Guía de Operaciones de OmniUPF

Tabla de Contenidos

1. Descripción General
2. Comprendiendo la Arquitectura del Plano de Usuario 5G
3. Componentes del UPF
4. Protocolo PFCP e Integración con SMF
5. Operaciones Comunes
6. Resolución de Problemas
7. Documentación Adicional
8. Glosario

Descripción General

OmniUPF (Función de Plano de Usuario basada en eBPF) es una Función de Plano de Usuario 5G/LTE de alto rendimiento que proporciona reenvío de paquetes de grado de operador, aplicación de QoS y gestión de tráfico para redes móviles. Construido sobre la tecnología eBPF de Linux (Filtro de Paquetes de Berkeley extendido) y mejorado con capacidades de gestión integrales, OmniUPF ofrece la infraestructura central de procesamiento de paquetes requerida para redes 5G SA, 5G NSA y LTE.

¿Qué es una Función de Plano de Usuario?

La Función de Plano de Usuario (UPF) es el elemento de red estandarizado por 3GPP responsable del procesamiento y reenvío de paquetes en redes 5G y LTE. Proporciona:

- **Reenvío de paquetes de alta velocidad** entre dispositivos móviles y redes de datos
- **Aplicación de Calidad de Servicio (QoS)** para diferentes tipos de tráfico
- **Detección y enrutamiento de tráfico** basado en filtros y reglas de paquetes
- **Informe de uso** para facturación y análisis
- **Almacenamiento en búfer de paquetes** para escenarios de gestión de movilidad y sesiones
- Soporte para **intercepción legal** para cumplimiento regulatorio

OmniUPF implementa la funcionalidad completa de UPF definida en 3GPP TS 23.501 (5G) y TS 23.401 (LTE), proporcionando una solución de plano de usuario completa y lista para producción utilizando la tecnología eBPF del núcleo de Linux para un rendimiento máximo.

Capacidades Clave de OmniUPF

Procesamiento de Paquetes:

- Procesamiento de paquetes de plano de usuario completamente conforme a 3GPP
- Ruta de datos basada en eBPF para un rendimiento a nivel de núcleo
- Encapsulación y desencapsulación de GTP-U (Protocolo de Túnel GPRS)
- Soporte para IPv4 e IPv6 tanto para redes de acceso como de datos
- XDP (Ruta de Datos eXpress) para procesamiento de latencia ultra baja
- Procesamiento de paquetes multihilo

QoS y Gestión de Tráfico:

- Reglas de Aplicación de QoS (QER) para gestión de ancho de banda
- Reglas de Detección de Paquetes (PDR) para clasificación de tráfico
- Reglas de Acción de Reenvío (FAR) para decisiones de enrutamiento
- Filtrado de Flujo de Datos de Servicio (SDF) para enrutamiento específico de aplicaciones
- Reglas de Informe de Uso (URR) para seguimiento de volumen y facturación

Control y Gestión:

- Interfaz PFCP (Protocolo de Control de Reenvío de Paquetes) a SMF/PGW-C
- API RESTful para monitoreo y diagnóstico
- Estadísticas y métricas en tiempo real
- Monitoreo de capacidad de mapas eBPF
- Panel de control basado en web

Características de Rendimiento:

- Procesamiento de paquetes sin copia a través de eBPF
- Reenvío de paquetes a nivel de núcleo (sin sobrecarga de espacio de usuario)
- Escalabilidad multinúcleo
- Capaz de descarga para aceleración de hardware
- Optimizado para implementaciones nativas en la nube

Para un uso detallado del panel de control, consulte Operaciones de UI Web.

Comprendiendo la Arquitectura del Plano de Usuario

OmniUPF es una solución unificada de plano de usuario que proporciona reenvío de paquetes de grado de operador para redes 5G Standalone (SA), 5G NSA y 4G LTE/EPC. **OmniUPF es un solo producto** que puede funcionar simultáneamente como:

- **UPF (Función de Plano de Usuario)** - plano de usuario 5G/NSA (controlado por OmniSMF a través de N4/PFCP)
- **PGW-U (Puerta de Enlace de PDN de Plano de Usuario)** - puerta de enlace EPC 4G a redes externas (controlado por OmniPGW-C a través de Sxc/PFCP)
- **SGW-U (Puerta de Enlace de Servicio de Plano de Usuario)** - puerta de enlace de servicio EPC 4G (controlado por OmniSGW-C a través de Sxb/PFCP)

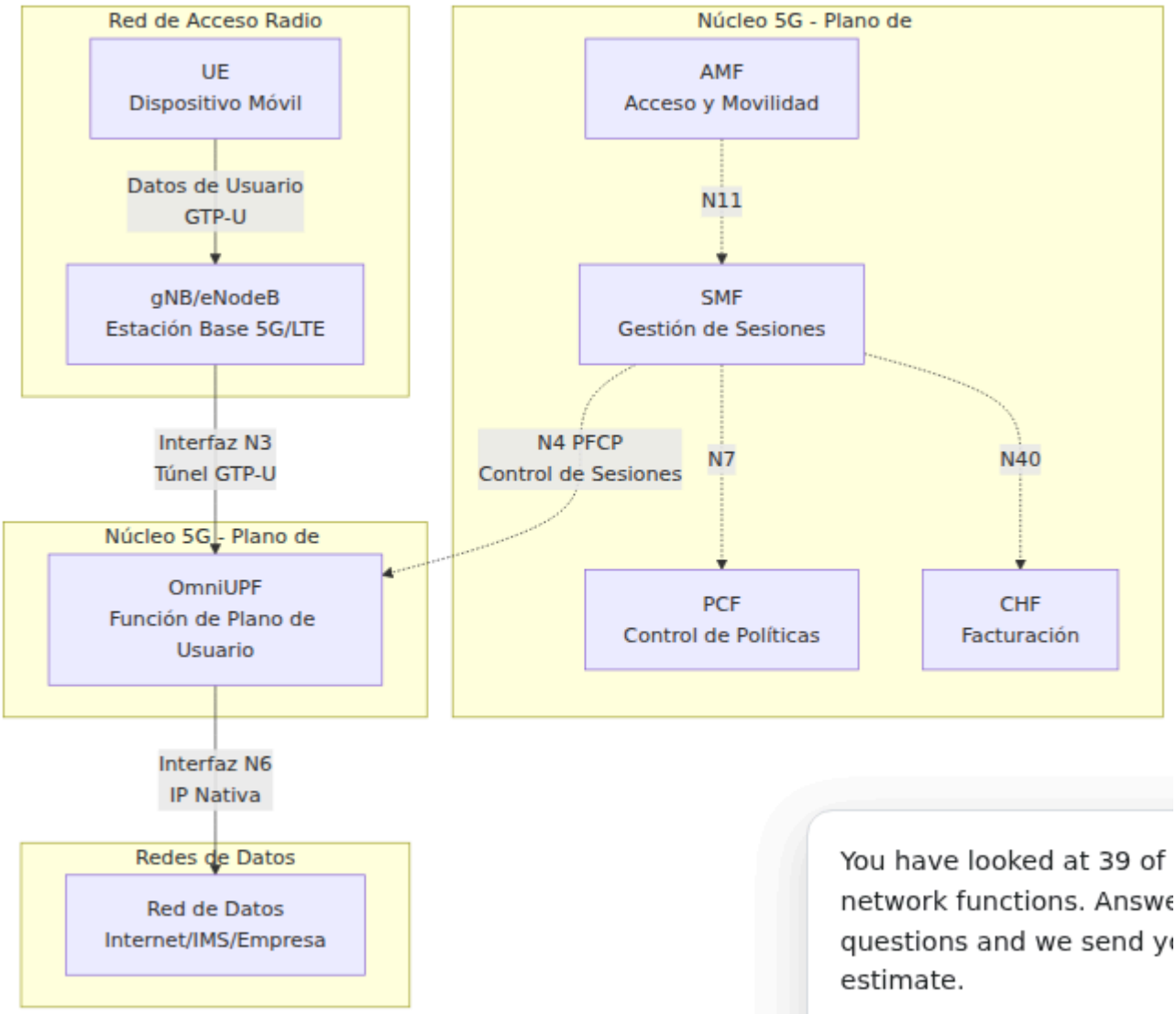
OmniUPF puede operar en **cualquier combinación** de estos modos:

- **Solo UPF**: Implementación pura de 5G
- **PGW-U + SGW-U**: Puerta de enlace 4G combinada (implementación típica de EPC)
- **UPF + PGW-U + SGW-U**: Soporte simultáneo para 4G y 5G (escenario de migración)

Todos los modos utilizan el mismo motor de procesamiento de paquetes basado en eBPF y el protocolo PFCP, proporcionando un alto rendimiento consistente ya sea operando como UPF, PGW-U, SGW-U, o los tres simultáneamente.

Arquitectura de Red 5G (Modo SA)

La solución OmniUPF se sitúa en el plano de datos de las redes 5G, proporcionando la capa de reenvío de paquetes de alta velocidad que conecta dispositivos móviles a redes y servicios de datos.



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

Arquitectura de Red 4G LTE/EPC

OmniUPF también soporta implementaciones 4G LTE y EPC (Núcleo de Paquetes Evolucionado), funcionando como OmniPGW-U o OmniSGW-U dependiendo de la arquitectura de la red.

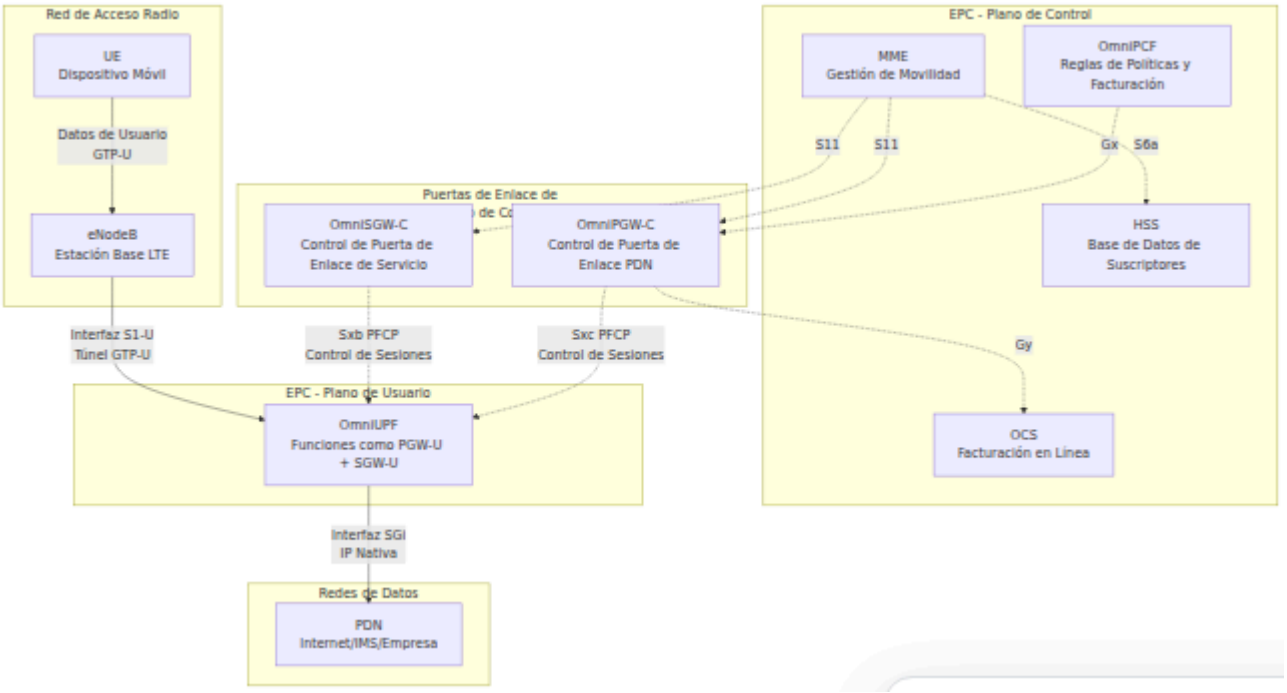
Modo Combinado PGW-U/SGW-U (Implementación Típica de 4G)

En este modo, OmniUPF actúa como SGW-U y PGW-U, controlado por funciones de plano de control separadas.



Modo Separado SGW-U y PGW-U (Roaming/Múltiples Sitios)

En implementaciones de roaming o múltiples sitios, se pueden desplegar dos instancias separadas de OmniUPF: una como SGW-U y otra como PGW-U.



Cómo Funcionan las Funciones de Plano de Usuario en la Red

La función de plano de usuario (OmniUPF, OmniPGW-U o OmniSGW-U) opera como el plano de reenvío controlado por el respectivo plano de control:

1. **Establecimiento de Sesión**
    - **5G**: OmniSMF establece la asociación PFCP a través de la interfaz N4 con OmniUPF
    - **4G**: OmniPGW-C o OmniSGW-C establece la asociación PFCP a través de Sxb/Sxc con OmniPGW-U/OmniSGW-U
    - El plano de control crea sesiones PFCP para cada sesión PDU de UE (5G) o contexto PDP (4G)
    - El plano de usuario recibe reglas PDR, FAR, QER y URR a través de PFCP
    - Los mapas eBPF se llenan con reglas de reenvío
2. **Procesamiento de Paquetes de Enlace Ascendente** (UE → Red de Datos)
    - **5G**: Los paquetes llegan a través de la interfaz N3 desde gNB con encapsulación GTP-U
    - **4G**: Los paquetes llegan a través de la interfaz S1-U (SGW-U) o S5/S8 (PGW-U) desde eNodeB con encapsulación GTP-U
    - El plano de usuario compara los paquetes con los PDR de enlace ascendente basándose en TEID
    - El programa eBPF aplica QER (limitación de tasa, marcado)
    - FAR determina la acción de reenvío (reenviar, descartar, almacenar en búfer, duplicar)
    - Se elimina el túnel GTP-U, los paquetes se reenvían a la interfaz N6 (5G) o SGi (4G)
    - URR rastrea el conteo de paquetes y bytes para la facturación
3. **Procesamiento de Paquetes de Enlace Descendente** (Red de Datos → UE)
    - **5G**: Los paquetes llegan a través de la interfaz N6 como IP nativa

- **4G**: Los paquetes llegan a través de la interfaz SGi como IP nativa
- El plano de usuario compara los paquetes con los PDR de enlace descendente basándose en la dirección IP de UE
- Los filtros SDF pueden clasificar aún más el tráfico por puerto, protocolo o aplicación
- FAR determina el túnel GTP-U y los parámetros de reenvío
- Se agrega la encapsulación GTP-U con el TEID apropiado
- **5G**: Los paquetes se reenvían a la interfaz N3 hacia gNB
- **4G**: Los paquetes se reenvían a S1-U (SGW-U) o S5/S8 (PGW-U) hacia eNodeB

4. **Movilidad y Transferencia**

   - **5G**: OmniSMF actualiza las reglas PDR/FAR durante escenarios de transferencia
   - **4G**: OmniSGW-C/OmniPGW-C actualiza las reglas durante la transferencia inter-eNodeB o TAU (Actualización de Área de Seguimiento)
   - El plano de usuario puede almacenar paquetes en búfer durante el cambio de ruta
   - Transición sin problemas entre estaciones base sin pérdida de paquetes

Integración con el Plano de Control (4G y 5G)

OmniUPF se integra con funciones de plano de control 5G y 4G a través de interfaces estándar de 3GPP:

Interfaces 5G

Interfaz	De → A	Propósito	Especificación 3GPP
N4	OmniSMF ↔ OmniUPF	Establecimiento, modificación, eliminación de sesión PFCP	TS 29.244
N3	gNB → OmniUPF	Tráfico de plano de usuario desde RAN (GTP-U)	TS 29.281
N6	OmniUPF → Red de Datos	Tráfico de plano de usuario hacia DN (IP nativa)	TS 23.501
N9	OmniUPF ↔ OmniUPF	Comunicación entre UPF para roaming/borde	TS 23.501

Interfaces 4G/EPC

Interfaz	De → A	Propósito	Especificación 3GPP
Sxb	OmniSGW-C ↔ OmniUPF (modo SGW-U)	Control de sesión PFCP para puerta de enlace de servicio	TS 29.244
Sxc	OmniPGW-C ↔ OmniUPF (modo PGW-U)	Control de sesión PFCP para puerta de enlace PDN	TS 29.244
S1-U	eNodeB → OmniUPF (modo SGW-U)	Tráfico de plano de usuario desde RAN (GTP-U)	TS 29.281
S5/S8	OmniUPF (SGW-U) ↔ OmniUPF (PGW-U)	Plano de usuario entre puertas de enlace (GTP-U)	TS 29.281
SGi	OmniUPF (modo PGW-U) → PDN	Tráfico de plano de usuario hacia la red de datos (IP nativa)	TS 23.401

Nota: Todas las interfaces PFCP (N4, Sxb, Sxc) utilizan el mismo protocolo PFCP definido en TS 29.244. Los nombres de las interfaces difieren, pero el protocolo y los formatos de mensaje son idénticos.

Componentes del UPF

Ruta de Datos eBPF

La **ruta de datos eBPF** es el motor central de procesamiento de paquetes que se ejecuta en el núcleo de Linux para un rendimiento máximo.

Funciones Principales:

- **Procesamiento de GTP-U**: Encapsulación y desencapsulación de túneles GTP-U
- **Clasificación de Paquetes**: Comparar paquetes con reglas PDR utilizando TEID, IP de UE o filtros SDF
- **Aplicación de QoS**: Aplicar limitación de tasa y marcado de paquetes según las reglas QER
- **Decisiones de Reenvío**: Ejecutar acciones FAR (reenviar, descartar, almacenar en búfer, duplicar, notificar)
- **Seguimiento de Uso**: Incrementar contadores URR para facturación basada en volumen

Mapas eBPF: La ruta de datos utiliza mapas eBPF (tablas hash en la memoria del núcleo) para el almacenamiento de reglas:

Nombre del Mapa	Propósito	Clave	Valor
`uplink_pdr_map`	PDR de enlace ascendente	TEID (32 bits)	Información PDR (ID de FAR, ID de QER, IDs de URR)
`downlink_pdr_map`	PDR de enlace descendente (IPv4)	Dirección IP de UE	Información PDR
`downlink_pdr_map_ip6`	PDR de enlace descendente (IPv6)	Dirección IPv6 de UE	Información PDR
`far_map`	Reglas de reenvío	ID de FAR	Parámetros de reenvío (acción, información de túnel)
`qer_map`	Reglas de QoS	ID de QER	Parámetros de QoS (MBR, GBR, marcado)
`urr_map`	Seguimiento de uso	ID de URR	Contadores de volumen (enlace ascendente, enlace descendente, total)
`sdf_filter_map`	Filtros SDF	ID de PDR	Filtros de aplicación (puertos, protocolos)

Características de Rendimiento:

- **Sin copia**: Paquetes procesados completamente en espacio de núcleo
- **Soporte XDP**: Adjuntar a nivel de controlador de red para latencia sub-microsegundo
- **Multinúcleo**: Escala a través de núcleos de CPU con soporte de mapa por CPU
- **Capacidad**: Millones de PDRs/FARs en mapas eBPF (limitado por la memoria del núcleo)

Para el monitoreo de capacidad, consulte Gestión de Capacidad.

Manejador de Interfaz PFCP

La **interfaz PFCP** implementa 3GPP TS 29.244 para la comunicación con SMF o PGW-C.

Funciones Principales:

- **Gestión de Asociación**: Latido PFCP y configuración/liberación de asociación
- **Ciclo de Vida de Sesión**: Crear, modificar y eliminar sesiones PFCP
- **Instalación de Reglas**: Traducir IEs de PFCP en entradas de mapa eBPF
- **Informe de Eventos**: Notificar a SMF sobre umbrales de uso, errores o eventos de sesión

Soporte de Mensajes PFCP:

Tipo de Mensaje	Dirección	Propósito
Configuración de Asociación	SMF → UPF	Establecer asociación de control PFCP
Liberación de Asociación	SMF → UPF	Destruir asociación PFCP
Latido	Bidireccional	Mantener viva la asociación
Establecimiento de Sesión	SMF → UPF	Crear nueva sesión PDU con PDR/FAR/QER/URR
Modificación de Sesión	SMF → UPF	Actualizar reglas para movilidad, cambios de QoS
Eliminación de Sesión	SMF → UPF	Eliminar sesión y todas las reglas asociadas
Informe de Sesión	UPF → SMF	Informar uso, errores o eventos

Elementos de Información (IE) Soportados:

- Crear PDR, FAR, QER, URR
- Actualizar PDR, FAR, QER, URR
- Eliminar PDR, FAR, QER, URR
- Información de Detección de Paquetes (IP de UE, F-TEID, filtro SDF)
- Parámetros de Reenvío (instancia de red, creación de encabezado externo)
- Parámetros de QoS (MBR, GBR, QFI)
- Disparadores de Informe de Uso (umbral de volumen, umbral de tiempo)

Servidor API REST

La **API REST** proporciona acceso programático al estado y operaciones del UPF.

Funciones Principales:

- **Monitoreo de Sesiones**: Consultar sesiones PFCP activas y asociaciones
- **Inspección de Reglas**: Ver configuraciones de PDR, FAR, QER, URR
- **Estadísticas**: Recuperar contadores de paquetes, estadísticas de rutas, estadísticas de XDP
- **Gestión de Búfer**: Ver y controlar búferes de paquetes
- **Información de Mapas**: Monitorear uso y capacidad de mapas eBPF

Puntos Finales de API: (34 puntos finales en total)

Categoría	Puntos Finales	Descripción
Salud	`/health`	Verificación de salud y estado
Configuración	`/config`	Configuración del UPF
Sesiones	`/pfcp_sessions`, `/pfcp_associations`	Datos de sesión/asociación PFCP
PDRs	`/uplink_pdr_map`, `/downlink_pdr_map`, `/downlink_pdr_map_ip6`, `/uplink_pdr_map_ip6`	Reglas de detección de paquetes
FARs	`/far_map`	Reglas de acción de reenvío
QERs	`/qer_map`	Reglas de aplicación de QoS
URRs	`/urr_map`	Reglas de informe de uso
Búferes	`/buffer`	Estado y control del búfer de paquetes
Estadísticas	`/packet_stats`, `/route_stats`, `/xdp_stats`, `/n3n6_stats`	Métricas de rendimiento
Capacidad	`/map_info`	Capacidad y uso de mapas eBPF
Plano de Datos	`/dataplane_config`	Direcciones de interfaz N3/N9

Para detalles y uso de la API, consulte **Guía de Monitoreo**.

Panel de Control Web

El **Panel de Control Web** proporciona un tablero en tiempo real para el monitoreo y gestión del UPF.

Características:

- **Vista de Sesiones**: Navegar por sesiones PFCP activas con IP de UE, TEID y conteos de reglas
- **Gestión de Reglas**: Ver y gestionar PDRs, FARs, QERs y URRs en todas las sesiones
- **Monitoreo de Búferes**: Rastrear paquetes almacenados en búfer y controlar el almacenamiento en búfer por FAR
- **Tablero de Estadísticas**: Estadísticas en tiempo real de paquetes, rutas, XDP y estadísticas de interfaces N3/N6
- **Monitoreo de Capacidad**: Uso de mapas eBPF con indicadores de capacidad codificados por colores
- **Vista de Configuración**: Mostrar configuración del UPF y direcciones del plano de datos
- **Visor de Registros**: Transmisión de registros en vivo para resolución de problemas

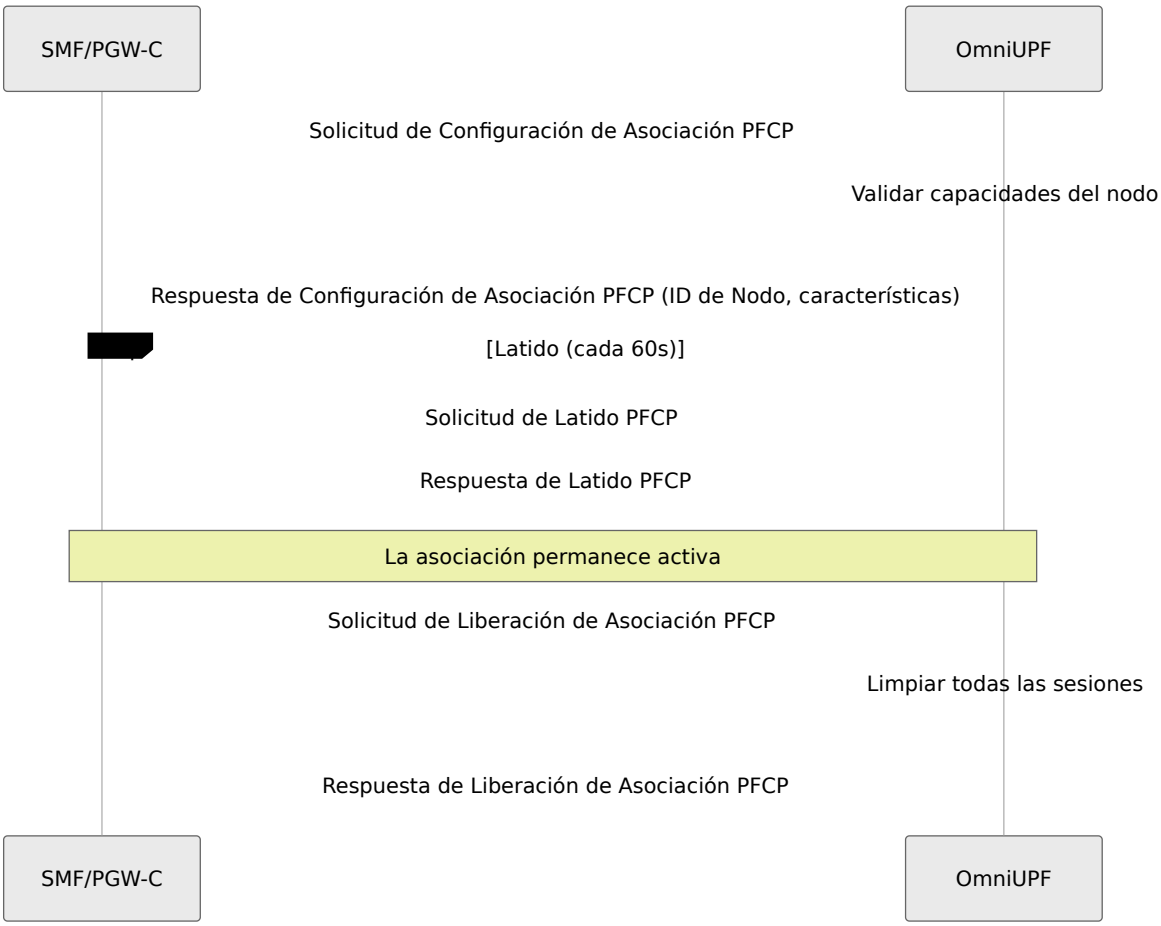
Para operaciones detalladas de la UI, consulte **Guía de Operaciones de UI Web**.

Protocolo PFCP e Integración con SMF

Asociación PFCP

Antes de que se puedan crear sesiones, el SMF debe establecer una asociación PFCP con el UPF.

Ciclo de Vida de Asociación:



Puntos Clave:

- Cada SMF establece una asociación con el UPF
- UPF rastrea la asociación por ID de Nodo (FQDN o dirección IP)
- Los mensajes de latido mantienen viva la asociación
- Todas las sesiones bajo una asociación se eliminan si se libera la asociación

Para ver asociaciones, consulte Vista de Sesiones.

Detección de Reinicio de SMF y Limpieza de Sesiones Huérfanas

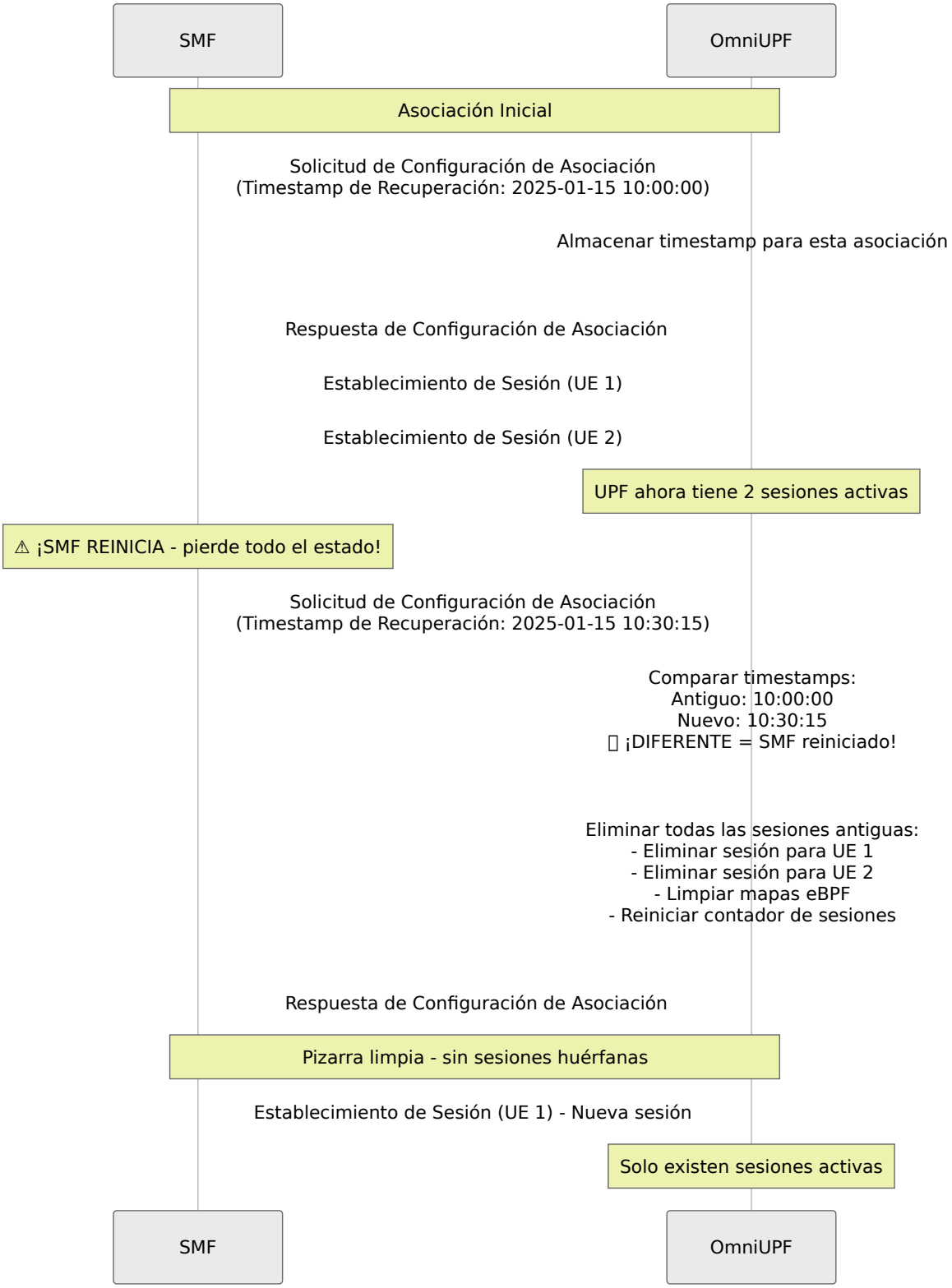
OmniUPF detecta automáticamente cuando un SMF se reinicia y limpia sesiones huérfanas según las especificaciones de 3GPP TS 29.244.

Cómo Funciona:

Cuando un SMF establece una asociación PFCP, proporciona un **Timestamp de Recuperación** que indica cuándo se inició. OmniUPF almacena este timestamp para cada asociación. Si el SMF se reinicia:

1. El SMF pierde todo el estado de sesión en memoria
2. El SMF restablece la asociación PFCP con el UPF
3. El SMF envía un **nuevo Timestamp de Recuperación** (diferente al anterior)
4. UPF detecta el cambio de timestamp = ¡SMF reiniciado!
5. UPF elimina automáticamente **todas las sesiones huérfanas** de la antigua instancia de SMF
6. El SMF crea nuevas sesiones para suscriptores activos

Flujo de Detección de Reinicio:



Ejemplo de Registro:

Cuando un SMF se reinicia, verás:

```
WARN: La asociación con NodeID: smf-1 y dirección: 192.168.1.10 ya
existe
WARN: El Timestamp de Recuperación del SMF cambió (antiguo: 2025-
01-15T10:00:00Z, nuevo: 2025-01-15T10:30:15Z) - SMF reiniciado,
eliminando 245 sesiones huérfanas
INFO: Eliminando sesión huérfana 2 (LocalSEID) debido a reinicio
de SMF
INFO: Eliminando sesión huérfana 3 (LocalSEID) debido a reinicio
de SMF
...
INFO: Eliminando sesión huérfana 246 (LocalSEID) debido a reinicio
de SMF
```

Notas Importantes:

1. **Aislamiento**: Solo se eliminan las sesiones del SMF reiniciado. Otras asociaciones de SMF y sus sesiones **no se ven afectadas**.
2. **Comparación de Tiempos**: Si el Tiempo de Recuperación es **idéntico**, las sesiones son **retenidas** (SMF reconectado sin reiniciar).
3. **Cumplimiento de 3GPP**: Este comportamiento está mandado por la sección 5.22.2 de 3GPP TS 29.244:

   > "Si el Tiempo de Recuperación de la función CP ha cambiado desde la última Configuración de Asociación, la función UP considerará que la función CP ha reiniciado y deberá eliminar todas las sesiones PFCP asociadas con esa función CP."

Para solucionar problemas de sesiones huérfanas, consulte la Guía de Solución de Problemas.

Manejo de Indicación de Error GTP-U

OmniUPF maneja mensajes de Indicación de Error GTP-U de pares descendentes (PGW-U, SGW-U, eNodeB, gNodeB) según las especificaciones de 3GPP TS 29.281.

¿Qué son las Indicaciones de Error?:

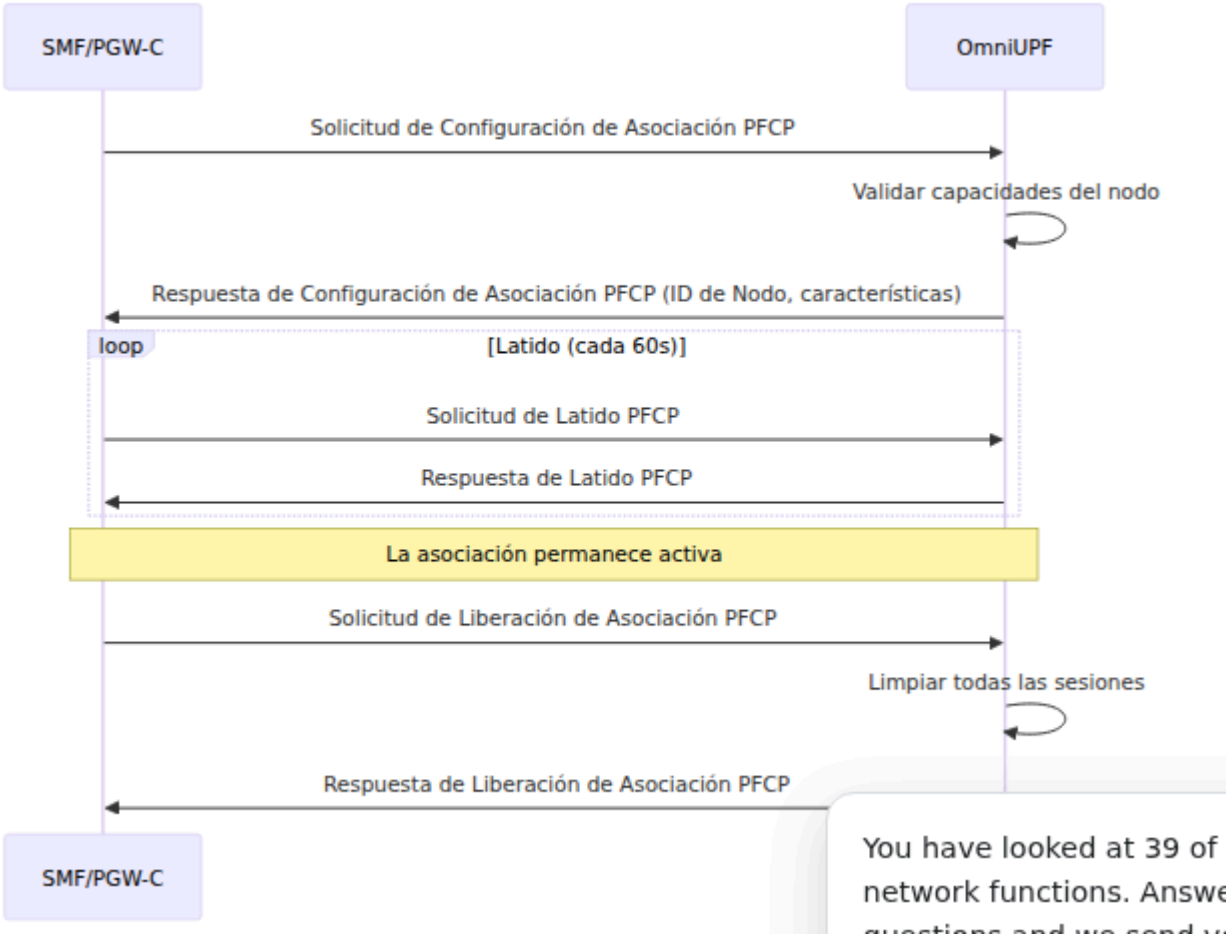
Cuando OmniUPF reenvía un paquete GTP-U a un par remoto (por ejemplo, PGW-U en una implementación SGW-U), el par puede enviar de vuelta una **Indicación de Error** si no reconoce el TEID (Identificador de Punto de Final de Túnel). Esto indica:

- El par remoto ha reiniciado y perdió el estado del túnel
- El túnel nunca se creó en el lado remoto (desajuste de configuración)
- El túnel ya fue eliminado en el lado remoto

Cómo Funciona:

1. **UPF reenvía paquete** → Envía paquete GTP-U con TEID X al par remoto (puerto 2152)
2. **El par remoto no reconoce TEID X** → Busca TEID en su tabla de túneles, no encontrado
3. **El par remoto envía Indicación de Error** → Mensaje GTP-U tipo 26 con IE que contiene TEID erróneo
4. **UPF recibe Indicación de Error** → Analiza el mensaje para extraer TEID X
5. **UPF encuentra sesiones afectadas** → Busca todas las sesiones para FARs que reenvían a TEID X
6. **UPF elimina sesiones** → Elimina sesiones de los mapas eBPF y del estado PFCP
7. **UPF actualiza métricas** → Incrementa contadores de Prometheus para monitoreo

Flujo de Indicación de Error:



Formato del Paquete (Sección 7.3.1 de 3GPP TS 29.281):

```
Indicación de Error GTP-U:
┌──────────────────────────────────────────────┐
│ Encabezado GTP-U (12 bytes)                  │
├──────────────────────────────────────────────┤
│ Versión, PT, Banderas      │ 0x32            │
│ Tipo de Mensaje            │ 26 (0x1A)       │
│ Longitud                   │ 9 bytes         │
│ TEID                       │ 0 (siempre)     │
│ Número de Secuencia        │ varía           │
│ Número N-PDU               │ 0               │
│ Siguiente Encabezado de Extensión │ 0        │
├──────────────────────────────────────────────┤
│ IE: Datos TEID I (5 bytes)                   │
├──────────────────────────────────────────────┤
│ Tipo                       │ 16 (0x10)       │
│ TEID erróneo               │ 4 bytes         │
└──────────────────────────────────────────────┘
```

Cuándo Esto Importa:

Escenario 1: Reinicio de PGW-U en Arquitectura GTP S5/S8

- SGW-U (OmniUPF) reenvía tráfico S5/S8 a PGW-U
- PGW-U reinicia y pierde todo el estado del túnel S5/S8
- SGW-U continúa reenviando a TEIDs antiguos
- PGW-U envía Indicaciones de Error
- SGW-U **deja de usar automáticamente túneles muertos**

Escenario 2: Reinicio de UPF Par en Arquitectura N9

- UPF-1 (OmniUPF) reenvía tráfico N9 a UPF-2
- UPF-2 reinicia
- UPF-1 recibe Indicaciones de Error
- UPF-1 limpia sesiones

Ejemplo de Registro:

Al recibir una Indicación de Error:

```
WARN: Recibida Indicación de Error GTP-U de 192.168.50.10:2152
para TEID 0x12345678 - el par remoto no reconoce este TEID
WARN: Sesión encontrada LocalSEID=42 con FAR GlobalId=1 reenviando
a TEID erróneo 0x12345678 desde el par 192.168.50.10
INFO: Eliminando sesión LocalSEID=42 debido a Indicación de Error
GTP-U para TEID 0x12345678 de 192.168.50.10
WARN: Eliminadas 1 sesión(es) debido a Indicación de Error GTP-U
para TEID 0x12345678 del par 192.168.50.10
```

Métricas de Prometheus:

Monitoree la actividad de Indicación de Error con granularidad por par y por nodo:

```
# Total de Indicaciones de Error recibidas de pares
upf_buffer_listener_error_indications_received_total{node_id="pgw-u-
1",peer_address="192.168.50.10"}

# Sesiones eliminadas debido a Indicaciones de Error
upf_buffer_listener_error_indication_sessions_deleted_total{node_id="
u-1",peer_address="192.168.50.10"}

# Indicaciones de Error enviadas (para TEIDs entrantes desconocidos)
upf_buffer_listener_error_indications_sent_total{node_id="enodeb-
1",peer_address="10.60.0.1"}
```

Etiquetas de Métricas:

- `node_id`: ID de Nodo PFCP de la asociación (o "desconocido" si no existe asociación)
- `peer_address`: Dirección IP del par remoto

Estas métricas ayudan a identificar pares problemáticos y rastrear patrones de Indicación de Error por nodo de plano de control.

Notas Importantes:

1. **Limpieza Automática**: No se necesita intervención del operador - las sesiones se eliminan automáticamente

2. **Coincidencia de TEID**: Solo se eliminan las sesiones con FARs que reenvían al TEID erróneo exacto

3. **Aislamiento por Par**: Las Indicaciones de Error de un par solo afectan las sesiones que reenvían a ese par

4. **Múltiples Sesiones**: Si múltiples sesiones reenvían al mismo TEID muerto, **todas son eliminadas**

5. **Complementario al Tiempo de Recuperación**:

    - Detección de Tiempo de Recuperación = proactivo (detecta reinicio durante la configuración de asociación)

- Manejo de Indicación de Error = reactivo (detecta túneles muertos cuando fluyen datos)

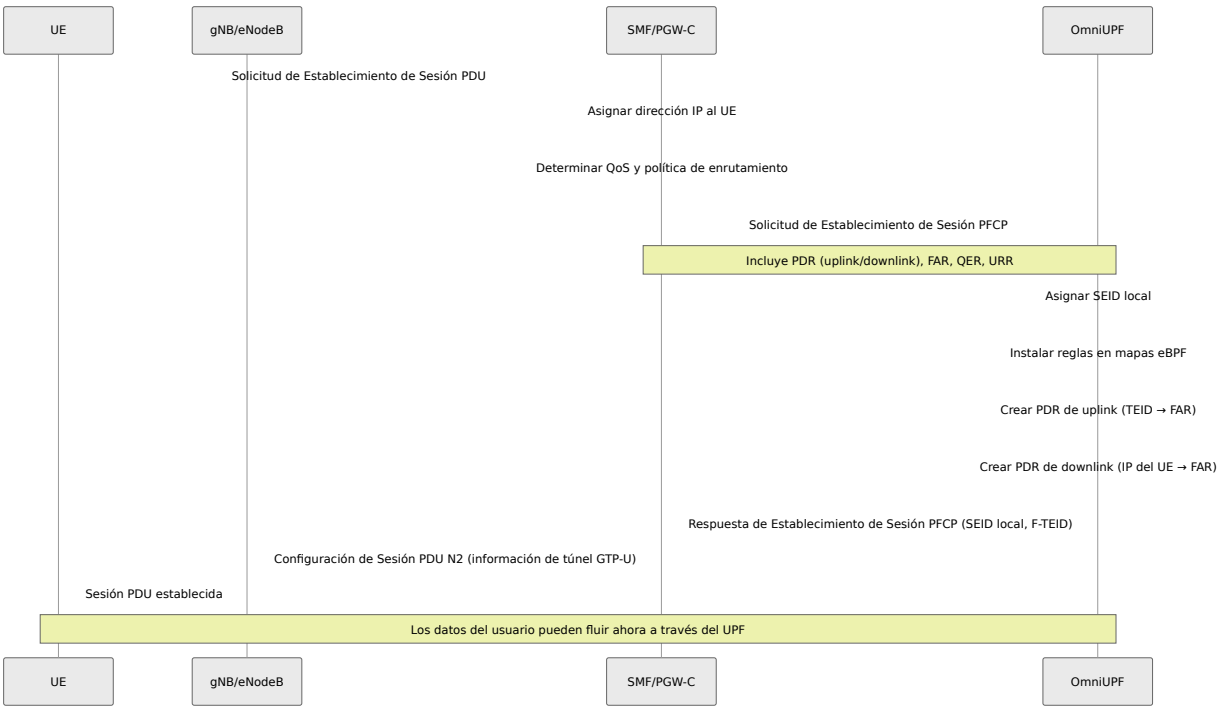
6. **Manejo de Paquetes Malformados**: Las Indicaciones de Error inválidas se registran e ignoran (no se eliminan sesiones)

Para solucionar problemas de Indicaciones de Error, consulte la Guía de Solución de Problemas.

Creación de Sesión PFCP

Cuando un UE establece una sesión PDU (5G) o contexto PDP (LTE), el SMF crea una sesión PFCP en el UPF.

Flujo de Establecimiento de Sesión:



Contenidos Típicos de la Sesión:

- **PDR de Uplink**: Coincidir en TEID N3, reenviar a través de FAR a N6
- **PDR de Downlink**: Coincidir en dirección IP del UE, reenviar a través de FAR a N3 con encapsulación GTP-U
- **FAR**: Parámetros de reenvío (creación de encabezado externo, instancia de red)

- **QER**: Límites de QoS (MBR, GBR) y marcado de paquetes (QFI)
- **URR**: Reporte de volumen para facturación (opcional)

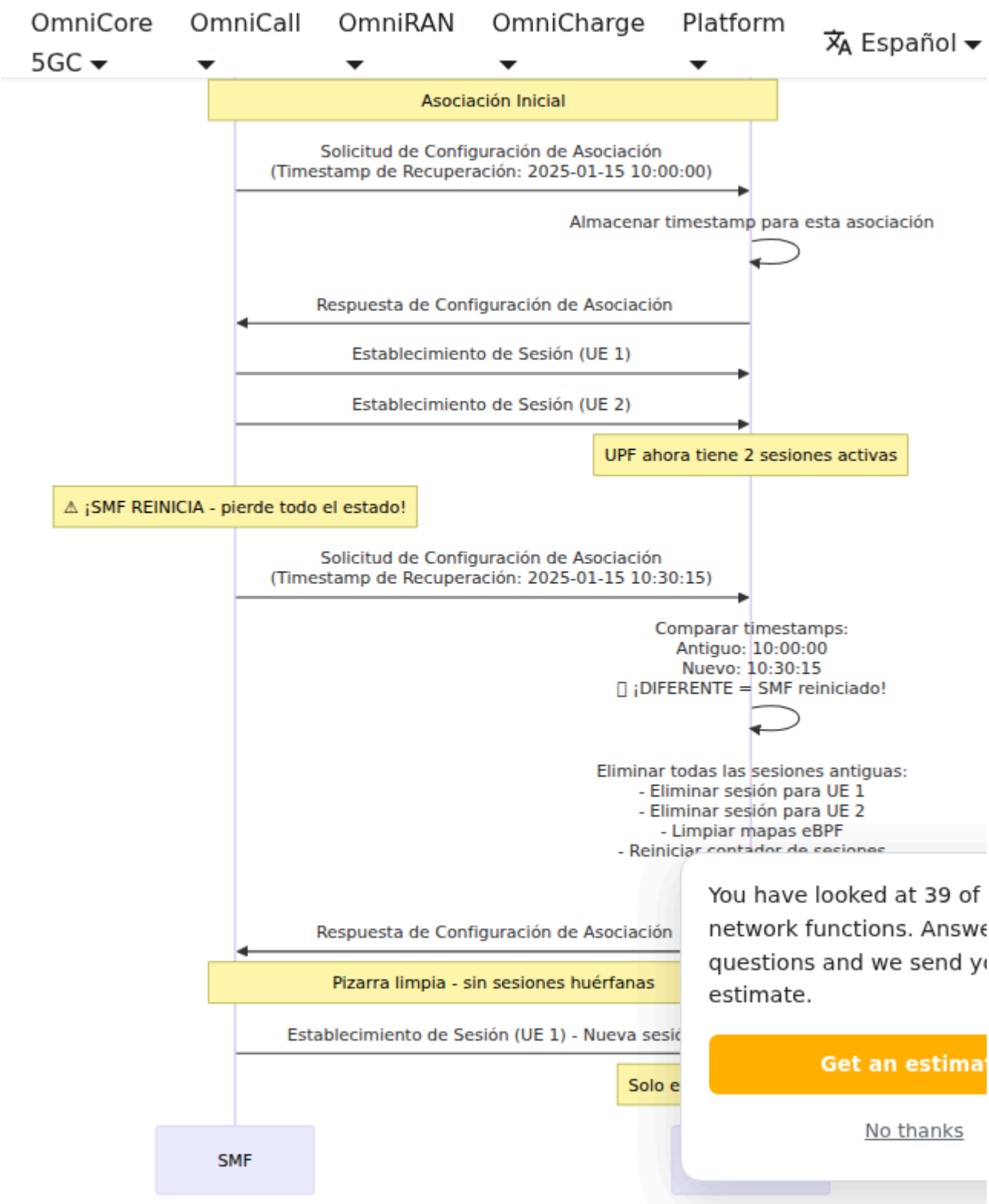
Modificación de Sesión PFCP

El SMF puede modificar sesiones para eventos de movilidad (cambio de mano), cambios de QoS o actualizaciones de servicio.

Escenarios Comunes de Modificación:

1. **Cambio de Mano (basado en N2)**
    - Actualizar FAR de uplink con nuevo punto final de túnel gNB (F-TEID)
    - Opcionalmente almacenar paquetes durante el cambio de ruta
    - Vaciar el búfer a la nueva ruta cuando esté listo
2. **Cambio de QoS**
    - Actualizar QER con nuevos valores MBR/GBR
    - Puede agregar/eliminar filtros SDF en PDR para QoS específico de la aplicación
3. **Actualización de Servicio**
    - Agregar nuevos PDRs para flujos de tráfico adicionales
    - Modificar FARs para cambios de enrutamiento

Flujo de Modificación de Sesión:

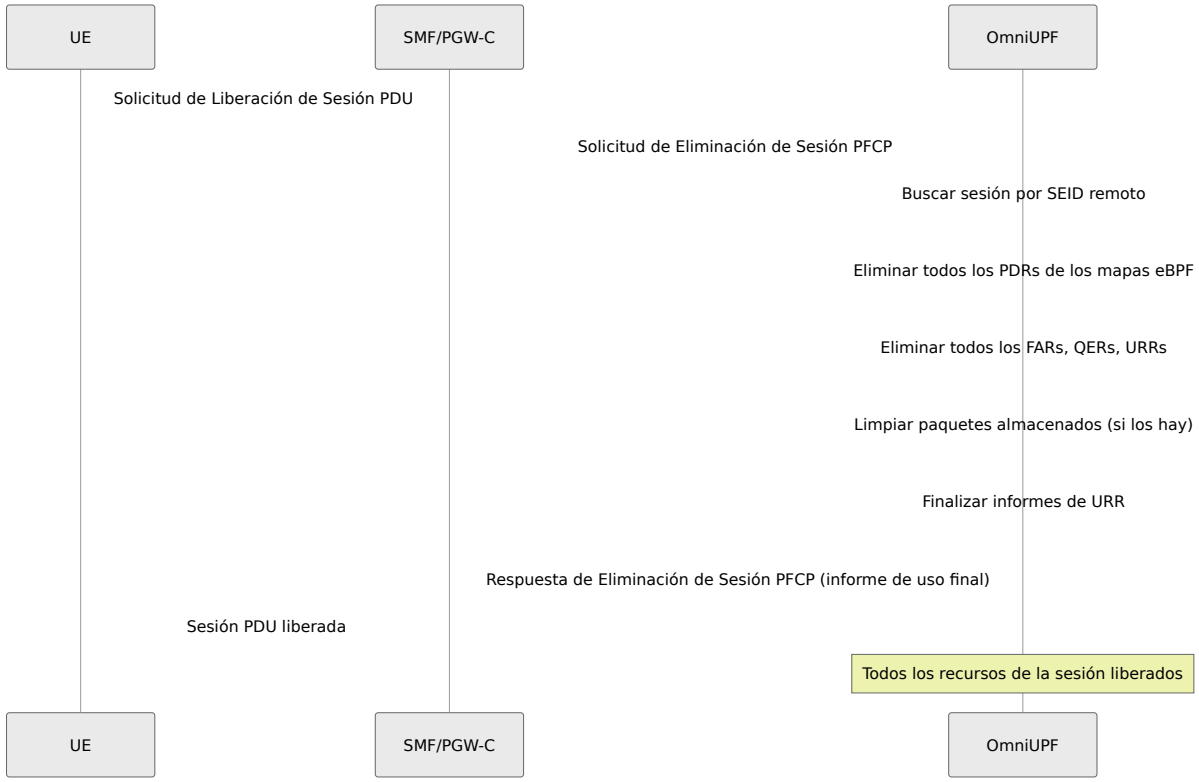


Para la gestión de reglas, consulte la Guía de Gestión de Reglas.

Eliminación de Sesión PFCP

Cuando se libera una sesión PDU, el SMF elimina la sesión PFCP en el UPF.

Flujo de Eliminación de Sesión:



Limpieza Realizada:

- Todos los PDRs eliminados (uplink y downlink)
- Todos los FARs, QERs, URRs eliminados
- Búferes de paquetes vaciados
- Informe de uso final enviado al SMF para facturación

Operaciones Comunes

OmniUPF proporciona capacidades operativas integrales a través de su panel de control basado en web y API REST. Esta sección cubre tareas operativas comunes y su significado.

Monitoreo de Sesiones

Entendiendo las Sesiones PFCP:

Las sesiones PFCP representan sesiones PDU activas de UE (5G) o contextos PDP (LTE). Cada sesión contiene:

- SEIDs locales y remotos (Identificadores de Punto de Final de Sesión)
- PDRs para clasificación de paquetes
- FARs para decisiones de reenvío
- QERs para aplicación de QoS (opcional)
- URRs para seguimiento de uso (opcional)

Operaciones Clave de Sesión:

- **Ver todas las sesiones** con direcciones IP de UE, TEIDs y conteos de reglas
- **Filtrar sesiones** por dirección IP o TEID
- **Inspeccionar detalles de la sesión** incluyendo configuraciones completas de PDR/FAR/QER/URR
- **Monitorear conteos de sesiones** por asociación PFCP

Para procedimientos detallados de sesión, consulte Vista de Sesiones.

Gestión de Reglas

Reglas de Detección de Paquetes (PDR):

Las PDR determinan qué paquetes coinciden con flujos de tráfico específicos. Los operadores pueden:

- **Ver PDRs de uplink** indexados por TEID de la interfaz N3
- **Ver PDRs de downlink** indexados por dirección IP del UE (IPv4 e IPv6)
- **Inspeccionar filtros SDF** para clasificación específica de la aplicación
- **Monitorear conteos de PDR** y uso de capacidad

Reglas de Acción de Reenvío (FAR):

Las FAR definen qué hacer con los paquetes coincidentes. Los operadores pueden:

- **Ver acciones de FAR** (REENVIAR, DESCARTAR, ALMACENAR, DUPLICAR, NOTIFICAR)

- **Inspeccionar parámetros de reenvío** (creación de encabezado externo, destino)
- **Monitorear estado de almacenamiento** por FAR
- **Alternar almacenamiento** para FARs específicos durante la solución de problemas

Reglas de Aplicación de QoS (QER):

Las QER aplican límites de ancho de banda y marcado de paquetes. Los operadores pueden:

- **Ver parámetros de QoS** (MBR, GBR, presupuesto de retraso de paquetes)
- **Monitorear QERs activos** por sesión
- **Inspeccionar marcas QFI** para flujos de QoS 5G

Reglas de Reporte de Uso (URR):

Las URRs rastrean volúmenes de datos para facturación. Los operadores pueden:

- **Ver contadores de volumen** (uplink, downlink, bytes totales)
- **Monitorear umbrales de uso** y desencadenadores de reporte
- **Inspeccionar URRs activos** en todas las sesiones

Para operaciones de reglas, consulte la Guía de Gestión de Reglas.

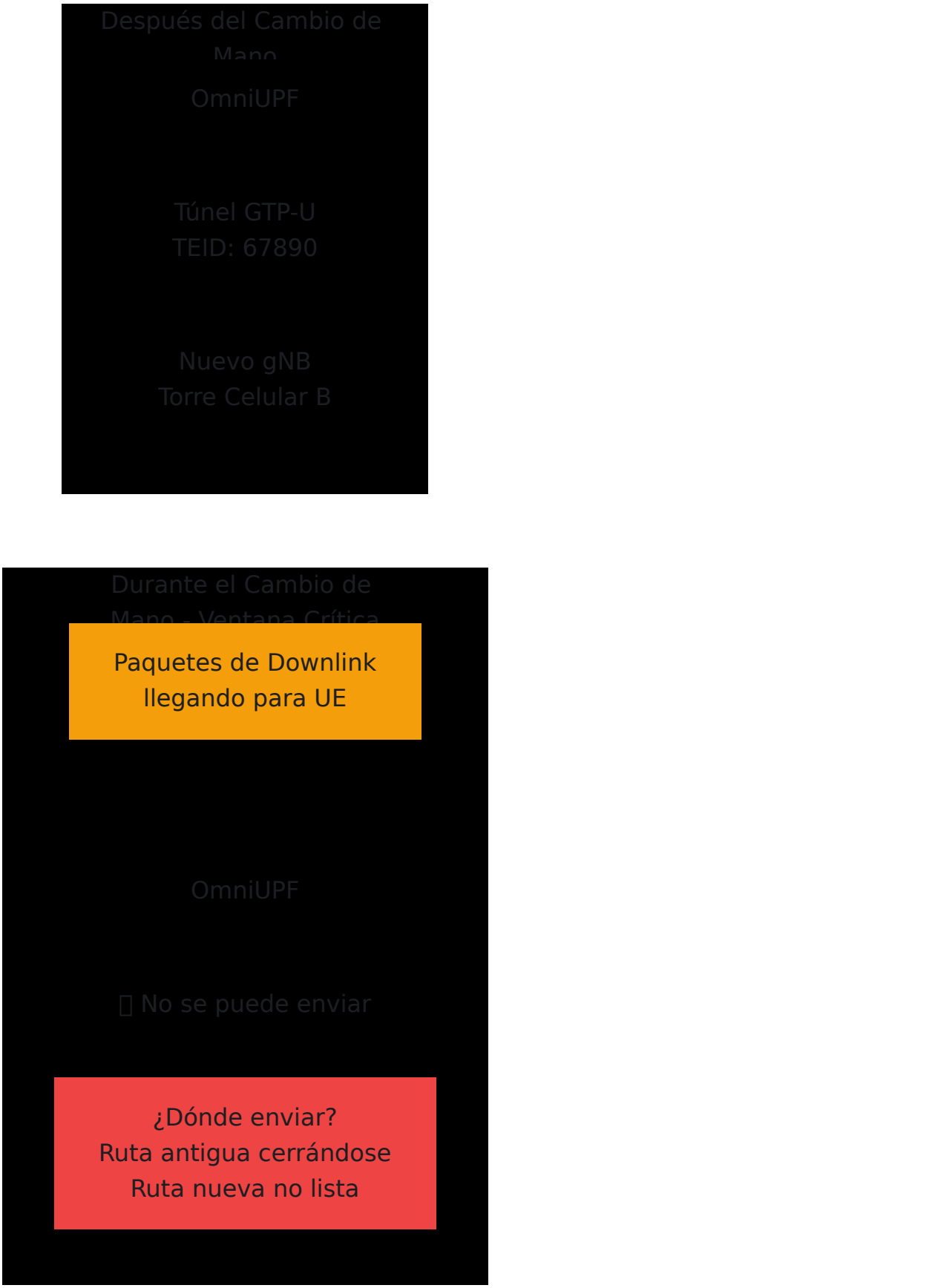
Almacenamiento de Paquetes

Por Qué el Almacenamiento es Crítico para UPF

El almacenamiento de paquetes es una de las funciones más importantes de un UPF porque previene la pérdida de paquetes durante eventos de movilidad y reconfiguraciones de sesión. Sin almacenamiento, los usuarios móviles experimentarían conexiones caídas, descargas interrumpidas y comunicaciones en tiempo real fallidas cada vez que se mueven entre torres de celular o cuando cambian las condiciones de la red.

El Problema: Pérdida de Paquetes Durante la Movilidad

En redes móviles, los usuarios están en constante movimiento. Cuando un dispositivo se mueve de una torre de celular a otra (cambio de mano), o cuando la red necesita reconfigurar la ruta de datos, hay una ventana crítica donde los paquetes están en vuelo pero la nueva ruta aún no está lista:


Después del Cambio de Mano
OmniUPF
Túnel GTP-U
TEID: 67890
Nuevo gNB
Torre Celular B
Durante el Cambio de Mano - Ventana Crítica
Paquetes de Downlink llegando para UE
OmniUPF
No se puede enviar
¿Dónde enviar?
Ruta antigua cerrándose
Ruta nueva no lista
Antes del Cambio de Mano



Sin almacenamiento: Los paquetes que llegan durante esta ventana crítica serían **descartados**, causando:

- **Conexiones TCP que se detienen** o se reinician (navegación web, descargas interrumpidas)
- **Llamadas de video que se congelan** o se caen (Zoom, Teams, llamadas de WhatsApp fallan)
- **Sesiones de juego que se desconectan** (juegos en línea, aplicaciones en tiempo real fallan)
- **Llamadas VoIP que tienen interrupciones** o se caen por completo (llamadas telefónicas interrumpidas)
- **Descargas que fallan** y necesitan reiniciarse

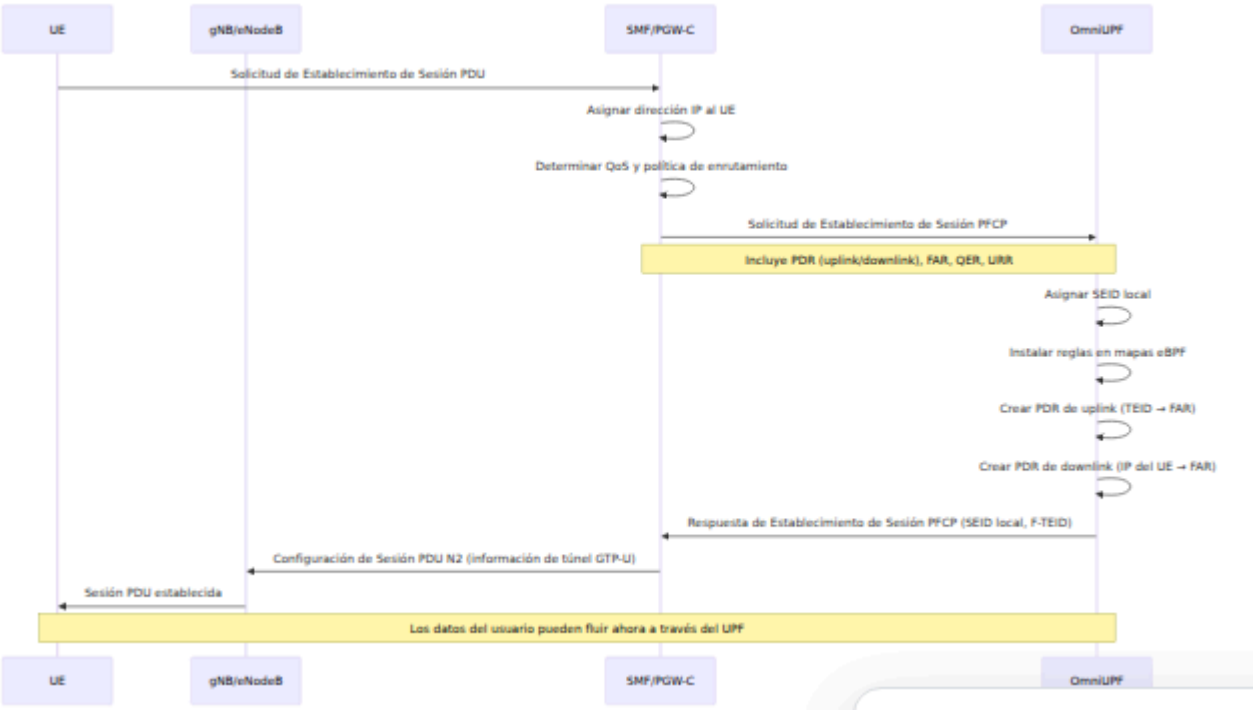
Con almacenamiento: OmniUPF retiene temporalmente los paquetes hasta que se establece la nueva ruta, luego los reenvía sin problemas. El usuario experimenta **cero interrupciones**.

