TP5 : Les réseaux 4G/LTE (Partie1)

Objectifs :

1. Analyser les trames échangées entre un utilisateur mobile et une station eNB.
2. Récupérer les différent paramètre et identificateur d'un réseau 4G et du mobile.
3. Analyser les étapes de l'attachement du mobile au réseau LTE et Cœur.
4. Analyser l'étape de la récupération d'une adresse IP par un mobile.

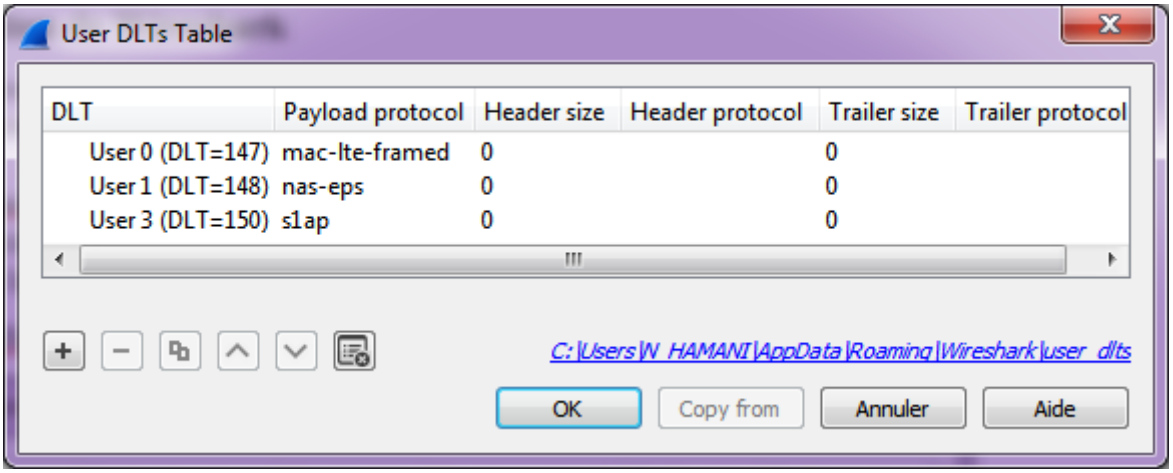
1- Préparation de Wireshark

Nous allons analyser des traces de réseaux cellulaire 4G en utilisant Wireshark. Ouvrir le fichier 4G-LTE.pcap

Wireshark nécessite une configuration pour afficher correctement les traces. Pour pouvoir analyser les traces, veuillez utiliser une version récente de Wireshark et faire les configurations suivantes :

- Preferences → Protocols → DLT_USER
- Edit Encapsulation Table
- Ajouter les entrées suivantes (+) :

Pour l'UE et l'eNodeB on rajoute *mac-lte-framed* et *nas-eps* et pour le l'EPC on rajoute *s1ap*.



2- Information sur la station de base

Sélectionner la première trame RRC

1. Quel est le canal utilisé ? BCCH
2. Quel est le rôle de ce canal ? Diffusion d'informations de contrôle sur la cellule.
3. De quel type est cette trame ? Type signalisation

Remarque : il existe deux types des trames, donnes ou signalisation (la signalisation est pour partager des informations de routage).

La trame est envoyée en plusieurs bloc. Nous allons nous intéresser à la trame concernant « Information System ». Dans LTE, le System Information Blocks, SIB transporte des informations qui permettent à l'UE d'accéder à la cellule. Il existe 13 types.

L'UE lit les information système dans le mode "RRC Idle" pour avoir les paramètres nécessaires pour la sélection et la réélection de la cellule et les paramètres d'accès au réseau.

Les information système sont diffusées en utilisant les Master Information Block (MIB) et une série de System Information Blocks (SIB).

4. Quel est le type de ce SIB ? Type 3
5. C'est quoi son rôle (recherche sur internet[1]) ? transporte des informations de resélection de cellule ainsi que des informations de resélection de cellule intrafréquence.
6. Quel est l'identificateur de l'eNB ? eNB ID = 144
7. Quel est l'identificateur de la cellule ? Cell ID = 32202

