

Redes Móviles Dual Stack

Ing. Gonzalo Escuder Bell



Agenda

- Arquitectura de una red móvil 2G/3G/LTE
 - Nodos, interfaces, protocolos, funciones, estándares y servicios
- Conectividad a Internet Dual Stack (IPv4/IPv6)
 - Drivers
 - Requerimientos (red, sistemas, terminal)
 - Funcionamiento y trazados de red
 - Conclusiones

Agenda

- Arquitectura de una red móvil 2G/3G/LTE
 - Nodos, interfaces, protocolos, funciones, estándares y servicios
- Conectividad a Internet Dual Stack (IPv4/IPv6)
 - Drivers
 - Requerimientos (red, sistemas, terminal)
 - Funcionamiento y trazados de red
 - Conclusiones

Servicios de una red móvil “tradicional”

- El operador es responsable de la cadena completa del servicio: homologación del terminal, gestión de SIM-cards, red de acceso y núcleo e infraestructura de los servicios:
 - Voz y SMS
 - Servicios sobre redes de paquetes (wap, MMS, redes privadas e Internet)
 - Servicios de valor agregado

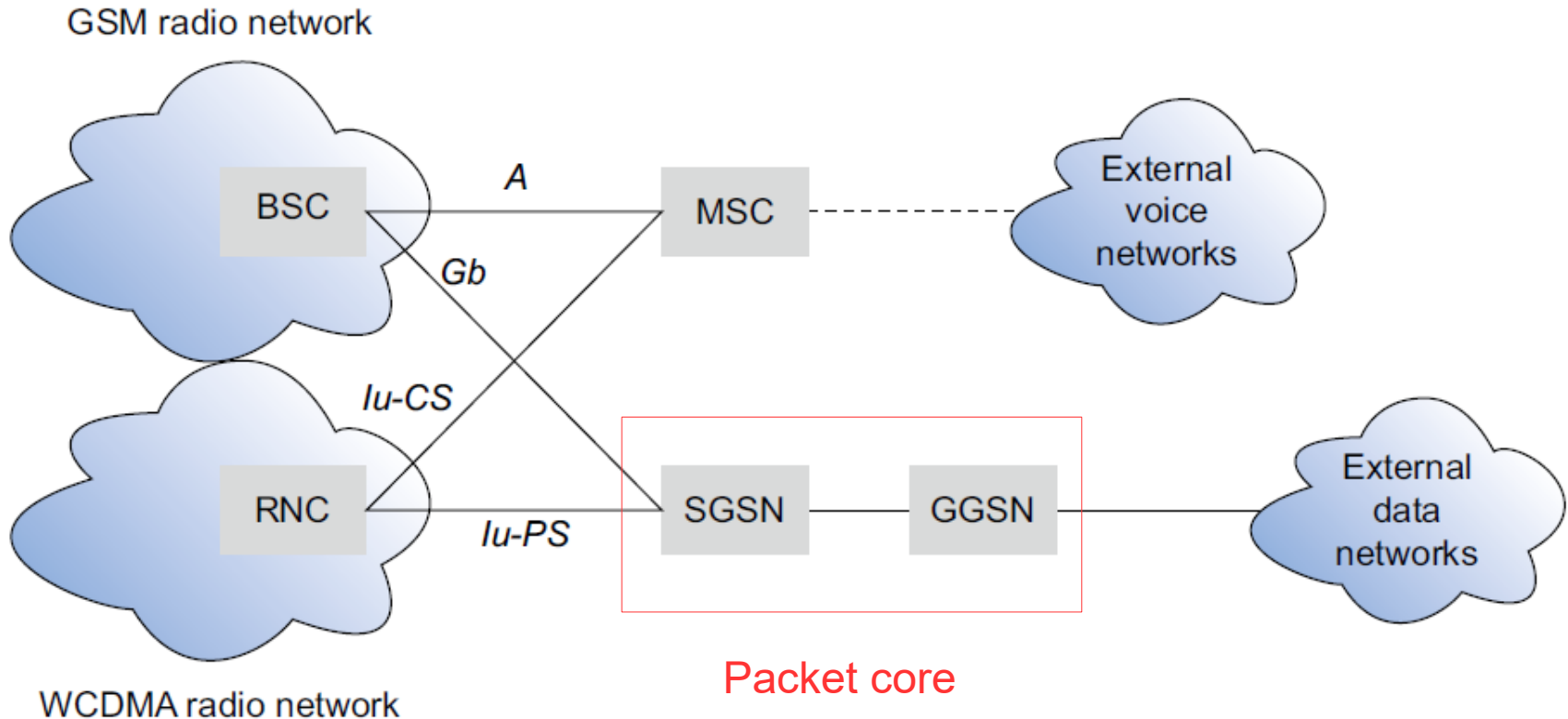
Servicios de una red móvil “actual”

- Los servicios “tradicionales” migran paulatinamente a una infraestructura sobre IP (LTE es todo sobre IP -ej: VoLTE) donde el servicio percibido por el cliente como más importante es el de conectividad a Internet.
- Sobre la conectividad a Internet se construyen nuevos servicios agnósticos al operador y orientados a una conectividad masiva (ej: servicios de mensajería, IoT, etc.)

Estándares de las redes móviles

- La arquitectura de una red GSM está especificada en la norma 3GPP TS 03.02 (originalmente ETSI)
- El backbone GPRS surge como la generación 2.5G extendiendo la red de paquetes hasta el terminal móvil, evitando así el tránsito por la red de circuitos (CS core)
- El packet core se especifica en el estándar 3GPP TS 23.060
- El mecanismo de encapsulamiento de los datos en el packet core (GTP) se especifica en la norma 3GPP TS 29.060
- La evolución del packet core para acceso eUTRAN (LTE) se especifica en el estándar 3GPP TS 23.401
- Los mecanismos de migración IPv6 para las redes móviles se especifican en la norma 3GPP TS 23.975

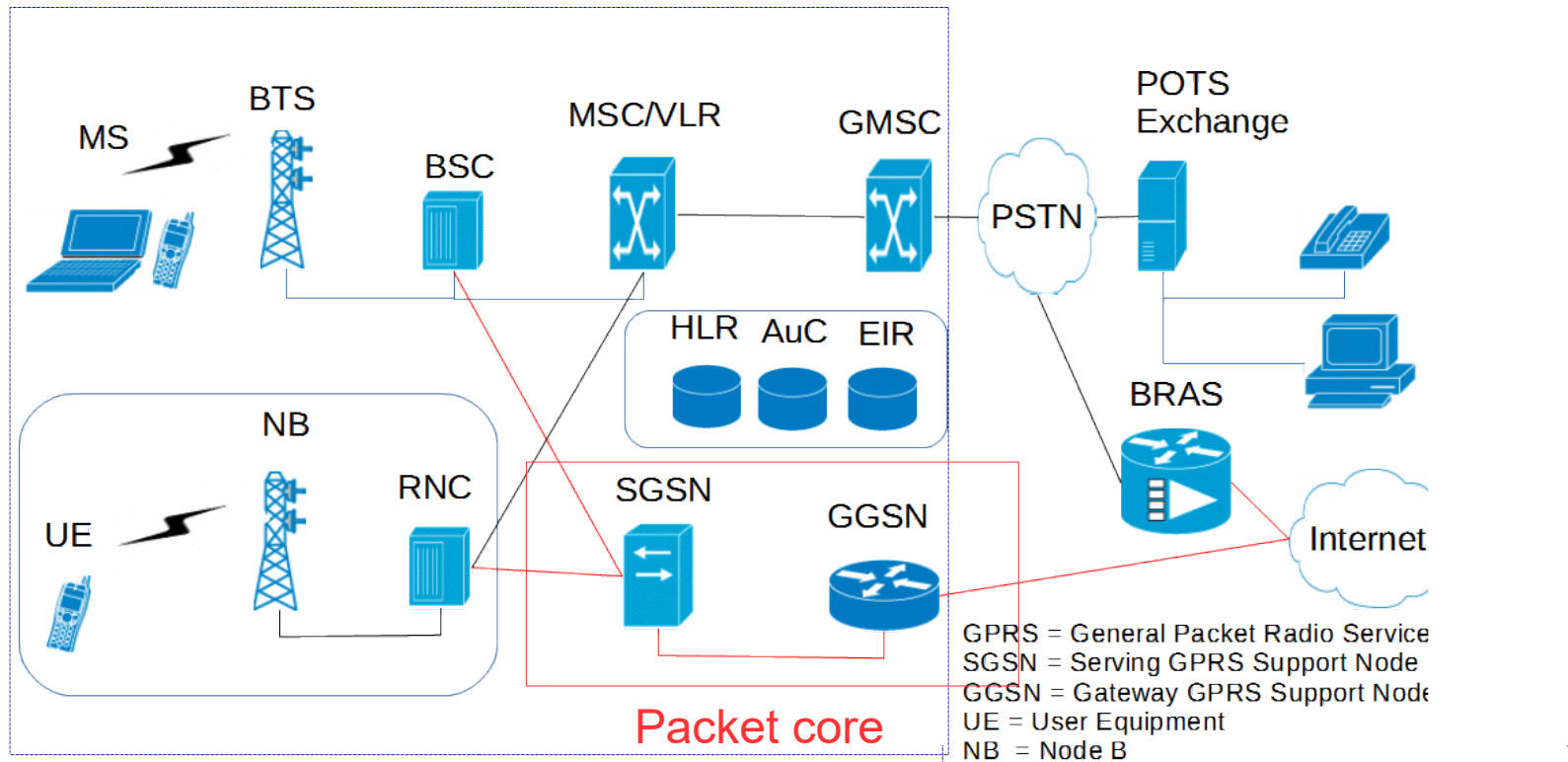
Arquitectura de una red móvil 2G/3G



Infraestructura del servicio móvil

- Red de acceso: se encarga de la conectividad y control de movilidad de los terminales para todas las tecnologías (GSM, UMTS, LTE) y los diferentes tipos servicios (voz y datos).
- Red de núcleo: tiene los datos de los servicios del cliente, realiza la autenticación del cliente, cifrado de comunicaciones, encaminamiento de llamadas y datos, interconexión con otros operadores telefónicos, conectividad a Internet, roaming, generación de CDRs, interconexión con billing e interceptación legal.