Cuándo Ocurre el Almacenamiento

OmniUPF almacena paquetes en estos escenarios críticos:

1. Cambio de Mano Basado en N2 (5G) / Cambio de Mano Basado en X2 (4G)

Cuando un UE se mueve entre torres de celular:



Línea de Tiempo:

- **T+0ms**: Ruta antigua aún activa
- **T+10ms**: SMF le dice a UPF que almacene (ruta antigua cerrándose, nueva ruta no lista)
- **T+10-50ms**: **Ventana crítica de almacenamiento** - los paquetes llegan pero no se pueden reenviar
- **T+50ms**: Nueva ruta lista, SMF le dice a UPF que reenvíe
- **T+50ms+**: UPF vacía los paquetes almacenados a la nueva ruta, luego reenvía nuevos paquetes normalmente

Sin almacenamiento: ~40ms de paquetes (potencialmente miles) serían **perdidos**. **Con almacenamiento**: Cero pérdida de paquetes, cambio de mano sin problemas.

---

2. Modificación de Sesión (Cambio de QoS, Actualización de Ruta)

Cuando la red necesita cambiar los parámetros de la sesión:

- **Actualización/disminución de QoS**: El usuario se mueve de cobertura 4G a 5G (modo NSA)

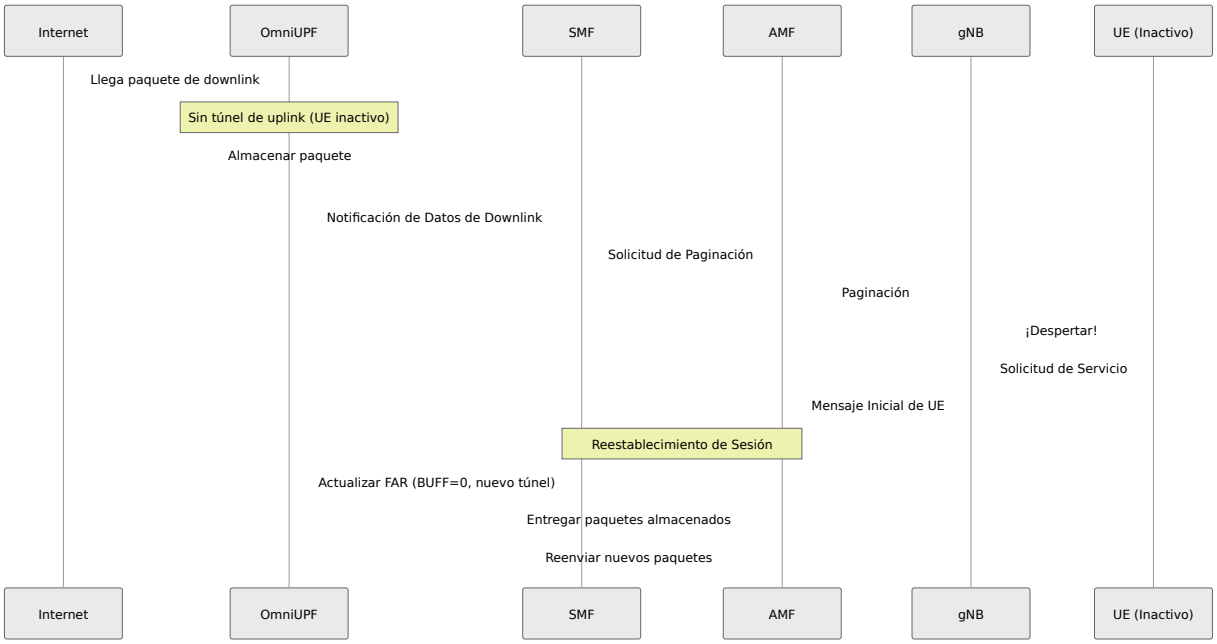
- **Cambio de política**: El usuario empresarial entra en el campus corporativo (cambios en la dirección del tráfico)
- **Optimización de red**: La red central redirige el tráfico a un UPF más cercano (actualización de ULCL)

Durante la modificación, el plano de control puede necesitar actualizar múltiples reglas de manera atómica. El almacenamiento asegura que los paquetes no se reenvíen con conjuntos de reglas parciales/inconsistentes.

---

3. Notificación de Datos de Downlink (Recuperación de Modo Inactivo)

Cuando un UE está en modo inactivo (pantalla apagada, ahorro de batería) y llegan datos de downlink:



Sin almacenamiento: El paquete inicial que activó la notificación sería **perdido**, requiriendo que el remitente lo retransmita (agrega latencia). **Con almacenamiento**: El paquete que despertó al UE se entrega inmediatamente cuando el UE se reconecta.

---

4. Cambio de Mano Inter-RAT (4G ↔ 5G)

Cuando un UE se mueve entre cobertura 4G y 5G:

- Cambios de arquitectura (eNodeB ↔ gNB)

- Cambios en los puntos finales de túnel (asignación diferente de TEID)
- El almacenamiento asegura una transición suave entre tipos de RAT

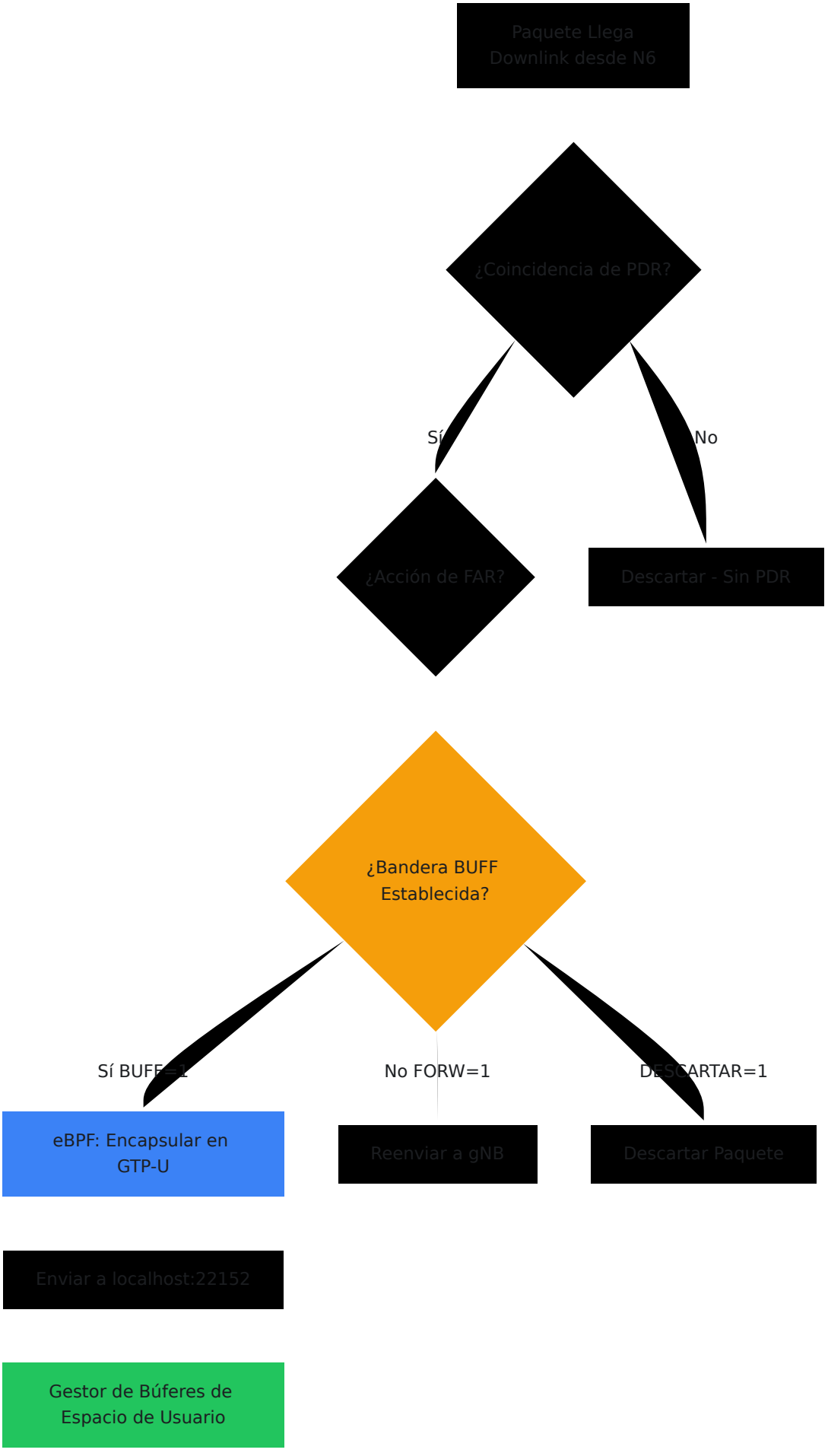
Cómo Funciona el Almacenamiento en OmniUPF

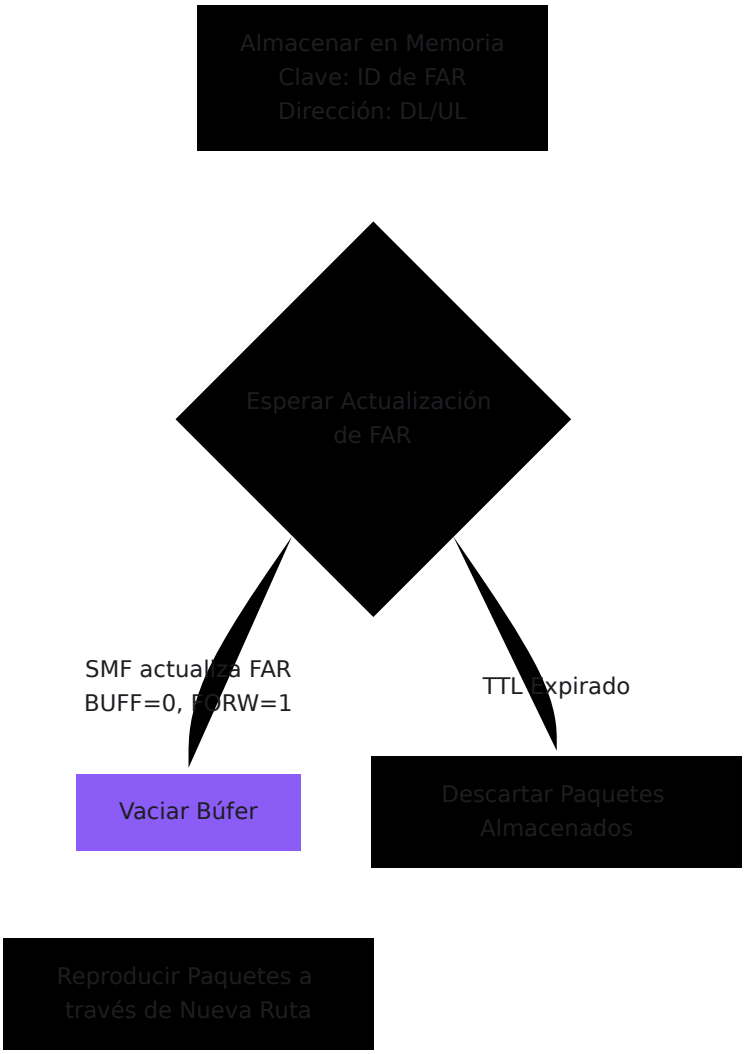
Mecanismo Técnico:

OmniUPF utiliza una **arquitectura de almacenamiento en dos etapas**:

1. **Etapa eBPF (Kernel)**: Detecta paquetes que requieren almacenamiento basándose en las banderas de acción de FAR
2. **Etapa de Espacio de Usuario**: Almacena y gestiona paquetes almacenados en memoria

Proceso de Almacenamiento:


Paquete Llega
Downlink desde N6
¿Coincidencia de PDR?
Sí
No
¿Acción de FAR?
Descartar - Sin PDR
¿Bandera BUFF
Establecida?
Sí BUFF=1
No FORW=1
DESCARTAR=1
eBPF: Encapsular en
GTP-U
Reenviar a gNB
Descartar Paquete
Enviar a localhost:22152
Gestor de Búferes de
Espacio de Usuario



Detalles Clave:

- **Puerto de Almacenamiento**: Puerto UDP 22152 (paquetes enviados desde eBPF al espacio de usuario)
- **Encapsulación**: Paquetes envueltos en GTP-U con ID de FAR como TEID
- **Almacenamiento**: Búferes en memoria por FAR con metadatos (marca de tiempo, dirección, tamaño del paquete)
- **Límites**:
  - Límite por FAR: 10,000 paquetes (por defecto)
  - Límite global: 100,000 paquetes en todos los FARs
  - TTL: 30 segundos (por defecto) - paquetes más antiguos que TTL son descartados
- **Limpieza**: Proceso en segundo plano elimina paquetes expirados cada 60 segundos

Ciclo de Vida del Búfer:

1. **Almacenamiento Habilitado**: SMF establece acción de FAR BUFF=1 (bit 2) a través de Modificación de Sesión PFCP
2. **Paquetes Almacenados**: eBPF detecta la bandera BUFF, encapsula paquetes, envía al puerto 22152
3. **Almacenamiento en Espacio de Usuario**: El gestor de búfer almacena paquetes con ID de FAR, marca de tiempo, dirección
4. **Almacenamiento Deshabilitado**: SMF establece acción de FAR FORW=1, BUFF=0 con nuevos parámetros de reenvío
5. **Vaciar Búfer**: El espacio de usuario reproduce paquetes almacenados utilizando nuevas reglas de FAR (nuevo punto final de túnel)
6. **Reanudar Normalidad**: Nuevos paquetes reenviados inmediatamente a través de la nueva ruta

---

Por Qué Esto Importa para la Experiencia del Usuario

Impacto en el Mundo Real:

Escenario	Sin Almacenamiento	Con Almacenamiento
Llamada de Video Durante el Cambio de Mano	La llamada se congela durante 1-2 segundos, puede caerse	Sin interrupciones, sin problemas
Descarga de Archivo en el Límite de la Celda	La descarga falla, debe reiniciarse	La descarga continúa sin interrupciones
Juego en Línea Mientras se Mueve	La conexión se cae, se expulsa del juego	Juego suave, sin desconexiones
Llamada VoIP en el Auto	La llamada se cae en cada cambio de mano	Cristalina, sin caídas
Video en Streaming en el Tren	El video se almacena en búfer, la calidad disminuye	Reproducción fluida
Hotspot Móvil para Laptop	La sesión SSH se cae, la llamada de video falla	Todas las conexiones mantenidas

Beneficios para el Operador de Red:

- **Tasa de Caída de Llamadas Reducida (CDR)**: KPI crítico para la calidad de la red
- **Mayor Satisfacción del Cliente**: Los usuarios no notan las transferencias
- **Menores Costos de Soporte**: Menos quejas sobre conexiones caídas
- **Ventaja Competitiva**: Marketing de "mejor red para cobertura"

Operaciones de Gestión de Buffers

Los operadores pueden monitorear y controlar el almacenamiento en búfer a través de la interfaz web y la API:

Monitoreo:

- **Ver paquetes en búfer** por ID de FAR (conteo, bytes, antigüedad)
- **Rastrear uso de búfer** contra límites (por FAR, global)
- **Alertar sobre desbordamiento de búfer** o duración excesiva de almacenamiento
- **Identificar búferes atascados** (paquetes en búfer > umbral TTL)

Operaciones de Control:

- **Vaciar búferes**: Activar manualmente la reproducción del búfer (solución de problemas)
- **Limpiar búferes**: Descartar paquetes en búfer (limpiar búferes atascados)
- **Ajustar TTL**: Cambiar el tiempo de expiración de paquetes
- **Modificar límites**: Aumentar la capacidad del búfer por FAR o global

Solución de Problemas:

- **Búfer no se vacía**: Verificar si el SMF envió una actualización de FAR para deshabilitar el almacenamiento en búfer
- **Desbordamiento de búfer**: Aumentar límites o investigar por qué la duración del almacenamiento es excesiva
- **Paquetes antiguos en el búfer**: El TTL puede ser demasiado alto, o la actualización de FAR se retrasó
- **Almacenamiento excesivo**: Puede indicar problemas de movilidad o problemas con el SMF

Para operaciones detalladas de búfer, consulte la Guía de Gestión de Buffers.

Configuración de Buffers

Configure el comportamiento del almacenamiento en búfer en `/etc/omniupf/runtime.exs`:

```
# Configuraciones de búfer
buffer_port = 22152                # Puerto UDP para paquetes en
búfer (predeterminado)
```

Recomendaciones:

- **Redes de alta movilidad** (autopistas, trenes): Aumentar `buffer_max_packets` a 20,000+
- **Áreas urbanas densas** (transferencias frecuentes): Disminuir `buffer_packet_ttl` a 15s
- **Aplicaciones de baja latencia**: Establecer `buffer_packet_ttl` a 10s para prevenir datos obsoletos
- **Redes IoT**: Disminuir límites (los dispositivos IoT generan menos tráfico durante la transferencia)

Para opciones de configuración completas, consulte la Guía de Configuración.

Estadísticas y Monitoreo

Estadísticas de Paquetes:

Métricas de procesamiento de paquetes en tiempo real que incluyen:

- **Paquetes RX**: Total recibido de todas las interfaces
- **Paquetes TX**: Total transmitido a todas las interfaces
- **Paquetes descartados**: Paquetes descartados debido a errores o políticas
- **Paquetes GTP-U**: Conteos de paquetes en túneles

Estadísticas de Rutas:

Métricas de reenvío por ruta:

- **Acercamientos de ruta**: Paquetes coincidentes con cada ruta
- **Conteos de reenvío**: Éxito/fallo por destino
- **Contadores de errores**: TEIDs inválidos, IPs de UE desconocidas

Estadísticas de XDP:

Métricas de rendimiento de eXpress Data Path:

- **XDP procesados**: Paquetes manejados en la capa XDP
- **XDP pasados**: Paquetes enviados a la pila de red
- **XDP descartados**: Paquetes descartados en la capa XDP
- **XDP abortados**: Errores de procesamiento

Estadísticas de Interfaz N3/N6:

Contadores de tráfico por interfaz:

- **N3 RX/TX**: Tráfico hacia/desde RAN (gNB/eNodeB)
- **N6 RX/TX**: Tráfico hacia/desde la red de datos
- **Conteos totales de paquetes**: Estadísticas agregadas de la interfaz

Para detalles de monitoreo, consulte la Guía de Monitoreo.

Gestión de Capacidad

Monitoreo de Capacidad del Mapa eBPF:

El rendimiento del UPF depende de la capacidad del mapa eBPF. Los operadores pueden:

- **Monitorear el uso del mapa** con indicadores de porcentaje en tiempo real
- **Ver límites de capacidad** para cada mapa eBPF
- **Alertas codificadas por colores**:
  - Verde (<50%): Normal
  - Amarillo (50-70%): Precaución
  - Ámbar (70-90%): Advertencia
  - Rojo (>90%): Crítico

Mapas Críticos a Monitorear:

- `uplink_pdr_map`: Clasificación de tráfico de enlace ascendente
- `downlink_pdr_map`: Clasificación de tráfico IPv4 de enlace descendente
- `far_map`: Reglas de reenvío
- `qer_map`: Reglas de QoS
- `urr_map`: Seguimiento de uso

Planificación de Capacidad:

- Cada PDR consume una entrada de mapa (tamaño de clave + tamaño de valor)
- La capacidad del mapa se configura al inicio del UPF (límite de memoria del kernel)
- Exceder la capacidad causa fallos en el establecimiento de sesiones

Para monitoreo de capacidad, consulte Gestión de Capacidad.

Gestión de Configuración

Configuración del UPF:

Ver y verificar parámetros operativos del UPF:

- **Interfaz N3**: Dirección IP para conectividad RAN (GTP-U)
- **Interfaz N6**: Dirección IP para conectividad de red de datos
- **Interfaz N9**: Dirección IP para comunicación entre UPFs (opcional)
- **Interfaz PFCP**: Dirección IP para conectividad SMF
- **Puerto API**: Puerto de escucha de la API REST
- **Punto de Métricas**: Puerto de métricas de Prometheus

Configuración del Dataplane:

Parámetros activos de la ruta de datos eBPF:

- **Dirección N3 activa**: Vinculación de la interfaz N3 en tiempo de ejecución
- **Dirección N9 activa**: Vinculación de la interfaz N9 en tiempo de ejecución (si está habilitada)

Para ver la configuración, consulte Vista de Configuración.

Solución de Problemas

Esta sección cubre problemas operativos comunes y sus estrategias de resolución.

Fallos en el Establecimiento de Sesiones

Síntomas: Las sesiones PFCP no se crean, el UE no puede establecer conectividad de datos

Causas Raíz Comunes:

1. **Asociación PFCP No Establecida**
    - Verifique que el SMF pueda alcanzar la interfaz PFCP del UPF (puerto 8805)
    - Verifique el estado de la asociación PFCP en la vista de Sesiones
    - Verifique que la configuración del ID de Nodo coincida entre el SMF y el UPF
2. **Capacidad del Mapa eBPF Agotada**
    - Verifique la vista de Capacidad para el uso del mapa rojo (>90%)
    - Aumente los tamaños de los mapas eBPF en la configuración del UPF
    - Elimine sesiones obsoletas si el mapa está lleno
3. **Configuración Inválida de PDR/FAR**
    - Verifique que la dirección IP del UE sea única y válida
    - Verifique que la asignación de TEID no tenga conflictos
    - Asegúrese de que el FAR haga referencia a instancias de red válidas
4. **Problemas de Configuración de Interfaz**
    - Verifique que la IP de la interfaz N3 sea accesible desde el gNB

- Verifique las tablas de enrutamiento para la conectividad N6 a la red de datos
- Confirme que el tráfico GTP-U no esté bloqueado por el firewall

Para una solución de problemas detallada, consulte la Guía de Solución de Problemas.

Pérdida de Paquetes o Problemas de Reenvío

Síntomas: El UE tiene conectividad pero experimenta pérdida de paquetes o no hay flujo de tráfico

Causas Raíz Comunes:

1. **Configuración Incorrecta de PDR**
   - Verifique que el TEID del PDR de enlace ascendente coincida con el TEID asignado por el gNB
   - Verifique que la IP del PDR de enlace descendente del UE coincida con la IP asignada
   - Inspeccione los filtros SDF por reglas excesivamente restrictivas
2. **Problemas de Acción FAR**
   - Verifique que la acción FAR sea REENVIAR (no DESCARTAR o ALMACENAR)
   - Verifique los parámetros de creación de encabezados externos para GTP-U
   - Asegúrese de que el punto final de destino sea correcto
3. **Límites de QoS Excedidos**
   - Verifique la configuración de MBR (Tasa de Bits Máxima) de QER
   - Verifique la asignación de GBR (Tasa de Bits Garantizada)
   - Monitoree la pérdida de paquetes debido a limitación de tasa
4. **Problemas de MTU de Interfaz**

- Verifique que el overhead de GTP-U (40-50 bytes) no cause fragmentación
- Verifique la configuración de MTU de las interfaces N3/N6
- Monitoree los mensajes ICMP que indican necesidad de fragmentación

---

Problemas Relacionados con el Buffer

Síntomas: Paquetes almacenados en búfer indefinidamente, desbordamiento de búfer

Causas Raíz Comunes:

1. **Almacenamiento en Búfer No Deshabilitado Después de la Transferencia**
   - Verifique la bandera de almacenamiento en búfer de FAR (bit 2)
   - Verifique que el SMF envió la Modificación de Sesión para deshabilitar el almacenamiento en búfer
   - Desactive manualmente el almacenamiento en búfer a través del panel de control si está atascado
2. **Expiración del TTL del Búfer**
   - Verifique la antigüedad del paquete en la vista de búfer
   - Verifique la configuración del TTL del búfer (el predeterminado puede ser demasiado largo)
   - Limpie los búferes expirados manualmente
3. **Capacidad del Búfer Agotada**
   - Monitoree el uso total del búfer y los límites por FAR
   - Verifique si hay reglas mal configuradas que causen almacenamiento excesivo
   - Ajuste los límites de búfer max_per_far y max_total

Para la solución de problemas de búfer, consulte Operaciones de Búfer.

Anomalías en las Estadísticas

Síntomas: Contadores de paquetes inesperados, estadísticas faltantes

Causas Raíz Comunes:

1. **Desbordamiento de Contador**
    - Los mapas eBPF utilizan contadores de 64 bits (no deberían desbordarse)
    - Verifique eventos de reinicio de contadores en los registros
    - Verifique que el informe de URR esté funcionando
2. **Estadísticas de Ruta No Actualizadas**
    - Verifique que el programa eBPF esté adjunto a las interfaces
    - Verifique que la versión del kernel soporte las características eBPF requeridas
    - Revise las estadísticas de XDP para errores de procesamiento
3. **Desajuste de Estadísticas de Interfaz**
    - Compare las estadísticas N3/N6 con los contadores de interfaz del kernel
    - Verifique si hay tráfico que elude eBPF (por ejemplo, enrutamiento local)
    - Verifique que todo el tráfico fluya a través de los ganchos de XDP

Degradación del Rendimiento

Síntomas: Alta latencia, bajo rendimiento, saturación de CPU

Diagnóstico:

1. **Monitorear Estadísticas de XDP**: Verifique si hay descartes o abortos de XDP
2. **Verificar Tiempo de Acceso al Mapa eBPF**: Las búsquedas hash deben ser sub-microsegundo

3. **Revisar Utilización de CPU**: eBPF debe distribuirse entre núcleos
4. **Analizar Interfaz de Red**: Verifique que el NIC soporte la descarga de XDP

Consideraciones de Escalabilidad:

- **Rendimiento de XDP**: 10M+ paquetes por segundo por núcleo
- **Capacidad de PDR**: Millones de PDRs limitados solo por la memoria del kernel
- **Conteo de Sesiones**: Miles de sesiones concurrentes por instancia de UPF
- **Rendimiento**: Rendimiento de múltiples gigabits con la descarga adecuada del NIC

Para la optimización del rendimiento, consulte la Guía de Arquitectura.

Documentación Adicional

Guías de Operaciones Específicas por Componente

Para operaciones detalladas y solución de problemas para cada componente del UPF:

Guía de Configuración

Referencia completa de configuración que incluye:

- Parámetros de configuración (YAML, variables de entorno, CLI)
- Modos de operación (UPF/PGW-U/SGW-U)
- Descripción general de modos de adjunto de XDP
- Compatibilidad con hipervisores (Proxmox, VMware, KVM, Hyper-V, VirtualBox)
- Compatibilidad de NIC y soporte de controladores de XDP
- Ejemplos de configuración para diferentes escenarios
- Dimensionamiento de mapas y planificación de capacidad

Guía de Modos XDP

Configuración y optimización detalladas de XDP que incluyen:

- Modos de adjunto de XDP explicados (genérico/nativo/descarga)
- Comparación de rendimiento y benchmarks
- Configuración nativa de XDP en Proxmox VE paso a paso
- Configuración de múltiples colas para un rendimiento óptimo
- Configuración de XDP en VMware ESXi, KVM y Hyper-V
- Verificación y solución de problemas de XDP
- Selección de hardware para el rendimiento de XDP

Guía de Arquitectura

Profundización técnica que incluye:

- Fundación de tecnología eBPF y ciclo de vida del programa
- Pipeline de procesamiento de paquetes XDP con llamadas finales
- Implementación del protocolo PFCP
- Arquitectura de almacenamiento en búfer (encapsulación GTP-U al puerto 22152)
- Limitación de tasa de ventana deslizante de QoS (ventana de 5ms)
- Características de rendimiento (latencia de 3.5µs, 10 Mpps/núcleo)

Guía de Gestión de Reglas

Referencia de reglas PFCP que incluye:

- Reglas de Detección de Paquetes (PDR) - Clasificación de tráfico
- Reglas de Acción de Reenvío (FAR) - Decisiones de enrutamiento con banderas de acción
- Reglas de Aplicación de QoS (QER) - Gestión de ancho de banda (MBR/GBR)
- Reglas de Informe de Uso (URR) - Seguimiento y reporte de volumen
- Diagramas de flujo de paquetes de enlace ascendente y descendente
- Lógica de procesamiento de reglas y precedencia

Guía de Monitoreo

Estadísticas y gestión de capacidad que incluyen:

- Estadísticas de interfaz N3/N6 y distribución de tráfico
- Estadísticas de procesamiento de XDP (pasar/descartar/redirigir/abortar)
- Monitoreo de capacidad del mapa eBPF con zonas codificadas por colores
- Métricas de rendimiento (tasa de paquetes, rendimiento, tasa de descarte)
- Fórmulas de planificación de capacidad y estimación de sesiones
- Umbrales de alerta y mejores prácticas

Guía de Operaciones de Interfaz Web

Uso del panel de control que incluye:

- Descripción general del panel y navegación
- Monitoreo de sesiones (estados saludables/no saludables)
- Inspección de reglas (detalles de PDR, FAR, QER, URR)
- Monitoreo de búfer y estado de almacenamiento de paquetes
- Panel de estadísticas en tiempo real
- Visualización de capacidad del mapa eBPF
- Visualización de configuración

Documentación de API

Referencia completa de la API REST que incluye:

- Documentación interactiva OpenAPI/Swagger
- Paginación de API (basada en páginas y basada en desplazamiento)
- Puntos finales de sesiones y asociaciones PFCP
- Reglas de Detección de Paquetes (PDR) - IPv4 e IPv6
- Reglas de Acción de Reenvío (FAR)
- Reglas de Aplicación de QoS (QER)
- Reglas de Informe de Uso (URR)
- Gestión de búfer de paquetes
- Puntos finales de estadísticas y monitoreo
- Gestión de rutas e integración FRR
- Información del mapa eBPF

- Gestión de configuración
- Directrices de autenticación y seguridad
- Flujos de trabajo y ejemplos comunes de API

Referencia de Métricas

Documentación de métricas de Prometheus que incluye:

- Métricas de mensajes PFCP (contadores, latencia, errores por par)
- Métricas de acción de XDP (veredictos del dataplane)
- Métricas de paquetes (contadores a nivel de protocolo con etiquetas de tipo_paquete)
- Métricas de sesión y asociación PFCP (por nodo de plano de control)
- Métricas de URR (volumen de tráfico por par PFCP)
- Métricas de almacenamiento en búfer de paquetes (estado de búfer, capacidad, rendimiento)
- Métricas de notificación de Informe de Datos de Enlace Descendente (seguimiento DLDR)
- Métricas de capacidad del mapa eBPF (utilización de recursos)
- Ejemplos de configuración de Prometheus
- Recomendaciones de panel de Grafana

Referencia de Códigos de Causa PFCP

Documentación de códigos de error PFCP que incluye:

- Definiciones de códigos de causa y cumplimiento de 3GPP (TS 129.244)
- Cuándo ocurre cada código de causa (éxito, errores del cliente, errores del servidor)
- Escenarios de fallo comunes con resoluciones
- Solución de problemas con métricas de Prometheus
- Fallos en la configuración de asociación y ciclo de vida de sesiones
- Pasos de depuración para altas tasas de rechazo
- Recomendaciones de alerta para códigos de causa

Guía de Gestión de Rutas de UE

Integración de enrutamiento FRR que incluye:

- Descripción general y arquitectura de FRR (Free Range Routing)
- Ciclo de vida de sincronización de rutas de UE
- Sincronización automática de rutas al demonio de enrutamiento
- Anuncio de rutas a través de OSPF y BGP
- Monitoreo de vecinos OSPF
- Verificación de base de datos LSA externa de OSPF
- Gestión de sesiones de pares BGP
- Interfaz de monitoreo de rutas de la interfaz web
- Operaciones de sincronización de rutas manuales
- Diagramas de Mermaid para flujo de rutas y arquitectura

Guía de IPv6 / Doble Pila

Operación de IPv6 en el plano de usuario para sesiones PDN IPv6 e IPv4v6:

- Requisitos previos del kernel (habilitar IPv6 y reenvío)
- Configuración del grupo de direcciones IPv6 del UE
- Anuncio OSPFv3 de rutas de host `/128` del UE
- Comportamiento del plano de datos de enlace descendente/enlace ascendente de IPv6
- Solución de problemas de reenvío de IPv6 y anuncio de rutas

Guía de Solución de Problemas

Diagnóstico integral de problemas que incluye:

- Lista de verificación de diagnóstico rápido y herramientas
- Problemas de instalación y configuración
- Fallos en asociaciones PFCP
- Problemas de procesamiento de paquetes
- Errores de XDP y eBPF
- Degradación del rendimiento
- Problemas específicos de hipervisores (Proxmox, VMware, VirtualBox)
- Problemas de NIC y controladores

- Procedimientos de resolución paso a paso

Documentación por Caso de Uso

Instalación y Configuración de OmniUPF

1. Comience con esta guía para una visión general
2. Guía de Configuración para parámetros de configuración
3. Guía de Interfaz Web para acceder al panel de control

Despliegue en Proxmox

1. Guía de Modos XDP - Configuración Nativa de XDP en Proxmox - **Comience aquí para rendimiento**
2. Guía de Configuración - Compatibilidad con Hipervisores
3. Guía de Configuración - Configuración SR-IOV en Proxmox
4. Solución de Problemas - Problemas en Proxmox

Optimización del Rendimiento

1. Guía de Modos XDP - **Habilite XDP nativo para un aumento de rendimiento de 5-10x**
2. Guía de Arquitectura - Optimización del Rendimiento
3. Guía de Configuración - Modos XDP
4. Guía de Monitoreo - Métricas de Rendimiento
5. Solución de Problemas - Problemas de Rendimiento

Comprensión del Procesamiento de Paquetes

1. Guía de Arquitectura - Pipeline de Procesamiento de Paquetes
2. Guía de Gestión de Reglas
3. Guía de Monitoreo - Estadísticas

Planificación de Capacidad

1. Guía de Configuración - Dimensionamiento de Mapas
2. Guía de Monitoreo - Planificación de Capacidad

3. Guía de Monitoreo - Estimación de Capacidad de Sesiones

Gestión de Rutas de UE e Integración FRR

1. Guía de Gestión de Rutas de UE - Guía completa de integración de enrutamiento
2. Documentación de API - Gestión de Rutas - Puntos finales de API de rutas
3. Guía de Interfaz Web - Operaciones de la página de rutas
4. Gestión de Rutas de UE - Verificación de FRR - Verificación de LSA de OSPF

Uso de la API REST

1. Documentación de API - Referencia completa de la API
2. Documentación de API - Swagger UI - Explorador de API interactivo
3. Documentación de API - Características de la API - Ejemplos de uso de la API
4. Guía de Interfaz Web - Ejemplo de cliente API como interfaz web

Solución de Problemas

1. Guía de Solución de Problemas - Comience aquí
2. Guía de Monitoreo - Verifique estadísticas y capacidad
3. Guía de Interfaz Web - Use diagnósticos del panel de control

---

Referencia Rápida

Puntos Finales Comunes de API

OmniUPF proporciona una API REST para monitoreo y gestión:

```
# Estado y salud
GET http://localhost:8080/api/v1/upf_status

# Asociaciones PFCP
GET http://localhost:8080/api/v1/upf_pipeline

# Sesiones
GET http://localhost:8080/api/v1/sessions

# Estadísticas
GET http://localhost:8080/api/v1/packet_stats
GET http://localhost:8080/api/v1/xdp_stats

# Monitoreo de capacidad
GET http://localhost:8080/api/v1/map_info

# Estadísticas de búfer
GET http://localhost:8080/api/v1/upf_buffer_info
```

Para documentación completa de la API, acceda a la interfaz Swagger en `http://<upf-ip>:8080/swagger/index.html`

Parámetros de Configuración Esenciales

```
# /etc/omniupf/runtime.exs
xdp_interfaces = "eth0"              # Interfaces para tráfico
N3/N6/N9
xdp_attach_mode = "native"           # "generic" | "native" |
"offload"
n3_address = "10.100.50.233"         # IP de la interfaz N3
pfcp_address = "10.100.50.241"       # Dirección de escucha PFCP
pfcp_port = 8805                     # Puerto PFCP
node_id = "10.100.50.241"            # ID de Nodo PFCP

# Capacidad
max_sessions = 100_000               # Máximo de sesiones
concurrentes

# API
api_port = 8080                      # Puerto de la API REST
```

Umbrales de Monitoreo Importantes

- **Capacidad del Mapa eBPF < 70%**: Operación normal
- **Capacidad del Mapa eBPF 70-90%**: Planificar aumento de capacidad dentro de 1 semana
- **Capacidad del Mapa eBPF > 90%**: Crítico - se requiere acción inmediata
- **Tasa de Pérdida de Paquetes < 0.1%**: Excelente
- **Tasa de Pérdida de Paquetes 0.1-1%**: Buena - problemas menores
- **Tasa de Pérdida de Paquetes > 5%**: Crítico - investigar de inmediato
- **XDP Abortado > 0**: Problema crítico con el programa eBPF

Referencia de Normas 3GPP

OmniUPF implementa las siguientes especificaciones 3GPP:

Especificación	Título	Relevancia
TS 23.501	Arquitectura del sistema para el Sistema 5G (5GS)	Arquitectura y interfaces del UPF 5G
TS 23.401	Mejoras del Servicio de Paquetes Generales (GPRS) para acceso E-UTRAN	Arquitectura del UPF LTE (PGW-U)
TS 29.244	Interfaz entre los nodos de plano de control y plano de usuario (PFCP)	Protocolo PFCP N4
TS 29.281	Protocolo de Túnel de Paquetes Generales (GPRS) en el Plano de Usuario (GTPv1-U)	Encapsulación GTP-U
TS 23.503	Marco de control de políticas y cobro para el Sistema 5G (5GS)	QoS y cobro
TS 29.212	Control de Políticas y Cobro (PCC)	Aplicación de QoS

Glosario

Términos de Arquitectura 5G

- **3GPP**: Proyecto de Asociación de Tercera Generación - Organismo de estándares para telecomunicaciones móviles
- **AMF**: Función de Gestión de Acceso y Movilidad - Elemento de red central 5G para control de acceso
- **CHF**: Función de Cobro - Sistema de cobro 5G
- **DN**: Red de Datos - Red externa (Internet, IMS, empresa)
- **eNodeB**: Nodo Evolved B - Estación base LTE

- **F-TEID**: Identificador de Punto de Túnel Totalmente Calificado - ID de túnel GTP-U con dirección IP
- **gNB**: Nodo de Nueva Generación - Estación base 5G
- **GTP-U**: Protocolo de Túnel de Paquetes GPRS en el Plano de Usuario - Protocolo de túnel para datos de usuario
- **MBR**: Tasa de Bits Máxima - Parámetro de QoS para ancho de banda máximo permitido
- **GBR**: Tasa de Bits Garantizada - Parámetro de QoS para ancho de banda mínimo garantizado
- **N3**: Interfaz entre RAN y UPF (tráfico de plano de usuario)
- **N4**: Interfaz entre SMF y UPF (control PFCP)
- **N6**: Interfaz entre UPF y Red de Datos (tráfico de plano de usuario)
- **N9**: Interfaz entre dos UPFs (tráfico de plano de usuario inter-UPF)
- **PCF**: Función de Control de Políticas - Servidor de políticas 5G
- **PDU**: Unidad de Datos de Protocolo - Sesión de datos en 5G
- **PGW-C**: Plano de Control de la Puerta de Acceso PDN - Equivalente de plano de control LTE al SMF
- **PGW-U**: Plano de Usuario de la Puerta de Acceso PDN - Plano de usuario LTE (equivalente al UPF)
- **QFI**: Identificador de Flujo QoS - Marcado de flujo QoS 5G
- **QoS**: Calidad de Servicio - Priorización de tráfico y gestión de ancho de banda
- **RAN**: Red de Acceso Radio - Red de estaciones base (gNB/eNodeB)
- **SEID**: Identificador de Punto de Sesión - ID de sesión PFCP
- **SMF**: Función de Gestión de Sesiones - Elemento de red central 5G para control de sesiones
- **TEID**: Identificador de Punto de Túnel - ID de túnel GTP-U
- **UE**: Equipo de Usuario - Dispositivo móvil
- **UPF**: Función de Plano de Usuario - Elemento de red de reenvío de paquetes 5G

Términos del Protocolo PFCP

- **Asociación**: Relación de control entre SMF y UPF

- **FAR**: Regla de Acción de Reenvío - Determina el comportamiento de reenvío de paquetes
- **IE**: Elemento de Información - Componente del mensaje PFCP
- **ID de Nodo**: Identificador de UPF o SMF (FQDN o dirección IP)
- **PDR**: Regla de Detección de Paquetes - Clasifica los paquetes en flujos
- **PFCP**: Protocolo de Control de Reenvío de Paquetes - Protocolo de control N4
- **QER**: Regla de Aplicación de QoS - Aplica límites de ancho de banda y marcado
- **SDF**: Flujo de Datos de Servicio - Filtro de tráfico específico de la aplicación
- **Sesión**: Sesión PFCP que representa la sesión PDU de UE o contexto PDP
- **URR**: Regla de Reporte de Uso - Rastrea volúmenes de datos para facturación

Términos de eBPF y del Núcleo de Linux

- **BPF**: Filtro de Paquetes de Berkeley - Tecnología de filtrado de paquetes en el núcleo
- **eBPF**: BPF Extendida - Ruta de datos programable en el núcleo
- **Hash Map**: Almacenamiento de clave-valor eBPF para búsquedas rápidas
- **XDP**: Ruta de Datos eXpress - Procesamiento de paquetes en el núcleo a nivel de controlador
- **Verificador**: Componente del núcleo que valida programas eBPF por seguridad
- **Mapa**: Estructura de datos eBPF compartida entre el núcleo y el espacio de usuario
- **Zero-copy**: Procesamiento de paquetes sin copiar al espacio de usuario

Términos del Producto OmniUPF

- **OmniUPF**: Función de Plano de Usuario basada en eBPF (este producto)
- **Datapath**: Motor de procesamiento de paquetes (programas eBPF)
- **Plano de Control**: Manejador PFCP y gestión de sesiones
- **REST API**: API HTTP para monitoreo y gestión

- **Web UI**: Panel de control basado en navegador

Guía de Arquitectura de OmniUPF

Tabla de Contenidos

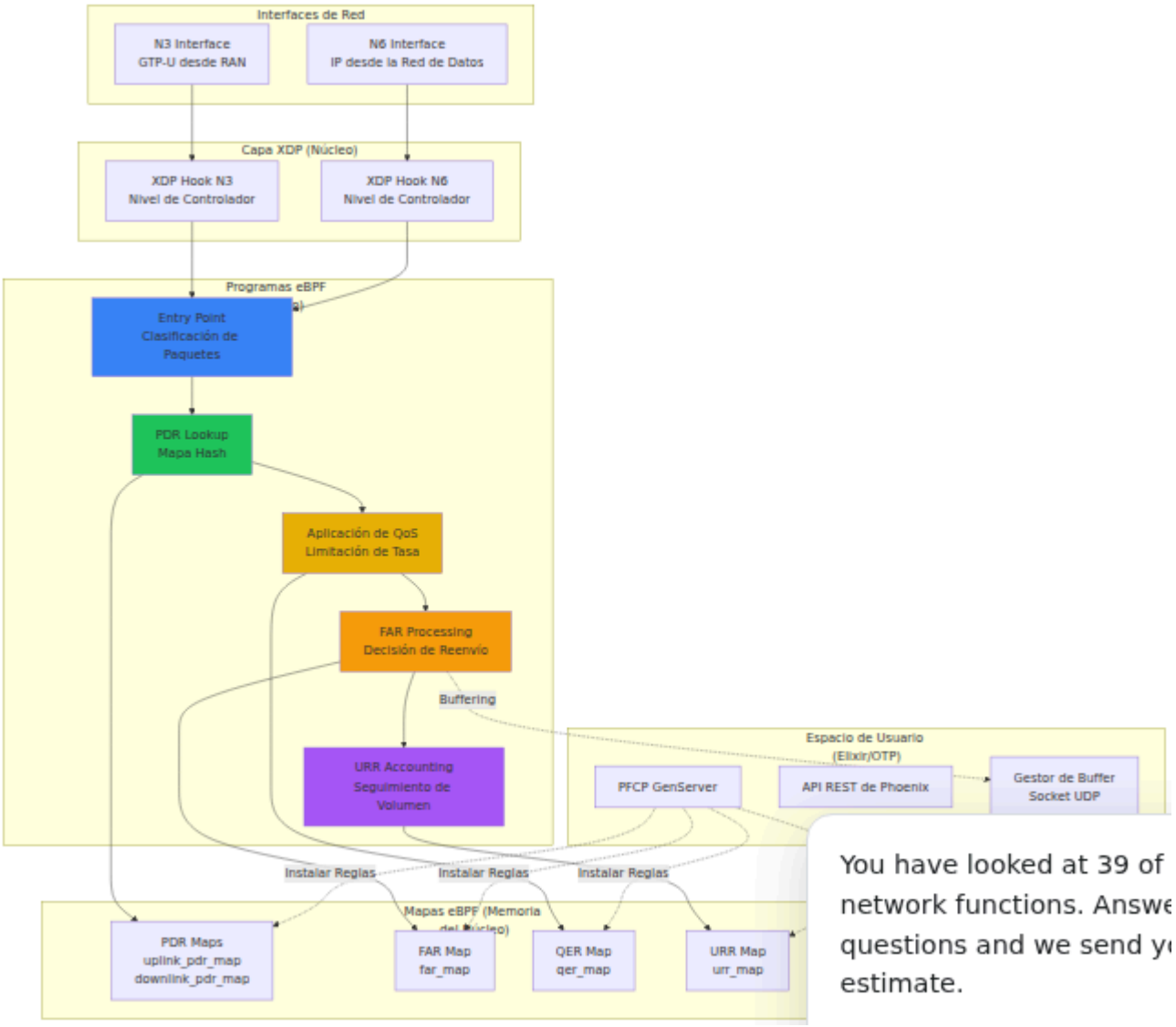
1. Descripción General
2. Fundación de Tecnología eBPF
3. Ruta de Datos XDP
4. Pipeline de Procesamiento de Paquetes
5. Arquitectura de Mapas eBPF
6. Mecanismo de Buffering
7. Aplicación de QoS
8. Características de Rendimiento
9. Escalabilidad y Ajustes

Descripción General

OmniUPF aprovecha eBPF (filtro de paquetes de Berkeley extendido) y XDP (ruta de datos eXpress) para lograr un rendimiento de grado de operador para el procesamiento de paquetes 5G/LTE. El plano de control se implementa en Elixir/OTP utilizando la gestión de sesiones PFCP basada en GenServer, mientras que el plano de datos ejecuta programas eBPF directamente en el núcleo de Linux. Esta separación elimina la sobrecarga del procesamiento de paquetes en espacio de usuario y logra un rendimiento de múltiples gigabits con latencia de microsegundos.

El archivo objeto eBPF (`ipentrypoint_bpf.o`) se compila a partir de código fuente C (en el directorio `ebpf/xdp/`) y se carga en tiempo de ejecución por el plano de control de Elixir a través de enlaces NIF a libbpf.

Capas de Arquitectura



Principios de Diseño Clave

Procesamiento Sin Copia:

- Paquetes procesados completamente en espacio del núcleo
- Sin copia de datos entre el núcleo y el espacio de usuario
- Manipulación directa de paquetes utilizando XDP

Estructuras de Datos Sin Bloqueo:

- Los mapas eBPF utilizan tablas hash por CPU
- Operaciones atómicas para acceso concurrente

- Sin sobrecarga de mutex/bloqueo

Listo para Desplazamiento de Hardware:

- El modo de desplazamiento XDP admite la ejecución de SmartNIC
- Compatible con tarjetas de red que admiten XDP
- Recaída a modos nativos de controlador o genéricos

Fundación de Tecnología eBPF

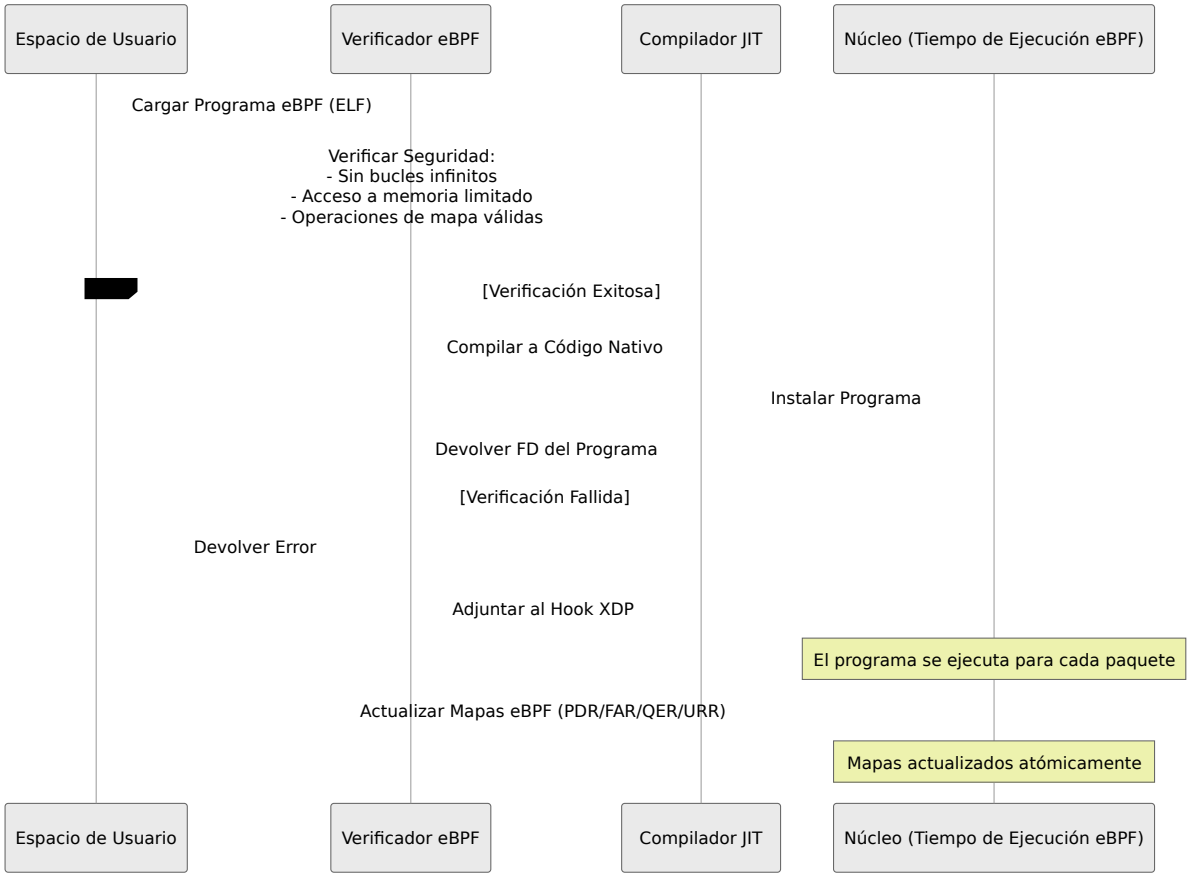
¿Qué es eBPF?

eBPF (filtro de paquetes de Berkeley extendido) es una tecnología revolucionaria del núcleo de Linux que permite que programas seguros y en sandbox se ejecuten en espacio del núcleo sin cambiar el código fuente del núcleo o cargar módulos del núcleo.

Características Clave:

- **Seguridad**: El verificador eBPF asegura que los programas no puedan bloquear el núcleo
- **Rendimiento**: Se ejecuta a velocidad nativa del núcleo (sin sobrecarga de interpretación)
- **Flexibilidad**: Puede ser actualizado en tiempo de ejecución sin reiniciar el núcleo
- **Observabilidad**: Trazado y estadísticas incorporadas

Ciclo de Vida del Programa eBPF



Mapas eBPF

Los mapas eBPF son estructuras de datos del núcleo compartidas entre programas eBPF y espacio de usuario.

Tipos de Mapa Utilizados en OmniUPF:

Tipo de Mapa	Descripción	Caso de Uso
`BPF_MAP_TYPE_HASH`	Tabla hash con pares clave-valor	Búsqueda de PDR por TEID o IP de UE
`BPF_MAP_TYPE_ARRAY`	Array indexado por entero	Búsqueda de QER, FAR, URR por ID
`BPF_MAP_TYPE_PERCPU_HASH`	Tabla hash por CPU (sin bloqueo)	Búsquedas de PDR de alto rendimiento
`BPF_MAP_TYPE_LRU_HASH`	Hash LRU (Menos Recientemente Usado)	Evicción automática de entradas antiguas

Operaciones de Mapa:

- **Búsqueda**: O(1) búsqueda hash (sub-microsegundo)
- **Actualizar**: Actualizaciones atómicas desde espacio de usuario
- **Eliminar**: Eliminación inmediata de entradas
- **Iterar**: Operaciones por lotes para volcar mapas

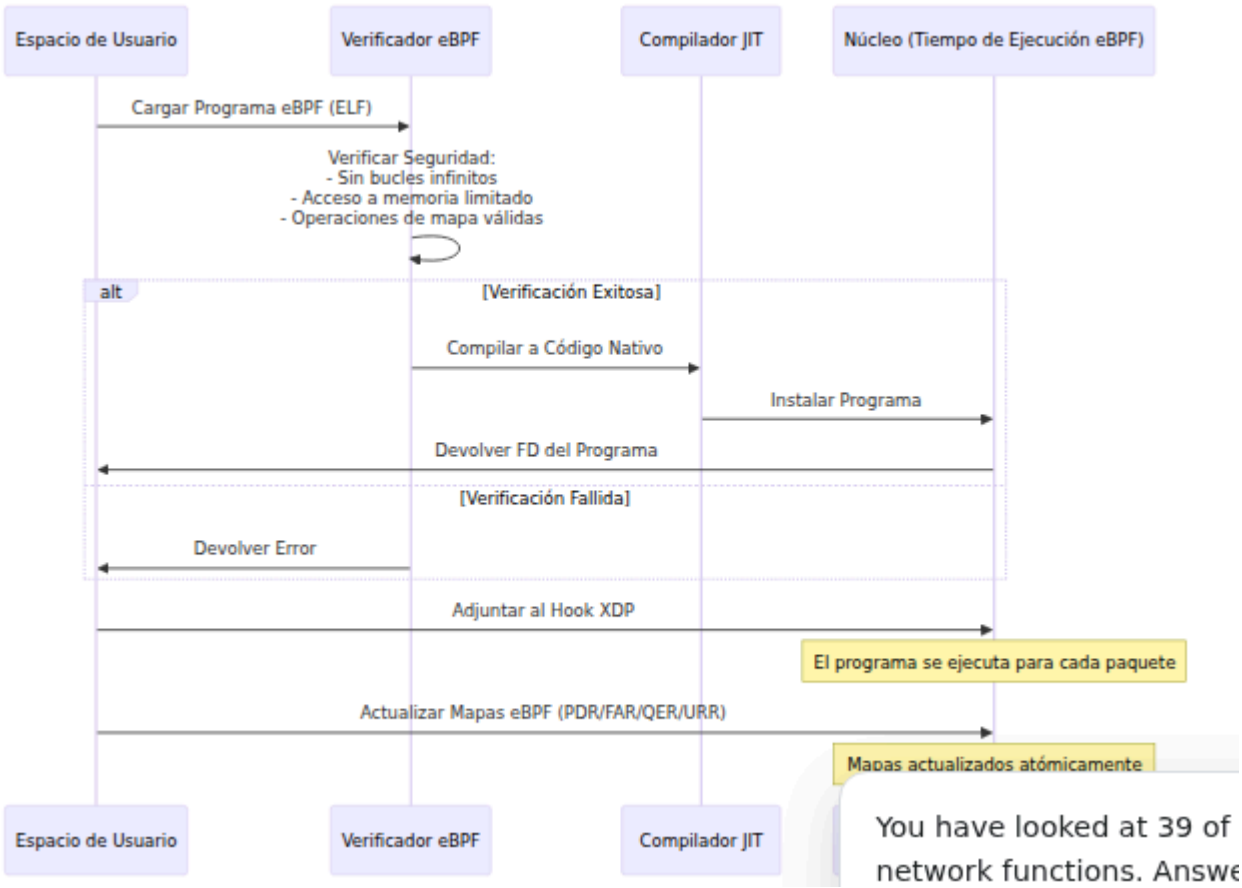
Ruta de Datos XDP

Descripción General de XDP

XDP (ruta de datos eXpress) es un gancho del núcleo de Linux que permite que programas eBPF procesen paquetes en el punto más temprano posible, justo después de que el controlador de red los recibe, antes de la pila de red del núcleo.

Modos de Adjuntar XDP

OmniUPF admite tres modos de adjuntar XDP, cada uno con diferentes características de rendimiento y compatibilidad.



1. Modo de Desplazamiento XDP

Ejecución de Hardware (Mejor Rendimiento):

- El programa eBPF se ejecuta directamente en el hardware de SmartNIC
- Procesamiento de paquetes en el NIC sin tocar la CPU
- Logra un rendimiento de más de 100 Gbps
- Requiere un SmartNIC compatible (Netronome, Mellanox ConnectX-6)

Configuración (en `runtime.exs`):

```
xdp_attach_mode = "offload"
```

Limitaciones:

- Requiere hardware SmartNIC costoso
- Complejidad limitada del programa eBPF
- No todas las características eBPF son compatibles con el hardware

---

2. Modo Nativo XDP (Predeterminado para Producción)

Ejecución a Nivel de Controlador (Alto Rendimiento):

- El programa eBPF se ejecuta en el contexto del controlador de red
- Los paquetes se procesan antes de la asignación de SKB (buffer de socket)
- Logra entre 10-40 Gbps por núcleo
- Requiere un controlador con soporte para XDP (la mayoría de los controladores modernos)

Configuración (en `runtime.exs`):

```
xdp_attach_mode = "native"
```

Ventajas:

- Rendimiento muy alto (millones de pps)
- Amplia compatibilidad de hardware
- Conjunto completo de características eBPF

Controladores Soportados:

- Intel: i40e, ice, ixgbe, igb
- Mellanox: mlx4, mlx5
- Broadcom: bnxt
- Amazon: ena
- La mayoría de las tarjetas de red de 10G+

---

3. Modo Genérico XDP

Emulación de Software (Compatibilidad):

- El programa eBPF se ejecuta después de que el núcleo asigna SKB
- Emulación de software del comportamiento de XDP
- Funciona en cualquier interfaz de red
- Útil para pruebas y desarrollo

Configuración (en `runtime.exs`):

```
xdp_attach_mode = "generic"
```

Casos de Uso:

- Desarrollo y pruebas
- Entornos virtualizados (VMs sin SR-IOV)
- Hardware de red más antiguo
- Pruebas de interfaz de loopback

Rendimiento: 1-5 Gbps (significativamente más lento que nativo/desplazamiento)

Códigos de Retorno de XDP

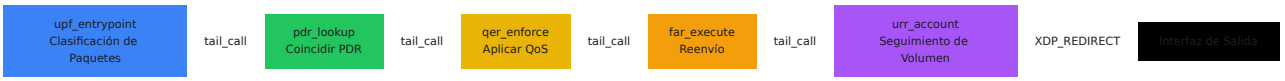
Los programas eBPF devuelven códigos de acción XDP para indicar al núcleo qué hacer con los paquetes:

Código de Retorno	Significado	Uso en OmniUPF
`XDP_PASS`	Enviar paquete a la pila de red del núcleo	Buffering (entrega local), ICMP, tráfico desconocido
`XDP_DROP`	Eliminar paquete inmediatamente	Paquetes inválidos, limitación de tasa, eliminaciones por política
`XDP_TX`	Transmitir paquete de vuelta por la misma interfaz	No se utiliza actualmente
`XDP_REDIRECT`	Enviar paquete a una interfaz diferente	Ruta principal de reenvío (N3 ↔ N6)
`XDP_ABORTED`	Error de procesamiento, eliminar paquete y registrar	Errores de programa eBPF

Pipeline de Procesamiento de Paquetes

Estructura del Programa

OmniUPF utiliza llamadas de cola eBPF para crear un pipeline modular de procesamiento de paquetes.



Llamadas de Cola:

- Permiten que programas eBPF llamen a otros programas eBPF
- Reutiliza el mismo marco de pila (profundidad de pila limitada)

- Permite un diseño modular del pipeline
- Profundidad máxima de 33 llamadas de cola

Procesamiento de Paquetes de Subida

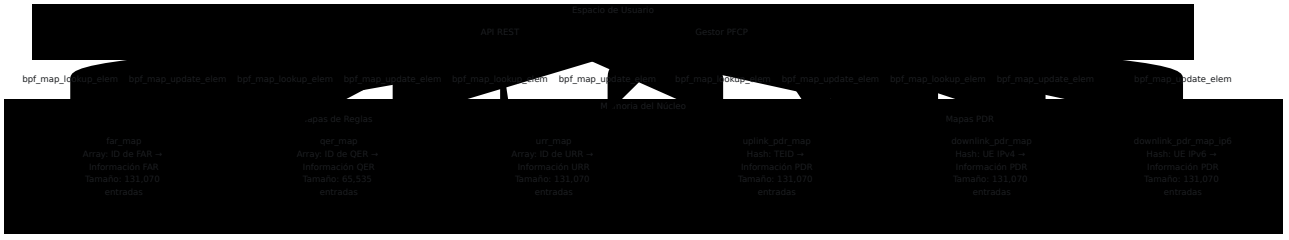


Procesamiento de Paquetes de Bajada



Arquitectura de Mapas eBPF

Diseño de Memoria del Mapa



Dimensionamiento del Mapa

OmniUPF calcula automáticamente los tamaños de los mapas en función de la configuración `max_sessions`:

```
Mapas PDR = 2 × max_sessions  (uplink + downlink)
Mapas FAR = 2 × max_sessions  (uplink + downlink)
Mapas QER = 1 × max_sessions  (compartido por sesión)
Mapas URR = 3 × max_sessions  (múltiples URRs por sesión)
```

Ejemplo (max_sessions = 65,535):

- Mapas PDR: 131,070 entradas cada uno
- Mapa FAR: 131,070 entradas
- Mapa QER: 65,535 entradas
- Mapa URR: 131,070 entradas

Memoria Total:

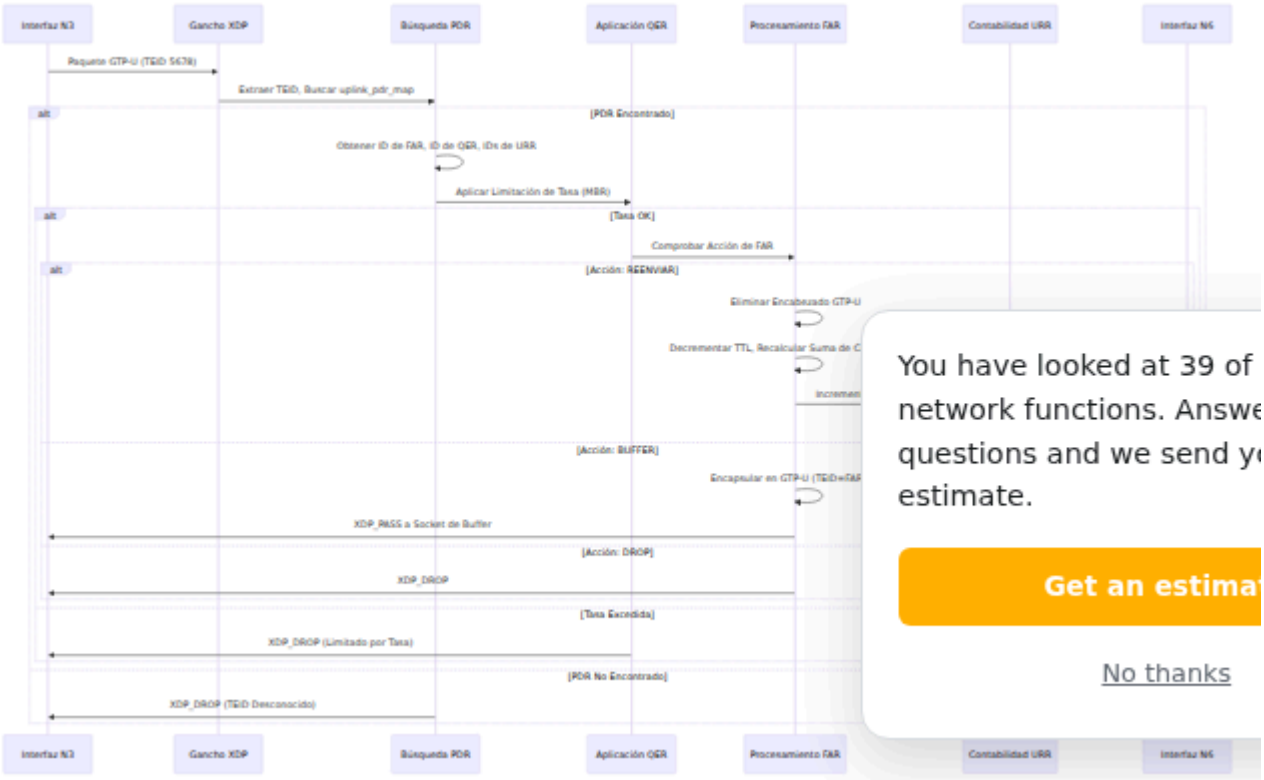
```
Mapas PDR: 3 × 131,070 × 212 B = ~83 MB
Mapa FAR:  131,070 × 20 B = ~2.6 MB
Mapa QER:  65,535 × 36 B = ~2.3 MB
Mapa URR:  131,070 × 20 B = ~2.6 MB
Total: ~91 MB de memoria del núcleo
```

Mecanismo de Buffering

Descripción General del Buffering

OmniUPF implementa buffering de paquetes para escenarios de traspaso encapsulando paquetes en GTP-U y enviándolos a un proceso de espacio de usuario a través de un socket UDP.

