BLG 609E - Mobile Broadband Networks: LTE and WiMAX

Homework Assignment #2: Standards and Network Architecture

Due Date: Feb 27th , 2012 at start of lecture

TOTAL POINTS: 25 POINTS

1. Look up DHCP specifications (eg. wikipedia), answer the following questions for EPC architecture, when the DHCP Server is part of the PGW. That is, the DHCP-client is in the UE and the DHCP Server is in the PGW: **(8 POINTS)**

    1. Draw the flow for DHCPv4 for a UE to get its IP address between the UE and P-GW(DHCP-Server)? **(3 POINTS)**

    2. Using a network sniffer (eg. Wireshark) on your laptop, study the DHCPv4 interaction between your computer and a DHCP Server (eg in your DSL router) and provide a print-out of the interaction. **(5 points)**

2. Please answer the following question about WiMAX architecture: **POINTS 5**

    a. If ASN-GW and BS were always co-located, which one(s) of the reference points would disappear from the Network Reference Model (NRM)?

    b. The MME and the SGW together are approximately equivalent in functionality to which node in the WiMAX architecture?

3. The following questions are related to the file **lte_attach.pcap** which is provided on the yahoo groups site. Please download that file and use Wireshark (www.wireshark.org) to analyze the packets and answer the following questions. Also use your lecture notes on LTE architecture. The file includes packets on the S1-MME interface (eNB <--> MME) and on the S11 interface (MME < -- > SGW)

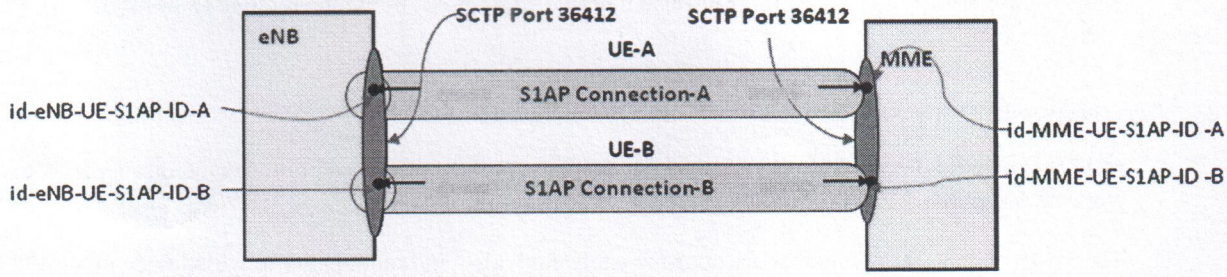
    UE's IMSI (Packet #187): Packet# 187 is an S1AP (S1 Application Protocol) message (i.e message between eNB and MME) which encapsulates the "Identity Response" NAS (Non Access Stratum) message from the UE to the MME. Write down the IMSI of the UE? Assuming that the MCC is 3 digits long and MNC is also 3 digits long, what is the PLMN-ID of the operator of the UE? **2 POINTS**

    Background: In this file, the UE had previously attached to the network and had received a temporary identity from the MME, this identity is called Globally Unique Temporary Identity (GUTI). The UE had then switched-off (detached) from the network. The UE in the "Attach Request" (Packet #176) provides this temporary identity GUTI and not the IMSI. The MME in this case is not able to recognize the UE by the GUTI (UE has probably moved from one area to another, eg the UE had previously attached to an MME is Maslak and is not attaching to an MME in Levent). Hence, the MME (in Levent) is now asking for the UE to provide its IMSI to the MME (Packet #186 Identity Request).

(5 POINTS) Setting up the S1-MME (S1AP) Connection (Packet # 176 and #186) for the UE (UE-A): A separate "logical" connection is setup between the eNB and MME for each user. On this logical connection, packets for only UE-A are sent. This logical connection runs on the S1 Application Layer (S1AP). This logical connection is identified by an S1AP identifier at the eNB side (called id-eNB-UE-S1AP-ID) and an S1AP identifier at the MME side (called id-MME-UE-S1AP-ID). At the eNB, to recognize packets from the MME that are related to UE-A, the eNB assigns a unique value to id-eNB-UE-S1AP-ID for UE-A. In the very first packet for UE-A that the eNB sends to the MME (packet #176 in our case), the eNB informs the MME about this Value. From this point onwards all packets for UE-A from the MME will set field id-eNB-UE-S1AP-ID to this value. What is the value of id-eNB-UE-S1AP-ID set by the eNB in Packet#176? Double-check that in message I86, the MME uses the same value when it talks to the eNB in message 186 (also message 189).