3- Information sur l'opérateur

Sélectionner la 2ème trame RRC qui vient juste après

1. Quel est le type de ce SIB ? Type 7
2. Naviguer dans les informations de la trame et pointer l'identité du PLMN. Que représente le PLMN ? Public Land Mobile Network, signifie un réseau mobile public présent dans un pays donné.
3. Quelle est la valeur du MCC ? MCC = 208
4. Que représente le MMC ? Mobile Country Code
5. Quelle est la valeur du MNC ? MNC = 10
6. Que représente le MNC ? Mobile Network Code
7. Chercher à quoi correspondent le MCC et le MNC ? c'est des chiffres qui font différencier entre les réseaux mobiles au monde (MCC) et au même pays (MNC).
   MCC = 208 = code du France.
   MNC = 10 en France = opérateur SFR (société française de radiotéléphonie).
8. Quelle est la valeur de l'identificateur du PLMN ? PLMN = 208 10
9. Déduire l'ID globale de l'eNB qui le distingue d'une façon unique dans le monde.
   eNB-ID Global = [208 10 144]

4- La procédure d'attachement

Les échanges entre l'UE et l'eNB sont caractérisés par les mentions : UL (Uplink) de l'UE vers l'eNB ou DL (Downlink) de l'eNB vers l'UE.

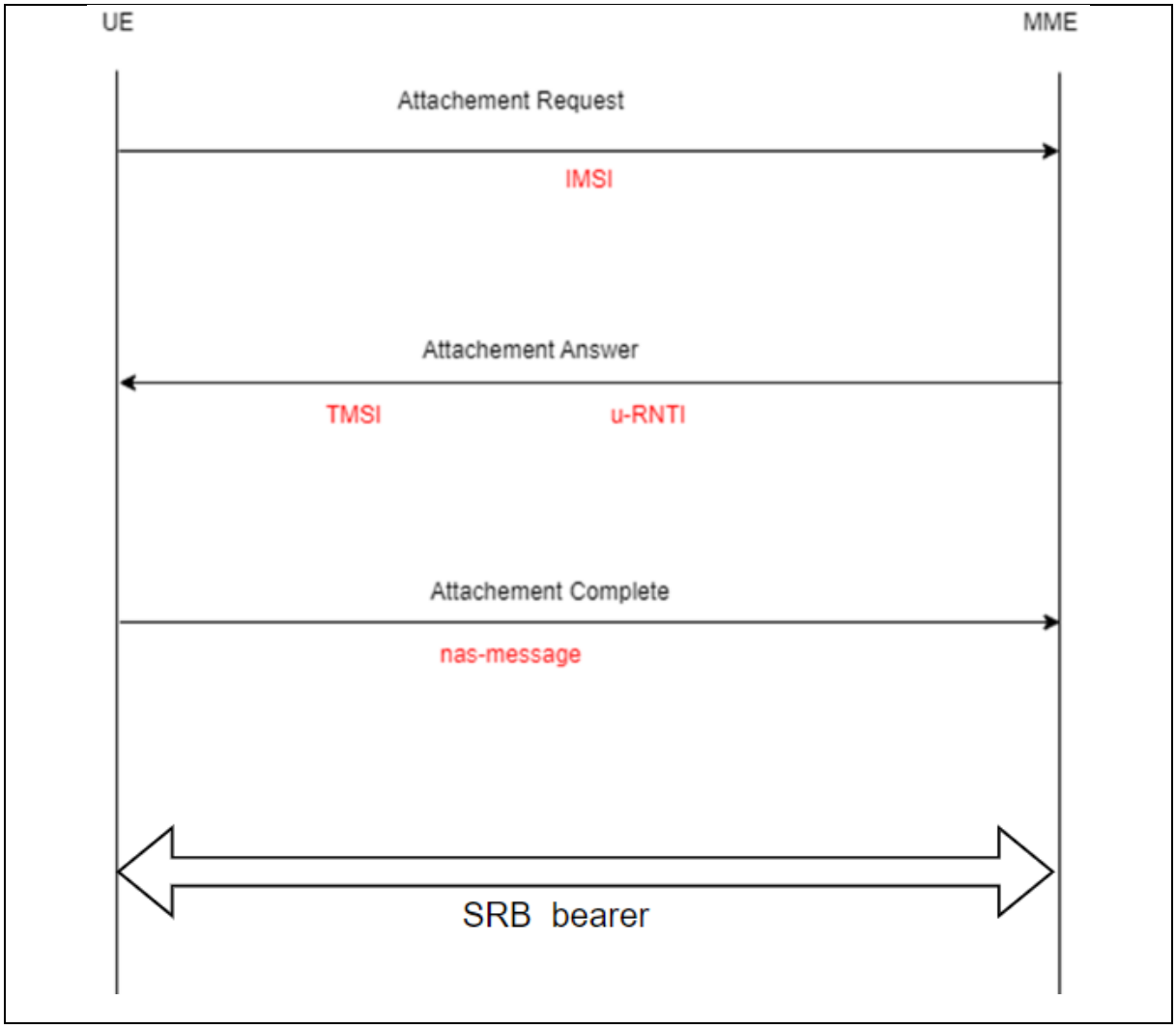
1. D'une manière générale, que se passe-t-il quand vous allumez votre téléphone (avant la procédure d'attachement) ? le téléphone essaye de détecter les eNB dans son endroit a partir des signaux qu'ils diffusent.