Arquitectura de una red móvil 2G/3G



BTS = Base Transceiver Station
 BSC = Base Station Controller
 MSC = Mobile Switching Center
 GMSC = Gateway MSC
 VLR = Visitor Location Register
 HLR = Home Locator Register
 AuC = Authentication Center
 EIR = Equipment Identity Register
 PSTN = Public Switched Telephony Network
 POTS = Plain Old Telephony System

Funcionalidades de los nodos 2G/3G/LTE

- BTS, nB, eNB: acceso de radio
- BSC, RNC: control de radiobases 2G/3G y handover
- MSC/VLR: encaminamiento de llamadas CS, tasación, registro de los abonados en una determinada zona
- HLR: base de datos de servicios de telecomunicaciones del abonado 2G/3G
- HSS: base de datos de servicios del abonado (LTE)
- AuC: base de datos de autenticación
- EIR: base de datos de terminales permitidos/prohibidos

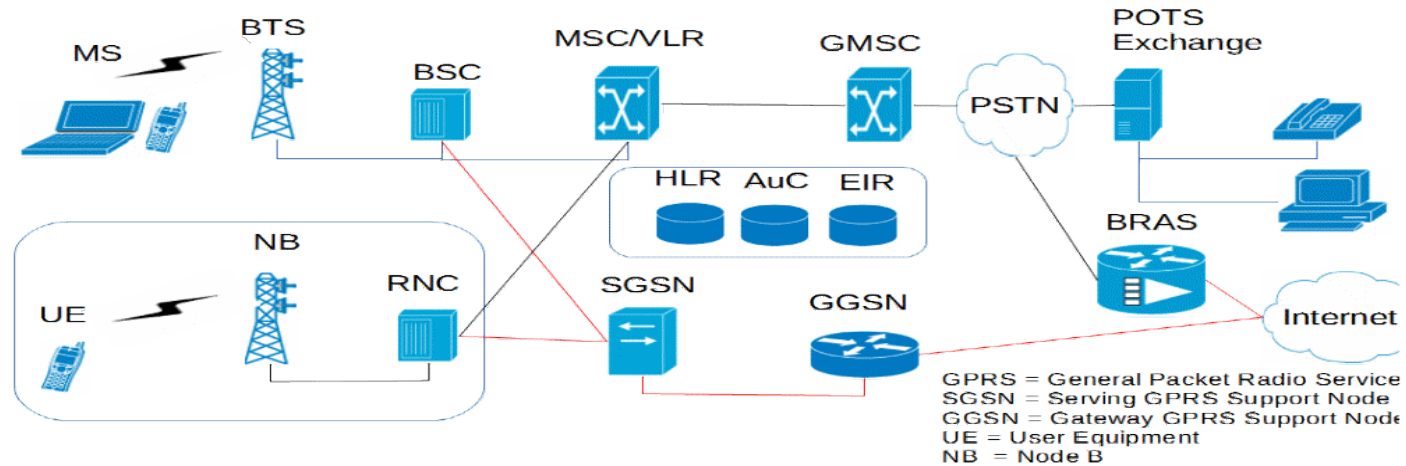
Funcionalidades de los nodos 2G/3G/LTE

- MME, SGSN: registro y control del abonado (consulta a HLR/HSS)
- S-GW/P-GW/GGSN: gateway de interconexión a las PDN
- OCS: online charging
- PCRF: policy and charging rules function
- LIG: lawful interception gateway

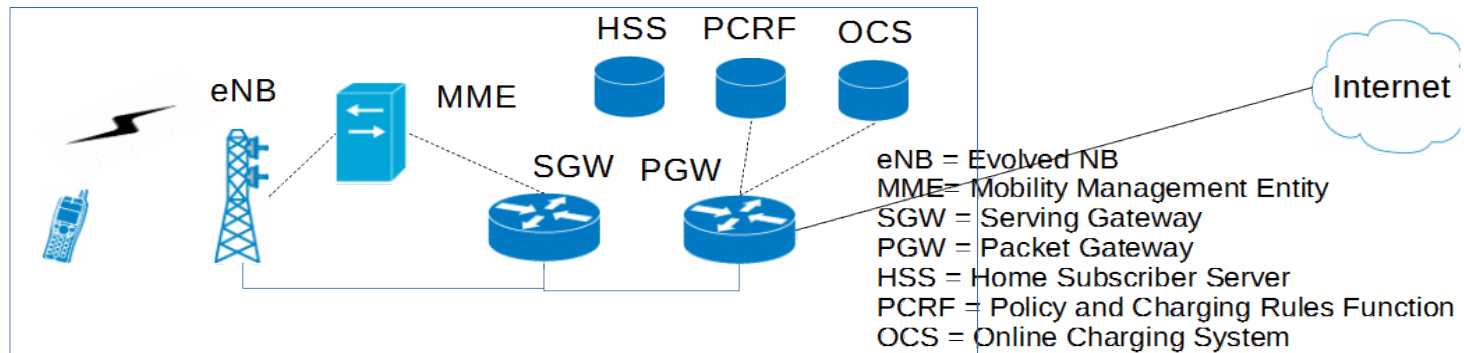
Algunos identificadores en una red móvil

- MSISDN (Mobile Station ISDN): es el “número” en una red pública telefónica
- IMSI (International Mobile Subscriber Identity): es la “identidad” del suscriptor en una red móvil
- IMEI (International Mobile Equipment Identity): es el identificador del terminal
- **APN (Access Point Name):** Es una “etiqueta” mediante la cual se identifica y selecciona un determinado servicio de datos móviles en un operador (ej: en la red de circuitos se realiza mediante un número telefónico enrutado en la PSTN/PLMN hasta un RAS de conectividad -normalmente Internet). En la red móvil define la infraestructura del servicio (topología y tasación).

Arquitectura de una red móvil 2G/3G/LTE



4ta Generación - LTE



Arquitectura de una red móvil 2G/3G/LTE (packet core)

