificador del dispositivo

Detalles de Conexión PDN:

- APN: "internet" (nombre de la red)
- Dirección IP UE: 100.64.1.42 (IP asignada)
- Tipo de PDN: IPv4, IPv6 o IPv4v6

Identificadores de Sesión:

- ID de Cobro: Identificador único de facturación
- EBI de Portadora Predeterminada: Identificador de Portadora EPS (típicamente 5)

Parámetros de QoS:

- APN-AMBR: Tasa Máxima de Bits Agregada
  - Subida: 100 Mbps
  - Bajada: 50 Mbps

Reglas de Reenvío:

- PDRs (Reglas de Detección de Paquetes): Coincidir paquetes
- FARs (Reglas de Acción de Reenvío): Acciones de reenvío/caída
- QERs (Reglas de Ejecución de QoS): Limitación de tasa
- BAR (Regla de Acción de Buffering): Buffering de bajada

Contexto de Interfaz:

- Estado S5/S8: TEIDs locales/remotos, dirección SGW-C
- Estado Sxb: SEIDs locales/remotos, dirección PGW-U
- Estado Gx: ID de Sesión Diameter, contador de solicitudes

Monitoreo de Sesiones en Vivo

OmniPGW expone una **API REST OAM** en tiempo real para inspeccionar y gestionar sesiones activas sin necesidad de consultar métricas o registros. La API se sirve a través de HTTPS/TLS en el puerto `8443` con todas las rutas bajo el prefijo `/api`:

```
GET    /api/sessions                 # todas las sesiones activas
GET    /api/sessions?search=<imsi>   # filtrar por IMSI / MSISDN /
IP
GET    /api/sessions/<imsi>          # detalle completo de una
sesión
PUT    /api/sessions/<imsi>          # actualizar estado de sesión
en vivo (acción del operador)
DELETE /api/sessions/<imsi>          # eliminar una sesión (acción
del operador)
```

Documentación interactiva de la API (Swagger UI) está disponible en `https://<omnipgw-ip>:8443/api/docs`.

```
# Listar todas las sesiones activas
curl -k https://<omnipgw-ip>:8443/api/sessions

# Filtrar por IMSI, MSISDN o dirección IP
curl -k "https://<omnipgw-ip>:8443/api/sessions?
search=310170123456789"
```

Búsqueda de UE y Análisis Profundo

Puntos finales:

```
GET /api/sessions?search=<imsi|msisdn|ip>   # encontrar sesiones
de un suscriptor
GET /api/sessions/<imsi>                    # detalle completo de
una sesión
```

El parámetro `search` acepta cualquiera de:

- **IMSI** (por ejemplo, "310170123456789")
- **MSISDN** (número de teléfono)
- **Dirección IP** (por ejemplo, "100.64.1.42")

```
# Análisis profundo de la sesión de un suscriptor
curl -k https://<omnipgw-ip>:8443/api/sessions/310170123456789
```

El detalle de la sesión devuelve información completa:

a) Sesiones Activas

- Todas las sesiones activas para este suscriptor
- IMSI, MSISDN, Dirección IP UE
- APN, Tipo de RAT
- TEID PGW, TEID SGW

b) Ubicación Actual Datos de ubicación en tiempo real de la sesión:

- **TAC** (Código de Área de Seguimiento) - Área de seguimiento donde se encuentra el UE
- **ID de Celda (ECI)** - Identificador de Celda E-UTRAN
- **ECGI** - Identificador Global de Celda E-UTRAN (PLMN + ECI)
- **MCC/MNC** - Código de País Móvil / Código de Red Móvil

c) Información de Portadora Listado detallado de portadoras con parámetros de QoS:

Portadora Predeterminada:

- EBI (Identificador de Portadora EPS)
- QCI (Identificador de Clase de QoS)
- Nombre de Regla de Cobro
- APN-AMBR (subida/bajada)

Portadoras Dedicadas (si están activas):

- EBI, QCI, Nombre de Regla de Cobro
- MBR UL/DL (Tasa Máxima de Bits)
- GBR UL/DL (Tasa Garantizada de Bits)

d) Información de Cobro (Interfaz Gy)

- ID de Sesión Gy
- Cuota Concedida, Cuota Usada
- Características de Cobro

e) Información de Política (Interfaz Gx)

- ID de Sesión Gx
- Host de Origen/Destino del PCRF
- Número de Solicitud CC
- Reglas de Cobro Instaladas (reglas PCC de portadoras)

f) Eventos Recientes

- Historial de eventos para este suscriptor (ver Historial de Sesiones y Registro de Auditoría)
- Eventos de creación/actualización/eliminación de sesiones

Casos de Uso:

- Solucionar problemas específicos de suscriptores
- Verificar el establecimiento de sesiones
- Comprobar la dirección IP asignada
- Inspeccionar parámetros de sesión

Todas las Sesiones Activas

Puntos finales:

```
GET    /api/sessions                 # listar todas las sesiones
PDN activas
GET    /api/sessions?search=<term>   # filtrar la lista
PUT    /api/sessions/<imsi>          # actualizar el estado de una
sesión en vivo
DELETE /api/sessions/<imsi>          # eliminar una sesión
```

Propósito: Enumerar todas las sesiones PDN activas. Consultar `GET /api/sessions` en su intervalo preferido para una vista en vivo de la tabla de sesiones.

```
# Instantánea de todas las sesiones activas
curl -k https://<omnipgw-ip>:8443/api/sessions

# Filtrar por prefijo IMSI, IP UE, MSISDN o APN
curl -k "https://<omnipgw-ip>:8443/api/sessions?search=100.64"

# Acciones del operador en una sesión específica
curl -k -X PUT    https://<omnipgw-
ip>:8443/api/sessions/310170123456789   # actualizar estado
curl -k -X DELETE https://<omnipgw-
ip>:8443/api/sessions/310170123456789   # eliminar
```

Información Rápida de la Sesión (devuelta por sesión):

- **IMSI** - Identidad del suscriptor
- **UE IP** - Dirección IP asignada
- **SGW TEID** - ID de túnel S5/S8 del SGW
- **PGW TEID** - ID de túnel S5/S8 de OmniPGW
- **APN** - Nombre del Punto de Acceso

Filtrado (a través de `?search=`):

- IMSI (por ejemplo, "310260")
- Dirección IP UE (por ejemplo, "100.64")
- MSISDN / número de teléfono
- Nombre de APN

Detalles Completos (`GET /api/sessions/<imsi>`):

- Información completa del suscriptor (IMSI, MSISDN, IMEI)
- Contexto de red (tipo de RAT, red de servicio MCC/MNC)
- Parámetros de QoS (AMBR subida/bajada)
- Identificadores de túnel (ambos TEIDs en formato hexadecimal)
- ID de proceso para depuración
- Estado completo de la sesión (estructura de datos en bruto)

Puntos Finales de Salud Referenciados Cruzadamente

La API OAM también expone la salud de pares/topología de la que depende la vista de sesión:

```
GET /api/upf         # estado y asociaciones de pares PFCP / UPF
GET /api/diameter    # conectividad de pares Diameter (Gx/Gy)
```

```
# Verificar conectividad de plano de usuario y pares Diameter
curl -k https://<omnipgw-ip>:8443/api/upf
curl -k https://<omnipgw-ip>:8443/api/diameter
```

Casos de Uso:

- Verificar conexiones de pares (asociaciones UPF, conectividad PCRF/OCS)
- Correlacionar fallas en el establecimiento de sesiones con la salud de pares
- Verificación rápida de la salud de la red

Historial de Sesiones y Registro de Auditoría

Punto Final:

```
GET /api/session_history[?type=&search=&page=&page_size=]
```

Propósito: Rastrear eventos históricos de sesiones y registro de auditoría.

Parámetros:

- `type` - filtrar por tipo de evento (por ejemplo, sesión creada, sesión eliminada)
- `search` - filtrar por IMSI, MSISDN, dirección IP o TEID
- `page`, `page_size` - paginar a través de resultados

```
# Eventos recientes de eliminación para un suscriptor, primera
página
curl -k "https://<omnipgw-ip>:8443/api/session_history?
type=session_deleted&search=310170123456789&page=1&page_size=50"
```

Tipos de Eventos Rastreados:

- Eventos de creación de sesiones
- Eventos de eliminación de sesiones
- Eventos de modificación
- Eventos de error

Casos de Uso:

- Registro de auditoría para cumplimiento (paginación y archivo de resultados)
- Análisis histórico de sesiones
- Solucionar problemas de eventos pasados
- Generar informes de uso
- Rastrear patrones de sesión a lo largo del tiempo

Casos de Uso Operacionales

Verificación de Sesiones:

```
1. El usuario informa un problema de conectividad
2. GET /api/sessions?search=<imsi|msisdn> para localizar al
suscriptor
3. GET /api/sessions/<imsi> para verificar que la sesión existe y
que el UE tiene una dirección IP
4. Comprobar que los valores de QoS coinciden con el plan del
suscriptor
5. Verificar que los puntos finales de túnel están establecidos
```

Monitoreo de Capacidad:

- Consultar `GET /api/sessions` (o la métrica `teid_registry_count`) para el conteo de sesiones activas
- Comparar contra la capacidad licenciada
- Identificar patrones de uso por APN (a través de `?search=<apn>`)

Solución de Problemas:

- Encontrar una sesión específica por cualquier identificador a través de `?search=`
- Inspeccionar el estado completo de la sesión (`GET /api/sessions/<imsi>`) sin SSH/IEx
- Verificar que los TEIDs de SGW y PGW coincidan entre sistemas
- Comprobar los valores de AMBR aplicados desde el PCRF

- Eliminar una sesión atascada con `DELETE /api/sessions/<imsi>`

Ventajas sobre Métricas:

- Ver detalles individuales de la sesión (las métricas muestran agregados)
- Capacidades de búsqueda y filtrado a través de `?search=`
- Inspección del estado en tiempo real
- Scriptable/automatizable (JSON sobre HTTPS) para integración con herramientas

---

Documentación Relacionada

Funciones Básicas de Sesión

- **Interfaz PFCP** - Establecimiento de sesión de plano de usuario, PDRs, FARs, QERs, URRs
- **Asignación de IP de UE** - Asignación de dirección IP, gestión de grupo de APN
- **Configuración de PCO** - Parámetros de DNS, P-CSCF, MTU entregados al UE
- **Guía de Configuración** - Selección de UPF, flujos de establecimiento de sesión

Política y Cobro

- **Interfaz Diameter Gx** - Control de política PCRF, reglas PCC, gestión de QoS
- **Interfaz Diameter Gy** - Cobro en línea OCS, seguimiento de cuotas
- **Formato de CDR de Datos** - Generación de registros de cobro offline

