LTE:

A feature based introduction

LTE Core Features

Annex. GTP Primer

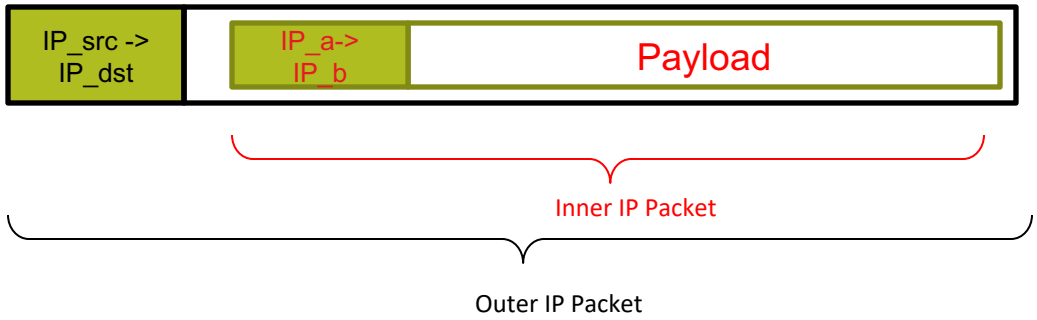
Irfan Ali

Video at youtube:
https://www.youtube.com/watch?v=FPfExr9bEEg&list=PLgQvzsPaZX_bimBc5Wu4m6-cVD4bZDav9&index=9

What is GTP?

- GTP = GPRS **Tunneling** Protocol

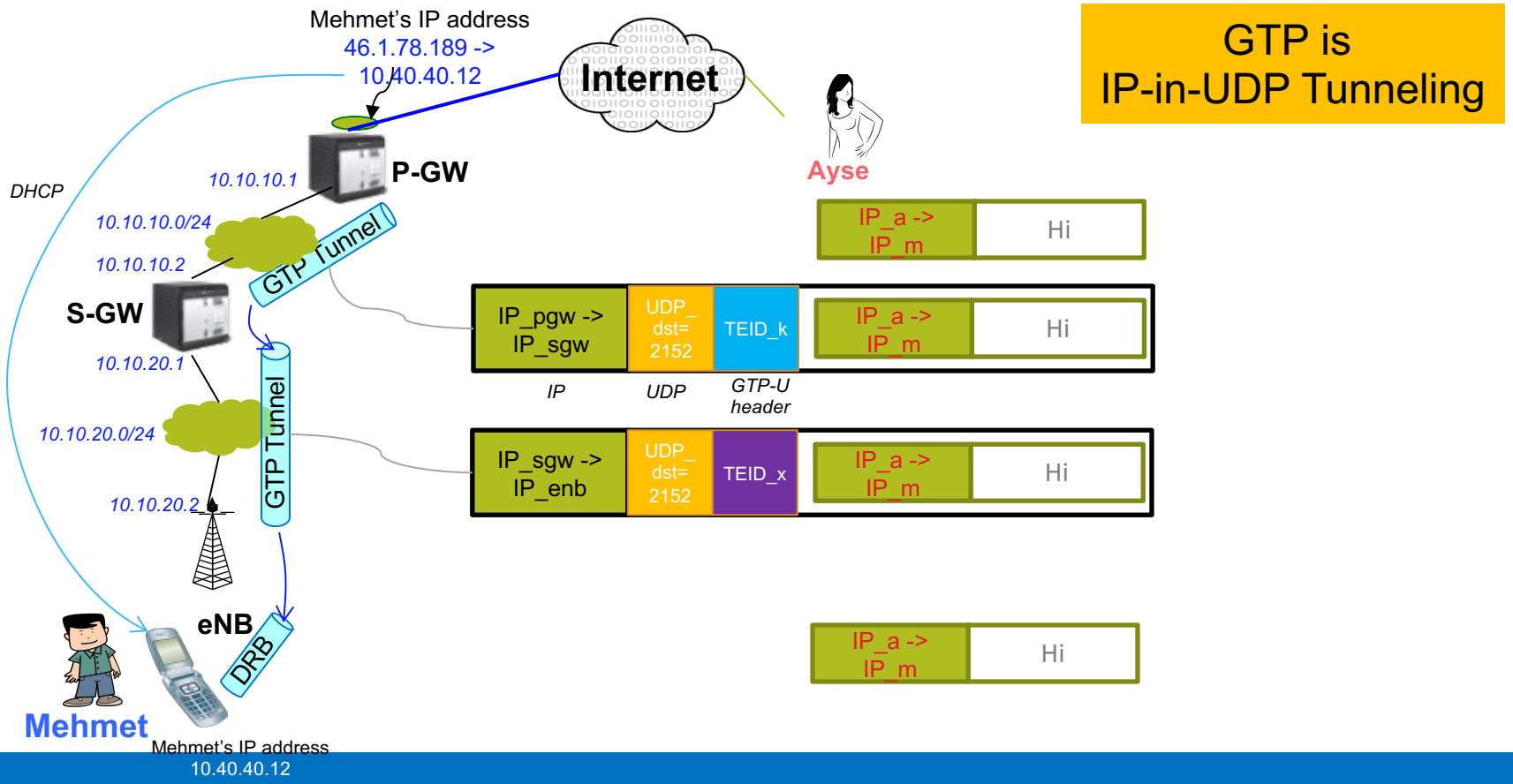
- What is **Tunneling** in the IP World?
  - Tunneling in the IP world means putting an IP packet inside another IP packet.