[1] https://www.rfwireless-world.com/Terminology/LTE-MIB-SIB-system-information-blocks.html

2. Quelle est la 1ère étape de communication l'UE aborde avec l'eNB ? C'est la « demande de connexion RCC » ou on peut dire l'identification, dont le UE doit fournir son identifiant d'équipement (IMEI) et de la carte SIM (IMSI).
3. A quel moment le mobile a déclenché cette procédure dans la trace Wireshark ? Au moment de l'envoi de la trame 30 : 0.387565s
4. Quel est l'objectif de la procédure d'attachement ? Enregistrement sur le réseau mobile afin d'avoir une adresse IP qui permet par la suite de connecter au réseau internet (au monde).
5. Quel est le canal utilisé ? CCCH
6. Quelle est la caractéristique principale de ce type de canal ? Transmission de la signalisation si on ne peut pas utiliser un canal dédié.
7. Pourquoi L'UE a fait recours à ce type de canal ? Car il Ya pas un canal de communication entre les deux (UE et eNB).
8. Il s'agit de quel message ? le message numéro 32.
9. Qui est l'initiateur du message et justifier ? C'est le UE car c'est en mode U (Uplink) qui signifier de UE vers eNB.
10. Quelle est l'identité utilisé par l'UE et quelle est sa valeur ? TMSI = 24203036
11. Pourquoi c'est le TMSI qui envoyé et n'est pas l'IMSI ? On limite l'utilisation du IMSI seulement pour la 1èr phase d'authentification, car le IMSI est une information critique, et si cette valeur est connue alors l'UE va être facilement suivie.
12. Quelle est la raison de l'utilisation de TMSI au lieu de l'IMSI ? sécurité, c'est pour ça on utilise de valeurs qui sont temporaires (mise à jour de la sécurité à chaque foix).
13. L'identité de la zone est composée du MNC et du code LAC[2] (Location Area Code)[3]. Donner l'identité de la zone actuelle ? LAC = 12102
14. Quelle est la raison de cette demande d'attachement ? La demande d'attachement a pour but de permettre à un dispositif mobile de s'inscrire et de s'identifier auprès d'un réseau mobile pour obtenir une connexion de données ou de voix.
15. Localiser le moment de la réponse d'attachement (instant) ? Au moment de l'envoi de la trame 52 : 4.442s
16. Il s'agit de quel message ? « DownlinkDirectTransfer »
17. Qui est l'origine de la réponse ? C'est le MME.
18. Vérifier les données de l'identification de l'UE. Est-ce que ce sont les mêmes que celles du la requête d'attachement ? Oui.
19. L'eNB affecte à l'UE un identificateur unique dans la cellule u-RNTI (UTRAN RNTI) qui est une composition de deux valeurs : SRNC[4] (Serving Radio Network Controller) et S-RNTI (Serving Radio Network Temporary Identifier). Déterminer la valeur de u-RNTI ? u-RNTI = SRNC S-RNTI = 0x09008763 en hexa ; SRNC = 144 décimal
    S-RNTI= 34659

[2] Location Area Code, also learned from the SIBs
[3] https://www.cellmapper.net/
[4] https://rncmobile.net

20. Dans le même message l'UE envoie également le « ***scrambling code*** » qui est un code qui permet à l'eNB de communiquer avec plusieurs UE. L'eNB reçoit plusieurs ondes radio à la fois de plusieurs UE, en utilisant le scrambling code elle parvient à différencier les ondes. Exemple : remplacer les bit 0 et 1 par d'autre séquence 1→ 00110, 0→11100.
    Cette opération fait partie de la négociation des paramètres radio.
    Quel est le scrambling code attribué par l'eNB[5] ? scrambling code = 1117851
21. Quel est le dernier message d'attachement envoyé ? Message N° 53 (Attache complet).
22. Quel est le canal utilisé ? DCCH
23. Pourquoi le type du canal de communication utilisé a changé ? pour améliorer l'efficacité de la communication et la capacité du réseau (envoi des donnes et pas seulement des signalisations).
24. Globalement, quelles sont les informations envoyées par l'UE dans ce message ? Informations pour vérifier l'intégrité, NAS-message.
25. Donner le diagramme résumé de la procédure d'attachement capturée et les principaux paramètres échangé entre l'UE et l'eNB et indiquer quel radio bearer est établi.