Interfaces de Red

- **Interfaz S5/S8** - Protocolo GTP-C, comunicación SGW-C
- **Gestión de QoS y Portadoras** - Ejecución de QoS de portadoras

Operaciones

- **Guía de Monitoreo** - Métricas de sesión, seguimiento de sesiones activas, alertas
- **Monitoreo de P-CSCF** - Monitoreo de sesión IMS

Volver a la Guía de Operaciones

Guía de Solución de Problemas de OmniPGW

Procedimientos de Solución de Problemas y Problemas Comunes

por Omnitouch Network Services

Tabla de Contenidos

1. Descripción General
2. Herramientas de Solución de Problemas
3. Problemas de Establecimiento de Sesiones
4. Problemas de PFCP / Plano de Usuario
5. Problemas de Diámetro (Gx/Gy)
6. Problemas de Asignación de IP
7. Referencia Rápida

Descripción General

Esta guía proporciona procedimientos de solución de problemas paso a paso para problemas operativos comunes de OmniPGW. Cada problema incluye:

- **Síntoma**: Lo que observarás
- **Causas Probables**: Causas comunes raíz
- **Diagnóstico**: Cómo confirmar la causa
- **Resolución**: Solución paso a paso
- **Prevención**: Cómo evitar la recurrencia

Documentación Relacionada

- **Guía de Monitoreo** - Métricas de Prometheus, alertas, monitoreo de rendimiento
- **Guía de Configuración** - Referencia de configuración del sistema

---

Herramientas de Solución de Problemas

API OAM

URL Base: `https://<omnipgw_ip>:8443` (HTTPS/TLS; todas las rutas bajo el prefijo `/api`)

Documentación API Interactiva (Swagger UI):
`https://<omnipgw_ip>:8443/api/docs`

Puntos Finales Clave:

- `GET /api/sessions[?search=<imsi|msisdn|ip>]`, `GET /api/sessions/<imsi>` - Visor de sesiones activas (buscar por IMSI, IP, MSISDN)
- `GET /api/diameter[?status=connected|disconnected]`, `GET /api/diameter/<origin-host>` - Estado del par de Diámetro (Gx PCRF, Gy OCS)
- `GET /api/charging[?search=<imsi>]`, `GET /api/charging/<imsi>` - Estado de carga en línea (Gy)
- `GET /api/upf`, `GET /api/upf/<ip>` - Estado del par UPF / PFCP (conectividad PGW-U)
- `GET /api/ip_pools`, `GET /api/ip_pools/<name>` - Utilización del pool de IP
- `GET /api/session_history[?type=&search=&page=&page_size=]` - Historial de sesiones
- `GET /api/status` - Verificación de salud (`{"result":"ok"}`)

Ejemplo:

```
curl -k https://<omnipgw_ip>:8443/api/sessions
```

La transmisión de registros ya no es proporcionada por la plataforma; utiliza registros de host (`journalctl`/archivos de registro) con los filtros a continuación.

Métricas de Prometheus

Acceso: `http://<omnipgw_ip>:9090/metrics`

Métricas Clave:

- `teid_registry_count` - Sesiones activas
- `address_registry_count` - IPs de UE asignadas
- `sxb_inbound_errors_total` - Errores de PFCP
- `gx_inbound_errors_total` - Errores de Diámetro Gx
- `gy_inbound_errors_total` - Errores de Diámetro Gy

Consulta la Guía de Monitoreo para la referencia completa de métricas.

Análisis de Registros

Registros: Inspecciona los registros del host (`journalctl -u omnipgw_c` o el archivo de registro configurado) y grep para las cadenas a continuación. Para una vista estructurada y consultable de los eventos del ciclo de vida de la sesión, utiliza `GET /api/session_history[?type=&search=&page=&page_size=]`.

Filtros Comunes de Registros:

- "create_session_request" - Establecimiento de sesión
- "Credit Control" - Interacciones Gx/Gy
- "PFCP Session" - Programación del plano de usuario
- "error" o "ERROR" - Mensajes de error
- "timeout" - Problemas de tiempo de espera

Problemas de Establecimiento de Sesiones

Problema: Solicitud de Crear Sesión Rechazada con "No Hay Recursos Disponibles"

Síntoma:

- SGW-C recibe Respuesta de Crear Sesión con causa "No hay recursos disponibles" (73)
- Todos los intentos de nueva sesión fallan
- Las sesiones existentes continúan funcionando
- Registros: `[PGW-C] Solicitud de Crear Sesión bloqueada - licencia inválida`

Captura de Wireshark mostrando Respuesta de Crear Sesión con causa "No hay recursos disponibles"

Causa Probable:

- Licencia de OmniPGW inválida o expirada
- Servidor de licencias inalcanzable

Diagnóstico:

1. **Verifica la métrica de licencia:**

   ```
   license_status
   ```

   - Un valor de 0 indica licencia inválida

2. **Verifica los registros para advertencias de licencia:**

   - Busca "license" o "License"
   - Busca mensajes de "No se puede contactar al servidor de licencias"

3. **Verifica la conectividad del servidor de licencias:**

   - Verifica la URL configurada en `config/runtime.exs` bajo `:license_client`
   - Predeterminado: `https://localhost:10443/api`

Resolución:

1. **Verifica que el servidor de licencias sea alcanzable:**

   ```
   curl -k https://<license_server_ip>:10443/api/status
   ```

2. **Verifica la configuración de la licencia en `config/runtime.exs`:**

   ```
   config :license_client,
     license_server_api_urls:
   ["https://<license_server_ip>:10443/api"],
     licensee: "Tu Nombre de Empresa"
   ```

3. **Verifica que el producto esté licenciado:**

   - Nombre del producto: `omnipgwc`
   - Contacta a Omnitouch para verificar el estado de la licencia

4. **Reinicia OmniPGW después de los cambios de configuración**

Prevención:

- Monitorea la métrica `license_status` con alertas críticas
- Asegura alta disponibilidad del servidor de licencias
- Configura alertas de expiración de licencia antes de la expiración

---

Problema: Solicitud de Crear Sesión Rechazada (Otras Causas)

Síntoma:

- SGW-C recibe Respuesta de Crear Sesión con causa de error
- Los usuarios no pueden establecer conexiones PDN
- Métrica: `s5s8_inbound_errors_total` en aumento

Causas Probables:

1. Pool de IP agotado
2. PCRF (Gx) inalcanzable o rechazando políticas
3. PGW-U (PFCP) no disponible
4. Configuración de APN inválida

Diagnóstico:

1. **Verifica la utilización del pool de IP:**

   ```
   address_registry_count
   ```

   - Si es igual al tamaño del pool configurado, el pool está agotado

2. **Verifica la conectividad del PCRF:**

   - Consulta `GET /api/diameter` (o `GET /api/diameter?status=disconnected`)
   - Busca el estado del par PCRF = "disconnected"
   - Registros: Busca "Credit Control Answer" para errores

3. **Verifica el estado del par PFCP:**
    - Consulta `GET /api/upf` (o `GET /api/upf/<ip>` para un PGW-U específico)
    - Busca "Association: DOWN"
    - Métrica: `pfcp_peer_associated` = 0
4. **Verifica la configuración de APN:**
    - Revisa `config/runtime.exs` bajo `ue.apn_map`
    - Verifica que el APN solicitado exista en la configuración

Resolución:

Para Agotamiento del Pool de IP:

1. Identifica sesiones obsoletas: consulta `GET /api/sessions` (opcionalmente `GET /api/sessions?search=<imsi|msisdn|ip>`), busca sesiones antiguas
2. Expande el pool de IP en `config/runtime.exs`:

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => "10.0.0.0/23"  # Cambiado de /24 a /23
(duplica la capacidad)
    }
  }
```

3. Reinicia OmniPGW
4. Verifica: `curl http://<ip>:9090/metrics | grep address_registry_count`

Para Problemas de Conectividad del PCRF:

1. Verifica la conectividad de red: `ping <pcrf_ip>`
2. Verifica el servicio de Diámetro del PCRF: `telnet <pcrf_ip> 3868`
3. Verifica la configuración del par de Diámetro en `config/runtime.exs`
4. Reinicia OmniPGW si se cambió la configuración

5. Verifica a través de `GET /api/diameter?status=connected` (el par debería mostrar "connected")

Para Problemas de PFCP:

- Consulta la sección Problemas de PFCP / Plano de Usuario

Prevención:

- Monitorea la utilización del pool de IP con alertas al 80%
- Monitorea la conectividad del PCRF con alertas del par de Diámetro
- Implementa limpieza de sesiones para sesiones inactivas

Problema: Sesiones Atascadas en Estado Intermedio

Síntoma:

- La sesión aparece en `GET /api/sessions` pero está incompleta
- Las métricas muestran un aumento en el conteo de sesiones pero sin tráfico de usuario
- La Solicitud de Eliminar Sesión falla o se agota

Causas Probables:

1. El establecimiento de la sesión PFCP falló pero se creó la sesión S5/S8
2. El CCR-Initial del PCRF se agotó
3. La Solicitud de Crear Portadora (portadora dedicada) falló
4. Interrupción de la red durante la configuración de la sesión

Diagnóstico:

1. **Busca la sesión a través de la API OAM:**
   - `GET /api/sessions/<imsi>` (o `GET /api/sessions?search=<imsi>`)
   - Verifica si `pfcp_seid` está presente (si falta, PFCP falló)
   - Verifica si `gx_session_id` está presente (si falta, Gx falló)

2. **Verifica los registros para el IMSI:**
    - Filtra los registros por IMSI
    - Busca "Solicitud de Establecimiento de Sesión" (PFCP)
    - Busca "Solicitud de Control de Crédito" (Gx)
    - Busca mensajes de tiempo de espera o error
3. **Verifica las métricas:**

```
# Sesiones con TEID pero sin sesión PFCP
teid_registry_count - seid_registry_count