Arquitectura de Buffering



Detalles de Encapsulación de Buffer

Cuando el buffering está habilitado (bit de acción FAR 2 establecido), el programa eBPF:

1. **Calcula el Tamaño Original del Paquete**:

```
orig_packet_len = ntohs(ip->tot_len);  // Desde el encabezado IP
```

2. **Expande el Encabezado del Paquete**:

```
// Agregar espacio para: IP Exterior + UDP + GTP-U
gtp_encap_size = sizeof(struct iphdr) + sizeof(struct udphdr) + sizeof(struct gtpuhdr);
bpf_xdp_adjust_head(ctx, -gtp_encap_size);
```

3. **Construye el Encabezado IP Exterior**:

```
ip->saddr = original_sender_ip;  // Preservar fuente para
evitar filtrado martiano
ip->daddr = local_upf_ip;        // IP local donde el oyente de
espacio de usuario se vincula
ip->protocol = IPPROTO_UDP;
ip->ttl = 64;
```

4. **Construye el Encabezado UDP**:

```
udp->source = htons(22152);  // BUFFER_UDP_PORT
udp->dest = htons(22152);
udp->len = htons(sizeof(udphdr) + sizeof(gtpuhdr) +
orig_packet_len);
```

5. **Construye el Encabezado GTP-U**:

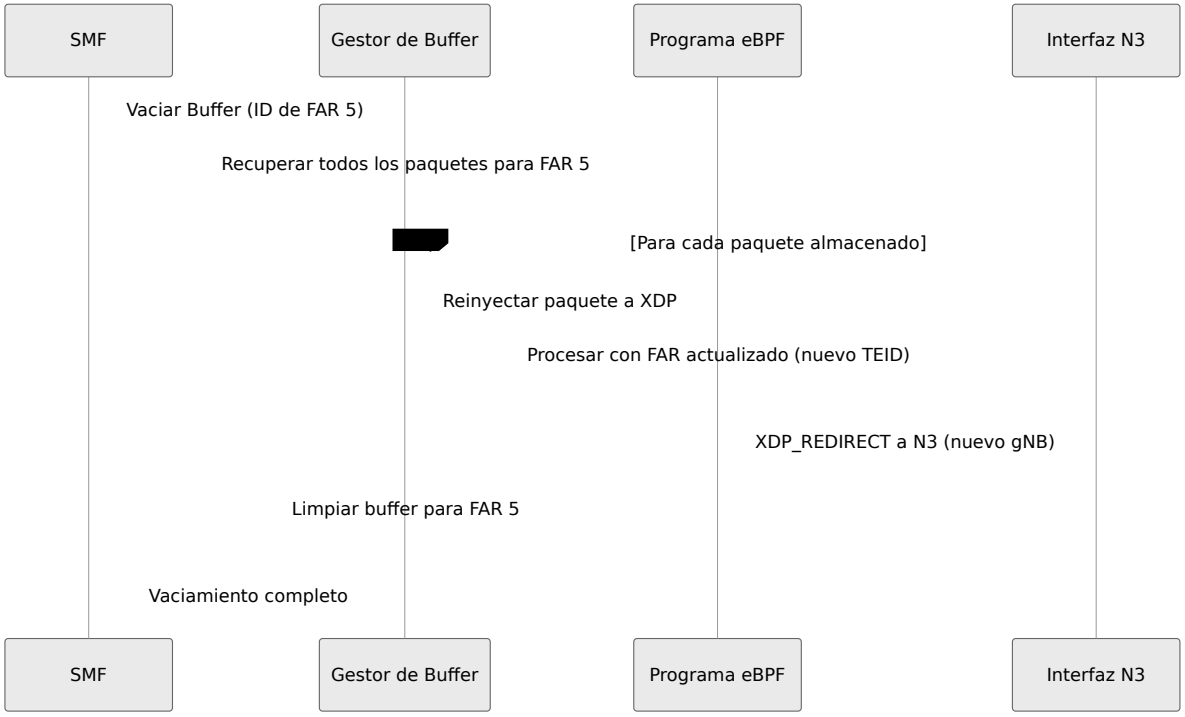
```
gtp->version = 1;
gtp->message_type = GTPU_G_PDU;
gtp->teid = htonl(far_id | (direction << 24));  // Codificar ID
de FAR y dirección
gtp->message_length = htons(orig_packet_len);
```

6. **Devuelve XDP_PASS**:

    - El núcleo entrega el paquete al socket UDP local en el puerto 22152
    - El gestor de buffer de espacio de usuario recibe y almacena el paquete

Operación de Vaciamiento de Buffer

Cuando se completa el traspaso, el SMF actualiza el FAR para limpiar la bandera BUFFER. Los paquetes almacenados se reproducen:



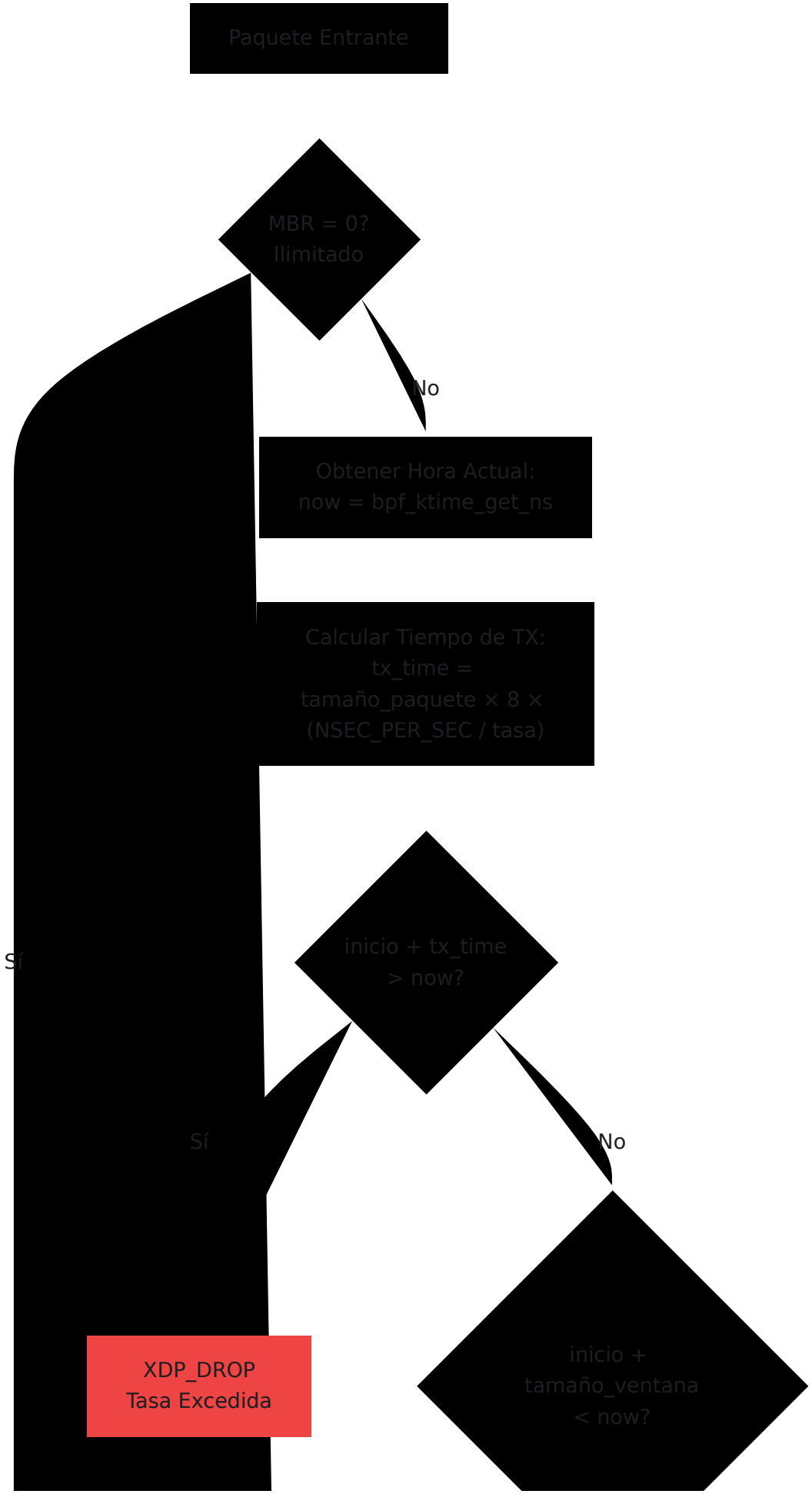
Parámetros de Gestión de Buffer

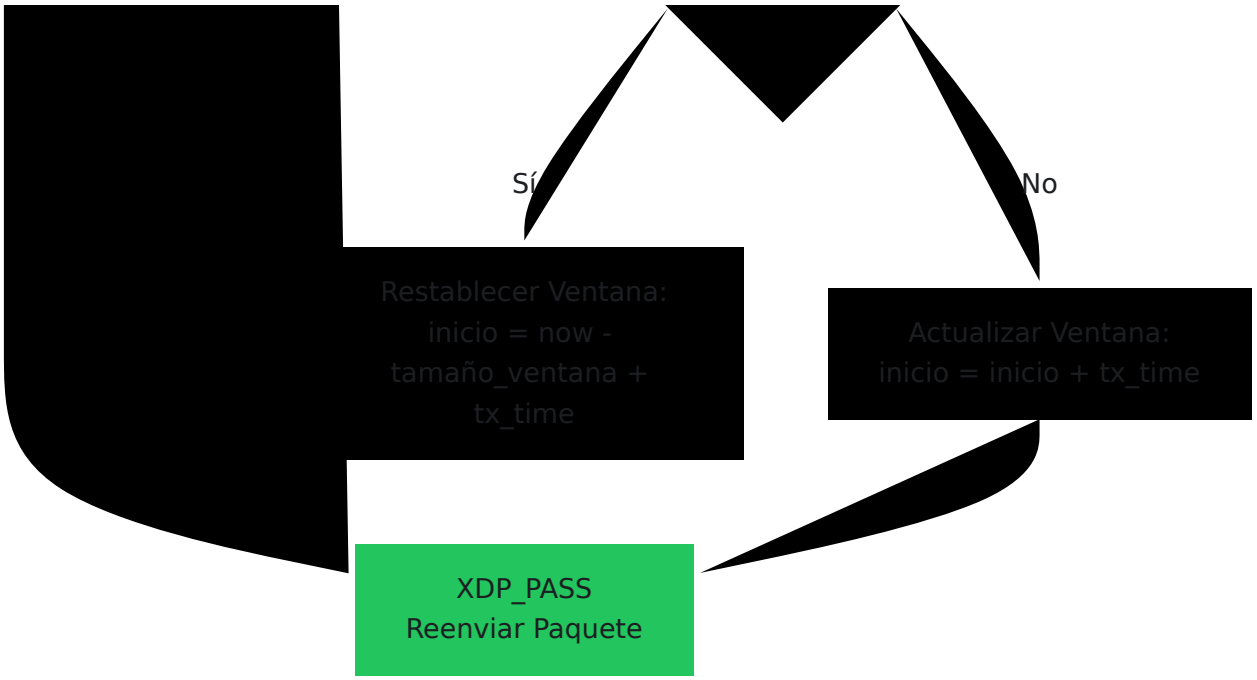
Parámetro	Predeterminado	Descripción
Máx. por FAR	10,000 paquetes	Máximo de paquetes almacenados por FAR
Máx. Total	100,000 paquetes	Máximo total de paquetes almacenados
TTL del Paquete	30 segundos	Tiempo antes de que los paquetes almacenados expiren
Puerto de Buffer	22152	Puerto UDP para entrega de buffer
Intervalo de Limpieza de Buffer	60 segundos	Frecuencia de verificación de paquetes expirados

Aplicación de QoS

Algoritmo de Limitación de Tasa

OmniUPF implementa un **limitador de tasa de ventana deslizante** para la aplicación de QoS.


Paquete Entrante
MBR = 0?
Ilimitado
No
Obtener Hora Actual:
now = bpf_ktime_get_ns
Calcular Tiempo de TX:
tx_time =
tamaño_paquete × 8 ×
(NSEC_PER_SEC / tasa)
inicio + tx_time
> now?
Sí
Sí
No
XDP_DROP
Tasa Excedida
inicio +
tamaño_ventana
< now?



Implementación de Ventana Deslizante

Algoritmo (desde `qer.h`):

```c
static __always_inline enum xdp_action limit_rate_sliding_window(
    const __u64 packet_size,
    volatile __u64 *window_start,
    const __u64 rate)
{
    static const __u64 NSEC_PER_SEC = 1000000000ULL;
    static const __u64 window_size = 5000000ULL;  // Ventana de 5ms

    // Tasa = 0 significa ilimitado
    if (rate == 0)
        return XDP_PASS;

    // Calcular tiempo de transmisión para este paquete
    __u64 tx_time = packet_size * 8 * (NSEC_PER_SEC / rate);
    __u64 now = bpf_ktime_get_ns();

    // Comprobar si estamos adelantados a la ventana (el paquete se transmitiría en el futuro)
    __u64 start = *window_start;
    if (start + tx_time > now)
        return XDP_DROP;  // Límite de tasa excedido

    // Si la ventana ha pasado, restablecerla
    if (start + window_size < now) {
        *window_start = now - window_size + tx_time;
        return XDP_PASS;
    }

    // Actualizar ventana para tener en cuenta este paquete
    *window_start = start + tx_time;
    return XDP_PASS;
}
```

Parámetros Clave:

- **Tamaño de Ventana**: 5ms (5,000,000 nanosegundos)
- **Por Dirección**: Ventanas separadas para subida y bajada
- **Actualizaciones Atómicas**: Utiliza punteros volátiles para acceso concurrente
- **MBR = 0**: Tratado como ancho de banda ilimitado

Ejemplo de Cálculo de QoS

Escenario: MBR = 100 Mbps, Tamaño de Paquete = 1500 bytes

1. **Tiempo de Transmisión**:

```
tx_time = 1500 bytes × 8 bits/byte × (1,000,000,000 ns/sec ÷
100,000,000 bps)
tx_time = 1500 × 8 × 10 = 120,000 ns = 120 µs
```

2. **Comprobación de Tasa**:

   - Si el último paquete se transmitió en `t=0`, el siguiente paquete puede transmitirse en `t=120µs`
   - Si el paquete llega en `t=100µs`, se elimina (demasiado temprano)
   - Si el paquete llega en `t=150µs`, se reenvía (ventana avanzada)

3. **Tasa Máxima de Paquetes**:

```
Max PPS = (100 Mbps ÷ 8) ÷ 1500 bytes = 8,333 paquetes/segundo
Intervalo entre paquetes = 120 µs
```

Características de Rendimiento

Rendimiento

Configuración	Rendimiento	Paquetes/Secundo	Latencia
XDP Offload (SmartNIC)	100 Gbps	148 Mpps	< 1 µs
XDP Nativo (NIC de 10G, núcleo único)	10 Gbps	8 Mpps	2-5 µs
XDP Nativo (NIC de 10G, 4 núcleos)	40 Gbps	32 Mpps	2-5 µs
XDP Genérico	1-5 Gbps	0.8-4 Mpps	50-100 µs

Desglose de Latencia

Latencia Total de Procesamiento de Paquetes (XDP Nativo):

Etapa	Latencia	Acumulativa
RX del NIC	0.5 µs	0.5 µs
Invocación del Gancho XDP	0.1 µs	0.6 µs
Búsqueda PDR (Hash)	0.3 µs	0.9 µs
Comprobación de Tasa QER	0.1 µs	1.0 µs
Procesamiento FAR	0.5 µs	1.5 µs
Actualización URR	0.2 µs	1.7 µs
Encapsulación/Decapsulación GTP-U	0.8 µs	2.5 µs
XDP_REDIRECT	0.5 µs	3.0 µs
TX del NIC	0.5 µs	3.5 µs

Total: ~3.5 µs por paquete (XDP Nativo, NIC de 10G)

Utilización de CPU

Capacidad de Procesamiento por Núcleo:

- Núcleo único: 8-10 Mpps (XDP Nativo)
- Con hyper-threading: 12-15 Mpps
- Escalado multi-núcleo: Casi lineal hasta 8 núcleos

Uso de CPU por Tasa de Paquetes:

```
CPU % ≈ (Tasa de Paquetes / 10,000,000) × 100% por núcleo
```

Ejemplo: Tráfico de 2 Mpps utiliza ~20% de un núcleo

Ancho de Banda de Memoria

Acceso a Mapas eBPF:

- Búsqueda hash: ~100 ns (acierto de caché)
- Búsqueda hash: ~300 ns (fallo de caché)
- Búsqueda de array: ~50 ns (siempre acierto de caché)

Ancho de Banda de Memoria Requerido:

```
Ancho de Banda = Tasa de Paquetes × (Tamaño Promedio del Paquete + Búsquedas de Mapa × 64 bytes)
```

Ejemplo: 10 Mpps × (1500 B + 3 búsquedas × 64 B) ≈ 160 Gbps de ancho de banda de memoria

Escalabilidad y Ajustes

Escalado Horizontal

Múltiples Instancias de UPF:

Setting SMF as parent of SMF would create a cycle

Intente de nuevo

Distribución de Sesiones:

- SMF distribuye sesiones entre instancias de UPF
- Cada UPF maneja un subconjunto de sesiones de UE
- No se necesita comunicación inter-UPF (sin estado)

Escalado Vertical

Ajuste de CPU:

1. Habilitar afinidad de CPU para procesamiento XDP

2. Utilizar RSS (Escalado Lateral de Recepción) para distribuir colas RX
3. Fijar programas eBPF a núcleos específicos

Ajuste de NIC:

1. Aumentar el tamaño del búfer de anillo RX
2. Habilitar NICs de múltiples colas (RSS)
3. Utilizar director de flujo para direccionamiento de tráfico

Ajuste del Núcleo:

```
# Aumentar el límite de memoria bloqueada para mapas eBPF
ulimit -l unlimited

# Deshabilitar el equilibrio de IRQ para núcleos XDP
systemctl stop irqbalance

# Establecer el gobernador de CPU en rendimiento
cpupower frequency-set -g performance

# Aumentar los tamaños de los búferes de red
sysctl -w net.core.rmem_max=134217728
sysctl -w net.core.wmem_max=134217728
```

Planificación de Capacidad

Fórmula:

```
Núcleos de CPU Requeridos = (PPS Esperados ÷ 10,000,000) × 1.5
(50% de margen)
Memoria Requerida = (Sesiones Máx. × 212 B × 3) + 100 MB (mapas
eBPF + sobrecarga)
Red Requerida = (Rendimiento Pico × 2) + 10 Gbps (margen)
```

Ejemplo (1 millón de sesiones, 20 Gbps pico):

- CPU: (20 Gbps ÷ 10 Gbps por núcleo) × 1.5 = 3-4 núcleos
- Memoria: (1M × 212 B × 3) + 100 MB ≈ 750 MB

- Red: (20 Gbps × 2) + 10 Gbps = 50 Gbps de interfaces

Documentación Relacionada

- **Guía de Operaciones de UPF** - Operaciones generales de UPF y despliegue
- **Guía de Gestión de Reglas** - Detalles de PDR, FAR, QER, URR
- **Guía de Monitoreo** - Monitoreo de rendimiento y métricas
- **Guía de Operaciones de Interfaz Web** - Uso del panel de control
- **Guía de Solución de Problemas** - Problemas comunes y diagnósticos
- **Guía de Jardín Amurallado** - Redirección fuera de crédito utilizando el mecanismo BUFF para la interceptación de paquetes en espacio de usuario

Guía de Configuración de OmniUPF

Tabla de Contenidos

1. Descripción General
2. Modos de Operación
3. Modos de Adjunto XDP
4. Parámetros de Configuración
5. Archivo de Configuración
6. Compatibilidad con Hypervisores
7. Compatibilidad con NIC
8. Ejemplos de Configuración
9. Dimensionamiento del Mapa y Planificación de Capacidad

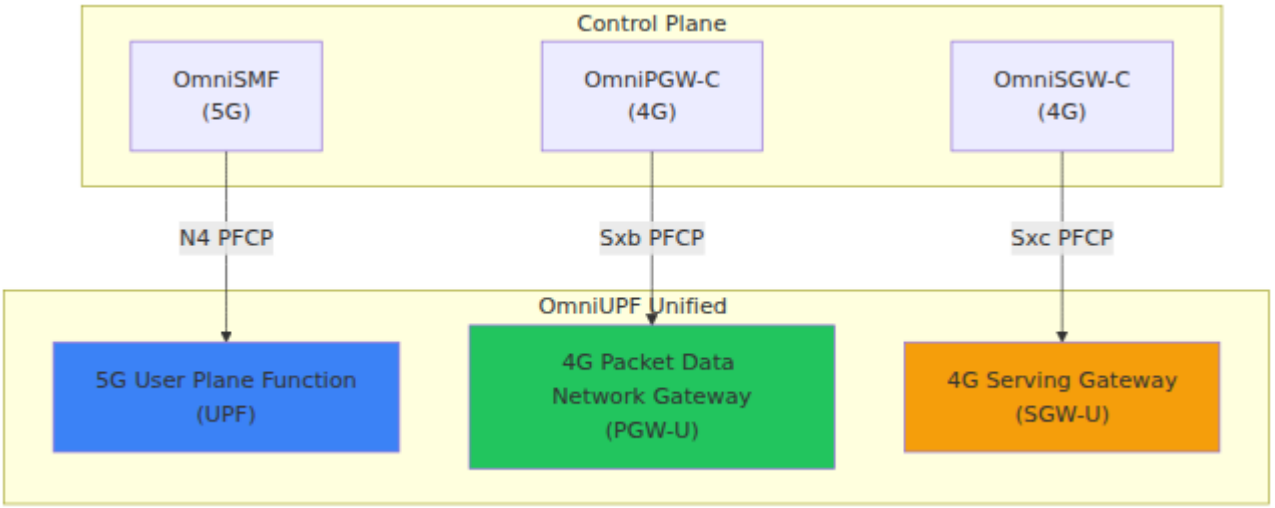
Descripción General

OmniUPF es una función de plano de usuario versátil que puede operar en múltiples modos para soportar tanto redes centrales 4G (EPC) como 5G. El plano de control está implementado en Elixir/OTP, y la configuración se gestiona a través de un archivo de configuración de Elixir (`runtime.exs`).

Al instalar el paquete, el archivo de configuración se coloca en `/etc/omniupf/runtime.exs` y se preserva a través de las actualizaciones. El UPF debe reiniciarse después de los cambios en la configuración.

Modos de Operación

OmniUPF es una **plataforma unificada** que puede operar simultáneamente como:



Configuración del Modo

El modo de operación es **determinado por el plano de control** (SMF, PGW-C o SGW-C) que establece asociaciones PFCP con OmniUPF. No se requiere una configuración específica de OmniUPF para cambiar entre modos.

Operación Simultánea:

- OmniUPF puede aceptar asociaciones PFCP de múltiples planos de control simultáneamente
- Una sola instancia de OmniUPF puede actuar como UPF, PGW-U y SGW-U **al mismo tiempo**
- Las sesiones de diferentes planos de control están aisladas y se gestionan de forma independiente

---

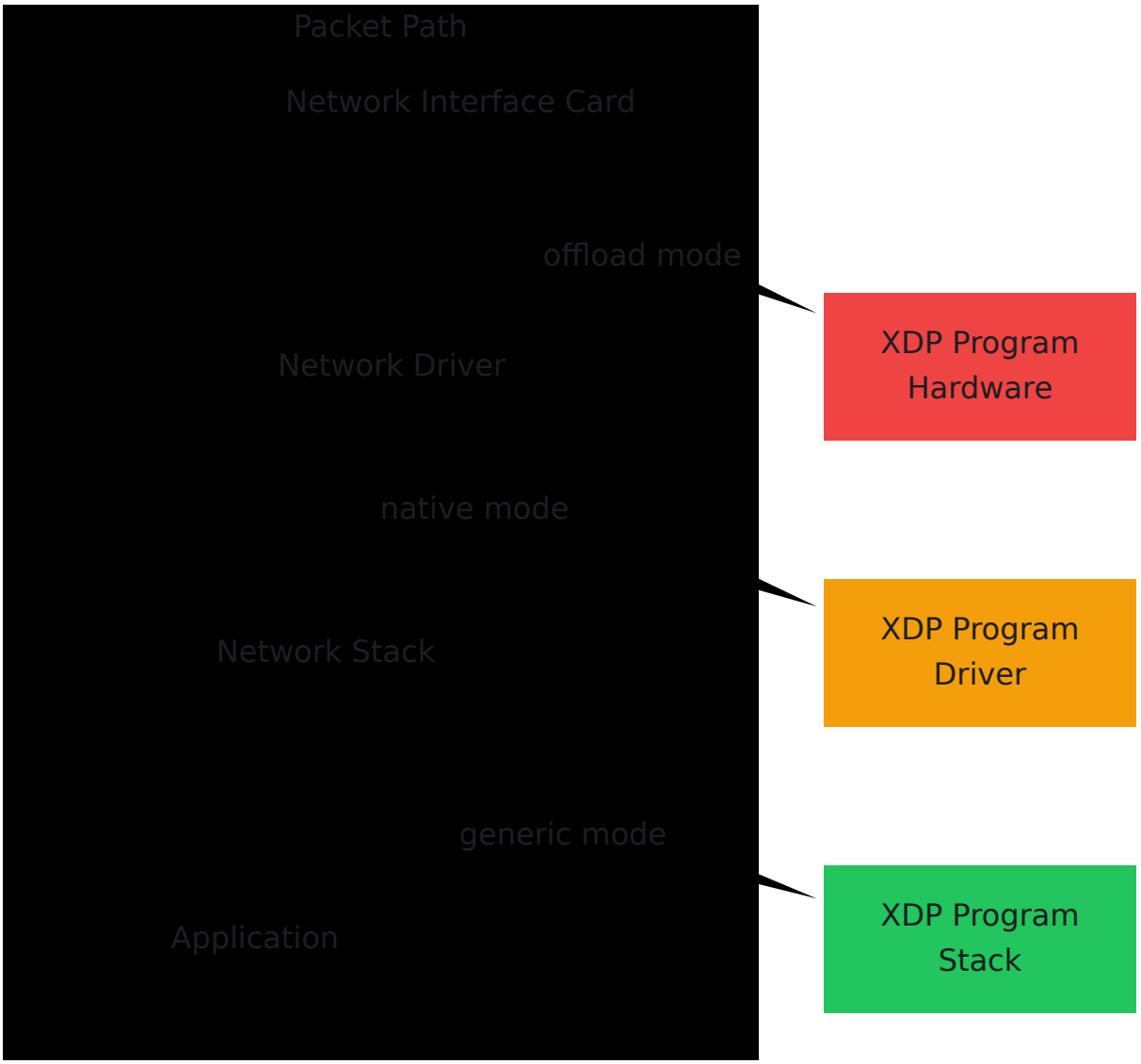
Modos de Adjunto XDP

OmniUPF utiliza XDP (eXpress Data Path) para el procesamiento de paquetes de alto rendimiento. Se admiten tres modos de adjunto.

Para instrucciones detalladas de configuración de XDP, especialmente para Proxmox y otros hypervisores, consulte la Guía de Modos XDP.

Comparación de Modos

Modo	Punto de Adjunto	Rendimiento	Caso de Uso	Requisitos de NIC
Genérico	Pila de red (núcleo)	~1-2 Mpps	Pruebas, desarrollo, compatibilidad	Cualquier NIC
Nativo	Controlador de red (núcleo)	~5-10 Mpps	Producción (bare metal, VM con SR-IOV)	Controlador compatible con XDP
Descarga	Hardware de NIC (SmartNIC)	~10-40 Mpps	Producción de alto rendimiento	SmartNIC con descarga XDP



Modo Genérico (Predeterminado)

Descripción: El programa XDP se ejecuta en la pila de red del núcleo

Ventajas:

- Funciona con **cualquier** interfaz de red
- No se requieren controladores o hardware especiales
- Ideal para pruebas y desarrollo
- Compatible con todos los hypervisores y plataformas de virtualización

Desventajas:

- Rendimiento más bajo (~1-2 Mpps por núcleo)

- Los paquetes ya han pasado por el controlador antes del procesamiento de XDP

Configuración (en `runtime.exs`):

```
xdp_attach_mode = "generic"
```

Mejor para:

- Máquinas virtuales sin SR-IOV
- Entornos de pruebas y validación
- NICs sin soporte de controlador XDP
- Hypervisores como Proxmox, VMware, VirtualBox

Modo Nativo (Recomendado)

Descripción: El programa XDP se ejecuta a nivel del controlador de red

Ventajas:

- Alto rendimiento (~5-10 Mpps por núcleo)
- Paquetes procesados antes de entrar en la pila de red
- Latencia significativamente más baja que el modo genérico
- Funciona en bare metal y VMs con SR-IOV

Desventajas:

- Requiere un controlador de red con soporte para XDP
- No todos los NICs/controladores soportan XDP nativo

Configuración (en `runtime.exs`):

```
xdp_attach_mode = "native"
```

Mejor para:

- Despliegues de producción en bare metal
- VMs con paso SR-IOV
- NICs con controladores compatibles con XDP (Intel, Mellanox, etc.)

Requisitos:

- Controlador de red compatible con XDP (ver Compatibilidad con NIC)
- Kernel de Linux 5.15+ con soporte XDP habilitado

Modo de Descarga (Rendimiento Máximo)

Descripción: El programa XDP se ejecuta directamente en el hardware de SmartNIC

Ventajas:

- Rendimiento máximo (~10-40 Mpps)
- Cero sobrecarga de CPU para el procesamiento de paquetes
- Latencia sub-microsegundo
- Libera CPU para el procesamiento del plano de control

Desventajas:

- Requiere hardware SmartNIC costoso
- Disponibilidad limitada de SmartNIC
- Configuración y ajuste complejos

Configuración (en `runtime.exs`):

```
xdp_attach_mode = "offload"
```

Mejor para:

- Despliegues de producción de ultra alto rendimiento
- Computación en el borde con estrictos requisitos de latencia
- Entornos donde los recursos de CPU son limitados

Requisitos:

- SmartNIC con soporte de descarga XDP (Netronome Agilio CX, Mellanox BlueField)
- Firmware y controladores especializados

Parámetros de Configuración

Interfaces de Red

Parámetro	Descripción	Tipo	Predeterminado
`xdp_interfaces`	Interfaces de red para tráfico N3/N6/N9 (separadas por comas, o `"auto"` para todas las no-loopback)	String	`"auto"`
`gtpu_interface`	NIC que transporta todo GTP-U (N3/N9/S5-S8). Configúrelo junto con `sgi_interface` para adjuntar un programa XDP solo GTP-U a esta NIC; déjelo sin configurar para el programa combinado	String	`nil`
`sgi_interface`	NIC que transporta SGi/N6 de IP simple. Configúrelo junto con `gtpu_interface` para adjuntar un programa XDP solo de bajada a esta NIC	String	`nil`
`n3_address`	Dirección IPv4 para la interfaz N3 (GTP-U desde RAN)	IP	`"127.0.0.1"`
`n9_address`	Dirección IPv4 para la interfaz N9 (UPF a UPF para ULCL)	IP	Igual que `n3_address`

Ejemplo (en `runtime.exs`):

```
xdp_interfaces = "eth0,eth1"
n3_address = "10.100.50.233"
n9_address = "10.100.50.234"
```

División de datapath por NIC. Cuando GTP-U y SGi utilizan NICs separadas, nombre cada una para que el cargador adjunte un programa XDP de un solo propósito por NIC (solo GTP-U en `gtpu_interface`, solo bajada en `sgi_interface`) en lugar del programa combinado "on-a-stick". Ambas también deben aparecer en `xdp_interfaces`. Deje ambas sin configurar (el valor predeterminado) para adjuntar el programa combinado a cada interfaz.

```
xdp_interfaces = "eth1,eth2"
gtpu_interface = "eth1"   # todo GTP-U (N3/N9/S5-S8)
sgi_interface  = "eth2"   # SGi/N6 de IP simple
```

Configuración de PFCP

Parámetro	Descripción	Tipo	Predeterminado
`pfcp_address`	Dirección local para el servidor PFCP (interfaz N4/Sxb/Sxc)	IP String	`"127.0.0.1"`
`pfcp_port`	Puerto PFCP	Integer	`8805`
`node_id`	ID de Nodo local para el protocolo PFCP	IP String	`"127.0.0.1"`
`heartbeat_interval_ms`	Intervalo de latido PFCP (milisegundos)	Integer	`5000`
`heartbeat_timeout_ms`	Tiempo de espera del latido PFCP (milisegundos)	Integer	`5000`
`heartbeat_retries`	Número de reintentos de latido antes de declarar al par como muerto	Integer	`3`
`association_setup_timeout`	Tiempo de espera para una Respuesta de	Integer	`5000`

Parámetro	Descripción	Tipo	Predeterminado
	Configuración de Asociación PFCP cuando el UPF inicia una asociación (milisegundos)		
`pfcp_remote_nodes`	Lista de cadenas de direcciones IP del plano de control con las que el UPF establece activamente asociaciones al inicio (iniciadas por el UPF). Vacío significa que el UPF solo acepta asociaciones iniciadas por el plano de control.	Lista de String	`[]`

Ejemplo (en `runtime.exs`):

```
pfcp_address = "10.100.50.241"
pfcp_port = 8805
node_id = "10.100.50.241"
heartbeat_interval_ms = 10_000
heartbeat_retries = 5
association_setup_timeout = 5_000
pfcp_remote_nodes = []                # o por ejemplo
["10.100.50.20", "10.100.50.22"]
```

API y Monitoreo

Parámetro	Descripción	Tipo	Predeterminado
`api_port`	Puerto local para el servidor REST API (Phoenix)	Integer	`8080`
`log_level`	Nivel de registro (`:debug`, `:info`, `:warning`, `:error`)	Atom	`:info`

Ejemplo (en `runtime.exs`):

```
api_port = 8080
log_level = :debug
```

Gestión de Ruta GTP

Parámetro	Descripción	Tipo	Predeterminado
`gtpu_port`	Puerto GTP-U	Integer	`2152`
`gtp_echo_interval`	Intervalo de eco predeterminado en segundos	Integer	`10`
`gtp_echo_retries`	Máximo de ecos perdidos antes de fallar la ruta	Integer	`3`
`gtp_peers`	Lista de pares GTP para mantener vivos los ecos de solicitud	Lista	`[]`

Ejemplo (en `runtime.exs`):

```
gtp_echo_interval = 15
gtp_echo_retries = 3
gtp_peers = [
  %{address: parse_ip.("10.100.50.50"), echo: true, echo_interval:
10},
  %{address: parse_ip.("10.100.50.60"), echo: false},
]
```

GTP-U Descarga Sobredimensionada

GTP-U añade 36 bytes a cada paquete de bajada. Por lo tanto, un paquete de tamaño completo de 1500 bytes de internet se convierte en un paquete GTP-U de 1536 bytes, que no cabe en un enlace N3 de 1500 bytes. Se requiere que el emisor de GTP-U fragmente tales paquetes (TS 29.281 §4.2.4), y muchos UE y enrutadores ignoran el MTU del enlace ofrecido en el PCO, por lo que esto sucede en operación normal.

La ruta rápida de XDP no puede fragmentar. Cuando un paquete GTP-U de bajada es más grande que el MTU de salida, se entrega a la ruta lenta del espacio de usuarios, que lo envía desde un socket UDP ordinario para que el núcleo fragmente el paquete exterior. Esto se aplica tanto cuando el UPF encapsula (N6 a N3) como cuando reenvía entre túneles GTP-U (SGW-U).

Parámetro	Descripción	Tipo	Predeterm
`gtpu_oversize_punt_enabled`	`true`: GTP-U de bajada sobredimensionado se envía al espacio de usuarios y se fragmenta. `false`: se descarta	Boolean	ninguno, **requerido**

El parámetro es requerido: el UPF no comenzará sin él. Cada paquete enviado se aleja de la ruta rápida, por lo que un suscriptor que envía tráfico sostenido de tamaño completo a través de un MTU de túnel más pequeño (por ejemplo, una descarga masiva a un dispositivo que ignora el MTU del PCO) mueve esa carga al espacio de usuarios. Observe `upf_gtpu_oversize_punted_total` (ver METRICS.md) y configure el parámetro en `false` para reducir la carga, a costa de descartar esos paquetes.

Ejemplo (en `runtime.exs`):

```
gtpu_oversize_punt_enabled = true
```

Los GTP-U fragmentados recibidos del RAN son reensamblados por el núcleo y reinyectados en el datapath. Eso no necesita configuración.

Limitación de MSS TCP

Un dispositivo que ignora el MTU del enlace en el PCO (o Anuncio de Enrutador) anuncia un MSS de 1460 bytes en su apretón de manos TCP. Ambos extremos envían entonces paquetes de 1500 bytes, y cada uno de ellos pasa por la ruta

lenta sobredimensionada descrita anteriormente. Limitar el MSS en el apretón de manos mantiene ese tráfico en la ruta rápida.

Parámetro	Descripción	Tipo	Predeterminado
`tcp_mss_clamp`	Mayor MSS TCP (IPv4) que un SYN o SYN-ACK puede anunciar a través de este UPF. Los valores más grandes se reducen a él. IPv6 utiliza un valor 20 menor. `false` deja el MSS sin tocar	`false` o entero 536-1460	ninguno, **requerido**

Solo se cambian los paquetes SYN y SYN-ACK, uno o dos por conexión; los paquetes de datos no se tocan. Ambas direcciones están limitadas: el SYN del UE limita lo que el servidor envía al UE, y el SYN-ACK del servidor limita lo que el UE envía. La suma de verificación TCP se actualiza de forma incremental. La limitación se aplica donde el UPF desencapsula o encapsula el paquete de usuario (PGW-U / UPF), no en un reenvío puro de SGW-U.

Establezca el valor en el MTU del enlace IPv4 ofrecido en el PCO menos 40 bytes: `1310` para un MTU de 1350.

Ejemplo (en `runtime.exs`):

```
tcp_mss_clamp = 1310
```

La limitación cubre solo TCP. El tráfico UDP y otros que superen el MTU del túnel aún toman la ruta lenta sobredimensionada, y también lo hace TCP cuyo apretón de manos el UPF no vio.

Capacidad del Mapa eBPF

Parámetro	Descripción	Tipo	Predeterminado
`max_sessions`	Número máximo de sesiones concurrentes	Integer	`1_000_000`
`far_map_size`	Tamaño del mapa eBPF FAR	Integer	`131_070`
`qer_map_size`	Tamaño del mapa eBPF QER	Integer	`65_535`
`urr_map_size`	Tamaño del mapa eBPF URR	Integer	`65_535`

Ejemplo (en `runtime.exs`):

```
max_sessions = 100_000
far_map_size = 131_070
qer_map_size = 65_535
urr_map_size = 131_070
```

Configuración de Buffer

Los paquetes de bajada se almacenan en búfer mientras un UE está inactivo, y luego se vacían cuando se busca al UE. Estos parámetros limitan cuánto se retiene y por cuánto tiempo.

Parámetro	Descripción	Tipo	Predeterminad
`buffer_port`	Puerto UDP para paquetes en búfer desde eBPF	Integer	`22152`
`buffer_max_total`	Máximo de paquetes en búfer en todos los FARs (límite global)	Integer	`10_000`
`buffer_max_per_far`	Máximo de paquetes en búfer por FAR	Integer	`100`
`buffer_ttl_ms`	Tiempo que se mantiene un paquete en búfer antes de ser descartado (milisegundos)	Integer	`30_000`
`buffer_cleanup_interval_ms`	Intervalo en el que se barren los paquetes en búfer expirados (milisegundos)	Integer	`5_000`

Ejemplo (en `runtime.exs`):

```
buffer_port = 22152
buffer_max_total = 10_000
buffer_max_per_far = 100
buffer_ttl_ms = 30_000
buffer_cleanup_interval_ms = 5_000
```

Los descartes causados por estos límites son contados por `upf_buffer_packets_dropped_total` (etiquetas `global_limit`, `far_limit`, `expired`). Consulte la Referencia de Métricas.

Banderas de Características

Parámetro	Descripción	Tipo	Predeterminado
`feature_ueip`	Habilitar la asignación de IP de UE por OmniUPF	Boolean	`false`
`ueip_pool`	Pool de IP para la asignación de IP de UE (requiere `feature_ueip`)	CIDR String	`"10.60.0.0/24"`
`feature_ftup`	Habilitar la asignación de F-TEID por OmniUPF	Boolean	`true`
`teid_pool_start`	Inicio del rango de asignación de TEID (inclusive)	Integer	`1`
`teid_pool_end`	Fin del rango de asignación de TEID (inclusive). Los TEIDs se eligen al azar del rango y no se reutilizan de inmediato, así que mantenga el rango amplio	Integer	`0xFFFFFFFF`

Ejemplo (asignación de IP de UE) (en `runtime.exs`):

```
feature_ueip = true
ueip_pool = "10.45.0.0/16"
```

Ejemplo (asignación de F-TEID) (en `runtime.exs`):

```
feature_ftup = true
teid_pool_start = 1
teid_pool_end = 0xFFFFFFFF
```

Configuración del Gestor de Rutas

Para la sincronización de rutas de UE con el demonio FRR (Free Range Routing). Consulte la Guía de Gestión de Rutas para más detalles.

Parámetro	Descripción	Tipo	Pred
`route_manager_enabled`	Habilitar la sincronización automática de rutas de UE	Boolean	`true`
`route_manager_type`	Tipo de demonio de enrutamiento (`"frr"` o `"static"`)	String	`"frr`
`route_manager_nexthop`	Dirección del siguiente salto para las rutas de UE inyectadas (vacío = directamente conectado)	String	`""`
`route_manager_vtysh_path`	Ruta al binario `vtysh` de FRR (usado cuando `route_manager_type` es `"frr"`)	String	`"/us`
`route_manager_sync_interval_ms`	Intervalo de reconciliación completo entre rutas rastreadas y el demonio de enrutamiento (milisegundos)	Integer	`600_`
`route_batch_interval_ms`	Ventana de debounce para agrupar operaciones incrementales de	Integer	`1_00`

Parámetro	Descripción	Tipo	Pred
	añadir/quitar rutas (milisegundos)		

Ejemplo (en `runtime.exs`):

```
route_manager_enabled = true
route_manager_type = "frr"
route_manager_nexthop = ""
route_manager_vtysh_path = "/usr/bin/vtysh"
route_manager_sync_interval_ms = 600_000
route_batch_interval_ms = 1_000
```

Cuándo Habilitar:

- Despliegues Multi-UPF que requieren publicidad de rutas
- Integración con protocolos de enrutamiento OSPF o BGP
- Requiere el demonio FRRouting instalado y configurado

Configuración eBPF / XDP

Parámetro	Descripción	Tipo	Predeterminado
`xdp_interfaces`	Lista separada por comas de interfaces para XDP, o `"auto"` para todas las no-loopback	String	`"auto"`
`xdp_attach_mode`	Modo XDP: `"generic"`, `"native"` o `"offload"`	String	`"generic"`
`ebpf_pin_path`	Ruta del sistema de archivos BPF para pin	String	`"/sys/fs/bpf/upf_pipeline`
`xdp_obj_path`	Ruta al objeto eBPF compilado	String	`"/etc/omniupf/ipentrypoi`
`ebpf_backend`	Backend del mapa de dataplane: `:nif` (NIF directo, predeterminado), `:port` (proceso de puerto externo), o `:mock` (en memoria, para pruebas sin eBPF)	Atom	`:nif`

Ejemplo (en `runtime.exs`):

```
xdp_interfaces = "auto"              # o "eth0,eth1" para
interfaces específicas
xdp_attach_mode = "native"
ebpf_pin_path = "/sys/fs/bpf/upf_pipeline"
xdp_obj_path = "/etc/omniupf/ipentrypoint_bpf.o"
ebpf_backend = :nif
```

Archivo de Configuración

Archivo de Configuración de Elixir (runtime.exs)

Archivo: `/etc/omniupf/runtime.exs`

El archivo de configuración utiliza la sintaxis de Elixir con asignaciones de variables simples para facilitar la lectura. Las variables se aplican a la configuración de la aplicación al final del archivo a través de `config :upf_ex, ...`.

```
import Config

parse_ip = fn str ->
  {:ok, addr} = :inet.parse_address(String.to_charlist(str))
  addr
end

#
============================================================================
# Configuración de PFCP (N4/Sx)
#
============================================================================
pfcp_address = "10.100.50.241"       # Dirección IP para escuchar mer
PFCP
pfcp_port = 8805                      # Puerto PFCP (estándar: 8805)
node_id = "10.100.50.241"            # ID de Nodo anunciado en Config
de Asociación

#
============================================================================
# Configuración del Plano de Datos GTP-U
#
============================================================================
n3_address = "10.100.50.233"         # IP de la interfaz N3 (GTP-U ha
n9_address = n3_address               # IP de la interfaz N9 (por def
gtpu_port = 2152                      # Puerto GTP-U (estándar: 2152)
buffer_port = 22152                   # Puerto del oyente de búfer

#
============================================================================
# Configuración eBPF / XDP
#
============================================================================
xdp_interfaces = "auto"              # "auto" para todas las no-loopb
lista separada por comas
xdp_attach_mode = "native"           # Modo XDP: "generic", "native"
"offload"
ebpf_pin_path = "/sys/fs/bpf/upf_pipeline"
xdp_obj_path = "/etc/omniupf/ipentrypoint_bpf.o"

#
============================================================================
# Configuración de Sesiones y Pool de Recursos
```

```
#
================================================================================
max_sessions = 100_000
teid_pool_start = 1
teid_pool_end = 0xFFFFFFFF
far_map_size = 131_070
qer_map_size = 65_535
urr_map_size = 65_535

#
================================================================================
# Banderas de Características
#
================================================================================
feature_ueip = true
feature_ftup = true
ueip_pool = "10.45.0.0/16"

#
================================================================================
# Gestión de Rutas
#
================================================================================
route_manager_enabled = true
route_manager_type = "frr"

#
================================================================================
# Configuración de Latidos
#
================================================================================
heartbeat_interval_ms = 10_000
heartbeat_timeout_ms = 5_000
heartbeat_retries = 5

#
================================================================================
# Monitoreo de Eco de Pares GTP-U
#
================================================================================
gtp_echo_interval = 10
gtp_echo_retries = 3
gtp_peers = [
  %{address: parse_ip.("10.100.50.50"), echo: true, echo_interval: 10
```

```
]

#
# ============================================================================
# API HTTP y Registro
#
# ============================================================================
api_port = 8080
log_level = :info

#
# ============================================================================
# Aplicar Configuración (no edite debajo de esta línea)
#
# ============================================================================
config :upf_ex,
  pfcp_address: parse_ip.(pfcp_address),
  pfcp_port: pfcp_port,
  n3_address: parse_ip.(n3_address),
  n9_address: parse_ip.(n9_address),
  node_id: parse_ip.(node_id),
  api_port: api_port,
  ebpf_pin_path: ebpf_pin_path,
  xdp_obj_path: xdp_obj_path,
  interface_names: String.split(xdp_interfaces, ","),
  xdp_attach_mode: xdp_attach_mode,
  feature_ueip: feature_ueip,
  feature_ftup: feature_ftup,
  ueip_pool: ueip_pool,
  teid_pool_start: teid_pool_start,
  teid_pool_end: teid_pool_end,
  far_map_size: far_map_size,
  qer_map_size: qer_map_size,
  urr_map_size: urr_map_size,
  max_sessions: max_sessions,
  route_manager_enabled: route_manager_enabled,
  route_manager_type: route_manager_type,
  buffer_port: buffer_port,
  gtpu_port: gtpu_port,
  heartbeat_interval_ms: heartbeat_interval_ms,
  heartbeat_timeout_ms: heartbeat_timeout_ms,
  heartbeat_retries: heartbeat_retries,
  gtp_echo_interval: gtp_echo_interval,
  gtp_echo_retries: gtp_echo_retries,
```

```
  gtp_peers: gtp_peers

config :logger, level: log_level
```

Gestión del Servicio

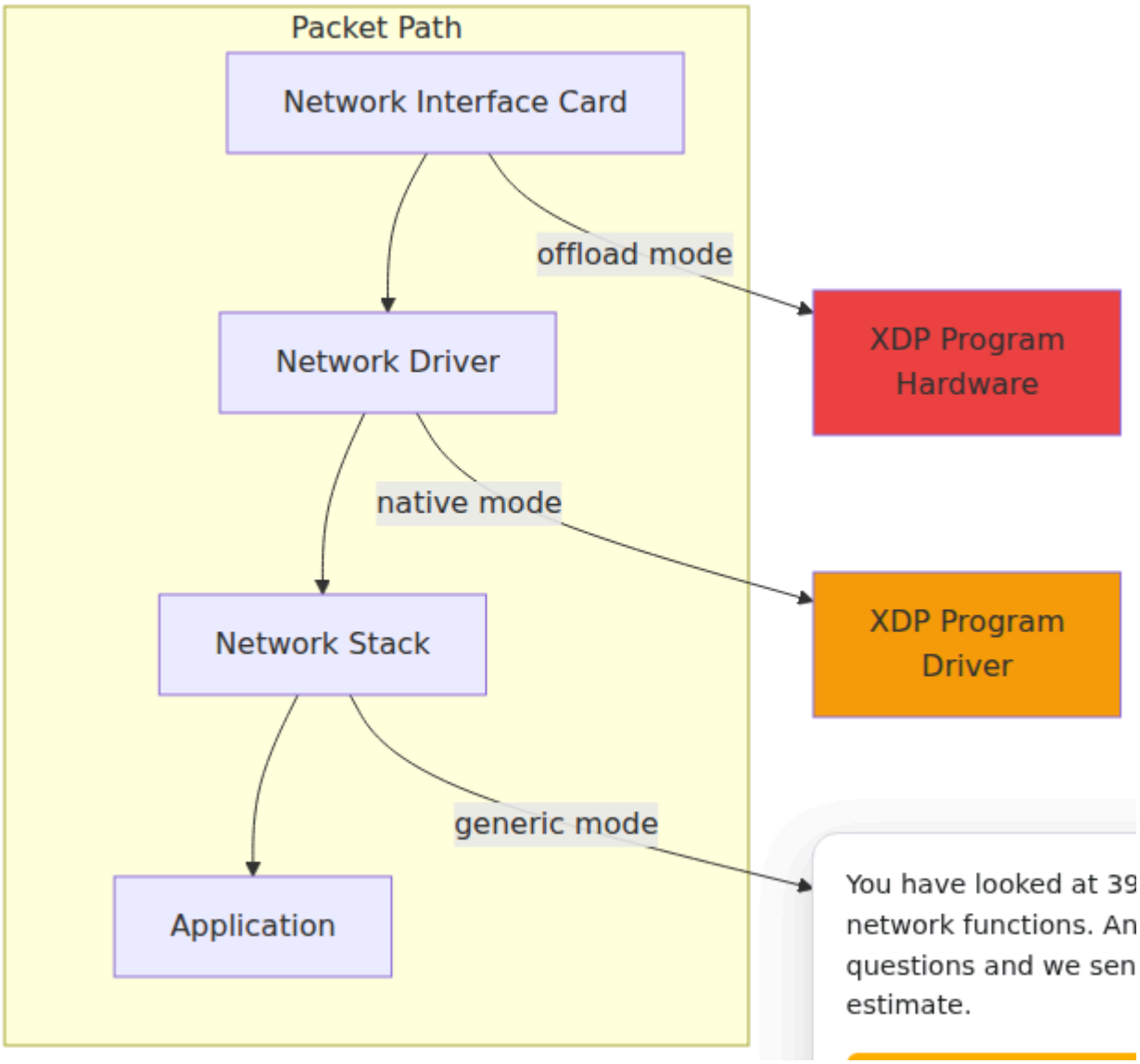
```
# Iniciar el UPF
sudo systemctl start omniupf

# Detener el UPF
sudo systemctl stop omniupf

# Reiniciar después de cambios de configuración
sudo systemctl restart omniupf

# Comprobar estado
sudo systemctl status omniupf

# Ver registros
sudo journalctl -u omniupf -f

# O usar el binario de lanzamiento directamente
sudo /opt/omniupf/bin/upf_ex start
sudo /opt/omniupf/bin/upf_ex stop
sudo /opt/omniupf/bin/upf_ex daemon   # iniciar como demonio en
segundo plano
```

Compatibilidad con Hypervisores

Descripción General

OmniUPF es compatible con todos los principales hypervisores y plataformas de virtualización. El modo de conexión XDP y la configuración de red dependen de las capacidades de red del hypervisor.

Para instrucciones paso a paso sobre cómo habilitar XDP nativo en Proxmox y otros hypervisores, consulte la Guía de Modos XDP.



Proxmox VE

Configuraciones Soportadas:

1. Modo Puente (XDP Genérico)

Caso de uso: Red estándar de VM

Configuración:

- Dispositivo de Red: VirtIO o E1000
- Modo XDP: `generic`
- Rendimiento: ~1-2 Mpps

Configuración de VM de Proxmox:

```
Dispositivo de Red: net0
Modelo: VirtIO (paravirtualizado)
Puente: vmbr0
```

Configuración de OmniUPF (en `runtime.exs`):

```
xdp_interfaces = "eth0"
xdp_attach_mode = "generic"
```

---

2. SR-IOV Passthrough (XDP Nativo)

Caso de uso: Producción de alto rendimiento

Configuración:

- Dispositivo de Red: Función Virtual SR-IOV
- Modo XDP: `native`
- Rendimiento: ~5-10 Mpps

Requisitos:

- NIC física con soporte SR-IOV (Intel X710, Mellanox ConnectX-5)
- SR-IOV habilitado en BIOS
- IOMMU habilitado (`intel_iommu=on` o `amd_iommu=on` en GRUB)

Habilitar SR-IOV en Proxmox:

```
# Editar configuración de GRUB
nano /etc/default/grub

# Agregar a GRUB_CMDLINE_LINUX_DEFAULT:
intel_iommu=on iommu=pt

# Actualizar GRUB y reiniciar
update-grub
reboot

# Habilitar VFs en NIC (ejemplo: 4 funciones virtuales en eth0)
echo 4 > /sys/class/net/eth0/device/sriov_numvfs

# Hacer persistente
echo "echo 4 > /sys/class/net/eth0/device/sriov_numvfs" >>
/etc/rc.local
chmod +x /etc/rc.local
```

Configuración de VM de Proxmox:

```
Hardware -> Agregar -> Dispositivo PCI
Seleccionar: Función Virtual SR-IOV
Todas las Funciones: No
GPU Primaria: No
PCI-Express: Sí (opcional)
```

Configuración de OmniUPF (en `runtime.exs`):

```
xdp_interfaces = "ens1f0"    # Nombre de VF SR-IOV
xdp_attach_mode = "native"
```

---

3. PCI Passthrough (XDP Nativo)

Caso de uso: NIC dedicada para una sola VM

Configuración:

- NIC física completa pasada a la VM

- Modo XDP: `native` o `offload` (si es SmartNIC)
- Rendimiento: ~5-40 Mpps (depende de la NIC)

Configuración de VM de Proxmox:

```
Hardware -> Agregar -> Dispositivo PCI
Seleccionar: NIC física (ej., 0000:01:00.0)
Todas las Funciones: Sí
GPU Primaria: No
PCI-Express: Sí
```

Configuración de OmniUPF (en `runtime.exs`):

```
xdp_interfaces = "ens1f0"
xdp_attach_mode = "native"    # o "offload" para SmartNIC
```

KVM/QEMU

Modo Puente:

```
virt-install \
  --name omniupf \
  --network bridge=br0,model=virtio \
  --disk path=/var/lib/libvirt/images/omniupf.qcow2 \
  ...
```

SR-IOV Passthrough:

```
<interface type='hostdev' managed='yes'>
  <source>
    <address type='pci' domain='0x0000' bus='0x01' slot='0x10'
function='0x1'/>
  </source>
</interface>
```

VMware ESXi

vSwitch Estándar (XDP Genérico):

- Adaptador de Red: VMXNET3
- Modo XDP: `generic`

SR-IOV (XDP Nativo):

- Habilitar SR-IOV en la configuración del host ESXi
- Agregar adaptador de red SR-IOV a la VM
- Modo XDP: `native`

Microsoft Hyper-V

Interruptor Virtual (XDP Genérico):

- Adaptador de Red: Sintético
- Modo XDP: `generic`

SR-IOV (XDP Nativo):

- Habilitar SR-IOV en el Administrador de Hyper-V
- Configurar SR-IOV en el adaptador de red virtual
- Modo XDP: `native`

VirtualBox

Modo NAT/Puente (solo XDP Genérico):

- Adaptador de Red: VirtIO-Net o Intel PRO/1000
- Modo XDP: `generic`
- Nota: VirtualBox **no** soporta SR-IOV

Compatibilidad con NIC

Comprendiendo Mpps vs Rendimiento

Los paquetes por segundo (Mpps) y el rendimiento (Gbps) no son directamente equivalentes - la relación depende completamente del tamaño del paquete. El tráfico de red móvil varía drásticamente en tamaño de paquete, desde pequeños paquetes de VoIP hasta grandes tramas de transmisión de video.

Impacto del Tamaño del Paquete en el Rendimiento

En las redes móviles, el UPF procesa paquetes encapsulados GTP-U en la interfaz N3 y paquetes IP nativos en la interfaz N6.

Sobrecarga de Encapsulación GTP-U (Interfaz N3):

- **Encabezado IPv4 externo**: 20 bytes
- **Encabezado UDP externo**: 8 bytes
- **Encabezado GTP-U**: 8 bytes
- **Total de sobrecarga GTP-U**: 36 bytes

Paquete Mínimo GTP-U (N3):

- **Encabezado IP interno**: 20 bytes (IPv4)
- **Encabezado UDP interno**: 8 bytes
- **Carga útil mínima**: 1 byte
- **Total del paquete interno**: 29 bytes
- **Más sobrecarga GTP-U**: 36 bytes
- **Tamaño total del paquete**: 65 bytes

Rendimiento a 1 Mpps con paquetes GTP-U mínimos:

```
65 bytes x 1,000,000 pps x 8 bits/byte = 520 Mbps
```

Paquete Máximo GTP-U (N3 con 1500 MTU):

- **MTU IP interno**: 1500 bytes (paquete IP interno completo)
- **Más sobrecarga GTP-U**: 36 bytes
- **Tamaño total del paquete**: 1536 bytes

Rendimiento a 1 Mpps con paquetes GTP-U máximos:

```
1536 bytes x 1,000,000 pps x 8 bits/byte = 12,288 Mbps ~ 12.3 Gbps
```

Paquetes IP Nativos (Interfaz N6):

En N6 (hacia Internet), los paquetes son IP nativos sin GTP-U:

Paquete N6 Mínimo:

- **Encabezado IP**: 20 bytes
- **Encabezado UDP**: 8 bytes
- **Carga útil mínima**: 1 byte
- **Total**: 29 bytes

Rendimiento a 1 Mpps con paquetes N6 mínimos:

```
29 bytes x 1,000,000 pps x 8 bits/byte = 232 Mbps
```

Paquete N6 Máximo (1500 MTU):

- **MTU IP**: 1500 bytes
- **Total**: 1500 bytes

Rendimiento a 1 Mpps con paquetes N6 máximos:

```
1500 bytes x 1,000,000 pps x 8 bits/byte = 12,000 Mbps = 12 Gbps
```

Ejemplos de Rendimiento en el Mundo Real

NIC Intel X710 (capacidad de 10 Mpps en la interfaz N3 con GTP-U):

Patrón de Tráfico	Tamaño de Paquete Interno	Total GTP-U	Rendimiento a 10 Mpps	Caso de Uso Típico
Llamadas VoIP (N3)	65-150 bytes	101-186 bytes	**0.8-1.5 Gbps**	Voz AMR-WB, G.711
Web ligera (N3)	400-600 bytes	436-636 bytes	**3.5-5.1 Gbps**	HTTP/HTTPS, mensajería
Móvil moderno (N3)	**1200 bytes**	**1236 bytes**	**9.9 Gbps**	**Mezcla de tráfico típica de 2024**
Transmisión de video (N3)	1400-1450 bytes	1436-1486 bytes	**11.5-11.9 Gbps**	Fragmentos de video HD/4K
MTU máxima (N3)	1500 bytes	1536 bytes	**12.3 Gbps**	Descargas grandes de TCP

En la interfaz N6 (IP nativa, sin GTP-U):

Patrón de Tráfico	Tamaño de Paquete	Rendimiento a 10 Mpps	Caso de Uso Típico
Paquetes VoIP	65-150 bytes	**0.5-1.2 Gbps**	Flujos de voz RTP
Web ligera	400-600 bytes	**3.2-4.8 Gbps**	Solicitudes HTTP
Móvil moderno	**1200 bytes**	**9.6 Gbps**	**Tráfico típico de 2024**
Transmisión de video	1400-1450 bytes	**11.2-11.6 Gbps**	Descargas de video
MTU máxima	1500 bytes	**12.0 Gbps**	Transferencias de archivos grandes

A 10 Mpps con tráfico móvil moderno (promedio de 1200 bytes), se espera un **rendimiento de ~10 Gbps** en ambas interfaces N3 y N6.

Planificación de Capacidad Práctica:

Con un tamaño de paquete promedio de 1200 bytes (típico para redes móviles modernas con transmisión de video):

Capacidad Mpps de NIC	Rendimiento N3 (GTP-U)	Rendimiento N6 (IP Nativa)	Despliegue Realista
1 Mpps	~1.0 Gbps	~1.0 Gbps	Sitio de pequeña celda, puerta de enlace IoT
5 Mpps	~4.9 Gbps	~4.8 Gbps	Sitio de celda mediana, empresa
10 Mpps	~9.9 Gbps	~9.6 Gbps	Sitio de celda grande, pequeña ciudad
20 Mpps	~19.7 Gbps	~19.2 Gbps	Área metropolitana, ciudad mediana
40 Mpps	~39.4 Gbps	~38.4 Gbps	Gran metrópoli, centro regional

---

Controladores de Red Compatibles con XDP

OmniUPF requiere controladores de red con soporte XDP para los modos **nativo** y **descarga**. El modo genérico funciona con **cualquier** NIC.

