LTE – Análisis de protocolos LTE

1. Ejercicio 1. Traza S1.pcap

- **¿Qué tipo de tráfico contiene la traza, qué está ocurriendo?**
  En la traza podemos observar que se utiliza constantemente el protocolo SIP para intentar hacer una llamada telefónica. Por tanto, la traza contiene tramas con tráfico de datos y de control.

```
GTP <S…   655 Request: REGISTER sip:apn.sip.voice.ng4t.com  (1 binding) |
GTP <S…   655 Status: 401 Unauthorized |
GTP <S…   921 Request: REGISTER sip:apn.sip.voice.ng4t.com  (1 binding) |
GTP <S…   582 Status: 200 OK (REGISTER)  (removed 1 binding) |
GTP <S…   900 Request: SUBSCRIBE sip:apn.sip.voice.ng4t.com, in-dialog |
GTP <S…   593 Status: 200 OK (SUBSCRIBE) |
GTP <S…   913 Request: NOTIFY sip:apn.sip.voice.ng4t.com |
GTP <S…   555 Status: 200 OK (NOTIFY) |
```

Primero se comprueba que el usuario es subscriptor de alguna tarifa telefónica

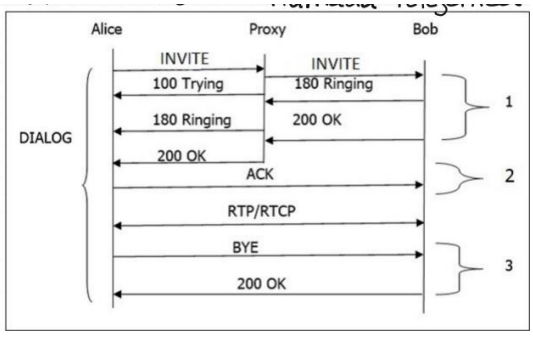
```
  54 Echo request
  60 Echo response
1015 Request: INVITE sip:ng40user11@apn.sip.voice.ng4t.com |
 478 Status: 100 Trying |
1019 Request: INVITE sip:ng40user11@apn.sip.voice.ng4t.com |
 955 Status: 183 Session Progress |
 876 Status: 183 Session Progress |
 853 Request: PRACK sip:ng40user11@apn.sip.voice.ng4t.com |
 857 Request: PRACK sip:ng40user11@apn.sip.voice.ng4t.com |
```

Una vez comprobado y verificado, se intenta hacer la llamada

Ambos procesos se repiten para ambas partes. Una vez todo este correcto y los usuarios estén disponibles y el destinatario coja la llamada, se inicia la llamada.

```
GTP <S…   869 Request: UPDATE sip:ng40user11@apn.sip.voice.ng4t.com |
GTP <S…   940 Status: 200 OK (UPDATE) |
GTP <S…   954 Status: 180 Ringing |
GTP <S…   861 Status: 200 OK (UPDATE) |
GTP <S…   875 Status: 180 Ringing |
GTP <S…   542 Request: PRACK sip:ng40user11@apn.sip.voice.ng4t.com |
GTP <S…   546 Request: PRACK sip:ng40user11@apn.sip.voice.ng4t.com |
GTP <S…   939 Status: 200 OK (PRACK) |
GTP <S…   940 Status: 200 OK (INVITE) |
GTP <S…   860 Status: 200 OK (PRACK) |
GTP <S…   861 Status: 200 OK (INVITE) |
GTP <S…   546 Request: ACK sip:10.255.1.111:5090 |
GTP <S…   550 Request: ACK sip:10.255.1.111:5090 |
GTP <U…   121 5092 → 5092 Len=43
GTP <U…   121 5092 → 5092 Len=43
GTP <U…   121 5092 → 5092 Len=43
GTP <U…   121 5092 → 5092 Len=43
```

Llamada establecida e iniciada

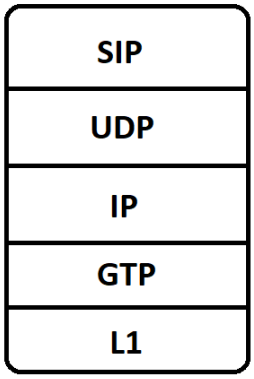


Esquema protocolo SIP

```
GTP <R…   142 Sender Report   Source description
GTP <R…   142 Sender Report   Source description
GTP <U…   121 5092 → 5092 Len=43
GTP <S…   546 Request: BYE sip:10.255.1.111:5090 |
GTP <S…   549 Request: BYE sip:10.255.1.111:5090 |
GTP <S…   615 Status: 200 OK (BYE) |
S1AP/N…   150 UplinkNASTransport, Bearer resource modification request
GTP <R…   142 Sender Report   Source description   Goodbye
GTP <S…   537 Status: 200 OK (BYE) |
S1AP/N…   126 SACK (Ack=17, Arwnd=62464) , E-RABReleaseCommand [NAS-cau
GTP <R…   146 Receiver Report   Source description   Goodbye
S1AP/N…   166 SACK (Ack=11, Arwnd=62419) , UplinkNASTransport, Bearer r
GTP <R…   142 Sender Report   Source description   Goodbye
```