# Sesiones con TEID pero sin sesión Gx
teid_registry_count - session_id_registry_count
```

Resolución:

1. **Para fallos en el establecimiento de PFCP:**
    - Verifica la salud y los registros de PGW-U
    - Verifica la asociación PFCP: `GET /api/upf`
    - Envía la Solicitud de Eliminar Sesión desde SGW-C para limpiar
2. **Para problemas de tiempo de espera de Gx:**
    - Verifica la latencia del PCRF: `histogram_quantile(0.95, rate(gx_outbound_transaction_duration_bucket[5m]))`
    - Aumenta el tiempo de espera de Gx en `config/runtime.exs` si es necesario
    - Envía la Solicitud de Eliminar Sesión para limpiar
3. **Limpieza manual (último recurso):**
    - Actualmente requiere reiniciar OmniPGW para limpiar sesiones atascadas
    - Monitorea `teid_registry_count` antes/después del reinicio para confirmar la limpieza

Prevención:

- Monitorea las métricas de latencia de PFCP y Gx
- Implementa un tiempo de espera/limpieza de sesiones para sesiones incompletas
- Alerta sobre discrepancias en el conteo de registros

Problemas de PFCP / Plano de Usuario

Problema: Asociación PFCP Caída

Síntoma:

- `GET /api/upf` muestra "Association: DOWN"
- Todos los nuevos establecimientos de sesión fallan
- Métrica: `pfcp_peer_associated` = 0
- Registros: "Tiempo de espera de latido de PFCP" o "Fallo en la Configuración de Asociación"

Causas Probables:

1. PGW-U inalcanzable (problema de red)
2. PGW-U se bloqueó o reinició
3. Desajuste de configuración de PFCP (IP, puerto)
4. Firewall bloqueando UDP 8805

Diagnóstico:

1. **Verifica la conectividad de red:**

   ```
   ping <pgw_u_ip>
   nc -u -v <pgw_u_ip> 8805
   ```

2. **Verifica la configuración de PFCP:**

- Revisa `config/runtime.exs` bajo `upf.peer_list`
- Verifica que la dirección IP y el ID del nodo coincidan con la configuración de PGW-U

3. **Verifica el estado de PGW-U:**

   - Accede a los registros de PGW-U
   - Verifica que PGW-U esté en ejecución: `systemctl status omnipgw_u` (o equivalente)

4. **Verifica las métricas:**

```
# Fallos de latido
pfcp_consecutive_heartbeat_failures

# Tasa de error de PFCP
rate(sxb_inbound_errors_total[5m])
```

Resolución:

1. **Para problemas de red:**

   - Verifica el enrutamiento: `traceroute <pgw_u_ip>`
   - Verifica las reglas del firewall: Asegúrate de que UDP 8805 esté permitido
   - Verifica grupos de seguridad (si es implementación en la nube)

2. **Para bloqueos de PGW-U:**

   - Reinicia el servicio PGW-U
   - Espera 30 segundos para la re-establecimiento de la asociación
   - Verifica a través de `GET /api/upf` (debería mostrar "Association: UP")

3. **Para problemas de configuración:**

   - Corrige la configuración del par PFCP en `config/runtime.exs`
   - Reinicia OmniPGW
   - Verifica que la asociación se haya establecido

Prevención:

- Monitorea la métrica `pfcp_peer_associated` con alertas críticas
- Monitorea `pfcp_consecutive_heartbeat_failures` (alerta en > 2)
- Implementa instancias redundantes de PGW-U
- Habilita el latido/keepalive de PFCP (debería ser el predeterminado)

Problema: Fallos en la Modificación de Sesión PFCP

Síntoma:

- La creación de portadora dedicada falla
- Las actualizaciones de políticas de QoS (desde PCRF RAR) fallan
- Registros: "Fallo en la Solicitud de Modificación de Sesión"
- Métrica: `sxb_inbound_errors_total{message_type="session_modification_response"}` en aumento

Causas Probables:

1. Reglas PFCP inválidas (referencias PDR/FAR/QER)
2. Agotamiento de recursos de PGW-U
3. Conflictos de ID de regla
4. Error de software de PGW-U

Diagnóstico:

1. **Verifica los registros:**
    - Filtra por "Modificaci��n de Sesión" y SEID
    - Busca códigos de causa de error en la respuesta PFCP
    - Causas comunes: "El ID de regla ya existe", "Fuera de recursos"
2. **Verifica los registros de PGW-U:**
    - Busca errores de procesamiento de PFCP

- Verifica la utilización de recursos (CPU, memoria)

3. **Verifica el estado de la sesión a través de la API OAM:**
   - `GET /api/sessions/<imsi>` (o `GET /api/sessions?search=<imsi>`)
   - Revisa `pdr_map`, `far_map`, `qer_map` para conflictos
   - Busca IDs duplicados

Resolución:

1. **Para conflictos de reglas:**
   - Elimina y recrea la portadora dedicada
   - Si persiste, Elimina la Sesión y haz que el UE se reconecte
2. **Para problemas de recursos de PGW-U:**
   - Verifica la capacidad de PGW-U (sesiones, PDRs, rendimiento)
   - Escala PGW-U si es necesario
   - Reduce la carga de sesiones en la instancia afectada de PGW-U
3. **Para errores de software:**
   - Captura el estado completo de la sesión (`GET /api/sessions/<imsi>`)
   - Captura los registros de mensajes PFCP
   - Informa al proveedor con pasos de reproducción

Prevención:

- Monitorea la utilización de recursos de PGW-U
- Prueba la creación de portadoras dedicadas en staging
- Monitorea `sxb_inbound_errors_total` con alertas

Problemas de Diámetro (Gx/Gy)

Problema: Par PCRF Desconectado (Gx)

Síntoma:

- `GET /api/diameter` (o `GET /api/diameter?status=disconnected`) muestra el par PCRF "desconectado"
- Sesiones creadas sin políticas de QoS (se aplica QCI=5 por defecto)
- Registros: "Fallo en la conexión del par de Diámetro" o "Tiempo de espera CER/CEA"

Causas Probables:

1. PCRF inalcanzable (problema de red)
2. Servicio PCRF caído
3. Desajuste de configuración de Diámetro (Origin-Host, Realm)
4. Firewall bloqueando TCP 3868

Diagnóstico:

1. **Verifica la conectividad de red:**

   ```
   ping <pcrf_ip>
   telnet <pcrf_ip> 3868
   ```

2. **Verifica la configuración de Diámetro:**

   - Revisa `config/runtime.exs` bajo `diameter.peer_list`
   - Verifica que `host`, `realm`, `ip` coincidan con la configuración del PCRF
   - Verifica que `origin_host` coincida con lo que espera el PCRF

3. **Verifica los registros del PCRF:**

   - Busca CER (Capabilities-Exchange-Request) desde PGW-C
   - Busca razones de rechazo

4. **Verifica las métricas:**

```
# Errores de conexión de Diámetro
diameter_peer_connected{peer="<pcrf_host>"}
```

Resolución:

1. **Para problemas de red:**
   - Verifica el enrutamiento hacia el PCRF
   - Verifica las reglas del firewall: Asegúrate de que TCP 3868 esté permitido
   - Prueba la conectividad: `nc -v <pcrf_ip> 3868`
2. **Para servicio PCRF caído:**
   - Reinicia el servicio PCRF
   - Espera la reconexión automática (intervalo de reintento de 30s)
   - Verifica a través de `GET /api/diameter?status=connected`
3. **Para desajuste de configuración:**
   - Corrige la configuración de Diámetro en `config/runtime.exs`:

```
config :pgw_c,
  diameter: %{
    host: "pgw-c.epc.mnc999.mcc999.3gppnetwork.org",  #
Debe coincidir con la configuración del PCRF
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "192.168.1.100",
        initiate_connection: true
      }
    ]
  }
```

   - Reinicia OmniPGW
   - Verifica que la conexión se haya establecido

Prevención:

- Monitorea la conectividad del par de Diámetro con alertas críticas
- Implementa instancias redundantes de PCRF (si es compatible)
- Documenta la configuración de Diámetro en el libro de operaciones

---

Problema: Tiempos de Espera CCR/CCA (Solicitudes de Políticas Gx)

Síntoma:

- Establecimiento de sesión lento (> 5 segundos)
- Registros: "Tiempo de espera de Solicitud de Control de Crédito"
- Métrica: `gx_outbound_transaction_duration` muy alta (> 5s)
- Sesiones creadas con QoS por defecto (comportamiento de respaldo)

Causas Probables:

1. PCRF sobrecargado
2. Base de datos del PCRF lenta
3. Latencia de red
4. Problema de software del PCRF

Diagnóstico:

1. **Verifica la latencia de Gx:**

```
# Latencia P95
histogram_quantile(0.95,
rate(gx_outbound_transaction_duration_bucket[5m]))

# Latencia P99 (valores atípicos)
histogram_quantile(0.99,
rate(gx_outbound_transaction_duration_bucket[5m]))
```

2. **Verifica la salud del PCRF:**

- Accede a los paneles de monitoreo del PCRF
- Verifica CPU, memoria, conexiones a la base de datos
- Revisa los registros del PCRF para consultas lentas

3. **Verifica la latencia de la red:**

```
ping -c 100 <pcrf_ip> | tail -1  # Verifica la latencia promedio
```

4. **Verifica los registros:**

- Cuenta los intercambios CCR/CCA: Filtra "Control de Crédito"
- Mide el tiempo entre "Enviando CCR" y "Recibido CCA"

Resolución:

1. **Para sobrecarga del PCRF:**

- Escala el PCRF (agrega instancias)
- Reduce el tamaño del mensaje CCR si es posible
- Ajusta los grupos de hilos/trabajadores del PCRF

2. **Para latencia de red:**

- Investiga la ruta de red (enrutadores, conmutadores)
- Considera co-localizar PGW-C y PCRF

3. **Solución temporal (aumentar tiempo de espera):**

- Edita `config/runtime.exs`:

```
config :pgw_c,
  diameter: %{
    transaction_timeout_ms: 10000  # Aumentar de 5000 por defecto
  }
```

- Reinicia OmniPGW
- **Nota:** Esto solo oculta el problema; soluciona la causa raíz

Prevención:

- Monitorea la latencia de Gx con alertas (advertencia > 1s, crítica > 5s)
- Planifica la capacidad del PCRF para la tasa de sesiones esperada
- Prueba el rendimiento del PCRF bajo carga

Problema: Par OCS Desconectado (Gy)

Síntoma:

- `GET /api/diameter` (o `GET /api/diameter?status=disconnected`) muestra el par OCS "desconectado"; `GET /api/charging` refleja el estado de carga en línea (Gy)
- Las sesiones no pueden ser cargadas (la carga en línea falla)
- Registros: "Fallo en la conexión del par Gy"

Diagnóstico y Resolución:

Similar a Par PCRF Desconectado, pero para la interfaz Gy.

Diferencias clave:

- Puerto: Típicamente TCP 3868 (igual que Gx)
- Impacto: La carga falla, las sesiones pueden ser rechazadas o permitidas sin carga (depende de la configuración)
- Configuración: Verifica `diameter.peer_list` para la entrada OCS

Ver: Interfaz Gy de Diámetro para solución de problemas específicos de Gy

---

Problemas de Asignación de IP

Problema: Pool de IP Agotado

Síntoma:

- Solicitud de Crear Sesión rechazada con causa "No hay recursos disponibles"
- Métrica: `address_registry_count` igual al tamaño del pool configurado
- `GET /api/sessions` muestra muchas sesiones activas; `GET /api/ip_pools` muestra el pool a capacidad
- Registros: "Fallo en la asignación de IP: pool agotado"

Causas Probables:

1. Pool demasiado pequeño para la base de suscriptores
2. Sesiones no liberando IPs (fallos en la Eliminación de Sesiones)
3. Rápido cambio de sesiones sin limpieza
4. Fuga de direcciones IP

Diagnóstico:

1. **Verifica la utilización del pool:**