NICs Intel

Modelo	Controlador	Soporte XDP	Modo	Rendimiento
Intel X710	i40e	Sí	Nativo	~10 Mpps
Intel XL710	i40e	Sí	Nativo	~10 Mpps
Intel E810	ice	Sí	Nativo	~15 Mpps
Intel 82599ES	ixgbe	Sí	Nativo	~8 Mpps
Intel I350	igb	Limitado	Genérico	~1 Mpps
Intel E1000	e1000	No	Solo genérico	~1 Mpps

NICs Mellanox/NVIDIA

Modelo	Controlador	Soporte XDP	Modo	Rendimiento
Mellanox ConnectX-5	mlx5	Sí	Nativo	~12 Mpps
Mellanox ConnectX-6	mlx5	Sí	Nativo	~20 Mpps
Mellanox BlueField	mlx5	Sí	Nativo + Descarga	~40 Mpps
Mellanox ConnectX-4	mlx4	Limitado	Genérico	~2 Mpps

NICs Broadcom

Modelo	Controlador	Soporte XDP	Modo	Rendimiento
Broadcom BCM57xxx	bnxt_en	Sí	Nativo	~8 Mpps
Broadcom NetXtreme II	bnx2x	No	Solo genérico	~1 Mpps

Otros Proveedores

Modelo	Controlador	Soporte XDP	Modo	Rendimiento
Netronome Agilio CX	nfp	Sí	Descarga	~30 Mpps
Amazon ENA	ena	Sí	Nativo	~5 Mpps
Solarflare SFC9xxx	sfc	Sí	Nativo	~8 Mpps
VirtIO	virtio_net	Limitado	Genérico	~2 Mpps

Comprobando el Soporte XDP de NIC

Verificar si el controlador soporta XDP:

```
# Encontrar controlador de NIC
ethtool -i eth0 | grep driver

# Comprobar soporte XDP en el controlador
modinfo <driver_name> | grep -i xdp

# Ejemplo para Intel i40e
modinfo i40e | grep -i xdp
```

Verificar la conexión del programa XDP:

```
# Comprobar si el programa XDP está conectado
ip link show eth0 | grep -i xdp

# Salida de ejemplo (XDP conectado):
# 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 xdp qdisc mq
```

NICs Recomendadas por Caso de Uso

Con un tamaño de paquete promedio de 1200 bytes (tráfico móvil moderno):

Caso de Uso	NIC Recomendada	Modo	Capacidad Mpps	Rendi (N
Pruebas/Desarrollo	Cualquier NIC (VirtIO, E1000)	Genérico	1-2 Mpps	1-2 Gb
Sitio de Pequeña Celda	Intel X710, Mellanox CX-5	Nativo	5-10 Mpps	5-10 G
Celda Mediana/Metrópolis	Intel E810, Mellanox CX-6	Nativo	10-20 Mpps	10-20
Gran Metrópolis	Mellanox CX-6, Intel E810 (dual)	Nativo	20-40 Mpps	20-40
Centro Regional	Mellanox BlueField, Netronome Agilio	Descarga	40+ Mpps	40+ Gb
VM de Proxmox (Puente)	VirtIO	Genérico	1-2 Mpps	1-2 Gb
VM de Proxmox (SR-IOV)	Intel X710/E810 VF, Mellanox CX-5 VF	Nativo	5-10 Mpps	5-10 G

Recursos Adicionales

Documentación Oficial de XDP:

- Proyecto XDP
- Documentación de XDP del Kernel

Listas de Compatibilidad de NIC:

- Soporte de Hardware XDP de Cilium
- Controladores XDP de IO Visor

Ejemplos de Configuración

Ejemplo 1: Entorno de Desarrollo (Modo Genérico)

Escenario: Pruebas de OmniUPF en laptop o VM sin SR-IOV

```
# Configuración de desarrollo (/etc/omniupf/runtime.exs)
xdp_interfaces = "eth0"
xdp_attach_mode = "generic"
api_port = 8080
pfcp_address = "127.0.0.1"
pfcp_port = 8805
node_id = "127.0.0.1"
n3_address = "127.0.0.1"
log_level = :debug
max_sessions = 1_000
```

Ejemplo 2: Producción Bare Metal (Modo Nativo)

Escenario: UPF de producción en servidor bare metal con NIC Intel X710

```
# Configuración bare metal de producción
(/etc/omniupf/runtime.exs)
xdp_interfaces = "ens1f0,ens1f1"    # N3 en ens1f0, N6 en ens1f1
xdp_attach_mode = "native"
api_port = 8080
pfcp_address = "10.100.50.241"
pfcp_port = 8805
node_id = "10.100.50.241"
n3_address = "10.100.50.233"
n9_address = "10.100.50.234"
log_level = :info
max_sessions = 500_000
gtp_echo_interval = 30
gtp_peers = [
  %{address: parse_ip.("10.100.50.10"), echo: true, echo_interval:
30},
  %{address: parse_ip.("10.100.50.11"), echo: true, echo_interval:
30},
]
heartbeat_interval_ms = 10_000
feature_ueip = true
ueip_pool = "10.45.0.0/16"
```

Ejemplo 3: VM de Proxmox con SR-IOV (Modo Nativo)

Escenario: UPF de producción en VM de Proxmox con passthrough SR-IOV

```
# Configuración SR-IOV de Proxmox (/etc/omniupf/runtime.exs)
xdp_interfaces = "ens1f0"           # VF SR-IOV
xdp_attach_mode = "native"
api_port = 8080
pfcp_address = "192.168.100.10"
pfcp_port = 8805
node_id = "192.168.100.10"
n3_address = "192.168.100.10"
log_level = :info
max_sessions = 100_000
gtp_echo_interval = 15
gtp_peers = [
  %{address: parse_ip.("192.168.100.50"), echo: true},
]
```

Ejemplo 4: Modo PGW-U (EPC 4G)

Escenario: OmniUPF actuando como PGW-U en red EPC 4G

```
# Configuración PGW-U (/etc/omniupf/runtime.exs)
xdp_interfaces = "eth0"
xdp_attach_mode = "native"
api_port = 8080
pfcp_address = "10.200.1.10"
pfcp_port = 8805
node_id = "10.200.1.10"
n3_address = "10.200.1.10"          # Interfaz S5/S8 (GTP-U)
log_level = :info
max_sessions = 200_000
gtp_echo_interval = 20
gtp_peers = [
  %{address: parse_ip.("10.200.1.50"), echo: true, echo_interval:
20},
]
heartbeat_interval_ms = 5_000
```

Ejemplo 5: Múltiples Modos (UPF + PGW-U Simultáneamente)

Escenario: OmniUPF sirviendo tanto redes 5G como 4G simultáneamente

```
# Configuración de múltiples modos (/etc/omniupf/runtime.exs)
xdp_interfaces = "eth0,eth1"
xdp_attach_mode = "native"
api_port = 8080
pfcp_address = "10.50.1.100"
pfcp_port = 8805
node_id = "10.50.1.100"
n3_address = "10.50.1.100"
n9_address = "10.50.1.101"
log_level = :info
max_sessions = 300_000
gtp_echo_interval = 15
gtp_peers = [
  %{address: parse_ip.("10.50.2.10"), echo: true, echo_interval:
15},
  %{address: parse_ip.("10.50.2.20"), echo: true, echo_interval:
15},
]
heartbeat_interval_ms = 10_000
feature_ueip = true
ueip_pool = "10.60.0.0/16"
```

Ejemplo 6: Modo de Descarga de SmartNIC

Escenario: Despliegue de ultra-alto rendimiento con Netronome Agilio CX SmartNIC

```
# Configuración de descarga de SmartNIC (/etc/omniupf/runtime.exs)
xdp_interfaces = "enp1s0np0"        # Interfaz SmartNIC
xdp_attach_mode = "offload"
api_port = 8080
pfcp_address = "10.10.1.50"
pfcp_port = 8805
node_id = "10.10.1.50"
n3_address = "10.10.1.50"
log_level = :warning
max_sessions = 1_000_000
far_map_size = 2_000_000
qer_map_size = 1_000_000
gtp_echo_interval = 30
gtp_peers = [
  %{address: parse_ip.("10.10.2.10"), echo: true},
  %{address: parse_ip.("10.10.2.20"), echo: true},
  %{address: parse_ip.("10.10.2.30"), echo: true},
]
heartbeat_interval_ms = 15_000
```

Dimensionamiento de Mapas y Planificación de Capacidad

Configuración de Tamaños de Mapas

Establezca `max_sessions` y configure los tamaños de mapa para su despliegue:

```
max_sessions = 100_000
far_map_size = 131_070
qer_map_size = 65_535
```

Uso de memoria: ~91 MB para 100K sesiones

Estimación de Capacidad

Calcular sesiones máximas:

```
Max Sessions = min(
  pdr_map_size / 2,
  far_map_size / 2,
  qer_map_size
)
```

Ejemplo:

- Mapa PDR: 200,000
- Mapa FAR: 200,000
- Mapa QER: 100,000

Max Sessions = min(100,000, 100,000, 100,000) = **100,000**

Requisitos de Memoria

Uso de memoria por sesión:

- PDR: 2 x 212 B = 424 B
- FAR: 2 x 20 B = 40 B
- QER: 1 x 36 B = 36 B
- URR: 2 x 20 B = 40 B
- **Total**: ~540 B por sesión

Para 100K sesiones: ~52 MB de memoria del kernel

Recomendación: Asegúrese de que el límite de memoria bloqueada permita 2x el uso estimado:

```
# Comprobar límite actual
ulimit -l

# Establecer ilimitado (requerido para eBPF)
ulimit -l unlimited
```

Documentación Relacionada

- **Guía de Arquitectura** - detalles técnicos de eBPF/XDP y optimización del rendimiento
- **Guía de Gestión de Reglas** - configuración de PDR, FAR, QER, URR
- **Guía de Monitoreo** - estadísticas, monitoreo de capacidad y alertas
- **Referencia de Métricas** - referencia completa de métricas de Prometheus
- **Guía de Interfaz Web** - operaciones del panel de control
- **Guía de Operaciones** - visión general de la arquitectura y despliegue del UPF
- **Guía de Jardín Amurallado** - redirección fuera de crédito, portal cautivo y configuración de lista blanca

IPv6 / Doble Pila en el Plano de Usuario

Cómo el OmniUPF maneja el tráfico de usuario IPv6 para sesiones PDN IPv6 e IPv4v6: los requisitos previos del kernel, el grupo de direcciones UE, la programación del enlace descendente IPv6 desde PFCP y la publicidad de rutas de host UE a la red a través de OSPFv3.

Esta página cubre las responsabilidades del **plano de usuario**. El plano de control (negociación de tipo PDN, PAA, Gx y señalización de la dirección IPv6 del UE al UPF a través de PFCP) es manejado por el SMF/PGW-C. Consulte también Gestión de Rutas y la Guía de Configuración.

Tabla de Contenidos

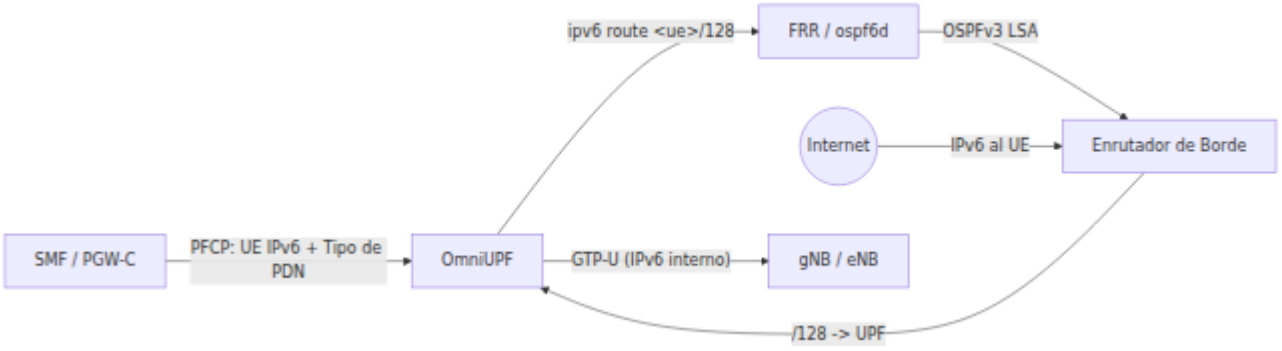
- Descripción General
- Requisitos Previos del Kernel
- Grupo de Direcciones IPv6 del UE
- Publicidad de Rutas OSPFv3
- Comportamiento del Plano de Datos
- Resolución de Problemas

Descripción General

Cuando se establece una sesión PDN IPv6 (o IPv4v6), el SMF/PGW-C envía la dirección IPv6 del UE y el tipo de PDN al UPF a través de PFCP. El UPF luego:

1. Programa la **búsqueda de enlace descendente IPv6** para que los paquetes destinados al UE sean emparejados y tunelados.
2. Agrega una **ruta de host** `/128` para la dirección del UE y la publicita al enrutador de borde a través de **OSPFv3**, de modo que el tráfico de enlace descendente sea atraído a este UPF.

3. Reenvía el tráfico de usuario en ambas direcciones (decapsulación de enlace ascendente, encapsulación GTP-U de enlace descendente) para paquetes internos IPv6.



Requisitos Previos del Kernel

IPv6 debe estar habilitado y el reenvío activado a nivel de host. Aplique a través de un sysctl drop-in (por ejemplo, bajo `/etc/sysctl.d/`).

Configuración	Valor requerido	Descripción
`net.ipv6.conf.all.disable_ipv6`	`0`	IPv6 debe estar habilitado. La interfaz del plano de datos del UPF necesita una dirección IPv6 global para tránsito y enrutamiento.
`net.ipv6.conf.default.disable_ipv6`	`0`	Asegura que IPv6 permanezca habilitado en interfaces que aparecen nuevas.
`net.ipv6.conf.all.forwarding`	`1`	Habilita el reenvío de IPv6 para que el tráfico de enlace ascendente del UE salga y el tráfico de enlace descendente se enrute al plano de datos.

La interfaz del plano de datos también necesita una dirección IPv6 global en el segmento de tránsito (hacia el enrutador de borde) para que OSPFv3 forme una adyacencia e intercambie rutas.

Grupo de Direcciones IPv6 del UE

Cuando el UPF asigna direcciones UE (en lugar de recibirlas del SMF), configure un grupo IPv6 en `runtime.exs`. Cuando el SMF/PGW-C proporciona la dirección

del UE a través de PFCP, esa dirección se utiliza directamente y este grupo no se consulta para la sesión.

```
# /etc/omniupf/runtime.exs
config :upf_ex,
  ueip_pool: "2001:db8:6f85:70::/64"
```

Parámetro	Tipo	Requerido	Predeterminado	Descripción
`ueip_pool`	String (CIDR)	No	-	Grupo de IP del UE utilizado cuando el UPF realiza la asignación de direcciones. Acepta un CIDR IPv4 o IPv6; la familia de direcciones se detecta a partir de la cadena.

Publicidad de Rutas OSPFv3

Cada dirección IPv6 activa del UE se instala como una ruta de host `/128` y se publicita al enrutador de borde, reflejando el comportamiento de IPv4 `/32`. Las rutas son gestionadas por el gestor de rutas y redistribuidas en OSPF por FRR.

```
# /etc/omniupf/runtime.exs
config :upf_ex,
  route_manager_enabled: true,
  route_manager_type: "frr"
```

Parámetro	Tipo	Requerido	Predeterminado	De
`route_manager_enabled`	Booleano	No	`false`	Ha ge rut UE `tr` pu rut
`route_manager_type`	String	No	-	Ba rut iny a t FR el es uti dir los co de ke `ip` Us pa pu de

La instancia de FRR debe ejecutar **OSPFv3** (`ospf6d`) en la interfaz de tránsito y redistribuir rutas estáticas, de modo que las rutas de host `/128` del UE se inunden al enrutador de borde. Las rutas de host IPv6 se agregan con el comando `ipv6 route <addr>/128`

- el comando IPv4 `ip route` no acepta prefijos IPv6. Consulte Gestión de Rutas para el ciclo de vida del gestor de rutas.

Comportamiento del Plano de Datos

Dirección	Comportamiento
Enlace descendente (red → UE)	El destino interno IPv6 se empareja con la tabla de enlace descendente IPv6 programada desde la sesión PFCP; los paquetes coincidentes son encapsulados en GTP-U hacia el gNB/eNB (o se almacenan en búfer si la acción de la regla es BUFF).
Enlace ascendente (UE → red)	GTP-U se decapsula y el paquete interno IPv6 se reenvía por la interfaz N6 utilizando la FIB IPv6 del kernel (de ahí el sysctl de reenvío).
Almacenamiento en búfer (BUFF)	Los paquetes de enlace descendente IPv6 almacenados en búfer se entregan al oyente de búfer de espacio de usuario y se vacían en la transición a reenvío, igual que con IPv4.

No se requiere relajación de `accept_local` / filtro de ruta inversa en las versiones actuales; la ruta de búfer utiliza una fuente externa no local, por lo que los paquetes no se descartan como martianos.

Resolución de Problemas

El tráfico de enlace descendente IPv6 no llega al UE

Síntomas: La sesión está establecida y el enlace ascendente funciona, pero el tráfico de la red al UE se descarta.

Causas posibles:

- La ruta de host `/128` del UE no se publicita (gestor de rutas deshabilitado, o OSPFv3 no ejecutándose en el UPF).
- La adyacencia OSPFv3 entre el UPF y el enrutador de borde no está establecida.
- El enrutador de borde aún no ha instalado el `/128` (retraso de convergencia).

Resolución:

1. Confirme `route_manager_enabled: true` y `route_manager_type: "frr"`.
2. Verifique que la instancia de FRR del UPF ejecute OSPFv3 en la interfaz de tránsito y redistribuya rutas estáticas.
3. Confirme que la adyacencia OSPFv3 esté completa y que el enrutador de borde muestre el `/128` del UE aprendido a través de OSPF.

El tráfico de usuario IPv6 no se reenvía en absoluto

Síntomas: Ni el enlace ascendente ni el enlace descendente IPv6 funcionan, incluso con rutas presentes.

Causas posibles:

- IPv6 está deshabilitado en el host, o el reenvío está apagado.
- La interfaz del plano de datos no tiene una dirección IPv6 global.

Resolución:

1. Verifique los requisitos previos del kernel (`disable_ipv6=0`, `forwarding=1`).
2. Confirme que la interfaz del plano de datos tenga una dirección IPv6 global en el segmento de tránsito.

Referencia de Métricas

Este documento describe todas las métricas de Prometheus expuestas por OmniUPF en el endpoint `/api/metrics` (la API HTTP se ejecuta en `api_port`, por defecto `8080`). Tenga en cuenta el prefijo `/api` - cada ruta de API se sirve bajo él.

Los nombres, tipos y etiquetas de las métricas a continuación reflejan las métricas que OmniUPF expone.

Categorías de Métricas

1. **Métricas PFCP** - contadores de mensajes de plano de control, asociaciones, sesiones y errores
2. **Métricas del ciclo de vida de la sesión** - contadores de creación/eliminación/modificación de sesiones y latencia de establecimiento
3. **Métricas de ruta lenta y almacenamiento en búfer del espacio de usuario** - contadores de punteo para almacenamiento en búfer de enlace descendente, jardín amurallado y notificaciones de error de TEID desconocido
4. **Métricas de Informe de Datos de Enlace Descendente (DLDR)** - notificaciones de solicitudes de informe de sesión PFCP y seguimiento del índice FAR
5. **Métricas GTP-U** - respuestas de eco y contadores de indicaciones de error
6. **Métricas URR** - contadores de informes de uso y temporizadores URR activos
7. **Métricas de mapa eBPF** - medidores de entradas de mapa de plano de datos
8. **Rendimiento del plano de datos** - contadores `_total` por dirección (N3/N6), controlados por `expose_xdp_metrics` (#57); también a demanda a través de `/api/v1/xdp_stats`
9. **Métricas de recursos / enrutamiento** - medidores de grupo de TEID/FAR-ID y rutas de UE

10. **Métricas de Jardín Amurallado** - intercepción de portal cautivo, reenvío y contadores de suplantación de DNS

Métricas PFCP

Contadores de protocolo de plano de control entre el UPF y sus pares PFCP (SMF / PGW-C / SGW-C).

Nombre de Métrica	Tipo	Etiquetas	D
`upf_pfcp_associations`	Gauge	none	Asociacior actualmer los pares)
`upf_pfcp_sessions`	Gauge	none	Sesiones F activas (to
`upf_pfcp_peer_restarts_total`	Counter	`peer`	Deteccion pares (car tiempo de
`upf_pfcp_duplicate_requests_total`	Counter	none	Solicitudes detectada
`upf_orphaned_sessions_deleted_total`	Counter	none	Sesiones e resultado par
`upf_pfcp_messages_rx_total`	Counter	`type`, `peer`	Mensajes tipo de me
`upf_pfcp_messages_tx_total`	Counter	`type`, `peer`	Mensajes tipo de me
`upf_pfcp_errors_total`	Counter	`type`	Rechazos PFCP, etiq causa del ejemplo, `session_c` `mandatory`

Métricas del ciclo de vida de la sesión

Nombre de Métrica	Tipo	Etiquet
`upf_sessions_created_total`	Counter	none
`upf_sessions_deleted_total`	Counter	none
`upf_sessions_modified_total`	Counter	none
`upf_session_establishment_duration_microseconds`	Histogram	none

Métricas de ruta lenta y almacenamiento en búfer del espacio de usuario

El plano de datos eBPF envía paquetes al camino lento del espacio de usuario (puerto UDP `22152`, por defecto) para tres trabajos distintos: **almacenamiento en búfer de enlace descendente** cuando un UE está inactivo (retenido hasta que se pague al UE), **redirección de jardín amurallado**, y responder a **G-**

PDUs de enlace ascendente de TEID desconocido con una Indicación de Error GTP-U. Solo las métricas `buffered`/`flushed`/`current` a continuación describen el búfer propiamente dicho; el jardín amurallado tiene sus propias métricas `upf_walled_garden_*` y el TEID desconocido se cuenta como `upf_gtpu_error_indications_sent_total`.

Nombre de Métrica	Tipo	Etiquetas	D
`upf_userspace_punt_received_total`	Counter	none	Todos los p al camino de usuario en búfer + + TEID de
`upf_gtpu_oversize_punted_total`	Counter	none	Paquetes descender excesivo (encapsula MTU de sa espacio de el kernel f paquete e crecimient significa q está envia tamaño co camino le `gtpu_over`
`upf_buffer_packets_buffered_total`	Counter	none	Paquetes al búfer
`upf_buffer_packets_flushed_total`	Counter	none	Paquetes
`upf_buffer_packets_dropped_total`	Counter	`reason`	Paquetes admitidos
`upf_buffer_packets_current`	Gauge	none	Paquetes retenidos
`upf_buffer_flush_operations_total`	Counter	none	Operacion búfer exit vaciado d

Nombre de Métrica	Tipo	Etiquetas	D
`upf_buffer_flush_packets_sent_total`	Counter	none	Paquetes operacion
`upf_buffer_flush_errors_total`	Counter	`reason`	Operacion búfer falli

Valores de `reason` de `upf_buffer_packets_dropped_total` (de descartes de agregar al búfer y errores de oyente de búfer):

- `global_limit` - capacidad total del búfer (`buffer_max_total`) alcanzada
- `far_limit` - límite de búfer por FAR (`buffer_max_per_far`) alcanzado
- `expired` - TTL (`buffer_ttl_ms`) excedido antes del vaciado
- `read_error` - error al leer desde el socket del búfer
- `too_small` - paquete demasiado pequeño para un encabezado GTP
- `invalid_gtp_type` - tipo de mensaje GTP no G-PDU
- `not_buffering_far` - FAR no tiene una acción BUFF
- `error_indication_failed` - no se pudo enviar la Indicación de Error GTP-U para un enlace ascendente de TEID desconocido

> El enlace ascendente de TEID desconocido **no** es un descarte de búfer: se responde con una Indicación de Error GTP-U y se cuenta mediante `upf_gtpu_error_indications_sent_total` (una respuesta correcta del camino lento, no pérdida de paquetes).

Valores de `reason` de `upf_buffer_flush_errors_total`:

- `far_lookup_failed` - no se pudo buscar información de FAR en el mapa eBPF
- `no_forw_action` - FAR no tiene una acción FORW configurada
- `connection_failed` - no se pudo abrir un socket UDP para el vaciado

Métricas de Informe de Datos de Enlace Descendente (DLDR)

Métricas para notificaciones de solicitudes de informe de sesión PFCP enviadas al plano de control cuando los paquetes de enlace descendente están almacenados en búfer. Estas notificaciones activan al SMF/PGW-C para que pague al UE.

Nombre de Métrica	Tipo	Etiquetas	Descripción
`upf_dldr_sent_total`	Counter	`peer`	Informes de Datos de Enlace Descendente enviados, etiquetados por la dirección SMF/PGW-C
`upf_dldr_errors_total`	Counter	none	Errores de codificación / envío de DLDR
`upf_dldr_skipped_total`	Counter	none	DLDR omitidos porque el FAR ya fue notificado
`upf_far_index_size`	Gauge	none	FARs registrados en el FarIndex para notificación DLDR

Métricas GTP-U

Contadores de gestión de ruta GTP-U e Indicación de Error. Las Indicaciones de Error se intercambian cuando un par recibe paquetes para un TEID desconocido (típicamente después de un reinicio).

Nombre de Métrica	Tipo	Etiquetas	
`upf_gtpu_echo_responses_tx_total`	Counter	none	R o e
`upf_gtpu_error_indications_sent_total`	Counter	none	I o U (e o
`upf_gtpu_error_indications_rx_total`	Counter	none	I o U p
`upf_error_indication_sessions_deleted_total`	Counter	none	S e o r u I E

Cuando se envían Indicaciones de Error: el UPF recibe un paquete GTP-U para un TEID que no existe (por ejemplo, después de un reinicio, o la sesión ya fue eliminada), e informa al remitente que se detenga.

Cuando se reciben Indicaciones de Error: un par aguas abajo no reconoce un TEID al que el UPF reenvió; el UPF elimina la sesión afectada para dejar de reenviar a un túnel muerto.

Métricas URR (Regla de Informe de Uso)

Nombre de Métrica	Tipo	Etiquetas	Descripción
`upf_urr_reports_sent_total`	Counter	`trigger`	Informes de uso URR enviados, etiquetados por el desencadenante de informe
`upf_urr_report_errors_total`	Counter	none	Errores de codificación / envío de informes URR
`upf_urr_active_timers`	Gauge	none	Temporizadores URR activos (periódicos / umbral de tiempo / validez de cuota)

`trigger` refleja el desencadenante de informe URR que se activó - por ejemplo, `periodic` (PERIO), `volume_threshold` (VOLTH), `time_threshold` (TIMTH), `quota_validity` (QUVTI).

Los contadores de bytes por URR no se exportan como métricas de Prometheus (para evitar alta cardinalidad). Lea estadísticas individuales de URR a través de la API REST en `/api/v1/urr_map`.

Métricas de mapa eBPF

Medidores para la utilización del mapa de plano de datos, actualizados en cada raspado.

Nombre de Métrica	Tipo	Etiquetas	Descripción
`upf_ebpf_far_entries`	Gauge	none	Entradas FAR en el mapa eBPF
`upf_ebpf_pdr_uplink_entries`	Gauge	none	Entradas PDR de enlace ascendente en el mapa eBPF (PDRs con un TEID)
`upf_ebpf_pdr_downlink_entries`	Gauge	none	Entradas PDR de enlace descendente en el mapa eBPF (PDRs indexados por IP de UE)

`upf_ebpf_far_entries` refleja el grupo de id-FAR asignados (`upf_far_ids_allocated`), ya que el far_map contiene una entrada por cada id-FAR asignado. Los medidores de PDR se agregan del estado de sesión en vivo en cada raspado (el costo es O(total de sesiones)).

Rendimiento del plano de datos (N3/N6)

Contadores de paquetes y bytes por dirección para tráfico de plano de usuario (**N3** = lado GTP-U hacia el gNB/eNB; **N6** = lado SGi hacia la red de datos) provienen del mapa percpu `upf_ext_stat` de eBPF.

Nombre de Métrica	Tipo	Etiquetas	Descripción
`upf_n3_rx_packets_total` / `upf_n3_tx_packets_total`	Counter	none	Paquetes N3 (GTP-U) entrantes / salientes del camino de datos XDP
`upf_n6_rx_packets_total` / `upf_n6_tx_packets_total`	Counter	none	Paquetes N6 (SGi) entrantes / salientes del camino de datos XDP
`upf_n3_rx_bytes_total` / `upf_n3_tx_bytes_total`	Counter	none	Bytes N3 (GTP-U) entrantes / salientes
`upf_n6_rx_bytes_total` / `upf_n6_tx_bytes_total`	Counter	none	Bytes N6 (SGi) entrantes / salientes
`upf_xdp_ttl_exceeded_total`	Counter	none	Paquetes descartados porque su TTL IPv4 / Límite de Salto IPv6 era 1 o menos cuando el UPF estaba a punto de reenviarlos. Cualquier tasa sostenida indica un bucle de reenvío

Controlado por `expose_xdp_metrics` (issue #57). Leer `upf_ext_stat` en la ruta de solicitud (por cada raspado de Prometheus) ha demostrado activar un **TX-ring wedge** genérico-XDP de `virtio_net`. Se aplican dos mitigaciones: la lectura se realiza fuera de la ruta de solicitud por el `Sampler` en segundo plano (en un intervalo fijo, nunca en un raspado), y está controlada por `config :upf_ex, expose_xdp_metrics: true`. Cuando está deshabilitado, estos contadores no se declaran ni se exportan.

Estos son contadores acumulativos `_total` **Counters**. El mapa subyacente `upf_ext_stat` está fijado, por lo que sobrevive a un reinicio de omniupf pero se reinicia en un redepliegue de eBPF `.o`; el colector traduce su valor absoluto en incrementos de contador monótonos para que `rate()` se mantenga correcto en ambos casos. No los lea como medidores. Use `rate()`.

JSON a demanda: `GET /api/v1/xdp_stats` devuelve los mismos campos y solo toca eBPF cuando lo llama explícitamente. Campos: `rx_n3` / `tx_n3` / `rx_n6` / `tx_n6` (paquetes) y `rx_n3_bytes` / `tx_n3_bytes` / `rx_n6_bytes` / `tx_n6_bytes`, además de `ttl_exceeded`.

TTL / Límite de Salto. El plano de datos envejece cada paquete que reenvía por un salto: el TTL IPv4 del paquete de usuario / Límite de Salto IPv6 en la desencapsulación (enlace ascendente hacia N6) y en la encapsulación (enlace descendente hacia el RAN), y el TTL del encabezado GTP-U externo en un relevo de GTP-U a GTP-U (SGW-U). Un paquete que llega sin nada más que gastar se descarta y se cuenta en `ttl_exceeded`, por lo que un bucle de reenvío entre UPFs se apaga y aparece como una tasa creciente de `upf_xdp_ttl_exceeded_total` en lugar de como un rendimiento descontrolado.

Métricas de recursos / enrutamiento

Nombre de Métrica	Tipo	Etiquetas	Descripción
`upf_routes_total`	Gauge	none	Rutas IP de UE actualmente rastreadas por el administrador de rutas
`upf_teid_allocated`	Gauge	none	TEIDs actualmente asignados del grupo
`upf_far_ids_allocated`	Gauge	none	IDs de FAR actualmente asignados del grupo

Métricas de Jardín Amurallado

Contadores para el jardín amurallado de crédito agotado / portal cautivo. Consulte la Guía del Jardín Amurallado para el comportamiento.

Nombre de Métrica	Tipo	Etiquetas	D
`upf_walled_garden_active_redirects`	Gauge	none	S r d a a
`upf_walled_garden_packets_intercepted_total`	Counter	none	P i p a
`upf_walled_garden_packets_dropped_total`	Counter	none	P d p a
`upf_walled_garden_packets_forwarded_total`	Counter	`dst_ip`	P l b r p d
`upf_walled_garden_bytes_forwarded_total`	Counter	`dst_ip`	B l r p d
`upf_walled_garden_dns_spoofed_total`	Counter	`domain`	C D s a d

Nombre de Métrica	Tipo	Etiquetas	E
`upf_walled_garden_dns_forwarded_total`	Counter	`domain`	C D r (l b o

> **Nota de cardinalidad.** Las etiquetas `dst_ip` y `domain` son ilimitadas. Mantenga la lista blanca ajustada y agregue estas etiquetas en reglas de grabación si raspa un jardín amurallado ocupado.

Uso de Métricas de Prometheus

Accediendo a las Métricas

Las métricas se exponen en el endpoint `/api/metrics` del servidor de API HTTP, que escucha en `api_port` (por defecto `8080`). Tenga en cuenta el prefijo `/api` - cada ruta de API se sirve bajo él:

```
# Ver métricas en bruto
curl http://localhost:8080/api/metrics

# Ejemplo de salida
upf_pfcp_sessions 42
upf_pfcp_associations 2
upf_dldr_sent_total{peer="10.100.50.241"} 17
```

Configuración de Prometheus

Agregue el objetivo OmniUPF a su `prometheus.yml`:

```
scrape_configs:
  - job_name: 'omniupf'
    metrics_path: /api/metrics
    static_configs:
      - targets: ['localhost:8080']
```

Paneles de Grafana

Paneles útiles para construir a partir de estas métricas:

- Conteos de sesiones y asociaciones (`upf_pfcp_sessions`, `upf_pfcp_associations`)
- El rendimiento N3/N6 por dirección está disponible a demanda a través de `/api/v1/xdp_stats` (eliminado del raspado, vea #57)
- Presión del búfer (`upf_buffer_packets_current`, tasa de descartes por `reason`)
- Actividad DLDR / de paginación (`rate(upf_dldr_sent_total[5m])`)
- Tasas de Indicación de Error y reinicio de pares para alertas de salud del túnel

Documentación Relacionada

- **Guía de Monitoreo** - Monitoreo de estadísticas, planificación de capacidad y alertas
- **Guía de Configuración** - Configurar `api_port`, ajuste de búfer y otras opciones de UPF
- **Guía de Interfaz Web** - Ver métricas en la página de Estadísticas
- **Guía de Arquitectura** - Ruta de datos eBPF y optimización del rendimiento
- **Guía de Gestión de Reglas** - Comprensión de métricas PDR, FAR, QER, URR
- **Guía del Jardín Amurallado** - Comportamiento de redirección de portal cautivo y lista blanca
- **Guía de Solución de Problemas** - Uso de métricas para diagnósticos

Guía de Monitoreo

Tabla de Contenidos

1. Descripción General
2. Monitoreo de Estadísticas
3. Monitoreo de Capacidad
4. Métricas de Rendimiento
5. Alertas y Umbrales
6. Planificación de Capacidad
7. Resolución de Problemas de Rendimiento

Descripción General

El monitoreo efectivo de OmniUPF es crítico para mantener la calidad del servicio, prevenir el agotamiento de capacidad y resolver problemas de rendimiento. OmniUPF proporciona métricas en tiempo real completas a través de su interfaz web y API REST.

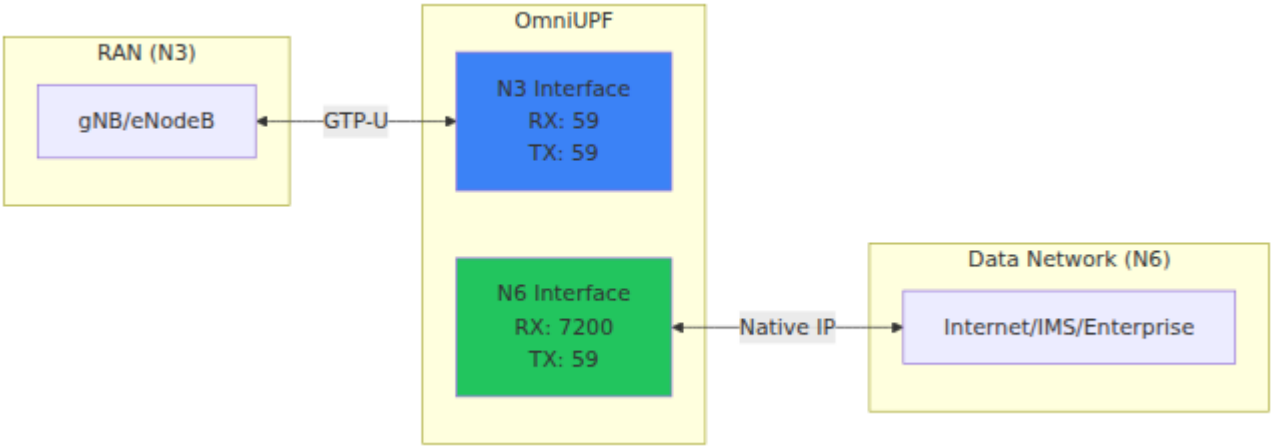
Categorías de Monitoreo

Categoría	Propósito	Frecuencia de Actualización	Métricas Clave
Estadísticas de Paquetes	Rastrear tasas de procesamiento de paquetes y errores	En tiempo real	Paquetes RX/TX, caídas, desglose de protocolos
Estadísticas de Interfaz	Monitorear la distribución de tráfico N3/N6	En tiempo real	N3 RX/TX, N6 RX/TX
Estadísticas de XDP	Rastrear el rendimiento del datapath del kernel	En tiempo real	XDP procesados, pasados, descartados, abortados
Estadísticas de Rutas	Monitorear decisiones de enrutamiento de paquetes	En tiempo real	Búsquedas FIB, aciertos/fallos de caché
Capacidad del Mapa eBPF	Prevenir el agotamiento de recursos	Cada 10s	Porcentajes de uso de mapas, usado vs. capacidad
Estadísticas de Buffers	Rastrear el almacenamiento de paquetes durante la movilidad	Cada 5s	Paquetes almacenados, edad del buffer, conteo de FAR

Monitoreo de Estadísticas

Estadísticas de Interfaz N3/N6

Las estadísticas de la interfaz N3/N6 proporcionan visibilidad sobre la distribución del tráfico entre la RAN (N3) y la Red de Datos (N6).



Métricas:

- **RX N3**: Paquetes recibidos de la RAN (tráfico GTP-U de enlace ascendente)
- **TX N3**: Paquetes transmitidos a la RAN (tráfico GTP-U de enlace descendente)
- **RX N6**: Paquetes recibidos de la Red de Datos (IP nativa de enlace descendente)
- **TX N6**: Paquetes transmitidos a la Red de Datos (IP nativa de enlace ascendente)
- **Total**: Conteo agregado de paquetes a través de todas las interfaces

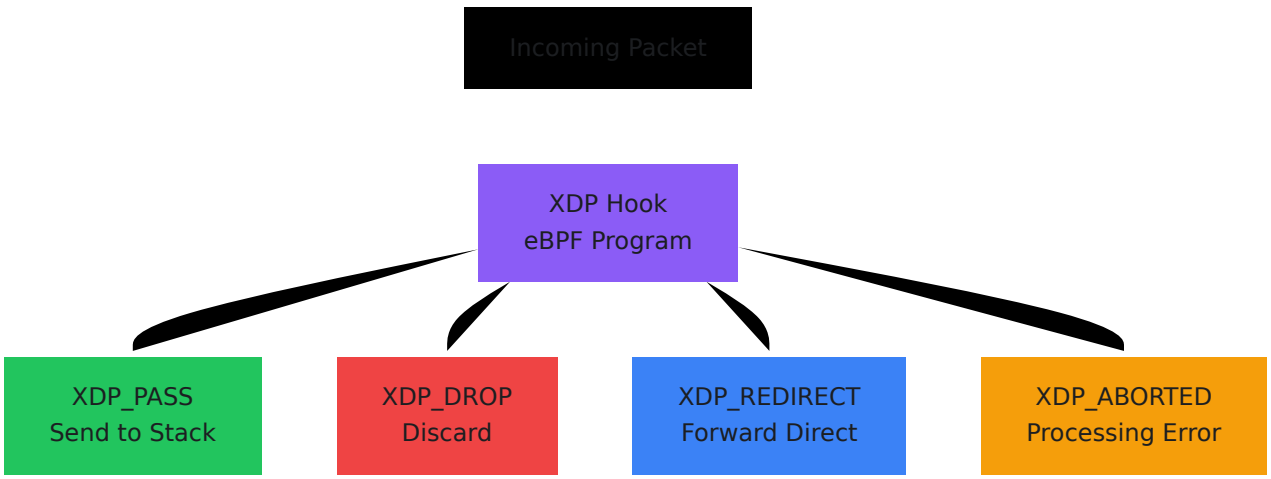
Comportamiento Esperado:

- **RX N3 ≈ TX N6**: Los paquetes de enlace ascendente fluyen de la RAN a la Red de Datos
- **RX N6 ≈ TX N3**: Los paquetes de enlace descendente fluyen de la Red de Datos a la RAN
- Un desequilibrio significativo puede indicar:
  - Tráfico asimétrico (descargas >> cargas)
  - Caídas de paquetes o errores de reenvío

- Errores de configuración de enrutamiento

Estadísticas de XDP

Las estadísticas de XDP (eXpress Data Path) muestran el rendimiento del procesamiento de paquetes a nivel de kernel.



Métricas:

- **Abortados**: El programa XDP encontró un error (debería ser siempre 0)
- **Descartar**: Paquetes descartados intencionalmente por el programa XDP
- **Pasar**: Paquetes pasados a la pila de red para un procesamiento adicional
- **Redirigir**: Paquetes redirigidos directamente a la interfaz de salida
- **TX**: Paquetes transmitidos a través de XDP

Interpretación:

- **Abortados > 0**: Problema crítico con el programa eBPF o compatibilidad del kernel
- **Descartar > 0**: Descargas basadas en políticas o paquetes inválidos
- **Pasar alto**: La mayoría de los paquetes procesados en la pila de red (normal)
- **Redirigir alto**: Paquetes reenviados directamente (rendimiento óptimo)

Estadísticas de Paquetes

Desglose detallado del protocolo de paquetes y contadores de procesamiento.

Contadores de Protocolo:

- **RX ARP**: Paquetes del Protocolo de Resolución de Direcciones
- **RX GTP ECHO**: Solicitud/Respuesta de Eco GTP-U (keepalive)
- **RX GTP OTHER**: Otros mensajes de control GTP
- **RX GTP PDU**: Datos de usuario encapsulados en GTP-U (tráfico principal)
- **RX GTP UNEXP**: Tipos de paquetes GTP inesperados
- **RX ICMP**: Protocolo de Mensajes de Control de Internet (ping, errores)
- **RX ICMP6**: Paquetes ICMPv6
- **RX IP4**: Paquetes IPv4
- **RX IP6**: Paquetes IPv6
- **RX OTHER**: Otros protocolos
- **RX TCP**: Paquetes del Protocolo de Control de Transmisión
- **RX UDP**: Paquetes del Protocolo de Datagramas de Usuario

Casos de Uso:

- **Monitorear el conteo de GTP-U PDU**: Indicador principal del tráfico de usuarios
- **Verificar ICMP para conectividad**: Prueba de accesibilidad de la red
- **Rastrear la relación TCP vs UDP**: Patrones de tráfico de aplicaciones
- **Detectar protocolos inesperados**: Problemas de seguridad o configuración incorrecta

---

Estadísticas de Rutas

Estadísticas de búsqueda de la FIB (Base de Información de Enrutamiento) para decisiones de enrutamiento.

Búsqueda de FIB IPv4:

- **Caché**: Búsquedas de ruta en caché (ruta rápida)
- **OK**: Búsquedas de ruta exitosas

Búsqueda de FIB IPv6:

- **Caché**: Búsquedas de ruta IPv6 en caché
- **OK**: Búsquedas de ruta IPv6 exitosas

Indicadores de Rendimiento:

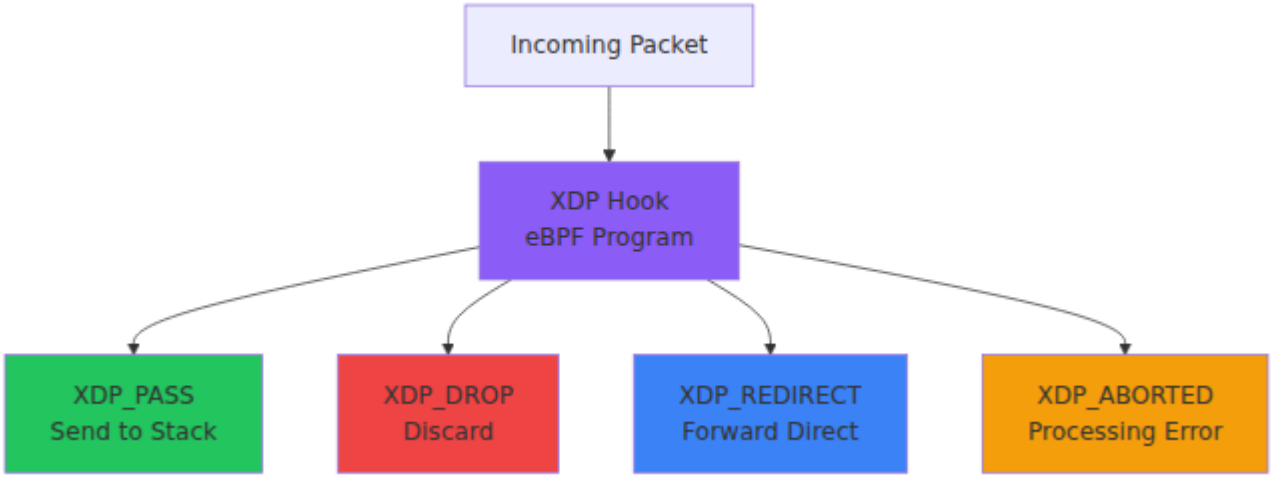
- **Alta Tasa de Aciertos en Caché**: Indica un buen rendimiento de la caché de enrutamiento
- **Alta Cantidad de OK**: Confirma que las tablas de enrutamiento están configuradas correctamente
- **Bajas o Cero Búsquedas**: Puede indicar que el tráfico no fluye o que se está evitando el enrutamiento

---

Monitoreo de Capacidad

Capacidad del Mapa eBPF

El monitoreo de la capacidad del mapa eBPF previene fallos en el establecimiento de sesiones debido al agotamiento de recursos.



Mapas eBPF Críticos

far_map (Reglas de Acción de Reenvío):

- **Capacidad**: 131,070 entradas
- **Tamaño de Clave**: 4 B (ID de FAR)
- **Tamaño de Valor**: 16 B (parámetros de reenvío)
- **Uso de Memoria**: ~2.6 MB
- **Criticidad**: Alta - Usado para todas las decisiones de reenvío de paquetes

pdr_map_downlin (PDRs de Enlace Descendente - IPv4):

- **Capacidad**: 131,070 entradas
- **Tamaño de Clave**: 4 B (dirección IPv4 del UE)
- **Tamaño de Valor**: 208 B (información de PDR)
- **Uso de Memoria**: ~27 MB
- **Criticidad**: Crítica - El establecimiento de sesiones falla si está lleno

pdr_map_downlin_ip6 (PDRs de Enlace Descendente - IPv6):

- **Capacidad**: 131,070 entradas
- **Tamaño de Clave**: 16 B (dirección IPv6 del UE)
- **Tamaño de Valor**: 208 B (información de PDR)
- **Uso de Memoria**: ~29 MB
- **Criticidad**: Crítica - El establecimiento de sesiones IPv6 falla si está lleno

pdr_map_teid_ip (PDRs de Enlace Ascendente):

- **Capacidad**: 131,070 entradas
- **Tamaño de Clave**: 4 B (TEID)
- **Tamaño de Valor**: 208 B (información de PDR)
- **Uso de Memoria**: ~27 MB
- **Criticidad**: Crítica - El tráfico de enlace ascendente falla si está lleno

qer_map (Reglas de Aplicación de QoS):

- **Capacidad**: 65,535 entradas
- **Tamaño de Clave**: 4 B (ID de QER)
- **Tamaño de Valor**: 32 B (parámetros de QoS)
- **Uso de Memoria**: ~2.3 MB
- **Criticidad**: Media - Solo afecta a la aplicación de QoS

urr_map (Reglas de Reporte de Uso):

- **Capacidad**: 131,070 entradas
- **Tamaño de Clave**: 4 B (ID de URR)
- **Tamaño de Valor**: 16 B (contadores de volumen)
- **Uso de Memoria**: ~2.6 MB
- **Criticidad**: Baja - Solo afecta a la facturación

Umbrales de Capacidad

Umbral	Acción Requerida
0-50% (Verde)	Operación normal - No se requiere acción
50-70% (Amarillo)	Precaución - Monitorear tendencias de crecimiento, planificar aumento de capacidad
70-90% (Ámbar)	Advertencia - Programar aumento de capacidad dentro de 1 semana
90-100% (Rojo)	Crítico - Se requiere acción inmediata, nuevas sesiones fallarán

Procedimiento para Aumentar la Capacidad

Antes de aumentar la capacidad:

1. Revisar tendencias de uso actuales
2. Estimar la tasa de crecimiento futura
3. Calcular la capacidad requerida

Pasos para aumentar la capacidad del mapa:

1. Detener el servicio OmniUPF
2. Actualizar el archivo de configuración del UPF con los nuevos tamaños de mapa
3. Reiniciar el servicio OmniUPF
4. Verificar la nueva capacidad en la vista de Capacidad
5. Monitorear el establecimiento exitoso de sesiones

Nota: Cambiar la capacidad del mapa eBPF requiere reiniciar el UPF y borra todas las sesiones existentes.

Métricas de Rendimiento

Para obtener información detallada sobre todas las métricas de Prometheus expuestas por OmniUPF, consulte la **Referencia de Métricas**.

Tasa de Procesamiento de Paquetes

Cálculo:

```
Tasa de Paquetes (pps) = (Delta de Conteo de Paquetes) / (Delta de Tiempo en segundos)
```

Ejemplo:

- Paquetes RX iniciales: 7,000

- Después de 10 segundos: 17,000
- Tasa de Paquetes = (17,000 - 7,000) / 10 = 1,000 pps

Objetivos de Rendimiento:

- **UPF Pequeño**: 10,000 - 100,000 pps
- **UPF Mediano**: 100,000 - 1,000,000 pps
- **UPF Grande**: 1,000,000 - 10,000,000 pps

Indicadores de Cuello de Botella:

- Aumento en el conteo de abortos de XDP
- Alta utilización de CPU
- Aumento en las caídas de paquetes
- Aumento en la latencia

Cálculo de Rendimiento

Cálculo:

```
Rendimiento (Mbps) = (Delta de Conteo de Bytes × 8) / (Delta de
Tiempo en segundos × 1,000,000)
```

Ejemplo:

- Bytes RX iniciales: 500 MB
- Después de 60 segundos: 800 MB
- Rendimiento = (300 MB × 8) / (60 × 1,000,000) = 40 Mbps

El rendimiento por dirección se exporta como contadores `_total` (`upf_n3_rx_packets_total`, `upf_n3_rx_bytes_total`, ... equivalentes de N6) cuando `expose_xdp_metrics` está habilitado. N3 es el lado GTP-U (gNB), N6 es el lado SGi (red de datos). La lectura de `upf_ext_stat` de eBPF se realiza fuera de la ruta de raspado por el `Sampler` de fondo (la lectura por raspado fue un desencadenante comprobado de `virtio_net` TX-ring-wedge, problema #57), y está controlada por la bandera. Los mismos campos también están disponibles

a demanda como JSON en `/api/v1/xdp_stats`. Consulte la Referencia de Métricas para más detalles.

Planificación de Capacidad:

- Monitorear los tiempos de rendimiento máximo (por ejemplo, horas de la tarde)
- Comparar con la capacidad del enlace (velocidades de interfaz N3/N6)
- Planificar para 2x el rendimiento máximo para margen de seguridad

---

Tasa de Caídas

Cálculo:

```
Tasa de Caídas (%) = (Paquetes Descargados / Total de Paquetes RX)
× 100
```

Umbrales Aceptables:

- **< 0.1%**: Excelente (pérdida de paquetes normal debido a errores)
- **0.1% - 1%**: Bueno (problemas menores o limitación de tasa)
- **1% - 5%**: Pobre (investigar problemas de QoS o capacidad)
- **> 5%**: Crítico (problema mayor de reenvío o capacidad)

Causas Comunes de Caídas:

- Limitación de tasa de QER (MBR excedido)
- Fallos en la búsqueda del mapa eBPF
- TEIDs o IPs de UE inválidos
- Errores de enrutamiento

Alertas y Umbrales

Alertas Recomendadas

Alertas Críticas (se requiere respuesta inmediata):

- Capacidad del mapa eBPF > 90%
- Conteo de abortos de XDP > 0
- Tasa de caídas > 5%
- Fallo en la verificación de salud del UPF

Alertas de Advertencia (respuesta dentro de 1 hora):

- Capacidad del mapa eBPF > 70%
- Tasa de caídas > 1%
- Tasa de paquetes acercándose a la capacidad del enlace
- TTL del buffer excedido (paquetes más antiguos que 30s)

Alertas Informativas (monitorear tendencias):

- Capacidad del mapa eBPF > 50%
- Aumento en el conteo de paquetes almacenados
- Nuevas asociaciones PFCP establecidas/liberadas
- Umbrales de volumen de URR excedidos

Configuración de Alertas

Las alertas se pueden configurar a través de:

1. **Métricas de Prometheus**: Exportar métricas para monitoreo externo (consulte la Referencia de Métricas para la lista completa)
2. **Monitoreo de Registros**: Analizar los registros de OmniUPF en busca de patrones de error
3. **Polling de API REST**: Consultar periódicamente los endpoints `/map_info`, `/packet_stats`

4. **Monitoreo de UI Web**: Monitoreo manual a través de las páginas de Estadísticas y Capacidad

---

Planificación de Capacidad

Estimación de Capacidad de Sesiones

Calcular sesiones máximas:

```
Sesiones Máximas = min(
  Capacidad del Mapa PDR / 2,  # PDRs de enlace descendente + ascendente por sesión
  Capacidad del Mapa FAR / 2,  # FARs de enlace descendente + ascendente por sesión
  Capacidad del Mapa QER       # Opcional, un QER por sesión
)
```

Ejemplo:

- Capacidad del Mapa PDR: 131,070
- Capacidad del Mapa FAR: 131,070
- Capacidad del Mapa QER: 65,535

Sesiones Máximas = min(131,070 / 2, 131,070 / 2, 65,535) = **65,535 sesiones**

Capacidad de Memoria

Calcular la memoria total del mapa eBPF:

```
Memoria = Σ (Capacidad del Mapa × (Tamaño de Clave + Tamaño de Valor))
```

Ejemplo de Configuración:

- Mapas PDR: 3 × 131,070 × 212 B = 83.3 MB

- Mapa FAR: 131,070 × 20 B = 2.6 MB
- Mapa QER: 65,535 × 36 B = 2.3 MB
- Mapa URR: 131,070 × 20 B = 2.6 MB
- **Total**: ~91 MB de memoria del kernel

Consideraciones de Memoria del Kernel:

- Asegurar un límite de memoria bloqueada suficiente (`ulimit -l`)
- Reservar 2x el uso estimado para margen de seguridad
- Monitorear la disponibilidad de memoria del kernel

Capacidad de Tráfico

Calcular la capacidad de rendimiento requerida:

1. **Estimar el rendimiento promedio por sesión**:
    - Streaming de video: ~5 Mbps
    - Navegación web: ~1 Mbps
    - VoIP: ~0.1 Mbps
2. **Calcular el rendimiento agregado**:

    ```
    Rendimiento Total = Sesiones × Rendimiento Promedio por Sesión
    ```

3. **Agregar margen**:

    ```
    Capacidad Requerida = Rendimiento Total × 2  # 100% de margen
    ```

Ejemplo:

- 10,000 sesiones concurrentes
- Promedio de 2 Mbps por sesión
- Total: 20 Gbps
- Capacidad requerida: 40 Gbps (interfaces N3 + N6)

Planificación de Crecimiento

Análisis de Tendencias:

1. Registrar el conteo máximo de sesiones diarias
2. Calcular la tasa de crecimiento semanal
3. Extrapolar al límite de capacidad

Fórmula de Tasa de Crecimiento:

```
Semanas hasta la Capacidad = (Capacidad - Uso Actual) /
(Crecimiento Semanal)
```

Ejemplo:

- Sesiones actuales: 30,000
- Capacidad: 65,535 sesiones
- Crecimiento semanal: 2,000 sesiones
- Semanas hasta la capacidad: (65,535 - 30,000) / 2,000 = **17.8 semanas**

Acción: Planificar la actualización de capacidad en 12 semanas (dejando un margen de 5 semanas).

Resolución de Problemas de Rendimiento

Alta Tasa de Caídas de Paquetes

Síntomas: Tasa de caídas > 1%, quejas de usuarios sobre mala conectividad

Diagnóstico:

1. Verificar Estadísticas → Estadísticas de Paquetes
2. Identificar si las caídas son específicas de un protocolo
3. Revisar Estadísticas de XDP para caídas vs. abortos de XDP

Causas Comunes:

- **Limitación de Tasa de QER**: Verificar valores de MBR de QER vs. tráfico real
- **TEIDs Inválidos**: Verificar que el TEID de PDR de enlace ascendente coincida con la asignación de gNB
- **IPs de UE Desconocidas**: Verificar que exista un PDR de enlace descendente para la IP de UE
- **Desbordamiento de Buffer**: Verificar estadísticas de buffer

Resolución:

- Aumentar el MBR de QER si hay limitación de tasa
- Verificar que el SMF haya creado los PDR correctos
- Limpiar buffers si se detecta desbordamiento

Errores de Procesamiento de XDP

Síntomas: Abortados de XDP > 0

Diagnóstico:

1. Navegar a Estadísticas → Estadísticas de XDP
2. Verificar el contador de abortos
3. Revisar los registros de OmniUPF en busca de errores de eBPF

Causas Comunes:

- Fallo en la verificación del programa eBPF
- Incompatibilidad de versión del kernel
- Errores de acceso al mapa eBPF
- Corrupción de memoria

Resolución:

- Reiniciar el servicio OmniUPF

- Verificar que la versión del kernel cumpla con los requisitos mínimos (Linux 5.4+)
- Revisar los registros del programa eBPF
- Contactar soporte si el problema persiste

Agotamiento de Capacidad

Síntomas: Fallos en el establecimiento de sesiones, capacidad del mapa al 100%

Diagnóstico:

1. Navegar a la página de Capacidad
2. Identificar qué mapa está al 100%
3. Verificar si las sesiones están atascadas (no se están eliminando)

Mitigación Inmediata:

1. Identificar sesiones obsoletas (verificar la página de Sesiones)
2. Solicitar al SMF que elimine sesiones antiguas
3. Limpiar buffers para liberar entradas de FAR

Resolución a Largo Plazo:

1. Aumentar la capacidad del mapa eBPF
2. Programar el reinicio del UPF con mapas más grandes
3. Implementar políticas de limpieza de sesiones

Degradación del Rendimiento

Síntomas: Alta latencia, bajo rendimiento, saturación de CPU

Diagnóstico:

1. Verificar la tasa de paquetes vs. línea de base histórica
2. Revisar estadísticas de XDP para retrasos en el procesamiento

3. Monitorear la utilización de CPU en el host del UPF
4. Verificar la utilización de las interfaces N3/N6

Causas Comunes:

- Tráfico que excede la capacidad del UPF
- Núcleos de CPU insuficientes para el procesamiento de paquetes
- Cuello de botella en la interfaz de red
- Colisiones de hash en el mapa eBPF

Resolución:

- Escalar el UPF horizontalmente (agregar más instancias)
- Mejorar la CPU o habilitar RSS (Escalado Lateral de Recepción)
- Mejorar las interfaces de red a velocidades más altas
- Ajustar la función hash del mapa eBPF

Documentación Relacionada

- **Referencia de Métricas** - Referencia completa de métricas de Prometheus
- **Guía de Operaciones de UPF** - Arquitectura y operaciones generales de UPF
- **Guía de Gestión de Reglas** - Configuración de PDR, FAR, QER, URR
- **Guía de Operaciones de UI Web** - Características de monitoreo del panel de control
- **Guía de Resolución de Problemas** - Problemas comunes y diagnósticos
- **Guía de Arquitectura** - Optimización del datapath eBPF y rendimiento

Referencia de Códigos de Causa PFCP

Descripción General

PFCP (Protocolo de Control de Reenvío de Paquetes) utiliza códigos de causa en mensajes de respuesta para indicar el resultado de las solicitudes. Este documento describe los códigos de causa implementados en OmniUPF y cuándo ocurren durante el procesamiento de mensajes PFCP.

Todos los códigos de causa se ajustan a las especificaciones de **3GPP TS 129.244** y se devuelven en los mensajes de respuesta PFCP para indicar éxito, fallo o condiciones de error específicas.

Monitoreo de Códigos de Causa

OmniUPF rastrea los resultados de los mensajes PFCP utilizando métricas de Prometheus. Cada respuesta PFCP incluye un código de causa que se registra en:

```
upf_pfcp_rx_errors{message_name="...", cause_code="...",
peer_address="..."}
```

Esto permite el monitoreo de:

- **Tasas de éxito** por tipo de mensaje y nodo de plano de control
- **Patrones de error** que indican configuraciones incorrectas o problemas de protocolo
- **Salud de la asociación** basada en tasas de rechazo

Consulte Referencia de Métricas para la documentación completa de métricas PFCP.

Categorías de Códigos de Causa

Códigos de Éxito

Código	Nombre	Cuándo Ocurre
1	**RequestAccepted**	Solicitud procesada con éxito. Todos los IEs obligatorios presentes y válidos. Reglas creadas/modificadas/eliminadas con éxito.

Códigos de Error del Cliente

Código	Nombre	Cuándo Ocurre
64	**RequestRejected**	Rechazo general por errores no especificados. Utilizado cuando no se aplica un código de causa específico.
65	**SessionContextNotFound**	Modificación o eliminación de sesión solicitada para SEID desconocido. La sesión especificada no existe en este UPF.
66	**MandatoryIEMissing**	Elemento de Información requerido ausente. Ejemplos: NodeID faltante en la Configuración de Asociación, F-SEID faltante en el Establecimiento de Sesión, RecoveryTimeStamp faltante.
67	**ConditionalIEMissing**	IE condicionalmente requerido ausente basado en otros IEs presentes. Utilizado cuando los IEs dependen de la presencia de otros.
69	**MandatoryIEIncorrect**	IE requerido presente pero contiene datos inválidos. Ejemplos: Formato de

Código	Nombre	Cuándo Ocurre
		NodeID no parseable, valor de RecoveryTimeStamp inválido, F-SEID mal formado.
72	**NoEstablishedPFCPAssociation**	Operación de sesión intentada sin asociación activa. Debe establecerse la asociación PFCP antes de crear sesiones.
73	**RuleCreationModificationFailure**	Error al aplicar reglas PDR, FAR, QER o URR al datapath eBPF. Causas posibles: capacidad del mapa eBPF agotada, parámetros de regla inválidos, fallo en la asignación de recursos.

Códigos de Error del Servidor/Recurso

Código	Nombre	Cuándo Ocurre
74	**PFCPEntityInCongestion**	UPF experimentando alta carga o agotamiento de recursos. Temporalmente incapaz de procesar solicitudes.
75	**NoResourcesAvailable**	Recursos insuficientes para cumplir con la solicitud. Ejemplos: capacidad del mapa eBPF agotada, fallo en la asignación de memoria, pool de TEID agotado.
77	**SystemFailure**	Error interno crítico que impide el procesamiento de la solicitud. Ejemplos: fallo del programa eBPF, error en la interfaz del kernel, corrupción de base de datos.

Códigos de Característica No Soportada

Código	Nombre	Cuándo Ocurre
68	**InvalidLength**	El campo de longitud de IE no coincide con la longitud de datos real. Actualmente no utilizado en OmniUPF.
70	**InvalidForwardingPolicy**	Política de reenvío no soportada por UPF. Actualmente no utilizado en OmniUPF.
71	**InvalidFTEIDAllocationOption**	Opción de asignación de F-TEID no soportada. Actualmente no utilizado en OmniUPF.
76	**ServiceNotSupported**	Servicio o característica solicitada no implementada. Actualmente no utilizado en OmniUPF.
78	**RedirectionRequested**	UPF solicita redirección a otra instancia de UPF. Actualmente no utilizado en OmniUPF.

Escenarios Comunes y Causas

Fallos en la Configuración de Asociación

Escenario: NodeID Faltante

```
SMF → UPF: Solicitud de Configuración de Asociación (sin NodeID)
UPF → SMF: Respuesta de Configuración de Asociación (Causa:
MandatoryIEMissing)
```

Resolución: Asegúrese de que SMF incluya el IE NodeID en todas las Solicitudes de Configuración de Asociación.

Escenario: Formato de NodeID Inválido

```
SMF → UPF: Solicitud de Configuración de Asociación
(NodeID="inválido")
UPF → SMF: Respuesta de Configuración de Asociación (Causa:
MandatoryIEIncorrect)
```

Resolución: NodeID debe ser un FQDN válido o una dirección IPv4/IPv6.

Escenario: Timestamp de Recuperación Faltante

```
SMF → UPF: Solicitud de Configuración de Asociación (sin
RecoveryTimeStamp)
UPF → SMF: Respuesta de Configuración de Asociación (Causa:
MandatoryIEMissing)
```

Resolución: Incluir RecoveryTimeStamp en la Solicitud de Configuración de Asociación.

Fallos en el Establecimiento de Sesión

Escenario: No Asociación Establecida

```
SMF → UPF: Solicitud de Establecimiento de Sesión
UPF → SMF: Respuesta de Establecimiento de Sesión (Causa:
NoEstablishedPFCPAssociation)
```

Resolución: Establecer la asociación PFCP antes de crear sesiones.

Escenario: Fallo en la Creación de Reglas

```
SMF → UPF: Solicitud de Establecimiento de Sesión
UPF procesa FARs, QERs, URRs con éxito
UPF falla al crear PDR (mapa eBPF lleno)
UPF → SMF: Respuesta de Establecimiento de Sesión (Causa:
RuleCreationModificationFailure)
```

Resolución:

- Verifique la capacidad del mapa eBPF (consulte Monitoreo de Capacidad)
- Aumente los tamaños de los mapas en la configuración de UPF
- Reduzca el conteo de sesiones activas

Escenario: F-SEID Faltante

```
SMF → UPF: Solicitud de Establecimiento de Sesión (sin CP F-SEID)
UPF → SMF: Respuesta de Establecimiento de Sesión (Causa:
MandatoryIEMissing)
```

Resolución: Incluir CP F-SEID en la Solicitud de Establecimiento de Sesión.

Fallos en la Modificación de Sesión

Escenario: SEID Desconocido

```
SMF → UPF: Solicitud de Modificación de Sesión (SEID=12345)
UPF no tiene sesión con SEID 12345
UPF → SMF: Respuesta de Modificación de Sesión (Causa:
SessionContextNotFound)
```

Resolución:

- Verifique que el SEID coincida con el valor de la Respuesta de Establecimiento de Sesión
- Verifique si la sesión ya fue eliminada
- Asegúrese de usar la instancia correcta de UPF (escenarios de bucle N9)

Fallos en la Eliminación de Sesión

Escenario: SEID Desconocido

```
SMF → UPF: Solicitud de Eliminación de Sesión (SEID=67890)
UPF no tiene sesión con SEID 67890
UPF → SMF: Respuesta de Eliminación de Sesión (Causa:
SessionContextNotFound)
```

Resolución: El SEID puede haber sido eliminado previamente o nunca existió.