GPRS General Packet Radio Service

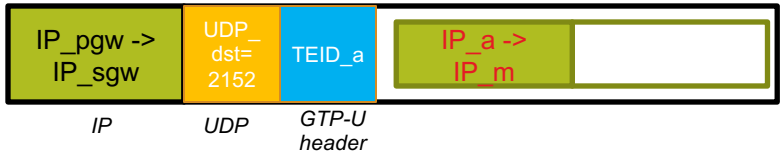
What is the purpose of GTP Tunneling?

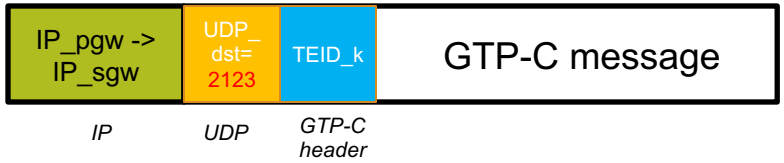
- Route an IP packet along a path that is not topologically correct for the packet.



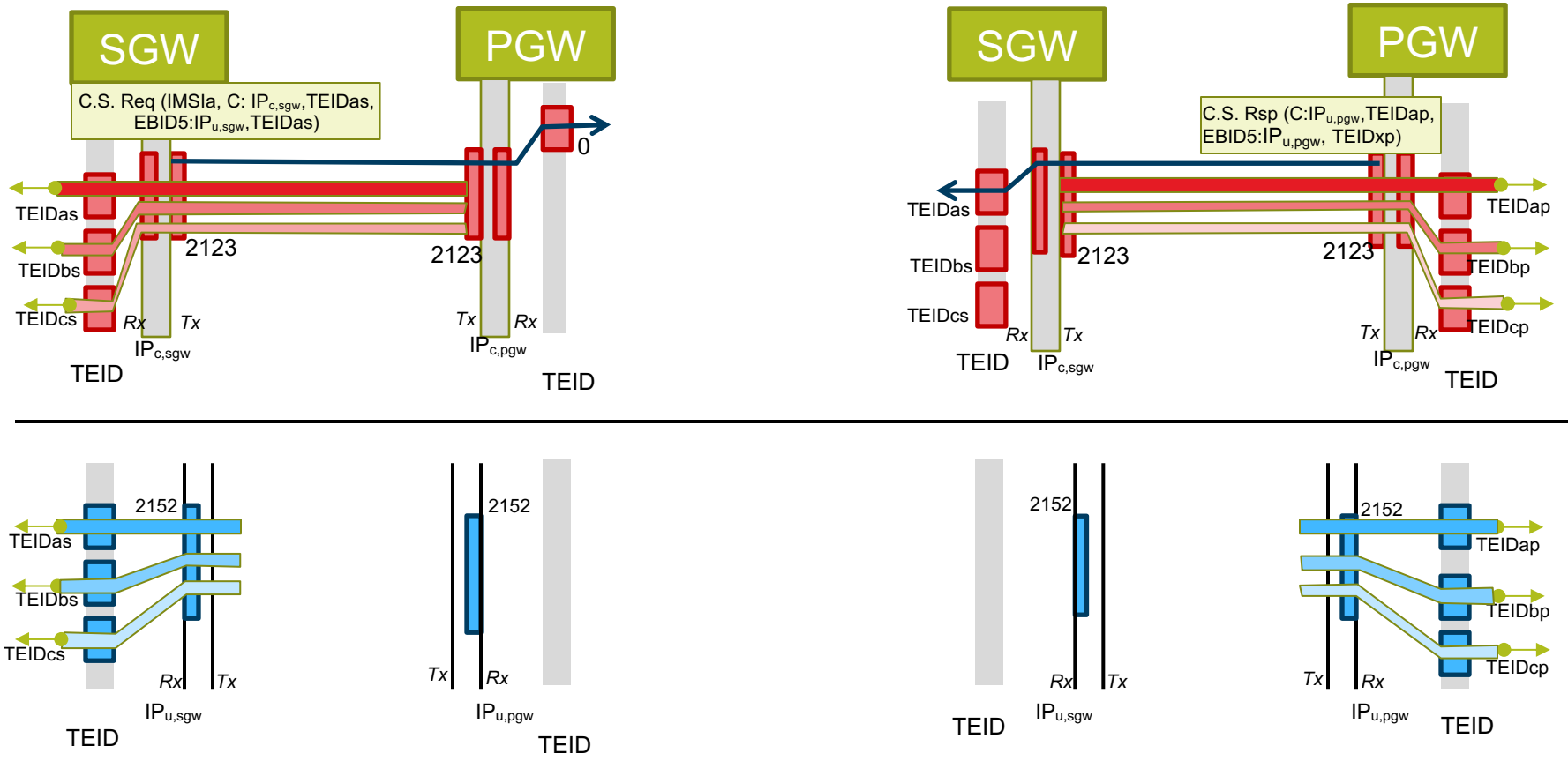
How does the GTP-U Tunnel get setup?

- GTP Protocol has two parts
  - Signaling part called GTP-C (GTP-Control)
  - User data part called GTP-U (GTP-User)
- GTP-C is used to setup GTP-U tunnel
- Both GTP-C and GTP-U run on top of UDP
- IP-in-UDP tunneling is only used for GTP-U
- GTP-C carries control/signaling messages





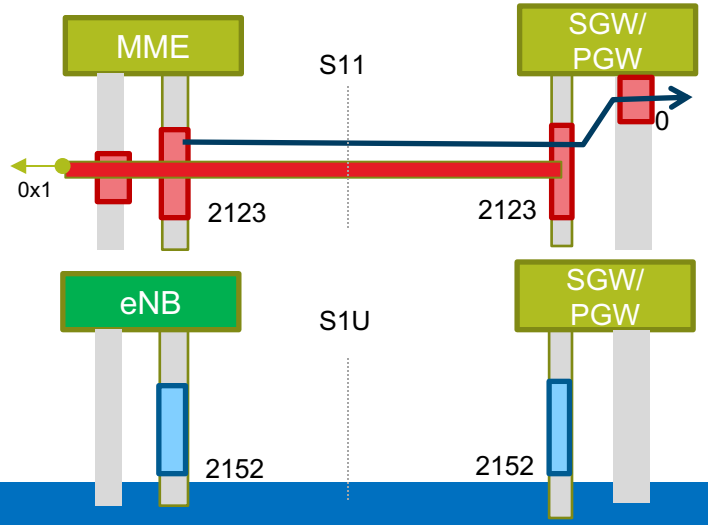
How does GTP-U Tunnel get setup: Example



Packet Trace: Create Session Request (S11); MME->SGW

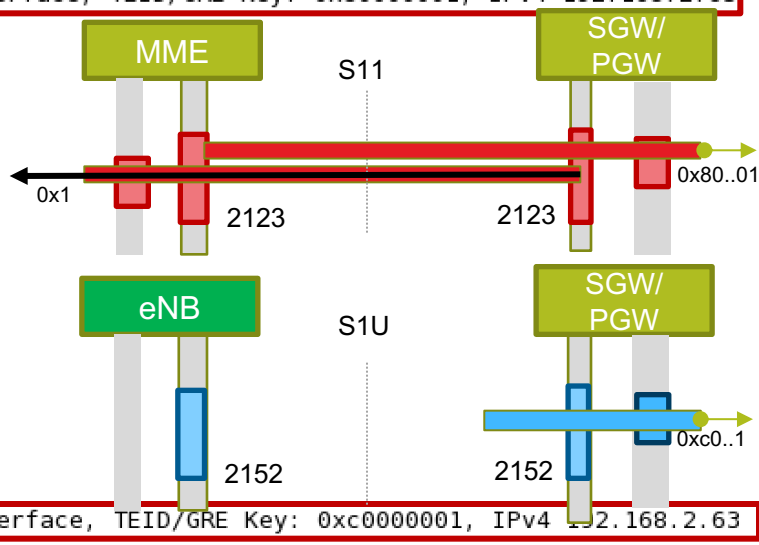
```
Frame 214: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits)
Ethernet II, Src: Continuo_53:20:89 (00:02:bb:53:20:89), Dst: Continuo_50:38:c4 (00:02:bb:50:38:c4)
Internet Protocol Version 4, Src: 192.168.2.53 (192.168.2.53), Dst: 192.168.2.63 (192.168.2.63)
User Datagram Protocol, Src Port: gtp-control (2123), Dst Port: gtp-control (2123)
GPRS Tunneling Protocol V2
Create Session Request
  Flags: 0x48
    010. .... = Version: 2
    ...0 .... = Piggybacking flag (P): 0
    .... 1... = TEID flag (T): 1
  Message Type: Create Session Request (32)
  Message Length: 163
  Tunnel Endpoint Identifier: 0
  Sequence Number: 2
  Spare: 0
  International Mobile Subscriber Identity (IMSI) : 325912900111225
  User Location Info (ULI) : TAI
  Serving Network : MCC 332 United States Virgin Islands, MNC 931
  RAT Type : EUTRAN (6)
  Indication :
  Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S11 MME GTP-C interface, TEID/GRE Key: 0x00000001, IPv4 192.168.2.53
  Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S5/S8 PGW GTP-C interface, TEID/GRE Key: 0x00000000, IPv4 0.0.0.0
  PDN Type : IPv4
  PDN Address Allocation (PAA) :
  APN Restriction : value 0
  Selection Mode : MS provided APN, subscription not verified
  Access Point Name (APN) : ltetr.mot.com
  Aggregate Maximum Bit Rate (AMBR) :
  Bearer Context : [Grouped IE]
    IE Type: Bearer Context (93)
    IE Length: 31
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    EPS Bearer ID (EBI) : 5
    Bearer Level Quality of Service (Bearer QoS) :
```

Octets	Bits 8	7	6	5	4	3	2	1
1	Version			P	T=1	Spare	Spare	Spare
2	Message Type							
3	Message Length (1st Octet)							
4	Message Length (2nd Octet)							
5	Tunnel Endpoint Identifier (1st Octet)							
6	Tunnel Endpoint Identifier (2nd Octet)							
7	Tunnel Endpoint Identifier (3rd Octet)							
8	Tunnel Endpoint Identifier (4th Octet)							
9	Sequence Number (1st Octet)							
10	Sequence Number (2nd Octet)							
11	Sequence Number (3rd Octet)							
12	Spare							



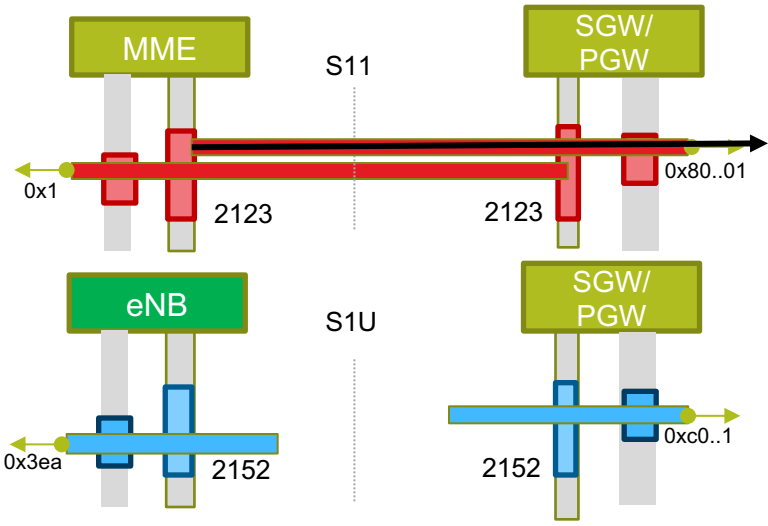
Packet Trace: Create Session Response (S11); SGW -> MME

```
Frame 215: 115 bytes on wire (920 bits), 115 bytes captured (920 bits)
Ethernet II, Src: Continuo_50:38:c4 (00:02:bb:50:38:c4), Dst: Continuo_53:20:89 (00:02:bb:53:20:89)
Internet Protocol Version 4, Src: 192.168.2.63 (192.168.2.63), Dst: 192.168.2.53 (192.168.2.53)
User Datagram Protocol, Src Port: gtp-control (2123), Dst Port: gtp-control (2123)
GPRS Tunneling Protocol V2
Create Session Response
  Flags: 0x48
      010. .... = Version: 2
      ...0 .... = Piggybacking flag (P): 0
      .... 1... = TEID flag (T): 1
    Message Type: Create Session Response (33)
    Message Length: 69
    Tunnel Endpoint Identifier: 1
    Sequence Number: 2
    Spare: 0
  Cause : Request accepted (16)
  Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S11/S4 SGW GTP-C interface, TEID/GRE Key: 0x80000001, IPv4 192.168.2.63
  PDN Address Allocation (PAA) :
  APN Restriction : value 0
  Bearer Context : [Grouped IE]
      IE Type: Bearer Context (93)
      IE Length: 24
      0010 .... = CR flag: 2
      .... 0000 = Instance: 0
    EPS Bearer ID (EBI) : 5
        IE Type: EPS Bearer ID (EBI) (73)
        IE Length: 1
        0010 .... = CR flag: 2
        .... 0000 = Instance: 0
        0000 .... = Spare bit(s): 0
        .... 0101 = EPS Bearer ID (EBI): 5
    Cause : Request accepted (16)
    Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S1-U SGW GTP-U interface, TEID/GRE Key: 0xc0000001, IPv4 192.168.2.63
```



Packet Trace: Modify Bearer Request (S11); MME ->SGW

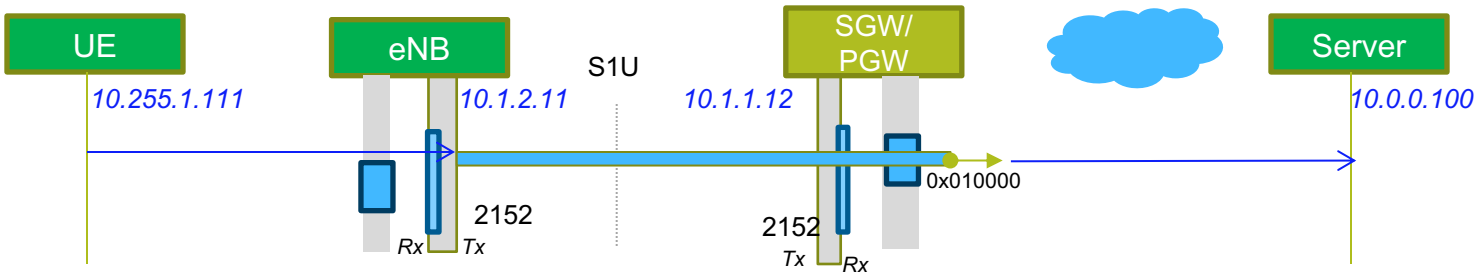
```
▷ Frame 221: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
▷ Ethernet II, Src: Continuo_53:20:89 (00:02:bb:53:20:89), Dst: Continuo_50:38:c4 (00:02:bb:50:38:c4)
▷ Internet Protocol Version 4, Src: 192.168.2.53 (192.168.2.53), Dst: 192.168.2.63 (192.168.2.63)
▷ User Datagram Protocol, Src Port: gtp-control (2123), Dst Port: gtp-control (2123)
  GPRS Tunneling Protocol V2
▽ Modify Bearer Request
  ▽ Flags: 0x48
      010. .... = Version: 2
      ...0 .... = Piggybacking flag (P): 0
      .... 1... = TEID flag (T): 1
    Message Type: Modify Bearer Request (34)
    Message Length: 30
    Tunnel Endpoint Identifier: 2147483649 0x800..001
    Sequence Number: 3
    Spare: 0
  ▽ Bearer Context : [Grouped IE]
      IE Type: Bearer Context (93)
      IE Length: 18
      0000 .... = CR flag: 0
      .... 0000 = Instance: 0
    ▽ EPS Bearer ID (EBI) : 5
        IE Type: EPS Bearer ID (EBI) (73)
        IE Length: 1
        0000 .... = CR flag: 0
        .... 0000 = Instance: 0
        0000 .... = Spare bit(s): 0
        .... 0101 = EPS Bearer ID (EBI): 5
    ▽ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S1-U eNodeB GTP-U interface, TEID/GRE Key: 0x000003ea, IPv4 192.168.2.75
        IE Type: Fully Qualified Tunnel Endpoint Identifier (F-TEID) (87)
        IE Length: 9
        0000 .... = CR flag: 0
        .... 0000 = Instance: 0
        1... .... = V4: IPv4 address present
        .0.. .... = V6: IPv6 address not present
        ..00 0000 = Interface Type: S1-U eNodeB GTP-U interface (0)
        TEID/GRE Key: 0x000003ea
        F-TEID IPv4: 192.168.2.75 (192.168.2.75)
```



Packet Trace: GTP-U: S1-U; eNB -> SGW/PGW

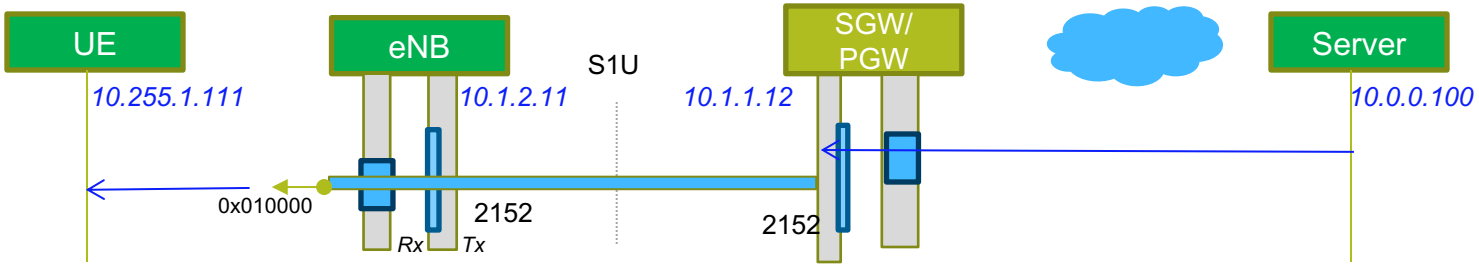
```
Frame 14: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits)
Ethernet II, Src: Vmware_6c:d6:e7 (00:0c:29:6c:d6:e7), Dst: Vmware_b1:35:bd (00:0c:29:b1:35:bd)
Internet Protocol Version 4, Src: 10.1.2.11 (10.1.2.11), Dst: 10.1.1.12 (10.1.1.12)
User Datagram Protocol, Src Port: gtp-user (2152), Dst Port: gtp-user (2152)
GPRS Tunneling Protocol
  Flags: 0x30
    001. .... = Version: GTP release 99 version (1)
    ...1 .... = Protocol type: GTP (1)
    .... 0... = Reserved: 0
    .... .0.. = Is Next Extension Header present?: No
    .... ..0. = Is Sequence Number present?: No
    .... ...0 = Is N-PDU number present?: No
  Message Type: T-PDU (0xff)
  Length: 605
  TEID: 0x01000000
T-PDU Data 605 bytes
Internet Protocol Version 4, Src: 10.255.1.111 (10.255.1.111), Dst: 10.0.0.100 (10.0.0.100)
User Datagram Protocol, Src Port: 5090 (5090), Dst Port: sip (5060)
Session Initiation Protocol (REGISTER)
```

Octets	Bits 8	7	6	5	4	3	2	1
1	Version			PT	(*)	E	S	PN
2	Message Type							
3	Length (1st Octet)							
4	Length (2nd Octet)							
5	Tunnel Endpoint Identifier (1st Octet)							
6	Tunnel Endpoint Identifier (2nd Octet)							
7	Tunnel Endpoint Identifier (3rd Octet)							
8	Tunnel Endpoint Identifier (4th Octet)							
9	Sequence Number (1st Octet)[1) 4)]							
10	Sequence Number (2nd Octet)[1) 4)]							
11	N-PDU Number[2) 4)]							
12	Next Extension Header Type[3) 4)]							

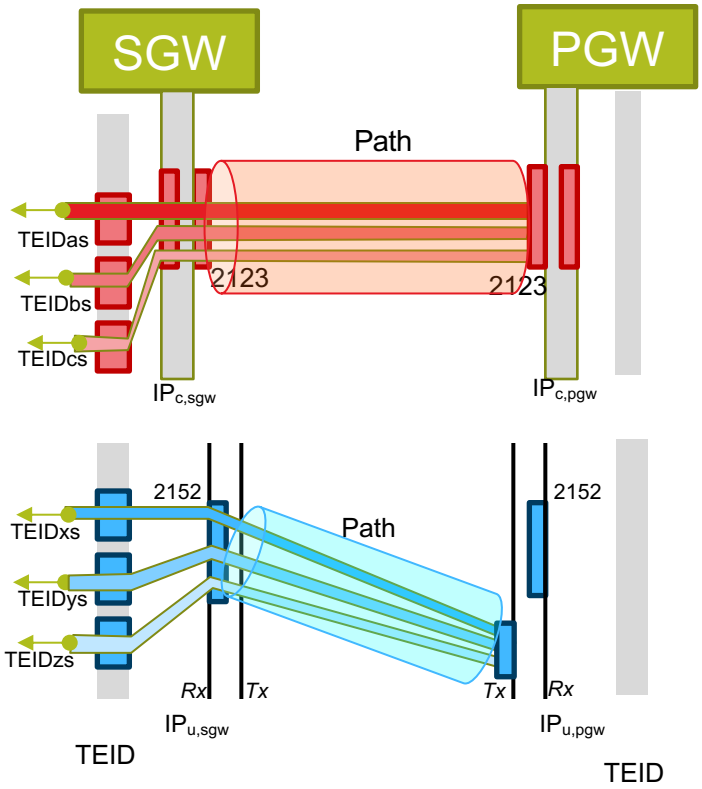


Packet Trace GTP-U: S1-U; eNB <- SGW/PGW

```
▷ Frame 15: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits)
▷ Ethernet II, Src: Vmware_b1:35:bd (00:0c:29:b1:35:bd), Dst: Vmware_6c:d6:e7 (00:0c:29:6c:d6:e7)
▷ Internet Protocol Version 4, Src: 10.1.1.12 (10.1.1.12), Dst: 10.1.2.11 (10.1.2.11)
▷ User Datagram Protocol, Src Port: gtp-user (2152), Dst Port: gtp-user (2152)
▽ GPRS Tunneling Protocol
  ▽ Flags: 0x30
      001. .... = Version: GTP release 99 version (1)
      ...1 .... = Protocol type: GTP (1)
      .... 0... = Reserved: 0
      .... .0.. = Is Next Extension Header present?: No
      .... ..0. = Is Sequence Number present?: No
      .... ...0 = Is N-PDU number present?: No
    Message Type: T-PDU (0xff)
    Length: 605
    TEID: 0x01000000
  T-PDU Data 605 bytes
▷ Internet Protocol Version 4, Src: 10.0.0.100 (10.0.0.100), Dst: 10.255.1.111 (10.255.1.111)
▷ User Datagram Protocol, Src Port: sip (5060), Dst Port: 5090 (5090)
▷ Session Initiation Protocol (401)
```