```
# Para subred /24 (254 IPs)
(address_registry_count / 254) * 100
```

2. **Verifica el tamaño del pool configurado:**
   - Revisa `config/runtime.exs` bajo `ue.subnet_map`
   - Ejemplo: "10.0.0.0/24" = 254 IPs utilizables
3. **Compara el conteo de sesiones con el conteo de IP:**

```
# Deberían ser aproximadamente iguales
teid_registry_count
address_registry_count
```

4. **Revisa las sesiones activas:**
   - `GET /api/sessions` (y `GET /api/ip_pools/<name>` para utilización por pool)
   - Ordena por tiempo de inicio de sesión

- Busca sesiones muy antiguas (posibles fugas)

Resolución:

Inmediata (expandir pool):

1. Edita `config/runtime.exs` (cada APN mapea a una **lista** de cadenas CIDR):

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => ["10.0.0.0/22"]  # 1022 IPs (era /24 = 254 IPs)
    }
  }
```

2. Reinicia OmniPGW
3. Verifica: Las sesiones ahora pueden establecerse

A Largo Plazo (limpieza):

1. Identifica sesiones obsoletas a través de `GET /api/sessions`
2. Coordina con SGW-C para enviar Solicitudes de Eliminar Sesiones
3. Implementa política de tiempo de espera de sesiones en PCRF/SGW
4. Monitorea `address_registry_count` para verificar que el pool se haya liberado después de la limpieza

Prevención:

- Monitorea la utilización del pool de IP con alertas:
  - Advertencia: > 70%
  - Crítica: > 85%
- Análisis de tendencias para predecir el agotamiento
- Implementa tiempo de espera de sesiones inactivas
- Auditorías regulares de sesiones

Problema: Dirección IP Duplicada Asignada

Síntoma:

- UE informa conflicto de dirección IP
- Registros: advertencia "IP ya asignada"
- Dos sesiones en `GET /api/sessions` con la misma dirección IP

Causas Probables:

1. Error de software (raro)
2. Inconsistencia en la base de datos después de un bloqueo
3. Error de intervención manual

Diagnóstico:

1. **Busca la IP a través de la API OAM:**
    - `GET /api/sessions?search=<ip>`
    - Verifica si múltiples IMSIs tienen la misma IP
2. **Verifica los registros:**
    - Busca la dirección IP
    - Busca eventos de "asignación de IP"

Resolución:

1. **Identifica las sesiones afectadas:**
    - Toma nota de ambos IMSIs con IP duplicada
2. **Elimina una sesión:**
    - Coordina con SGW-C para enviar la Solicitud de Eliminar Sesión para un IMSI
    - Prefiere eliminar la sesión más nueva
3. **UE se reconecta:**
    - UE debería reconectarse automáticamente

- Recibirá una nueva IP única

4. **Si persiste:**
   - Reinicia OmniPGW para reconstruir el registro de IP
   - Se perderán todas las sesiones (coordina una ventana de mantenimiento)

Prevención:

- Monitorea asignaciones duplicadas (actualmente no hay métrica incorporada)
- Verificaciones regulares de integridad de la base de datos (si corresponde)

Problema: Sesión IPv4v6 en un APN Sin Pool IPv6

Síntoma:

- Un UE solicita un PDN **IPv4v6** pero el APN coincidente solo tiene un CIDR IPv4 configurado en `ue.subnet_map`
- Un APN **de emergencia (SOS)** aparece **solo IPv4** (sin IPv6 en el PAA); los registros muestran una `advertencia` como "No hay pool IPv6 para el APN de emergencia ...; concediendo solo IPv4"
- Un APN **regular** tiene la sesión **rechazada**; los registros muestran un `error` como "No hay pool IPv6 para el APN ...; rechazando solicitud IPv4v6"

Causas Probables:

1. El APN intencionalmente no tiene rango IPv6 (común en implementaciones solo IPv4)
2. Se omitió un CIDR IPv6 de la entrada `ue.subnet_map` del APN por error

Comportamiento:

- El asignador de IPv6 informa que no hay pool IPv6 (no se bloquea en un pool vacío).

- Los APNs de emergencia (el nombre contiene `"sos"`) degradan a solo IPv4 — dirección IPv4 mantenida, IPv6 borrada, tipo de PDN establecido en IPv4, y el P-CSCF aún se devuelve en el PCO para que funcione el registro IMS de emergencia.
- Los APNs regulares son rechazados (sin degradación silenciosa), mostrando la solicitud no soportada / mala configuración.

Resolución:

1. Si el APN debería ofrecer doble pila, agrega un CIDR IPv6 a su entrada `ue.subnet_map` y reinicia OmniPGW.
2. Si el comportamiento solo IPv4 es intencionado (por ejemplo, un APN SOS en una red solo IPv4), no se requiere ninguna acción.

Consulta Solicitud IPv4v6 cuando el APN no tiene pool IPv6 y Asignación de IP de UE → Problema 4.

Referencia Rápida

Consultas Comunes de Prometheus

```
# Sesiones activas
teid_registry_count

# Tasa de configuración de sesiones (por segundo)
rate(s5s8_inbound_messages_total{message_type="create_session_request

# Utilización del pool de IP (para subred /24)
(address_registry_count / 254) * 100

# Latencia de configuración de sesión P95
histogram_quantile(0.95,
rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m]))

# Tasa de error
rate(s5s8_inbound_errors_total[5m])

# Latencia del PCRF
histogram_quantile(0.95, rate(gx_outbound_transaction_duration_bucket

# Estado de asociación PFCP
pfcp_peer_associated
```

Filtros Comunes de Registros

Grep estas cadenas en los registros del host (`journalctl -u omnipgw_c` o el archivo de registro configurado). Para eventos del ciclo de vida de la sesión, `GET /api/session_history[?type=&search=]` proporciona la misma información en forma estructurada.

Filtro	Propósito
IMSI	Encuentra todos los registros para un suscriptor específico
"create_session"	Flujo de establecimiento de sesión
"delete_session"	Flujo de finalización de sesión
"Credit Control"	Interacciones Gx PCRF
"PFCP Session"	Programación del plano de usuario
"error"	Todos los mensajes de error
"timeout"	Problemas de tiempo de espera
"Association"	Eventos de asociación PFCP

Comandos de Verificación de Salud

```
# Verificar estado del servicio
systemctl status omnipgw_c

# Verificar salud de la API OAM (HTTPS/TLS)
curl -k https://<omnipgw_ip>:8443/api/status

# Verificar el endpoint de métricas
curl http://<omnipgw_ip>:9090/metrics

# Verificar sesiones activas
curl http://<omnipgw_ip>:9090/metrics | grep teid_registry_count

# Verificar asociación PFCP
curl http://<omnipgw_ip>:9090/metrics | grep pfcp_peer_associated

# Verificar uso del pool de IP
curl http://<omnipgw_ip>:9090/metrics | grep
address_registry_count
```

Documentación Relacionada

- **Guía de Monitoreo** - Métricas de Prometheus, paneles de Grafana, alertas
- **Guía de Configuración** - Referencia de configuración del sistema
- **Gestión de Sesiones** - Detalles del ciclo de vida de la sesión
- **Interfaz PFCP** - Detalles de solución de problemas de PFCP
- **Interfaz Gx de Diámetro** - Solución de problemas de políticas Gx
- **Interfaz Gy de Diámetro** - Solución de problemas de carga Gy
- **QoS y Gestión de Portadoras** - Problemas relacionados con QoS

Volver a la Guía de Operaciones

Guía de Solución de Problemas de OmniPGW - *por Omnitouch Network Services*

Documentación de Asignación de Pool de IP de UE

Gestión de Direcciones IP para Dispositivos Móviles

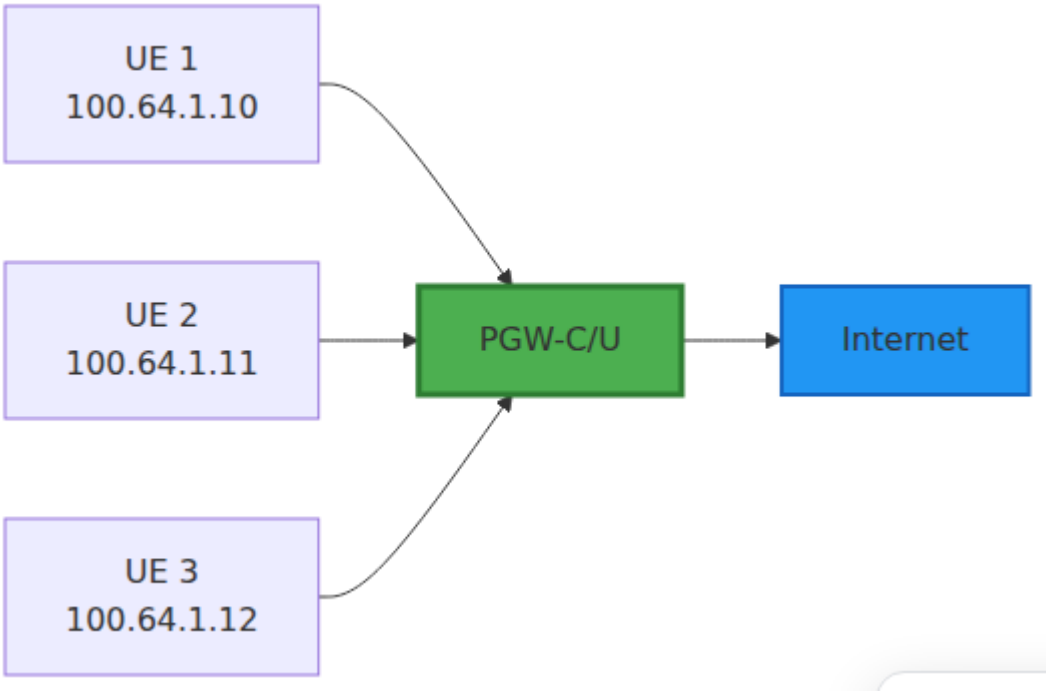
Tabla de Contenidos

1. Descripción General
2. Conceptos de Asignación de IP
3. Configuración
4. Proceso de Asignación
5. Temas Avanzados
6. Monitoreo
7. Resolución de Problemas

Descripción General

El PGW-C asigna direcciones IP a dispositivos UE (Equipo de Usuario) cuando establecen conexiones PDN (Red de Datos por Paquete). Esta es una función crítica que permite a los dispositivos móviles comunicarse con redes externas.