[5] Chercher dans FDD (Frequency Division Duplex)

26. Question de réflexion : Pourquoi dans le message NAS attach Request on envoie également le PLMN ?

    Le message NAS Attach Request est utilisé pour demander une connexion à un réseau mobile. Le PLMN (Public Land Mobile Network) est l'identifiant unique du réseau mobile auquel l'utilisateur souhaite se connecter. Il est donc nécessaire d'inclure le PLMN dans la demande d'attachement pour que le réseau mobile sache à quel réseau l'utilisateur souhaite se connecter.

TP5 : Les réseaux 4G/LTE (Part 2-suite)

Objectifs :

1. Analyser les trames échangées entre un utilisateur mobile et une station eNB.
2. Récupérer les différent paramètre et identificateur d'un réseau 4G et du mobile.
3. Analyser les étapes de l'attachement du mobile au réseau LTE et Cœur.
4. Analyser l'étape de la récupération d'une adresse IP par un mobile.

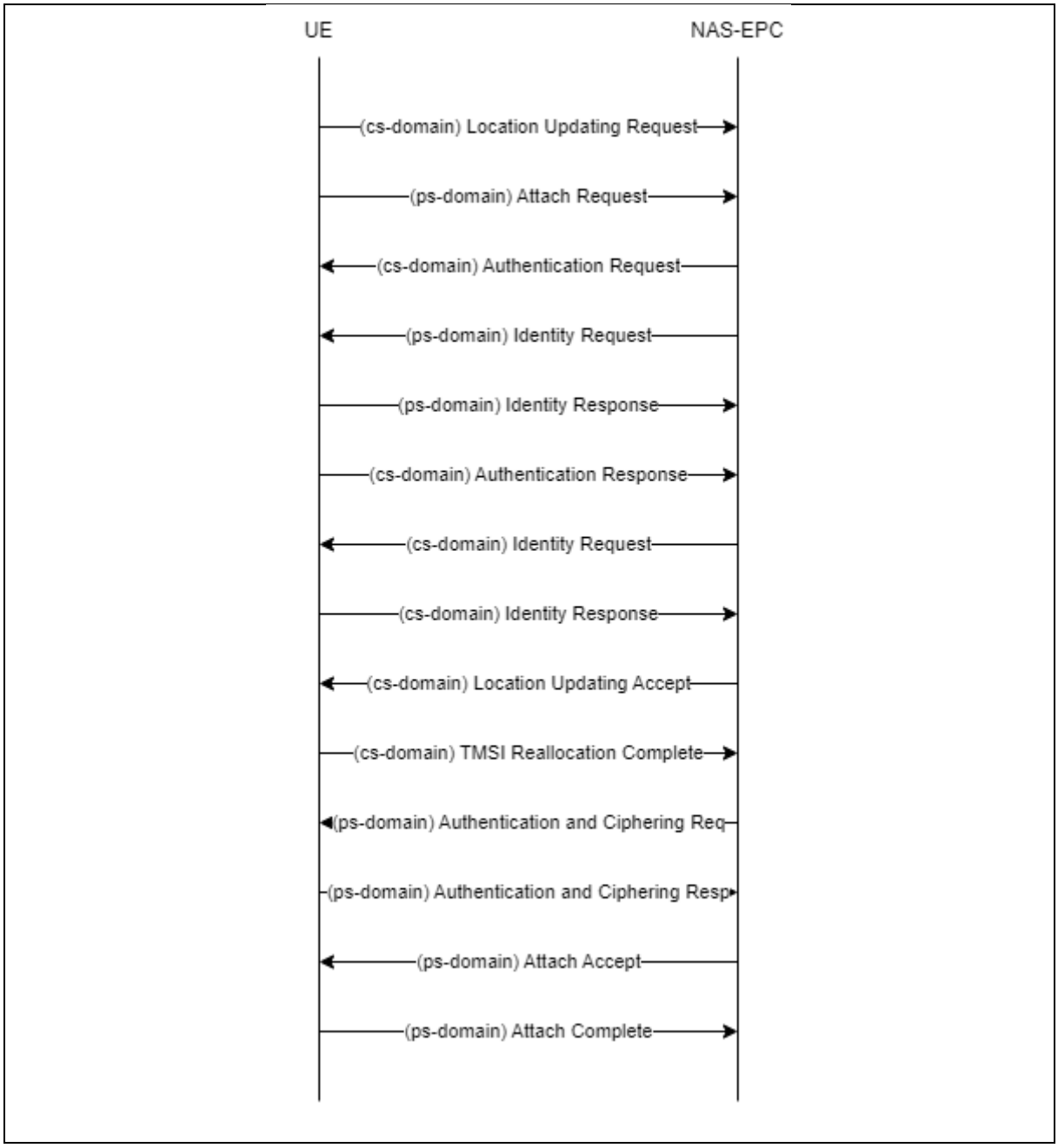
1- Echange de données

Analysons le message à l'instant 0.60 « InitialDIrectTransfer ». Le mot Direct veut dire que l'UE envoi une donnée directement vers le réseau EPC (Evolved Packet Core).

1. Que représente le premier message (cs-domain : Circuit-Switched)[1]? une demande d'établissement de connexion, Il contient des informations sur l'appelant et le destinataire, ainsi que des informations sur les services de communication souhaités.
2. Que veut dire la mention NAS-Message ? Le NAS (strate de non accès) représente un ensemble de protocoles qui s'établit entre l'UE et le réseau cœur. Le NAS permet l'échange d'information de contrôle ou de données quelques soit l'accès radio.
3. Il est de quelle direction ? de l'UE vers l'eNB car le canal utilisé est U (uplink).
4. Quelles sont les principales informations échangées pour assurer cette opération ? l'identité de l'appelant (UE), l'identité du destinataire (eNB).
5. Quelle identité l'UE associé en réponse à la 1ère demande d'identité ? l'UE doit d'abord fournir un identifiant temporaire, appelé IMSI (International Mobile Subscriber Identity), qui est stocké sur la carte SIM.