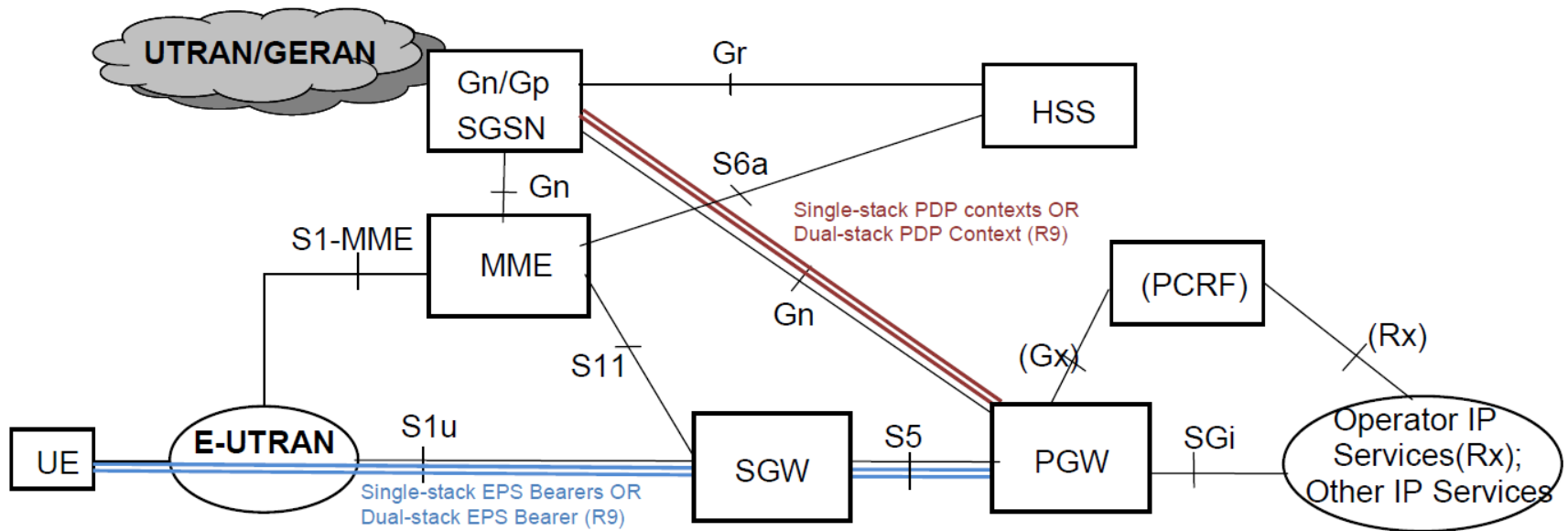
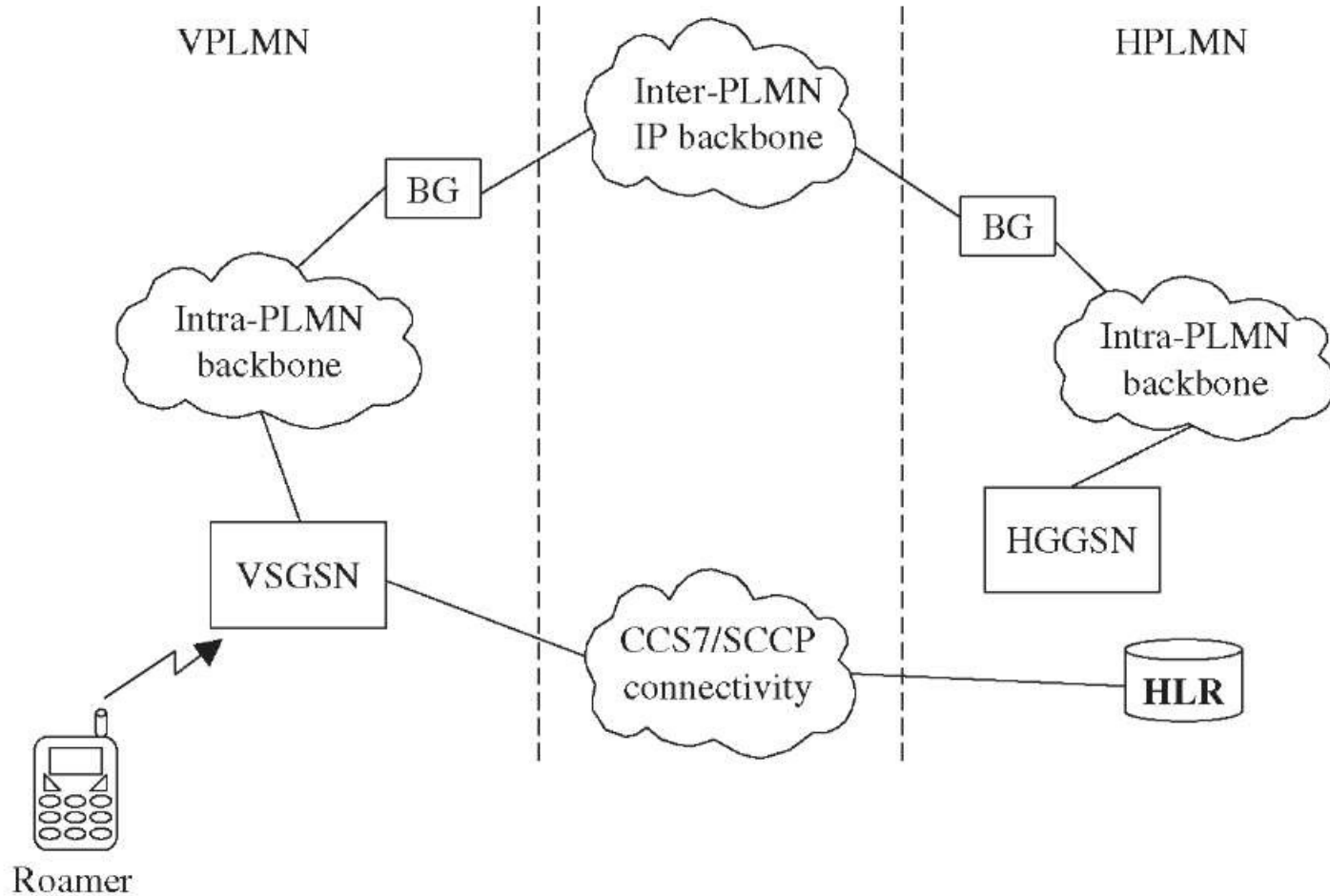


Figure 4.2: EPS Non-roaming Architecture for interoperation with Gn/Gp SGSNs in Rel-8

Fuente: 3GPP TS 23.975

Arquitectura de una red móvil (interconexión roaming)



Arquitectura de una red móvil 2G/3G/LTE (roaming de datos)