Por Qué Importa la Asignación de IP



Cada UE recibe una **dirección IP única** del PGW-C que:

- Identifica el dispositivo en la red
- Rutea el tráfico hacia/desde el dispositivo
- Permite la facturación y la aplicación de políticas
- Persiste durante la duración de la conexión PDN

Versiones de IP Soportadas

Versión IP	Soporte	Descripción
IPv4	□ Completo	Direcciones IPv4 estándar
IPv6	□ Completo	Direcciones y prefijos IPv6
IPv4v6	□ Completo	Doble pila (tanto IPv4 como IPv6)

Conceptos de Asignación de IP

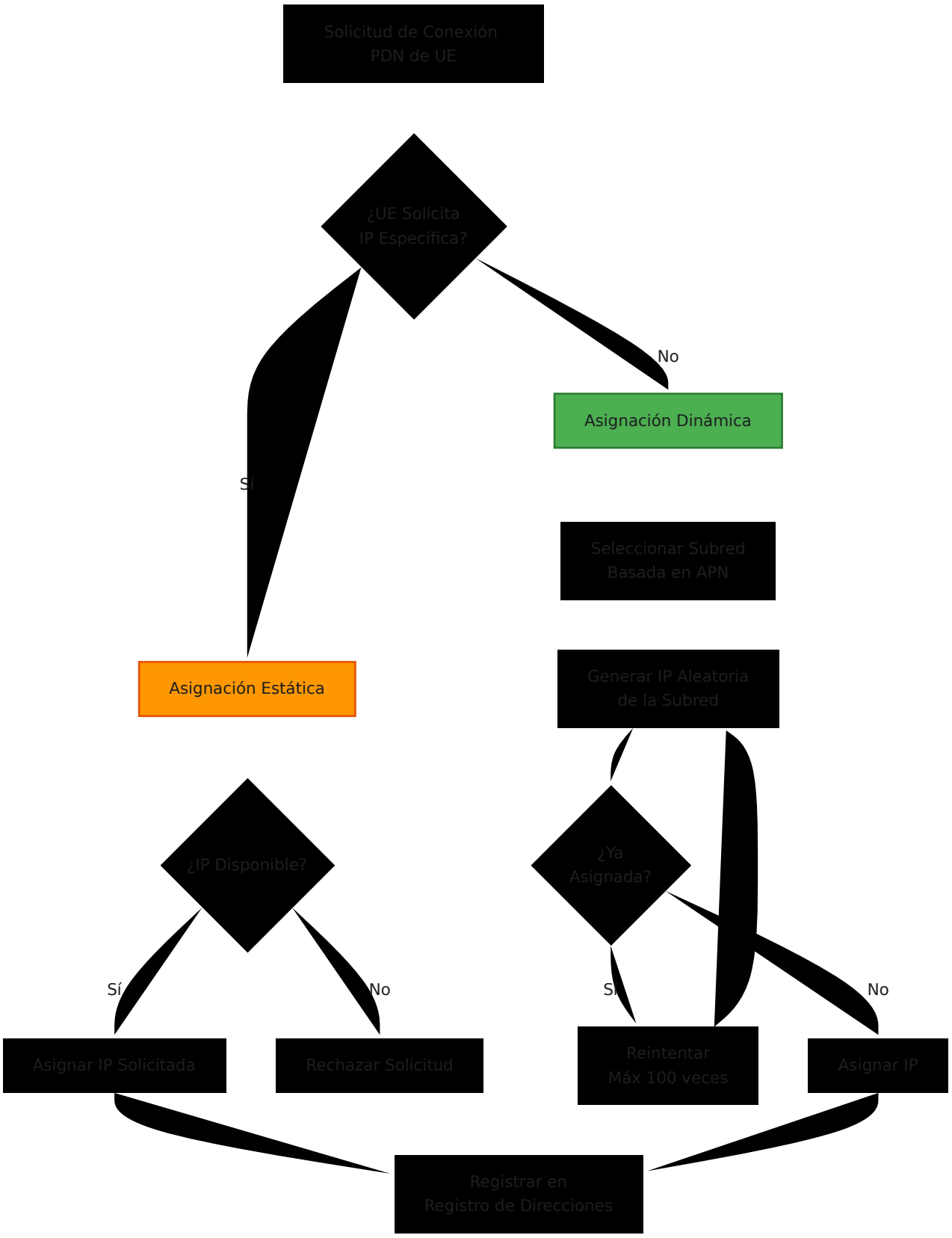
Tipo de PDN

Cuando un UE solicita una conexión PDN, especifica un **Tipo de PDN**:

Tipo de PDN	Descripción	Direcciones Asignadas
IPv4	Conexión solo IPv4	Dirección IPv4 única
IPv6	Conexión solo IPv6	Prefijo IPv6 (por ejemplo, /64)
IPv4v6	Conexión de doble pila	Tanto dirección IPv4 como prefijo IPv6

Métodos de Asignación

El PGW-C soporta dos métodos de asignación de IP:



1. Asignación Dinámica (Más Común):

- El PGW-C selecciona IP del pool configurado
- Selección aleatoria para evitar previsibilidad
- Detección de colisiones asegura unicidad

2. Asignación Estática:

- UE solicita IP específica en el mensaje GTP-C
- El PGW-C valida la disponibilidad
- Útil para dispositivos empresariales con IPs fijas

Selección de Subred Basada en APN

Diferentes **APNs (Nombres de Puntos de Acceso)** pueden utilizar diferentes pools de IP:



Beneficios:

- **Segregación de Tráfico** - Diferentes APNs rutean a diferentes redes
- **Diferenciación de Políticas** - Aplicar diferentes políticas por APN
- **Planificación de Capacidad** - Dimensionar pools según el uso esperado

- **Facturación** - Rastrear uso por tipo de servicio

Registro de Direcciones

El **Registro de Direcciones** rastrea las IPs asignadas:

Función	Descripción
Registro	Mapea IP de UE → PID del Proceso de Sesión
Búsqueda	Encontrar sesión por IP de UE
Deregistro	Liberar IP cuando la sesión termina
Detección de Colisiones	Prevenir asignaciones duplicadas

Configuración

Configuración Básica

Edita `config/runtime.exs`:

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # APN "internet" utiliza dos subredes
      "internet" => [
        "100.64.1.0/24",    # 254 IPs utilizables
        "100.64.2.0/24"     # 254 IPs utilizables
      ],

      # APN "ims" utiliza una subred
      "ims" => [
        "100.64.10.0/24"
      ],

      # Pool predeterminado para APNs desconocidos
      default: [
        "42.42.42.0/24"
      ]
    }
  }
```

Coincidencia de Patrones Regex para APNs

Para escenarios donde múltiples APNs comparten el mismo pool de subred, puedes usar **patrones regex** en lugar de nombres de APN exactos. Esto es útil para coincidencias de APN comodín.

Reglas de Patrón:

- Las claves que comienzan con `^` se tratan como patrones regex
- Las claves sin `^` se coinciden exactamente (compatible hacia atrás)
- Los patrones se evalúan en orden - la primera coincidencia gana
- Se retrocede a `default` si no hay coincidencias de patrón

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # Regex: APNs que comienzan con "ims" (por ejemplo, "ims",
"ims.apn", "ims.something.else")
      "^ims" => [
        "100.64.10.0/24"
      ],

      # Regex: APNs que comienzan con "m2m." (por ejemplo,
"m2m.test", "m2m.prod")
      "^m2m\." => [
        "100.64.20.0/24"
      ],

      # Coincidencia exacta solo - "enterprise.corp" exactamente
      "enterprise.corp" => [
        "10.100.0.0/16"
      ],

      # Pool predeterminado para APNs no coincidentes
      default: [
        "42.42.42.0/24"
      ]
    }
  }
```

Notas Importantes:

- Los patrones regex utilizan la sintaxis estándar de regex de Elixir/Erlang
- Las barras invertidas deben ser escapadas en cadenas de Elixir (usa `\\` para `\`)
- El `^` al inicio es necesario para indicar un patrón regex
- Las coincidencias exactas y los patrones regex pueden mezclarse en la misma configuración
- El orden importa para los patrones regex - coloca patrones más específicos primero

Ejemplos Comunes de Patrones:

Tipo de Patrón	Clave Regex	Coincide
Comienza con	`"^ims"`	`ims`, `ims.apn`, `ims.anything`
Termina con	`"^.*\.corp$"`	`foo.corp`, `bar.corp`
Contiene	`"^.*test.*"`	`test`, `foo.test.bar`, `testing`
Exacto (con puntos)	`"^internet\.apn$"`	`internet.apn` solo

Ejemplo de Coincidencia de Sufijos:

Para coincidir APNs que terminan con un sufijo específico (como `.corp`), usa `^.*\.suffix$`:

```
subnet_map: %{
  # Coincidir APNs que terminan con ".corp"
  "^.*\.corp$" => ["10.100.0.0/16"],

  # Coincidir APNs que terminan con ".iot"
  "^.*\.iot$" => ["10.200.0.0/16"],

  default: ["42.42.42.0/24"]
}
```

Ejemplo de Coincidencia de Patrones:

Solicitud de APN	Clave Coincidente	Pool Usado
`ims`	`^ims`	100.64.10.0/24
`ims.apn`	`^ims`	100.64.10.0/24
`ims.something.else`	`^ims`	100.64.10.0/24
`m2m.test`	`^m2m\.`	100.64.20.0/24
`m2m`	*predeterminado*	42.42.42.0/24
`enterprise.corp`	`enterprise.corp`	10.100.0.0/16
`foo.corp`	`^.*\.corp$`	10.100.0.0/16
`unknown.apn`	*predeterminado*	42.42.42.0/24

Notación de Subred

Notación CIDR: `<red>/<longitud_prefijo>`

CIDR	IPs Utilizables	Rango de Ejemplo
/24	254	100.64.1.1 - 100.64.1.254
/23	510	100.64.0.1 - 100.64.1.254
/22	1022	100.64.0.1 - 100.64.3.254
/20	4094	100.64.0.1 - 100.64.15.254
/16	65534	100.64.0.1 - 100.64.255.254

Notas:

- La dirección de red (por ejemplo, 100.64.1.0) no se asigna
- La dirección de difusión (por ejemplo, 100.64.1.255) no se asigna
- El PGW-C asigna desde `<red> + 1` hasta `<difusión> - 1`

Múltiples Subredes por APN

Balanceo de Carga a Través de Subredes:

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => [
        "100.64.1.0/24",
        "100.64.2.0/24",
        "100.64.3.0/24",
        "100.64.4.0/24"
      ]
    }
  }
```

Método de Selección:

- El PGW-C selecciona aleatoriamente una subred de la lista
- Proporciona un balanceo de carga básico
- Cada sesión selecciona una subred de manera independiente

Beneficios:

- Distribuir la carga a través de múltiples subredes
- Expansión de capacidad más fácil (agregar nuevas subredes)
- Flexibilidad para políticas de enrutamiento

Ejemplo del Mundo Real

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # Acceso general a internet
      "internet" => [
        "100.64.0.0/20"     # 4094 IPs para uso general
      ],

      # IMS (Voz sobre LTE)
      "ims" => [
        "100.64.16.0/22"    # 1022 IPs para IMS
      ],

      # APN Empresarial
      "enterprise.corp" => [
        "10.100.0.0/16"     # 65534 IPs para empresas
      ],

      # Dispositivos IoT (bajo bitrate)
      "iot.m2m" => [
        "100.64.20.0/22"    # 1022 IPs para IoT
      ],

      # Fallback predeterminado
      default: [
        "42.42.42.0/24"     # 254 IPs para APNs desconocidos
      ]
    }
  }
```

Configuración de IPv6

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => [
        # Pools de IPv4
        "100.64.1.0/24"
      ],
      "internet.ipv6" => [
        # Pools de IPv6 (delegación de prefijos)
        "2001:db8:1::/48"
      ],
      default: [
        "42.42.42.0/24"
      ]
    }
  }
```

Delegación de Prefijos IPv6:

- UE típicamente recibe un prefijo /64
- Permite que UE asigne múltiples IPs (por ejemplo, para tethering)
- Ejemplo: UE recibe `2001:db8:1:a::/64`

Configuración de Doble Pila (IPv4v6)

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => [
        "100.64.1.0/24",        # Pool de IPv4
        "2001:db8:1::/48"       # Pool de IPv6 (se usará para
asignación de IPv6)
      ]
    }
  }
```

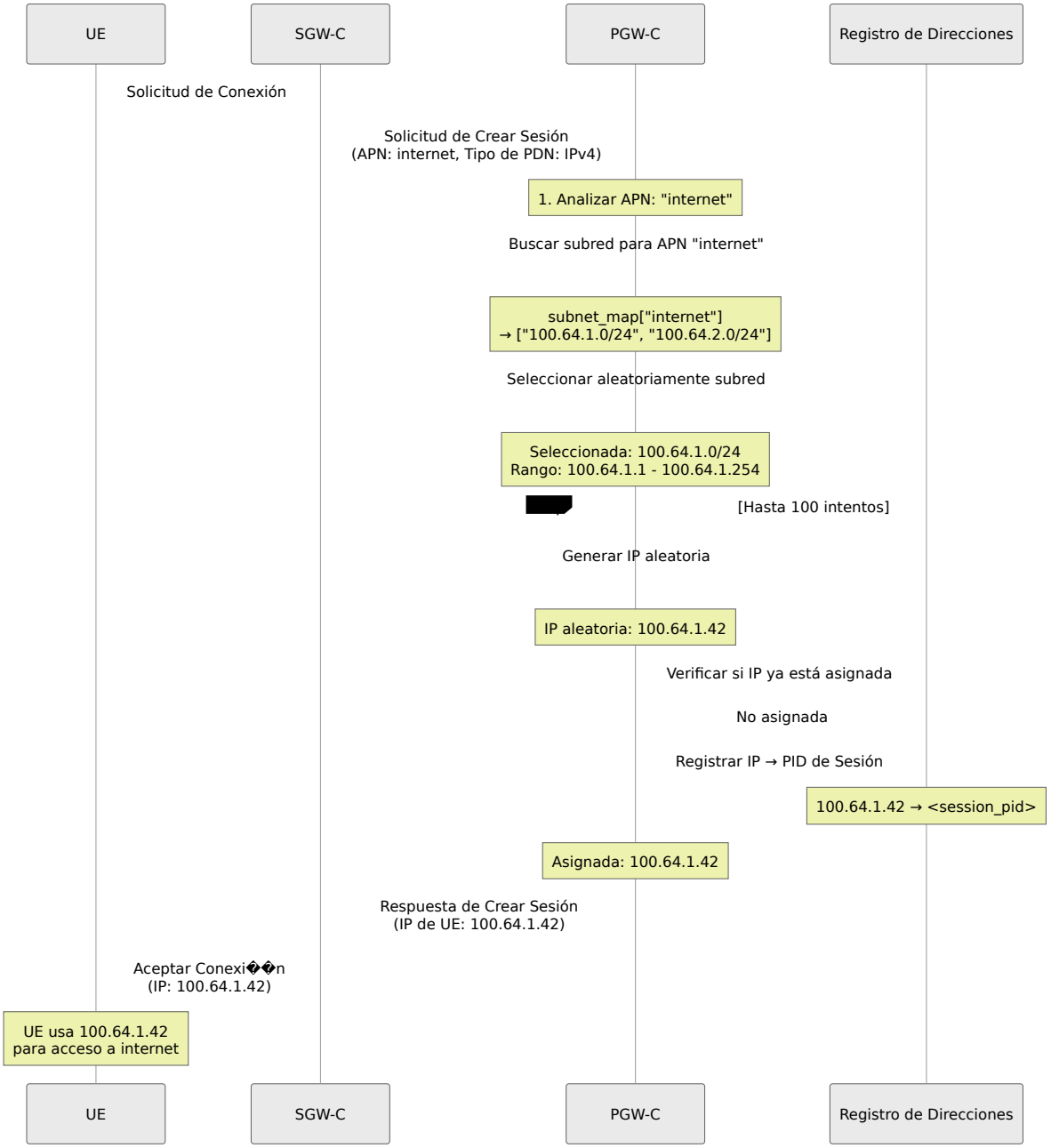
Asignación de Doble Pila:

- UE solicita Tipo de PDN: IPv4v6
- El PGW-C asigna tanto dirección IPv4 como prefijo IPv6
- Ambas direcciones activas simultáneamente

Proceso de Asignación

La asignación de IP ocurre durante la creación de sesión cuando el PGW-C recibe una Solicitud de Crear Sesión a través de la interfaz S5/S8. Consulta Interfaz S5/S8 para detalles del mensaje GTP-C y Gestión de Sesiones para el ciclo de vida de la sesión.

Paso a Paso: Asignación Dinámica de IPv4



Cómo Funciona

Proceso de Asignación Dinámica:

1. **Búsqueda de Subred:** El sistema recupera las subredes configuradas para el APN solicitado
2. **Selección Aleatoria:** Se selecciona aleatoriamente una subred de la lista disponible

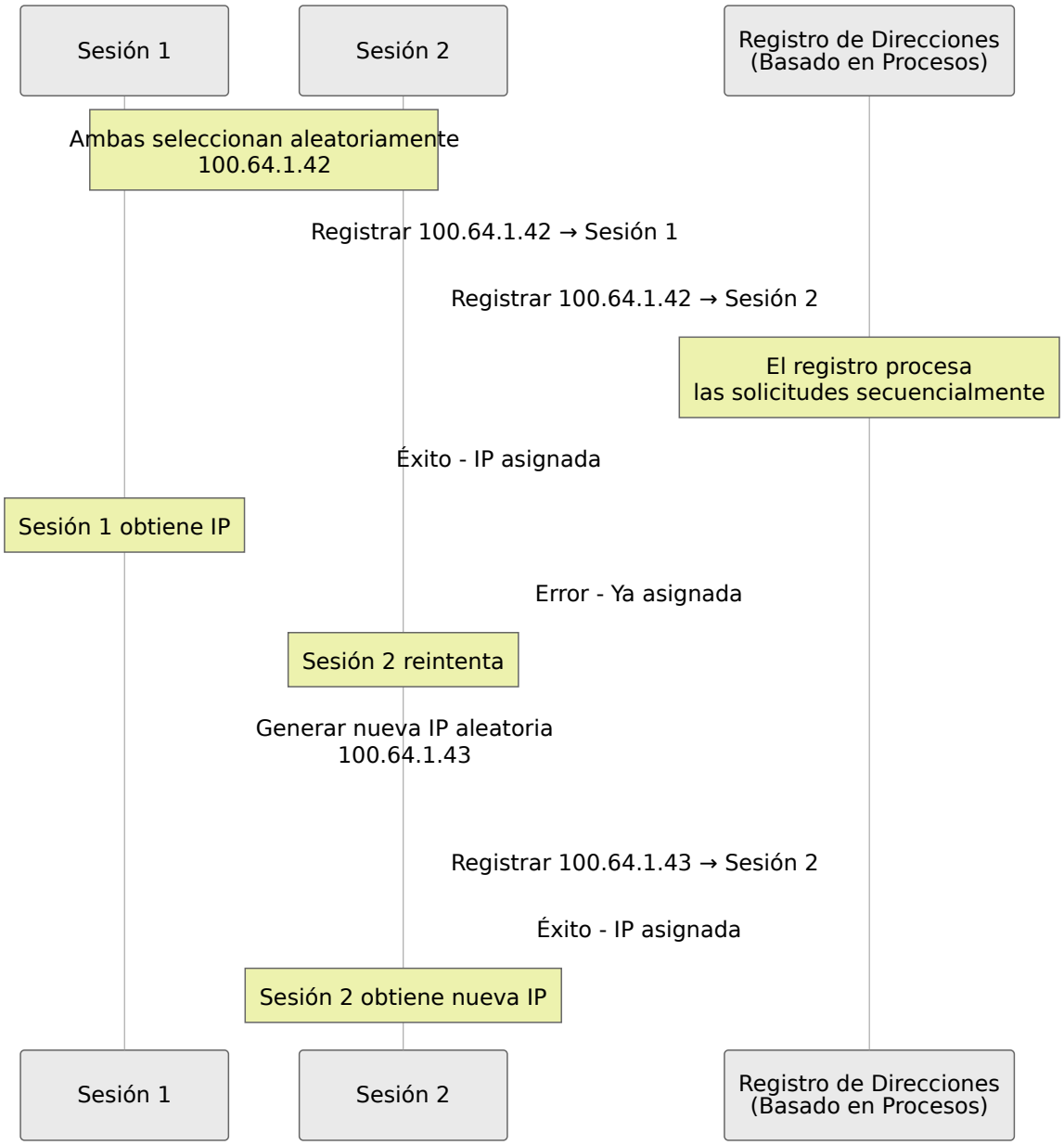
3. **Generación de IP:** Se genera una IP aleatoria dentro del rango de la subred
4. **Verificación de Unicidad:** El sistema verifica que la IP no haya sido asignada
5. **Lógica de Reintento:** Si se detecta una colisión, se reintenta hasta 100 veces con una nueva IP aleatoria
6. **Registro:** Una vez que se encuentra una IP única, se registra a la sesión