Finaliza la llamada y cuelgan

- **Dibuja la torre de protocolos del paquete de datos de usuario que le llega al S-GW incluyendo los protocolos de nivel de aplicación identificados en la pregunta anterior.**



Protocolo de Aplicación: (SIP para llamadas VoIP).
Protocolo de Transporte: (UDP para SIP).
Nivel de Red: IP (Internet Protocol) para el enrutamiento a través de la red IP.
Nivel de Enlace: GTP (GPRS Tunneling Protocol) para la creación de un túnel para el transporte del paquete a través de la red móvil.
Nivel Físico: Capa física, que incluye la modulación y transmisión de la señal a través del medio físico (por ejemplo, ondas de radio en el caso de LTE).

- **¿Cuál es la IP del UE? Indica si hay varios UEs involucrados en la comunicación y dé qué modo.**

Hay **dos UEs**, que serían los usuarios que quieren hacer la llamada. La mayoría de las llamadas VoIP comienzan con un mensaje SIP INVITE. Examinando estos mensajes podremos identificar las direcciones IP de los UEs.
Véase un ejemplo:

```
10.255.1.1          10.0.0.100          GTP <S…  1015 Request: INVITE sip:ng40user11@apn.sip.voice.ng4t.com |
10.0.0.100          10.255.1.1          GTP <S…   478 Status: 100 Trying |
```

IP del interesado: 10.255.1.1
IP del usuario que recibe la llamada: 10.255.1.111

La dirección IP **10.0.0.100** es de un *proxy SIP.*
Un proxy SIP es un servidor intermedio que ayuda en la enrutación y procesamiento de mensajes SIP y que en este caso nos ayuda a encontrar a la persona con quien el interesado quiera hacer la llamada. Puede estar ubicado entre dos UEs para facilitar el establecimiento de sesiones SIP.
Los proxies SIP pueden realizar funciones como retransmisión de mensajes, enrutamiento de llamadas, autenticación, autorización, y registro de ubicación, pero **no son UEs en sí mismos**.

- **¿Cuál es la IP del eNodeB?**

IP del eNodeB: 10.1.1.2

10.1.1.2	10.1.2.10	S1AP/N…	306	SACK (Ack=4, Arwnd=62464) , InitialContextSetupRequest,
10.1.2.10	10.1.1.2	S1AP	118	SACK (Ack=4, Arwnd=62464) , InitialContextSetupResponse

- **¿Cuál es la IP del S-GW?**

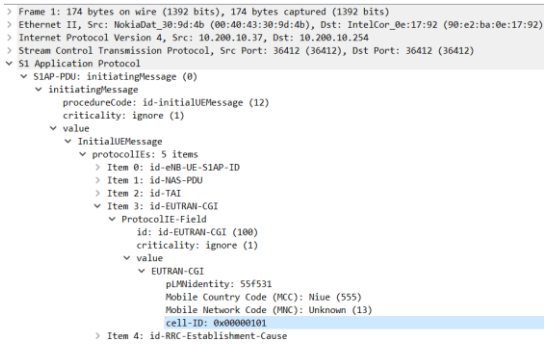
En los mensajes GTP podemos encontrar la dirección IP del S-GW (*Echo request*), ya que estos mensajes se utilizan para el transporte de datos.

IP del S-GW: 10.1.1.12

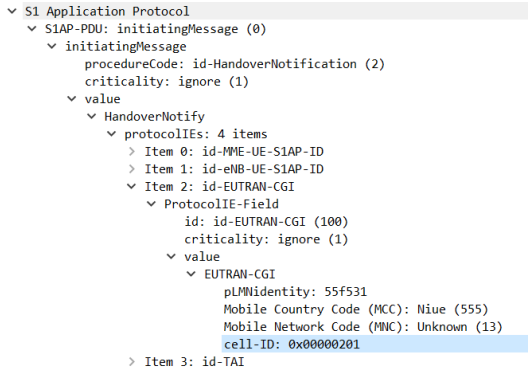
10.1.2.11	10.1.1.12	GTP	60 Echo request
10.1.1.12	10.1.2.11	GTP	56 Echo response

2. Ejercicio 2. Traza handover.pcap

- **¿Cuál es el id de la celda destino? 0x00000101**



- **¿Cuál es el id de la celda origen? 0x00000201**



- **¿Cuándo se ejecuta el procedimiento de actualización de posición?**

10.200.10.37	10.200.10.254	S1AP	302	HandoverRequired [RadioNetwork-cause=handover-desirable-for-radio-reason]
10.200.10.253	10.200.10.38	S1AP	362	HandoverRequest [RadioNetwork-cause=s1-intra-system-handover-triggered]

La red de radio ha evaluado condiciones específicas, como la calidad de la señal, la congestión de la celda actual, o cualquier otro factor de radio que sugiere que realizar un *handover* sería beneficioso para la calidad de la conexión.