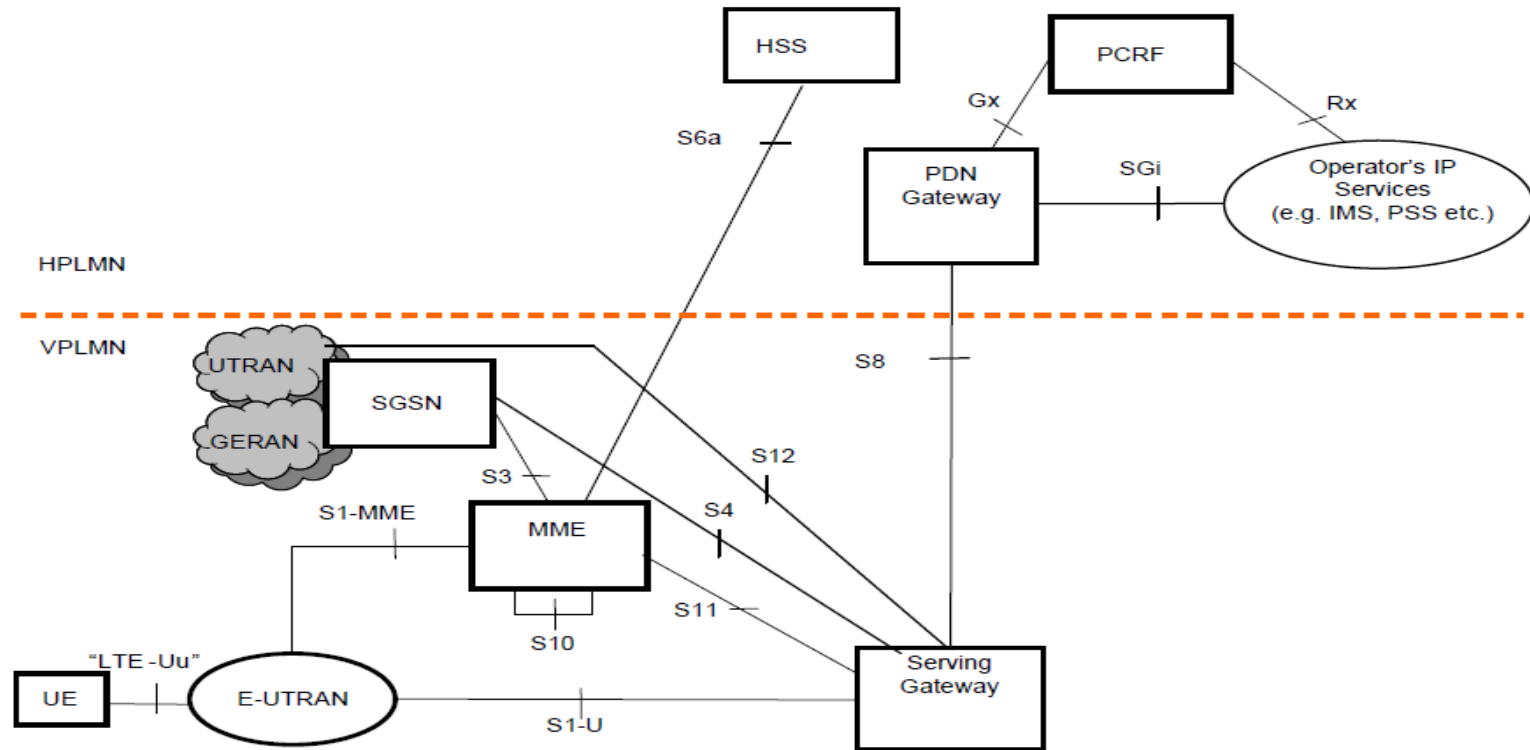
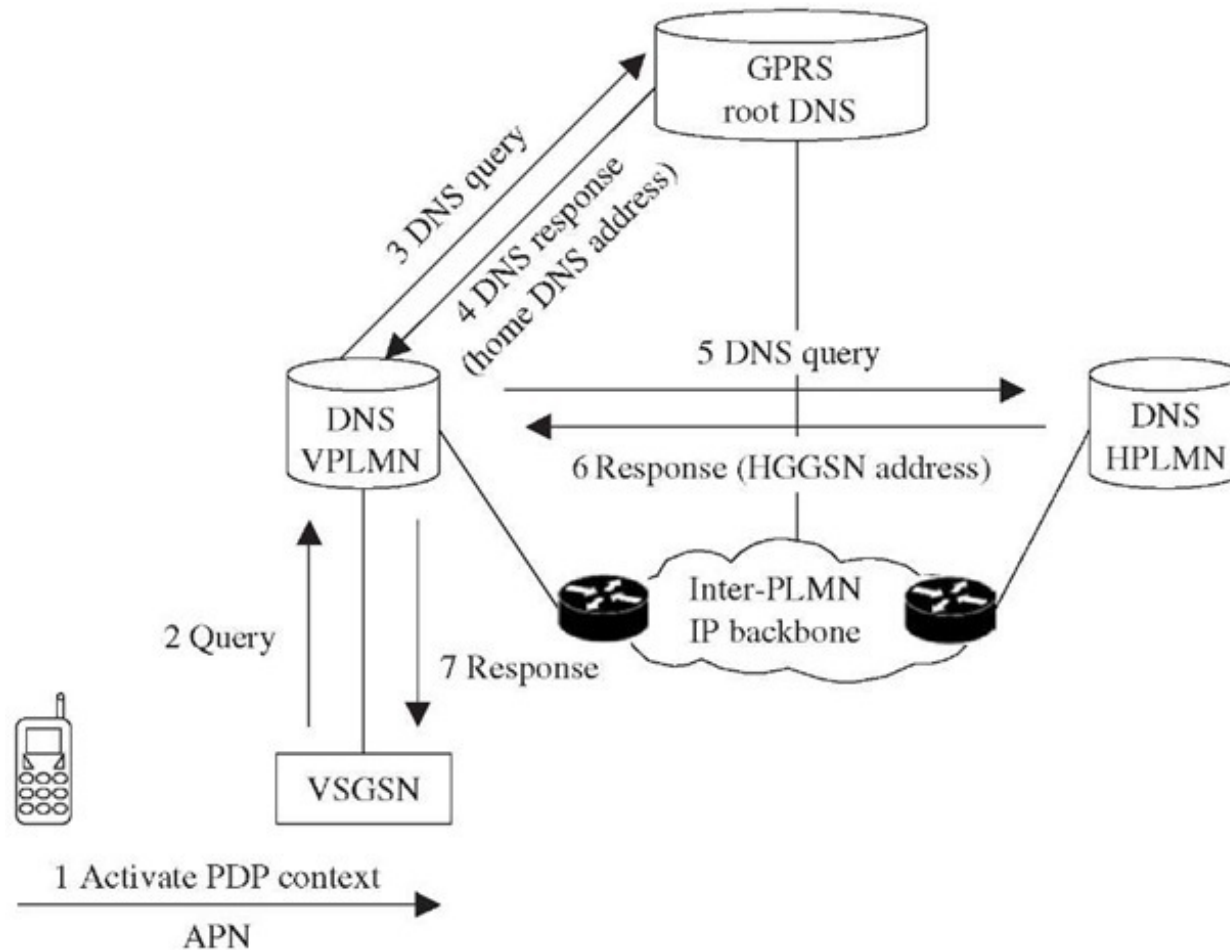
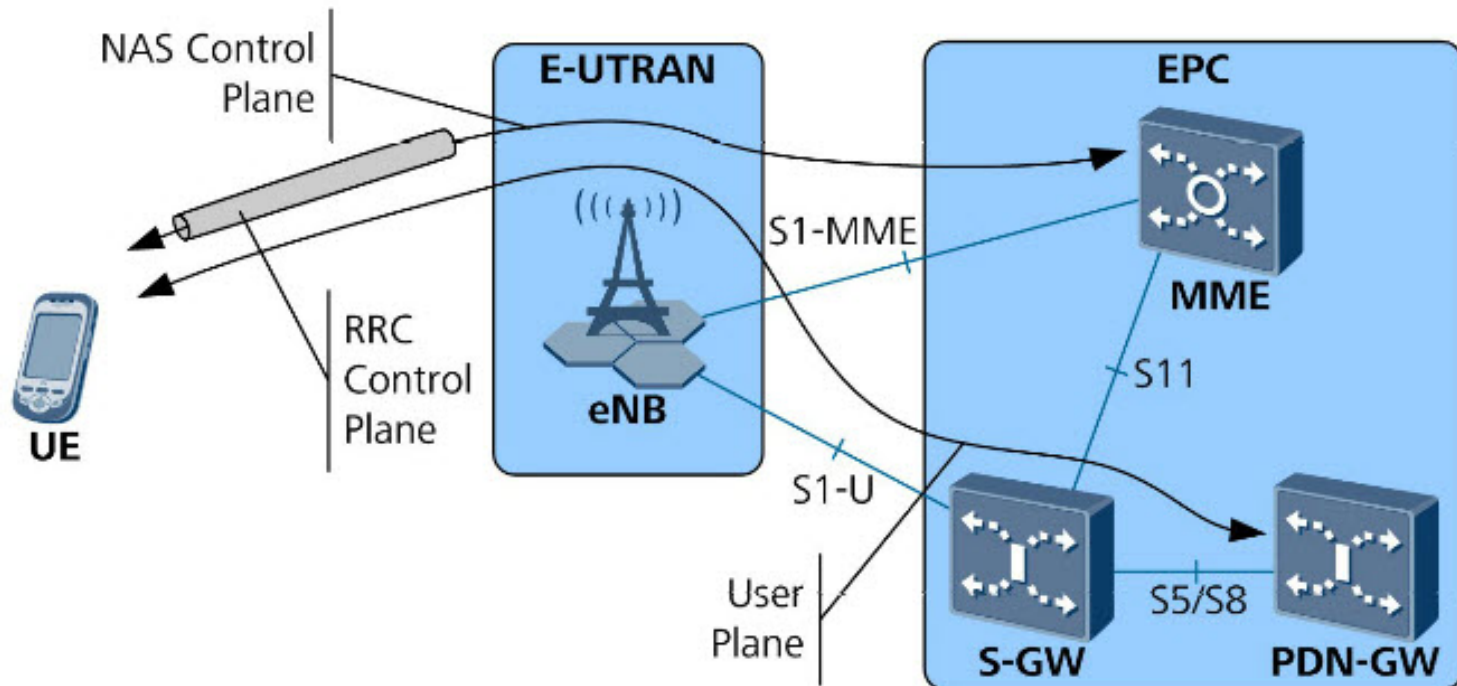


Figure 4.2.2-1: Roaming architecture for 3GPP accesses. Home routed traffic

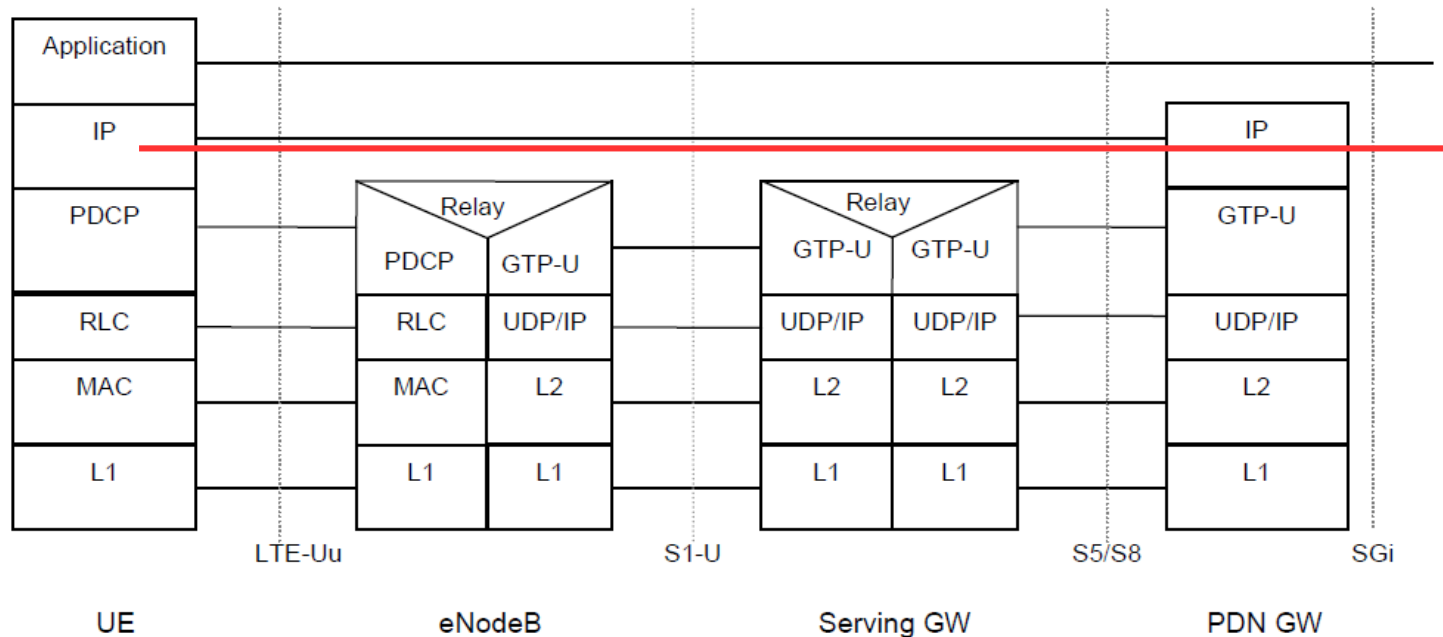
Activación de un servicio de datos en la red móvil: APN