Puntos Clave de Diseño:

- **Máximo 100 intentos:** Previene bucles infinitos cuando el pool está casi agotado
- **Selección aleatoria:** Evita patrones de asignación de IP predecibles por razones de seguridad
- **Operaciones atómicas:** El registro basado en procesos asegura que no haya asignaciones duplicadas
- **Retroceso a predeterminado:** Si el APN no se encuentra en la configuración, se utiliza el pool predeterminado

Manejo de Colisiones

Escenario: Dos sesiones intentan asignar la misma IP simultáneamente



Cómo Funciona la Prevención de Colisiones:

- El registro procesa las solicitudes una a la vez (serializado)
- No hay condiciones de carrera posibles
- La primera solicitud para registrar una IP tiene éxito
- Las solicitudes subsiguientes para la misma IP son rechazadas
- Las sesiones rechazadas reintentan automáticamente con una nueva IP aleatoria

Retroceso a Subred Predeterminada

Escenario: UE solicita APN desconocido

Ejemplo de Configuración:

```
# Config
subnet_map: %{
  "internet" => ["100.64.1.0/24"],
  default: ["42.42.42.0/24"]
}
```

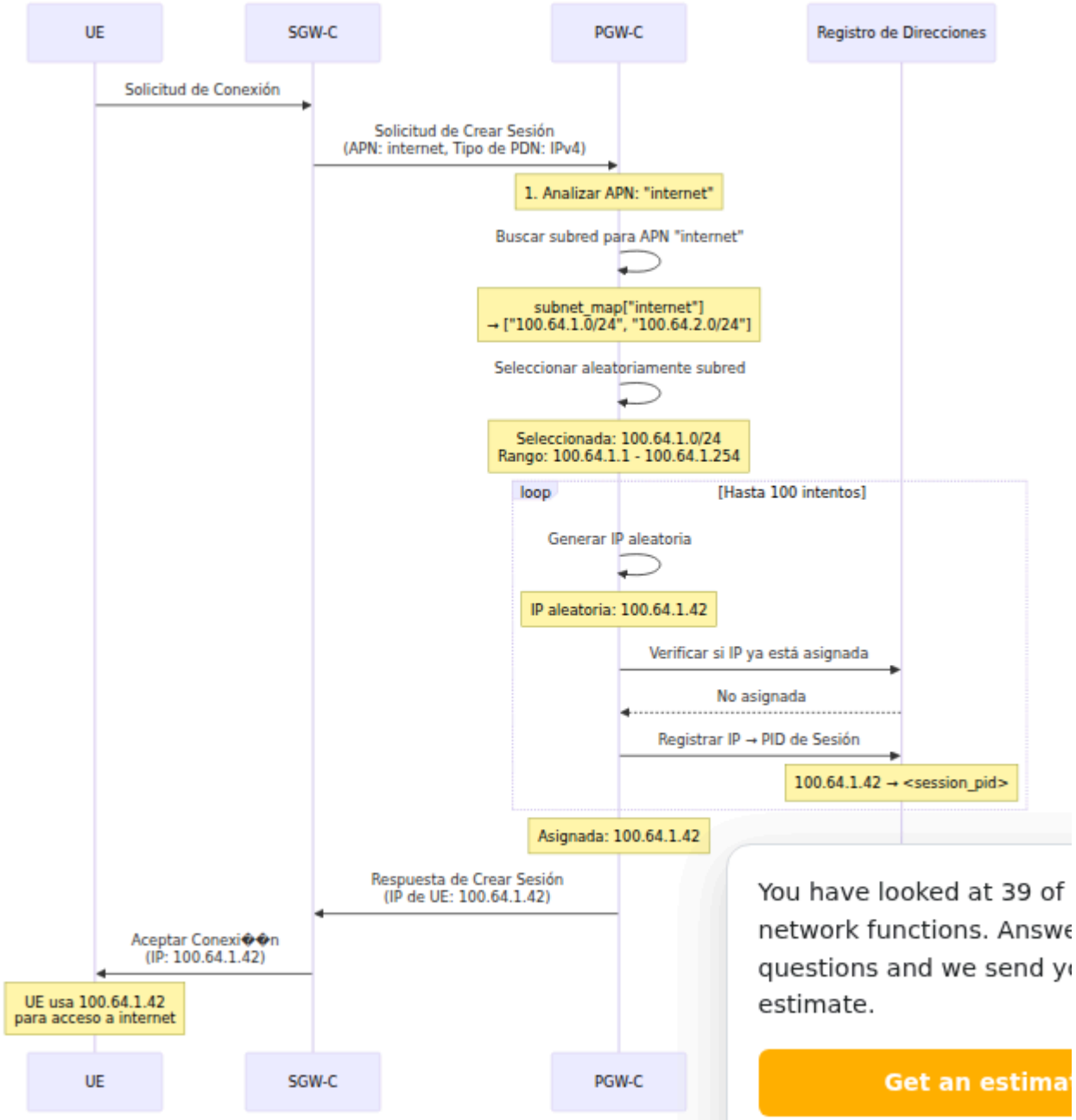
Comportamiento:

- UE solicita APN: "unknown.apn"
- El sistema busca "unknown.apn" en subnet_map
- No se encuentra, por lo que retrocede al pool predeterminado
- Asigna IP del 42.42.42.0/24

Lógica de Retroceso:

1. Primero, intenta encontrar el pool específico del APN en la configuración
2. Si no se encuentra, utiliza el pool `default`
3. Si no hay predeterminado configurado, la asignación falla

Desasignación al Terminar la Sesión



Limpieza Automática:

- Cuando el proceso de sesión termina, el registro se limpia
- IP inmediatamente disponible para nuevas asignaciones
- No se requiere intervención manual

Temas Avanzados

Agotamiento del Pool

Escenario: Todas las IPs en el pool están asignadas

```
Pool: 100.64.1.0/24 (254 IPs utilizables)
Asignadas: 254 IPs
Nueva solicitud llega → Agotamiento
```

Qué Ocurre:

1. El PGW-C intenta 100 asignaciones aleatorias
2. Todos los intentos encuentran IP ya asignada
3. Retorna: `{:error, :ue_ip_address_allocation_failed}`
4. El establecimiento de la sesión falla
5. El SGW-C recibe respuesta de error

Prevención:

```
# Monitorear la utilización del pool
address_registry_count / total_pool_size > 0.8  # Alerta al 80%

# Expandir pool antes del agotamiento
"internet" => [
  "100.64.1.0/24",
  "100.64.2.0/24",  # Agregar subred adicional
  "100.64.3.0/24"
]
```

Asignación Estática de IP

Caso de Uso: Dispositivo empresarial necesita IP fija

Formato del Mensaje GTP-C:

```
Crear Solicitud de Sesión
├── IMSI: 310260123456789
├── APN: enterprise.corp
├── Asignación de Dirección PDN (IE)
│   └── Tipo de PDN: IPv4
│   └── Dirección IPv4: 10.100.0.50  ← UE solicita IP específica
```

Procesamiento de OmniPGW:

1. **Extraer IP Solicitada:** Analizar IE de Asignación de Dirección PDN de la solicitud
2. **Validar IP:** Verificar si la IP solicitada está en el pool configurado para este APN
3. **Verificar Disponibilidad:** Confirmar que la IP no esté ya asignada a otra sesión
4. **Asignar o Rechazar:**
   - Si está disponible: Asignar IP solicitada a esta sesión
   - Si no está disponible: Rechazar la sesión con el código de causa apropiado

Resultados Posibles:

- **Éxito:** UE recibe exactamente la dirección IP que solicitó
- **Fallo (IP en uso):** Sesión rechazada - IP ya asignada
- **Fallo (IP no en pool):** Sesión rechazada - IP no en el rango configurado

Delegación de Prefijos IPv6

UE solicita IPv6:

```
Crear Solicitud de Sesión
├── Tipo de PDN: IPv6
```

El PGW-C asigna prefijo /64:

```
Prefijo Asignado: 2001:db8:1:a::/64

UE puede usar:
- 2001:db8:1:a::1
- 2001:db8:1:a::2
- ... (18 quintillones de direcciones)
```

Beneficios:

- UE puede asignar múltiples IPs (por ejemplo, tethering)
- Soporta SLAAC (Configuración Automática de Direcciones Sin Estado)
- Elimina la necesidad de NAT

Asignación de Doble Pila

UE solicita IPv4v6:

```
Crear Solicitud de Sesión
├── Tipo de PDN: IPv4v6
```

El PGW-C asigna ambos:

```
IPv4: 100.64.1.42
IPv6: 2001:db8:1:a::/64
```

Manejo del Tráfico:

- El tráfico IPv4 utiliza la dirección IPv4
- El tráfico IPv6 utiliza el prefijo IPv6
- Ambos activos simultáneamente
- Túneles GTP separados (o túnel de doble pila)

Cuando el APN no tiene pool de IPv6:

Si se solicita un PDN IPv4v6 pero el APN coincidente solo tiene un CIDR de IPv4 (sin rango IPv6), el asignador de IPv6 devuelve `{:error, :no_ipv6_pool}` en

lugar de fallar, y el procedimiento de sesión decide por tipo de APN:

Tipo de APN	Resultado
APN de Emergencia (SOS) (nombre contiene `"sos"`)	**Degradar a solo IPv4** — mantener la dirección IPv4, limpiar la dirección IPv6, y establecer el tipo de PDN negociado a IPv4. El PAA, PFCP y Gx salen todos solo IPv4, y el P-CSCF aún se devuelve en el PCO para que el registro IMS de emergencia pueda proceder (TS 29.274 / TS 23.401 portador de dirección única / degradación de tipo de PDN).
APN Regular	**Rechazar** — la solicitud no se degrada silenciosamente; la mala configuración (o solicitud no soportada) se hace evidente.

Las solicitudes solo de IPv6 contra un APN sin pool de IPv6 también son rechazadas. Consulta Solicitud IPv4v6 cuando el APN no tiene pool de IPv6 en la guía de IPv6 / Doble Pila para la tabla de comportamiento completa.