Similarly at the MME, to recognize packets from the eNB that are related to UE-A, the MME assigns a unique value to the id-MME-UE-S1AP-ID for UE-A. In the very first packet for UE-A that the MME sends to the eNB (packet #186 in our case), the MME informs the eNB about this value for id-MME-UE-S1AP-ID. From this point onwards all packets for UE-A from the eNB will set id-MME-UE-S1AP-ID to this value. What is the value of id-MME-UE-S1AP-ID set by the MME in Packet#186? Double-check in message I87 to make sure that the eNB sets field id-MME-UE-S1AP-ID to this value for packets related to UE-A (also message 191).

The following figure illustrates the concept. Hence, the "logical" connection for UE-A at S1AP layer is represented by (id-eNB-UES1AP-ID-A, id-eNB-UES1AP-ID-B). S1AP packets with these values in the appropriate field in the packet belong to this "logical connection". Creation of such a logical connection helps the eNB and MME to identify packets are related to a particular UE (UE-A, in our case).



(5 POINTS) Setting up the S11 GTP-C Connection (Packet # 214 and #215) for particular UE (say UE-A): Similar to setting up a separate "logical" connection for each UE on the S1AP interface (eNB < --> MME), a separate "logical" GTP-C connections is created for each UE. On this logical connection (which is identified a pair of tunnel endpoint identifiers (TEIDs), one on the MME and the other on the SGW) all packets for a particular UE are carried. The creation of such a connection is done by messages "Create Session Request" (Packet #214) and "Create Session Response" (Packet # 215). In the Create Session Request the MME allocates a unique TEID for UE-A and provides this TEID to the SGW. The SGW subsequently will set the "Tunnel Endpoint Identifier" field to this value in the GTP-C header for all packets related to the UE-A when communicating with the MME. What is the value of the MME S11 GTP-C interface TEID for UE-A that the MME sends to SGW in Packet #214. Double-check in message 222 to make sure that the SGW sets the TEID in the Modify Message Response message header to this value when it talks to the MME.

Similarly in the Create Session Response the SGW allocates a unique TEID for UE-A and provides this TEID to the MME. The MME subsequently will set the "Tunnel Endpoint Identifier" field to this value in the GTP-C header for all packets related to the UE-A when communicating with the SGW. What is the value of the SGW S11/S4 GTP-C interface TEID for UE-A that the SGW sends to MME in Packet #215. Double-check in message 221 to make sure that the MME sets the TEID field in the Modify Message Request message header to this value when it talks to the SGW.

The pictorial representation for this is in Slide-28 of LTE Architecture lecture notes.

504112505 G. Selda UYANIK
Feburary 27, 2012

23/25

BLG609E - Special Topics: 4G Wideband Wireless Network Architectures
(Spring 2012)

Homework-2: Standards and Network Architecture

1. Look up DHCP specifications (eg. wikipedia), answer the following questions for EPC architecture, when the DHCP Server is part of the PGW. That is, the DHCP-client is in the UE and the DHCP Server is in the PGW: (8 POINTS)

   1. Draw the flow for DHCPv4 for a UE to get its IP address between the UE and P-GW (DHCP-Server)? (3 POINTS)

UE (DHCP Client) — DHCP Server (PGW)

Broadcasts a *DHCP Discovery Message*
(can also request its last-known IP address)

DHCP Discover →

The DHCP server manages a pool of IP addresses and information about client configuration parameters. After a proper request is received, it reserves an IP address for the client (with dynamic, automatic or static allocation): sends a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

← DHCP Offer

Requesting the offered address with a unicast message. A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer.

DHCP Request →

Final phase: ACK packet includes the lease duration and any other configuration information.