Solución de Problemas con Códigos de Causa

Usando Métricas de Prometheus

Consulta Prometheus para identificar patrones de error:

```
# Tasa de error por código de causa
rate(upf_pfcp_rx_errors{cause_code!="RequestAccepted"}[5m])

# Principales causas de rechazo
topk(5, sum by (cause_code) (upf_pfcp_rx_errors))

# Errores por par SMF
sum by (peer_address, cause_code)
(upf_pfcp_rx_errors{cause_code!="RequestAccepted"})

# Fallos en el establecimiento de sesión
upf_pfcp_rx_errors{message_name="SessionEstablishmentRequest",
cause_code!="RequestAccepted"}
```

Usando la Interfaz Web

Navegue a la página de **Sesiones** para ver:

- Conteo de sesiones activas por nodo de plano de control
- Tasas de éxito/fallo en el establecimiento de sesiones
- Errores recientes de sesión

Navegue a la página de **Capacidad** para diagnosticar:

- Utilización del mapa eBPF (causa raíz de RuleCreationModificationFailure)
- Indicadores de agotamiento de recursos

Consulte Guía de Interfaz Web para instrucciones detalladas de monitoreo.

Pasos Comunes de Depuración

Alta Tasa de MandatoryIEMissing:

1. Verifique la configuración de SMF para los IEs requeridos
2. Verifique la compatibilidad de la versión de la biblioteca PFCP
3. Revise los registros de SMF en busca de errores de construcción de IE

Frecuentes RuleCreationModificationFailure:

1. Verifique la capacidad del mapa eBPF: `GET /api/v1/map_info`
2. Monitoree el uso del mapa: `upf_ebpf_map_used / upf_ebpf_map_capacity`
3. Aumente los tamaños de los mapas en la configuración si > 70% utilizado
4. Consulte Planificación de Capacidad

Errores NoEstablishedPFCPAssociation:

1. Verifique que la asociación exista: `GET /api/v1/pfcp_associations`
2. Verifique la configuración del tiempo de espera del heartbeat
3. Revise los registros de configuración de la asociación
4. Asegúrese de que SMF y UPF puedan alcanzarse mutuamente

SessionContextNotFound en Modificación:

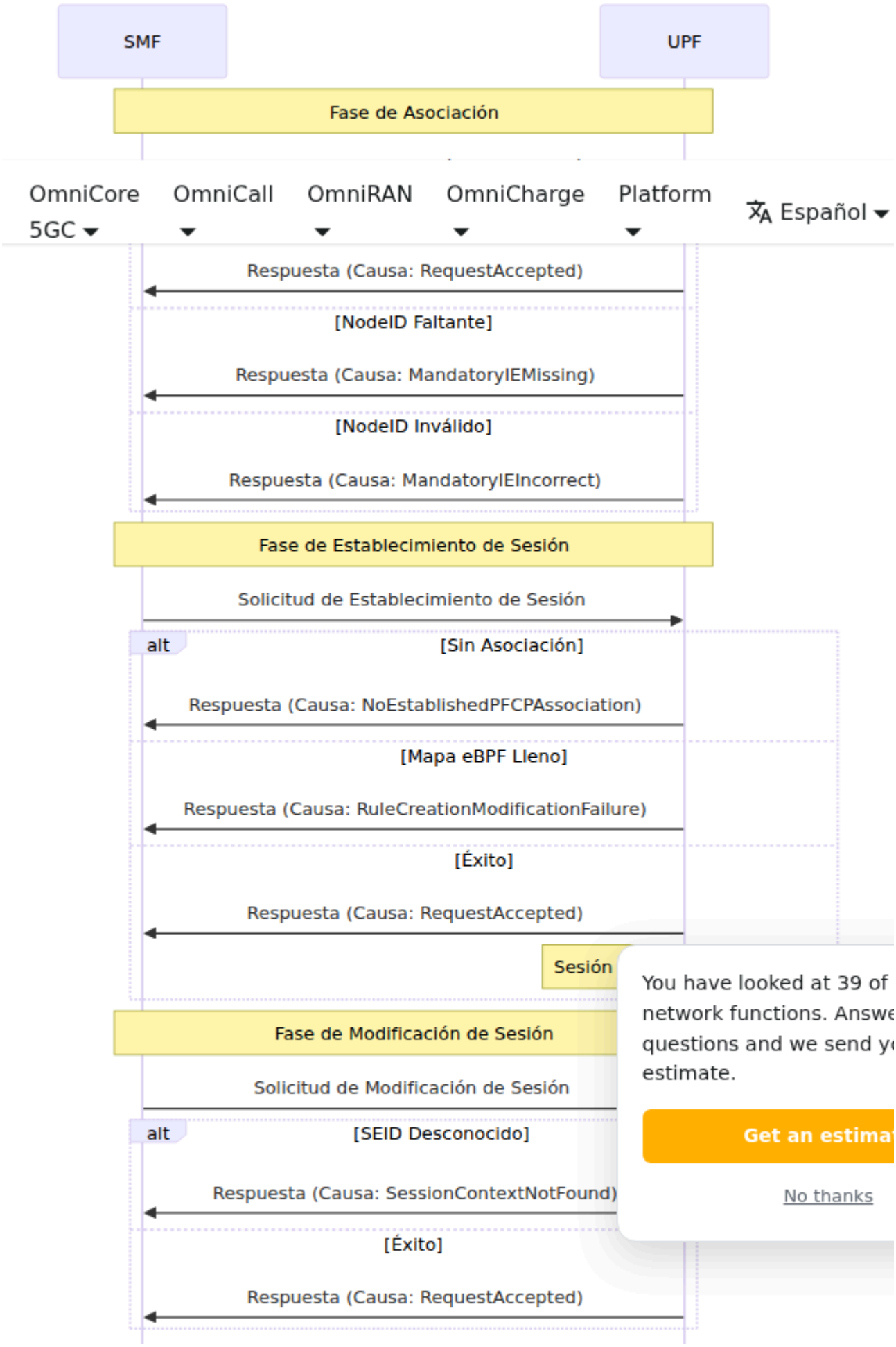
1. Verifique el SEID de la respuesta de establecimiento de sesión
2. Verifique si la sesión fue eliminada
3. Para bucle N9: Asegúrese de usar el endpoint correcto de UPF

4. Consulte sesiones activas: `GET /api/v1/pfcp_sessions`

Impacto del Código de Causa en las

Operaciones

Ciclo de Vida de la Sesión



You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima
No thanks



Métricas y Alertas

Alertas Recomendadas:

```
# Crítico: Alta tasa de rechazo
- alert: PfcpHighRejectionRate
  expr: |
    rate(upf_pfcp_rx_errors{cause_code!="RequestAccepted"}[5m]) > 0.1
  annotations:
    summary: "Alta tasa de rechazo PFCP: {{ $value }}/s"

# Advertencia: Problemas de capacidad
- alert: PfcpRuleCreationFailures
  expr: |

rate(upf_pfcp_rx_errors{cause_code="RuleCreationModificationFailure"}
[5m]) > 0
  annotations:
    summary: "Se detectaron fallos en la creación de reglas PFCP"

# Advertencia: Problemas de asociación
- alert: PfcpNoAssociation
  expr: |

rate(upf_pfcp_rx_errors{cause_code="NoEstablishedPFCPAssociation"}
[5m]) > 0
  annotations:
    summary: "Sesiones PFCP intentadas sin asociación"
```

Cumplimiento de Normas 3GPP

OmniUPF implementa códigos de causa de acuerdo con:

- **3GPP TS 129.244 v16.4.0** - Especificación PFCP
- **Sección 8.2.1** - Definición de IE de Causa
- **Sección 8.19** - Tabla de valores de Causa

Documentación Relacionada

- **Integración del Protocolo PFCP** - Arquitectura PFCP y manejo de mensajes
- **Referencia de Métricas** - Documentación de la métrica upf_pfcp_rx_errors
- **Guía de Monitoreo** - Monitoreo de capacidad y alertas
- **Guía de Solución de Problemas** - Problemas de asociación y sesión PFCP
- **Guía de Interfaz Web** - Monitoreo de sesiones y asociaciones

Guía de Gestión de Reglas

Tabla de Contenidos

1. Descripción General
2. Reglas de Detección de Paquetes (PDR)
3. Reglas de Acción de Reenvío (FAR)
4. Reglas de Aplicación de QoS (QER)
5. Reglas de Reporte de Uso (URR)
6. Relaciones de Reglas
7. Operaciones Comunes
8. Solución de Problemas

Descripción General

OmniUPF utiliza un conjunto de reglas interconectadas para clasificar, reenviar, dar forma y rastrear el tráfico del plano de usuario. Estas reglas son instaladas por el SMF a través de PFCP y almacenadas en mapas eBPF para un procesamiento de paquetes de alto rendimiento. Comprender estas reglas y sus relaciones es crítico para operar y solucionar problemas en el UPF.

Tipos de Reglas

Tipo de Regla	Propósito	Campo Clave	Instalado Por
PDR (Regla de Detección de Paquetes)	Clasificar paquetes en flujos	TEID o IP de UE	SMF a través de Establecimiento/Modificación de Sesión PFCP
FAR (Regla de Acción de Reenvío)	Determinar la acción de reenvío	ID de FAR	SMF a través de Establecimiento/Modificación de Sesión PFCP
QER (Regla de Aplicación de QoS)	Aplicar límites de ancho de banda y marcado	ID de QER	SMF a través de Establecimiento/Modificación de Sesión PFCP
URR (Regla de Reporte de Uso)	Rastrear volúmenes de datos para cobro	ID de URR	SMF a través de Establecimiento/Modificación de Sesión PFCP

Flujo de Procesamiento de Reglas



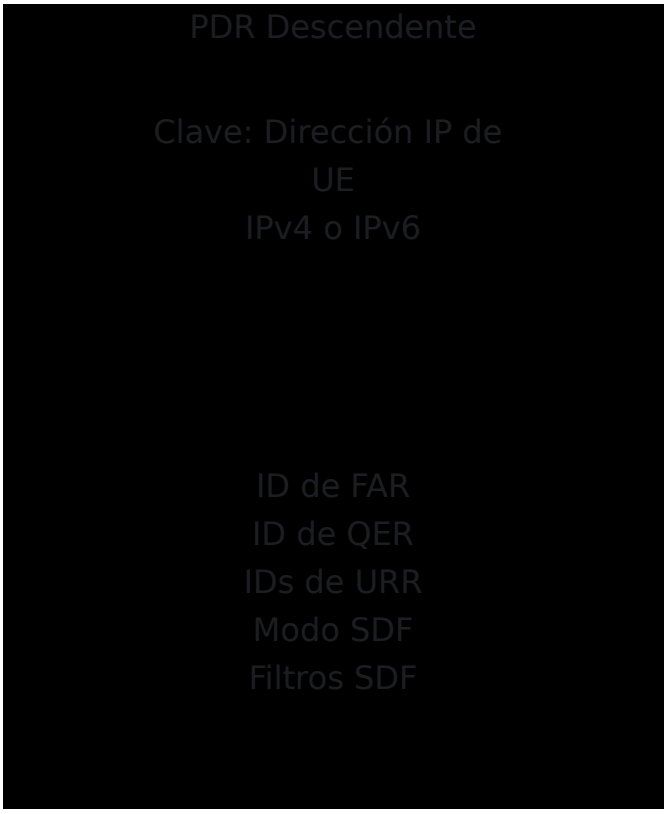


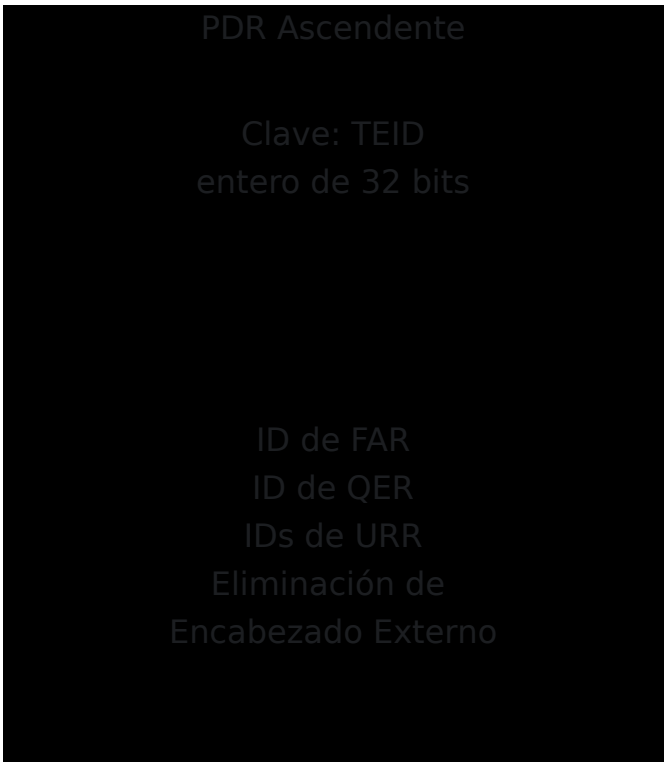
Reglas de Detección de Paquetes (PDR)

Propósito

Los PDR clasifican los paquetes entrantes en flujos de tráfico. Son el punto de entrada para todo el procesamiento de paquetes en el UPF.

Estructura de PDR





PDR Ascendentes

Los PDR ascendentes coinciden con los paquetes que llegan a la interfaz N3 desde el RAN.

Campo Clave: TEID (Identificador de Punto Final de Túnel)

- Entero sin signo de 32 bits
- Asignado por SMF y señalado al gNB
- Único por flujo de tráfico de UE

Campos de Valor:

- **ID de FAR**: Referencia a la regla de acción de reenvío
- **ID de QER**: Referencia a la regla de aplicación de QoS (opcional)
- **IDs de URR**: Lista de reglas de reporte de uso (opcional)
- **Eliminación de Encabezado Externo**: Indicador para eliminar la encapsulación GTP-U

Proceso de Búsqueda:

1. Extraer TEID del encabezado GTP-U
2. Búsqueda hash en el mapa eBPF `uplink_pdr_map`
3. Si se encuentra coincidencia, recuperar ID de FAR, ID de QER y IDs de URR
4. Si no hay coincidencia, descartar paquete

Ejemplo:

```
TEID: 5678
ID de FAR: 2
ID de QER: 1
Eliminación de Encabezado Externo: Falso
Modo SDF: Sin SDF
```

PDR Descendentes

Los PDR descendentes coinciden con los paquetes que llegan a la interfaz N6 desde la red de datos.

Campo Clave: Dirección IP de UE

- Dirección IPv4 (32 bits) o dirección IPv6 (128 bits)
- Asignada por SMF durante el establecimiento de la sesión PDU
- Única por UE

Campos de Valor:

- **ID de FAR**: Referencia a la regla de acción de reenvío
- **ID de QER**: Referencia a la regla de aplicación de QoS (opcional)
- **IDs de URR**: Lista de reglas de reporte de uso (opcional)
- **Modo SDF**: Modo de filtro de Flujo de Datos de Servicio
  - `Sin SDF`: Sin filtrado, todo el tráfico coincide

    - `Solo SDF`: Solo el tráfico que coincide con SDF se reenvía
    - `SDF + Predeterminado`: El tráfico que coincide con SDF utiliza reglas específicas, otro tráfico utiliza el FAR predeterminado
- **Filtros SDF**: Filtros específicos de la aplicación (puertos, protocolos, rangos de IP)

Proceso de Búsqueda:

1. Extraer IP de destino del encabezado del paquete
2. Búsqueda hash en `downlink_pdr_map` (IPv4) o `downlink_pdr_map_ip6` (IPv6)
3. Si se encuentra coincidencia, verificar filtros SDF (si están configurados)
4. Recuperar ID de FAR, ID de QER y IDs de URR
5. Si no hay coincidencia, descartar paquete

Ejemplo:

```
IP de UE: 10.45.0.1
ID de FAR: 1
ID de QER: 1
Eliminación de Encabezado Externo: Falso
Modo SDF: Sin SDF
```

Filtros SDF (Flujo de Datos de Servicio)

Los filtros SDF proporcionan clasificación de tráfico específica de la aplicación dentro de un PDR.

Casos de Uso:

- Diferenciar el tráfico de YouTube del de navegación web
- Aplicar diferentes QoS a VoIP frente a datos de mejor esfuerzo
- Enrutar aplicaciones específicas a través de diferentes rutas de red

Criterios de Filtro:

- **Protocolo**: TCP, UDP, ICMP
- **Rango de Puertos**: Puertos de destino (por ejemplo, 443 para HTTPS, 5060 para SIP)
- **Rango de Direcciones IP**: Redes de destino específicas
- **Descripción del Flujo**: Plantillas de flujo definidas por 3GPP

Ejemplo de Configuración de SDF:

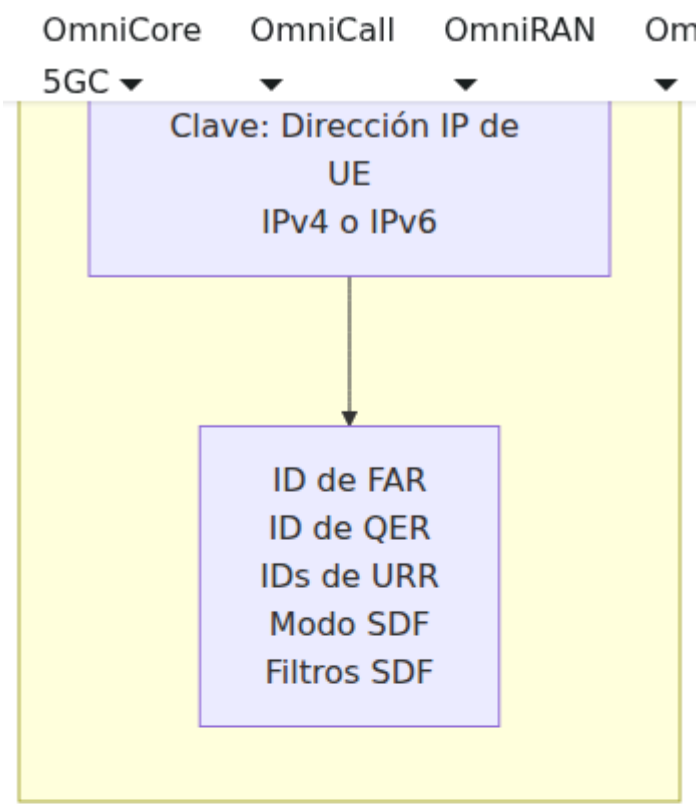
```
ID de PDR: 10
IP de UE: 10.45.0.1
Modo SDF: Solo SDF
Filtros SDF:
  - Protocolo: UDP, Puertos: 5060-5061 → ID de FAR 5 (FAR de VoIP)
  - Protocolo: TCP, Puerto: 443 → ID de FAR 1 (FAR Predeterminado)
```

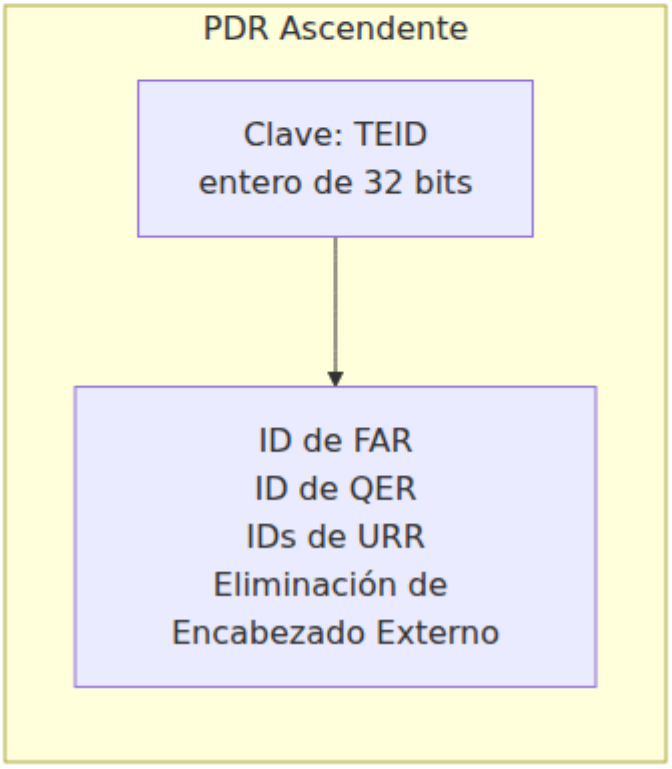
Reglas de Acción de Reenvío (FAR)

Propósito

Las FAR determinan qué hacer con los paquetes que coinciden con un PDR. Definen acciones de reenvío, parámetros de encapsulación GTP-U y puntos finales de destino.

Estructura de FAR





Flags de Acción

Las acciones de FAR son flags a nivel de bits que se pueden combinar:

Flag	Bit	Valor	Descripción
REENVIAR	1	2	Reenviar paquete al destino
BUFFER	2	4	Almacenar paquete en el búfer
DESCARTAR	0	1	Descartar paquete
NOTIFICAR	3	8	Enviar notificación al plano de control
DUPLICAR	4	16	Duplicar paquete a múltiples destinos

Combinaciones de Acción Comunes:

- `Acción: 2 (REENVIAR)` - Reenvío normal (más común)
- `Acción: 6 (REENVIAR + BUFFER)` - Reenviar y almacenar durante la transferencia
- `Acción: 4 (BUFFER)` - Solo almacenar (durante el cambio de ruta)
- `Acción: 1 (DESCARTAR)` - Descartar paquete (raro, generalmente para hacer cumplir políticas)

Control de Almacenamiento

El flag BUFFER (bit 2) controla el almacenamiento de paquetes durante eventos de movilidad. El almacenamiento es una característica crítica del UPF que previene la pérdida de paquetes durante las transiciones de estado de UE.

Cuándo se Utiliza el Almacenamiento

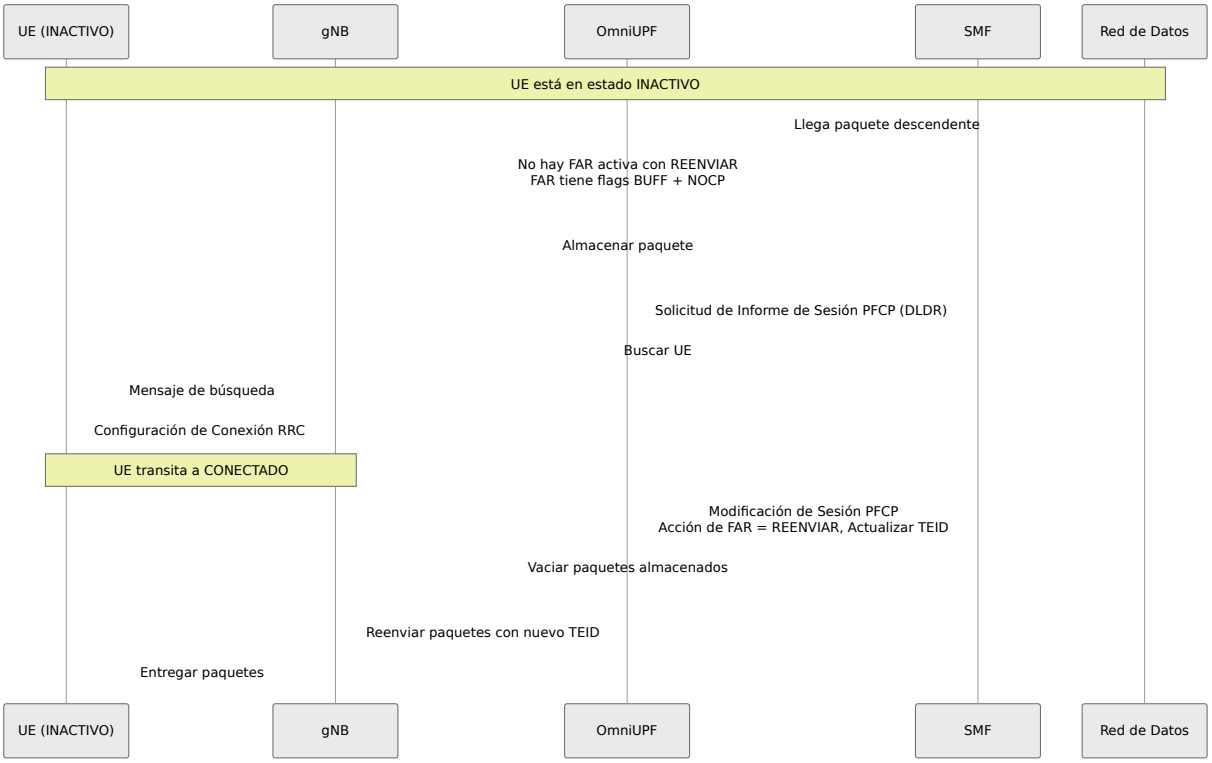
Transición de Inactivo a Conectado: Cuando llegan paquetes descendentes para un UE en estado INACTIVO (no conectado al gNB), el UPF:

1. Almacena los paquetes

2. Envía una Notificación de Datos Descendentes (DLDR) al SMF
3. El SMF busca al UE para despertarlo y conectarlo
4. Una vez conectado, el SMF actualiza la FAR con la acción de REENVIAR
5. El UPF vacía los paquetes almacenados al UE

Transferencia (Conectado a Conectado): Durante la transferencia de gNB a gNB, el UPF almacena temporalmente los paquetes para prevenir pérdidas:

1. La conexión del antiguo gNB se cae
2. El SMF establece la acción de FAR en BUFFER
3. Los paquetes se encolan durante el cambio de ruta
4. El UE se conecta al nuevo gNB
5. El SMF actualiza la FAR con el nuevo TEID y la acción de REENVIAR
6. El UPF vacía los paquetes al nuevo gNB



Capacidad y Límites de Almacenamiento

Límites Globales de Almacenamiento:

- **Máx. Total de Paquetes**: 100,000 (configurable)
- **Máx. Total de Bytes**: Basado en la memoria disponible

- **TTL (Tiempo de Vida)**: 60 segundos (configurable)
- **Paquetes que exceden TTL**: Se descartan automáticamente

Límites por FAR:

- **Máx. Paquetes por FAR**: 10,000 (configurable)
- **Propósito**: Prevenir que un solo FAR agote la capacidad del búfer

Comportamiento de Desbordamiento del Búfer:

- Cuando se alcanza el límite global o por FAR, se descartan nuevos paquetes
- Las métricas rastrean los descartes con `reason="global_limit"` o `reason="far_limit"`
- Los paquetes más antiguos NO se expulsan automáticamente (solo se descartan explícitamente al expirar el TTL)

Notificación de Datos Descendentes (DLDR)

Cuando el UPF almacena un paquete para un UE INACTIVO, envía una Solicitud de Informe de Sesión PFCP al SMF:

Contenidos de DLDR:

- **Tipo de Informe**: Informe de Datos Descendentes (DLDR)
- **ID de FAR**: La FAR que activó el almacenamiento
- **Información del Servicio de Datos Descendentes**: QFI opcional, Indicador de Política de Búsqueda

Acciones del SMF en DLDR:

1. Buscar al UE a través de AMF → gNB
2. Esperar a que el UE establezca la conexión RRC
3. Enviar Solicitud de Modificación de Sesión PFCP para actualizar la FAR
4. La acción de FAR cambia de `BUFF+NOCP` a `REENVIAR`
5. El UPF vacía los paquetes almacenados

Métricas para DLDR:

- `upf_dldr_sent_total`: Total de DLDR enviados
- `upf_dldr_send_errors`: DLDR fallidos
- `upf_buffer_notify_to_flush_duration_seconds`: Latencia desde DLDR hasta el vaciado

Ver Referencia de Métricas para la lista completa.

Operaciones de Almacenamiento

Habilitar Almacenamiento (Establecer flag BUFF):

- Acción de FAR `|= 0x04` (establecer bit 2)
- Ejemplo: `Acción: 2 (REENVIAR)` → `Acción: 6 (REENVIAR+BUFF)`
- Usado durante la preparación de la transferencia

Modo Solo Almacenamiento (BUFF sin REENVIAR):

- Acción de FAR `= 0x04` (solo BUFF)
- Los paquetes se almacenan pero NO se reenvían
- Usado para el estado INACTIVO de UE (pendiente de búsqueda)

Deshabilitar Almacenamiento (Limpiar flag BUFF):

- Acción de FAR `&= ~0x04` (limpiar bit 2)
- Ejemplo: `Acción: 6 (REENVIAR+BUFF)` → `Acción: 2 (REENVIAR)`
- Los paquetes almacenados permanecen hasta que se vacían o se limpian

Vaciar Búfer:

- Reenviar todos los paquetes almacenados utilizando las reglas de FAR **actuales**
- Los paquetes se reenvían con el TEID/destino actualizado
- El búfer se vacía después de un vaciado exitoso
- La FAR debe tener la acción de REENVIAR establecida

Limpiar Búfer:

- Descartar todos los paquetes almacenados sin reenviar

- Usar cuando la transferencia falla o la sesión se elimina
- Las métricas rastrean con `reason="cleared"`

Monitoreo de Paquetes Almacenados

Página de Búferes (Interfaz Web): Navegar a **Búferes** para ver:

- Total de paquetes almacenados
- Total de bytes almacenados
- Número de FARs con paquetes almacenados
- Conteos de paquetes por FAR
- Marca de tiempo del paquete más antiguo
- Habilitar/Deshabilitar almacenamiento por FAR
- Operaciones de vaciado o limpieza

Indicadores Clave:

- **Paquetes > 10 segundos antiguos**: Posible retraso en la búsqueda
- **Paquetes > 30 segundos antiguos**: Probable falla en la búsqueda, limpiar búfer
- **Alto conteo de paquetes**: Verificar sesiones atascadas o fallas en la búsqueda

Métricas de Prometheus:

- `upf_buffer_packets_current`: Paquetes almacenados actuales
- `upf_buffer_bytes_current`: Bytes almacenados actuales
- `upf_buffer_fars_active`: FARs con paquetes almacenados
- `upf_buffer_packets_dropped{reason}`: Conteos de paquetes descartados

Ver Referencia de Métricas para métricas completas de búfer.

Escenarios Comunes de Almacenamiento

Escenario 1: UE INACTIVO Datos Descendentes

```
Estado Inicial:
- UE en modo INACTIVO (sin conexión gNB)
- Acción de FAR: 0x04 (solo BUFF)

Llegada de Datos:
1. DN envía paquete descendente
2. UPF coincide con PDR, aplica FAR
3. FAR tiene flag BUFF → paquete almacenado
4. UPF envía DLDR al SMF
5. SMF busca al UE
6. UE se conecta al gNB
7. SMF modifica la FAR: Acción = 0x02 (REENVIAR)
8. UPF vacía los paquetes almacenados con nuevo TEID
```

Escenario 2: Preparación para Transferencia

```
Estado Inicial:
- UE conectado a gNB-1 (TEID 1234)
- Acción de FAR: 0x02 (REENVIAR)

Proceso de Transferencia:
1. SMF modifica la FAR: Acción = 0x06 (REENVIAR+BUFF)
2. Paquetes reenviados a gNB-1 Y almacenados
3. UE cambia a gNB-2
4. SMF modifica la FAR: TEID = 5678, Acción = 0x02 (REENVIAR)
5. UPF vacía los paquetes almacenados a gNB-2 con nuevo TEID
6. No hay pérdida de paquetes durante la transferencia
```

Escenario 3: Cambio de Ruta

```
Estado Inicial:
- UE conectado, flujo de datos activo

Cambio de Ruta:
1. SMF modifica la FAR: Acción = 0x04 (solo BUFF)
2. Todos los paquetes entrantes se almacenan (no se reenvían)
3. La red reconfigura la ruta
4. SMF modifica la FAR: Acción = 0x02 (REENVIAR), nuevo destino
5. UPF vacía todos los paquetes almacenados a la nueva ruta
```

Creación de Encabezado Externo

Determina si se debe agregar la encapsulación GTP-U.

FAR Ascendente (N3 → N6):

- Creación de Encabezado Externo: Falso
- Acción: Eliminar GTP-U, reenviar paquete IP nativo

FAR Descendente (N6 → N3):

- Creación de Encabezado Externo: Verdadero
- IP Remota: dirección IP del gNB (por ejemplo, 198.51.100.10)
- TEID: ID de túnel para tráfico de UE
- Acción: Agregar encabezado GTP-U, reenviar al gNB

Búsqueda de FAR en la Interfaz Web

La página de Gestión de Reglas proporciona búsqueda de FAR por ID:

Pasos:

1. Navegar a Reglas → pestaña FARs
2. Ingresar ID de FAR en el campo de búsqueda
3. Hacer clic en "Buscar" para ver detalles de FAR

Información Mostrada:

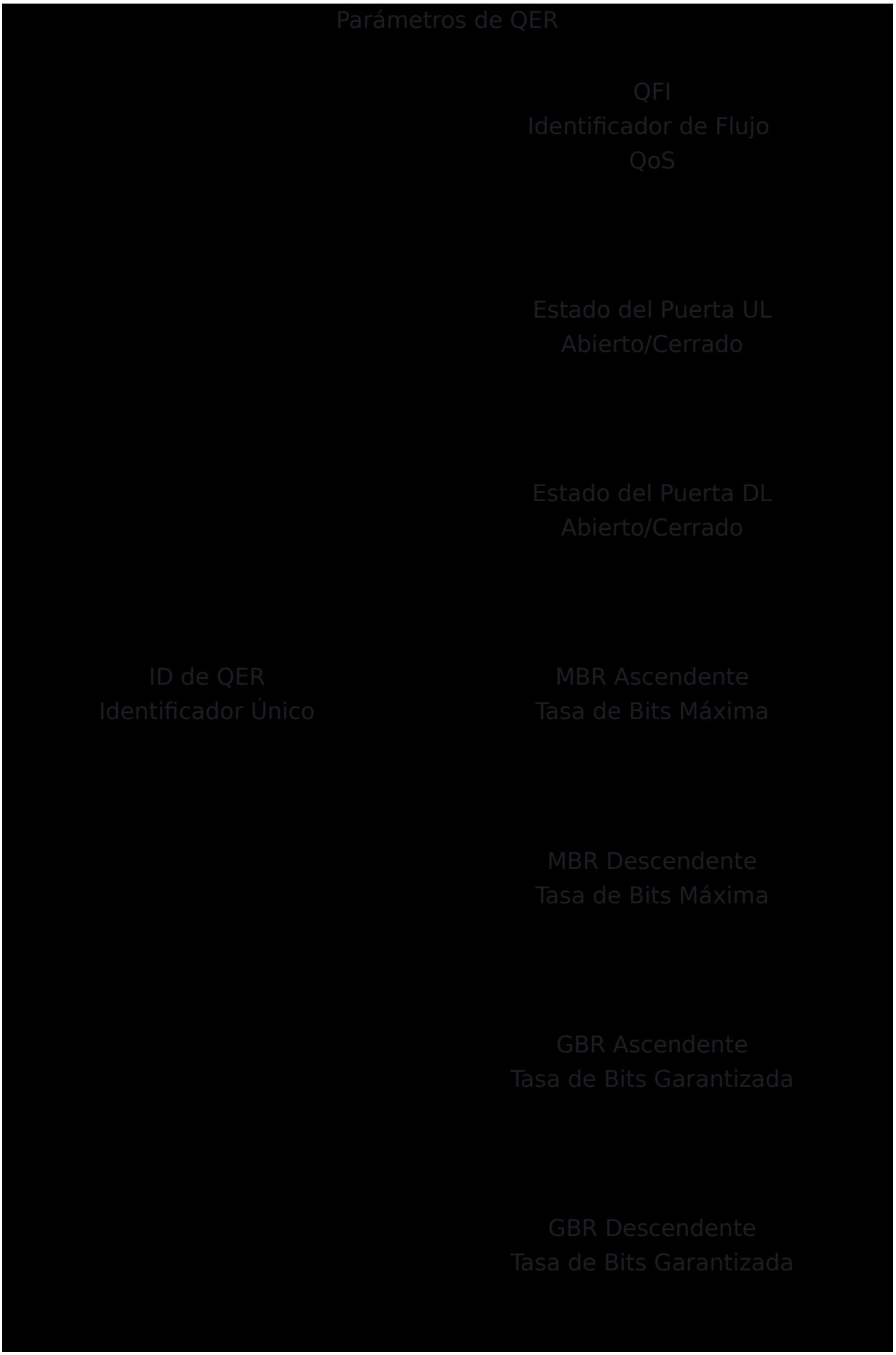
- ID de FAR
- Acción (numérica + flags decodificados)
- Estado de Almacenamiento (ON/OFF)
- Creación de Encabezado Externo
- Dirección IP remota (con representación entera)
- TEID
- Marcado de Nivel de Transporte

Reglas de Aplicación de QoS (QER)

Propósito

Las QER aplican parámetros de Calidad de Servicio a los flujos de tráfico, incluyendo límites de ancho de banda y marcado de paquetes.

Estructura de QER


Parámetros de QER
QFI
Identificador de Flujo
QoS
Estado del Puerta UL
Abierto/Cerrado
Estado del Puerta DL
Abierto/Cerrado
ID de QER
Identificador Único
MBR Ascendente
Tasa de Bits Máxima
MBR Descendente
Tasa de Bits Máxima
GBR Ascendente
Tasa de Bits Garantizada
GBR Descendente
Tasa de Bits Garantizada

Parámetros de QoS

QFI (Identificador de Flujo QoS):

- Identificador de 6 bits para flujos QoS 5G
- Los valores 1-9 están estandarizados (por ejemplo, QFI 9 = portadora predeterminada)
- Utilizado para el marcado de paquetes en 5GC

Estado de la Puerta:

- **Abierto (0)**: Tráfico permitido
- **Cerrado (no cero)**: Tráfico bloqueado

Tasa de Bits Máxima (MBR):

- Ancho de banda máximo permitido para el flujo de tráfico
- Especificado en kbps
- **MBR = 0**: Sin límite de tasa (ilimitado)
- El tráfico que excede MBR es descartado

Tasa de Bits Garantizada (GBR):

- Ancho de banda mínimo garantizado para el flujo de tráfico
- Especificado en kbps
- **GBR = 0**: Mejor esfuerzo (sin garantía)
- **GBR > 0**: Flujo priorizado con ancho de banda garantizado

Tipos de Flujos QoS

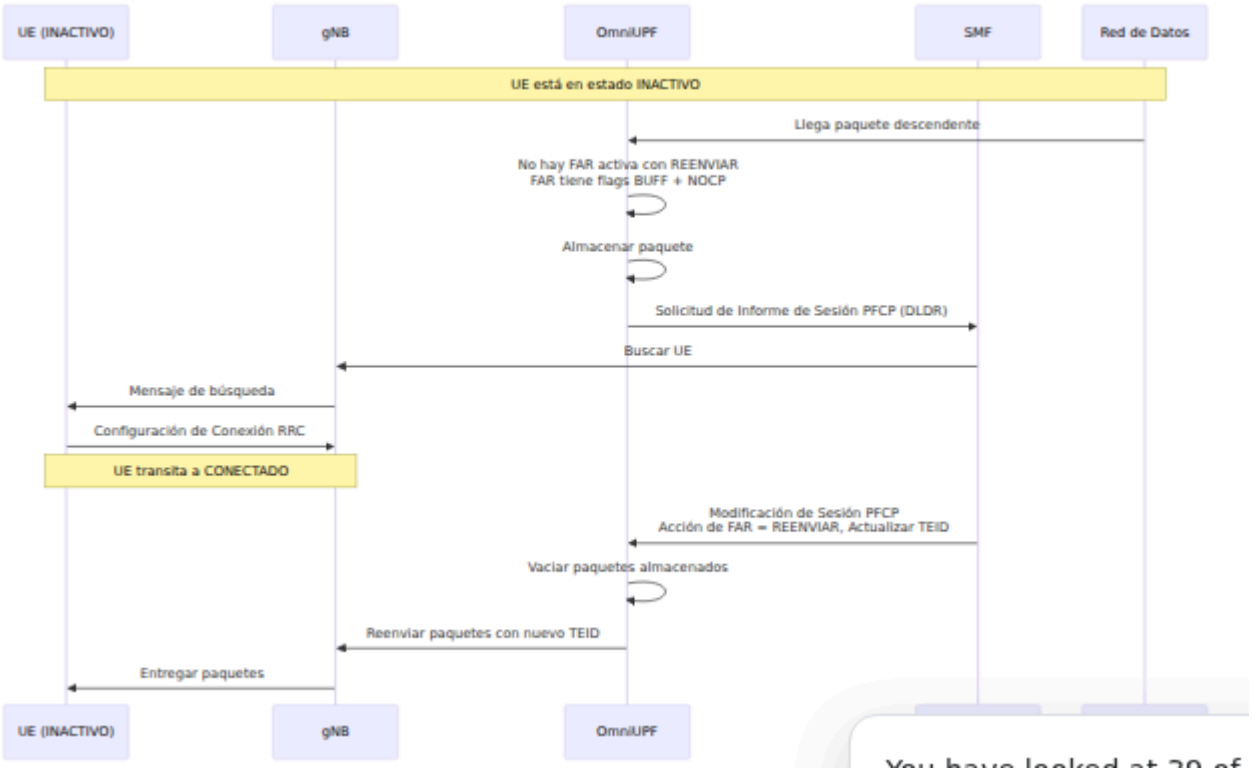
Flujos de Mejor Esfuerzo (GBR = 0):

```
ID de QER: 1
QFI: 9
MBR Ascendente: 100000 kbps (100 Mbps)
MBR Descendente: 100000 kbps (100 Mbps)
GBR Ascendente: 0 kbps
GBR Descendente: 0 kbps
```

Flujos Garantizados (GBR > 0):

```
ID de QER: 2
QFI: 1
MBR Ascendente: 10000 kbps (10 Mbps)
MBR Descendente: 10000 kbps (10 Mbps)
GBR Ascendente: 5000 kbps (5 Mbps)
GBR Descendente: 5000 kbps (5 Mbps)
```

Algoritmo de Aplicación de QoS



Mecanismo de Aplicación de MBR

OmniUPF aplica límites de MBR (Tasa de Bits Máxima) utilizando un **limitador de tasa de ventana deslizante** implementado en la ruta de datos eBPF. Este algoritmo opera con precisión de nanosegundos directamente en la capa XDP, asegurando rendimiento a tasa de línea sin cambios de contexto del kernel.

Cómo Funciona

Algoritmo: Limitación de Tasa de Ventana Deslizante

Para cada paquete, el UPF realiza las siguientes comprobaciones:

1. **Comprobación del Estado de la Puerta**: Si el estado de la puerta es `CERRADO` (no cero), descartar el paquete de inmediato
2. **Comprobación de MBR**: Si MBR = 0, omitir la limitación de tasa (ancho de banda ilimitado)
3. **Cálculo del Tiempo de Transmisión**:

```
tx_time = (tamaño_paquete_bytes × 8) × (1,000,000,000 ns/sec) /
MBR_kbps
```

4. **Comprobación de Ventana**: Si el tiempo actual está dentro de la ventana deslizante de 5 ms, descartar el paquete
5. **Avance de Ventana**: Si se permite el paquete, avanzar la ventana por `tx_time`

Ejemplo de Cálculo:

Supongamos:

- MBR = 100,000 kbps (100 Mbps)
- Tamaño del paquete = 1500 bytes
- Tamaño de la ventana = 5,000,000 ns (5 ms)

```
Paso 1: Calcular el tiempo de transmisión a 100 Mbps
tx_time = (1500 bytes × 8 bits/byte) × (1,000,000,000 ns/sec) /
100,000,000 bps
        = 12,000,000,000 / 100,000,000
        = 120 ns

Paso 2: Verificar si el paquete cabe en la ventana
current_time = 1000000000 ns
window_start = 999990000 ns
if (window_start + tx_time > current_time):
    DESCARTAR paquete (excedería el límite de tasa)

Paso 3: Si se permite, avanzar ventana
window_start = window_start + 120 ns
PASAR paquete
```

Comportamiento de Ventana Deslizante

Tamaño de Ventana de 5 ms:

- El algoritmo utiliza una ventana deslizante de 5 milisegundos
- La ventana se restablece automáticamente si está inactiva durante más de 5 ms

- Previene la inanición de ráfagas mientras aplica la tasa promedio

Manejo de Ráfagas:

- Se permiten ráfagas pequeñas dentro de la ventana de 5 ms
- El tráfico sostenido por encima de MBR es limitado en tasa
- Más preciso que los algoritmos simples de cubo de tokens

Limitación de Tasa por Dirección:

- MBR ascendente utiliza la marca de tiempo `qer->ul_start`
- MBR descendente utiliza la marca de tiempo `qer->dl_start`
- Cada dirección se limita en tasa de manera independiente

Puntos de Aplicación de Limitación de MBR

Ascendente (N3 → N6):

1. El paquete llega a la interfaz N3 (desde gNB)
2. Búsqueda de PDR por TEID
3. Búsqueda de QER por ID de QER
4. Verificar `ul_gate_status` → descartar si está cerrado
5. Aplicar `limit_rate_sliding_window()` con `ul_maximum_bitrate`
6. Si se permite, reenviar a N6 y actualizar contadores de URR

Descendente (N6 → N3):

1. El paquete llega a la interfaz N6 (desde la Red de Datos)
2. Búsqueda de PDR por dirección IP de UE
3. Búsqueda de QER por ID de QER
4. Verificar `dl_gate_status` → descartar si está cerrado
5. Aplicar `limit_rate_sliding_window()` con `dl_maximum_bitrate`
6. Si se permite, agregar encabezado GTP-U y reenviar a N3

Bucle N9 (SGWU ↔ PGWU):

- Tanto las QER ascendentes como descendentes pueden aplicarse en escenarios de bucle N9

- Cada QER se verifica de manera independiente en los límites de SGWU y PGWU

MBR vs. Rendimiento Observado

Por qué el rendimiento observado puede diferir de MBR:

- **Sobrecarga de Protocolo**: Encabezados GTP-U, UDP, IP añaden ~50-60 bytes por paquete
- **Variación en Tamaño de Paquete**: Paquetes más pequeños = más sobrecarga, menor eficiencia
- **Precisión de Limitación de Tasa**: La aplicación se realiza por paquete, no por byte
- **Comportamiento de Restablecimiento de Ventana**: Períodos de inactividad de 5 ms permiten ráfagas breves por encima de MBR

Ejemplo:

```
MBR Configurado: 100 Mbps
Rendimiento Observado: ~95-98 Mbps (debido a la sobrecarga GTP-U/UDP/IP)
```

Cómo Verificar la Limitación de Tasa:

1. Verificar contadores de volumen de URR a lo largo del tiempo: `upf_urr_*_volume_bytes`
2. Calcular rendimiento: `(volume_delta_bytes × 8) / time_delta_seconds / 1000` = kbps
3. Comparar con MBR configurado en QER

GBR (Tasa de Bits Garantizada)

Importante: OmniUPF **no** aplica actualmente mínimos de GBR. GBR se almacena en la QER pero no se utiliza para priorización de tráfico o control de admisión.

Comportamiento de GBR:

- Los valores de GBR son aceptados del SMF a través de PFCP
- GBR se almacena en el mapa de QER y es visible a través de la API
- **Sin reserva de ancho de banda** o priorización de tráfico basada en GBR
- GBR sirve como metadato para rastrear el tipo de flujo (mejor esfuerzo vs. garantizado)

Mejora Futura:

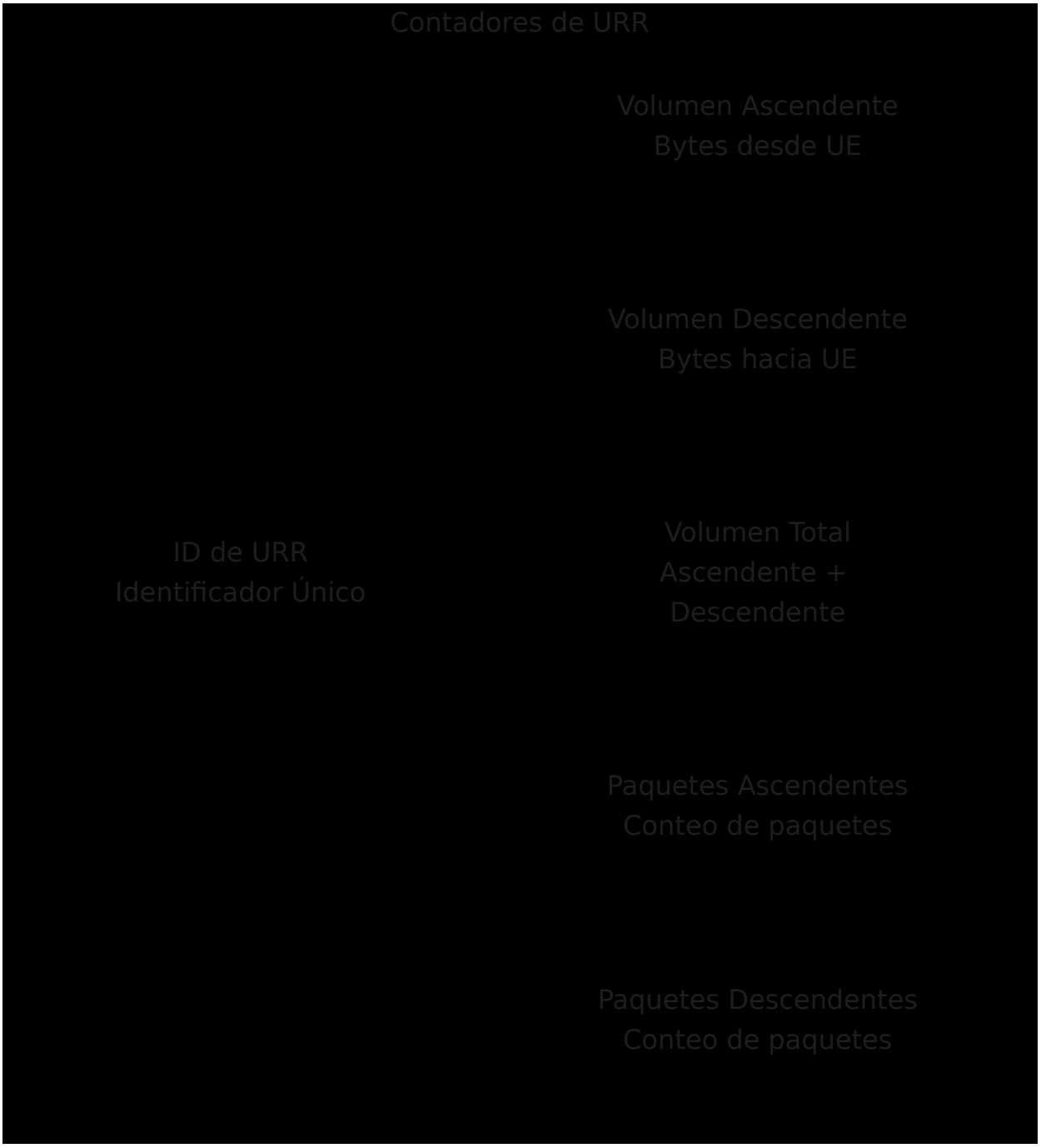
- La aplicación de GBR requiere programación de tráfico o encolado ponderado
- Puede implementarse utilizando capacidades de QoS de eBPF en futuras versiones

Reglas de Reporte de Uso (URR)

Propósito

Las URR rastrean volúmenes de datos para cobro, análisis y aplicación de políticas. Mantienen contadores de paquetes y bytes que se informan al SMF para registros de cobro.

Estructura de URR



Rastreo de Volumen

Volumen Ascendente:

- Bytes transmitidos desde UE a la Red de Datos
- Medido después de la desencapsulación GTP-U
- Incluye encabezado IP y carga útil

Volumen Descendente:

- Bytes transmitidos desde la Red de Datos a UE
- Medido antes de la encapsulación GTP-U
- Incluye encabezado IP y carga útil

Volumen Total:

- Suma de volúmenes ascendentes y descendentes
- Utilizado para el reporte total de uso

Disparadores de Reporte de Uso

Las URR pueden disparar informes basados en:

Umbral de Volumen:

- Informar cuando el volumen exceda el límite configurado
- Ejemplo: Informar cada 1 GB de uso

Umbral de Tiempo:

- Informar en intervalos periódicos
- Ejemplo: Informar cada 5 minutos

Basado en Eventos:

- Informar sobre la terminación de la sesión
- Informar sobre el cambio de QoS
- Informar sobre la transferencia

Formato de Visualización de Volumen

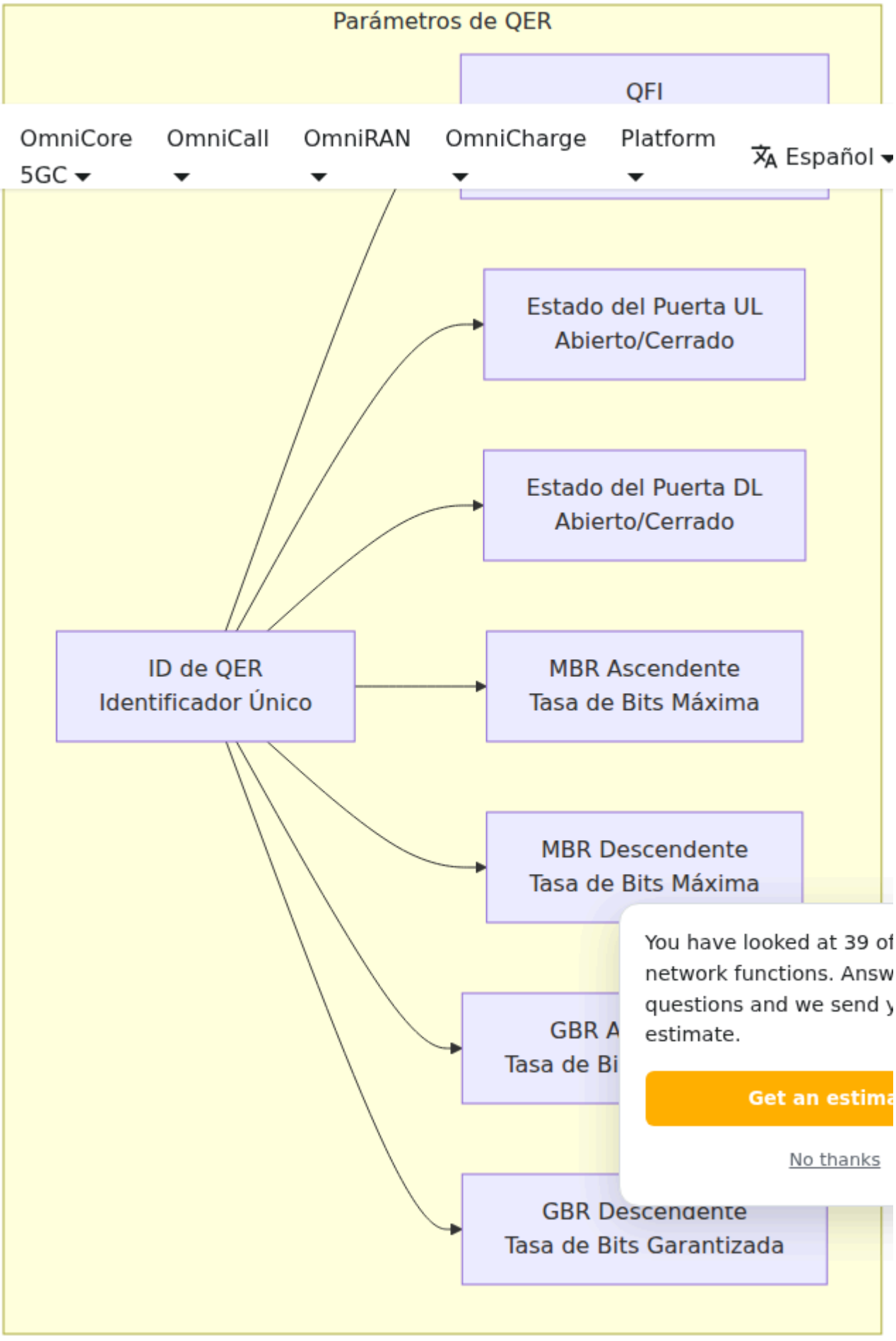
La interfaz web formatea automáticamente el volumen en unidades legibles por humanos:

Bytes	Visualización
0 - 1023	B (Bytes)
1024 - 1048575	KB (Kilobytes)
1048576 - 1073741823	MB (Megabytes)
1073741824 - 1099511627775	GB (Gigabytes)
1099511627776+	TB (Terabytes)

Ejemplo:

```
ID de URR: 0
Volumen Ascendente: 12.3 KB
Volumen Descendente: 9.0 KB
Volumen Total: 21.3 KB
```

Flujo de Reporte de URR

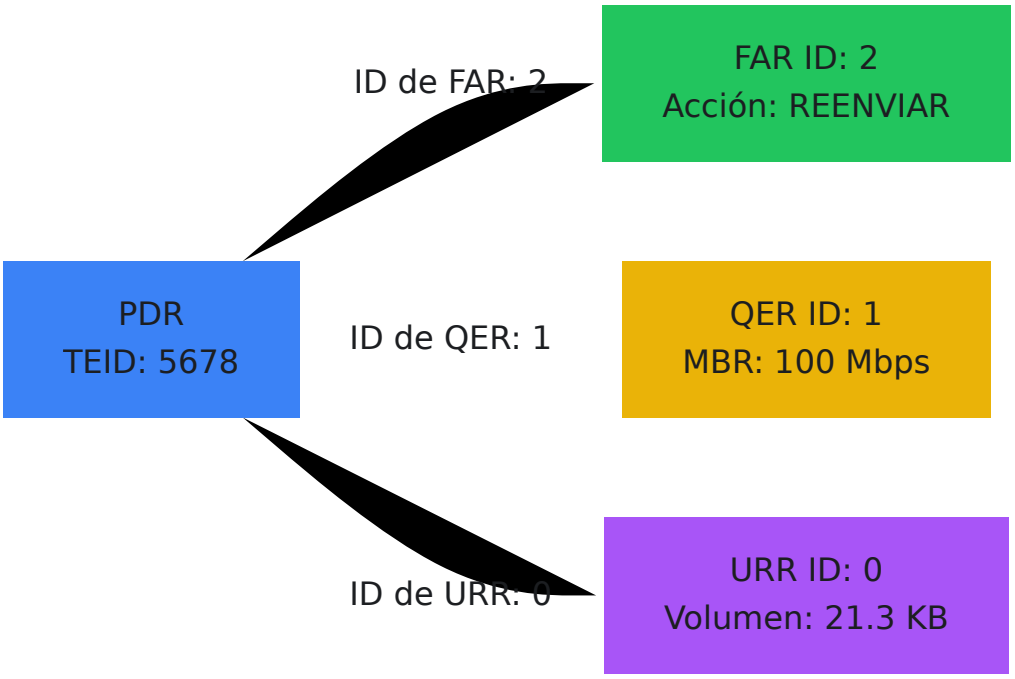


OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Español
You have looked at 39 of
network functions. Answ
questions and we send y
estimate.
Get an estima
No thanks

Relaciones de Reglas

Cadena PDR → FAR → QER → URR

Cada PDR hace referencia a un FAR, que puede hacer referencia a un QER y uno o más URRs.



Ejemplo de Configuración de Sesión

PDR Ascendente:

```
TEID: 5678
ID de FAR: 2
ID de QER: 1
IDs de URR: [0]
Eliminación de Encabezado Externo: Falso
```

PDR Descendente:

```
IP de UE: 10.45.0.1
ID de FAR: 1
ID de QER: 1
IDs de URR: [0]
Modo SDF: Sin SDF
```

FAR ID 1 (Descendente):

```
Acción: 2 (REENVIAR)
Creación de Encabezado Externo: Verdadero
IP Remota: 198.51.100.10
TEID: 5678
```

FAR ID 2 (Ascendente):

```
Acción: 2 (REENVIAR)
Creación de Encabezado Externo: Falso
```

QER ID 1:

```
QFI: 9
MBR Ascendente: 100000 kbps
MBR Descendente: 100000 kbps
GBR Ascendente: 0 kbps
GBR Descendente: 0 kbps
```

URR ID 0:

```
Volumen Ascendente: 12.3 KB
Volumen Descendente: 9.0 KB
Volumen Total: 21.3 KB
```

Operaciones Comunes

Ver Reglas para una Sesión

A través de la Página de Sesiones:

1. Navegar a Sesiones
2. Encontrar UE por IP o TEID
3. Hacer clic en "Expandir" para ver todas las reglas (PDR, FAR, QER, URR)

A través de la Página de Reglas:

1. Navegar a Reglas
2. Usar búsqueda por TEID (ascendente) o IP de UE (descendente) en la pestaña PDR
3. Anotar el ID de FAR, ID de QER, IDs de URR
4. Cambiar a las pestañas FAR/QER/URR para ver las reglas referenciadas

Habilitar/Deshabilitar Almacenamiento

Escenario: Durante la transferencia, almacenar paquetes para prevenir pérdidas

Pasos:

1. Navegar a Reglas → FARs
2. Ingresar ID de FAR en el campo de búsqueda
3. Hacer clic en "Buscar"
4. Si el almacenamiento está DESACTIVADO, hacer clic en "Habilitar Almacenamiento"
5. Verificar que el bit 2 de la acción de FAR esté establecido (el valor de acción aumenta en 4)

Alternativa a través de la Página de Búferes:

1. Navegar a Búferes
2. Ver FARs con almacenamiento habilitado

3. Hacer clic en "Deshabilitar Búfer" cuando la transferencia se complete

Monitorear Cumplimiento de QoS

Verificar si el tráfico está siendo limitado en tasa:

1. Navegar a Reglas → QERs
2. Encontrar ID de QER asociado con la sesión de UE
3. Anotar valores de MBR Ascendente y MBR Descendente
4. Comparar con la tasa de crecimiento del volumen de URR

Calcular Rendimiento Promedio:

```
Rendimiento (kbps) = (Delta de Volumen en bytes × 8) / (Delta de
Tiempo en segundos × 1000)
```

Si el rendimiento se acerca a MBR, el tráfico está siendo limitado en tasa.

Rastrear Uso de Datos

Monitorear volúmenes de URR:

1. Navegar a Reglas → URRs
2. Ver volúmenes ascendentes, descendentes y totales
3. Ordenar por Volumen Total para encontrar los mayores usuarios
4. Actualizar periódicamente para observar el crecimiento del volumen

Casos de Uso:

- Verificar integración de cobro
- Detectar uso anormal de datos
- Planificar capacidad basada en patrones de tráfico

Solución de Problemas

No Flujo de Tráfico

Verificar PDR:

1. Verificar que exista PDR para TEID (ascendente) o IP de UE (descendente)
2. Confirmar que el ID de FAR sea válido
3. Verificar que los filtros SDF no estén bloqueando el tráfico

Verificar FAR:

1. Verificar que la acción de FAR sea REENVIAR (no DESCARTAR o solo BUFFER)
2. Confirmar que la creación de encabezado externo coincida con la dirección
3. Verificar que la IP Remota y el TEID sean correctos para el descenso

Verificar QER:

1. Verificar que el Estado de la Puerta esté Abierto (0)
2. Comprobar que el MBR no sea demasiado restrictivo

Paquetes Siendo Descartados

Verificar Limitación de Tasa de QER:

1. Navegar a Reglas → QERs
2. Verificar que el MBR sea adecuado para la carga de tráfico
3. Comprobar que el crecimiento del volumen de URR coincida con el rendimiento esperado

Verificar Acción de FAR:

1. Navegar a Reglas → FARs
2. Verificar que la acción sea REENVIAR, no DESCARTAR
3. Comprobar que el almacenamiento no esté atascado en modo solo BUFFER

Problemas de Almacenamiento

Paquetes atascados en el búfer:

1. Navegar a la página de Búferes
2. Verificar la marca de tiempo del paquete más antiguo
3. Si > 30 segundos, la transferencia puede haber fallado
4. Limpiar o vaciar manualmente el búfer
5. Deshabilitar el almacenamiento en FAR

Desbordamiento del Búfer:

1. Verificar total de paquetes vs. Máx. Total (predeterminado 100,000)
2. Verificar paquetes por FAR vs. Máx. Por FAR (predeterminado 10,000)
3. Limpiar búferes si están llenos
4. Investigar por qué el almacenamiento no se deshabilitó

URR No Rastreando

Contadores de volumen en cero:

1. Verificar que el PDR haga referencia al ID de URR
2. Comprobar que los paquetes estén coincidiendo con el PDR
3. Verificar que la FAR esté reenviando (no descartando) paquetes
4. Confirmar que el ID de URR exista en el mapa de URR

Volumen no reportando al SMF:

1. Verificar la configuración de Solicitud de Informe de Sesión PFCP
2. Comprobar los disparadores de reporte de URR (umbrales de volumen/tiempo)
3. Revisar registros para mensajes de Informe de Sesión PFCP

Documentación Relacionada

- **Guía de Operaciones de UPF** - Descripción general de la arquitectura y componentes de OmniUPF
- **Guía de Operaciones de Interfaz Web** - Uso del panel de control para ver reglas
- **Guía de Monitoreo** - Estadísticas y monitoreo de capacidad
- **Guía de Solución de Problemas** - Problemas comunes y diagnósticos

Guía de Solución de Problemas de OmniUPF

Tabla de Contenidos

1. Descripción General
2. Herramientas de Diagnóstico
3. Problemas de Instalación
4. Problemas de Configuración
5. Problemas de Asociación PFCP
6. Problemas de Procesamiento de Paquetes
7. Problemas de XDP y eBPF
8. Problemas de Rendimiento
9. Problemas Específicos del Hipervisor
10. Problemas de NIC y Controladores
11. Fallos en el Establecimiento de Sesiones
12. Problemas de Buffering

Descripción General

Esta guía proporciona procedimientos sistemáticos de solución de problemas para problemas comunes de OmniUPF. Cada sección incluye síntomas, pasos de diagnóstico, causas raíz y procedimientos de resolución.