Planos de usuario y control en LTE



Plano de usuario en LTE

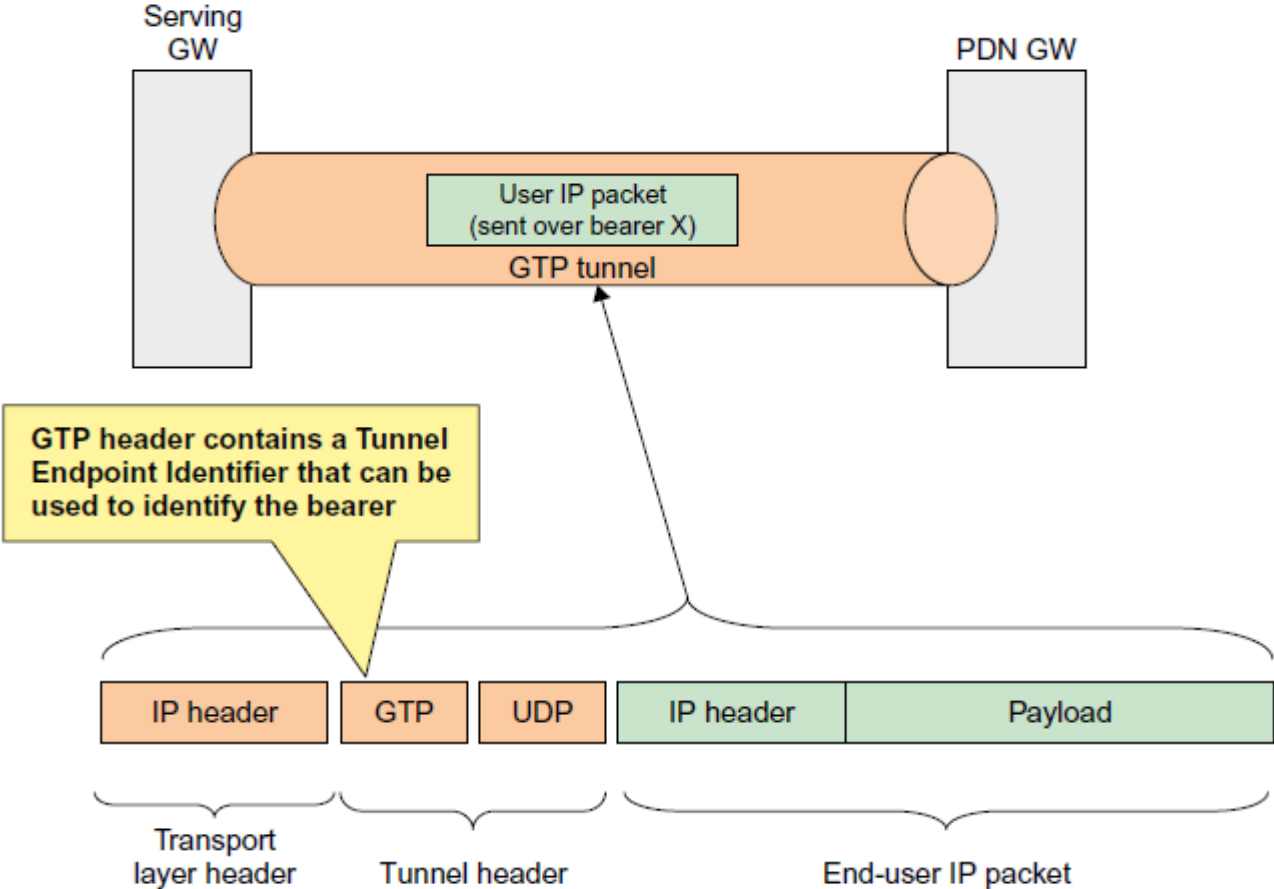


Legend:

- **GPRS Tunnelling Protocol for the user plane (GTP-U):** This protocol tunnels user data between eNodeB and the S-GW as well as between the S-GW and the P-GW in the backbone network. GTP shall encapsulate all end user IP packets.
- **MME** controls the user plane tunnel establishment and establishes User Plane Bearers between eNodeB and S-GW.
- **UDP/IP:** These are the backbone network protocols used for routing user data and control signalling.
- **LTE-Uu:** The radio protocols of E-UTRAN between the UE and the eNodeB are specified in TS 36.300 [5].

Figure 5.1.2.1-1: User Plane

GTP Tunnel



PDP context vs EPS bearer

- GERAN (2G) /UTRAN (3G) data session:
 - 1. procedimiento de Attach (alert SGSN)
 - 2. establecimiento de un Packet Data Protocol (PDP) Context
- eUTRAN (LTE) data session:
 - Se establece un EPS bearer
- Ambos utilizan:
 - APN
 - IP address type
 - QoS parameters

PDP context activation (Iu)