← DHCP ACK

[1]

   2. Using a network sniffer (eg. Wireshark) on your laptop, study the DHCPv4 interaction between your computer and a DHCP Server (eg in your DSL router) and provide a print-out of the interaction. (5 points)

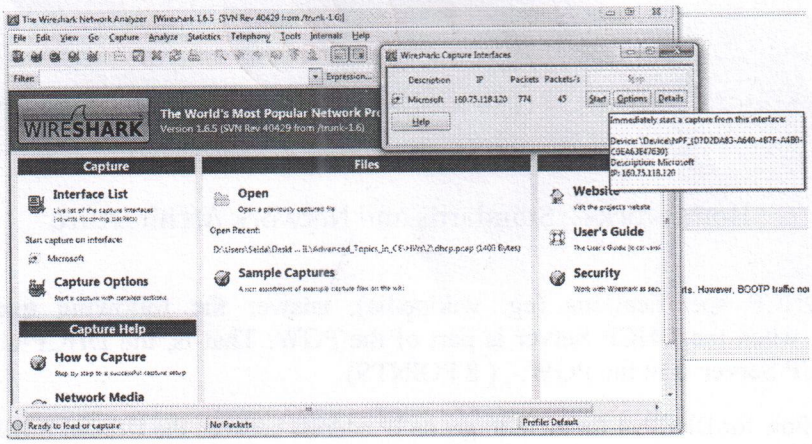
Wireshark is opened. The interface to be captured is chosen when wireless adapter was on. A capture was started. Then, the wireless adapter was closed during the capture process. No packets were captured in this period since there was no additional network connection like cabled Ethernet.

DORA : Discover, offer, Request, ACK , in some cases, notify → contains other configurations for PC (optional)
ack ←

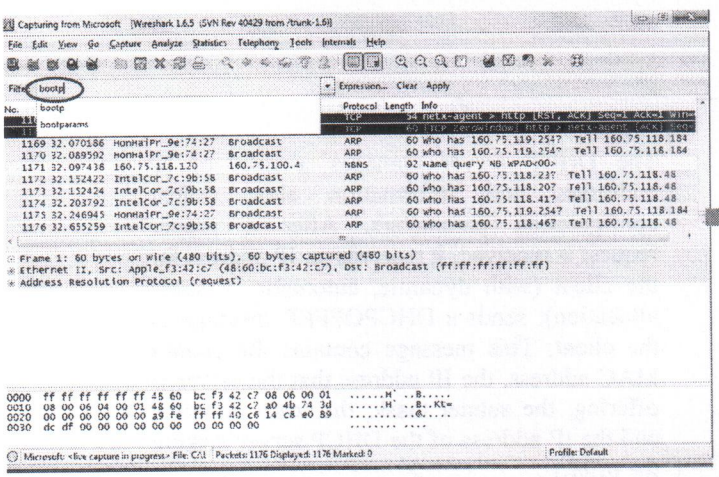
① → ← → ←

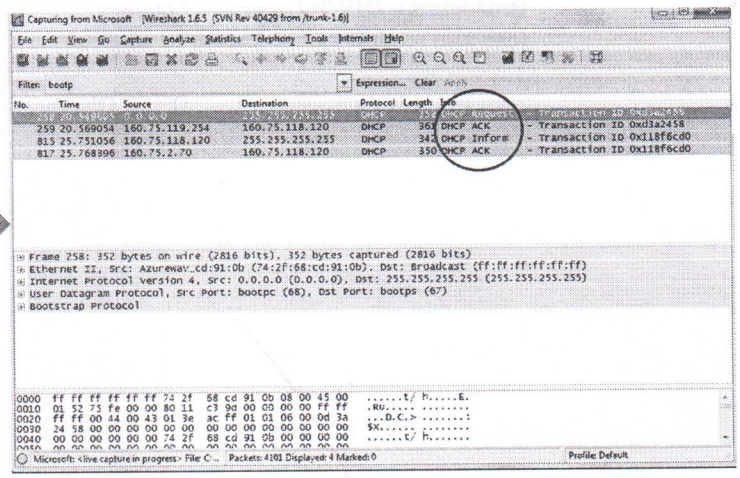
can come from multiple DHCP servers

goes to 1 DHCP server.