6. Quelle est sa valeur ? IMSI = 208109876543120
7. Quelle identité l'UE associé en réponse à la 2ème demande d'identité ? MSISDN (Mobile Subscriber Integrated Services Digital Network Number).
8. Quelle est sa valeur ? IMEIe = 3957705957856664?4
9. A quoi sert cet identifiant ? C'est un numéro identifier de téléphone dans le monde.

[1] It send two ***InitialDirectTransfer*** : one that will be sent to the CS (**Circuit-Switched**) domain, which is the core network for voice traffic and one to the PS (**Packet-Switched**) domain, which is the core network for data traffic.

10. Etablir un diagramme d'échange entre l'UE et le NAS à partir des messages avec l'EPC (les messages portant la mention DTAP) jusqu'à l'instant 4.6 l'instant 4.62 en précisant si l'opération concerne l'attachement au réseau de données ou bien de la téléphonie.



11. Vérifier le TMSI utilisé par l'UE lors de la requête Location Updating Request et celui lor de la réponse Location Updating Accept ? Ce n'est pas le même, il a été changé.
12. Pourquoi il y a eu une réallocation d'un TMSI ? Il y a eu une réallocation d'un TMSI (Temporary Mobile Subscriber Identity) lorsque l'identité d'un abonné mobile a été modifiée pour des raisons de sécurité ou pour éviter des conflits d'identité.

2- Accès internet

Aller sur le message de la ligne 37.71 (6.49). Le message service request indique que l'UE demande un accès internet. Dans ce cas il doit demander auprès une adresse IP. Utiliser le filtre suivant :

(gsmtap.rrc_sub_type==0||gsmtap.rrc_sub_type==1)&&!(rrc.message==8)

Le message Activate PDP Context consiste à échanger les paramètres de connexion.

1. Dans la requête, l'UE précise le nom du P-GW (ANP : Acces Point Name) auquel il est associé, quel est ce nom ? APN = websfr
2. Inspecter la réponse de l'EPC et déterminer les paramètre IP du mobile lui permettant d'accéder à internet. Adresse IPv4 : 10.175.144.168, Primary DNS server IP adresse : 172.20.2.39 et Secondary DNS server IP adresse : 172.20.2.10.