GTP Path and Path Management



- Path is between two endpoints. Each end point is IP_address+UDP_Port#
- There can be several GTP tunnels on a path (each with different TEIDs).
- There is typically a “software process” that binds to each end-point.
- **Path Management messages**: To ensure that a path is alive (both the physical link and process at the endpoint), periodic echo-request and echo-response are sent.
- Failure-detection and error-recovery mechanisms are defined.

Packet Traces: GTP-U Echo-request & Echo Response

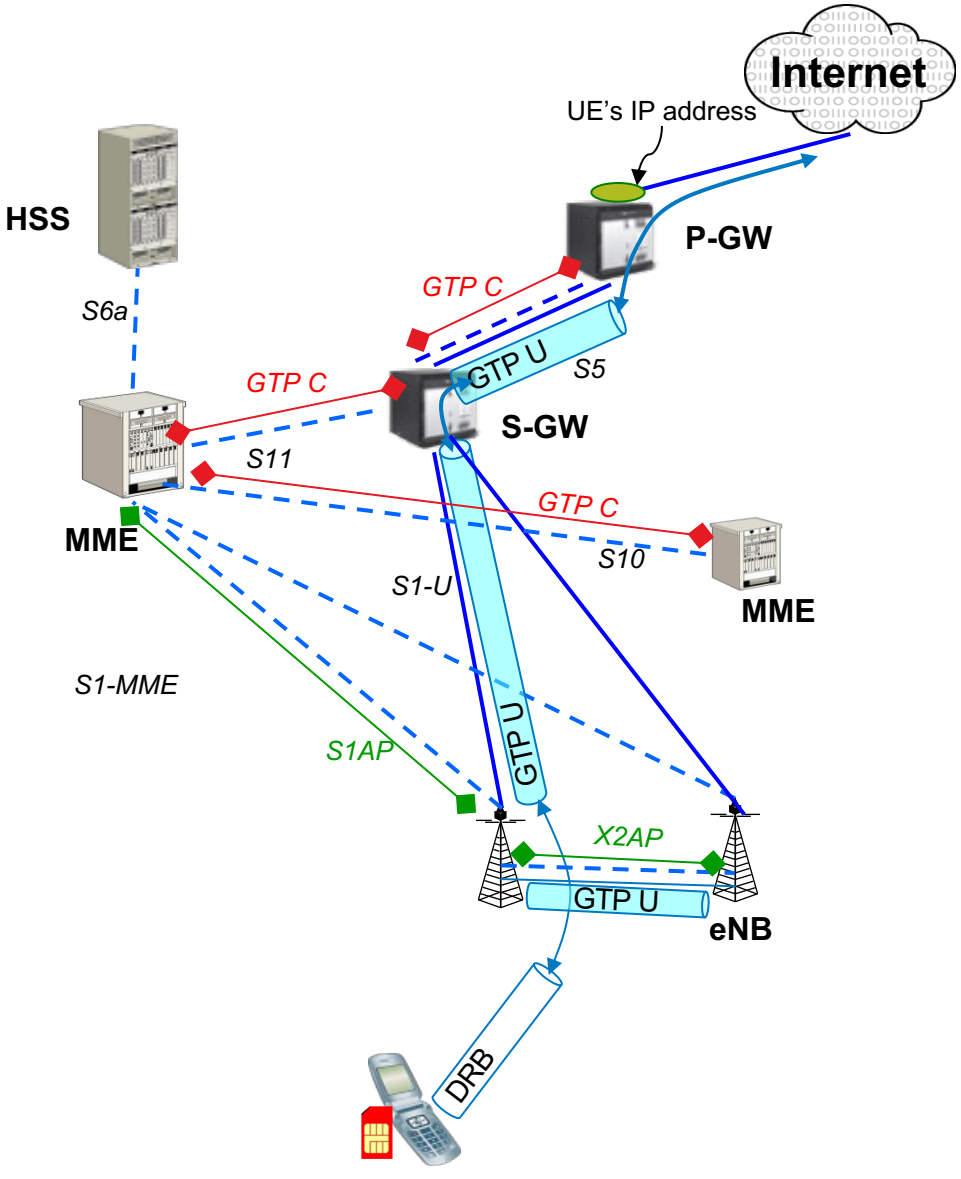
```
Frame 39: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: Vmware_6c:d6:e7 (00:0c:29:6c:d6:e7), Dst: Vmware_b1:35:bd (00:0c:29:b1:35:bd)
Internet Protocol Version 4, Src: 10.1.2.11 (10.1.2.11), Dst: 10.1.1.12 (10.1.1.12)
User Datagram Protocol, Src Port: gtp-user (2152), Dst Port: gtp-user (2152)
GPRS Tunneling Protocol
  Flags: 0x32
      001. .... = Version: GTP release 99 version (1)
      ...1 .... = Protocol type: GTP (1)
      .... 0... = Reserved: 0
      .... .0.. = Is Next Extension Header present?: No
      .... ..1. = Is Sequence Number present?: Yes
      .... ...0 = Is N-PDU number present?: No
    Message Type: Echo request (0x01)
    Length: 4
    TEID: 0x00000000
    Sequence number: 0x0000
```