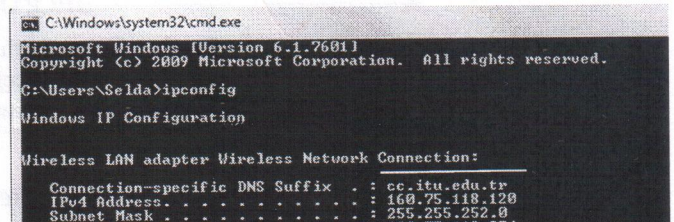


Then, wireless adapter was turned on again, during capture process in order to catch DHCP messages. Many packets were captured. A filter of "bootp" [2] showing only BOOTP packets (DHCP uses BOOTP as its transport protocol) was applied and resulting capture view:

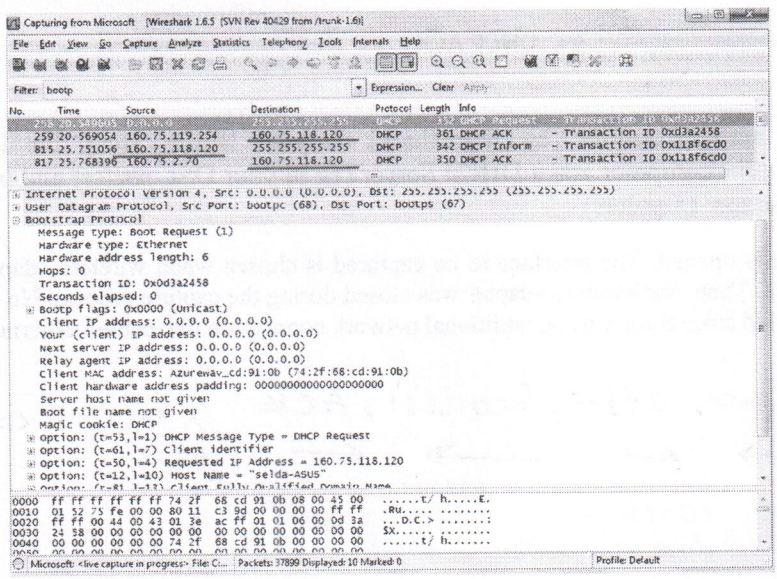




Request ≡ DHCP Discover bcast packet
ACK ≡ DHCP Offer
Inform ≡ DHCP Request
ACK ≡ DHCP ACK
IP address of 160.75.118.120 is retrieved via this process:



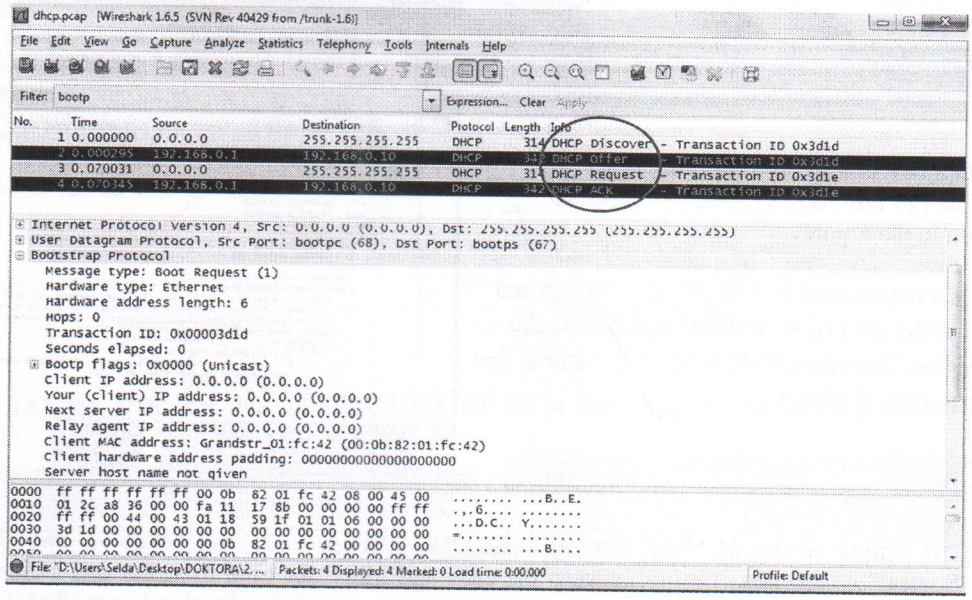
Bootstrap message details can also be seen:

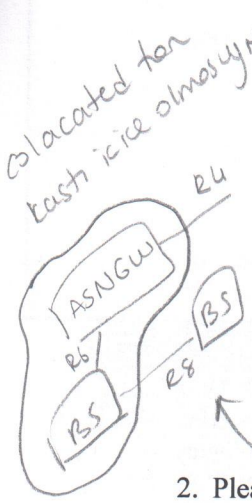


Capture process is saved into selda_capturedDHCP.pcap file.