Lista de Verificación Rápida de Diagnóstico

Antes de realizar una solución de problemas profunda, verifique:

```
# 1. Verifique que OmniUPF esté en ejecución
systemctl status omniupf

# 2. Verifique la asociación PFCP
curl http://localhost:8080/api/v1/upf_pipeline

# 3. Verifique que los mapas eBPF estén cargados
ls /sys/fs/bpf/

# 4. Verifique que el programa XDP esté adjunto
ip link show | grep -i xdp

# 5. Verifique los registros del kernel en busca de errores
dmesg | tail -50
journalctl -u omniupf -n 50
```

Herramientas de Diagnóstico

API REST de OmniUPF

Verifique el estado del UPF:

```
curl http://localhost:8080/api/v1/upf_status
```

Verifique las asociaciones PFCP:

```
curl http://localhost:8080/api/v1/upf_pipeline
```

Verifique el conteo de sesiones:

```
curl http://localhost:8080/api/v1/sessions | jq 'length'
```

Verifique la capacidad del mapa eBPF:

```
curl http://localhost:8080/api/v1/map_info
```

Verifique las estadísticas de paquetes:

```
curl http://localhost:8080/api/v1/packet_stats
```

Verifique las estadísticas de XDP:

```
curl http://localhost:8080/api/v1/xdp_stats
```

Inspección de Mapas eBPF

Liste todos los mapas eBPF:

```
ls -lh /sys/fs/bpf/
bpftool map list
```

Muestre los detalles del mapa:

```
bpftool map show
bpftool map dump name pdr_map_downlin
```

Cuente las entradas en el mapa:

```
bpftool map dump name far_map | grep -c "key:"
```

Inspección del Programa XDP

Verifique si el programa XDP está adjunto:

```
ip link show eth0 | grep xdp
```

Liste todos los programas XDP:

```
bpftool net list
```

Muestre los detalles del programa XDP:

```
bpftool prog show
```

Volcar estadísticas de XDP:

```
bpftool prog dump xlated name xdp_upf_func
```

Depuración de Red

Capture tráfico PFCP en N4 (plano de control):

```
# PFCP no es procesado por XDP, tcpdump funciona normalmente
tcpdump -i eth0 -n udp port 8805 -w /tmp/pfcp_traffic.pcap
```

Capture tráfico GTP-U en N3 (requiere captura fuera de banda):

```
# ADVERTENCIA: El tcpdump estándar en el host UPF NO PUEDE
capturar paquetes procesados por XDP!
# XDP procesa GTP-U antes de que la pila de red del kernel vea los
paquetes.

# Use captura fuera de banda en su lugar:
# 1. TAP de red entre gNB y UPF
# 2. Espejo de puerto de conmutador/SPAN para copiar tráfico N3
# 3. Espejo de puerto de conmutador virtual a VM de analizador

# En el host de análisis/monitoreo (NO en UPF):
# tcpdump -i <mirror_interface> -n udp port 2152 -w
/tmp/n3_capture.pcap

# O use la API de estadísticas para conteos de paquetes:
curl http://localhost:8080/api/v1/packet_stats
curl http://localhost:8080/api/v1/n3n6_stats
```

Monitoree los contadores de paquetes:

```
watch -n 1 'ip -s link show eth0'
```

Verifique la tabla de enrutamiento:

```
ip route show
ip route get 10.45.0.100  # Verifique la ruta para la IP del UE
```

Verifique la tabla ARP:

```
ip neigh show
```

Problemas de Instalación

Problema: "sistema de archivos eBPF no montado"

Síntomas:

```
ERRO[0000] failed to load eBPF objects: mount bpf filesystem at
/sys/fs/bpf
```

Causa: sistema de archivos eBPF no montado

Resolución:

```
# Montar el sistema de archivos eBPF
sudo mount bpffs /sys/fs/bpf -t bpf

# Hacer persistente (agregar a /etc/fstab)
echo "bpffs /sys/fs/bpf bpf defaults 0 0" | sudo tee -a /etc/fstab

# Verificar montaje
mount | grep bpf
```

Problema: Versión del kernel demasiado antigua

Síntomas:

```
ERRO[0000] kernel version 5.4.0 is too old, minimum required is
5.15.0
```

Causa: versión del kernel de Linux por debajo del requisito mínimo

Resolución:

```
# Verificar versión del kernel
uname -r

# Actualizar kernel (Ubuntu/Debian)
sudo apt update
sudo apt install linux-generic-hwe-22.04
sudo reboot

# Verificar nuevo kernel
uname -r  # Debería ser >= 5.15.0
```

Problema: Dependencia de libbpf faltante

Síntomas:

```
error while loading shared libraries: libbpf.so.0: cannot open
shared object file
```

Causa: biblioteca libbpf no instalada

Resolución:

```
# Instalar libbpf (Ubuntu/Debian)
sudo apt update
sudo apt install libbpf-dev

# Verificar instalación
ldconfig -p | grep libbpf
```

Problemas de Configuración

Problema: Archivo de configuración inválido

Síntomas:

```
ERRO[0000] unable to read config file: unmarshal errors
```

Causa: error de sintaxis en el archivo de configuración de Elixir

Resolución:

```
# Verificar sintaxis del archivo de configuración
cd /opt/omniupf && bin/upf_ex eval "IO.puts(:ok)"

# Problemas comunes:
# - Faltan comillas alrededor de valores de cadena
# - Sintaxis incorrecta de Elixir (por ejemplo, usar : en lugar de
=)
# - Cadenas o corchetes no cerrados

# El archivo de configuración está en /etc/omniupf/runtime.exs
# Ejemplo de sintaxis correcta:
# xdp_interfaces = "eth0"
# xdp_attach_mode = "generic"
# api_port = 8080
# pfcp_address = "10.0.0.1"
```

Problema: Nombre de interfaz no encontrado

Síntomas:

```
ERRO[0000] interface eth0 not found
```

Causa: la interfaz configurada no existe

Resolución:

```
# Listar todas las interfaces de red
ip link show

# Verificar estado de la interfaz
ip addr show eth0

# Si la interfaz tiene un nombre diferente, actualizar
/etc/omniupf/runtime.exs:
# xdp_interfaces = "ens1f0"  # Usar el nombre real de la interfaz

# Para VMs, verificar el esquema de nombres de interfaz
ls /sys/class/net/
```

Problema: Puerto ya en uso

Síntomas:

```
ERRO[0000] failed to start API server: address already in use
```

Causa: puerto 8080, 8805 o 9090 ya está vinculado por otro proceso

Resolución:

```
# Encontrar proceso que usa el puerto
sudo lsof -i :8080
sudo netstat -tulpn | grep :8080

# Matar proceso en conflicto
sudo kill <PID>

# O cambiar el puerto de OmniUPF en /etc/omniupf/runtime.exs
# api_port = 8081
# pfcp_port = 8806
```

Problema: ID de nodo PFCP inválido

Síntomas:

```
ERRO[0000] invalid pfcp_node_id: must be valid IPv4 address
```

Causa: el ID de nodo PFCP no es una dirección IPv4 válida

Resolución:

```
# En /etc/omniupf/runtime.exs
# Correcto: usar dirección IP (no nombre de host)
node_id = "10.100.50.241"

# Incorrecto:
# node_id = "localhost"
# node_id = "upf.example.com"
```

Problemas de Asociación PFCP

Problema: No se establecieron asociaciones PFCP

Síntomas:

- La interfaz web muestra "No hay asociaciones"
- Los registros de SMF muestran "Fallo en la configuración de la asociación PFCP"

Diagnóstico:

```
# 1. Verifique si el servidor PFCP está escuchando
sudo netstat -ulpn | grep 8805

# 2. Verifique las reglas del firewall
sudo iptables -L -n | grep 8805
sudo ufw status

# 3. Capture tráfico PFCP
tcpdump -i any -n udp port 8805 -vv

# 4. Verifique las asociaciones PFCP a través de la API
curl http://localhost:8080/api/v1/upf_pipeline
```

Causas Comunes y Resoluciones:

Firewall bloqueando PFCP

Resolución:

```
# Permitir tráfico PFCP (UDP 8805)
sudo ufw allow 8805/udp
sudo iptables -A INPUT -p udp --dport 8805 -j ACCEPT
```

ID de nodo PFCP incorrecto

Resolución:

```
# En /etc/omniupf/runtime.exs, establecer ID de nodo a la IP
correcta de la interfaz N4
node_id = "10.100.50.241"    # Debe coincidir con la IP en la red
N4
```

Red inalcanzable para SMF

Resolución:

```
# Probar conectividad con SMF
ping <SMF_IP>

# Verificar enrutamiento hacia SMF
ip route get <SMF_IP>

# Agregar ruta si falta
sudo ip route add <SMF_NETWORK>/24 via <GATEWAY>
```

SMF configurado con IP de UPF incorrecta

Resolución:

- Verificar la configuración de SMF para la dirección de UPF
- Asegurarse de que SMF tenga configurada la IP de `pfcp_node_id` de UPF
- Verificar que SMF pueda enrutar a la red N4 de UPF

Problema: Fallos de latido PFCP

Síntomas:

```
WARN[0030] PFCP heartbeat timeout for association 10.100.50.10
```

Diagnóstico:

```
# Verificar estadísticas PFCP
curl http://localhost:8080/api/v1/upf_pipeline | jq
'.associations[] | {remote_id, uplink_teid_count}'

# Monitorear registros de latidos
journalctl -u omniupf -f | grep heartbeat
```

Causas y Resoluciones:

Pérdida de paquetes en la red

Resolución:

```
# Verificar pérdida de paquetes hacia SMF
ping -c 100 <SMF_IP> | grep loss

# Si hay alta pérdida, investigar la red:
# - Verificar estado del enlace
# - Verificar salud del conmutador/router
# - Verificar congestión
```

Intervalo de latido demasiado agresivo

Resolución:

```
# En /etc/omniupf/runtime.exs
heartbeat_interval_ms = 30_000    # Aumentar de 5000 a 30000 ms
heartbeat_retries = 5             # Aumentar reintentos
heartbeat_timeout_ms = 10_000     # Aumentar tiempo de espera
```

Problemas de Procesamiento de Paquetes

Problema: No fluyen paquetes (contadores RX/TX en 0)

Síntomas:

- La página de estadísticas muestra 0 paquetes RX/TX
- UE no puede establecer sesión de datos

Diagnóstico:

```
# 1. Verifique si el programa XDP está adjunto
ip link show eth0 | grep xdp

# 2. Verifique que la interfaz esté ACTIVADA
ip link show eth0

# 3. Verifique estadísticas de paquetes (consciente de XDP)
# Nota: tcpdump no puede ver paquetes GTP-U procesados por XDP
curl http://localhost:8080/api/v1/packet_stats
```

Resoluciones:

Programa XDP no adjunto

Resolución:

```
# Reinicie OmniUPF para volver a adjuntar XDP
sudo systemctl restart omniupf

# Verifique el adjunto
ip link show eth0 | grep xdp
bpftool net list
```

Interfaz caída o sin enlace

Resolución:

```
# Activar interfaz
sudo ip link set eth0 up

# Verificar estado del enlace
ethtool eth0 | grep "Link detected"

# Si el enlace está caído, verificar conexión física o
configuración de red de VM
```

Interfaz configurada incorrectamente

Resolución:

```
# En /etc/omniupf/runtime.exs
xdp_interfaces = "ens1f0"    # Usar el nombre real de la interfaz
de 'ip link show'
```

Problema: Paquetes recibidos pero no reenviados (alta tasa de caída)

Síntomas:

- Contadores RX en aumento pero contadores TX no
- Tasa de caída > 1%

Diagnóstico:

```
# Verificar estadísticas de caída
curl http://localhost:8080/api/v1/xdp_stats | jq '.drop'

# Verificar estadísticas de ruta
curl http://localhost:8080/api/v1/packet_stats | jq '.route_stats'

# Monitorear caídas de paquetes
watch -n 1 'curl -s http://localhost:8080/api/v1/packet_stats | jq
".total_rx, .total_tx, .total_drop"'
```

Causas Comunes:

Sin coincidencia de PDR (TEID desconocido o IP de UE)

Resolución:

```
# Verificar si existen sesiones
curl http://localhost:8080/api/v1/sessions

# Si no hay sesiones, verificar:
# - La asociación PFCP está establecida
# - SMF ha creado sesiones
# - El establecimiento de sesiones fue exitoso

# Verificar entradas en el mapa PDR
bpftool map dump name pdr_map_teid_ip | grep -c key
bpftool map dump name pdr_map_downlin | grep -c key
```

Fallos de enrutamiento

Resolución:

```
# Verificar fallos de búsqueda FIB
curl http://localhost:8080/api/v1/packet_stats | jq '.route_stats'

# Probar enrutamiento para IP de UE
ip route get 10.45.0.100

# Agregar ruta faltante
sudo ip route add 10.45.0.0/16 dev eth1  # Ruta del grupo de UE a
N6
```

Limitación de tasa QER

Síntomas:

- Rendimiento inferior al esperado
- Tráfico limitado a una tasa específica
- Contadores de volumen URR muestran comportamiento de meseta
- Contadores de caída de XDP en aumento durante ráfagas de tráfico

Diagnóstico:

1. **Verificar MBR configurado para la sesión**:

```
# Encontrar el ID de QER de la sesión
curl http://localhost:8080/api/v1/pfcp_sessions | jq '.data[] |
select(.ue_ip == "10.45.0.1")'

# Buscar la configuración de QER
curl http://localhost:8080/api/v1/qer_map | jq '.data[] |
select(.qer_id == 1)'
```

2. **Verificar estado de la puerta**:

```
# El estado de la puerta debe ser 0 (ABIERTA) tanto para uplink
como para downlink
curl http://localhost:8080/api/v1/qer_map | jq '.data[] |
{qer_id, ul_gate: .ul_gate_status, dl_gate: .dl_gate_status}'
```

3. **Calcular rendimiento real desde URR**:

```
# Consultar contadores de volumen URR en dos puntos en el
tiempo
curl http://localhost:8080/api/v1/urr_map | jq '.data[] |
select(.urr_id == 0)'

# Calcular rendimiento (manual):
# throughput_kbps = (volume_delta_bytes × 8) /
time_delta_seconds / 1000
```

4. **Comparar MBR vs. rendimiento real**:

   - Rendimiento esperado ≈ 95-98% de MBR (debido a la sobrecarga del protocolo)
   - Si el rendimiento está significativamente por debajo de MBR, verificar otros cuellos de botella
   - Si el rendimiento coincide exactamente con MBR, la limitación de tasa está funcionando como se esperaba

Resolución:

- **Si MBR es demasiado bajo**: Solicitar a SMF que actualice QER con un MBR más alto a través de la modificación de sesión PFCP
- **Si la puerta está cerrada**: Investigar por qué SMF cerró la puerta (política, cuota o error)
- **Si la limitación de tasa es inesperada**: Verificar la configuración de política de SMF y perfil de QoS

Entendiendo la Aplicación de MBR:

OmniUPF utiliza un algoritmo de ventana deslizante para hacer cumplir los límites de MBR con precisión en nanosegundos en la ruta de datos eBPF. Consulte la Guía de Gestión de Reglas - Mecanismo de Aplicación de MBR para una explicación detallada de:

- Cómo el tamaño del paquete y la tasa determinan las decisiones de caída
- Por qué el rendimiento observado difiere del MBR configurado
- Limitación de tasa por dirección (uplink/downlink)
- Comportamiento de ventana deslizante de 5 ms

Escenarios Comunes:

- **Caídas de llamadas VoIP**: Verificar si el MBR es suficiente para la tasa de bits del códec (G.711 = ~80 kbps)
- **Buffering en streaming de video**: Asegurarse de que MBR > tasa de bits de video + sobrecarga (1080p = ~5-10 Mbps)
- **Tráfico de ráfagas**: Pequeñas ráfagas permitidas dentro de la ventana de 5 ms, tráfico sostenido limitado por tasa

---

Problema: Tráfico unidireccional (uplink funciona, downlink no)

Síntomas:

- Paquetes RX N3 pero no paquetes TX N3 (problema de downlink)
- Paquetes RX N6 pero no paquetes TX N6 (problema de uplink)

Diagnóstico:

```
# Verificar estadísticas de interfaz N3/N6 (método consciente de
XDP)
curl http://localhost:8080/api/v1/n3n6_stats
curl http://localhost:8080/api/v1/packet_stats

# Nota: El tcpdump estándar no puede capturar tráfico GTP-U
procesado por XDP
# Use la API de estadísticas o xdpdump para análisis de tráfico
# Consulte la sección "Captura de Paquetes con XDP" para más
detalles
```

Fallo de Uplink (RX N3, sin TX N6):

Causa: Sin acción FAR o problema de enrutamiento hacia N6

Resolución:

```
# Verificar que FAR tenga acción FORWARD
curl http://localhost:8080/api/v1/sessions | jq '.[].fars[] |
select(.applied_action == 2)'

# Verificar que exista ruta N6
ip route get 8.8.8.8  # Probar ruta a internet

# Agregar ruta predeterminada si falta
sudo ip route add default via <N6_GATEWAY> dev eth1
```

Fallo de Downlink (RX N6, sin TX N3):

Causa: Sin PDR de downlink o encapsulación GTP faltante

Resolución:

```
# Verificar que exista PDR de downlink para la IP de UE
curl http://localhost:8080/api/v1/sessions | jq '.[].pdrs[] |
select(.pdi.ue_ip_address)'

# Verificar que FAR tenga CREACIÓN_DE_HEADER_EXTERNO
curl http://localhost:8080/api/v1/sessions | jq '.[].fars[] |
.outer_header_creation'

# Verificar conectividad con gNB
ping <GNB_N3_IP>
```

Problemas de XDP y eBPF

Para obtener detalles sobre la configuración de XDP, selección de modo y solución de problemas, consulte la Guía de Modos de XDP.

Problema: El programa XDP no se pudo cargar

Síntomas:

```
ERRO[0000] failed to load XDP program: invalid argument
```

Diagnóstico:

```
# Verificar soporte de XDP en el kernel
grep XDP /boot/config-$(uname -r)

# Debería mostrar:
# CONFIG_XDP_SOCKETS=y
# CONFIG_BPF=y
# CONFIG_BPF_SYSCALL=y

# Verificar dmesg para error detallado
dmesg | grep -i bpf
```

Causas y Resoluciones:

El kernel carece de soporte para XDP

Resolución:

```
# Reconstruir el kernel con soporte para XDP o actualizar a un
kernel más nuevo
# Ubuntu 22.04+ tiene XDP habilitado por defecto
sudo apt install linux-generic-hwe-22.04
sudo reboot
```

Fallo de verificación del programa XDP

Resolución:

```
# Verificar registros de OmniUPF en busca de errores de
verificador
journalctl -u omniupf | grep verifier

# Problemas comunes:
# - La complejidad de eBPF excede los límites (aumentar límites
del kernel)
# - Acceso a memoria inválido (error en el código eBPF)

# Aumentar el nivel de registro del verificador eBPF para
depuración
sudo sysctl kernel.bpf_stats_enabled=1
```

Problema: Contador de abortos de XDP en aumento

Síntomas:

- Las estadísticas de XDP muestran abortos > 0
- Aumento de caídas de paquetes

Diagnóstico:

```
# Verificar contador de abortos de XDP
curl http://localhost:8080/api/v1/xdp_stats | jq '.aborted'

# Monitorear estadísticas de XDP
watch -n 1 'curl -s http://localhost:8080/api/v1/xdp_stats'
```

Causa: el programa eBPF encontró un error en tiempo de ejecución

Resolución:

```
# Verificar registros del kernel en busca de errores de eBPF
dmesg | grep -i bpf

# Reiniciar OmniUPF para recargar el programa eBPF
sudo systemctl restart omniupf

# Si el problema persiste, habilitar el registro de eBPF (requiere
reconstrucción):
# Construir OmniUPF con BPF_ENABLE_LOG=1
```

Problema: Mapa eBPF lleno (capacidad agotada)

Síntomas:

- Fallo en el establecimiento de sesiones
- Capacidad del mapa al 100%

Diagnóstico:

```
# Verificar capacidad del mapa
curl http://localhost:8080/api/v1/map_info | jq '.[] | {map_name,
capacity, used, usage_percent}'

# Identificar mapas llenos
curl http://localhost:8080/api/v1/map_info | jq '.[] |
select(.usage_percent > 90)'
```

Mitigación Inmediata:

```
# 1. Identificar sesiones obsoletas
curl http://localhost:8080/api/v1/sessions | jq '.[] | {seid,
uplink_teid, created_at}'

# 2. Solicitar a SMF que elimine sesiones antiguas
# (a través de la interfaz de administración de SMF o API)

# 3. Monitorear disminución del uso del mapa
watch -n 5 'curl -s http://localhost:8080/api/v1/map_info | jq ".
[] | select(.map_name==\"pdr_map_downlin\") | .usage_percent"'
```

Resolución a Largo Plazo:

```
# En /etc/omniupf/runtime.exs
max_sessions = 200_000    # Aumentar de 100_000

# O establecer tamaños individuales de mapa
far_map_size = 400_000
qer_map_size = 200_000
```

Importante: Cambiar los tamaños de los mapas requiere reiniciar OmniUPF y **borra todas las sesiones existentes**.

Problemas de Rendimiento

Problema: Bajo rendimiento (por debajo de lo esperado)

Síntomas:

- Rendimiento < 1 Gbps a pesar de NIC capaz
- Alta utilización de CPU

Diagnóstico:

```
# Verificar tasa de paquetes
curl http://localhost:8080/api/v1/packet_stats | jq '.total_rx,
.total_tx'

# Verificar estadísticas de NIC
ethtool -S eth0 | grep -i drop

# Verificar modo XDP
ip link show eth0 | grep xdp
```

Resoluciones:

Usando modo XDP genérico

Resolución:

```
# En /etc/omniupf/runtime.exs
xdp_attach_mode = "native"    # Requiere NIC/controlador
compatible con XDP
```

Cuello de botella de un solo núcleo

Resolución:

```
# Habilitar RSS (Recepción de Distribución de Carga) en NIC
ethtool -L eth0 combined 4  # Usar 4 colas RX/TX

# Verificar que RSS esté habilitado
ethtool -l eth0

# Fijar interrupciones a CPUs específicas
# Ver /proc/interrupts y usar irqbalance o afinidad manual
```

Bloat de buffer

Resolución:

```
Los límites de buffer son gestionados por el plano de control de
Elixir.
Verifique la configuración del buffer en /etc/omniupf/runtime.exs.
```

Problema: Alta latencia

Síntomas:

- Latencia de ping > 50ms
- Degradación de la experiencia del usuario

Diagnóstico:

```
# Probar latencia hacia UE
ping -c 100 <UE_IP> | grep avg

# Verificar paquetes en buffer
curl http://localhost:8080/api/v1/upf_buffer_info | jq
'.total_packets_buffered'

# Verificar rendimiento de caché de ruta
curl http://localhost:8080/api/v1/packet_stats | jq '.route_stats'
```

Resoluciones:

Paquetes siendo almacenados en exceso

Resolución:

```
# Verificar por qué los paquetes están en buffer
curl http://localhost:8080/api/v1/upf_buffer_info | jq '.buffers[]
| {far_id, packet_count, direction}'

# Limpiar buffers si están atascados
# (reiniciar OmniUPF o activar modificación de sesión PFCP para
aplicar FAR)
```

Latencia de búsqueda FIB

Resolución:

```
# Asegurarse de que la caché de rutas esté habilitada (opción de
tiempo de construcción)
# Construir con BPF_ENABLE_ROUTE_CACHE=1

# Optimizar tabla de enrutamiento
# Usar rutas más específicas en lugar de muchas rutas pequeñas
```

Problema: Caídas de paquetes bajo carga

Síntomas:

- La tasa de caída aumenta con el tráfico
- Errores RX en NIC

Diagnóstico:

```
# Verificar errores en NIC
ethtool -S eth0 | grep -E "drop|error|miss"

# Verificar tamaño del buffer de anillo
ethtool -g eth0

# Monitorear caídas en tiempo real
watch -n 1 'ethtool -S eth0 | grep -E "drop|miss"'
```

Resolución:

```
# Aumentar tamaño del buffer de anillo RX
ethtool -G eth0 rx 4096

# Aumentar tamaño del buffer de anillo TX
ethtool -G eth0 tx 4096

# Verificar nuevas configuraciones
ethtool -g eth0
```

Problemas Específicos del Hipervisor

Para instrucciones de configuración del hipervisor paso a paso, consulte la Guía de Modos XDP.

Proxmox: XDP no funciona en VM

Síntomas:

- No se puede adjuntar el programa XDP en modo nativo
- Solo funciona el modo genérico

Causa: VM utilizando red puente sin SR-IOV

Resolución:

Opción 1: Usar modo genérico (más simple)

```
# En /etc/omniupf/runtime.exs
xdp_attach_mode = "generic"
```

Opción 2: Configurar SR-IOV passthrough

```
# En el host Proxmox:
# 1. Habilitar IOMMU
nano /etc/default/grub
# Agregar: intel_iommu=on iommu=pt
update-grub
reboot

# 2. Crear VFs
echo 4 > /sys/class/net/eth0/device/sriov_numvfs

# 3. Asignar VF a la VM en la interfaz de usuario de Proxmox
# Hardware → Agregar → Dispositivo PCI → Seleccionar VF
```

En `/etc/omniupf/runtime.exs`:

```
xdp_interfaces = "ens1f0"    # SR-IOV VF
xdp_attach_mode = "native"
```

VMware: Se requiere modo promiscuo

Síntomas:

- Paquetes no recibidos por OmniUPF

Causa: vSwitch bloqueando direcciones MAC no coincidentes

Resolución:

```
# Habilitar modo promiscuo en vSwitch (en vSphere Client):
# 1. Seleccionar vSwitch → Editar Configuración
# 2. Seguridad → Modo Promiscuo: Aceptar
# 3. Seguridad → Cambios de Dirección MAC: Aceptar
# 4. Seguridad → Transmisiones Falsificadas: Aceptar
```

VirtualBox: Rendimiento muy bajo

Síntomas:

- Rendimiento < 100 Mbps

Causa: VirtualBox no soporta SR-IOV ni XDP nativo

Resolución:

```
# En /etc/omniupf/runtime.exs
xdp_attach_mode = "generic"    # Única opción para VirtualBox
```

Optimizar la configuración de VirtualBox:

- Usar adaptador VirtIO-Net (si está disponible)
- Habilitar modo promiscuo "Permitir Todo"
- Asignar más núcleos de CPU a la VM
- Usar red puente en lugar de NAT
- Considerar migrar a KVM/Proxmox para un mejor rendimiento

Problemas de NIC y Controlador

Problema: El controlador de NIC no soporta XDP

Síntomas:

```
ERRO[0000] failed to attach XDP program: operation not supported
```

Diagnóstico:

```
# Comprobar el controlador de NIC
ethtool -i eth0 | grep driver

# Comprobar si el controlador soporta XDP
modinfo <driver_name> | grep -i xdp

# Listar interfaces capaces de XDP
ip link show | grep -B 1 "xdpgeneric\|xdpdrv\|xdpoffload"
```

Resolución:

Opción 1: Usar modo genérico

```
# En /etc/omniupf/runtime.exs
xdp_attach_mode = "generic"
```

Opción 2: Actualizar el controlador de NIC

```
# Comprobar actualizaciones del controlador (Ubuntu)
sudo apt update
sudo apt install linux-modules-extra-$(uname -r)

# O instalar controlador específico del proveedor
# Ejemplo para Intel:
# Descargar de https://downloadcenter.intel.com/
```

Opción 3: Reemplazar NIC

```
# Usar NIC capaz de XDP:
# - Intel X710, E810
# - Mellanox ConnectX-5, ConnectX-6
# - Broadcom BCM57xxx (controlador bnxt_en)
```

Problema: El controlador se bloquea o causa pánicos en el kernel

Síntomas:

- Pánico del kernel después de adjuntar XDP
- NIC deja de responder

Diagnóstico:

```
# Comprobar registros del kernel
dmesg | tail -100

# Comprobar errores del controlador
journalctl -k | grep -E "BUG:|panic:"
```

Resolución:

```
# 1. Actualizar kernel y controladores
sudo apt update
sudo apt upgrade
sudo reboot

# 2. En /etc/omniupf/runtime.exs, deshabilitar la descarga de XDP
(usar solo nativo)
# xdp_attach_mode = "native"

# 3. Usar modo genérico como solución alternativa
# xdp_attach_mode = "generic"

# 4. Reportar error al proveedor de NIC o al equipo del kernel de
Linux
```

Problema: Errores intermitentes de SLAAC IPv6 / errores de suma de verificación UDP (generic-XDP + virtio)

Síntomas:

```
# Los UEs IPv6 intermitentemente (~50%) nunca forman una dirección
global a través de SLAAC.
# El RA es emitido por el UPF pero nunca es visto por el RAN.
# En el eNB/gNB (o cualquier host descendente) el contador de
errores de suma de verificación UDP del kernel
# aumenta, uno por cada RA descartado:
nstat -az | grep UdpInCsumErrors      # se incrementa durante los
intentos fallidos de SLAAC
```

- Afecta **solo** a SLAAC IPv6 / Anuncios de Router — los datos del plano de usuario están bien.
- Ocurre **solo** cuando los SGW-U y PGW-U de un portador aterrizan en **diferentes** miembros del grupo (dividido); un portador SGW-U+PGW-U en la misma caja siempre tiene éxito.

Causa: El Anuncio de Router se genera en **espacio de usuario** (plano de control), por lo que su buffer de socket está marcado para descarga de suma de verificación TX (`CHECKSUM_PARTIAL`; el NIC del datapath tiene `tx-checksum-ip-generic: on`). En un datapath de **modo XDP genérico**, el paquete reenviado es un `skb` del kernel: cuando un miembro SGW-U de un grupo dividido reenvía ese RA, reescribe el IP externo + TEID y pone a cero `udp->check`, pero el skb mantiene el ahora obsoleto `csum_start`/`csum_offset` de descarga. Al salir, el NIC (virtio) vuelve a calcular la suma de verificación UDP sobre el paquete modificado desde ese offset obsoleto, produciendo una suma de verificación incorrecta, y el receptor lo descarta. El tráfico del plano de usuario XDP nativo no se ve afectado porque se construye en eBPF con `CHECKSUM_NONE` (una suma de verificación cero genuina), por lo que el NIC nunca la vuelve a calcular — por eso solo SLAAC se rompe. Los modos XDP nativo/descarga no se ven afectados (sin skb, sin recalculo de descarga); es específico del **modo genérico en un NIC que descarga la suma de verificación (por ejemplo, virtio)**.

Resolución:

```
# Deshabilitar la descarga de suma de verificación TX en el(los)
NIC del datapath para que el kernel calcule la
# suma de verificación UDP en línea (correctamente) para los
paquetes de control originados en espacio de usuario. El XDP
# del plano de datos evita la ruta de suma de verificación del
kernel, por lo que el rendimiento de reenvío no se ve afectado.
ethtool -K <n3_iface> tx off
ethtool -K <n6_iface> tx off

# Verificar (debería leer "off"):
ethtool -k <n3_iface> | awk '/^tx-checksumming/{print}'

# Volver a probar: SLAAC ahora debería tener éxito para cada
portador y UdpInCsumErrors debe permanecer plano.
```

> Hágalo persistente en su implementación (por ejemplo, en la unidad de activación del NIC del datapath) para que sobreviva a los reinicios. Donde el NIC lo soporte, el modo XDP nativo (`xdp_attach_mode: native`) también evita el problema por completo.

Fallos en el Establecimiento de Sesiones

Problema: Fallo en el establecimiento de la sesión

Síntomas:

- SMF informa fallo en el establecimiento de la sesión
- UE no puede establecer la sesión PDU

Consulte Códigos de Causa PFCP para escenarios de fallo comunes y resoluciones.

Diagnóstico:

```
# Comprobar registros de OmniUPF para errores de sesión
journalctl -u omniupf | grep -i "session establishment"

# Comprobar el conteo de sesiones PFCP
curl http://localhost:8080/api/v1/sessions | jq 'length'

# Capturar tráfico PFCP durante el establecimiento de la sesión
tcpdump -i any -n udp port 8805 -w /tmp/pfcp_session.pcap
```

Causas Comunes:

Capacidad del mapa llena

Resolución:

```
# Comprobar uso del mapa
curl http://localhost:8080/api/v1/map_info | jq '.[] |
select(.usage_percent > 90)'

# Aumentar capacidad (ver sección de mapa eBPF llena arriba)
```

Parámetros PDR/FAR inválidos

Resolución:

```
# Comprobar registros de OmniUPF para errores de validación
journalctl -u omniupf | grep -E "invalid|error" | tail -20

# Problemas comunes:
# - Dirección IP de UE inválida (0.0.0.0 o duplicada)
# - TEID inválido (0 o duplicado)
# - FAR faltante para PDR
# - Acción FAR inválida

# Verificar configuración de SMF y parámetros de sesión
```

Característica no soportada (UEIP/FTUP)

Resolución:

```
# En /etc/omniupf/runtime.exs
feature_ueip = true
ueip_pool = "10.60.0.0/16"

feature_ftup = true
teid_pool_start = 1
teid_pool_end = 0xFFFFFFFF
```

Problemas de Buffer

Problema: Paquetes atascados en el buffer

Síntomas:

- Conteo de paquetes en buffer en aumento
- Paquetes no entregados después de la transferencia

Diagnóstico:

```
# Comprobar estadísticas del buffer
curl http://localhost:8080/api/v1/upf_buffer_info

# Comprobar buffers de FAR individuales
curl http://localhost:8080/api/v1/upf_buffer_info | jq '.buffers[]
| {far_id, packet_count, oldest_packet_ms}'

# Monitorear tamaño del buffer
watch -n 5 'curl -s http://localhost:8080/api/v1/upf_buffer_info |
jq ".total_packets_buffered"'
```

Causas y Resoluciones:

FAR nunca actualizado a FORWARD

Causa: SMF nunca envió modificación de sesión PFCP para aplicar FAR

Resolución:

```
# Comprobar estado de FAR
curl http://localhost:8080/api/v1/sessions | jq '.[].fars[] |
{far_id, applied_action}'

# Acción BUFF = 1 (almacenamiento)
# Acción FORW = 2 (reenvío)

# Si está atascado en estado BUFF, solicitar a SMF que:
# - Enviar solicitud de modificación de sesión PFCP
# - Actualizar FAR con acción FORW
```

Expiración de TTL del buffer

Causa: Paquetes expiraron antes de la actualización de FAR

Resolución: El TTL del buffer es gestionado por el plano de control de Elixir. Verifique la configuración del buffer en `/etc/omniupf/runtime.exs`.

Desbordamiento del buffer

Causa: Demasiados paquetes almacenados por FAR

Resolución: Los límites del buffer son gestionados por el plano de control de Elixir. Verifique la configuración del buffer en `/etc/omniupf/runtime.exs`.

Depuración Avanzada

Habilitar Registro de Depuración

```
# En /etc/omniupf/runtime.exs
log_level = :debug    # :debug | :info | :warning | :error
```

```
# Reiniciar OmniUPF con registro de depuración
sudo systemctl restart omniupf

# Monitorear registros en tiempo real
journalctl -u omniupf -f --output cat
```

Trazado de Programas eBPF

```
# Rastrear la ejecución del programa eBPF (requiere bpftrace)
sudo bpftrace -e 'tracepoint:xdp:* { @[probe] = count(); }'

# Rastrear operaciones de mapa
sudo bpftrace -e 'tracepoint:bpf:bpf_map_lookup_elem {
printf("%s\n", str(args->map_name)); }'
```

Captura de Paquetes con XDP

Entendiendo las Limitaciones de Captura de Paquetes XDP:

XDP procesa paquetes **antes** de la pila de red del kernel, por lo que `tcpdump` estándar **no puede ver el tráfico procesado por XDP**. Los paquetes GTP-U (puerto UDP 2152) en N3 son procesados por XDP y no aparecerán en tcpdump en el host UPF.

Métodos Recomendados para Análisis de Tráfico:

```
# Método 1: Usar API de estadísticas para monitoreo (RECOMENDADO)
curl http://localhost:8080/api/v1/xdp_stats
curl http://localhost:8080/api/v1/packet_stats | jq
curl http://localhost:8080/api/v1/n3n6_stats

# Método 2: Capturar tráfico PFCP (no afectado por XDP)
tcpdump -i any -n udp port 8805 -w /tmp/pfcp.pcap

# Método 3: Captura de paquetes fuera de banda (RECOMENDADO para
GTP-U)
# Usar TAP de red o espejado de puerto de switch para capturar
tráfico
# Ejemplos:
# - TAP físico entre gNB y UPF
# - Puerto SPAN/espejado de switch copiando tráfico N3 a
analizador
# - Espejado de puerto de switch virtual en hipervisor
#
# En el host de captura (NO el UPF):
# tcpdump -i <mirror_interface> -n udp port 2152 -w
/tmp/n3_mirror.pcap
```

Ejemplos de Configuración de Captura Fuera de Banda:

Red Física:

```
# Usar un TAP de red o configurar el espejado de puerto del switch
# Ejemplo: configuración SPAN de switch Cisco
(config)# monitor session 1 source interface Gi1/0/1
(config)# monitor session 1 destination interface Gi1/0/24

# En el host de monitoreo conectado a Gi1/0/24:
tcpdump -i eth0 -n udp port 2152 -w /tmp/n3_capture.pcap
```

Entorno Virtual (VMware, KVM, etc.):

```
# Configurar el espejado de puerto del switch virtual para enviar
tráfico UPF a la VM analizador
# Ejemplo: puente de Linux con tcpdump en VM diferente
# En el hipervisor, espejar la interfaz N3 del UPF a la interfaz
del analizador

# En la VM analizador:
tcpdump -i eth1 -n udp port 2152 -w /tmp/n3_virtual.pcap
```

Por qué se requiere captura fuera de banda:

- XDP evita completamente la pila de red del kernel
- Los paquetes se procesan en el controlador NIC o hardware
- `tcpdump` basado en host ve los paquetes DESPUÉS del procesamiento de XDP (demasiado tarde)
- La captura fuera de banda ve el tráfico en crudo antes del procesamiento del UPF

Lo que PUEDE Capturar en el Host UPF:

- □ Tráfico PFCP (UDP 8805) - plano de control, no procesado por XDP
- □ Respuestas de API y métricas
- □ Tráfico GTP-U (UDP 2152) - plano de datos, procesado por XDP

Obtener Ayuda

Si los pasos de solución de problemas no resuelven su problema:

1. **Recopilar información de diagnóstico**:

```
# Información del sistema
uname -a
cat /etc/os-release

# Información de OmniUPF
curl http://localhost:8080/api/v1/upf_status
curl http://localhost:8080/api/v1/map_info
curl http://localhost:8080/api/v1/packet_stats

# Registros
journalctl -u omniupf --since "1 hour ago" > /tmp/omniupf.log
dmesg > /tmp/dmesg.log

# Información de red
ip addr > /tmp/network.txt
ip route >> /tmp/network.txt
ethtool eth0 >> /tmp/network.txt
```

2. **Reportar problema** con:
    - Versión de OmniUPF
    - Versión del kernel de Linux
    - Diagrama de topología de red
    - Archivo de configuración (redactar información sensible)
    - Extractos de registros relevantes
    - Pasos para reproducir

Documentación Relacionada

- **Guía de Configuración** - Parámetros de configuración y ejemplos
- **Guía de Arquitectura** - Internos de eBPF/XDP y ajuste de rendimiento
- **Guía de Monitoreo** - Estadísticas, capacidad y alertas
- **Referencia de Métricas** - Métricas de Prometheus para solución de problemas
- **Códigos de Causa PFCP** - Códigos de error PFCP y solución de problemas
- **Guía de Gestión de Reglas** - Conceptos de PDR, FAR, QER, URR

- **Guía de Operaciones** - Arquitectura y visión general del UPF

OmniUPF Jardín Amurallado / Redirección Fuera de Crédito

Tabla de Contenidos

1. Descripción General
2. Arquitectura
3. Flujo de Señalización PFCP
4. Detección de Portal Captivo
5. Configuración
6. Gestión de Lista Blanca
7. URLs de Redirección por Sesión
8. API
9. Métricas de Prometheus
10. Solución de Problemas

Descripción General

La función de Jardín Amurallado proporciona **aplicación nativa de fuera de crédito** directamente en el UPF, eliminando la necesidad de sistemas de aplicación externos (listas de direcciones MikroTik, reglas de mangle, DNAT).

Cuando un suscriptor se queda sin crédito, el SMF envía una Modificación de Sesión PFCP con un FAR que contiene `redirect_information`. OmniUPF intercepta todo el tráfico de esa sesión en el espacio de usuarios y aplica una experiencia de portal cautivo:

- **Las consultas DNS** son suplantadas para devolver la IP del servidor del portal, activando la detección de portal cautivo en todos los dispositivos principales (Apple, Android, Windows)
- **El tráfico hacia el portal y las IPs en la lista blanca** (procesadores de pago, servicios CAPTCHA) se reenvía normalmente para que el suscriptor pueda recargar
- **Todo el demás tráfico** se descarta silenciosamente

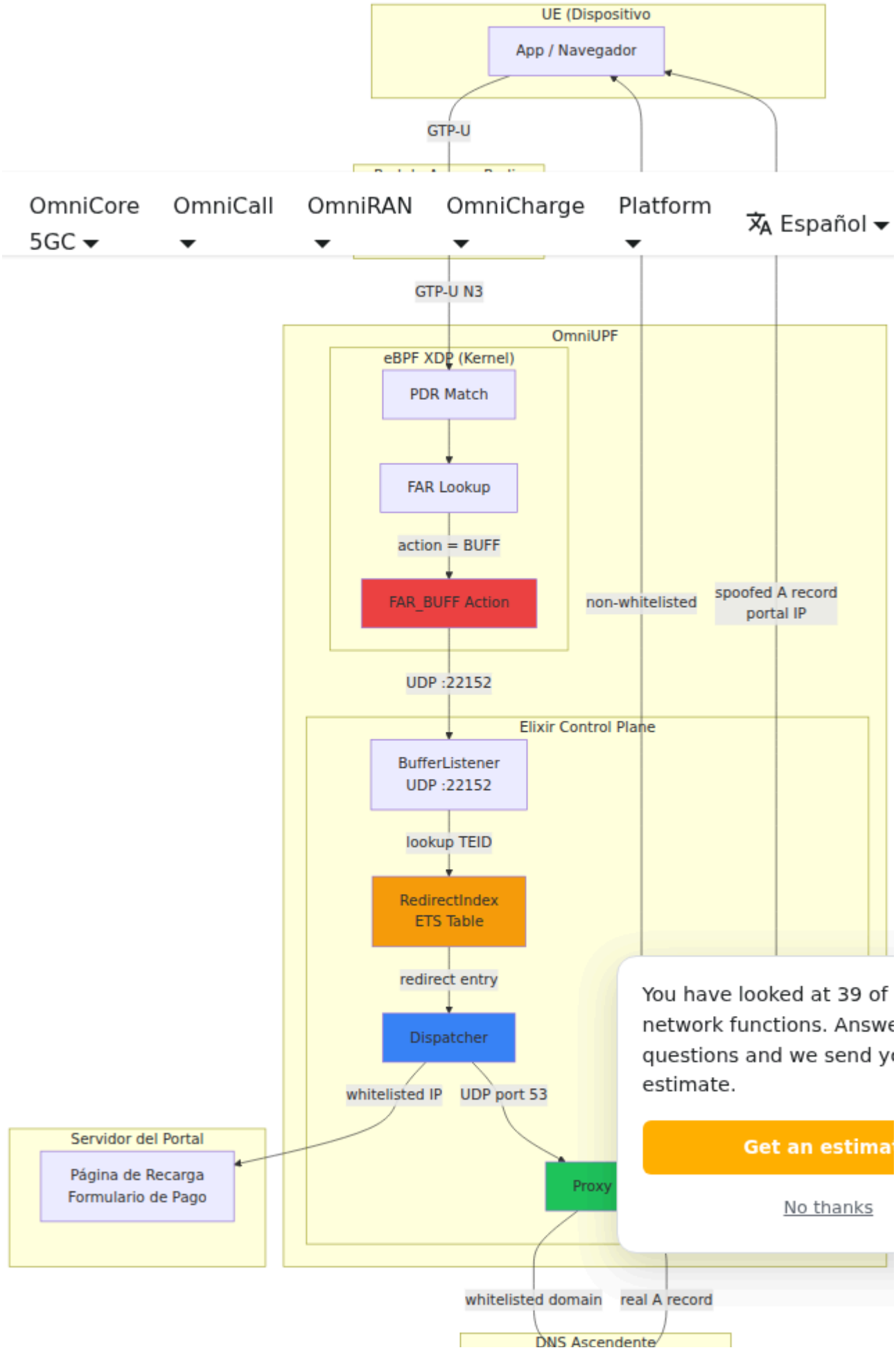
El suscriptor ve un aviso de portal cautivo y es dirigido a una página de recarga/pago. Una vez que se restaura el crédito, el SMF actualiza el FAR de nuevo a FORW y el reenvío normal se reanuda inmediatamente.

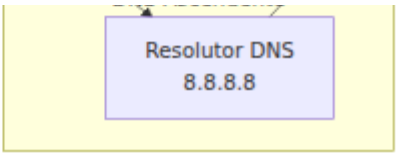
Puntos Clave de Diseño

- **No se requieren cambios en eBPF** -- reutiliza la acción existente `FAR_BUFF` para redirigir paquetes al espacio de usuarios
- **Redirección por sesión** -- cada sesión puede tener una IP de portal y URL de redirección diferentes, determinadas por el IE `redirect_information` del SMF
- **La lista blanca vive en el UPF** -- el SMF solo dice "redirigir esta sesión"; el UPF decide qué tráfico permitir
- **Intercepción solo de enlace ascendente** -- el FAR de enlace descendente permanece FORW para que las respuestas del portal lleguen al UE a través de la ruta de encapsulación GTP normal

---

Arquitectura


UE (Dispositivo
App / Navegador
GTP-U
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Español
GTP-U N3
OmniUPF
eBPF XDP (Kernel)
PDR Match
FAR Lookup
action = BUFF
FAR_BUFF Action
non-whitelisted
spoofed A record portal IP
UDP :22152
Elixir Control Plane
BufferListener UDP :22152
lookup TEID
RedirectIndex ETS Table
redirect entry
Dispatcher
whitelisted IP
UDP port 53
Servidor del Portal
Página de Recarga Formulario de Pago
Proxy
whitelisted domain
real A record
DNS Ascendente
You have looked at 39 of
network functions. Answe
questions and we send y
estimate.
Get an estima
No thanks



Flujo de Paquetes

1. **UE envía paquete de enlace ascendente** (consulta DNS, solicitud HTTP, etc.) a través de GTP-U al UPF
2. **Coincidencia de PDR eBPF** encuentra el PDR coincidente, busca el FAR
3. **La acción del FAR es BUFF** (sobrescrita de FORW cuando la redirección está activa) -- eBPF envía el paquete al BufferListener en el puerto UDP 22152
4. **BufferListener** extrae el TEID, verifica la tabla ETS RedirectIndex
5. Si el TEID está en el RedirectIndex: **Dispatcher** procesa el paquete IP interno
6. **Árbol de decisiones**:
   - Consulta DNS para dominio no en la lista blanca: suplantar A record con IP del portal
   - Consulta DNS para dominio en la lista blanca: reenviar al resolutor real, almacenar IPs resueltas
   - Tráfico a IP del portal o IP en la lista blanca: reenviar a través de socket crudo
   - Todo lo demás: descartar silenciosamente
7. **Respuestas DNS/GTP-U** se envían de vuelta al UE a través de la ruta GTP-U de enlace descendente (encapsuladas con el TEID DL y enviadas al gNB)

Manejo de Loopback N9 (Sesión Dual SGW + PGW)

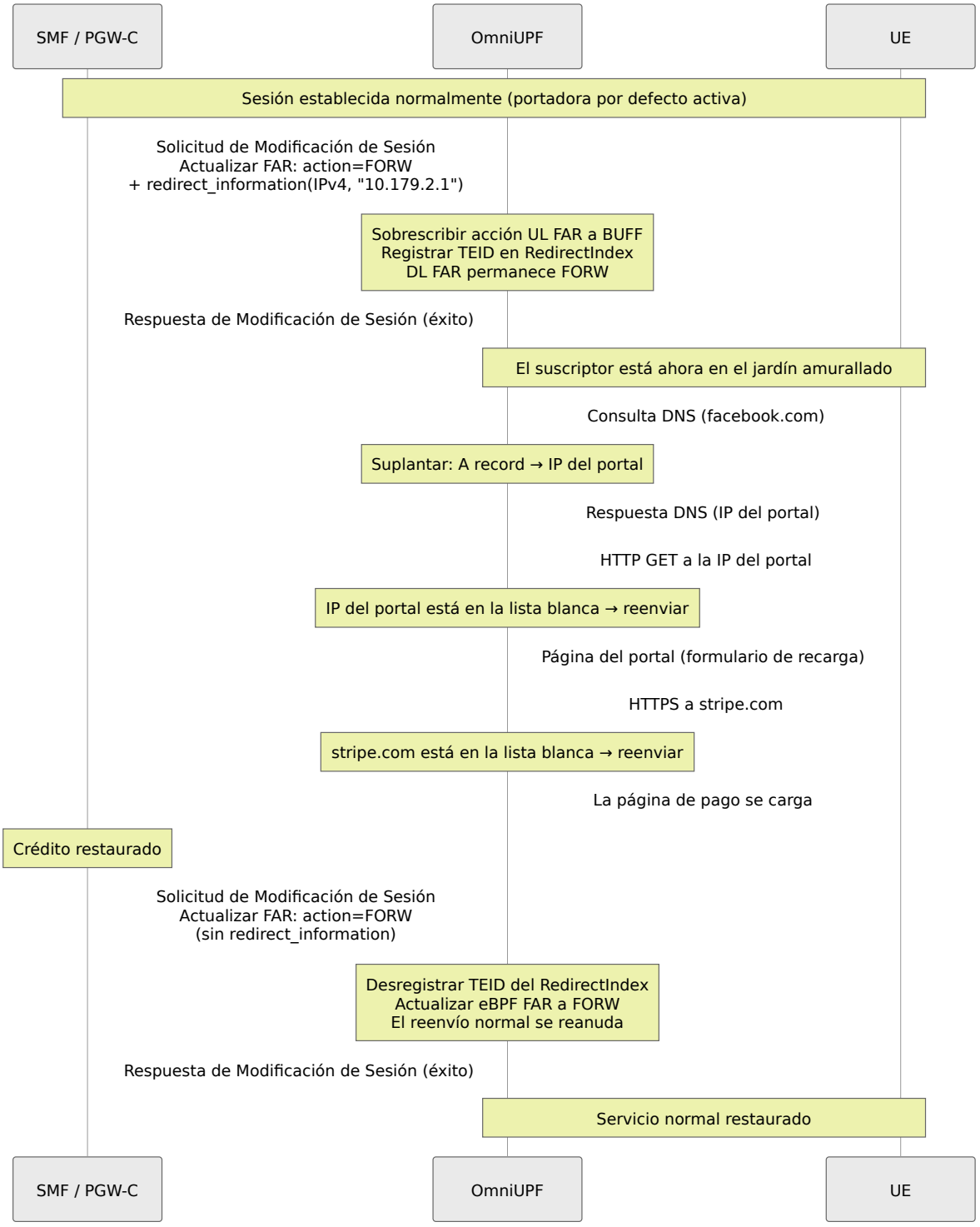
En implementaciones EPC 4G, OmniUPF a menudo actúa como **SGW-U y PGW-U simultáneamente** en el mismo nodo. El SGW-C y el PGW-C establecen cada uno una sesión PFCP separada. La sesión SGW tiene un FAR N9 que reenvía paquetes al TEID de enlace ascendente de la sesión PGW (un loopback a través de la interfaz N3). La sesión PGW realiza la aplicación real de políticas del suscriptor.

Al activar una redirección de jardín amurallado a través de `POST /v1/walled_garden`, la lógica de activación detecta automáticamente esta topología:

1. **TEID(s) de sesión PGW** se identifican a partir de los PDRs de enlace ascendente del SEID objetivo.
2. El código escanea todas las sesiones PFCP para encontrar una sesión (la sesión SGW) que tenga un FAR cuyo `teid` coincida con uno de los TEIDs de PDR UL de PGW y tenga `outer_header_creation` configurado. Ese FAR es el FAR de avance N9 que apunta al PGW.
3. **Ambos** los FARs UL de PGW y los FARs UL de SGW que miran hacia el gNB se sobrescriben a `BUFF` en el mapa eBPF. Esto es necesario porque el programa eBPF ve el paquete a medida que llega desde el eNB con el TEID de SGW, no el TEID de PGW.
4. Solo los **PDRs UL de SGW que miran hacia el gNB** se registran en el RedirectIndex (no los PDRs UL de PGW). El TEID del PDR UL de SGW es lo que eBPF verá en el paquete entrante del eNB.
5. Para la **ruta DL** (enviando respuestas de vuelta al UE), el Dispatcher utiliza el **FAR DL de la sesión SGW** (el FAR que reenvía hacia el eNB, con `remoteip != n3_address`). Este FAR contiene el TEID actual del eNB y la IP del gNB. El TEID DL se busca en vivo desde el estado de la sesión en el momento de la respuesta, no se almacena en caché en el momento de la activación - esto maneja el caso donde el TEID del eNB es asignado por una modificación de sesión posterior a la activación de la redirección.

En una topología UPF directa (sin SGW, SMF habla directamente con UPF), solo se involucran los propios FARs y TEIDs UL de la sesión - el código de detección de SGW no encuentra nada y los PDRs UL de la sesión principal se registran directamente.

Flujo de Señalización PFCP



IEs PFCP Involucrados

El SMF activa una redirección incluyendo `redirect_information` en los `forwarding_parameters` del FAR:

IE	Descripción
`apply_action`	Establecido en FORW por SMF (UPF lo sobrescribe a BUFF internamente)
`redirect_information`	Contiene el tipo de redirección y la dirección
`forwarding_parameters`	Contiene la `redirect_information` y `outer_header_creation`

Tipos de Información de Redirección (según 3GPP TS 29.244 Tabla 8.2.20-1):

Tipo	Valor	Comportamiento del UPF
IPv4	0	Utiliza la cadena de dirección IPv4 proporcionada como la IP del portal
IPv6	1	Utiliza la cadena de dirección IPv6 proporcionada como la IP del portal
URL	2	Resuelve el nombre de host de la URL a una IP; utiliza eso como la IP del portal. La ruta de la URL no es utilizada por el UPF -- se almacena en la API solo para visibilidad. El servidor web del portal es responsable de manejar cualquier enrutamiento basado en la ruta.
SIP URI	3	No soportado actualmente

Detección de Portal Captivo

El jardín amurallado activa **detección automática de portal cautivo** en todas las principales plataformas de dispositivos al suplantar las respuestas

DNS. Cuando un dispositivo se conecta e intenta verificar la conectividad a Internet, consulta dominios bien conocidos. La respuesta DNS suplantada redirige estas verificaciones a la IP del portal, que el dispositivo interpreta como un portal cautivo.

Dominios de Detección de Plataforma

Plataforma	Dominio de Detección	Respuesta Esperada
Apple (iOS/macOS)	`captive.apple.com`	HTTP 200 con `<HTML> <HEAD> <TITLE>Success</TITLE> </HEAD> <BODY>Success</BODY> </HTML>`
Android	`connectivitycheck.gstatic.com`	HTTP 204
Windows	`www.msftconnecttest.com`	HTTP 200 con `Microsoft Connect Test`
Samsung	`connectivitycheck.samsung.com`	HTTP 200

Cuando estos dominios se resuelven a la IP del portal en lugar de sus direcciones reales, el dispositivo detecta un portal cautivo y presenta la página del portal al usuario ya sea como:

- Una notificación/popup (iOS, Android)
- Un redireccionamiento automático del navegador (Windows)

El servidor del portal en la IP del portal configurada debe servir respuestas apropiadas para estas URLs de detección y luego redirigir a la página de recarga/pago.

Requisitos del Servidor del Portal (IP Dedicada / vHost por Defecto)

El portal debe servir la página de portal cautivo como la *respuesta por defecto* de su dirección IP, independientemente del encabezado HTTP `Host`. En la práctica, esto significa darle al portal su **propia IP dedicada**, o hacerlo el **host virtual por defecto** en un host compartido.

Este requisito sigue directamente de cómo funciona el jardín amurallado:

1. Cada consulta DNS no en la lista blanca es **suplantada a la IP del portal** -- incluyendo las sondas de portal cautivo de la plataforma (`connectivitycheck.gstatic.com`, `captive.apple.com`, `www.msftconnecttest.com`, ...).
2. El UE luego abre HTTP a la IP del portal, pero la solicitud lleva el encabezado `Host` de la **sonda** (por ejemplo, `Host: connectivitycheck.gstatic.com`), no el nombre de host del portal.
3. El UPF reenvía esa solicitud al servidor del portal **verbatim, sin reescribir el encabezado `Host`** (ver Reenvío de Socket Crudo).

Si la IP del portal es un **host virtual basado en nombre** -- es decir, la página del portal solo se sirve para un valor específico de `Host:` y la IP se comparte con otros vhosts -- el servidor no encontrará un vhost que coincida con el encabezado `Host` de la sonda y servirá su **vhost por defecto**, que es la página incorrecta. El suscriptor aterriza en cualquier otra cosa que esté alojada en esa IP (otra aplicación, un CRM, un sitio en blanco por defecto) en lugar de la página de recarga.

Hacer esto:

- Dar al portal cautivo su **propia dirección IP** (cualquier `Host` servido por esa IP devuelve la página del portal), **o**
- Hacer del portal el **host virtual por defecto** en el host compartido, de modo que cualquier `Host:` no coincidente caiga en la página del portal.

Evitar: apuntar `walled_garden_portal_ip` (o un `redirect_information` de tipo URL cuyo nombre de host se resuelve) a una IP cuya **respuesta HTTP por**

defecto *no* sea la página del portal. El UPF no realiza selección de vhost basada en `Host` ni reescribe `Host` en nombre del portal.

Configuración

La configuración del jardín amurallado vive en el archivo de configuración en tiempo de ejecución. En una instalación de producción (`.deb` package), el archivo de configuración está en `/etc/omniupf/runtime.exs`. El script de inicio de la versión (`rel/env.sh`) verifica este archivo y, si está presente, establece `RELEASE_CONFIG_DIR=/etc/omniupf` para que la versión de Erlang lo use en lugar del `config/runtime.exs` empaquetado. El UPF debe reiniciarse después de los cambios en la configuración.

```
#
================================================================
# Jardín Amurallado / Redirección Fuera de Crédito
#
================================================================

# Habilitar la aplicación de redirección del jardín amurallado
walled_garden_enabled = true

# IP del servidor del portal (portal cautivo / página de recarga)
walled_garden_portal_ip = "10.179.2.1"

# Dirección del servidor del portal IPv6 opcional (fallback para susc
IPv6)
walled_garden_portal_ip6 = "fd00:179:2::1"

# Resolutor DNS ascendente para búsquedas de dominios en la lista bla
walled_garden_dns_resolver = "8.8.8.8"

# Dominios en la lista blanca (los suscriptores pueden acceder a estc
mientras están redirigidos)
# Soporta comodines: "*.stripe.com" coincide con "api.stripe.com"
walled_garden_whitelist = [
  "stripe.com",
  "*.stripe.com",
  "js.stripe.com",
  "hcaptcha.com",
  "*.hcaptcha.com",
  "newassets.hcaptcha.com",
]
```

Parámetros

Parámetro	Tipo	Requerido	Por Defecto	

`walled_garden_enabled`	Booleano	No	`false`	Int
				la f
				am
				`fa`
				`re`
				los

`walled_garden_portal_ip`	Cadena (IPv4)	Sí (si está habilitado)	`10.179.2.1`	Dir cau rec por util pue de `re` del de Par util dir tip hos mo del
`walled_garden_portal_ip6`	Cadena (IPv6)	No	`nil`	Dir opc por sus mis util `wa`

Parámetro	Tipo	Requerido	Por Defecto	
				par cor res IPv
`walled_garden_dns_resolver`	Cadena (IPv4)	No	`8.8.8.8`	Res util cor en cor la l est der sup
`walled_garden_whitelist`	Lista de Cadenas	No	`[]`	Pat que pue est am de sin

Gestión de Lista Blanca

La lista blanca controla qué dominios (y sus IPs resueltas) pueden alcanzar los suscriptores mientras están redirigidos. Esto se configura en el UPF, no en el SMF -- el SMF solo activa la redirección.

Sintaxis de Patrones

Patrón	Coincide	No Coincide
`stripe.com`	`stripe.com`, `api.stripe.com`, `js.stripe.com`	`evilstripe.com`, `notstripe.com`
`*.stripe.com`	`api.stripe.com`, `js.stripe.com`, `dashboard.stripe.com`	`stripe.com` (exacto), `evilstripe.com`
`hcaptcha.com`	`hcaptcha.com`, `newassets.hcaptcha.com`	`evihcaptcha.com`

Los patrones utilizan **anclaje de subdominio**: `stripe.com` coincide con el dominio en sí y cualquier subdominio (`foo.stripe.com`), pero no con dominios que simplemente contienen la cadena (`evilstripe.com`). La coincidencia no distingue entre mayúsculas y minúsculas.

Caché de IP

Cuando el proxy DNS reenvía una consulta para un dominio en la lista blanca, las direcciones IP resueltas se **almacenan automáticamente en caché** en la lista blanca. Esto significa:

1. El suscriptor consulta `api.stripe.com`
2. El proxy DNS reenvía al resolutor real, recibe `203.0.113.7`
3. `203.0.113.7` se agrega a la caché de IPs en la lista blanca
4. El tráfico HTTP/HTTPS subsiguiente a `203.0.113.7` se reenvía (no se descarta)

La IP del portal siempre está en la lista blanca independientemente de la configuración.

Dominios Recomendados en la Lista Blanca

Para un portal de recarga típico con procesamiento de pagos de Stripe y hCaptcha:

```
walled_garden_whitelist = [
  # Procesador de pagos
  "stripe.com",
  "*.stripe.com",

  # Servicio CAPTCHA
  "hcaptcha.com",
  "*.hcaptcha.com",

  # Fuentes de Google (si el portal las utiliza)
  "fonts.googleapis.com",
  "fonts.gstatic.com",

  # CDN para activos del portal (si se alojan externamente)
  "cdn.example.com",
]
```

URLs de Redirección por Sesión

Cada sesión PFCP puede tener un **objetivo de redirección diferente**. El SMF controla esto a través del IE `redirect_information` en el FAR:

- **Tipo IPv4**: La cadena de IP proporcionada se analiza y se utiliza como la IP del portal para esa sesión
- **Tipo IPv6**: La cadena IPv6 proporcionada se analiza y se utiliza como la IP del portal para esa sesión
- **Tipo URL**: El nombre de host se extrae y se resuelve a través de DNS en el momento de la creación del FAR. La IP resuelta se utiliza como la IP del portal. La ruta de la URL no es utilizada por el UPF -- se almacena solo para visibilidad en la API.

Esto permite escenarios donde diferentes niveles de suscriptores, MVNOs o planes de servicio redirigen a diferentes portales:

Sesión	`redirect_information` del SMF	IP del Portal Utilizada	UR
Sesión A	`IPv4: 10.179.2.1`	`10.179.2.1`	`10.179.2`
Sesión B	`IPv6: 2001:db8::1`	`2001:db8::1`	`2001:db8`
Sesión C	`URL: https://topup.mvno.com/recharge`	IP resuelta de `topup.mvno.com`	`https://`

El UPF almacena la IP del portal por sesión y la URL de redirección, que son visibles a través de la API.

API

La ruta base para todos los puntos finales del jardín amurallado es `/v1/walled_garden` (sin prefijo `/api`). Estos puntos finales son servidos por el servidor HTTP Phoenix en el `api_port` configurado (por defecto: 8080).

GET /v1/walled_garden

Devuelve todas las sesiones de redirección activas del jardín amurallado, IPs en la lista blanca, rangos CIDR en caché y detalles de la sesión.