Direcciones IP Privadas vs. Públicas

Pools de IP Privadas (RFC 1918):

```
# No enrutables en internet pública
subnet_map: %{
  "internet" => [
    "10.0.0.0/8",
    "172.16.0.0/12",
    "192.168.0.0/16"
  ]
}
```

Requiere NAT en PGW-U para acceder a internet

Pools de IP Públicas:

```
# IPs públicas enrutables (solo un ejemplo)
subnet_map: %{
  "internet" => [
    "203.0.113.0/24"  # Bloque de IP pública
  ]
}
```

No se requiere NAT - enrutamiento directo a internet

Recomendación:

- Usar **IPs privadas (RFC 6598)**: `100.64.0.0/10` (NAT de Grado de Transportista)
- Reservar IPs públicas solo para servicios especiales

Monitoreo

Gestión del Pool de IP

La asignación y utilización del pool de IP se monitorean a través de la API REST de OAM (HTTPS/TLS en el puerto `8443`, rutas bajo el prefijo `/api`). La documentación interactiva (Swagger UI) está disponible en `https://<omnipgw-ip>:8443/api/docs`.

```
GET /api/ip_pools            # todos los pools + utilización
GET /api/ip_pools/<name>     # un pool por nombre
```

Ejemplo:

```
curl -k https://<omnipgw-ip>:8443/api/ip_pools
curl -k https://<omnipgw-ip>:8443/api/ip_pools/Internet
```

Información por Pool devuelta para cada pool configurado:

Campo	Descripción
Nombre	Identificador de Pool / APN (por ejemplo, "predeterminado", "ims.something.else", "Internet")
Total	Número de IPs en el pool
Usado	IPs actualmente asignadas
Libre	IPs restantes disponibles para asignación
Utilización %	Porcentaje del pool actualmente asignado

Casos de Uso:

- Verificación rápida de capacidad antes del mantenimiento
- Identificar pools que se acercan al agotamiento
- Verificar configuración del pool
- Monitorear patrones de asignación por APN

Métricas Clave

Conteo del Registro de Direcciones:

```
# IPs actualmente asignadas
address_registry_count

# Utilización del pool (requiere cálculo)
address_registry_count / <total_pool_size> * 100
```

Ejemplo:

```
Pool: 100.64.1.0/24 (254 IPs)
Asignadas: 150 IPs
Utilización: 150 / 254 = 59%
```

Alertas

```yaml
# Alerta sobre alta utilización del pool
- alert: UEIPPoolUtilizationHigh
  expr: address_registry_count > 200  # Para pool /24
  for: 10m
  annotations:
    summary: "Utilización del pool de IP de UE por encima del 80%"
    description: "Actual: {{ $value }} / 254 IPs asignadas"

# Alerta sobre agotamiento del pool
- alert: UEIPPoolExhausted
  expr: address_registry_count >= 254  # Para pool /24
  for: 1m
  annotations:
    summary: "Pool de IP de UE agotado - no hay IPs disponibles"

# Alerta sobre fallos de asignación
- alert: UEIPAllocationFailures
  expr: rate(ue_ip_allocation_failures_total[5m]) > 0
  for: 5m
  annotations:
    summary: "Ocurriendo fallos en la asignación de IP de UE"
```

Dashboard de Grafana

Panel 1: Utilización del Pool de IP

```
# Medida que muestra el porcentaje
(address_registry_count / 254) * 100
```

Panel 2: IPs Asignadas a lo Largo del Tiempo

```
# Serie temporal
address_registry_count
```

Panel 3: Tasa de Asignación

```
# Tasa de nuevas asignaciones
rate(address_registry_count[5m])
```

Panel 4: Riesgo de Agotamiento del Pool

```
# Días hasta el agotamiento (basado en la tasa actual)
(254 - address_registry_count) / rate(address_registry_count[1h])
```

Resolución de Problemas

Problema 1: Falla en el Establecimiento de la Sesión (No hay IP Disponible)

Síntomas:

- Respuesta de Crear Sesión: Causa "Solicitud rechazada"
- Registro: "Fallo en la asignación de dirección IP de UE"

Causas Posibles:

1. **Pool Agotado**

   ```
   # Verificar asignación actual
   curl http://<pgw_c_ip>:42069/metrics | grep
   address_registry_count
   ```

2. **Error de Configuración**

```
# Verificar configuración de subred
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => [
        "100.64.1.0/24"  # Asegurarse de que sea un CIDR válido
      ]
    }
  }
```

3. **Mala Configuración de APN**

```
# Si el APN no se encuentra, retrocede al predeterminado
# Asegurarse de que exista un pool predeterminado
subnet_map: %{
  default: ["42.42.42.0/24"]
}
```

Resolución:

- **Expandir pool:** Agregar más subredes
- **Limpiar sesiones obsoletas:** Reiniciar PGW-C para liberar IPs filtradas
- **Verificar configuración:** Revisar `runtime.exs` en busca de errores tipográficos

Problema 2: Colisión de Direcciones IP

Síntomas:

- Dos UEs reciben la misma IP (muy raro)
- Problemas de enrutamiento

Causa:

- Error en el Registro de Direcciones (no debería ocurrir)

Depurar:

```
# Verificar duplicados de IP en los registros
grep "already_registered" /var/log/pgw_c.log
```

Resolución:

- Debería corregirse automáticamente (la segunda sesión reintenta)
- Si persiste, reportar error

Problema 3: Se Utiliza el Pool de IP Incorrecto

Síntomas:

- UE recibe IP de subred inesperada
- APN "internet" obtiene IP del pool "ims"

Causa:

- Configuración incorrecta de subnet_map

Verificar:

```
# Verificar coincidencia exacta de la cadena de APN
subnet_map: %{
  "internet" => [...],    # Sensible a mayúsculas
  "Internet" => [...]     # ¡APN diferente!
}
```

Resolución:

- Asegurarse de que los nombres de APN coincidan exactamente (sensible a mayúsculas)
- Usar el pool predeterminado para capturas

Problema 4: Falla en la Asignación de IPv6

Síntomas:

- UE solicita IPv6, recibe error
- Un UE solicita un **IPv4v6** PDN contra un APN sin rango IPv6 y recibe una sesión **solo IPv4** (APN SOS) o tiene la sesión **rechazada** (APN regular)

Causas Posibles:

1. **No hay pool de IPv6 configurado**

```
# Falta subredes IPv6
subnet_map: %{
  "internet" => [
    "100.64.1.0/24"  # Solo IPv4
  ]
}
```

2. **Prefijo IPv6 no válido**

```
# Prefijo demasiado pequeño (debería ser /48 o mayor)
"internet" => [
  "2001:db8::/128"  # Incorrecto - no hay espacio para
asignación
]
```

IPv4v6 sin pool de IPv6 (degradar vs. rechazar):

Cuando una solicitud **IPv4v6** golpea un APN sin rango IPv6, `register_new_ipv6/1` devuelve `{:error, :no_ipv6_pool}` (no **se** bloquea). La sesión entonces:

- **APN de Emergencia (SOS)** (nombre contiene `"sos"`): se degrada a **solo IPv4** — asigna la dirección IPv4, limpia la dirección IPv6, establece el tipo de PDN negociado a IPv4, y aún devuelve el P-CSCF en el PCO. Registrado como una `advertencia`.
- **APN Regular**: **rechaza** con `{:error, :no_ipv6_pool}` — no hay degradación silenciosa. Registrado como un `error`.

Consulta Solicitud IPv4v6 cuando el APN no tiene pool de IPv6.

Resolución:

```
# Agregar pool de IPv6 (para un APN regular que debería ofrecer
doble pila)
subnet_map: %{
  "internet" => [
    "100.64.1.0/24",
    "2001:db8:1::/48"  # Pool de IPv6
  ]
}
```

Para un APN de emergencia (SOS) en un despliegue solo de IPv4, la degradación solo de IPv4 es intencional — agrega un CIDR de IPv6 solo si los PDNs SOS deben ser de doble pila.

Problema 5: Alta Utilización del Pool

Síntomas:

- Acercándose al agotamiento del pool
- `address_registry_count` acercándose al máximo

Medidas Proactivas:

1. **Agregar Subredes:**

   ```
   "internet" => [
     "100.64.1.0/24",   # Existente
     "100.64.2.0/24",   # Nueva subred (agrega 254 IPs)
     "100.64.3.0/24"    # Nueva subred (agrega 254 IPs)
   ]
   ```

2. **Usar Subredes Más Grandes:**

   ```
   # Reemplazar /24 con /22
   "internet" => [
     "100.64.0.0/22"  # 1022 IPs utilizables
   ]
   ```

3. **Limpieza de Sesiones:**
    - Monitorear sesiones obsoletas
    - Asegurarse de que se maneje correctamente la Solicitud de Eliminar Sesión

---

Mejores Prácticas

Planificación de Capacidad

Calcular el tamaño del pool requerido:

```
Usuarios concurrentes esperados: 10,000
Concurrencia máxima: 30% (3,000 sesiones simultáneas)
Buffer de crecimiento: 50%
IPs requeridas: 3,000 * 1.5 = 4,500 IPs

Subred: /20 (4,094 IPs utilizables) - Demasiado pequeña
Subred: /19 (8,190 IPs utilizables) - Suficiente
```

Selección de Subred

Recomendado:

- Usar `100.64.0.0/10` (RFC 6598 - NAT de Grado de Transportista)
- Proporciona 4 millones de IPs
- Reservado para NAT de proveedores de servicios

Evitar:

- IPs públicas (costosas, limitadas)
- Rangos privados comunes que conflijan con VPNs empresariales

Diseño de Configuración

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # APN principal de internet - pool grande
      "internet" => [
        "100.64.0.0/18"  # 16,382 IPs
      ],

      # IMS - pool dedicado más pequeño
      "ims" => [
        "100.64.64.0/22"  # 1,022 IPs
      ],

      # Empresarial - pool mediano
      "enterprise.corp" => [
        "100.64.68.0/22"  # 1,022 IPs
      ],

      # IoT - pool grande para muchos dispositivos
      "iot.m2m" => [
        "100.64.72.0/20"  # 4,094 IPs
      ],

      # Predeterminado - fallback pequeño
      default: [
        "100.64.127.0/24"  # 254 IPs
      ]
    }
  }
```

Documentación Relacionada

Configuración

- **Guía de Configuración** - Configuración del pool de IP de UE, mapeo de subredes APN

- **Configuración de PCO** - DNS, P-CSCF, MTU entregados con dirección IP
- **Gestión de Sesiones** - Ciclo de vida de la sesión, asignación de IP durante la configuración de PDN
- **Interfaz PFCP** - Asignación de direcciones de UE a través de PFCP a UPF

Planificación de Redes

- **Interfaz S5/S8** - Entrega de direcciones IP a través de GTP-C
- **Interfaz Diameter Gx** - Control de políticas para la asignación de IP

Operaciones

- **Guía de Monitoreo** - Métricas de utilización del pool de IP, seguimiento de asignaciones
- **Formato de CDR de Datos** - Direcciones IP de UE en CDRs para correlación de facturación

---

Volver a la Guía de Operaciones