504112505 G. Selda UYANIK
Feburary 27, 2012

Note: sample DHCP capture packet file retrieved from:
http://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=view&target=dhcp.pcap
is also examined and bootp filter gave more expected names for DHCP packets there:





2. Please answer the following question about WiMAX architecture: POINTS 5

a) ASN-GW and BS were always co-located, which one(s) of the reference points would disappear from the Network Reference Model (NRM)?

R4 interface that is used for both data and control signalling among differnet ASN-GWs would then disseppear. If BS-ASN-GW connection is not lost due to BS mobility since they are always co-lotcated (means no handoff), the data forwarding and controlling siganalling among differnet ASN-GW would not be needed.

b) The MME and the SGW together are approximately equivalent in functionality to which node in the WiMAX architecture?

MME is a control plane entity in LTE that controls authentication and idle mode mobility, SGW is a data plane entity handling inter eNB mobility and access to PGW, equivalant functionalities are performed by a single entity in WiMAX: ASNGW (both connects to Ha and AAA) [3]

3. The following questions are related to the file lte_attach.pcap which is provided on the yahoo groups site. Please download that file and use Wireshark (www.wireshark.org) to analyze the packets and answer the following questions. Also use your lecture notes on LTE architecture. The file includes packets on the S1-MME interface (eNB <--> MME) and on the S11 interface (MME < -- > SGW)

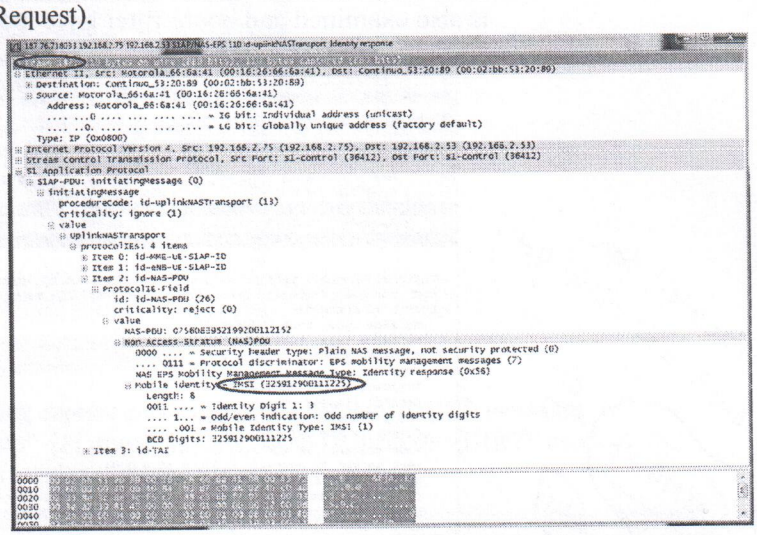
UE's IMSI (Packet #187): Packet# 187 is an S1AP (S1 Application Protocol) message (i.e message between eNB and MME) which encapsulates the "Identity Response" NAS (Non Access Stratum) message from the UE to the MME. Write down the IMSI of the UE? Assuming that the MCC is 3 digits long and MNC is also 3 digits long, what is the PLMN-ID of the operator of the UE? 2 POINTS

Background: In this file, the UE had previously attached to the network and had received a temporary identity from the MME, this identity is called Globally Unique Temporary Identity (GUTI). The UE had then switched-off (detached) from the network. The UE in the "Attach Request" (Packet #176) provides this temporary identity GUTI and not the IMSI. The MME in this case is not able to recognize the UE by the

GUTI (UE has probably moved from one area to another, eg the UE had previously attached to an MME is Maslak and is not attaching to an MME in Levent). Hence, the MME (in Levent) is now asking for the UE to provide its IMSI to the MME (Packet #186 Identity Request).

