**TP5 : Les réseaux 4G/LTE (Partie1)**

**Objectifs :**

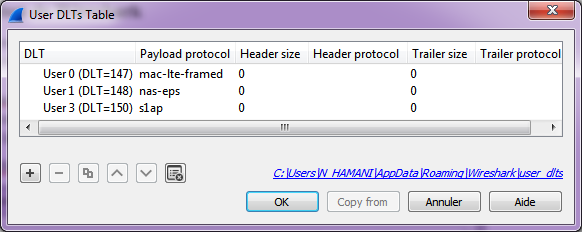
1. Analyser les trames échangées entre un utilisateur mobile et une station eNB.
2. Récupérer les différent paramètre et identificateur d’un réseau 4G et du mobile.
3. Analyser les étapes de l’attachement du mobile au réseau LTE et Cœur.
4. Analyser l’étape de la récupération d’une adresse IP par un mobile.
5. **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*.



1. **Information sur la station de base**

Sélectionner la première trame RRC

1. Quel est le canal utilisé ? Cliquez ou appuyez ici pour entrer du texte.
2. Quel est le rôle de ce canal ? Cliquez ou appuyez ici pour entrer du texte.
3. De quel type est cette trame ? Cliquez ou appuyez ici pour entrer du texte.

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).

1. Quel est le type de ce SIB ? Cliquez ou appuyez ici pour entrer du texte.
2. C’est quoi son rôle (recherche sur internet[[1]](#footnote-1)) ? Cliquez ou appuyez ici pour entrer du texte.
3. Quel est l’identificateur de l’eNB ? Cliquez ou appuyez ici pour entrer du texte.
4. Quel est l’identificateur de la cellule ? Cliquez ou appuyez ici pour entrer du texte.
5. **Information sur l’opérateur**

Sélectionner la 2ème trame RRC qui vient juste après

1. Quel est le type de ce SIB ? Cliquez ou appuyez ici pour entrer du texte.
2. Naviguer dans les informations de la trame et pointer l’identité du PLMN. Que représente le PLMN ? Cliquez ou appuyez ici pour entrer du texte.
3. Quelle est la valeur du MCC ? Cliquez ou appuyez ici pour entrer du texte.
4. Que représente le MMC ? Cliquez ou appuyez ici pour entrer du texte.
5. Quelle est la valeur du MNC ? Cliquez ou appuyez ici pour entrer du texte.
6. Que représente le MNC ? Cliquez ou appuyez ici pour entrer du texte.
7. Chercher à quoi correspondent le MCC et le MNC ? Cliquez ou appuyez ici pour entrer du texte.
8. Quelle est la valeur de l’identificateur du PLMN ? Cliquez ou appuyez ici pour entrer du texte.
9. Déduire l’ID globale de l’eNB qui le distingue d’une façon unique dans le monde. Cliquez ou appuyez ici pour entrer du texte.
10. **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) ? Cliquez ou appuyez ici pour entrer du texte.
2. Quelle est la 1ère étape de communication l’UE aborde avec l’eNB ? Cliquez ou appuyez ici pour entrer du texte.
3. A quel moment le mobile a déclenché cette procédure dans la trace Wireshark ? Cliquez ou appuyez ici pour entrer du texte.
4. Quel est l’objectif de la procédure d’attachement ? Cliquez ou appuyez ici pour entrer du texte.
5. Quel est le canal utilisé ? Cliquez ou appuyez ici pour entrer du texte.
6. Quelle est la caractéristique principale de ce type de canal ? Cliquez ou appuyez ici pour entrer du texte.
7. Pourquoi L’UE a fait recours à ce type de canal ? Cliquez ou appuyez ici pour entrer du texte..
8. Il s’agit de quel message ? Cliquez ou appuyez ici pour entrer du texte.
9. Qui est l’initiateur du message et justifier ? Cliquez ou appuyez ici pour entrer du texte.
10. Quelle est l’identité utilisé par l’UE et quelle est sa valeur ? Cliquez ou appuyez ici pour entrer du texte.
11. Pourquoi c’est le TMSI qui envoyé et n’est pas l’IMSI ? Cliquez ou appuyez ici pour entrer du texte.
12. Quelle est la raison de l’utilisation de TMSI au lieu de l’IMSI ? sécurité
13. L’identité de la zone est composée du NMC et du code LAC[[2]](#footnote-2) (Location Area Code)[[3]](#footnote-3). Donner l’identité de la zone actuelle ? Cliquez ou appuyez ici pour entrer du texte.
14. Quelle est la raison de cette demande d’attachement ? Cliquez ou appuyez ici pour entrer du texte.
15. Localiser le moment de la réponse d’attachement (instant) ? Cliquez ou appuyez ici pour entrer du texte.
16. Il s’agit de quel message ? Cliquez ou appuyez ici pour entrer du texte.
17. Qui est l’origine de la réponse ? Cliquez ou appuyez ici pour entrer du texte.
18. Vérifier les données de l’identification de l’UE. Est-ce que ce sont les mêmes que celles du la requête d’attachement ? Cliquez ou appuyez ici pour entrer du texte.
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]](#footnote-4) (Serving Radio Network Controller) et S-RNTI (Serving Radio Network Temporary Identifier). Déterminer la valeur de u-RNTI ? Cliquez ou appuyez ici pour entrer du texte.
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 déférencier 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 scramblig code attribué par l’eNB[[5]](#footnote-5) ? Cliquez ou appuyez ici pour entrer du texte.

1. Quel est le dernier message d’attachement envoyé ? Cliquez ou appuyez ici pour entrer du texte.
2. Quel est le canal utilisé ? Cliquez ou appuyez ici pour entrer du texte.
3. Pour le type du canal de communication utilisé a changé ? Le ca Cliquez ou appuyez ici pour entrer du texte.
4. Globalement, quelles sont les informations envoyées par l’UE dans ce message ? Cliquez ou appuyez ici pour entrer du texte.
5. 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.
6. Question de réflexion : Pourquoi dans le message NAS attach Request on envoie également le PLMN ? Cliquez ou appuyez ici pour entrer du texte.

1. https://www.rfwireless-world.com/Terminology/LTE-MIB-SIB-system-information-blocks.html [↑](#footnote-ref-1)
2. Location Area Code, also learned from the SIBs [↑](#footnote-ref-2)
3. https://www.cellmapper.net/ [↑](#footnote-ref-3)
4. https://rncmobile.net [↑](#footnote-ref-4)
5. Chercher dans FDD (Frequency Division Duplex) [↑](#footnote-ref-5)