Respuesta:

```
{
  "redirect_count": 2,
  "redirects": [
    {
      "teid": "0x4000",
      "session_seid": 1,
      "portal_ip": "10.179.2.1",
      "redirect_url": null,
      "ue_ip": "10.60.0.1",
      "gnb_ip": "10.179.1.21",
      "dl_teid": "0x5000",
      "far_global_id": 42
    },
    {
      "teid": "0x4001",
      "session_seid": 2,
      "portal_ip": "10.179.2.2",
      "redirect_url": "https://topup.mvno.com",
      "ue_ip": "10.60.0.2",
      "gnb_ip": "10.179.1.21",
      "dl_teid": "0x5001",
      "far_global_id": 43
    }
  ],
  "whitelisted_ips": [
    {"ip": "10.179.2.1", "type": "portal"},
    {"ip": "203.0.113.7", "type": "resolved"},
    {"ip": "203.0.113.6", "type": "resolved"}
  ],
  "whitelisted_cidrs": ["192.168.0.0/24"]
}
```


Campos de Respuesta:

Campo	Descripción
`redirect_count`	Número de sesiones activas en el jardín amurallado
`redirects[].teid`	TEID de enlace ascendente que está siendo interceptado (hex)
`redirects[].session_seid`	SEID de sesión PFCP
`redirects[].portal_ip`	IP del portal para esta sesión específica
`redirects[].redirect_url`	URL de redirección del SMF (si es tipo URL), o null
`redirects[].ue_ip`	Dirección IP del UE
`redirects[].gnb_ip`	IP del gNB para respuestas GTP-U
`redirects[].dl_teid`	TEID de enlace descendente para encapsulación GTP-U
`redirects[].far_global_id`	ID global FAR interno
`whitelisted_ips`	Todas las IPs actualmente en la lista blanca (portal + resoluciones DNS en caché)
`whitelisted_cidrs`	Rangos CIDR añadidos a través de la API de lista blanca

POST /v1/walled_garden

Activa la redirección del jardín amurallado en una sesión PFCP existente por SEID. Este es el camino activado por el operador/API - el camino normal es a través de la Modificación de Sesión PFCP con `redirect_information` en un

FAR. La ruta de la API es útil para pruebas y para operadores que necesitan redirigir manualmente una sesión sin la participación del SMF.

Cuerpo de la solicitud:

```
{
  "seid": 1,
  "url": "http://10.179.2.1/"
}
```

Campo	Tipo	Requerido	Descripción
`seid`	Entero	Sí	SEID local de la sesión PFCP a redirigir
`url`	Cadena	Sí	Objetivo de redirección - una dirección IPv4/IPv6 o una URL. Si se proporciona una URL, se resuelve el nombre de host y se utiliza la IP resultante como la IP del portal. La cadena completa de la URL se almacena para visibilidad en la API.

Respuesta (200 OK):

```
{
  "status": "redirect activated",
  "info": {
    "seid": 1,
    "sgw_seid": 7,
    "portal_ip": "10.179.2.1",
    "ue_ip": "10.60.0.1",
    "gnb_ip": "10.179.1.21",
    "ul_teids": ["0x4000", "0x4006"]
  }
}
```

El campo `sgw_seid` es no nulo cuando se detectó un loopback N9 (sesión emparejada SGW+PGW) y su TEID de enlace ascendente también fue BUFF'd.

`ul_teids` lista todos los TEIDs de enlace ascendente que fueron registrados en el índice de redirección.

Respuestas de error:

Estado	Significado
404	Sesión no encontrada (SEID no coincide con ninguna sesión PFCP activa)
400	Parámetros requeridos faltantes

DELETE /v1/walled_garden/:seid

Desactiva la redirección del jardín amurallado para una sesión, restaurando el reenvío normal. Todos los FARs de enlace ascendente para la sesión (incluyendo los FARs de sesión SGW emparejados en una topología de loopback N9) se restablecen a `action=FORW` en el mapa eBPF, y los TEIDs se desregistran del índice de redirección.

Parámetro de ruta: `:seid` - el SEID local de la sesión a desactivar.

Respuesta (200 OK):

```
{"status": "redirect removed", "info": {"seid": 1}}
```

Respuestas de error:

Estado	Significado
404	Sesión no encontrada

GET /v1/walled_garden/whitelist

Devuelve la lista blanca actual: IPs individuales en caché (IP del portal y IPs resueltas por DNS) y cualquier rango CIDR añadido a través de la API.

Respuesta:

```
{
  "ips": [
    {"ip": "10.179.2.1", "type": "portal"},
    {"ip": "203.0.113.7", "type": "resolved"}
  ],
  "cidrs": ["192.168.100.0/24"]
}
```

POST /v1/walled_garden/whitelist

Agrega una dirección IP o rango CIDR a la lista blanca en tiempo de ejecución, sin reiniciar el UPF. Los cambios son solo en memoria y no persisten entre reinicios - agrega entradas permanentes a `walled_garden_whitelist` en `runtime.exs`.

Cuerpo de la solicitud (agregar una IP):

```
{"ip": "203.0.113.10"}
```

Cuerpo de la solicitud (agregar un rango CIDR):

```
{"cidr": "192.168.100.0/24"}
```

Exactamente uno de `ip` o `cidr` debe estar presente. Agregar un rango CIDR significa que cualquier tráfico a IPs dentro de ese rango es reenviado por el dispatcher sin necesidad de una entrada de caché DNS por IP.

Respuesta (200 OK - IP agregada):

```
{"status": "added", "ip": "203.0.113.10"}
```

Respuesta (200 OK - CIDR agregado):

```
{"status": "added", "cidr": "192.168.100.0/24"}
```

Respuestas de error:

Estado	Significado
400	IP inválida, CIDR inválido o campos del cuerpo faltantes

Métricas de Prometheus

Medidores

Métrica: `upf_walled_garden_active_redirects` **Tipo**: Medidor **Descripción**: Número de sesiones actualmente en estado de redirección del jardín amurallado

Consultas de ejemplo:

```
# Conteo de redirecciones actuales
upf_walled_garden_active_redirects
```

Contadores

Métrica: `upf_walled_garden_packets_intercepted_total` **Tipo**: Contador **Descripción**: Total de paquetes interceptados por el jardín amurallado (todo el tráfico de enlace ascendente de sesiones redirigidas)

Métrica: `upf_walled_garden_packets_dropped_total` **Tipo**: Contador **Descripción**: Total de paquetes descartados por el jardín amurallado (tráfico no en la lista blanca, no DNS)

Métrica: `upf_walled_garden_packets_forwarded_total` **Tipo**: Contador **Etiquetas**:

- `dst_ip` - IP de destino del paquete reenviado **Descripción**: Paquetes reenviados a través del jardín amurallado a destinos en la lista blanca. Etiquetado por IP de destino para visibilidad por destino.

Métrica: `upf_walled_garden_bytes_forwarded_total` **Tipo**: Contador **Etiquetas**:

- `dst_ip` - IP de destino del tráfico reenviado **Descripción**: Bytes reenviados a través del jardín amurallado por IP de destino. Utiliza esto para identificar qué servicios en la lista blanca acceden los suscriptores mientras están redirigidos.

Métrica: `upf_walled_garden_dns_spoofed_total` **Tipo**: Contador **Etiquetas**:

- `domain` - El dominio que fue suplantado **Descripción**: Consultas DNS suplantadas por el jardín amurallado. Etiquetado por dominio consultado.

Métrica: `upf_walled_garden_dns_forwarded_total` **Tipo**: Contador **Etiquetas**:

- `domain` - El dominio en la lista blanca que fue reenviado **Descripción**: Consultas DNS reenviadas al resolutor real (dominios en la lista blanca). Etiquetado por dominio.

Consultas de Ejemplo

```
# Sesiones activas del jardín amurallado
upf_walled_garden_active_redirects

# Tasa de interceptación (paquetes/segundo)
rate(upf_walled_garden_packets_intercepted_total[5m])

# Tasa de descartes (debería ser la mayoría de los interceptados)
rate(upf_walled_garden_packets_dropped_total[5m])

# Tráfico reenviado por destino (bytes/segundo)
sum by (dst_ip)
(rate(upf_walled_garden_bytes_forwarded_total[5m]))

# Top 5 destinos en la lista blanca por volumen de tráfico
topk(5, sum by (dst_ip)
(rate(upf_walled_garden_bytes_forwarded_total[5m])))

# Dominios suplantados más consultados
topk(10, sum by (domain)
(rate(upf_walled_garden_dns_spoofed_total[5m])))

# Tasa de búsqueda de dominios en la lista blanca
sum by (domain) (rate(upf_walled_garden_dns_forwarded_total[5m]))

# Relación de descartes vs reenviados
sum(rate(upf_walled_garden_packets_dropped_total[5m]))
  / sum(rate(upf_walled_garden_packets_intercepted_total[5m]))
```

Solución de Problemas

Portal Captivo No Aparece en el Dispositivo

Síntomas: El suscriptor está redirigido (visible en la API) pero el dispositivo no muestra el aviso del portal cautivo.

Causas posibles:

- El servidor del portal no responde en la IP del portal configurada
- El servidor del portal no maneja las URLs de detección específicas de la plataforma
- La respuesta DNS no llega al UE (verificar la ruta GTP-U)

Resolución:

1. Verificar que el servidor del portal sea accesible: `curl http://<portal_ip>/`
2. Confirmar que el portal maneje las URLs de detección (por ejemplo, `GET /hotspot-detect.html` para Apple)
3. Verificar `GET /v1/walled_garden` para confirmar que la sesión esté registrada
4. Verificar métricas de Prometheus: `upf_walled_garden_dns_spoofed_total` debería estar incrementando
5. Verificar que la ruta GTP-U de enlace descendente esté funcionando (DL FAR debería permanecer FORW)

Página de Pago No Carga

Síntomas: El suscriptor ve el portal cautivo pero no puede acceder a la página de pago (Stripe, etc.).

Causas posibles:

- Dominio del procesador de pagos no en la lista blanca
- Procesador de pagos utilizando una IP de CDN que no fue almacenada en caché
- Patrón de lista blanca no coincidiendo correctamente con subdominios

Resolución:

1. Verificar `GET /v1/walled_garden` - confirmar que `whitelisted_ips` incluye las IPs del procesador de pagos
2. Verificar Prometheus: `upf_walled_garden_dns_forwarded_total{domain="stripe.com"}` debería mostrar búsquedas

3. Agregar dominios faltantes a la lista blanca (común: `js.stripe.com`, `m.stripe.network`)
4. Verificar `upf_walled_garden_bytes_forwarded_total` por `dst_ip` para ver qué tráfico está fluyendo realmente

Redirección No Se Activa

Síntomas: El SMF envía la Modificación de Sesión con `redirect_information` pero el tráfico del suscriptor no es interceptado.

Causas posibles:

- `walled_garden_enabled` es `false`
- El IE `redirect_information` está en el FAR incorrecto (debe estar en el FAR **de enlace ascendente**)
- La acción del FAR no se está sobrescribiendo a BUFF

Resolución:

1. Verificar configuración: `walled_garden_enabled = true`
2. Verificar `GET /v1/pfcp_sessions` - observar la acción del FAR para la sesión. El FAR de enlace ascendente debería mostrar acción `0x04` (BUFF)
3. Verificar `GET /v1/walled_garden` - el TEID de la sesión debería aparecer en la lista de redirección
4. Verificar los registros del UPF para mensajes de `redirect_info` durante la modificación de sesión

Redirección No Se Limpia Después de la Recarga

Síntomas: El suscriptor ha recargado pero el tráfico sigue siendo interceptado.

Causas posibles:

- El SMF no ha enviado la Modificación de Sesión para eliminar la redirección
- La transición de BUFF->FORW no se está detectando

Resolución:

1. Verificar `GET /v1/walled_garden` - ¿la sesión sigue listada?
2. Verificar `GET /v1/pfcp_sessions` - confirmar que la acción del FAR se ha actualizado de nuevo a `0x02` (FORW)
3. Verificar registros del SMF para confirmar que envió la Modificación de Sesión
4. Verificar los registros del UPF para el mensaje "redirect removed, unregistering walled garden"

TEID de Enlace Descendente Incorrecto (Obsoleto Después de la Modificación de Sesión)

Síntomas: Respuestas DNS suplantadas o tráfico reenviado no llegan al UE; los paquetes GTP-U se envían a la IP correcta del gNB pero el eNB los descarta como TEID desconocido.

Causa: En topologías 4G/SGW+PGW, el TEID del eNB en el FAR DL de SGW puede ser cero o un TEID de marcador de posición en el momento en que se activa la redirección del jardín amurallado (por ejemplo, el intercambio de `Initial Context Setup` ocurre después del Establecimiento de Sesión). Cuando el eNB asigna su TEID y lo envía de vuelta a través de la Modificación de Sesión, el FAR DL en la sesión SGW se actualiza - pero si el Dispatcher había almacenado en caché el valor antiguo, usaría el TEID incorrecto.

Resolución: El Dispatcher resuelve el TEID DL **en vivo** en el momento de la respuesta buscando el FAR DL actual de la sesión SGW (el FAR con `outer_header_creation` configurado y `remoteip != n3_address`). Solo recurre al valor almacenado en el momento de la activación si la búsqueda de la sesión falla. Por lo tanto, un TEID obsoleto debería corregirse por sí mismo tan pronto como se envíe la siguiente respuesta DNS o reenviada. Si aún ves el TEID incorrecto:

1. Verificar `GET /v1/walled_garden` - verificar que `dl_teid` en la entrada de redirección parezca plausible (no cero).
2. Verificar `GET /v1/pfcp_sessions` - observar las entradas FAR de la sesión SGW; el FAR que mira hacia el gNB debería tener el `teid` y `remoteip` actuales.

3. Si la sesión SGW ha sido eliminada (por ejemplo, por traspaso o liberación), la entrada de redirección permanecerá en el RedirectIndex pero la búsqueda en vivo fallará. En este caso, usar `DELETE /v1/walled_garden/:seid` para limpiar la entrada obsoleta y permitir que el SMF restablezca.

El Portal Devuelve 304 No Modificado

Síntomas: El navegador del suscriptor muestra una página en blanco o la página del portal cautivo se carga una vez pero las visitas subsiguientes aparecen vacías.

Causa: Las respuestas HTTP 304 (No Modificado) se envían cuando el navegador tiene una versión en caché de la página y el servidor confirma que nada ha cambiado. Para los flujos de portal cautivo, algunos servidores web de portal envían 304 en respuesta a las solicitudes de detección de la plataforma (`/hotspot-detect.html`, `/generate_204`, etc.) si el navegador envía encabezados `If-Modified-Since` o `If-None-Match`. Algunas implementaciones de portal cautivo también envían 304 para la propia página de redirección.

Resolución:

1. El UPF reenvía las respuestas HTTP del servidor del portal de manera transparente - no modifica los códigos de respuesta. El problema está en la configuración del servidor web del portal.
2. En el servidor del portal, asegúrate de que los puntos finales de detección de la plataforma devuelvan el código de estado correcto (200, no 304) con el contenido del cuerpo esperado (ver Detección de Portal Captivo).
3. Configura el servidor del portal para enviar `Cache-Control: no-store` y omitir los encabezados `ETag`/`Last-Modified` en los puntos finales de detección para que los navegadores no los almacenen en caché.
4. Verificar con: `curl -v -H "If-None-Match: foo" http://<portal_ip>/hotspot-detect.html` - la respuesta debería ser 200, no 304.

El Portal Muestra la Página Incorrecta (Host Virtual Basado en Nombre)

Síntomas: El suscriptor es redirigido (visible en `GET /v1/walled_garden`) y aparece el aviso del portal cautivo, pero al tocarlo se abre el **sitio incorrecto** -- una aplicación diferente, un CRM o una página por defecto genérica -- en lugar de la página de recarga/registro. `curl` confirma que la página del portal solo se carga con un encabezado `Host:` específico:

```
curl -s -H 'Host: portal.example'
http://<portal_ip>/   # -> página cautiva/registro   (correcto)
curl -s -H 'Host: connectivitycheck.gstatic.com'
http://<portal_ip>/   # -> vhost POR DEFECTO (incorrecto)
curl -s -H 'Host: <portal_ip>'
http://<portal_ip>/   # -> vhost POR DEFECTO (incorrecto)
```

Causa: La IP del portal es un **host virtual basado en nombre** compartido con otros sitios. El jardín amurallado suplantan cada sonda de portal cautivo a la IP del portal y reenvía la solicitud HTTP del UE **verbatim, manteniendo el encabezado `Host` original de la sonda** (por ejemplo, `Host: connectivitycheck.gstatic.com`). El servidor web del portal no tiene un vhost que coincida con ese `Host`, por lo que sirve su **vhost por defecto** -- la página incorrecta. El UPF no reescribe el encabezado `Host` ni realiza selección de vhost en nombre del portal. Ver Requisitos del Servidor del Portal.

Resolución:

1. Dar al portal cautivo su **propia IP dedicada** para que cualquier `Host:` servido por esa IP devuelva la página del portal, **o**
2. Hacer del portal el **host virtual por defecto** en el host compartido, de modo que los valores `Host:` no coincidentes caigan en la página del portal.
3. Verificar con los comandos `curl` anteriores: con una IP dedicada o un vhost por defecto, **los tres** deberían devolver la página del portal.

Reenvío de Socket Crudo

Cuando el Dispatcher reenvía un paquete a una IP en la lista blanca, utiliza un **socket crudo** (`IPPROTO_RAW`, número de protocolo 255) a través del módulo `:socket` de Erlang. Se abre un nuevo socket crudo por paquete, se envía el paquete IP interno completo (como se recibió de eBPF) con `sendto`, y el socket se cierra inmediatamente.

Cómo funciona esto: El paquete IP interno del payload GTP-U ya tiene un encabezado IP válido con la IP del UE como origen y la IP del servidor de destino como destino. Al inyectar este paquete a través de un socket crudo utilizando `IPPROTO_RAW`, el kernel lo enruta según la IP de destino utilizando la tabla de enrutamiento del host. La interfaz N6 del UPF debe tener una ruta hacia el servidor del portal/en la lista blanca para que esto funcione.

Problemas comunes:

Síntoma	Causa Probable	Solución
El reenvío falla silenciosamente	`EPERM` - el socket crudo requiere root o `CAP_NET_RAW`	Asegúrate de que OmniUPF se ejecute como root o tenga la capacidad `CAP_NET_RAW`
Los paquetes se reenvían pero ninguna respuesta llega al UE	Falta ruta N6 hacia el portal	Agregar ruta a la subred del portal en el host UPF
`Walled garden: raw socket open failed` en los registros	Falta capacidad o restricción del kernel	Verificar el servicio `systemd` `AmbientCapabilities=CAP_NET_RAW`
El reenvío funciona pero el UE recibe la IP incorrecta como origen	NAT en N6 reescribe el origen	Asegúrate de que las respuestas del portal a la IP del UE sean enrutadas de vuelta a través del UPF

Verifica los registros del UPF para mensajes de `Walled garden forward failed` y `raw socket open failed`. Utiliza las métricas de Prometheus `upf_walled_garden_packets_forwarded_total` y `upf_walled_garden_bytes_forwarded_total` para confirmar que el tráfico esté fluyendo.

Advertencia de Alta Cardinalidad para Prometheus

Nota: Las etiquetas `dst_ip` y `domain` en las métricas del jardín amurallado pueden producir alta cardinalidad si se consultan muchos destinos o dominios únicos. En implementaciones grandes, considera usar reglas de grabación para agregar estas métricas:

```
# Regla de grabación para agregar por subred /24 en lugar de IPs
individuales
sum by (dst_subnet) (
  label_replace(
    rate(upf_walled_garden_bytes_forwarded_total[5m]),
    "dst_subnet", "$1.0/24", "dst_ip", "(\d+\.\d+\.\d+)\.\d+"
  )
)
```

Guía de Operaciones de la Interfaz Web

Tabla de Contenidos

1. Descripción General
2. Acceso al Panel de Control
3. Vista de Sesiones
4. Gestión de Reglas
5. Gestión de Buffers
6. Panel de Estadísticas
7. Monitoreo de Capacidad
8. Vista de Configuración
9. Vista de Rutas
10. Vista de Capacidades XDP
11. Visor de Registros

Descripción General

La Interfaz Web de OmniUPF proporciona un panel de control integral para el monitoreo y gestión en tiempo real de la Función de Plano de Usuario. La interfaz está construida sobre Phoenix LiveView y proporciona:

- **Visibilidad en tiempo real** de sesiones PFCP y conexiones PDU activas
- **Inspección de reglas** para PDR, FAR, QER y URR en todas las sesiones
- **Gestión de buffers** para el almacenamiento de paquetes durante eventos de movilidad
- **Monitoreo de estadísticas** para el procesamiento de paquetes, rutas e interfaces
- **Seguimiento de capacidad** para el uso y límites del mapa eBPF
- **Visualización de registros en vivo** para la solución de problemas

Arquitectura

El panel de control se comunica con múltiples instancias de OmniUPF a través de su API REST para:

- Consultar sesiones y asociaciones PFCP
- Inspeccionar reglas de detección y reenvío de paquetes
- Monitorear buffers de paquetes y su estado
- Acceder a estadísticas y métricas de rendimiento en tiempo real
- Rastrear la capacidad y utilización del mapa eBPF

Acceso al Panel de Control

Acceso por Defecto

El panel de control es accesible a través de HTTPS en el servidor de gestión de OmniUPF:

```
https://<upf-server>:443/
```

Puerto por Defecto: 443 (HTTPS con certificado autofirmado)

Configuración

El panel de control requiere la configuración del host de OmniUPF en `config/config.exs`:

Se pueden configurar múltiples instancias de UPF para implementaciones de múltiples instancias:

La configuración `upf_hosts` define qué instancias de OmniUPF están disponibles en el menú desplegable del selector de host en toda la interfaz.

Navegación

El panel de control proporciona pestañas de navegación para cada área operativa:

- **Sesiones** - `/sessions` - Sesiones y asociaciones PFCP
- **Reglas** - `/rules` - Inspección de reglas PDR, FAR, QER, URR
- **Buffers** - `/buffers` - Monitoreo y control de buffers de paquetes
- **Estadísticas** - `/statistics` - Estadísticas de paquetes, rutas, XDP e interfaces
- **Capacidad** - `/capacity` - Uso y monitoreo de capacidad del mapa eBPF
- **Config** - `/upf_config` - Configuración de UPF y direcciones del plano de datos
- **Rutas** - `/routes` - Rutas de UE y sesiones de protocolo de enrutamiento (OSPF, BGP)
- **Capacidades XDP** - `/xdp_capabilities` - Soporte de modo XDP y capacidades de rendimiento
- **Registros** - `/logs` - Transmisión de registros en vivo

Vista de Sesiones

URL: `/sessions`

Características

La vista de Sesiones muestra todas las sesiones PFCP activas y asociaciones de las instancias de OmniUPF seleccionadas.

Resumen de Asociaciones PFCP

Muestra todas las asociaciones PFCP activas (conexiones de control desde SMF/PGW-C):

Columna	Descripción
ID de Nodo	Identificador de nodo SMF o PGW-C (FQDN o IP)
Dirección	Dirección IP de SMF/PGW-C para comunicación PFCP
Siguiente ID de Sesión	Siguiente ID de sesión PFCP disponible para esta asociación

Propósito:

- Verificar la conectividad de SMF a UPF
- Monitorear el número de conexiones de plano de control
- Rastrear la asignación de ID de sesión por asociación

Tabla de Sesiones Activas

Muestra todas las sesiones PFCP que representan sesiones PDU activas de UE:

Columna	Descripción
SEID Local	Identificador de punto final de sesión asignado por UPF
SEID Remoto	Identificador de punto final de sesión asignado por SMF
IP de UE	Dirección IP IPv4 o IPv6 del equipo de usuario
TEID	Identificador de punto final de túnel GTP-U para tráfico ascendente
PDRs	Número de reglas de detección de paquetes en la sesión
FARs	Número de reglas de acción de reenvío en la sesión
QERs	Número de reglas de aplicación de QoS en la sesión
URRs	Número de reglas de informes de uso en la sesión
Acciones	Botón de expandir para ver información detallada de la regla

Características:

- **Filtrar por IP**: Encontrar sesiones para una dirección IP específica de UE
- **Filtrar por TEID**: Encontrar sesiones por ID de punto final de túnel
- **Expandir sesión**: Ver detalles completos de PDR/FAR/QER/URR en JSON
- **Actualización automática**: Se actualiza cada 10 segundos

Vista de Sesión Expandida:

Cuando haces clic en "Expandir" en una sesión, la vista muestra:

- **Reglas de Detección de Paquetes (PDRs)**: JSON completo con TEID, IP de UE, ID de FAR, ID de QER, filtros SDF

    - **Los IDs de PDR son clicables** - Haz clic para navegar a la pestaña Reglas y ver los detalles completos de PDR
    - PDRs ascendentes (TEID ≠ 0) enlazan a la búsqueda de PDR ascendente
    - PDRs descendentes (IPv4) enlazan a la búsqueda de PDR descendente
    - PDRs descendentes (IPv6) enlazan a la búsqueda de PDR descendente IPv6
- **Reglas de Acción de Reenvío (FARs)**: Banderas de acción, creación de encabezado externo, puntos finales de destino
- **Reglas de Aplicación de QoS (QERs)**: MBR, GBR, QFI y otros parámetros de QoS
- **Reglas de Informes de Uso (URRs)**: Contadores de volumen (ascendente, descendente, bytes totales)

Vista expandida de sesión mostrando PDRs, FARs y QERs detallados para una sesión específica.

Casos de Uso

Verificar Conectividad de UE:

1. Navegar a la vista de Sesiones
2. Ingresar la dirección IP de UE en el filtro
3. Confirmar que la sesión existe con el TEID correcto
4. Expandir para verificar la configuración de PDR/FAR

Monitorear Conteo de Sesiones:

- Verificar el conteo total de sesiones en el encabezado
- Comparar entre múltiples instancias de UPF
- Rastrear el crecimiento de sesiones a lo largo del tiempo

Solucionar Problemas de Sesiones:

- Buscar una IP de UE o TEID específico
- Expandir la sesión para inspeccionar la configuración de reglas
- Verificar los parámetros de reenvío de FAR
- Comprobar la configuración de QoS de QER

Actualizaciones en Tiempo Real

La vista de Sesiones se actualiza automáticamente cada 10 segundos. Un indicador de verificación de salud muestra el estado de conectividad de UPF:

- **SALUDABLE** (verde): UPF es alcanzable y está respondiendo
- **NO SALUDABLE** (rojo): UPF no es alcanzable o no está respondiendo
- **DESCONOCIDO** (gris): Estado de salud aún no determinado

Gestión de Reglas

URL: `/rules`

La vista de Reglas proporciona una inspección integral de todas las reglas de detección de paquetes, reenvío, QoS e informes de uso en todas las sesiones.

Pestaña PDR - Reglas de Detección de Paquetes

Ver e inspeccionar todos los PDR en el UPF con **formularios de búsqueda** y **navegación clicable**:

PDRs Ascendentes (N3 → N6):

- **Formulario de Búsqueda**: Buscar por TEID para ver detalles específicos de PDR ascendente
- **TEID**: ID de punto final de túnel GTP-U desde gNB (clicable - navega a búsqueda)
- **ID de FAR**: Regla de acción de reenvío asociada (clicable - navega a la pestaña FAR)
- **ID de QER**: Regla de aplicación de QoS asociada (clicable - navega a la pestaña QER)
- **IDs de URR**: Reglas de informes de uso asociadas (clicable - navega a la pestaña URR)
- **Eliminación de Encabezado Externo**: Bandera de desencapsulación GTP-U
- **Filtros SDF**: Reglas de clasificación de flujo de datos de servicio

PDRs Descendentes (N6 → N3):

- **Formulario de Búsqueda**: Buscar por dirección IPv4 de UE para ver detalles específicos de PDR descendente
- **IP de UE**: Dirección IPv4 del equipo de usuario (mostrada en resultados de búsqueda)
- **ID de FAR**: Regla de acción de reenvío asociada (clicable - navega a la pestaña FAR)
- **ID de QER**: Regla de aplicación de QoS asociada (clicable - navega a la pestaña QER)
- **IDs de URR**: Reglas de informes de uso asociadas (clicable - navega a la pestaña URR)
- **Modo SDF**: Modo de filtro de flujo de datos de servicio (ninguno, solo sdf, sdf + predeterminado)

- **Paginación**: Navegar por PDRs con controles de página (predeterminado 100 por página, máximo 1000)

PDRs Descendentes IPv6:

- La API admite paginación para PDRs descendentes IPv6
- La misma estructura que IPv4 pero indexada por direcciones IPv6
- Se puede agregar una pestaña completa de UI si es necesario

Pestaña FAR - Reglas de Acción de Reenvío

Ver todas las FARs con sus acciones de reenvío y parámetros:

Características:

- **Formulario de Búsqueda**: Buscar por ID de FAR para ver detalles específicos de FAR
- **Búsqueda Automática**: Hacer clic en IDs de FAR desde detalles de PDR automáticamente llena la búsqueda
- **Actualizaciones en Tiempo Real**: El estado de FAR refleja el estado actual de almacenamiento en buffer

Columna	Descripción
ID de FAR	Identificador único de regla de reenvío
Acción	Banderas de acción de reenvío (REENVIAR, DESCARTAR, BUFFER, DUPLICAR, NOTIFICAR)
Almacenamiento en Buffer	Estado actual de almacenamiento en buffer (Habilitado/Deshabilitado)
Destino	Parámetros de creación de encabezado externo (TEID, dirección IP)

Banderas de Acción de FAR:

- **REENVIAR (1)**: Reenviar paquete al destino

- **DESCARTAR (2)**: Descartar paquete
- **BUFFER (4)**: Almacenar paquete en buffer
- **NOTIFICAR (8)**: Enviar notificación al plano de control
- **DUPLICAR (16)**: Duplicar paquete a múltiples destinos

Alternar Almacenamiento en Buffer:

- Hacer clic en "Habilitar Buffer" o "Deshabilitar Buffer" para alternar la bandera de almacenamiento en buffer
- Útil para solucionar problemas en escenarios de traspaso
- Cambia la acción de FAR inmediatamente en el mapa eBPF

Pestaña QER - Reglas de Aplicación de QoS

Ver reglas de QoS aplicadas a flujos de tráfico:

Características:

- **Navegación Clicable**: Hacer clic en IDs de QER desde detalles de PDR para navegar y resaltar QER específico
- **Auto-resaltado**: La fila de QER se resalta cuando se navega desde PDR
- **Paginación**: Navegar por QERs con controles de página (predeterminado 100 por página, máximo 1000)

Columna	Descripción
ID de QER	Identificador único de regla de QoS (clicable cuando se referencia desde PDRs)
MBR (Ascendente)	Tasa máxima de bits para tráfico ascendente (kbps)
MBR (Descendente)	Tasa máxima de bits para tráfico descendente (kbps)
GBR (Ascendente)	Tasa garantizada de bits para tráfico ascendente (kbps)
GBR (Descendente)	Tasa garantizada de bits para tráfico descendente (kbps)
QFI	Identificador de Flujo QoS (marcado 5G)

Interpretación de QoS:

- **MBR = 0**: Sin límite de tasa
- **GBR = 0**: Mejor esfuerzo (sin ancho de banda garantizado)
- **GBR > 0**: Flujo de tasa garantizada (priorizado)

Pestaña URR - Reglas de Informes de Uso

Ver reglas de seguimiento de uso y contadores de volumen:

Características:

- **Formulario de Búsqueda**: Buscar por ID de URR para encontrar y resaltar URR específico
- **Navegación Clicable**: Hacer clic en IDs de URR desde detalles de PDR para navegar y resaltar URR específico
- **Auto-resaltado**: La fila de URR se resalta en azul cuando se navega desde PDR o se busca a través de búsqueda

- **Paginación**: Navegar por URRs con controles de página (predeterminado 100 por página, máximo 1000)

Columna	Descripción
ID de URR	Identificador único de regla de informes de uso (clicable cuando se referencia desde PDRs)
Volumen Ascendente	Bytes enviados desde UE a la red de datos
Volumen Descendente	Bytes enviados desde la red de datos a UE
Volumen Total	Total de bytes en ambas direcciones
Acciones	Botón de eliminar para restablecer contadores para este URR

Visualización de Volumen:

- Formateado automáticamente (B, KB, MB, GB, TB)
- Contadores en tiempo real actualizados en cada actualización
- Usado para facturación y análisis

Filtrado:

- Solo muestra URRs con volumen distinto de cero
- URRs inactivas (todos los contadores en 0) se filtran para mejorar el rendimiento

Casos de Uso

Inspeccionar Clasificación de Tráfico:

1. Navegar a Reglas → pestaña PDR
2. Buscar por TEID o IP de UE específica

3. Verificar que PDR se asocie con el FAR y QER correctos

Solucionar Problemas de Reenvío:

1. Navegar a Reglas → pestaña FAR
2. Localizar ID de FAR desde PDR de sesión
3. Verificar que la acción sea REENVIAR (no DESCARTAR o BUFFER)
4. Comprobar los parámetros de creación de encabezado externo

Monitorear Aplicación de QoS:

1. Navegar a Reglas → pestaña QER
2. Verificar que los valores de MBR y GBR coincidan con la política
3. Comprobar el marcado QFI para flujos 5G

Rastrear Uso de Datos:

1. Navegar a Reglas → pestaña URR
2. Ordenar por volumen total para encontrar los usuarios más altos
3. Monitorear el crecimiento del volumen a lo largo del tiempo
4. Verificar la integración de facturación

Gestión de Buffers

URL: `/buffers`

Características

La vista de Buffers muestra los buffers de paquetes mantenidos por el UPF durante eventos de movilidad o cambios de ruta.

Estadísticas Totales

El panel muestra estadísticas agregadas de buffers:

- **Total de Paquetes**: Número de paquetes almacenados en todos los FARs
- **Total de Bytes**: Tamaño total de datos almacenados

- **Total de FARs**: Número de FARs con paquetes almacenados
- **Máx. Por FAR**: Máximo de paquetes permitidos por FAR
- **Máx. Total**: Máximo total de paquetes almacenados
- **TTL de Paquete**: Tiempo de vida para paquetes almacenados (segundos)

Buffers por FAR

Tabla de todos los FARs con paquetes almacenados:

Columna	Descripción
ID de FAR	Identificador de regla de acción de reenvío
Conteo de Paquetes	Número de paquetes almacenados para este FAR
Conteo de Bytes	Total de bytes almacenados para este FAR
Paquete Más Antiguo	Marca de tiempo del paquete almacenado más antiguo
Paquete Más Nuevo	Marca de tiempo del paquete almacenado más nuevo
Acciones	Botones de control de buffer (estilo píldora)

Acciones de Control de Buffer

Para cada FAR con paquetes almacenados, están disponibles los siguientes botones de estilo píldora:

Control de Almacenamiento en Buffer:

- **Deshabilitar Buffer** (rojo): Apagar el almacenamiento en buffer para este FAR (actualiza la bandera de acción de FAR)
- **Habilitar Buffer** (púrpura): Activar el almacenamiento en buffer para este FAR

Operaciones de Buffer:

- **Vaciar** (azul): Reproducir todos los paquetes almacenados utilizando las reglas actuales de FAR
- **Limpiar** (gris): Eliminar todos los paquetes almacenados sin reenviar

Limpiar Todos los Buffers:

- Botón rojo "Limpiar Todo" en el encabezado
- Limpia los buffers para todos los FARs
- Requiere confirmación

Casos de Uso

Monitorear Almacenamiento en Buffer durante el Traspaso:

1. Durante el traspaso, verificar que los paquetes se estén almacenando
2. Comprobar el estado de almacenamiento en buffer de FAR (debería estar habilitado)
3. Monitorear el conteo y la antigüedad de paquetes

Completar el Traspaso:

1. Después del cambio de ruta, hacer clic en "Vaciar" para reproducir los paquetes almacenados
2. Verificar que los paquetes se reenvíen a la nueva ruta
3. Hacer clic en "Deshabilitar Buffer" para detener el almacenamiento en buffer

Limpiar Buffers Atascados:

1. Identificar FARs con paquetes almacenados antiguos (comprobar la marca de tiempo más antigua)
2. Hacer clic en "Limpiar" para descartar paquetes obsoletos
3. O hacer clic en "Deshabilitar Buffer" para evitar más almacenamiento en buffer

Solucionar Problemas de Desbordamiento de Buffer:

1. Comprobar el conteo total de paquetes vs. máximo total

2. Identificar FARs con almacenamiento en buffer excesivo
3. Verificar que SMF haya enviado modificación de sesión para deshabilitar el almacenamiento en buffer
4. Deshabilitar manualmente el almacenamiento en buffer si se perdió el comando de SMF

Actualizaciones en Tiempo Real

La vista de Buffers se actualiza automáticamente cada 5 segundos para mostrar el estado actual del buffer.

Panel de Estadísticas

URL: `/statistics`

Características

La vista de Estadísticas proporciona métricas de rendimiento en tiempo real del plano de datos de OmniUPF. Para información detallada sobre métricas de Prometheus, consulte la **Referencia de Métricas**.

Estadísticas de Paquetes

Contadores agregados de procesamiento de paquetes:

- **Paquetes RX**: Total de paquetes recibidos en todas las interfaces
- **Paquetes TX**: Total de paquetes transmitidos en todas las interfaces
- **Paquetes Descartados**: Paquetes descartados debido a errores o políticas
- **Paquetes GTP-U**: Paquetes procesados con encapsulación GTP-U

Uso: Monitorear la carga de tráfico general de UPF y la tasa de paquetes descartados

Estadísticas de Rutas

Métricas de reenvío por ruta (si están disponibles):

- **Acercamientos de Ruta**: Paquetes coincidentes con cada regla de enrutamiento
- **Éxito de Reenvío**: Conteo de paquetes reenviados con éxito
- **Errores de Reenvío**: Intentos de reenvío fallidos

Uso: Identificar rutas ocupadas y errores de reenvío

Estadísticas XDP

Métricas de rendimiento de eXpress Data Path:

- **XDP Procesados**: Total de paquetes procesados en la capa XDP
- **XDP Pasados**: Paquetes enviados a la pila de red
- **XDP Descartados**: Paquetes descartados en la capa XDP
- **XDP Abortados**: Errores de procesamiento en el programa XDP

Uso: Monitorear el rendimiento de XDP y detectar errores de procesamiento

Causas de Descartes de XDP:

- Formato de paquete inválido
- Fallo en la búsqueda de mapa eBPF
- Descartes basados en políticas
- Agotamiento de recursos

Estadísticas de Interfaces N3/N6

Contadores de tráfico por interfaz:

Interfaz N3 (conectividad RAN):

- **RX N3**: Paquetes recibidos desde gNB/eNodeB
- **TX N3**: Paquetes transmitidos a gNB/eNodeB

Interfaz N6 (conectividad de red de datos):

- **RX N6**: Paquetes recibidos desde la red de datos (Internet/IMS)
- **TX N6**: Paquetes transmitidos a la red de datos

Total: Conteo agregado de paquetes a través de las interfaces

Uso: Monitorear el equilibrio de tráfico y problemas específicos de la interfaz

Casos de Uso

Monitorear Carga de Tráfico:

1. Comprobar tasas de paquetes RX/TX
2. Verificar que el tráfico fluya en ambas direcciones
3. Comparar tráfico N3 vs N6 (debería ser aproximadamente igual)

Detectar Paquetes Descartados:

1. Comprobar contador de paquetes descartados
2. Revisar contador de paquetes descartados de XDP
3. Investigar la causa en los registros si los descartes son altos

Análisis de Rendimiento:

1. Monitorear la relación entre XDP procesados y pasados
2. Comprobar abortos de XDP (indica errores)
3. Verificar la distribución del tráfico de interfaces N3/N6

Planificación de Capacidad:

1. Rastrear la tasa de paquetes a lo largo del tiempo
2. Comparar con los límites de capacidad de UPF
3. Planificar escalado si se acercan a los límites

Actualizaciones en Tiempo Real

Las estadísticas se actualizan automáticamente cada 5 segundos.

Monitoreo de Capacidad

URL: `/capacity`

Características

La vista de Capacidad muestra el uso del mapa eBPF y los límites de capacidad para todos los mapas en el plano de datos de UPF.

Tabla de Uso del Mapa eBPF

Tabla de todos los mapas eBPF con información de uso:

Columna	Descripción
Nombre del Mapa	Nombre del mapa eBPF (por ejemplo, `uplink_pdr_map`, `far_map`)
Usado	Número de entradas actualmente en el mapa
Capacidad	Máximo de entradas permitidas en el mapa
Uso	Barra de progreso visual con porcentaje
Tamaño de Clave	Tamaño de las claves del mapa en bytes
Tamaño de Valor	Tamaño de los valores del mapa en bytes

Indicadores de Uso Codificados por Color

La barra de progreso de uso está codificada por color según la utilización:

- **Verde (<50%)**: Operación normal, capacidad amplia
- **Amarillo (50-70%)**: Precaución, monitorear crecimiento
- **Ámbar (70-90%)**: Advertencia, planificar aumento de capacidad
- **Rojo (>90%)**: Crítico, se requiere acción inmediata

Mapas Críticos a Monitorear

uplink_pdr_map:

- Almacena PDRs ascendentes indexados por TEID
- Una entrada por flujo de tráfico ascendente
- **Crítico**: El agotamiento impide el establecimiento de nuevas sesiones

downlink_pdr_map / **downlink_pdr_map_ip6**:

- Almacena PDRs descendentes indexados por dirección IP de UE
- Una entrada por dirección IPv4/IPv6 de UE
- **Crítico**: El agotamiento impide el establecimiento de nuevas sesiones

far_map:

- Almacena reglas de acción de reenvío indexadas por ID de FAR
- Compartido entre múltiples PDRs
- **Alta Prioridad**: Afecta decisiones de reenvío

qer_map:

- Almacena reglas de aplicación de QoS indexadas por ID de QER
- **Prioridad Media**: Afecta QoS pero no conectividad básica

urr_map:

- Almacena reglas de informes de uso indexadas por ID de URR
- **Baja Prioridad**: Afecta facturación pero no conectividad

Casos de Uso

Planificación de Capacidad:

1. Monitorear tendencias de uso de mapas a lo largo del tiempo
2. Identificar qué mapas están creciendo más rápido
3. Planificar aumentos de capacidad antes de alcanzar límites

Prevenir Fallos en el Establecimiento de Sesiones:

1. Comprobar el uso del mapa PDR antes de un aumento de tráfico esperado
2. Aumentar la capacidad del mapa si se acercan a los límites
3. Monitorear después del aumento de capacidad para verificar

Solucionar Fallos de Sesión:

1. Cuando falla el establecimiento de sesión, comprobar la vista de Capacidad
2. Si los mapas PDR están en rojo (>90%), la capacidad está agotada
3. Aumentar la capacidad del mapa o limpiar sesiones obsoletas

Optimizar la Configuración del Mapa:

1. Revisar tamaños de clave y valor
2. Calcular uso de memoria por mapa
3. Optimizar tamaños de mapa según patrones de uso reales

Configuración de Capacidad

Las capacidades de los mapas eBPF se configuran al inicio de UPF en el archivo de configuración de UPF. Valores típicos:

- Implementación pequeña: 10,000 - 100,000 entradas por mapa
- Implementación mediana: 100,000 - 1,000,000 entradas por mapa
- Implementación grande: 1,000,000+ entradas por mapa

Cálculo de Memoria:

```
Memoria del Mapa = (Tamaño de Clave + Tamaño de Valor) × Capacidad
```

Por ejemplo, un mapa PDR con 1 millón de entradas y valores de 64 bytes utiliza aproximadamente 64 MB de memoria del kernel.

Actualizaciones en Tiempo Real

La vista de capacidad se actualiza automáticamente cada 10 segundos.

Vista de Configuración

URL: `/upf_config`

Características

La vista de Configuración muestra parámetros operativos de UPF y configuración del plano de datos.

Configuración de UPF

Muestra la configuración estática de UPF:

- **Interfaz PFCP**: Dirección IP y puerto para conectividad SMF/PGW-C
- **Interfaz N3**: Dirección IP para conectividad RAN (gNB/eNodeB)
- **Interfaz N6**: Dirección IP para conectividad de red de datos
- **Interfaz N9**: Dirección IP para comunicación entre UPFs (opcional)
- **Puerto API**: Puerto de escucha de la API REST
- **Versión**: Versión del software OmniUPF

Configuración del Plano de Datos (eBPF)

Muestra parámetros de plano de datos en tiempo de ejecución activos:

- **Dirección N3 Activa**: Vinculación de interfaz N3 en tiempo de ejecución
- **Dirección N9 Activa**: Vinculación de interfaz N9 en tiempo de ejecución (si está habilitada)

Estos valores reflejan la configuración real del plano de datos eBPF y pueden diferir de la configuración estática si se han cambiado las interfaces.

Casos de Uso

Verificar Conectividad de UPF:

1. Comprobar que la IP de la interfaz N3 coincida con la configuración de gNB
2. Verificar que la interfaz N6 pueda enrutar a la red de datos
3. Confirmar que la interfaz PFCP sea alcanzable desde SMF

Solucionar Problemas de Problemas de Interfaz:

1. Comparar la configuración estática con las direcciones activas del plano de datos
2. Verificar que las interfaces estén vinculadas correctamente
3. Comprobar si ha habido cambios en la configuración de la interfaz

Documentación y Auditoría:

1. Registrar la configuración de UPF para documentación
2. Verificar que la implementación coincida con las especificaciones de diseño
3. Auditar las asignaciones de interfaz

Vista de Rutas

URL: `/routes`

Características

La vista de Rutas proporciona un monitoreo integral de las rutas IP de Equipos de Usuario (UE) y sesiones de protocolo de enrutamiento (OSPF y BGP).

Resumen del Estado de Rutas

El panel muestra estadísticas agregadas de rutas:

- **Estado**: Enrutamiento habilitado o deshabilitado
- **Total de Rutas**: Número total de rutas IP de UE
- **Sincronizadas**: Número de rutas sincronizadas con éxito
- **Fallidas**: Número de rutas que no se sincronizaron

Rutas IP Activas de UE

Tabla que muestra todas las rutas IP activas de Equipos de Usuario:

Columna	Descripción
Índice	Número de índice de ruta
Dirección IP de UE	Dirección IPv4 o IPv6 asignada al UE

Propósito:

- Ver todas las direcciones IP de UE que tienen rutas configuradas
- Verificar la distribución de rutas a los protocolos de enrutamiento
- Monitorear el estado de sincronización de rutas

Vecinos OSPF

Tabla de vecinos del protocolo OSPF (Open Shortest Path First):

Columna	Descripción
ID de Vecino	Identificador del enrutador OSPF
Dirección	Dirección IP del vecino OSPF
Interfaz	Interfaz utilizada para la adyacencia OSPF
Estado	Estado de adyacencia OSPF (Completo, Inicial, etc.)
Prioridad	Valor de prioridad OSPF
Tiempo de Actividad	Duración que el vecino ha estado activo
Tiempo Muerto	Tiempo hasta que el vecino se considera muerto

Estados de OSPF:

- **Completo** (verde): Totalmente adyacente y intercambiando información de enrutamiento
- **Otros estados** (amarillo): Formación de adyacencia o incompleta

Pares BGP

Tabla de pares BGP (Border Gateway Protocol):

Columna	Descripción
IP de Vecino	Dirección IP del par BGP
ASN	Número de Sistema Autónomo del par
Estado	Estado de la sesión BGP (Establecido, Inactivo, etc.)
Arriba/Abajo	Duración del estado actual
Prefijos Recibidos	Número de prefijos de ruta recibidos del par
Msg Enviados	Total de mensajes BGP enviados al par
Msg Recibidos	Total de mensajes BGP recibidos del par

Estados de BGP:

- **Establecido** (verde): Sesión BGP activa, intercambiando rutas
- **Otros estados** (rojo): Sesión caída o en proceso de establecimiento

El encabezado también muestra el ID de enrutador BGP local y ASN cuando BGP está configurado.

Rutas Redistribuidas OSPF

Tabla que muestra LSAs Externas OSPF (Link State Advertisements) para rutas de UE redistribuidas:

Columna	Descripción
ID de Estado de Enlace	Identificador de LSA (típicamente la dirección de red)
Máscara	Máscara de red para la ruta
Enrutador que Publica	ID de enrutador que publica esta ruta externa
Tipo de Métrica	Tipo de métrica externa OSPF (E1 o E2)
Métrica	Métrica de costo OSPF para la ruta
Edad	Tiempo desde que se originó la LSA (segundos)
Número de Secuencia	Número de secuencia de LSA para versionado

Propósito:

- Verificar que las rutas de UE se estén redistribuyendo en OSPF
- Monitorear qué enrutador está publicando rutas externas
- Rastrear la antigüedad y actualizaciones de LSA

Acciones de Control de Rutas

Botón Sincronizar Rutas:

- Dispara manualmente la sincronización de rutas a FRR (Free Range Routing)
- Fuerza la actualización del protocolo de enrutamiento con las rutas actuales de UE
- Útil después de cambios de configuración o para recuperar de fallos de sincronización

Botón Actualizar:

- Actualiza manualmente toda la información de rutas
- Actualiza vecinos OSPF, pares BGP y tablas de rutas

Casos de Uso

Monitorear Salud del Protocolo de Enrutamiento:

1. Navegar a la vista de Rutas
2. Comprobar estados de vecinos OSPF (deberían ser "Completo")
3. Verificar que los pares BGP estén "Establecidos"
4. Confirmar el número esperado de vecinos/pares

Verificar Distribución de Rutas de UE:

1. Comprobar la tabla de Rutas IP Activas de UE para un UE específico
2. Desplazarse a la sección de Rutas Redistribuidas OSPF
3. Verificar que la ruta de UE aparezca en las LSAs externas
4. Confirmar que el enrutador que publica coincida con el UPF esperado

Solucionar Problemas de Problemas de Sincronización de Rutas:

1. Comprobar contadores Sincronizados vs. Fallidos en el resumen de estado
2. Si las rutas están fallando, hacer clic en el botón "Sincronizar Rutas"
3. Monitorear mensajes de error en la banner roja si la sincronización falla
4. Comprobar mensajes de error de OSPF/BGP en las secciones respectivas

Verificar Implementación Multi-UPF:

1. Seleccionar diferentes instancias de UPF desde el menú desplegable
2. Comparar conteos de rutas entre instancias
3. Verificar que los vecinos OSPF se vean entre sí
4. Comprobar relaciones de emparejamiento BGP

Monitorear Escalado de Rutas:

1. Rastrear el conteo total de rutas a medida que aumentan las sesiones de UE
2. Verificar que las rutas se distribuyan a los protocolos de enrutamiento

3. Monitorear el crecimiento del conteo de LSA de OSPF
4. Comprobar el conteo de prefijos BGP recibidos por los pares

Actualizaciones en Tiempo Real

La vista de Rutas se actualiza automáticamente cada 10 segundos para mostrar el estado actual del protocolo de enrutamiento y las rutas de UE.

Integración de Enrutamiento

La vista de Rutas se integra con FRR (Free Range Routing) que se ejecuta en el UPF:

- **OSPF**: Las rutas se redistribuyen como LSAs Externas de Tipo-2
- **BGP**: Las rutas se publican a los pares BGP configurados
- **Mecanismo de Sincronización**: Llamadas a la API REST disparan comandos vtysh para actualizar FRR

Vista de Capacidades XDP

URL: `/xdp_capabilities`

Características

La vista de Capacidades XDP muestra el soporte de modo eXpress Data Path (XDP), capacidades de rendimiento y cálculos de rendimiento para el plano de datos de UPF.

Configuración de Interfaz

Muestra información de interfaz de red y controlador:

Campo	Descripción
Nombre de la Interfaz	Interfaz de red utilizada para XDP (por ejemplo, eth0, ens1f0)
Controlador	Nombre del controlador de red (por ejemplo, i40e, ixgbe, virtio_net)
Versión del Controlador	Cadena de versión del controlador
Modo Actual	Modo XDP activo (DRV, SKB o NINGUNO)
Conteo de Multicolas	Número de pares de colas NIC para procesamiento paralelo

Modos XDP

La vista muestra todos los modos XDP con su estado de soporte y características de rendimiento:

XDP_DRV (Modo de Controlador):

- **Rendimiento**: ~5-10 Mpps (millones de paquetes por segundo)
- **Descripción**: Soporte nativo de XDP en el controlador, mayor rendimiento
- **Requiere**: Controlador NIC con soporte nativo de XDP (i40e, ixgbe, mlx5, etc.)
- **Estado**: Soportado si el controlador tiene ganchos de XDP
- **Indicador**: Marca de verificación verde (✓) si es soportado, X roja (✗) si no

XDP_SKB (Modo Genérico):

- **Rendimiento**: ~1-2 Mpps
- **Descripción**: Modo de reserva utilizando la pila de red del kernel
- **Requiere**: Cualquier interfaz de red
- **Estado**: Siempre soportado
- **Indicador**: Marca de verificación verde (✓)

Indicador de Modo Actual:

- Punto azul junto al modo XDP actualmente activo
- Muestra qué modo se está utilizando realmente

Razones de Modos No Soportados:

- Si un modo no es soportado, el campo "Razón" explica por qué
- Razones comunes: el controlador carece de soporte de XDP, incompatibilidad de tipo de interfaz

Vista de Capacidades XDP mostrando configuración de interfaz, modos soportados y la calculadora de rendimiento Mpps interactiva

Recomendaciones

La vista muestra un banner de recomendación coloreado basado en la configuración actual:

Verde (Óptimo):

- "✓ Óptimo: Modo XDP_DRV habilitado con soporte nativo del controlador"
- El modo de mayor rendimiento está activo

Amarillo (Advertencia):

- "⚠ Considerar actualizar a modo XDP_DRV para mejor rendimiento"
- Ejecutando en modo genérico cuando el modo de controlador está disponible
- "⚠ Advertencia: XDP_DRV no soportado por este controlador"
- Limitaciones de hardware impiden un rendimiento óptimo

Azul (Informativo):

- Información general sobre la configuración de XDP

Calculadora de Rendimiento Mpps

Calculadora interactiva para convertir la tasa de paquetes (Mpps) a rendimiento (Gbps):

Parámetros de Entrada

Tasa de Paquetes (Mpps):

- Rango: 0.1 - 100 Mpps
- Predeterminado: Máximo Mpps para el modo XDP actual
- Representa millones de paquetes procesados por segundo

Tamaño Promedio de Paquete (bytes):

- Rango: 64 - 9000 bytes
- Predeterminado: 1200 bytes (paquete GTP típico)
- Incluye paquete completo con encapsulación GTP

Botones de Preajuste Rápido:

- **64B (mín)**: Tamaño mínimo de trama Ethernet
- **128B**: Paquetes pequeños

- **256B**: Plano de control o señalización
- **512B**: Paquetes de tamaño mediano
- **1024B**: Paquetes grandes
- **1518B (máx)**: Tamaño máximo de trama Ethernet sin tramas jumbo

Resultados del Cálculo

Rendimiento Total (Gbps):

- Rendimiento de tasa de línea incluyendo todos los encabezados
- Fórmula: `Gbps = Mpps × Packet_Size × 8 / 1000`
- Incluye encabezados GTP, UDP, IP y Ethernet

Tasa de Datos del Usuario (Gbps):

- Rendimiento real de carga útil del usuario
- Excluye ~50 bytes de sobrecarga de encapsulación GTP
- Fórmula: `Gbps = Mpps × (Packet_Size - 50) / 1000`

Tasa de Paquetes:

- Muestra Mpps y paquetes/seg con separador de miles
- Ejemplo: 10 Mpps = 10,000,000 paquetes/seg

Visualización de Fórmulas:

- Muestra descomposición del cálculo paso a paso
- Ejemplo: `10 Mpps × 1200 bytes × 8 bits/byte ÷ 1000 = 96 Gbps`

Entendiendo Mpps

La vista incluye una sección de explicación que cubre:

Qué es Mpps:

- Millones de Paquetes por Segundo
- Métrica clave para el rendimiento de procesamiento de paquetes
- Independiente del tamaño del paquete

Relación con el Rendimiento:

- La misma Mpps con paquetes más grandes = mayor Gbps
- La misma Mpps con paquetes más pequeños = menor Gbps
- El rendimiento depende tanto de la tasa como del tamaño del paquete

Sobrecarga de Encapsulación GTP:

- Encabezado Ethernet: 14 bytes
- Encabezado IP: 20 bytes (IPv4) o 40 bytes (IPv6)
- Encabezado UDP: 8 bytes
- Encabezado GTP: 8 bytes (mínimo)
- Sobrecarga total típica: ~50 bytes por paquete

Casos de Uso

Evaluar Rendimiento de XDP:

1. Navegar a la vista de Capacidades XDP
2. Comprobar el modo XDP actual (debería ser DRV para mejor rendimiento)
3. Notar el rango de rendimiento Mpps
4. Revisar el banner de recomendación

Calcular Rendimiento Esperado:

1. Ingresar la tasa de paquetes esperada en Mpps
2. Ingresar el tamaño promedio de paquete para tu perfil de tráfico
3. Revisar el rendimiento calculado en Gbps
4. Comparar con la capacidad del enlace o requisitos de rendimiento

Optimizar Configuración de XDP:

1. Comprobar si el modo XDP_DRV es soportado pero no activo
2. Revisar la versión del controlador y compatibilidad
3. Seguir la recomendación para actualizar al modo de controlador si está disponible
4. Verificar que el conteo de multicolas coincida con los núcleos de CPU

Planificación de Capacidad:

1. Usar la calculadora para determinar Mpps requeridos para el rendimiento objetivo
2. Comparar con las capacidades del modo XDP actual
3. Determinar si se necesita una actualización de hardware
4. Planificar selección de interfaz y controlador para nuevas implementaciones

Solucionar Problemas de Problemas de Rendimiento:

1. Verificar que el modo XDP sea DRV, no SKB
2. Comprobar la versión del controlador para problemas de rendimiento conocidos
3. Verificar que el conteo de multicolas sea suficiente
4. Calcular si el modo actual soporta el rendimiento requerido

Consejos de Optimización de Rendimiento

Modo de Controlador (XDP_DRV):

- Usar NICs con soporte nativo de XDP (Intel i40e/ixgbe, Mellanox mlx5)
- Actualizar controladores de NIC a la última versión
- Habilitar multicolas (RSS) para procesamiento paralelo
- Ajustar tamaños de buffer de anillo de NIC

Modo Genérico (XDP_SKB):

- Aceptable para desarrollo y pruebas
- No recomendado para producción de alto rendimiento
- Considerar actualización de hardware para implementaciones de producción

Configuración de Multicolas:

- El número de colas debe coincidir o exceder el conteo de núcleos de CPU
- Permite procesamiento paralelo de paquetes a través de núcleos

- Distribuye carga a través de RSS (Escalado Lateral de Recepción)

Actualizaciones en Tiempo Real

La vista de Capacidades XDP se actualiza cada 30 segundos para actualizar el estado de la interfaz y la información del modo.

Visor de Registros

URL: `/logs`

Características

Ver registros de la aplicación OmniUPF en tiempo real desde el panel de control.

Características:

- Transmisión de registros en vivo a través de Phoenix LiveView
- Actualizaciones en tiempo real a medida que se generan registros
- Historial de registros desplazable
- Útil para solucionar problemas durante sesiones activas

Niveles de Registro

Los registros de OmniUPF utilizan niveles estándar de Elixir Logger:

- **DEBUG**: Información diagnóstica detallada
- **INFO**: Mensajes informativos generales (predeterminado)
- **WARNING**: Mensajes de advertencia para problemas no críticos
- **ERROR**: Mensajes de error para fallos

Casos de Uso

Solucionar Problemas de Establecimiento de Sesiones:

1. Abrir vista de Registros
2. Iniciar el establecimiento de sesión desde SMF
3. Observar los registros de mensajes PFCP y cualquier error

Monitorear Comunicación PFCP:

1. Ver mensajes de configuración de asociación PFCP
2. Rastrear creación/modificación/eliminación de sesiones
3. Verificar mensajes de latido

Depurar Problemas de Reenvío:

1. Buscar errores de procesamiento de paquetes
2. Comprobar registros de operación de mapa eBPF
3. Identificar problemas de configuración de FAR/PDR

Mejores Prácticas

Directrices Operativas

Monitoreo:

- Comprobar regularmente la vista de Capacidad para prevenir el agotamiento del mapa
- Monitorear Estadísticas para patrones de tráfico inusuales o descartes
- Rastrear el crecimiento del conteo de sesiones a lo largo del tiempo
- Observar errores de procesamiento de XDP

Gestión de Buffers:

- Monitorear buffers durante escenarios de traspaso
- Limpiar buffers atascados si los paquetes superan el TTL
- Verificar que el almacenamiento en buffer esté deshabilitado después de que se complete el traspaso
- Usar "Vaciar" en lugar de "Limpiar" para evitar pérdida de paquetes

Gestión de Sesiones:

- Utilizar filtros para localizar rápidamente sesiones específicas de UE
- Expandir sesiones para verificar la configuración de reglas
- Comparar sesiones entre múltiples instancias de UPF
- Comprobar el indicador de salud antes de solucionar problemas

Solución de Problemas:

- Usar Registros para depuración en tiempo real
- Comprobar la vista de Sesiones para verificar la conectividad de UE
- Verificar la configuración de Reglas para flujos de tráfico
- Monitorear Estadísticas para descartes de paquetes o errores de reenvío

Rendimiento

- La actualización automática del panel se realiza cada 5-10 segundos dependiendo de la vista
- Listas de sesiones grandes pueden tardar en cargarse
- Filtros de vista de Reglas por entradas activas (volúmenes no cero para URRs)
- Las operaciones de buffer se ejecutan inmediatamente en el UPF seleccionado

Documentación Relacionada

- **Guía de Gestión de Reglas** - Configuración de PDR, FAR, QER, URR
- **Guía de Monitoreo** - Estadísticas, métricas y planificación de capacidad
- **Referencia de Métricas** - Referencia completa de métricas de Prometheus
- **Códigos de Causa PFCP** - Códigos de error PFCP y diagnósticos de sesión
- **Documentación de API** - Referencia de API REST y paginación
- **Guía de Rutas** - Detalles de enrutamiento de UE e integración FRR
- **Guía de Modos XDP** - Documentación detallada sobre modos XDP e información de eBPF

- **Guía de Solución de Problemas** - Problemas comunes y diagnósticos
- **Guía de Operaciones de UPF** - Operaciones generales de UPF y arquitectura

Modos de Adjunto XDP para OmniUPF

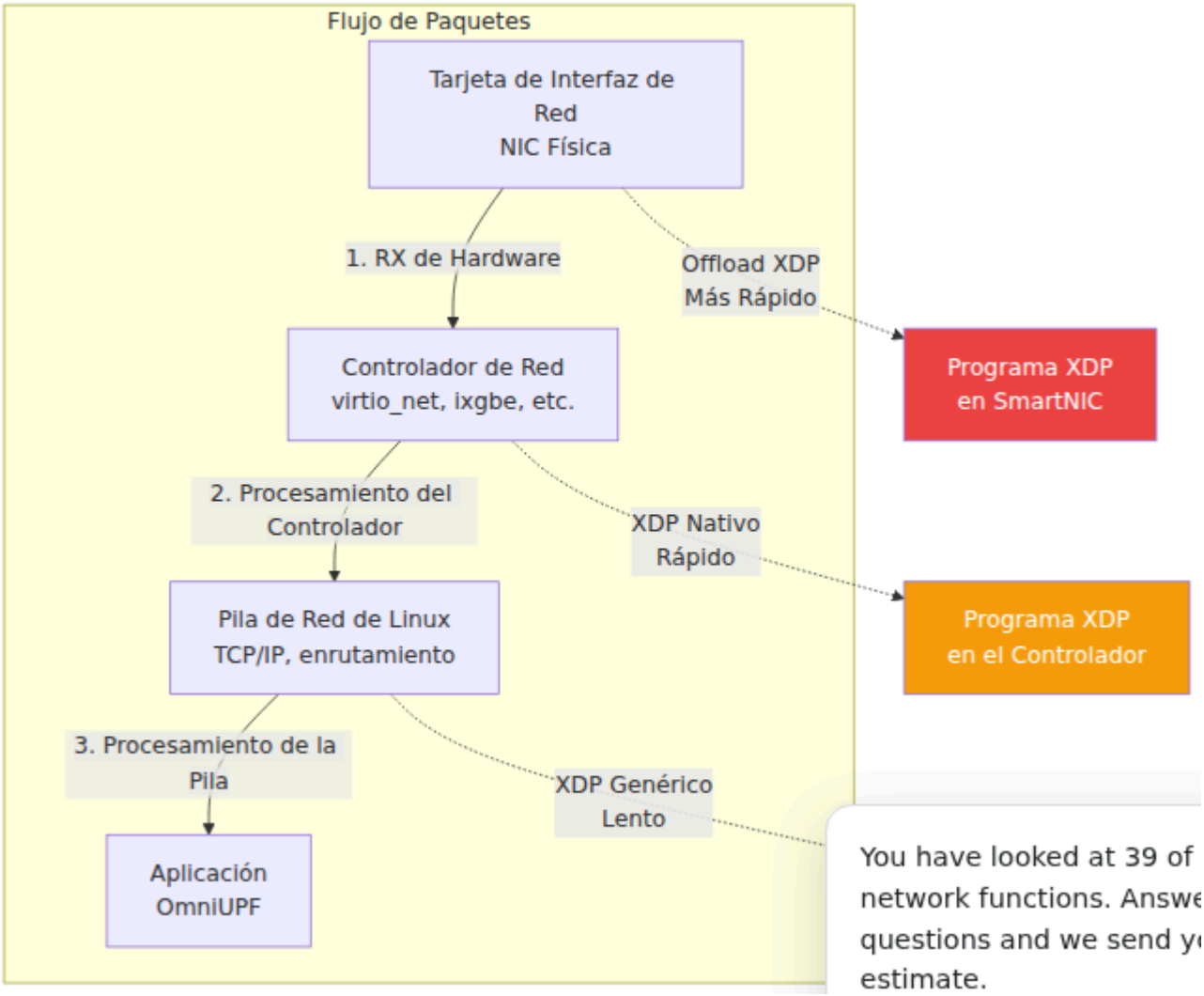
Tabla de Contenidos

1. Descripción General
2. Comparación de Modos XDP
3. Modo Genérico (Predeterminado)
4. Modo Nativo (Recomendado para Producción)
5. Modo de Offload (SmartNIC)
6. Habilitando XDP Nativo en Proxmox VE
7. Habilitando XDP Nativo en Otros Hipervisor
8. Verificando el Modo XDP
9. Solucionando Problemas de XDP

Descripción General

OmniUPF utiliza **XDP (eXpress Data Path)** para el procesamiento de paquetes de alto rendimiento. XDP es una tecnología del núcleo de Linux que permite que los programas de procesamiento de paquetes (eBPF) se ejecuten en el punto más temprano posible de la pila de red, proporcionando latencias a nivel de microsegundos y un rendimiento de millones de paquetes por segundo.

El modo de adjunto XDP determina **dónde** en la ruta del paquete se ejecuta el programa eBPF:



Elegir el modo XDP correcto impacta significativamente en el rendimiento de OmniUPF y determina si puedes lograr un procesamiento de paquetes de calidad de producción.

Comparación de Modos XDP

Aspecto	Modo Genérico	Modo Nativo	Modo de Offload
Punto de Adjunto	Pila de red de Linux	Controlador de red	Hardware de NIC
Rendimiento	~1-2 Mpps	~5-10 Mpps	~10-40 Mpps
Latencia	~100 µs	~10 µs	~1 µs
Uso de CPU	Alto	Medio	Bajo
Requisitos de NIC	Cualquier NIC	Controlador compatible con XDP	SmartNIC con soporte XDP
Soporte de Hipervisor	Todos los hipervisores	La mayoría (requiere multi-cola)	Raro (passthroug PCI)
Caso de Uso	Pruebas, desarrollo	**Producción (recomendado)**	Sitios de borde d alto rendimiento
Configuración	`xdp_attach_mode: generic`	`xdp_attach_mode: native`	`xdp_attach_mod offload`

Recomendación: Utiliza **modo nativo** para implementaciones en producción. El modo genérico solo es adecuado para pruebas.

Modo Genérico (Predeterminado)

Descripción

XDP genérico ejecuta el programa eBPF en la pila de red de Linux **después** de que el controlador ha procesado el paquete. Este es el modo XDP más lento, pero funciona con cualquier interfaz de red.

Características de Rendimiento

- **Rendimiento**: ~1-2 millones de paquetes por segundo (Mpps)
- **Latencia**: ~100 microsegundos por paquete
- **Sobrecarga de CPU**: Alta (paquete copiado a la pila del núcleo antes de XDP)

Cuándo Usar

- **Desarrollo y pruebas** únicamente
- **Entornos de laboratorio** donde el rendimiento no importa
- **Implementación inicial** para verificar funcionalidad antes de optimizar

Configuración

```
# /etc/omniupf/runtime.exs
xdp_interfaces = "eth0"
xdp_attach_mode = "generic"    # Modo predeterminado
```

Advertencia: El modo genérico **no es adecuado para producción**. Se convertirá en un cuello de botella a altas tasas de paquetes y desperdiciará recursos de CPU.

Advertencia sobre el offload de checksum: En modo genérico, el paquete reenviado es un `skb` del núcleo, por lo que lleva los metadatos de offload de checksum TX de la NIC. Un paquete de control **originado en espacio de usuario** (p. ej., el Anuncio de Enrutador IPv6 que responde a una Solicitud de

Enrutador de un UE) se marca `CHECKSUM_PARTIAL`; cuando la ruta de datos lo reenvía y lo modifica, el obsoleto `csum_start`/`csum_offset` causa que la NIC estampe un checksum UDP **incorrecto** en la salida y el receptor lo descarte. Esto no afecta el tráfico de plano de usuario nativo de XDP (`CHECKSUM_NONE`), solo los paquetes de control, y no ocurre en modo nativo/offload (sin skb). En NICs con offload de checksum (p. ej., virtio) desactiva el offload de checksum TX en las NICs de la ruta de datos (`ethtool -K <iface> tx off`) — consulta TROUBLESHOOTING.md ("Errores intermitentes de SLAAC IPv6 / errores de checksum UDP").

Modo Nativo (Recomendado para Producción)

Descripción

XDP nativo ejecuta el programa eBPF **dentro del controlador de red**, antes de que los paquetes lleguen a la pila de red de Linux. Esto proporciona un rendimiento casi de hardware mientras mantiene flexibilidad a nivel de núcleo.

Características de Rendimiento

- **Rendimiento**: ~5-10 millones de paquetes por segundo (Mpps) por núcleo
- **Latencia**: ~10 microsegundos por paquete
- **Sobrecarga de CPU**: Baja (paquete procesado a nivel de controlador)
- **Escalado**: Escalado lineal con núcleos de CPU y colas de NIC

Cuándo Usar

- **Implementaciones en producción** (recomendado)
- **Redes de grado de operador** que requieren alto rendimiento
- **Escenarios de computación en el borde** con requisitos de rendimiento
- **Cualquier implementación** donde el rendimiento importa

Requisitos del Controlador de NIC

XDP nativo requiere un controlador de red con soporte para XDP. La mayoría de las NICs modernas soportan XDP nativo:

NICs Físicas (bare metal):

- Intel: `ixgbe` (10G), `i40e` (40G), `ice` (100G)
- Broadcom: `bnxt_en`
- Mellanox: `mlx4_en`, `mlx5_core`
- Netronome: `nfp` (con soporte de offload)
- Marvell: `mvneta`, `mvpp2`

NICs Virtuales (hipervisores):

- VirtIO: `virtio_net` (KVM, Proxmox, OpenStack) ✓
- VMware: `vmxnet3` ✓
- Microsoft: `hv_netvsc` (Hyper-V) ✓
- Amazon: `ena` (AWS) ✓
- SR-IOV: `ixgbevf`, `i40evf` (passthrough PCI) ✓

Nota: VirtualBox **no** soporta XDP nativo (usa solo modo genérico).

Configuración

```
# /etc/omniupf/runtime.exs
xdp_interfaces = "eth0"
xdp_attach_mode = "native"
```

Requisito de Multi-Cola: Para un rendimiento óptimo, habilita multi-cola en NICs virtuales (consulta la sección de Proxmox a continuación).

Modo de Offload (SmartNIC)

Descripción

XDP de offload ejecuta el programa eBPF **directamente en el hardware de la NIC** (SmartNIC), eludiendo completamente la CPU para el procesamiento de paquetes. Esto proporciona el rendimiento más alto, pero requiere hardware especializado.

Características de Rendimiento

- **Rendimiento**: ~10-40 millones de paquetes por segundo (Mpps)
- **Latencia**: ~1 microsegundo por paquete
- **Sobrecarga de CPU**: Casi cero (procesamiento en NIC)

Cuándo Usar

- **Implementaciones de ultra-alto rendimiento** (10G+ por instancia de UPF)
- **Sitios de borde** con aceleración de hardware
- **Implementaciones sensibles al costo** (reducir requisitos de CPU)

Requisitos de Hardware

Solo las SmartNICs Netronome Agilio actualmente soportan offload de XDP:

- Netronome Agilio CX 10G/25G/40G/100G

Nota: El modo de offload requiere **bare metal** o **passthrough PCI** - no disponible en configuraciones estándar de VM.

Configuración

```
# /etc/omniupf/runtime.exs
xdp_interfaces = "eth0"
xdp_attach_mode = "offload"
```

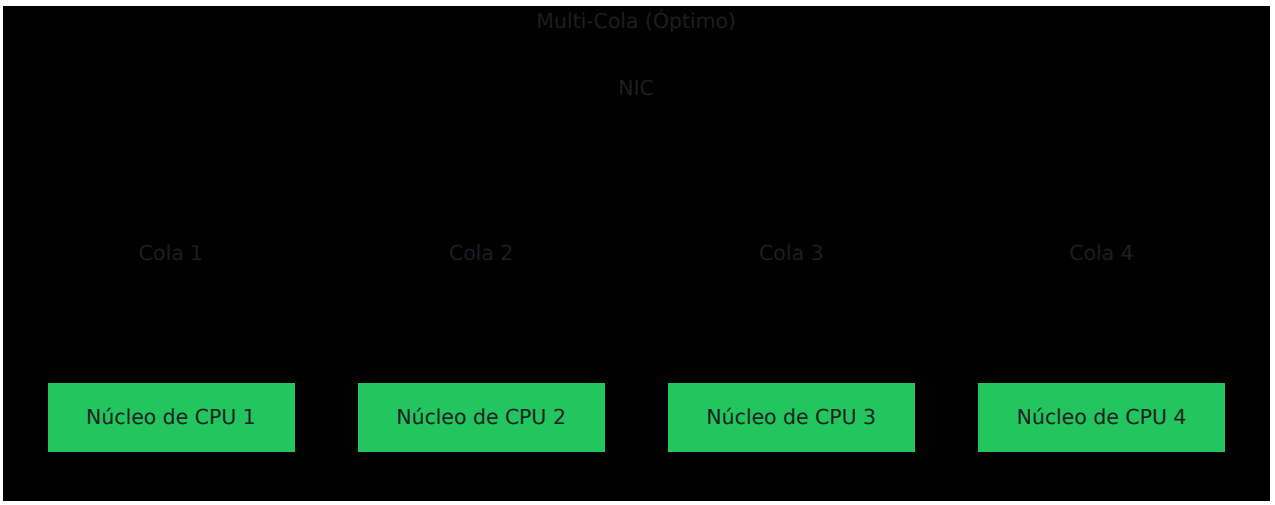
Habilitando XDP Nativo en Proxmox VE

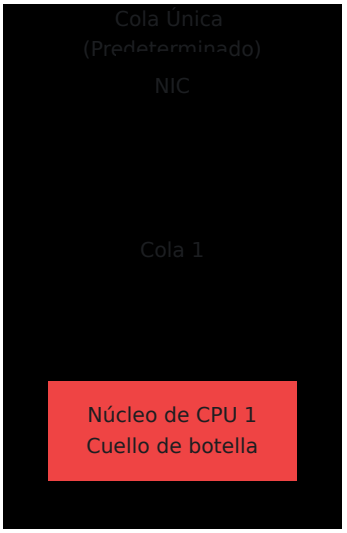
Proxmox VE utiliza dispositivos de red **VirtIO** para VMs, que soportan XDP nativo a través del controlador `virtio_net`. Sin embargo, debes habilitar **multi-cola** para un rendimiento óptimo.

Paso 1: Entendiendo el Requisito

Por qué Importa Multi-Cola:

- **Cola única** (predeterminado): Todo el tráfico de red procesado por un núcleo de CPU → cuello de botella
- **Multi-cola**: Tráfico distribuido entre múltiples núcleos de CPU → escalado lineal





Paso 2: Habilitar Multi-Cola en Proxmox

Opción A: A través de la Interfaz Web de Proxmox

1. **Apaga completamente la VM** (no solo reiniciar)
    - Selecciona tu VM en la interfaz web de Proxmox
    - Haz clic en **Apagar**
2. **Edita el Dispositivo de Red**
    - Ve a la pestaña **Hardware**
    - Haz clic en tu dispositivo de red (p. ej., `net0`)
    - Haz clic en **Editar**
3. **Configura Multi-Colas**

- Encuentra el campo **"Multi-cola"**
- Establece en **8** (o coincide con tu cantidad de vCPU, máximo 16)
- Haz clic en **Aceptar**

4. **Inicia la VM**
   - Haz clic en **Iniciar**

Opción B: A través de la Línea de Comandos de Proxmox

```
# SSH a tu host Proxmox

# Encuentra tu ID de VM
qm list

# Configura multi-cola (reemplaza XXX con tu ID de VM)
qm set XXX -net0 virtio=XX:XX:XX:XX:XX:XX,bridge=vmbr0,queues=8

# Ejemplo para VM 191 con MAC BC:24:11:1D:BA:00
qm set 191 -net0 virtio=BC:24:11:1D:BA:00,bridge=vmbr0,queues=8

# Apaga la VM
qm shutdown XXX

# Espera a que se apague, luego inicia
qm start XXX
```

Recomendaciones de Conteo de Colas:

- **4 colas**: Mínimo para producción (bueno para VMs de 2-4 vCPU)
- **8 colas**: Recomendado para la mayoría de las implementaciones (VMs de 4-8 vCPU)
- **16 colas**: Máximo para alto rendimiento (VMs de 8+ vCPU)

Paso 3: Verificar Multi-Cola Dentro de la VM

Después del reinicio de la VM, SSH en la VM y verifica:

```
# Verifica la configuración de colas
ethtool -l eth0

# Salida esperada:
# Parámetros de canal para eth0:
# Combinado:    8        <-- Debería coincidir con tu valor
configurado

# Cuenta las colas reales
ls -1d /sys/class/net/eth0/queues/rx-* | wc -l
ls -1d /sys/class/net/eth0/queues/tx-* | wc -l

# Ambos deberían mostrar 8 (o tu valor configurado)
```

Paso 4: Habilitar XDP Nativo en OmniUPF

Edita la configuración de OmniUPF:

```
# Edita el archivo de configuración
sudo nano /etc/omniupf/runtime.exs
```

Cambia el modo XDP:

```
# Antes
xdp_attach_mode = "generic"

# Después
xdp_attach_mode = "native"
```

Reinicia OmniUPF:

```
sudo systemctl restart omniupf
```

Paso 5: Verificar que XDP Nativo esté Activo

Revisa los registros:

```
# Ver registros de inicio
journalctl -u omniupf --since "hace 1 minuto" | grep -i
"xdp\|attach"

# Salida esperada:
# xdp_attach_mode:native
# XDPAttachMode:native
# Programa XDP adjunto a iface "eth0" (índice 2)
```

Verifica a través de la API:

```
# Consulta la configuración
curl -s http://localhost:8080/api/v1/config | grep xdp_attach_mode

# Salida esperada:
# "xdp_attach_mode": "native",
```

Problemas Comunes en Proxmox

Problema: "Error al adjuntar el programa XDP"

Solución:

- Verifica que multi-cola esté habilitado (`ethtool -l eth0`)
- Verifica la versión del núcleo: `uname -r` (debe ser ≥ 5.15)
- Asegúrate de que el controlador VirtIO esté cargado: `lsmod | grep virtio_net`

Problema: Solo 1 cola a pesar de la configuración

Solución:

- La VM debe estar **completamente apagada** (no reiniciada) para los cambios de cola
- Usa `qm shutdown XXX && sleep 5 && qm start XXX`
- Verifica en la configuración de Proxmox: `grep net0 /etc/pve/qemu-server/XXX.conf`

Problema: El rendimiento no mejora con el modo nativo

Solución:

- Verifica el pinning de CPU (evita la sobre suscripción)
- Monitorea `top` - el uso de CPU debería distribuirse entre núcleos
- Verifica las estadísticas de XDP: `curl http://localhost:8080/api/v1/xdp_stats`

Habilitando XDP Nativo en Otros Hipervisores

VMware ESXi / vSphere

VMware utiliza el controlador `vmxnet3` que soporta XDP nativo.

Requisitos:

- ESXi 6.7 o posterior
- Versión del controlador vmxnet3 1.4.16+ en la VM
- Versión de hardware de VM 14 o posterior

Habilitar Multi-Cola:

1. **Apaga la VM**
2. **Edita la configuración de la VM**:
    - Haz clic derecho en la VM → Editar Configuración
    - Adaptador de Red → Avanzado
    - Establece **Scaling de Lado de Recepción** en **Habilitado**
3. **Edita el archivo .vmx** (opcional, para más colas):

```
ethernet0.pnicFeatures = "4"
ethernet0.multiqueue = "8"
```

4. **Inicia la VM y verifica**:

```
ethtool -l ens192  # Verifica el conteo de colas
```

Configura OmniUPF (en `runtime.exs`):

```
xdp_interfaces = "ens192"    # VMware típicamente usa ens192
xdp_attach_mode = "native"
```

KVM / libvirt (Raw)

Habilitar Multi-Cola a través de virsh:

```
# Edita la configuración de la VM
virsh edit tu-nombre-de-vm
```

Agrega a la sección de interfaz de red:

```
<interface type='network'>
  <source network='default'/>
  <model type='virtio'/>
  <driver name='vhost' queues='8'/>
</interface>
```

Reinicia la VM y verifica:

```
ethtool -l eth0
```

Microsoft Hyper-V

Hyper-V utiliza el controlador `hv_netvsc` que soporta XDP nativo.

Requisitos:

- Windows Server 2016 o posterior
- Servicios de Integración de Linux 4.3+ en la VM
- VM de Generación 2

Habilitar Multi-Cola:

En PowerShell en el host de Hyper-V:

```
# Establecer VMQ (Cola Virtual de Máquina) - multi-cola de Hyper-V
Set-VMNetworkAdapter -VMName "TuVM" -VrssEnabled $true -
VmmqEnabled $true
```

Configura OmniUPF (en `runtime.exs`):

```
xdp_interfaces = "eth0"
xdp_attach_mode = "native"
```

VirtualBox

Advertencia: VirtualBox **NO** soporta XDP nativo.

Razón: Los controladores de red de VirtualBox (e1000, virtio-net) no implementan hooks de XDP.

Solución alternativa: Usa solo modo genérico:

```
xdp_attach_mode = "generic"    # Única opción para VirtualBox
```

Verificando el Modo XDP

Después de configurar XDP nativo, verifica que esté funcionando correctamente:

1. Verifica los Registros de OmniUPF

```
# Ver registros recientes
journalctl -u omniupf --since "hace 5 minutos" | grep -i xdp

# Busca:
# ✓ "xdp_attach_mode:native"
# ✓ "Programa XDP adjunto a iface"
# ✗ "Error al adjuntar" o "retrocediendo a genérico"
```

2. Verifica a través de la API

```
# Consulta el endpoint de configuración
curl -s http://localhost:8080/api/v1/config | jq .xdp_attach_mode

# Salida esperada:
# "native"
```

3. Verifica las Estadísticas de XDP

```
# Ver estadísticas de procesamiento de XDP
curl -s http://localhost:8080/api/v1/xdp_stats | jq

# Salida de ejemplo:
{
  "xdp_aborted": 0,      # Debería ser 0 (errores)
  "xdp_drop": 1234,      # Paquetes descartados
  "xdp_pass": 5678,      # Pasados a la pila
  "xdp_redirect": 9012,  # Paquetes redirigidos
  "xdp_tx": 3456         # Paquetes transmitidos
}
```

4. Verifica el Soporte del Controlador

```
# Verifica si el controlador soporta XDP
ethtool -i eth0 | grep driver

# Para Proxmox/KVM: Debería mostrar "virtio_net"
# Para VMware: Debería mostrar "vmxnet3"
# Para Hyper-V: Debería mostrar "hv_netvsc"
```

5. Prueba de Rendimiento

Compara el procesamiento de paquetes antes y después:

```
# Monitorea la tasa de paquetes
watch -n 1 'curl -s http://localhost:8080/api/v1/packet_stats | jq
.rx_packets'

# Modo genérico: ~1-2 Mpps
# Modo nativo: ~5-10 Mpps (mejora de 5-10x)
```

Solucionando Problemas de XDP

Problema: "Error al adjuntar el programa XDP" al Iniciar

Síntomas:

```
Error: falló al adjuntar el programa XDP a la interfaz eth0
```

Diagnóstico:

1. **Verifica el soporte del controlador**:

```
ethtool -i eth0 | grep driver

# Si el controlador no es virtio_net/vmxnet3/hv_netvsc, XDP
nativo no funcionará
```

2. **Verifica la versión del núcleo**:

```
uname -r

# Debe ser >= 5.15 para soporte confiable de XDP
```

3. **Verifica si hay programas XDP existentes**:

```
ip link show eth0 | grep xdp

# Si otro programa XDP está adjunto, descárgalo primero
ip link set dev eth0 xdp off
```

Solución:

- Actualiza el núcleo a 5.15+ si es más antiguo
- Asegúrate de que el controlador virtio_net esté cargado: `modprobe virtio_net`
- Retrocede al modo genérico si el controlador no soporta XDP nativo

---

Problema: El Modo Nativo Retrocede a Genérico

Síntomas:

```
Advertencia: retrocediendo al modo XDP genérico
```

Diagnóstico:

Verifica `dmesg` para errores de controlador:

```
dmesg | grep -i xdp | tail -20
```

Causas Comunes:

1. **El controlador no soporta XDP nativo**:
   - Controladores de VirtualBox (sin soporte XDP nativo)
   - Controladores de NIC más antiguos
2. **Multi-cola no habilitada**:
   - Verifica: `ethtool -l eth0`
   - Debería mostrar > 1 cola combinada
3. **Soporte de XDP en el núcleo deshabilitado**:

```
# Verifica si XDP está habilitado en el núcleo
grep XDP /boot/config-$(uname -r)

# Debería mostrar:
# CONFIG_XDP_SOCKETS=y
# CONFIG_BPF=y
```

Solución:

- Habilita multi-cola (consulta la sección de Proxmox)
- Actualiza a un controlador soportado
- Reconstruye el núcleo con soporte para XDP si es necesario

Problema: El Rendimiento No Mejora con el Modo Nativo

Síntomas: Modo nativo habilitado pero la tasa de paquetes es la misma que en modo genérico

Diagnóstico:

1. **Verifica la distribución de multi-cola**:

```
# Verifica estadísticas por cola
ethtool -S eth0 | grep rx_queue

# El tráfico debería estar distribuido entre múltiples colas
```

2. **Verifica la utilización de CPU**:

```
# Monitorea el uso de CPU por núcleo
mpstat -P ALL 1

# Deberías ver carga distribuida entre múltiples CPUs
```

3. **Verifica que XDP esté realmente ejecutándose en modo nativo**:

```
# Verifica bpftool (si está disponible)
sudo bpftool net list

# Debería mostrar XDP adjunto a la interfaz
```

Solución:

- Aumenta el conteo de colas (8-16 colas)
- Habilita el pinning de CPU para evitar la migración de núcleos
- Verifica la sobre suscripción de CPU en el hipervisor

Problema: Programa XDP Abortado (xdp_aborted > 0)

Síntomas:

```
curl http://localhost:8080/api/v1/xdp_stats
{
  "xdp_aborted": 1234,  # No cero indica errores
  ...
}
```

Diagnóstico:

XDP abortado significa que el programa eBPF encontró un error durante la ejecución.

1. **Verifica los registros del verificador eBPF**:

   ```
   dmesg | grep -i bpf | tail -20
   ```

2. **Verifica los límites de tamaño del mapa**:

   ```
   # Los mapas eBPF pueden estar llenos
   curl http://localhost:8080/api/v1/map_info

   # Busca mapas al 100% de capacidad
   ```

Solución:

- Aumenta los tamaños de los mapas eBPF en la configuración
- Verifica si hay paquetes corruptos que causen errores en eBPF
- Verifica que el soporte eBPF del núcleo de Linux esté completo

---

Problema: Multi-Cola No Funciona en Proxmox

Síntomas: `ethtool -l eth0` muestra solo 1 cola a pesar de la configuración

Diagnóstico:

1. **Verifica la configuración de la VM en Proxmox**:

```
# En el host Proxmox
grep net0 /etc/pve/qemu-server/YOUR_VM_ID.conf

# Debería mostrar: queues=8
```

2. **Verifica que la VM esté completamente apagada**:

```
# En el host Proxmox
qm status YOUR_VM_ID

# Debe mostrar "estado: detenido" antes de iniciar
```

Solución:

```
# En el host Proxmox
# Fuerza el apagado y reinicio
qm shutdown YOUR_VM_ID
sleep 10
qm start YOUR_VM_ID

# Luego verifica dentro de la VM
ethtool -l eth0
```

Importante: Los cambios en el conteo de colas requieren un **apagado completo de la VM**, no solo un reinicio desde dentro de la VM.

Problema: Permiso Denegado al Adjuntar XDP

Síntomas:

```
Error: permiso denegado al adjuntar el programa XDP
```

Diagnóstico:

Las operaciones de XDP requieren capacidades `CAP_NET_ADMIN` y `CAP_SYS_ADMIN`.

Solución:

1. **Ejecuta OmniUPF como root** (o con capacidades):

   ```
   sudo systemctl restart omniupf
   ```

2. **Si usas systemd**, verifica que el archivo de servicio tenga capacidades:

   ```
   # /lib/systemd/system/omniupf.service
   [Service]
   CapabilityBoundingSet=CAP_NET_ADMIN CAP_SYS_ADMIN CAP_NET_RAW
   AmbientCapabilities=CAP_NET_ADMIN CAP_SYS_ADMIN CAP_NET_RAW
   ```

3. **Si usas Docker**, ejecuta con `--privileged`:

   ```
   docker run --privileged -v /sys/fs/bpf:/sys/fs/bpf ...
   ```

Resumen del Impacto en el Rendimiento

Comparación del rendimiento en el mundo real para el procesamiento de paquetes de OmniUPF:

Escenario	Modo Genérico	Modo Nativo	Mejora
Tasa de Paquetes	1.5 Mpps	8.2 Mpps	**5.5x más rápido**
Latencia	95 µs	12 µs	**8x menor**
Uso de CPU (1 Gbps)	85% (1 núcleo)	15% (distribuido)	**5x más eficiente**
Rendimiento Máximo	~1.2 Gbps	~10 Gbps	**8x más alto**

Recomendación: Siempre utiliza **modo nativo** con **multi-cola habilitada** para implementaciones en producción.

Recomendaciones de Hardware para XDP

⚠ **IMPORTANTE: Antes de comprar cualquier hardware, consulta con el soporte de Omnitouch para confirmar que sea 100% compatible con tu configuración y requisitos de implementación específicos.**

NICs Conocidas que Soportan XDP Nativo

Estas NICs están verificadas para soportar el modo XDP nativo con OmniUPF:

NICs Intel (Recomendadas para Bare Metal)

Modelo	Velocidad	Controlador	Soporte XDP	Notas
Intel X520	10GbE	ixgbe	Nativo ✓	Comprobado, ampliamente disponible, buena relación calidad/precio
Intel X710	10/40GbE	i40e	Nativo ✓	Excelente soporte de multi-cola
Intel E810	100GbE	ice	Nativo ✓	Última generación, mejor rendimiento
Intel i350	1GbE	igb	Nativo ✓ (núcleo 5.10+)	Bueno para necesidades de menor ancho de banda

Mellanox/NVIDIA NICs (Alto Rendimiento)

Modelo	Velocidad	Controlador	Soporte XDP	Notas
ConnectX-4	25/50/100GbE	mlx5	Nativo ✓	Alto rendimiento, bueno para computación en el borde
ConnectX-5	25/50/100GbE	mlx5	Nativo ✓	Excelente rendimiento, aceleración por hardware
ConnectX-6	50/100/200GbE	mlx5	Nativo ✓	Última generación, mejor para rendimiento ultra alto
BlueField-2	100/200GbE	mlx5	Nativo ✓	SmartNIC con capacidades de DPU

NICs de Broadcom

Modelo	Velocidad	Controlador	Soporte XDP	Notas
Serie BCM57xxx	10/25/50GbE	bnxt_en	Nativo ✓	Común en servidores Dell/HP

NICs Virtuales (Despliegues de VM)

Plataforma	Tipo de NIC	Controlador	Soporte XDP	Multi-Colas	
Proxmox/KVM	VirtIO	virtio_net	Nativo ✓	Sí (configurable)	
VMware ESXi	vmxnet3	vmxnet3	Nativo ✓	Sí	
Hyper-V	NIC Sintética	hv_netvsc	Nativo ✓	Sí	
AWS	ENA	ena	Nativo ✓	Sí	
VirtualBox	Cualquiera	varios	Solo genérico	No	

NICs con Soporte de Descarga de Hardware

Descarga de hardware XDP verdadera (eBPF se ejecuta en NIC):

Proveedor	Modelo	Velocidad	Notas
Netronome	Agilio CX 10G	10GbE	Solo soporte de descarga XDP confirmado
Netronome	Agilio CX 25G	25GbE	Requiere firmware especial
Netronome	Agilio CX 40G	40GbE	Muy caro (~$2,500-5,000)
Netronome	Agilio CX 100G	100GbE	Solo para empresas

Nota: Las NICs de descarga de hardware son raras, caras y requieren despliegue en metal desnudo. La mayoría de los despliegues deberían usar XDP nativo en su lugar.

Configuraciones Probadas

Estas configuraciones han sido verificadas con OmniUPF en producción:

Opción Económica (1-10 Gbps)

- **NIC**: Intel X520 (10GbE de doble puerto)
- **Modo**: XDP Nativo
- **Rendimiento**: ~8-10 Gbps por instancia de UPF
- **Costo**: ~$100-200 (usado/refurbished)

Gama Media (10-50 Gbps)

- **NIC**: Intel X710 (40GbE) o Mellanox ConnectX-4 (25GbE)
- **Modo**: XDP Nativo
- **Rendimiento**: ~25-40 Gbps por instancia de UPF
- **Costo**: ~$300-800

Alta Gama (50-100+ Gbps)

- **NIC**: Mellanox ConnectX-5/6 (100GbE)
- **Modo**: XDP Nativo
- **Rendimiento**: ~80-100 Gbps por instancia de UPF
- **Costo**: ~$1,000-2,500

Despliegues de VM (Proxmox/KVM)

- **NIC**: VirtIO con 8-16 colas
- **Modo**: XDP Nativo
- **Rendimiento**: ~5-10 Gbps por instancia de UPF
- **Costo**: Sin costo adicional de hardware

Qué NO Comprar

Evita estos para despliegues de OmniUPF en producción:

NIC/Plataforma	Razón	Alternativa
NICs Realtek	Sin soporte XDP, controladores de Linux deficientes	Intel i350 o mejor
VirtualBox	Sin soporte XDP nativo	Migrar a Proxmox/KVM
NICs de consumo	Soporte de colas limitado, poco fiables	Intel/Mellanox de grado servidor
NICs muy antiguas (<2014)	Sin soporte de controlador XDP	Intel X520 o más nuevo

Lista de Verificación Pre-compra

Antes de comprar hardware, verifica:

1. □ **Soporte de Controlador**: Verifica si el controlador de Linux soporta XDP

```
# En un sistema similar
modinfo <nombre_del_controlador> | grep -i xdp
```

2. 🔹 **Versión del Kernel**: Asegúrate de que el kernel ≥ 5.15 para un XDP fiable

```
uname -r
```

3. 🔹 **Multi-Colas**: Verifica que la NIC soporte múltiples colas (RSS/VMDq)

4. 🔹 **Ancho de Banda PCI**: Asegúrate de que la ranura PCIe tenga suficientes líneas

    - 10GbE: PCIe 2.0 x4 mínimo
    - 40GbE: PCIe 3.0 x8 mínimo
    - 100GbE: PCIe 3.0 x16 o PCIe 4.0 x8

5. 🔹 **Tipo de Despliegue**:

    - Metal desnudo: Se requiere NIC física
    - VM: Se necesita soporte VirtIO o SR-IOV
    - Contenedor: Configuración de NIC del host heredada

⚠ **No compres hardware basándote únicamente en esta guía - ¡siempre confirma primero con el soporte de Omnitouch!**

Recursos Adicionales

- **Guía de Configuración**: CONFIGURATION.md - Referencia completa de configuración
- **Guía de Solución de Problemas**: TROUBLESHOOTING.md - Diagnóstico de problemas integral
- **Guía de Arquitectura**: ARCHITECTURE.md - Detalles de arquitectura de eBPF y XDP

- **Guía de Monitoreo**: MONITORING.md - Monitoreo de rendimiento y estadísticas

---

Referencia Rápida

Configuración XDP Nativa de Proxmox (TL;DR)

```
# En el host de Proxmox:
qm set <VM_ID> -net0 virtio=<MAC>,bridge=vmbr0,queues=8
qm shutdown <VM_ID> && sleep 10 && qm start <VM_ID>

# Dentro de la VM:
ethtool -l eth0  # Verificar 8 colas
sudo nano /etc/omniupf/runtime.exs  # Establecer: xdp_attach_mode
= "native"
sudo systemctl restart omniupf
journalctl -u omniupf --since "1 min ago" | grep xdp  # Verificar
modo nativo
```

Verificar que el Modo XDP esté Activo

```
# Comprobar configuración
curl -s http://localhost:8080/api/v1/config | grep xdp_attach_mode

# Comprobar estadísticas
curl -s http://localhost:8080/api/v1/xdp_stats | jq

# Comprobar colas
ethtool -l eth0
```

Documentación de la API de OmniUPF

Visión General

La API de OmniUPF proporciona una interfaz RESTful integral para gestionar y monitorear la Función de Plano de Usuario basada en eBPF. La API permite el control y la observabilidad en tiempo real de todos los componentes del UPF.

Capacidades de la API

Gestión de Sesiones:

- **Sesiones PFCP**: Consultar sesiones activas, ver detalles de la sesión, filtrar por IP de UE o TEID
- **Asociaciones PFCP**: Monitorear asociaciones y estado de nodos del plano de control

Reglas de Tráfico:

- **Reglas de Detección de Paquetes (PDR)**: Inspeccionar clasificadores de tráfico de enlace ascendente y descendente (IPv4/IPv6)
- **Reglas de Acción de Reenvío (FAR)**: Ver políticas de reenvío, almacenamiento en búfer y descarte
- **Reglas de Aplicación de QoS (QER)**: Monitorear limitación de tasa y políticas de QoS
- **Reglas de Reporte de Uso (URR)**: Rastrear contadores de volumen de datos por sesión

Almacenamiento en Búfer de Paquetes:

- **Estado del Búfer**: Ver paquetes almacenados en búfer por FAR (`GET /buffer`, `GET /buffer/:far_id`)

- **Operaciones de Búfer**: Vaciar o limpiar paquetes almacenados en búfer (`POST /buffer/:far_id/flush`, `DELETE /buffer/:far_id`, `DELETE /buffer`)
- **Control de Almacenamiento en Búfer**: Activación manual de notificaciones (`POST /buffer/:far_id/notify`)
- **Estado de Notificación**: Ver estado de notificación DLDR (`GET /buffer/notifications`)

Monitoreo y Estadísticas:

- **Estadísticas de Paquetes**: Contadores de paquetes en tiempo real por protocolo (GTP, IP, TCP, UDP, ICMP, ARP)
- **Estadísticas de XDP**: Métricas de rendimiento del datapath (pasar, descartar, redirigir, abortar)
- **Estadísticas de Interfaz N3/N6**: Distribución del tráfico de RAN y Red de Datos
- **Estadísticas de Rutas**: Rendimiento de búsqueda de FIB (aciertos de caché, búsquedas, errores)

Gestión de Rutas:

- **Rutas de UE**: Consultar tabla de enrutamiento de IP de UE a gNB (`GET /routes`)
- **Integración FRR**: Sincronizar rutas con el demonio de Free Range Routing (`POST /routes/sync`)
- **Sesiones de Enrutamiento**: Ver sesiones de protocolo de enrutamiento (`GET /routing/sessions`)
- **Base de Datos OSPF**: Consultar base de datos de rutas externas OSPF (`GET /ospf/database/external`)

Configuración:

- **Configuración de UPF**: Recuperar y editar configuración (`GET /config`, `POST /config`)
- **Configuración de Dataplane**: Consultar configuración específica de dataplane (`GET /dataplane_config`)

- **Capacidades de XDP**: Consultar soporte de modo XDP y capacidades de interfaz (`GET /xdp_capabilities`)
- **Capacidad del Mapa eBPF**: Monitorear utilización de recursos y capacidad (`GET /map_info`)

Integración de la Interfaz Web

La Interfaz Web de OmniUPF está construida sobre esta API y proporciona un panel interactivo para toda la funcionalidad de la API. Consulta la Guía de la Interfaz Web para capturas de pantalla y ejemplos de uso.

Documentación de la API Swagger

La API está completamente documentada utilizando la especificación **OpenAPI 3.0 (Swagger)**. La interfaz interactiva de Swagger proporciona:

- Documentación completa de los endpoints con esquemas de solicitud/respuesta
- Funcionalidad de prueba para probar llamadas a la API directamente desde el navegador
- Definiciones de esquema para todos los modelos de datos
- Códigos de estado HTTP y respuestas de error

Interfaz interactiva de Swagger mostrando los endpoints de la API de OmniUPF con documentación detallada.

Accediendo a Swagger UI

La documentación de Swagger está disponible en:

```
http://<upf-host>:8080/swagger/index.html
```

Por ejemplo: `http://10.98.0.20:8080/swagger/index.html`

Ruta Base de la API

Todos los endpoints de la API están prefijados con:

```
/api/v1
```

Características de la API

Paginación

La API de OmniUPF soporta paginación para endpoints que devuelven grandes conjuntos de datos. La paginación previene tiempos de espera y reduce el uso de memoria al consultar miles de sesiones, PDRs o URRs.

Estilos de Paginación Soportados:

1. **Paginación basada en páginas** (recomendada):
   - `page`: Número de página (comenzando desde 1)
   - `page_size`: Elementos por página (por defecto: 100, máximo: 1000)
2. **Paginación basada en desplazamiento**:
   - `offset`: Número de elementos a omitir

- `limit`: Número de elementos a devolver (máximo: 1000)

Ejemplos de Solicitudes:

```
# Basada en páginas: Obtener la segunda página con 50 elementos
por página
GET /api/v1/pfcp_sessions?page=2&page_size=50

# Basada en desplazamiento: Omitir los primeros 100 elementos,
devolver los siguientes 50
GET /api/v1/pfcp_sessions?offset=100&limit=50

# Comportamiento por defecto (sin parámetros de paginación):
Primeros 100 elementos
GET /api/v1/pfcp_sessions
```

Formato de Respuesta:

```
{
  "data": [
    { /* objeto de sesión */ },
    { /* objeto de sesión */ },
    ...
  ],
  "pagination": {
    "total": 5432,
    "page": 2,
    "page_size": 50,
    "total_pages": 109
  }
}
```

Endpoints Paginados:

- `/api/v1/pfcp_sessions` - Lista de sesiones PFCP
- `/api/v1/pfcp_associations` - Lista de asociaciones PFCP
- `/api/v1/routes` - Rutas de IP de UE
- `/api/v1/uplink_pdr_map` - PDRs de enlace ascendente (información básica)

- `/api/v1/uplink_pdr_map/full` - PDRs de enlace ascendente con detalles completos del filtro SDF
- `/api/v1/downlink_pdr_map` - PDRs de enlace descendente IPv4 (información básica)
- `/api/v1/downlink_pdr_map/full` - PDRs de enlace descendente IPv4 con detalles completos del filtro SDF
- `/api/v1/downlink_pdr_map_ip6` - PDRs de enlace descendente IPv6 (información básica)
- `/api/v1/downlink_pdr_map_ip6/full` - PDRs de enlace descendente IPv6 con detalles completos del filtro SDF
- `/api/v1/far_map` - Reglas de Acción de Reenvío
- `/api/v1/qer_map` - Reglas de Aplicación de QoS
- `/api/v1/urr_map` - Reglas de Reporte de Uso

Endpoints de Gestión de Búfer:

- `GET /api/v1/buffer` - Listar todos los búferes FAR con estadísticas
- `GET /api/v1/buffer/:far_id` - Obtener estado del búfer para FAR específico
- `GET /api/v1/buffer/notifications` - Listar estado de notificación DLDR
- `DELETE /api/v1/buffer` - Limpiar todos los paquetes almacenados en búfer
- `DELETE /api/v1/buffer/:far_id` - Limpiar búfer para FAR específico
- `POST /api/v1/buffer/:far_id/flush` - Vaciar (repetir) paquetes almacenados en búfer
- `POST /api/v1/buffer/:far_id/notify` - Enviar manualmente notificación DLDR

Endpoints de Configuración:

- `GET /api/v1/config` - Obtener configuración actual de UPF
- `POST /api/v1/config` - Actualizar configuración de UPF (campos editables en tiempo de ejecución)
- `GET /api/v1/dataplane_config` - Obtener configuración específica de dataplane

Endpoints de Integración de Enrutamiento:

- `GET /api/v1/routes` - Listar rutas de UE
- `POST /api/v1/routes/sync` - Activar sincronización de rutas con FRR
- `GET /api/v1/routing/sessions` - Obtener sesiones de protocolo de enrutamiento
- `GET /api/v1/ospf/database/external` - Obtener base de datos externa LSA de OSPF

Mejores Prácticas:

- Usar `page_size=100` para visualización en la Interfaz Web
- Usar `page_size=1000` para exportaciones masivas (límite máximo)
- Consultar `pagination.total_pages` para determinar el conteo de iteraciones
- Aumentar `page_size` para un mejor rendimiento de la API (menos solicitudes)

Soporte CORS

El intercambio de recursos de origen cruzado (CORS) está habilitado por defecto para todos los endpoints de la API, permitiendo que la Interfaz Web y aplicaciones de terceros consuman la API desde diferentes orígenes.

Métricas de Prometheus

Además de la API REST, OmniUPF expone métricas de Prometheus en el endpoint `/metrics` (puerto por defecto `:9090`).

Las métricas proporcionan:

- Contadores de mensajes PFCP y latencia por par
- Estadísticas de paquetes por tipo de protocolo
- Veredictos de acción de XDP
- Estadísticas de búfer
- Utilización de capacidad del mapa eBPF

- Seguimiento de volumen de URR

Consulta la Referencia de Métricas para la documentación completa.

Documentación Relacionada

- **Guía de la Interfaz Web** - Panel interactivo construido sobre esta API
- **Referencia de Métricas** - Documentación de métricas de Prometheus
- **Códigos de Causa PFCP** - Códigos de error PFCP y solución de problemas
- **Guía de Gestión de Reglas** - Configuración de PDR, FAR, QER, URR
- **Guía de Gestión de Rutas** - Integración FRR y enrutamiento de UE
- **Guía de Monitoreo** - Monitoreo de estadísticas y planificación de capacidad
- **Guía de Configuración** - Opciones de configuración de UPF
- **Swagger UI** - Documentación interactiva de la API (reemplaza `localhost` con tu host de UPF)

Gestión de Rutas UE

> **Documentación Relacionada**:
>
> - Documentación de la API - Referencia completa de la API incluyendo puntos finales de gestión de rutas
> - Guía de Operaciones - Operaciones y monitoreo de la interfaz web

Visión General

El UPF (Función de Plano de Usuario) se integra con **FRR (Free Range Routing)** para gestionar dinámicamente las rutas IP del Equipo de Usuario (UE). Esta integración asegura que, a medida que se establecen o terminan sesiones de UE, la infraestructura de enrutamiento se adapte automáticamente para reflejar la topología actual de la red.

¿Qué es FRR?

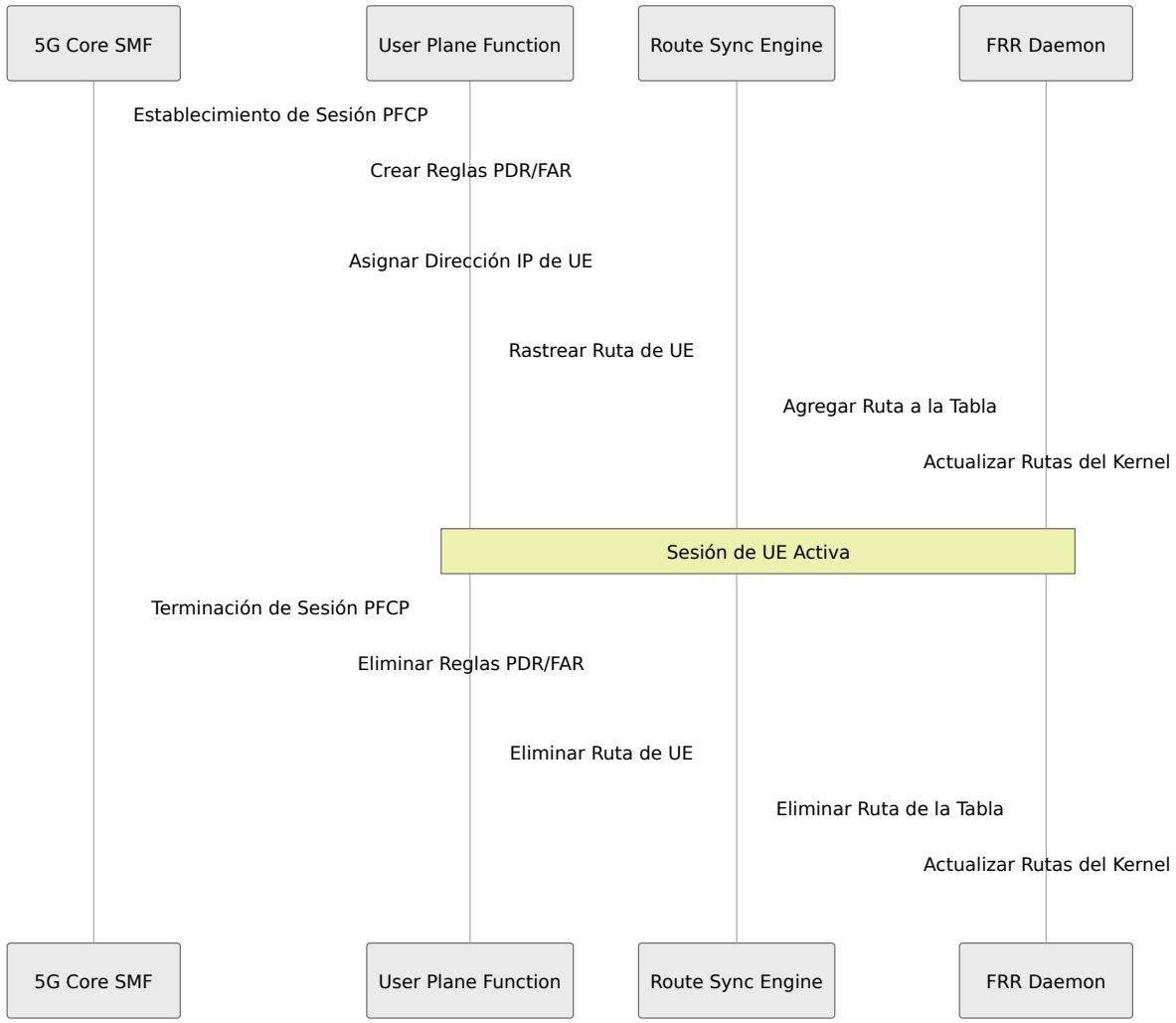
FRR (Free Range Routing) es un robusto conjunto de protocolos de enrutamiento de código abierto para plataformas Linux y Unix. Implementa varios protocolos de enrutamiento, incluyendo BGP, OSPF, RIP, y otros. En nuestra implementación, FRR actúa como el demonio de enrutamiento que mantiene la tabla de enrutamiento del kernel y puede redistribuir rutas a otros elementos de la red.

Arquitectura



Cómo Funciona la Sincronización de Rutas

Ciclo de Vida de la Ruta



Sincronización Automática

El UPF mantiene un registro interno de todas las direcciones IP de UE activas. Cuando está habilitado, el sistema de sincronización de rutas:

1. **Monitorea Sesiones de UE**: Rastrea todas las sesiones PFCP activas y sus direcciones IP de UE asociadas
2. **Mantiene Lista de Rutas**: Mantiene una lista actualizada de rutas que deben estar en la tabla de enrutamiento

3. **Sincroniza con FRR**: Envía automáticamente actualizaciones de rutas al demonio FRR a través de su API
4. **Maneja Fallos**: Rastrea el estado de sincronización (sincronizado/fallido) para cada ruta y reintenta según sea necesario

Configuración de FRR

Configuración

FRR se despliega y configura utilizando **plantillas de Ansible** para establecer los parámetros básicos de enrutamiento. Definas la configuración de FRR una vez como una **plantilla Jinja2** en tu libro de jugadas de Ansible, y Ansible la propaga automáticamente a todas tus instancias de UPF durante el despliegue.

Una plantilla típica de configuración Jinja2 para FRR incluye:

```
frr version 7.2.1
frr defaults traditional
hostname pgw02
log syslog informational
service integrated-vtysh-config
!
ip route {{ hostvars[inventory_hostname]['ansible_default_ipv4']
['gateway'] }}/32 {{ ansible_default_ipv4['interface'] }}
!
interface {{ ansible_default_ipv4['interface'] }}
 ip address ospf router-id {{hostvars[inventory_hostname]
['ansible_host']}}
 ip ospf authentication null
!
router ospf
 ospf router-id {{hostvars[inventory_hostname]['ansible_host']}}
 redistribute static
 network {{ hostvars[inventory_hostname]['ansible_default_ipv4']
['network'] }}/{{ mask_cidr }} area 0
 area 0 authentication message-digest
!
line vty
!
end
```

Modelo de Despliegue:

1. **Definir Una Vez**: Crea la plantilla Jinja2 de FRR en tu rol de Ansible (por ejemplo, `roles/frr/templates/frr.conf.j2`)
2. **Configurar Parámetros**: Establece variables en tu inventario de Ansible para cada host de UPF
3. **Desplegar en Todas Partes**: Ejecuta el libro de jugadas de Ansible para desplegar la configuración de FRR a todos los nodos de UPF
4. **Personalización Automática**: Ansible utiliza variables específicas del host (direcciones IP, IDs de router, etc.) para personalizar la configuración de FRR de cada UPF

Parámetros Personalizables en la plantilla Jinja2:

- **Parámetros OSPF**: ID de router, configuración de área, métodos de autenticación, anuncios de red
- **Configuración BGP**: ASN, relaciones de vecinos, políticas de ruta, comunidades
- **Redistribución de Rutas**: Qué rutas redistribuir (por ejemplo, `redistribute static` para rutas de UE)
- **Filtrado de Rutas**: Mapas de ruta, listas de prefijos, listas de acceso
- **Configuraciones de Interfaz**: Parámetros de interfaz OSPF/BGP

Integración UPF: Una vez que la configuración base de FRR se despliega en cada instancia de UPF, el UPF agrega dinámicamente direcciones IP de UE como **rutas de host** (/32 para IPv4, /128 para IPv6) a través de la interfaz vtysh de FRR basada en sesiones PFCP activas. Estas rutas son luego:

1. **Agregadas como rutas estáticas de FRR** por el motor de sincronización de rutas de UPF (a través de vtysh)
2. **Recogidas por FRR** a través de la directiva `redistribute static`
3. **Anunciadas a protocolos de enrutamiento** (OSPF, BGP) de acuerdo con tu configuración de FRR
4. **Propagadas a la red** para que el tráfico de UE pueda ser enrutado a esta instancia de UPF

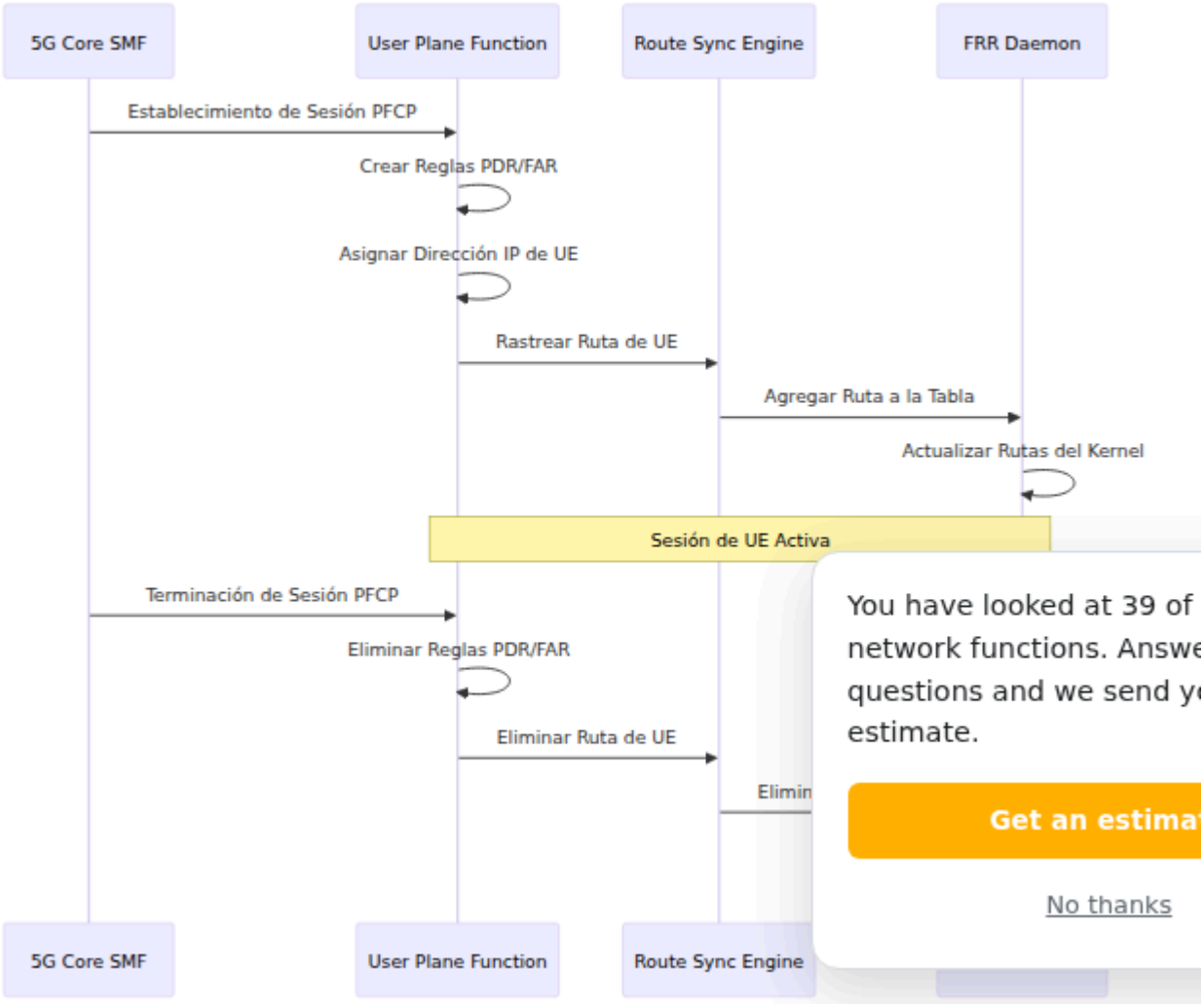
> **Importante**: El UPF agrega rutas a través de la interfaz vtysh de FRR, convirtiéndolas en rutas estáticas de FRR (no rutas del kernel). Debes usar `redistribute static` en tu configuración de OSPF/BGP, no `redistribute kernel`.

Puntos Clave:

- **Definir Una Vez, Desplegar en Todas Partes**: Define la plantilla Jinja2 de FRR una vez en Ansible, y se despliega automáticamente a todas las instancias de UPF
- **Ansible maneja la configuración estática**: La plantilla Jinja2 configura todos los parámetros de los protocolos de enrutamiento (áreas OSPF, vecinos BGP, autenticación, políticas de ruta, etc.)
- **UPF maneja rutas dinámicas**: Cada instancia de UPF gestiona dinámicamente solo las rutas IP de UE /32 basadas en sus sesiones PFCP activas

- **Anuncio automático de rutas**: FRR en cada UPF redistribuye automáticamente las rutas locales de UE de acuerdo con tus políticas configuradas
- **Gestión centralizada**: Actualiza la plantilla de Ansible y vuelve a ejecutar el libro de jugadas para cambiar la configuración de enrutamiento en todos los UPFs simultáneamente

Anuncio de Rutas



Monitoreo y Gestión

Integración de la Interfaz Web

El Panel de Control de UPF proporciona una página de **Rutas** que muestra:

- **Estado de Ruta**: Si la sincronización de rutas está habilitada o deshabilitada
- **Total de Rutas**: Número de direcciones IP de UE que se están rastreando
- **Estadísticas de Sincronización**: Conteo de rutas sincronizadas con éxito y cualquier fallo
- **Rutas Activas**: Lista en tiempo real de todas las direcciones IP de UE actualmente en la tabla de enrutamiento
- **Vecinos OSPF**: Estado en vivo de las adyacencias OSPF con detalles de vecinos
- **Vecinos BGP**: Estado de sesión BGP y estadísticas de prefijos (cuando están configurados)
- **Rutas Redistribuidas OSPF**: Vista completa de LSAs externas que muestran cómo se anuncian las rutas de UE

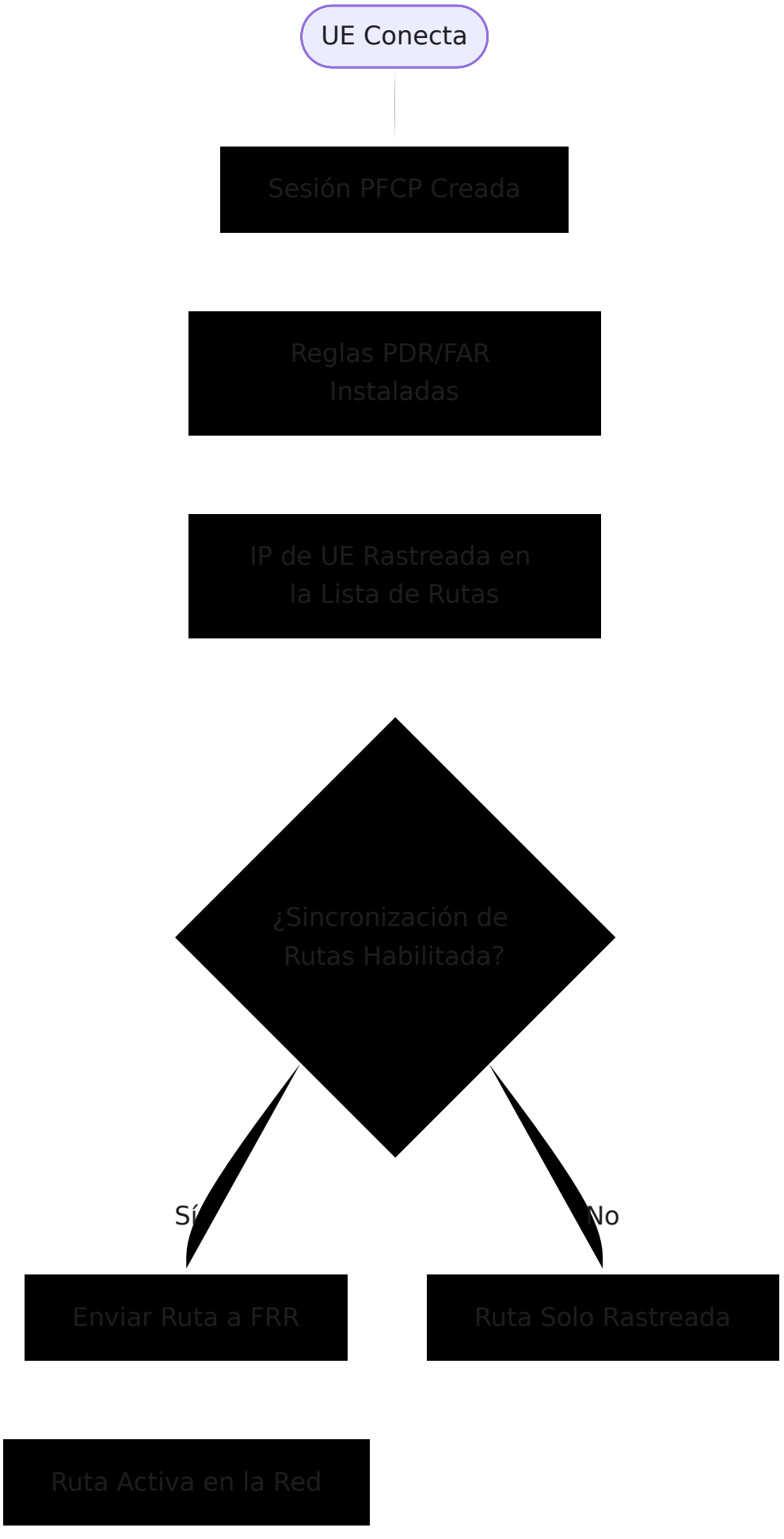
La página de Rutas proporciona una visibilidad completa sobre la sincronización de rutas de UE, vecinos de protocolos de enrutamiento y anuncios de rutas redistribuidas.

Operación de Sincronización Manual

Los administradores pueden activar una sincronización manual de rutas a través de la interfaz web utilizando el botón **Sincronizar Rutas**. Esta operación:

1. Vuelve a leer la lista actual de sesiones de UE activas desde el UPF
2. Compara con la tabla de enrutamiento de FRR
3. Agrega cualquier ruta faltante
4. Elimina cualquier ruta obsoleta
5. Devuelve estadísticas de sincronización actualizadas

Flujo de Rutas


UE Conecta
Sesión PFCP Creada
Reglas PDR/FAR Instaladas
IP de UE Rastreada en la Lista de Rutas
¿Sincronización de Rutas Habilitada?
Sí
No
Enviar Ruta a FRR
Ruta Solo Rastreada
Ruta Activa en la Red



Beneficios

- **Provisionamiento Sin Toque**: Las rutas se gestionan automáticamente sin intervención manual
- **Adaptación Dinámica**: El enrutamiento de la red se adapta en tiempo real a la movilidad de UE y cambios en las sesiones
- **Escalabilidad**: Soporta miles de rutas de UE concurrentes
- **Resiliencia**: Las operaciones de sincronización fallidas se rastrean y pueden reintentarse
- **Visibilidad**: Visibilidad completa del estado de las rutas a través de la interfaz web

Detalles Técnicos

Puntos Finales de la API

El UPF expone los siguientes puntos finales de gestión de rutas:

- `GET /api/v1/routes` - Listar todas las rutas de UE rastreadas sin sincronización
- `POST /api/v1/routes/sync` - Sincronizar rutas con FRR y devolver lista actualizada
- `GET /api/v1/route_stats` - Obtener estadísticas detalladas de enrutamiento
- `GET /api/v1/routing/sessions` - Obtener sesiones de protocolo de enrutamiento (vecinos OSPF, pares BGP)
- `GET /api/v1/ospf/database/external` - Obtener base de datos LSA externa OSPF (rutas redistribuidas)

> **Ver También**: Documentación de la API - Gestión de Rutas para detalles completos de los puntos finales y ejemplos

Formato de Ruta

Las rutas se almacenan y gestionan como simples direcciones IP (por ejemplo, `100.64.18.5`). El demonio de enrutamiento maneja todos los detalles de la entrada de ruta, incluyendo:

- Prefijo/máscara de destino
- Puerta de enlace/siguiente salto
- Vinculación de interfaz
- Métrica y distancia administrativa

Soporte IPv6

El gestor de rutas soporta direcciones de UE tanto IPv4 como IPv6:

Tipo de Dirección	Longitud de Prefijo	Ejemplo
IPv4	/32	`100.64.18.5/32`
IPv6	/128	`2001:db8::1/128`

Para IPv6, asegúrate de que tu configuración de FRR incluya la redistribución OSPFv3 o BGP IPv6 apropiada:

```
router ospf6
 redistribute static
```

o para BGP:

```
router bgp <asn>
 address-family ipv6 unicast
  redistribute static
```

Verificación de FRR

Base de Datos LSA Externa OSPF

Puedes verificar que las rutas de UE se están redistribuyendo correctamente en OSPF examinando la Base de Datos de Estado de Enlace OSPF de FRR. Las LSAs

externas (Tipo 5) muestran rutas que han sido inyectadas en OSPF desde fuentes externas.

Base de datos OSPF de FRR mostrando LSAs externas incluyendo la ruta de UE 100.64.18.5/32 siendo anunciada como una ruta E2 (Tipo Externo 2).

En el ejemplo anterior, puedes ver:

- **LSA de Red (10.98.0.20)**: El anuncio de red propio del UPF
- **LSA de Router (192.168.1.1)**: Anuncio de router OSPF
- **LSAs Externas**: Incluyendo la ruta de UE `100.64.18.5` redistribuida en OSPF con tipo de métrica E2 (Tipo Externo 2)

Esta verificación confirma que:

1. El UPF está rastreando correctamente la dirección IP de UE
2. El motor de sincronización de rutas ha enviado la ruta a FRR
3. FRR ha redistribuido la ruta en OSPF
4. Los vecinos OSPF están recibiendo los anuncios de ruta