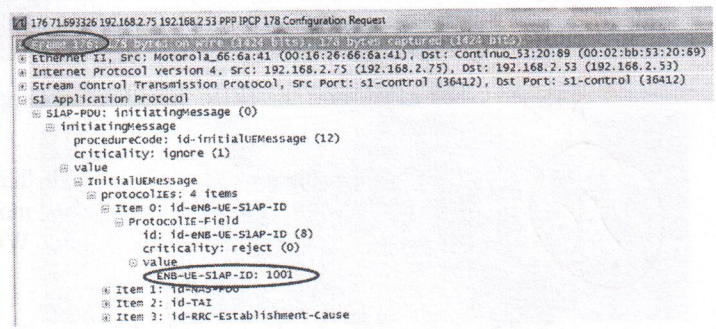
Packet #187 is looked in detail:
IMSI of the UE : 325912900111225
(as seen in the Figure)

IMSI is a sequence of PLMN (MMC + MNC) and MSIN of the UE [3]. PLMN is 6 digits acc to the description. Therefore, PLMN-ID of operator is first 6 digits and is: 325912

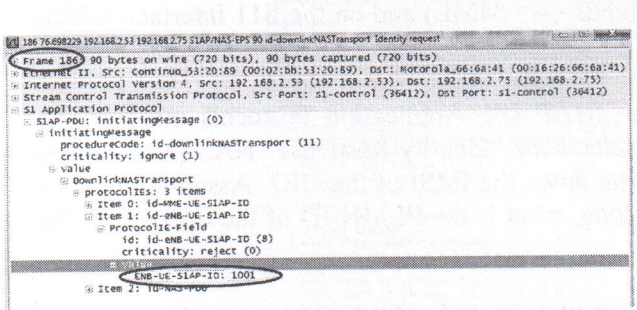


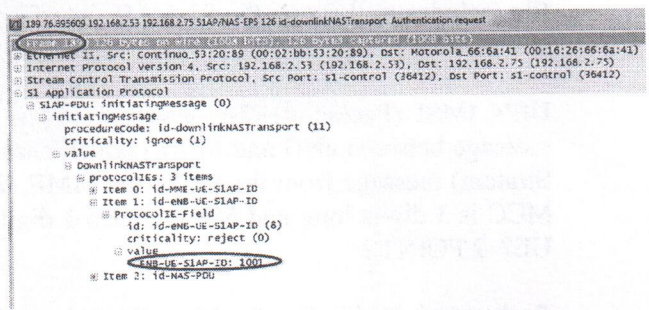
(5 POINTS) Setting up the S1-MME (S1AP) Connection (Packet # 176 and #186) for the UE (UE-A): A separate "logical" connection is setup between the eNB and MME for each user. On this logical connection, packets for only UE-A are sent. This logical connection runs on the S1 Application Layer (S1AP). This logical connection is identified by an S1AP identifier at the eNB side (called id-eNB-UE-S1AP-ID) and an S1AP identifier at the MME side (called id-MME-UE-S1AP-ID). At the eNB, to recognize packets from the MME that are related to UE-A, the eNB assigns a unique value to id-eNB-UE-S1AP-ID for UE-A. In the very first packet for UE-A that the eNB sends to the MME (packet #176 in our case), the eNB informs the MME about this Value. From this point onwards all packets for UE-A from the MME will set field id-eNB-UE-S1AP-ID to this value. What is the value of id-eNB-UE-S1AP-ID set by the eNB in Packet#176? Double-check that in message I86, the MME uses the same value when it talks to the eNB in message 186 (also message 189).

id-eNB-UE-S1AP-ID set by the eNB in Packet#176 : 1001



The MME uses the same value when it talks to the eNB in message 186 (also message 189):