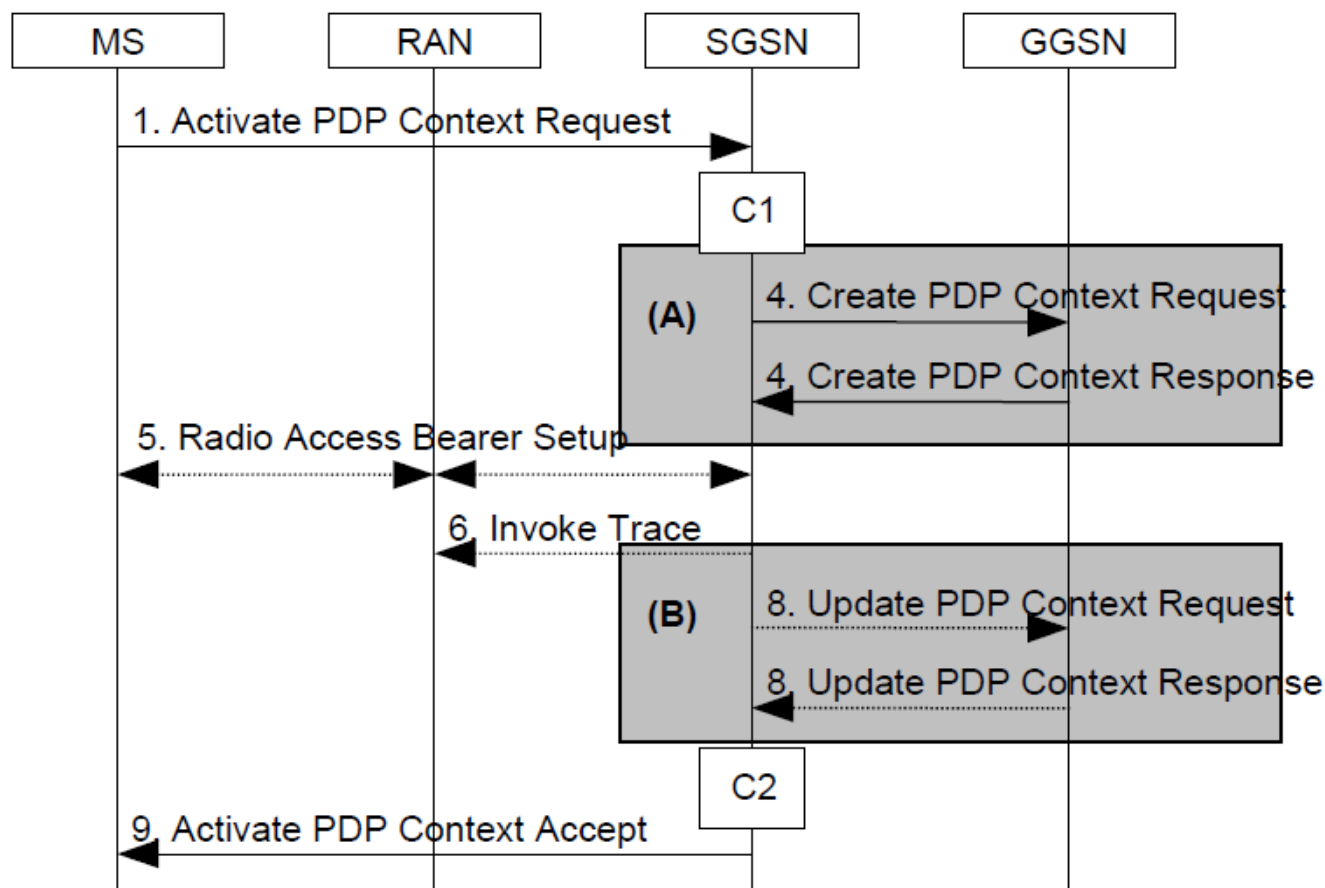
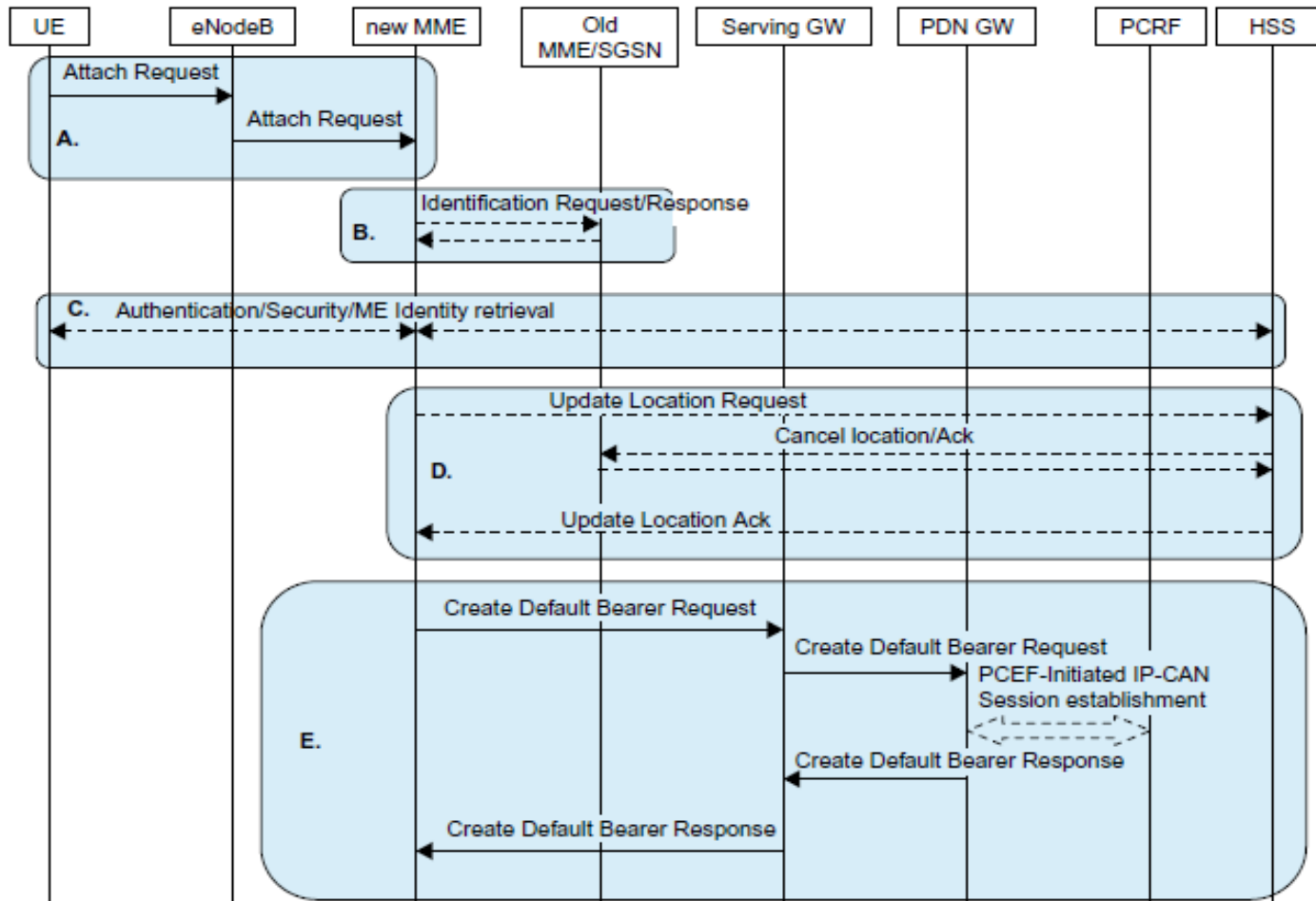
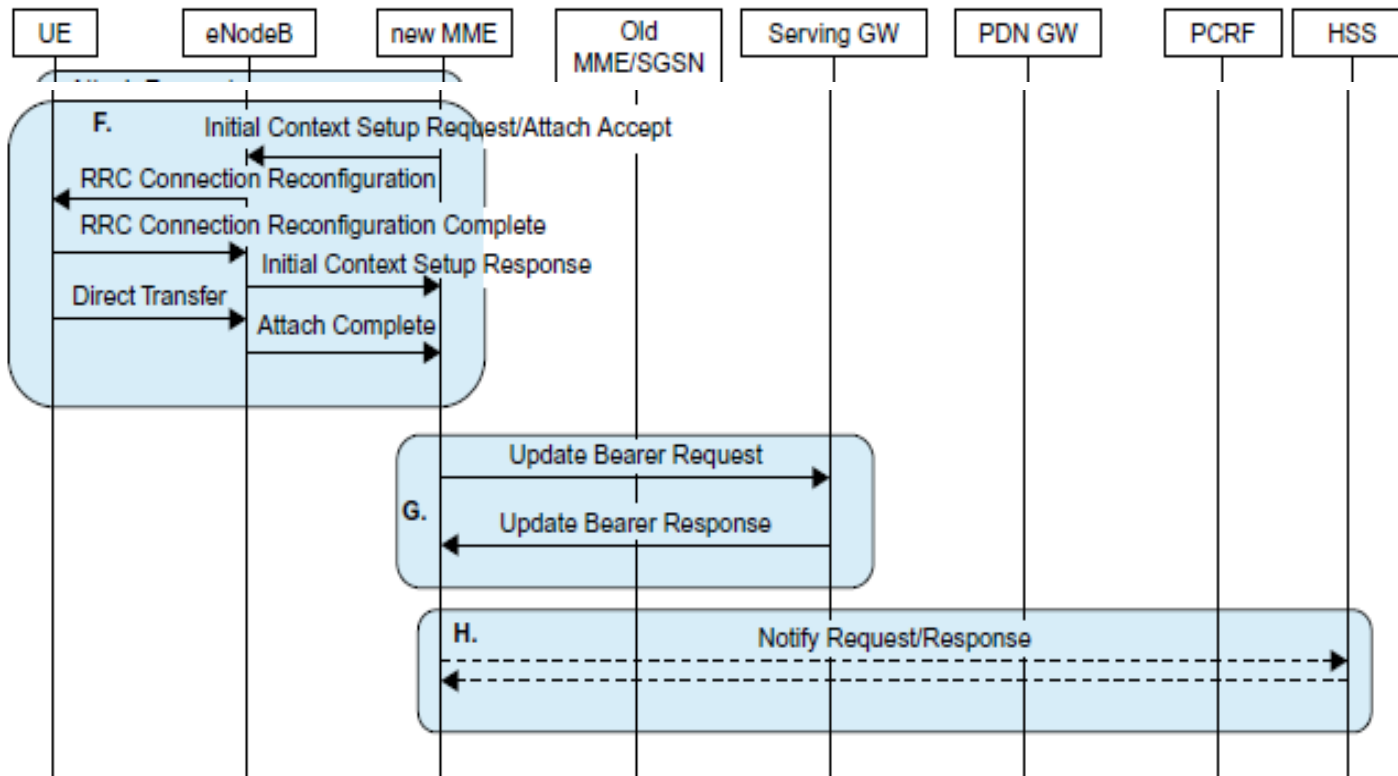


Figure 64: PDP Context Activation Procedure for Iu mode

eUTRAN initial attach



eUTRAN initial attach



Agenda

- Arquitectura de una red móvil 2G/3G/LTE
 - Nodos, interfaces, protocolos, funciones, estándares y servicios
- Conectividad a Internet Dual Stack (IPv4/IPv6)
 - Drivers
 - Requerimientos (red, sistemas, terminal)
 - Funcionamiento y trazados de red
 - Conclusiones

Drivers para dual-stack

- Mecanismo ideal de transición en una red en producción:
 - Sin impacto al servicio del cliente
 - Migración gradual del tráfico al protocolo IPv6
 - Prepara la red y sistemas para despliegue masivo IPv6
 - Previene futuras inversiones en CGN
- Es uno de los mecanismos estándar definidos en la norma 3GPP TS 23.975

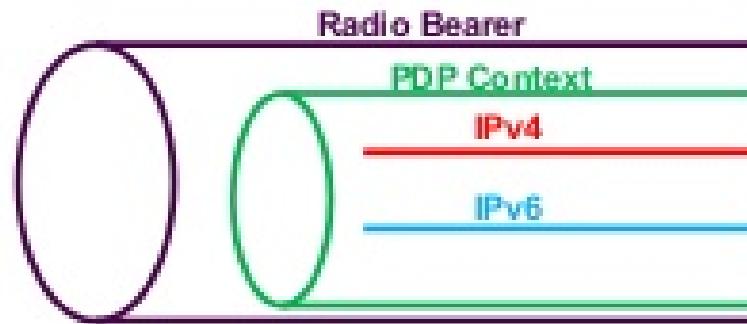
Requerimientos para el cliente

- El terminal debe soportar dual stack (apn type v4v6).
- El stack TCP/IP del sistema usado debe soportar dual-stack (ej: notebook con módem celular)
- OBS: si no se soporta, sigue usando la conectividad IPv4 “usual”

Requerimientos para la red

- Mecanismo ideal: EPS bearer dual-stack (soportado a partir de la 3GPP Rel.9)