In GTP-Cv2 Echo request/response messages do not contain TEID field

```
Frame 40: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
Ethernet II, Src: Vmware_b1:35:bd (00:0c:29:b1:35:bd), Dst: Vmware_6c:d6:e7 (00:0c:29:6c:d6:e7)
Internet Protocol Version 4, Src: 10.1.1.12 (10.1.1.12), Dst: 10.1.2.11 (10.1.2.11)
User Datagram Protocol, Src Port: gtp-user (2152), Dst Port: gtp-user (2152)
GPRS Tunneling Protocol
  Flags: 0x32
      001. .... = Version: GTP release 99 version (1)
      ...1 .... = Protocol type: GTP (1)
      .... 0... = Reserved: 0
      .... .0.. = Is Next Extension Header present?: No
      .... ..1. = Is Sequence Number present?: Yes
      .... ...0 = Is N-PDU number present?: No
    Message Type: Echo response (0x02)
    Length: 6
    TEID: 0x00000000
    Sequence number: 0x0000
    Recovery: 0
```

In GTP-Cv2 Echo request/response messages do not contain TEID field

Interfaces on which GTP is used



- GTP-Cv2 is used not only for mobility management, but also for general signaling purposes, eg providing UE's cell information to the PGW and from there to operator's service network.

Specifications

- GTPC v2 TS 29.274
- GTPU v1 TS 29.281

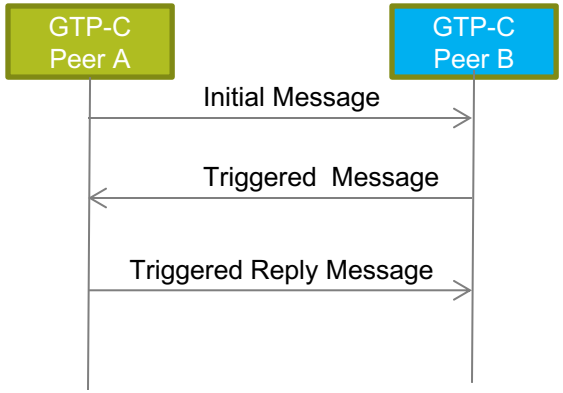
- GTPC v1 TS 29.060

- Historically (before Rel-8, i.e. before 2009Q1), TS 29.060 used to be the key GTP specification (both GTPC v1 and GTPU v1). But since Rel-8, TS 29.060 is only applicable to 3G interfaces (Gn/Gp, between SGSN <-> GGSN and between SGSNs) and not to EPC interfaces. Its specification only applies to GTPC v1
  - Ignore anything that 29.060 says about GTPU.

Annex

Rules for GTP-C IP address and port numbers

- Three types of messages



- Rules for Port# and IP addresses
  - Initial Message:
    1. **The UDP Destination Port number for GTPv2 Initial messages shall be 2123**
    2. The UDP Source Port for a GTPv2 Initial message is a locally allocated port number.
    3. During the establishment of the GTP tunnel, the GTPv2 entity selects and communicates to the peer GTPv2 entity the IP Destination Address at which it expects to receive subsequent control plane Initial messages related to that GTP tunnel via the "Sender F-TEID for Control Plane" IE
  - Triggered message
    1. The IP Source Address of a GTPv2 Triggered message and for a Triggered Reply message shall be copied from the IP destination address of the message to which this GTPv2 entity is replying
    2. The IP Destination Address of a GTPv2 Triggered message and for a Triggered Reply message shall be copied from the IP Source Address of the message to which this GTPv2 entity is replying
    3. The UDP Source Port of a GTPv2 Triggered message shall be the value from the UDP Destination Port of the corresponding message to which this GTPv2 entity is replying
    4. The UDP Destination Port value of a GTPv2 Triggered message shall be the value of the UDP Source Port of the corresponding message to which this GTPv2 entity is replying
  - Triggered Reply message
    1. Same rules as triggered message.
- Rules for TEID#
  - The first Create Session Request message on S11 for a UE shall have TEID = 0x0
  - The (first and subsequent) Create Session Request message on S5 for a UE shall have TEID = 0x0