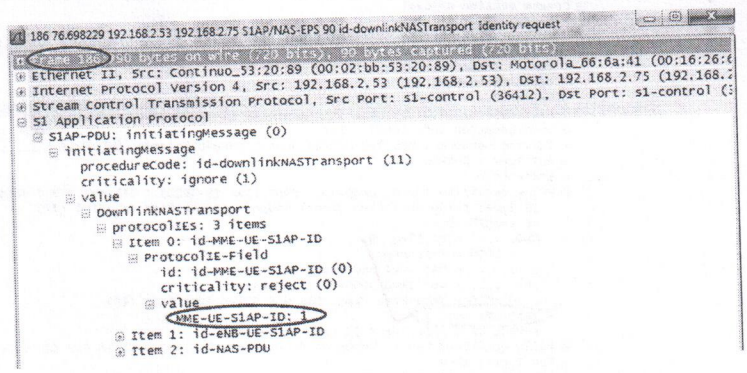




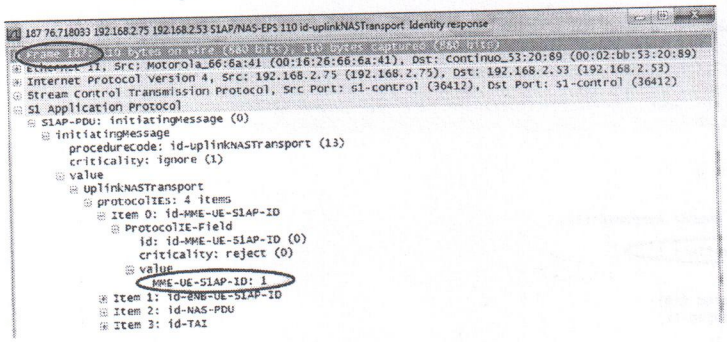
Similarly at the MME, to recognize packets from the eNB that are related to UE-A, the MME assigns a unique value to the id-MME-UE-S1AP-ID for UE-A. In the very first packet for UE-A that the MME sends to the eNB (packet #186 in our case), the MME informs the eNB about this value for id-MME-UE-S1AP-ID. From this

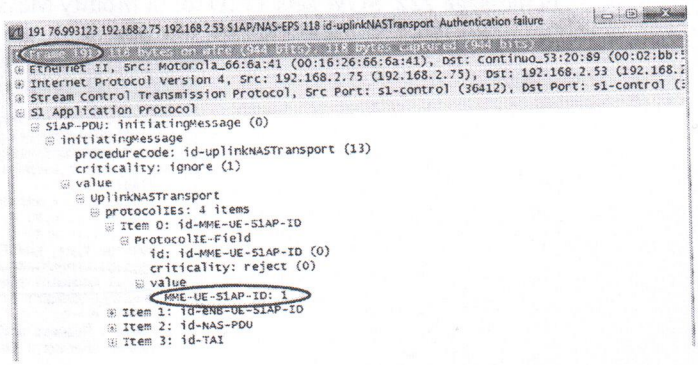
point onwards all packets for UE-A from the eNB will set id-MME-UE-S1AP-ID to this value. What is the value of id-MME-UE-S1AP-ID set by the MME in Packet#186? Double-check in message I87 to make sure that the eNB sets field id-MME-UE-S1AP-ID to this value for packets related to UE-A (also message 191).

Value of id-MME-UE-S1AP-ID set by the MME in Packet#186 is: 1

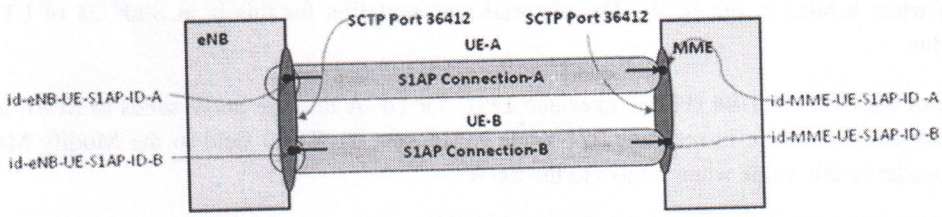


In message 187, the eNB sets field id-MME-UE-S1AP-ID to this value for packets related to UE-A (also message 191):