✓ Dual Stack – 3GPP Release 9



Requerimientos para la red

- Soporte en:
 - HLR/HSS
 - MME/SGSN
 - GGSN/S-GW/P-GW/Firewall
 - PCRF
- Red de transporte (routers, DNSs, conectividad a Internet)

Requerimientos para la red

- OSS (contadores, MIBs, reportes, etc.)
- BSS (billing) y mediación (CDRs)
- Sistemas de gestión comercial
- Gestión de reclamos (capacitación interna)
- Lawful interception

Arquitectura dual-stack

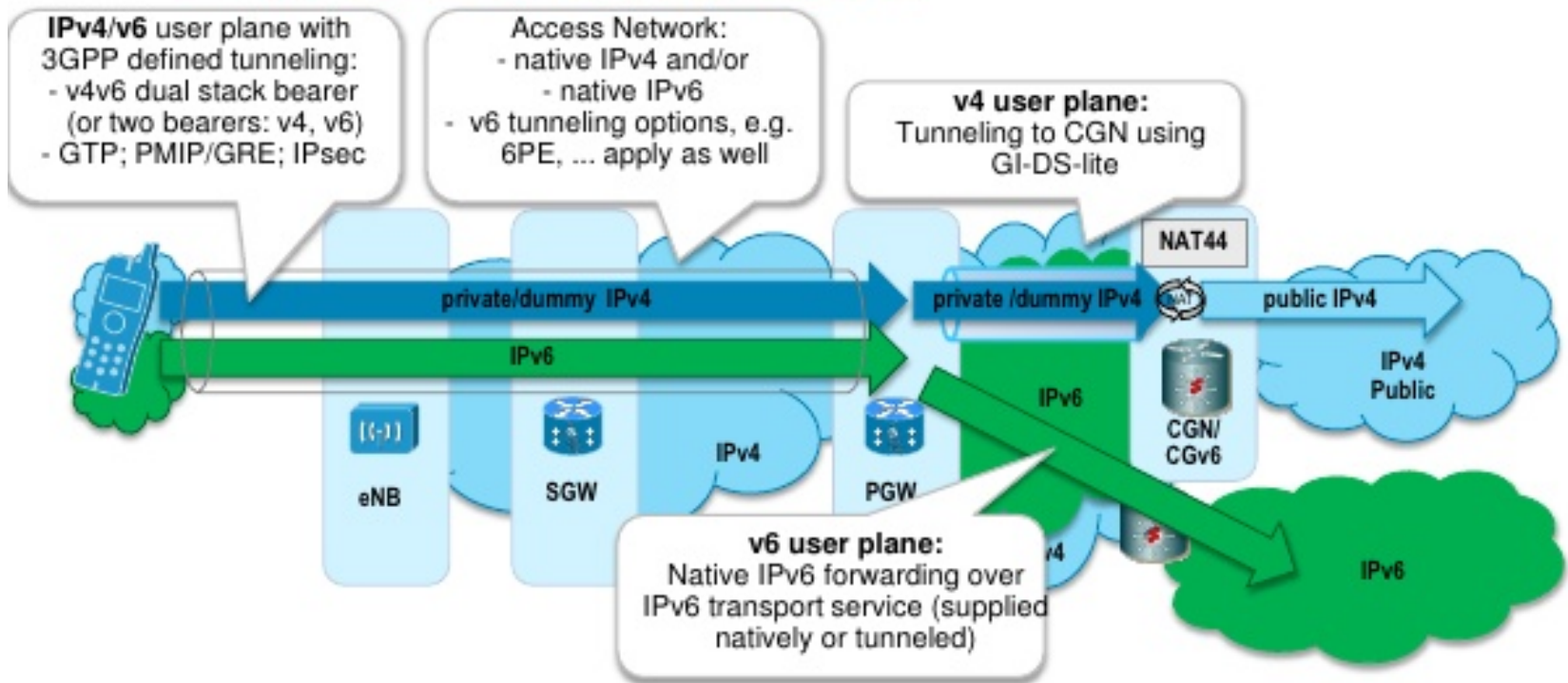
- En la norma 3GPP TS 23.975 se especifican algunas soluciones de transición:

1) Dual-stack with NAPT44

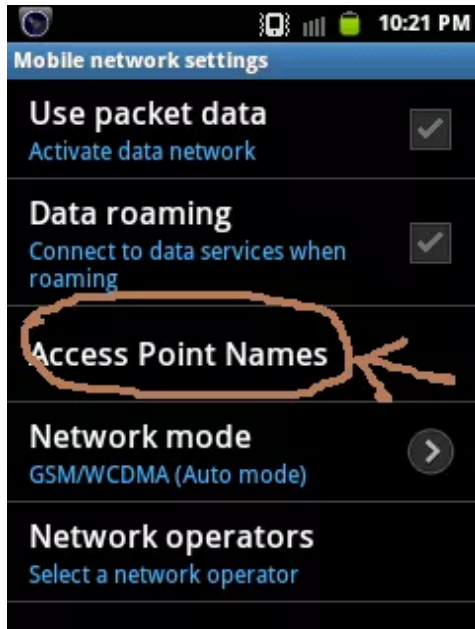
2) Gateway-initiated dual-stack Lite

3) IPv6-only with stateful NAT64

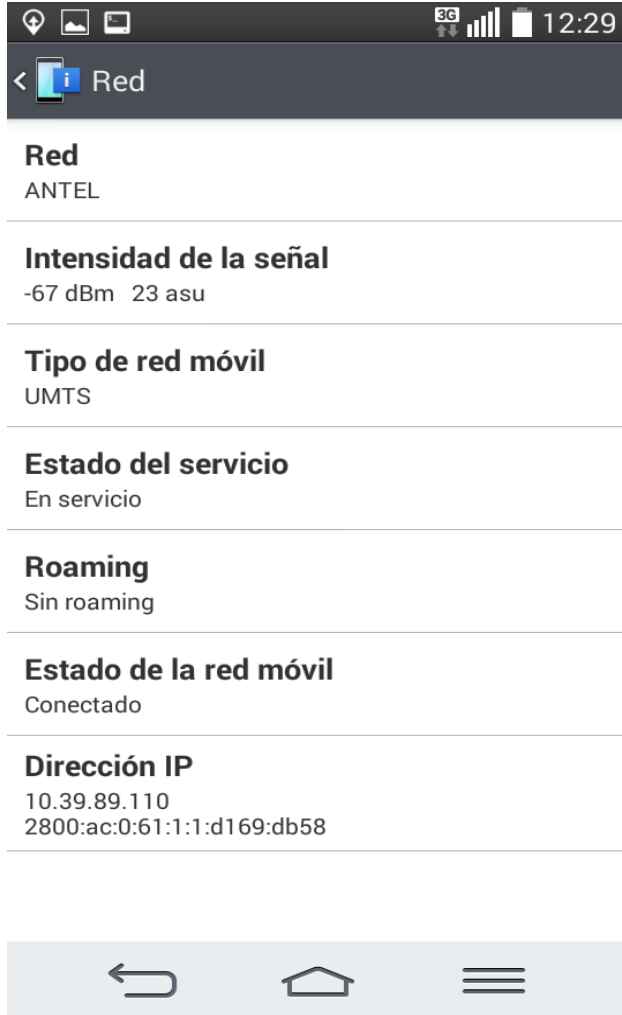
Funcionamiento



Configuración del terminal



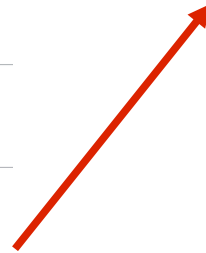
Verificación en el terminal



Dual Stack

10.39.89.110

2800:ac:0:61:1:1:d169:db58



Funcionamiento (3GPP 23.401)

- Durante el establecimiento del contexto, la red asigna al móvil una IPv4 privada + prefijo /64 IPv6
- La IPv6 se asigna mediante el mecanismo stateless address configuration (RFC 4862)
- El PGW envía un RA con el prefijo /64 al móvil, quien construye la IP con un identificador de interfaz también enviado por el PGW (unicidad)
- Como el /64 es asignado completamente al móvil, no realiza el procedimiento DAD (Duplicate Address Detection)

Algunos trazados

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save Filter_GGSN_SGSN RNC_1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.40.58.16	200.40.58.30	GTP	226	Create PDP context request
2	0.003000	200.40.58.30	200.40.58.16	GTP	221	Create PDP context response
3	1.311000	fe80::1:1:d169:db58	ff02::2	ICMPV6	62	Router Solicitation
4	1.311000	fe80::5	fe80::1:1:d169:db58	ICMPV6	102	Router Advertisement
5	2.637000	fe80::5	ff02::1	ICMPV6	102	Router Advertisement
6	5.637000	fe80::5	ff02::1	ICMPV6	102	Router Advertisement
7	8.637000	fe80::5	ff02::1	ICMPV6	102	Router Advertisement

Frame 1: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)

- Ethernet II, Src: 00:e1:fc:45:2b:f3 (00:e1:fc:45:2b:f3), Dst: 00:e0:fc:06:5f:38 (00:e0:fc:06:5f:38)
- Internet Protocol Version 4, Src: 200.40.58.16 (200.40.58.16), Dst: 200.40.58.30 (200.40.58.30)
- User Datagram Protocol, Src Port: 2123 (2123), Dst Port: 2123 (2123)
- GPRS Tunneling Protocol
 - Flags: 0x32
 - Message Type: Create PDP context request (0x10)
 - Length: 176
 - TEID: 0x00000000
 - Sequence number: 0xa288
 - IMSI: 748010037314296
 - Routing Area Identity
 -00 = Selection mode: MS or network provided APN, subscribed verified (0)
 - TEID Data I: 0x3c4590ad
 - TEID Control Plane: 0xb64f561e
 - NSAPI: 5
 - Charging characteristics: 2048
 - End user address (IETF/IPv4v6)
 - Access Point Name: ANTELV6
 - Protocol configuration options
 - GSN address : 200.40.58.16
 - GSN address : 200.40.58.20
 - MS international PSTN/ISDN number
 - Quality of service
 - Common Flags :
 - RAT Type: UTRAN
 - User Location Information
 - MS Time Zone: GMT - 3 hours 0 minutes
 - IMEI(SV): 3528580642592200
 - Evolved Allocation/Retention Priority I

[Response In: 2]

Solicitud "request" para crear el PDP Context con los datos del suscriptor

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save Filter_GGSN_SGSN RNC_1

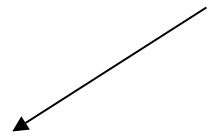
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.40.58.16	200.40.58.30	GTP	226	Create PDP context request
2	0.003000	200.40.58.30	200.40.58.16	GTP	221	Create PDP context response
3	1.311000	fe80::1:1:d169:db58	ff02::2	ICMPv6	62	Router solicitation
4	1.311000	fe80::5	fe80::1:1:d169:db58	ICMPv6	102	Router Advertisement
5	2.637000	fe80::5	ff02::1	ICMPv6	102	Router Advertisement
6	5.637000	fe80::5	ff02::1	ICMPv6	102	Router Advertisement
7	8.637000	fe80::5	ff02::1	ICMPv6	102	Router Advertisement

Frame 2: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits)

- Ethernet II, Src: 00:e1:fc:45:2b:f3 (00:e1:fc:45:2b:f3), Dst: 00:e0:fc:06:5f:38 (00:e0:fc:06:5f:38)
- Internet Protocol Version 4, Src: 200.40.58.30 (200.40.58.30), Dst: 200.40.58.16 (200.40.58.16)
- User Datagram Protocol, Src Port: 2123 (2123), Dst Port: 2123 (2123)
- GPRS Tunneling Protocol
 - Flags: 0x32
 - Message Type: Create PDP context response (0x11)
 - Length: 171
 - TEID: 0xb64f561e
 - Sequence number: 0xa288
 - Cause: Request accepted (128)
 - Reordering required: False
 - Recovery: 249
 - TEID Data I: 0x018881cf
 - TEID Control Plane: 0x018a81cf
 - Charging ID: 0x179ae838
 - End user address (IETF/IPv4v6) : 10.39.89.110 / 2800:ac:0:61:1:1:d169:db58
 - Length : 22
 - PDP type organization: IETF (1)
 - PDP type number: IPv4v6 (0x8d)
 - End user address IPv4: 10.39.89.110 (10.39.89.110)
 - End user address IPv6: 2800:ac:0:61:1:1:d169:db58 (2800:ac:0:61:1:1:d169:db58)
 - Protocol configuration options
 - GSN address : 200.40.58.3
 - GSN address : 200.40.58.3
 - Quality of Service
 - Charging Gateway address : 10.68.189.140

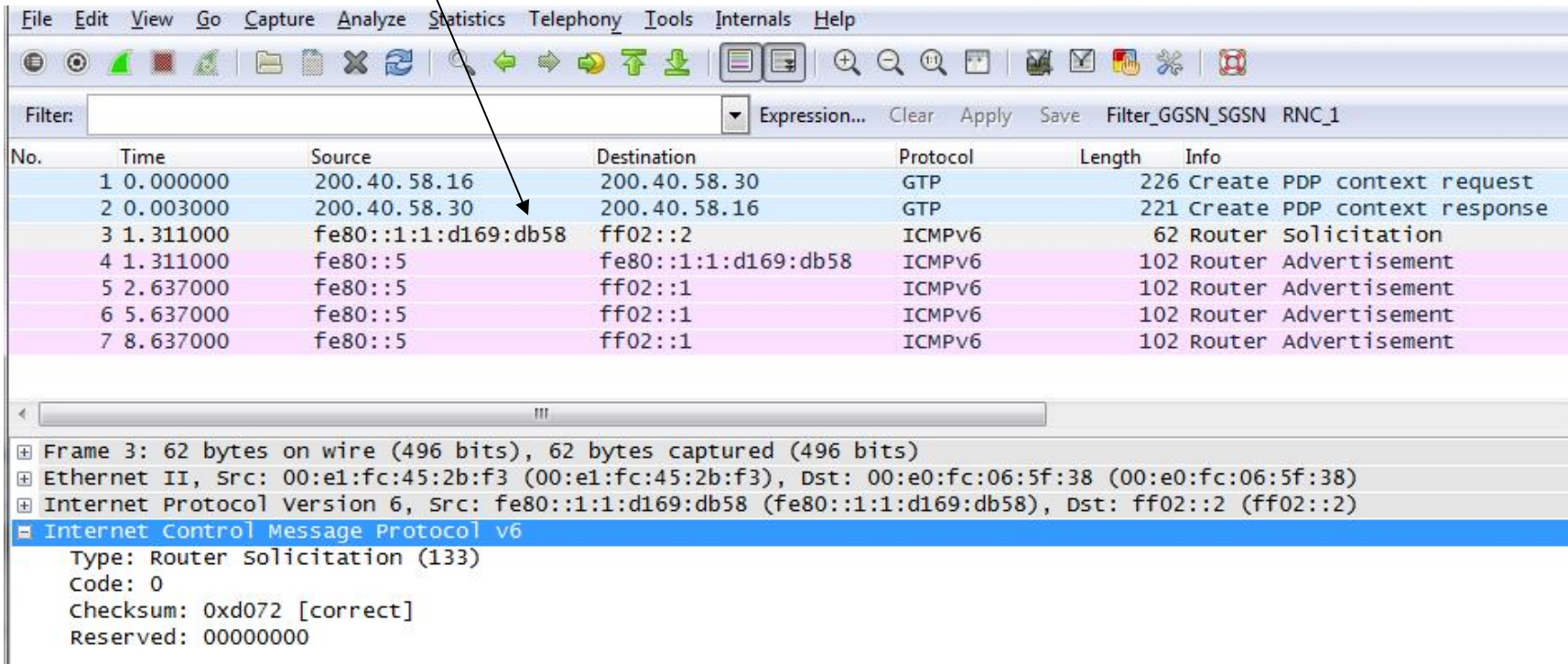
[Response To: 1]
[Time: 0.003000000 seconds]

En el *response*, ya se pasan las direcciones IPv4, IPv6 que usará el móvil



RS y RA desde y hacia el móvil

La IP de origen es la Link-local del móvil



The screenshot shows a Wireshark capture of network traffic. The packet list pane displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.40.58.16	200.40.58.30	GTP	226	Create PDP context request
2	0.003000	200.40.58.30	200.40.58.16	GTP	221	Create PDP context response
3	1.311000	fe80::1:1:d169:db58	ff02::2	ICMPv6	62	Router solicitation
4	1.311000	fe80::5	fe80::1:1:d169:db58	ICMPv6	102	Router Advertisement
5	2.637000	fe80::5	ff02::1	ICMPv6	102	Router Advertisement
6	5.637000	fe80::5	ff02::1	ICMPv6	102	Router Advertisement
7	8.637000	fe80::5	ff02::1	ICMPv6	102	Router Advertisement

The packet details pane for the selected packet (Frame 3) shows:

- Frame 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
- Ethernet II, Src: 00:e1:fc:45:2b:f3 (00:e1:fc:45:2b:f3), Dst: 00:e0:fc:06:5f:38 (00:e0:fc:06:5f:38)
- Internet Protocol Version 6, Src: fe80::1:1:d169:db58 (fe80::1:1:d169:db58), Dst: ff02::2 (ff02::2)
- Internet Control Message Protocol v6
 - Type: Router solicitation (133)
 - Code: 0
 - Checksum: 0xd072 [correct]
 - Reserved: 00000000

Tethering

- El móvil actúa como un “router” y ejecuta los procedimientos usuales para un acceso WiFi
- IPv4: realiza NAT a los equipos conectados
- IPv6: utiliza IPv6 stateless address autoconfiguration mediante los procedimientos normales (usa el mismo /64 asignado)
- OBS: no propaga hacia el packet core dichos procedimientos

Conclusiones

- Dual-stack con NAT44 es ideal para una red en producción sin grandes problemas de masividad (ej: overlapping private IPv4 addresses)
- Permite una introducción gradual según la penetración del protocolo en el parque de terminales (y su configuración)
- Requiere un análisis detallado del soporte en los diferentes planos y equipos de la red

Preguntas?

Muchas gracias!