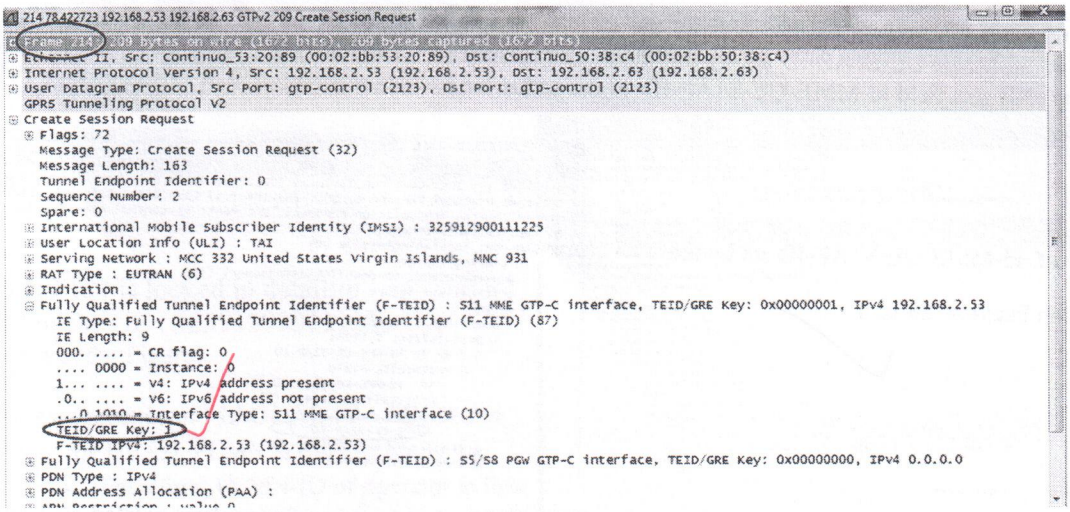


The following figure illustrates the concept. Hence, the "logical" connection for UE-A at S1AP layer is represented by (id-eNB-UES1AP-ID-A, id-eNB-UES1AP-ID-B). S1AP packets with these values in the appropriate field in the packet belong to this "logical connection". Creation of such a logical connection helps the eNB and MME to identify packets are related to a particular UE (UE-A, in our case).

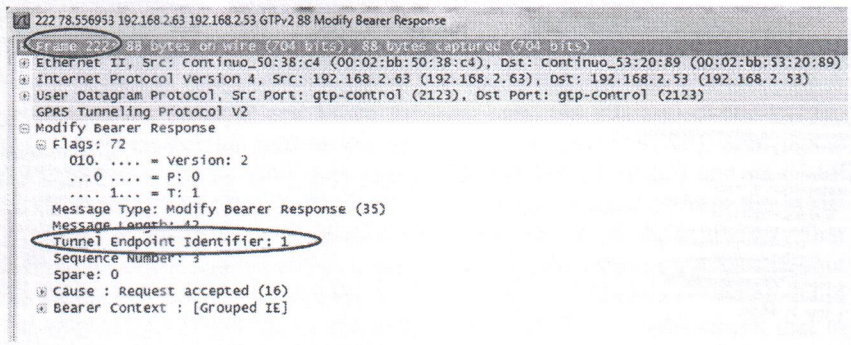


(5 POINTS) Setting up the S11 GTP-C Connection (Packet # 214 and #215) for particular UE (say UE-A): Similar to setting up a separate "logical" connection for each UE on the S1AP interface (eNB < --> MME), a separate "logical" GTP-C connections is created for each UE. On this logical connection (which is identified a pair of tunnel endpoint identifiers (TEIDs), one on the MME and the other on the SGW) all packets for a particular UE are carried. The creation of such a connection is done by messages "Create Session Request" (Packet #214) and "Create Session Response" (Packet # 215). In the Create Session Request the MME allocates a unique TEID for UE-A and provides this TEID to the SGW. The SGW subsequently will set the "Tunnel Endpoint Identifier" field to this value in the GTP-C header for all packets related to the UE-A when communicating with the MME. What is the value of the MME S11 GTP-C interface TEID for UE-A that the MME sends to SGW in Packet #214. Double-check in message 222 to make sure that the SGW sets the TEID in the Modify Message Response message header to this value when it talks to the MME.

The value of the MME S11 GTP-C interface TEID for UE-A that the MME sends to SGW in Packet #214: 1



In message 222, SGW sets TEID to: in Modify Message Response message header when it talks to the MME: 1



Similarly in the Create Session Response the SGW allocates a unique TEID for UE-A and provides this TEID to the MME. The MME subsequently will set the "Tunnel Endpoint Identifier" field to this value in the GTP-C header for all packets related to the UE-A when communicating with the SGW. What is the value of the SGW S11/S4 GTP-C interface TEID for UE-A that the SGW sends to MME in Packet #215. Double-check in message 221 to make sure that the MME sets the TEID field in the Modify Message Request message header to this value when it talks to the SGW. The pictorial representation for this is in Slide-28 of LTE Architecture lecture notes.

The value of the SGW S11/S4 GTP-C interface TEID for UE-A that the SGW sends to MME in Packet #215: 2147483649 and it is same in message 221 when MME sets the TEID field in the Modify Message Request message header to this value when it talks to the SGW: