Catalogue de Formations 5G EFORT 2026

Table des matières

Formations EFORT

EFORT (**E**tudes et **FOR**mations en **T**élécommunication) est une société de formation créée en 1998 et spécialisée dans le domaine des réseaux et services de télécommunication.

Des experts de premier plan

Les animateurs/concepteurs des cours EFORT sont des spécialistes reconnus dans leur domaine. Ils sont responsables de projets d'avant-garde pour de grandes entreprises, experts connus dans le monde de la recherche et généralement auteurs d'ouvrages dans leur domaine de compétence. Pédagogues hors pair, ils savent faire la synthèse de leur expérience pour en tirer enseignements et démarches nouvelles.

Une orientation opérationnelle

Les cours ont lieu sous forme de séminaires. L'exposé des concepts, des architectures, des produits est confronté en permanence à l'application pratique. Les études de cas sont issues de projets réalisés par les animateurs. Elles permettent d'aborder les difficultés techniques mais aussi organisationnelles.

Nos clients

Nous comptons parmi nos clients dans le domaine de la formation Intra-entreprise les sociétés suivantes.
Opérateurs : Groupe Orange, SFR, Bouygues Telecom, Telefonica Spain, Verizon Wireless, Vodafone UK, Swisscom, Telecom Argentina, Telecom Italia, Entel PCS, Etecsa, Telmex, Telma, Sonatel, Croatian Telecom, Monaco Telecom, Proximus, Telenet, BICS, Onatel, Completel, UNE, INWI, OPT, MTN, Viti, Telna, Andorra Telecom.
Constructeurs : Nokia, Cisco, Oracle, Ericsson, Fujitsu, Bull, IBM, Hewlett Packard, Avaya, Thomson Multimedia, Sofrecom, Keymile, Comverse, Cirpack, Genesys, eServGlobal, NSoft, EXFO, Viavi, Intel, Expandium, Sierra Wireless.
Sociétés de service et Utilisateurs : EDF, La Française des Jeux, Air France, SNCF, RATP, Swatch, Carrefour, Groupe ESR, AFD Technologies, Alten, Altran, Atos, Technoserv, SII, Setelia, CAP GEMINI, Ercom, GMV, T&T Consulting.
Centres de Recherche : Cintel, Cenet, Itba, Cmtl, Esmt.

Organisation des cours

Les formations inter-entreprises sont organisées à Paris.
Les formations intra-entreprise sont organisées dans votre entreprise en fonction du profil des participants.
Les formations intra-entreprise peuvent être assurées en **français**, **anglais** ou **espagnol**.
Notre site WEB informant des formations inter et intra entreprises dispensées par EFORT est régulièrement mis à jour : http://www.efort.fr

Pour toute demande d'information, n'hésitez pas de contacter :
Simon ZNATY, EFORT
Tel : +33672193726
E-mail : sznaty@efort.com

5G Edge Computing : Architecture, Déploiement et Services Associés

Durée : 2 jours

Objectifs : Comprendre l'architecture edge computing dans le contexte de la 5G SA basée sur les standards ETSI et 3GPP ainsi que l'architecture 5G SA Media Streaming qui peut être considérée comme un exemple d'architecture qui utilise l'Edge Computing.

Public : Ingénieur télécom et IT, architecte télécom et IT, chef de projet télécom et IT

Pré-requis : Connaissance minimum du réseau data mobile

Le cloud computing est un mode de traitement des données informatiques qui repose sur l'utilisation de data centers (centres de données) pour traiter, analyser et conserver les données. L'information transite donc en permanence entre l'utilisateur et les data centers.
Actuellement, le cloud computing reste la méthode de traitement de données privilégiée par beaucoup.

Le cloud computing présente deux inconvénients majeurs :
• Le temps de latence : la position géographique des data centers est souvent éloignée du point d'entrée des données. Il y a donc un temps de latence dans le traitement inacceptable pour des applications demandant une latence très courte comme le transport autonome.
• L'utilisation de la bande passante : les communications incessantes entre serveurs et utilisateurs utilisent la bande passante et pourraient, à terme la saturer. Les contraintes en matière de scalabilité sont donc bien présentes.

L'edge computing est un mode du traitement de données qui vise à effectuer les opérations au plus proche de la source des données. Les calculs prennent place à la périphérie du réseau ce qui diminue les temps de latence. L'edge computing implique donc une infrastructure locale sous forme de edge data centers.
Une telle infrastructure nécessite l'utilisation de normes communes et de bonnes pratiques pour garantir la disponibilité des applications aux utilisateurs et fournir un cadre de référence aux développeurs pour développer des applications compatibles.

Cette formation présente le concept de Edge Computing, présente les architectures Edge Computing ETSI et 3GPP correspondantes, leur déploiement, les procédures associées et les modèles de connectivité pour l'Edge Computing en 5G SA et les enablers pour leur mise en œuvre.

Cette formation présente aussi l'architecture media streaming 5G (5GMS) et l'utilisation 5GMS notamment dans le contexte Edge Computing.

1. Introduction à Edge Computing

1.1. Définition de l'edge computing
1.2. Avantages de l'Edge Computing
1.3. Domaines d'application de l'Edge Computing
1.4. Device edge computing aware versus Device edge computing unaware
1.5. Mobilité Edge Computing versus mobilité radiomobile
1.6. Acteurs de l'edge computing
    1.6.1. ASP : Application Service Provider
    1.6.2. ECSP : Edge Computing Service Provider
    1.6.3. CSP : Communications Service Provider
    1.6.4. Fonctions prises en charge par chaque acteur dans l'architecture edge computing
1.7. Les différents types de Edge Computing
    1.7.1. Device edge
    1.7.2. On-premise edge
    1.7.3. CSP telco edge
    1.7.4. Extended public cloud edge

2. Framework Edge Computing ETSI appelé MEC (Multi-Access Edge Computing)
    2.1. MEC host
        2.1.1. MEC platform
        2.1.2. MEC app
        2.1.3. Infrastructure de virtualisaiton
    2.2. MEC system level management
        2.3. MEC host level management
        2.4. Interfaces entre les entités de l'architecture
        2.5. Procédures MEC

3. Architecture Edge Computing 3GPP
    3.1. Fonctionnalités EDGEAPP (Architecture for enabling Edge Applications)
    3.2. AC (Application Client)
    3.3. EEC (Edge Enabler Client)
    3.4. EES (Edge Enabler Server)
    3.5. EAS (Edge Application Server)
    3.6. ECS (Edge Configuration Server)
    3.7. Interfaces EDGE entre les entités de l'architecture : EDGE 1 à EDGE 9
    3.8. Identités Edge Computing
        3.8.1. ACID
        3.8.2. EECID
        3.8.3. EASID
        3.8.4. EESID
        3.8.5. UEID
        3.8.6. EECContextID
    3.9. Modèles de déploiement possibles de l'architecture Edge Computing 3GPP
    3.10. Comparaison entre l'architecture MEC ETSI et l'architecture Edge Computing 3GPP

4. Procédures Edge Computing 3GPP
    4.1. Obtention des informations de configuration incluant les adresses d'ECS par l'EEC lors de l'activation d'une session PDU
    4.2. Découverte des EES par l'EEC auprès de l'ECS

4.3. Enregistrement de l'EEC à l'EES
4.4. Enregistrement de l'EAS à l'EES
4.5. Enregistrement de l'EAS à l'ECS
4.6. Découverte des EAS par l'EEC auprès de l'EES
4.7. Scénarios d'Application Context Relocation (ACR)
4.8. Souscriptions aux événements d'ACR par l'EEC auprès de l'EES
4.9. Echange de contexte de l'EEC entre EES source et EES cible
4.10. APIs exposées par le réseau 5G SA via la NEF ou la PCF à l'architecture Edge Computing 3GPP et procédures associées
4.10.1. API AF Traffic Influence
4.10.2. API UE Location
4.10.3. API UE Identifier
4.10.4. AF Session With QoS
4.10.5. API UE Expected Behavior

5. Modèles de connectivité pour l'Edge Computing 3GPP et enablers pour les mettre en œuvre
5.1. Modèles de connectivité possibles
5.1.1. Distributed Anchor point
5.1.2. Session breakout
5.1.3. Multiple PDU sessions
5.2. Modes SSC 1, 2 et 3
5.2.1. Différentes entre les modes SSC 1, 2 et 3
5.2.2. Modes SSC et préservation d'adresse IP
5.2.3. Scénarios de mobilité et reconfiguration de la session PDU en mode SSC 2 et SSC 3
5.2.4. DNN et LADN (Local Access Data Network)
5.3. ULCL et BP
5.3.1. Session PDU avec ULCL (Uplink Classifier)
5.3.2. Session PDU avec BP (Branching Point)
5.3.3. Scénarios de mobilité et reconfiguration de la session PDU avec ULCL et BP
5.4. Différences entre ULCL et BP
5.5. EASDF (EAS Discovery Function) pour la prise en charge des messages DNS
5.6. EAS IP Replacement

6. Interception légale Edge Computing

7. Architecture 5GMS (5G Media Streaming
7.1. 5GMS Client
7.2. AF
7.3. AS
7.4. Interface entre les composants de l'architecture
7.5. Architecture 5GMSd
7.6. Architecture 5GMSu
7.7. Intrégration d'Edge Computing dans 5GMS
7.8. Intégration d'eMBMS dans 5GMS
7.9. Configuration du 5GMS Client

7.10. Consumption reporting
7.11. Metrics reporting

5G FRMCS : Futur Railway Mobile Communication System

Durée : 2 jours

Objectifs : Présenter FRMCS, clarifier l'apport de la 5G au domaine ferroviaire, comparer FRMCS à GSM-R, montrer la relation entre FRMCS et MCX (Mission Critical Communication), décrire l'architecture et les services FRMCS.

Public : Ingénieur télécom, architecte télécom, chef de projet télécom

Pré-requis : Connaissance minimum du réseau 5G

FRMCS (Future Railway Mobile Communication System) est le système de communication mobile ferroviaire du futur qui devrait remplacer la technologie actuelle GSM-R (Global System for Mobile Communications-Railway), qui est utilisée pour la communication vocale et de données dans de nombreux réseaux ferroviaires à travers le monde.
Les principaux objectifs du FRMCS qui s'appuie sur le réseau 5G sont d'améliorer la sécurité, l'efficacité et la capacité des opérations ferroviaires. Il est conçu pour prendre en charge un large éventail d'applications et de services, notamment la communication vocale, le contrôle des trains, la signalisation, la communication train à train, les systèmes d'information aux passagers, etc. Le FRMCS devrait offrir des taux de transmission de données améliorés, une latence réduite, une capacité accrue et une meilleure couverture par rapport au GSM-R. Le FRMCS devrait également permettre l'évolution vers les trains autonomes et la mise en œuvre de systèmes de contrôle avancés des trains.
Le but de cette formation est de présenter FRMCS, de clarifier l'apport de la 5G au domaine ferroviaire, de comparer FRMCS à GSM-R, de montrer la relation entre FRMCS et MCX (Mission Critical Communication), de décrire l'architecture et les services FRMCS.

1. Introduction
   1.1. Qu'est-ce que le domaine ferroviaire : particularités, services et exigences ?
   1.2. Evolutions des services ferroviaires : voix, signalisation ETCS, évolutions vidéos, ATO, convoyage, …
   1.3. Quel spectre pour les systèmes ferroviaires ?
   1.4. Organisation et acteurs de l'écosystème ferroviaire : UIC, 3GPP, ERA

1. GSM-R :
   2.1. Rappels 2G en matière d'interface radio, d'architecture, de protocole, de procédures et de services
   2.2. Evolutions du GSM pour le domaine ferroviaire : numérotation fonctionnelle, routage d'appel en fonction de la localisation, mécanismes de priorité et de préemption, traitement de l'alerte radio, GSM-R & ETCS niveau 2, autres

applications du GSM-R, les équipements spécifiques d'un système GSM-R
2.3. Ingénierie radio d'un système GSM-R

2. Réseaux 4G (LTE/LTE-A)
   3.1. Architecture globale & Interface radio
   3.2. Procédures (mobilité, sécurité, gestion des appels et des sessions, gestion de la QoS)
   3.3. Évolution des services
   3.4. Performances
   3.5. LTE Advanced Pro : M2M & IoT (LTE-M & NB-IoT), de la PMR 2G à la PMR-4G, en route vers le V2X

3. Réseaux 5G
   4.1. Architecture & Interface radio
   4.2. Evolutions des services : eMBB, uRLLC et mMTC
   4.3. Evolutions Radio : De l'OFDM 4G à l'OFDM 5G
   4.4. Evolution de l'architecture : Clouding, SDN & NFV, Slicing
   4.5. Procédures (mobilité, sécurité, gestion des appels et des sessions, gestion de la QoS)

4. Evolutions 4G & 5G pour le ferroviaire :
   4.1. Les besoins d'évolutions du GSM-R
   4.2. Evolutions PMR pour le domaine ferroviaire : services MCX (MCPTT, MCVIDEO, MCDATA), D2D & ProSe
   4.3. L'apport de la 5G au domaine ferroviaire :
      4.3.1. Du spectre pour le ferroviaire
      4.3.2. L'apport du slicing
      4.3.3. L'apport de l'extension 5G uRLLC
      4.3.4. L'apport du V2X
      4.3.5. L'apport du MBMS 5G
      4.3.6. L'évolution FRMCS du domaine MCX : functional alias, appel multi-talker
   4.4. Stratégie de migration et coexistence FRMCS & GSM-R : concept Whitespace, 5G below 5MHz
   4.5. Le point sur la standardisation FRMCS

5G Network Slicing

Durée : 2 jours

Objectifs : Comprendre le Network Slicing dans le contexte du système 5G

Public : Ingénieurs télécom, Architectes télécom, Consultants télécom, ingénieur cœur de réseau

Pré-requis : Connaissance minimum du réseau coeur 5G (5GC)

Le network slicing consiste à découper le réseau en plusieurs sous-réseaux, que l'on appelle des "slices" en anglais. Chaque slice fonctionne de façon indépendante, bien qu'ils soient déployés sur une même infrastructure physique.
Le network slicing permet d'optimiser la gestion des flux sur le réseau mobile 5G en mode SA. Les opérateurs peuvent, grâce à cette méthode, adapter le réseau et la qualité du service selon les besoins des utilisateurs.
Bien que le network slicing ne soit pas un nouveau concept, il représente un concept fondamental dans le contexte du système 5G dans le but de fournir des réseaux privés dédiés adaptés aux besoins des différentes industries sur la base des exigences spécifiques d'une diversité de nouveaux services.
La possibilité d'instancier dynamiquement des instances de slice de réseau grâce à l'automatisation permet la fourniture d'instances de slice de réseau à la demande, traitant du concept de Slice-as-a-service (SaaS) dans un contexte Telco Cloud.

Le but de cette formation est de :
- Présenter le concept de slicing dans le système 5G
- Décrire les types de slices définis par le systmèe 5G et les comparer
- Présenter des exemples d'instance de slice, de leur caractéristique via un formulaire à leur conception et déploiement
- Décrire le cycle de vie d'une instance de slice
- Décrire les identités associées au network slicing
- Décrire les fonctions réseau 5G relatives au network slicing
- Illustrer la procédure d'enregistrement et l'identification des slices auquel l'UE aura le droit d'accéder
- Illustrer la procédure d'authentification spécifique à une instance de slice
- Illustrer la procédure d'établissemennt de session PDU spécifique à une instance de slice

1. Network slicing dans le système 5G
   1.1. RAN slice
   1.2. Transport Network slice
   1.3. Core Network slice
   1.4. Exemples

2. Les types de Slice dans le 5GS
   2.1. eMBB : Enhanced Mobile Broadband
   2.2. uRLLC : Ultra Reliable Low Latency Communication
   2.3. MIoT : Massive IoT

2.4. HMTC : High Performance Machine Type Communications
2.5. V2X : Vehicle to Everything
2.6. HDLLC : High Data rate and Low Latency Communications.
2.7. Comparaison entre les six différents types de slice standard

3. Caractérisation d'une instance de slice
   3.1. Template de description de slice selon la spécification GSMA NG.116

4. Exemples d'instance de slice
   4.1. Exemples d'instances de slice eMBB et leur caractéristation
   4.2. Exemple d'instance de slice uRLLC et sa caractéristation
   4.3. Exemples d'instances de slice MIoT et leur caractéristation
   4.4. Exemple d'instance de slice HMTC et sa caractéristation

5. Cycle de vie d'une instance de slice de réseau
   5.1. Caractérisation
   5.2. Design
   5.3. Commissioning
   5.4. Operation
   5.5. De-commissioning

6. Identification d'instance de slice
   6.1. S-NSSAI (Network Slice Selection Assistance Information)
      6.1.1. Configured NSSAI
      6.1.2. Subscribed S-NSSAI(s)
      6.1.3. Requested NSSAI
      6.1.4. Allowed NSSAI
      6.1.5. Rejected S-NSSAI(s)
      6.1.6. S-NSSAI : Single Network Slice Selection and Assistance Information
         6.1.6.1. SST : Slice Service Type
         6.1.6.2. SD : Slice Differentiator
   6.2. NSI : Network Slice Instance
   6.3. NSSI : Network Slice Subnet Instance
   6.4. NSSP (Network Slice Selection Policy) dans les policies URSP (UE Route Selection Policies)

7. Fonctions réseau relatives au network slicing
   7.1. AMF : doit prendre en charge l'ensemble des instances de slices d'un UE
   7.2. NSSAAF : doit authentifier l'UE de manière spécifique à une instance de slice
   7.3. NSACF : assure le contrôle d'admission à une instance de slice
   7.4. SMF : assure l'établissement/la modification/la libération d'une session PDU dans une instance de slice
   7.5. UPF : Prendre en charge le plan usager dans une instance de slice
   7.6. NSSF : Identifier les instances de slice auxquelles l'UE peut accéder
   7.7. NWDAF : Mesure des KPIs par instance de slice, tel que le niveau de charge d'une instance de slice

8. Enregistrement au 5GS et identification des instances de slice auxquelles l'UE peut accéder

9. Authentification spécifique à une instance de slice
   9.1. NSSAAF
   9.2. AAA Server
   9.3. Procédure d’authentification spécifique à une instance slice lors de la phase d’enregistrement de l’UE

10. Etablissement de session PDU dans une instance de slice

5G Non Terrestrial Network : Satellites, Drones & UAV

Durée : 2 jours

Objectifs : Avec les nouveaux travaux en cours de développement sur la 3GPP, l'hypothèse de réseaux de communications omniprésents incluant les réseaux satellites devenir une réalité. Le but de cette formation est de présenter l'écosystème 5G dans le contexte des réseaux satellites.

Public : Ingénieurs télécom et réseau, Architectes réseau, Consultants réseaux et télécom

Pré-requis : Connaissance du réseau d'accès 5G et de la radio 5G sinon prévoir un jour supplémentaire.

1. Introduction

2. Réseaux de communications par satellite
   - 2.1. Evolution des solutions des systèmes de communications par satellite
   - 2.2. Modèles de services par satellite : broadcast, fixe et mobile
   - 2.3. Aspects radio et fréquentiel
   - 2.4. Types de satellites (: GEO, LEO, MEO, HEO)
   - 2.5. Terminaux satellitaires
   - 2.6. Architecture du réseau terrestre : composants, équipements, interfaces et protocoles
   - 2.7. Aspects services : type de service, modèle de trafic, gestion de la QoS, impact de la latence sur les services
   - 2.8. Design radio : techniques d'accès (FDMA, TDMA, CDMA, OFDMA), techniques de modulation et codage
   - 2.9. Ingénierie radio : canal de propagation radio, lois génériques, bilan de liaison, gestion de la puissance, spécificités des réseaux satellites (effets ionosphériques et troposphériques), gestion des interférences, planification satellitaire
   - 2.10. Performances radio : débits, délais, taux d'erreurs, portée

3. Satellite et Géolocalisation :
   - 3.1. Principaux systèmes GNSS
   - 3.2. Localisation : concepts & principes
   - 3.3. Architecture & Aspects radio

4. Systèmes Satellitaires & TV
   - 4.1. Principaux systèmes de diffusion TV
   - 4.2. Transmissions TV : concepts & principes
   - 4.3. Architecture & Aspects radio

5. Solutions 3GPP pré-5G (UMTS & LTE) par Satellite

5.1. Genèse et rappels 3G & 4G en matière de :
  5.1.1. Panel des services
  5.1.2. Aspects radio : techniques choisies, ingénierie et performances
  5.1.3. Architecture : structure, équipements, interfaces & protocoles
  5.1.4. Principales Procédures

6. Solutions 3GPP 5G par Satellite
  6.1. La 5G :
    6.1.1. Sa genèse
    6.1.2. Ses Services : eMBB, uRLLC & mMTC
    6.1.3. Son Architecture : structure, équipements, interfaces & protocoles
    6.1.4. Ses Spécificités : Slicing, NFV, QoS, MEC
    6.1.5. Sa Radio : fréquence, canaux, OFDMA, modulation, protection et principales procédures
  6.2. Le domaine IoT
    6.2.1. Du M2M au LTE-M
    6.2.2. De SigFox/Lora au NB-IoT
    6.2.3. De NR-Light (RedCap) au NB-5G (Narrowband)
  6.3. L'évolution NTN (Non Terrestrial Network) de la 5G (R15/R16/R17) :
    6.3.1. C'est quoi un réseau NTN ?
    6.3.2. Bilan des évolutions 5G à effectuer
    6.3.3. Pour quels services ?
    6.3.4. Evolutions MAC & PHY de l'interface radio, aspects fréquences
    6.3.5. Evolutions d'architecture : mode Transparent / Régénératif, gestion des sessions et de la QoS, gestion du roaming et de la mobilité, interaction 5G NTN & 5G terrestre
    6.3.6. Impact sur les procédures
  6.4. Optimisations 5G NTN & IoT
    6.4.1. Cas d'usage IoT et NTN
    6.4.2. NB-IOT/LTE-M over GEO
    6.4.3. NB-IOT/LTE-M over LEO
    6.4.4. Ce qui est prévu en R18 pour la 5G NTN
    6.4.5. Modèles NTN commerciaux

7. 5G et les Drones et autres UAV (Unmanned Aerial Vehicle)

5G O-RAN : Architecture, components, and mise en œuvre et déploiement

Durée : 2 jours

Objectifs : Comprendre l'architecture O-RAN, ses composants, sa mise en œuvre et son déploiement. Étudier des cas d'utilisation d'O-RAN dans différents scénarios.

Public : Ingénieur télécom, architecte télécom, chef de projet télécom

Pré-requis : Connaissance minimum du réseau d'accès 5G

O-RAN (Open Radio Access Network) proposé par O-RAN Alliance est une architecture de réseau qui vise à transformer les réseaux d'accès radio (RAN), en adoptant des concepts d'ouverture, de virtualisation et d'interopérabilité. Traditionnellement, les réseaux d'accès radio étaient proposés par des fournisseurs de solutions verticales, où les différentes composantes du réseau d'accès, telles que les antennes, les stations de base et les contrôleurs de réseau, étaient fournies par un seul fournisseur et même fournisseur, souvent verrouillées et non interchangeables avec d'autres fournisseurs.
O-RAN vise à changer cela en introduisant une approche ouverte et décentralisée. Il définit des interfaces standardisées entre les différentes composantes du RAN, permettant ainsi une interopérabilité entre les équipements fournis par différents fournisseurs. Cela permet aux opérateurs de télécommunications d'éviter un verrouillage fournisseur, d'intégrer des équipements de différents fournisseurs et de bénéficier d'une plus grande flexibilité et de meilleures possibilités d'innovation.
L'architecture O-RAN est basée sur la virtualisation des fonctions réseau (NFV) et l'utilisation de logiciels définis par l'utilisateur (SDN). Elle permet la centralisation de certaines fonctions de contrôle et d'intelligence, tout en déployant des éléments de traitement de données distribués. Cela permet une meilleure utilisation des ressources réseau et une gestion plus efficace des capacités.
Le but de cette formation est d'introduire O-RAN dans le contexte RAN 5G, son architecture, ses composants, sa mise en œuvre et son déploiement.

1. Introduction
   1.1. Rappels sur l'évolution des réseaux radio mobiles depuis la 2G jusqu'à la 5G : architecture, interface, protocoles, procédures, services, sécurité
   1.2. Pourquoi l'Open RAN : principes et avantages

2. Standardisation & Open RAN
   2.1. Genèse de l'Open RAN
   2.2. Différences entre O-RAN, Open RAN, v-RAN, c-RAN
   2.3. Initiatives & Groupes de travail : TIP, alliance O-RAN, xRAN Forum, Cisco Open vRAN Alliance
   2.4. Lien avec le 3GPP

3. Focus RAN
   3.1. Evolution de l'architecture des RAN

3.2. Focus RAN 5G :
  3.2.1. Architecture globale : entités fonctionnelles & équipements
  3.2.2. Aspects interfaces & protocoles : User Plane/Control Plane, GTP-u/NG-AP/Xn-AP
  3.2.3. Découpes gNB-CU – gNB-DU :
    3.2.3.1. Principes
    3.2.3.2. Options possibles : avantages/inconvénients de chacune des 8 options,
    3.2.3.3. Séparation gNB-CU-CP/gNB-CU-UP :
      3.2.3.3.1. Protocoles associés (F1/E1)
      3.2.3.3.2. Impacts sur les procédures principales : gestion de la mobilité/gestion des sessions/gestion de la sécurité

4. Spécificités Techniques de l'O-RAN
  4.1. Architecture fonctionnelle et logique
    4.1.1. RIC : RAN Intelligent Controller, non-RT / near-RT
    4.1.2. SMO : Service & Management Orchestration
    4.1.3. Interfaces et protocoles
  4.2. Du CPRI à l'eCPRI : principes, architectures, interfaces et protocoles
  4.3. Aspects virtualisation
  4.4. Aspects sécurité
  4.5. Aspects Slicing
  4.6. Aspects Intelligence Artificielle et Maching Learning (AI/ML)
  4.7. Options de déploiements

5. Tendances & Perspectives
  5.1. Acteurs du marché
  5.2. Exemple de scénarios de déploiements

Roaming 5G SA

Durée : 2 jours

Objectifs : Comprendre les architectures de roaming data et voix dans le contexte 5G SA.

Pré-requis : Connaissance minimum du réseau coeur 5G

Public : Ingénieur télécom, architecte telecom, chef de projet telecom

La mobilité est la clé du succès des réseaux mobiles. Le roaming a étendu la définition de la mobilité au-delà de la technologie, des réseaux et des frontières des pays. Le but de cette formation est de présenter le roaming 5G SA à travers :

- Son architecture.
- Ses modes de fonctionnement : HR et LBO.
- Ses interfaces.
- Les procédures en roaming 5G SA ; enregistrement, établissement de session PDU, envoi et réception de SMS over NAS.
- La nouvelle approche pour fournir les données de steering of roaming à l'UE
- L'adressage des nœuds et le routage du trafic
- La sécurité des échanges entre réseau visité et réseau nominal
- Les services data et voix en roaming 5S SA.
- La facturation inter-opérateur pour les services en roaming basée sur BCE versus TAP en 2G à 5G NSA

1. Introduction
   - 1.1. Eléments clé du roaming 5G SA
   - 1.2. Exigences pour roaming 5G SA
     - 1.2.1. Exigences en matière d'architecture fonctionnelle
     - 1.2.2. Exigences en matière de sécurité
   - 1.3. Modèles d'architecture 5GA pour le roaming
     - 1.3.1. Pour la data
       - 1.3.1.1. Home routing
       - 1.3.1.2. Virtual home routing
       - 1.3.1.3. Local breakout
     - 1.3.2. Pour la voix
       - 1.3.2.1. N9HR
       - 1.3.2.2. LBO pour l'appel d'urgence
   - 1.4. Entités pour l'interconnexion des réseaux dans le contexte du roaming
     - 1.4.1. SEPP
     - 1.4.2. IPX HTTP Proxy
     - 1.4.3. Réseau IPX
   - 1.5. Roaming Hub
   - 1.6. Roaming Sponsor

2. Steering of roaming (SOR)
   - 2.1. SOR dans les réseaux 2G/3G/4G/5G NSA
   - 2.2. SOR dans le réseau 5G SA

2.2.1. Signalisation NAS pour les SOR data

3. Interfaces pour HR et LBO
   3.1. Interfaces HTTP/2 et JSON pour le plan contrôle
      3.1.1. N.8. AMF – UDM : LBO & HR
      3.1.2. N.10. SMF – UDM : LBO
      3.1.3. N.14. AMF – AMF : LBO & HR, pour la mobilité Inter-réseaux
      3.1.4. N.12. AMF – AUSF : LBO & HR
      3.1.5. N.16. vSMF – hSMF : HR
      3.1.6. N.21. SMSF – UDM : LBO & HR
      3.1.7. N.24. vPCF – hPCF : LBO & HR
      3.1.8. N.27. vNRF – hNRF : LBO & HR
      3.1.9. N.31. vNSSF – hNSSF : LBO & HR
      3.1.10. N32-c N32-f. SEPP – SEPP : LBO & HR
         3.1.10.1. Interface N32-c
         3.1.10.2. Interface N32-f
   3.2. Interfaces GTP-U pour le plan usager
      3.2.1. N9. vUPF – hUPF : HR

4. Procédures en roaming 5G SA
   4.1. Procédure d'enregistrement
   4.2. Procédure d'établissement de session PDU
   4.3. Procédure d'envoi et de réception de SMS over NAS

5. Nommage, adressage et routage pour le roaming 5G SA
   5.1. FQDN SEPP
   5.2. Distribution de la charge entre SEPPs du réseau visité et du réseau nominal
   5.3. Déclaration FQDN SEPP dans le document IR.21
   5.4. Découverte dynamique des SEPPs via DNS et redirection HTTP
   5.5. Telescopic FQDN pour la communication entre NFs de réseaux différents dans le contexte du roaming 5G SA
   5.6. Routage par les SEPP en fonction des telescopic FQDN

6. Sécurité du trafic HTTP/2 entre SEPP du réseau visité et SEPP du réseau nominal
   6.1. Architecture TLS directe entre SEPPs dans le contexte du roaming national par exemple
   6.2. Architecture PRINS (PRotocol for N32 INterconnect Security) entre SEPP via des IPX HTTP Proxy (roaming via des carrier internationaux)
   6.3. Comparaison entre les deux approches
   6.4. Case d'usage TLS et PRINS entre SEPPs

7. Interfonctionnement 5GC/EPC dans le contexte du roaming
   7.1. Architecture pour l'interfonctionnement 5GC/EPC en roaming
   7.2. Sélection du PGW
   7.3. Handover Intra-RAT 5G/4G ou 4G/5G

8. Slicing en roaming 5G SA
   8.1. Support UE pour le network slicing en roaming 5G SA
   8.2. Support 5GC pour le network slicing en roaming 5G SA

Architecture des données 5G : UDM, UDR, UDSF

Durée : 3 jours

Objectifs : Présenter les fonctions 5G relatives aux données, en particulier UDM, UDR et UDSF

Pré-requis : Connaissance minimum du HSS dans le contexte 4G

Public : **Ingénieurs télécom, Consultants réseaux et télécom, Architectes réseau et télécom**

Le but de cette formation est :

- d'introduire les interfaces du HSS pour mieux comprendre son évolution vers la 5G,
- décrire les interfaces de service liées aux fonctions de stockage de données dans le 5GS, en particulier, UDM, UDR et UDSF
- présenter les call flows impliquant ces fonctions pour la compréhension de leur interface de service.
- présenter l'interfonctionnement entre HSS et UDM lorsque les UDRs EPS et 5GS sont distinctes.

1. Rappel sur les interfaces du HSS
   1.1. S6a/S6d
   1.2. S6c
   1.3. S6t
   1.4. SWx
   1.5. Cx
   1.6. Sh
   1.7. Call flows pour la compréhension des interfaces
      1.7.1. Attachement/détachement dans le contexte EPS (S6a)
      1.7.2. Attachement/détachement dans le contexte WiFi connecté à l'ePC (SWx)
      1.7.3. Enregistrement/désenregistrement dans le contexte IMS (Cx, Sh)
      1.7.4. Envoi/Réception de SMS dans le contexte EPS (S6c)
      1.7.5. Souscription/Notification à des évènements dans le contexte LTE-M/NB-IoT (S6t)
      1.7.6. Autorisation NIDD dans le contexte NB-IoT (S6t)
      1.7.7. Configuration de paramètres d'application dans le contexte LTE-M/NB-IoT

2. Introduction au 5GC
   2.1. Architecture basée sur le service
   2.2. Principes de slices de réseau
   2.3. NFs (Network Functions) du 5GC
   2.4. Découverte des instances NFs via la NRF
   2.5. Principes de Services NF associés aux interfaces de services des NFs

3. Interface Nudm associée à la fonction UDM
   3.1. Services NF associés à l'interface de service Nudm de l'UDM
      3.1.1. Nudm_UEContextManagement (Nudm_uecm)
      3.1.2. Nudm_SubscriberDataManagement (Nudm_sdm)

3.1.3. Nudm_UEAuthentication Service (Nudm_ueau)
3.1.4. Nudm_EventExposure Service (Nudm_ee)
3.1.5. Nudm_ParameterProvision Service (Nudm_pp)
3.1.6. Nudm_NIDDAuthorization Service (Nudm-niddau)
3.1.7. Numd_MobileTerminated Service (Nudm_mt)
3.1.8. Notifications explicités versus notifications implicités
3.2. Call flows pour la compréhension de l'interface Nudm
3.2.1. Enregistrement
3.2.2. Changement de tracking Area et ré-enregistrement
3.2.3. Désenregistrement
3.2.4. Relocalisation d'AMF
3.2.5. Etablissement de session PDU
3.2.6. Souscription/Notification à des événements
3.2.7. Autorisation NIDD dans le contexte mMTC
3.2.8. Configuration de paramètres d'application

4. Interface Nausf associée à la fonction AUSF
4.1. Architecture d'authentification 5G
4.1.1. ARPF
4.1.2. AUSF
4.1.3. SEAF
4.1.4. SIDF
4.1.5. Third party authentication center
4.2. Procédure d'authentification Non-3GPP
4.3. Procédure d'authentification 3GPP
4.4. Interface Nausf
4.5. Mapping entre interfaces Nausf et Nudm pour la procédure d'authentification
4.6. Différence entre l'authentification LTE et l'authentification 5G

5. Interface Nudr associée à la fonction UDR 5G
5.1. Interface de service Nudr
5.2. Données stockées dans l'UDR 5G
5.2.1. Données de souscription
5.2.1.1. Authentication data
5.2.1.2. Context data
5.2.1.3. Provisioned data
5.2.1.4. Shared data
5.2.1.5. Group data
5.2.2. Données de politiques
5.2.2.1. AM policy data
5.2.2.2. UE policy data
5.2.2.3. SM policy data
5.2.2.4. Background data transfer policy data
5.2.3. Données structurées exposées à des applications externes
5.2.3.1. Access and mobility data
5.2.3.2. Session management data
5.2.4. Données d'application
5.2.4.1. Packet flow descriptor data
5.2.4.2. Influence data
5.3. Clients de l'interface Nudr : UDM, PCF et NEF

Architectures 3GPP pour les Communications V2X et eV2X

Durée : 2 jours

Objectifs : décrire les services et l'architecture V2X ; décrire les besoins eV2X, les services eV2X associés, l'architecture 5G pour eV2X et le slice de réseau uRLLC pour satisfaire les exigences de latence, gigue, et fiabilité.

Prérequis : Connaissance minimum du réseau 5G

Public : Ingénieurs télécom, Architectes télécom, Consultants télécom

Les véhicules connectés existent depuis environ 10 ans avec un développement des services qui a suivi celui des technologies cellulaires (2G, 3G, 4G). Aujourd'hui, il est possible de recevoir et de signaler des informations de trafic ou d'accéder à des services d'Infotainment à bord. Au-delà de ces développements commerciaux et métiers, le service d'appels d'urgence (eCall) est le premier service de connectivité à être obligatoire sur l'ensemble des nouveaux véhicules depuis 2018. Il impose donc une connectivité des véhicules aux réseaux cellulaires et une géolocalisation grâce aux systèmes de localisation satellitaires (e.g., GPS). A ce titre, l'eCall marque le démarrage à grand échelle des services de connectivité pour les véhicules.

Dans le contexte global du transport routier, la connectivité sera un atout majeur pour accompagner le démarrage de nouveaux services commerciaux et l'émergence de nouvelles orientations de la communauté européenne et des états membres dans ce domaine. L'échange de données entre véhicules, les centres de gestion de trafic et l'Internet permettront de développer de nouveaux services pour les utilisateurs de la voiture. L'industrie automobile va subir deux évolutions majeures avec le développement de la conduite autonome et celui des services de sécurité routière et de gestion de trafic. Ces deux évolutions nécessiteront le déploiement de la nouvelle technologie 5G.
La conduite autonome va exiger qu'un grand nombre de données issues de capteurs de la voiture soient agrégées pour calculer la trajectoire de la voiture ; les communications entre véhicules et entre véhicules et infrastructures permettront à celles-ci d'échanger des messages temps réel plus riches concernant les évolutions du trafic routier. Elles contribueront à l'acquisition d'une vision plus large de l'espace de déplacement propre à chaque véhicule.

L'adoption de standards de qualité est absolument indispensable pour offrir aux véhicules des communications fiables et sécurisées tout en permettant l'interopérabilité des services au niveau global. Des standards basés sur des plateformes ouvertes sont nécessaires pour le déploiement des systèmes et leur interopérabilité mais aussi pour éviter la fragmentation du marché et le report du déploiement des technologies V2X. Les travaux de standardisation menés initialement par 3GPP appelés V2X sont actuellement étendus pour concerner de

nouveaux schémas d'architecture destinés à supporter les communications eV2X (pour Vehicule to Everything) pour permettre de faire communiquer en temps réel les véhicules avec leur environnement afin d'améliorer la sécurité routière, l'efficacité du trafic et les économies d'énergie.

Le but de cette formation est de présenter l'écosystème V2X et de décrire les besoins eV2X, les services associés, l'architecture 5G pour eV2X et le slice de réseau uRLLC pour satisfaire les exigences de latence, gigue, et fiabilité.

1. De V2X à eV2X
   - 1.1. Standards V2X
   - 1.2. Support des types d'application V2X avec 3GPP
     - 1.2.1. Vehicle-to-Vehicle (V2V)
     - 1.2.2. Vehicle-to-Pedestrian (V2P)
     - 1.2.3. Vehicle-to-Network (V2N)
     - 1.2.4. Vehicle-to-Infrastructure (V2I)
   - 1.3. Niveau d'automatisation
     - 1.3.1. Niveau 0: no automation
     - 1.3.2. Niveau 1: driver assistance
     - 1.3.3. Niveau 2: partial automation
     - 1.3.4. Niveau 3: conditional automation
     - 1.3.5. Niveau 4: high automation
     - 1.3.6. Niveau 5: full automation
   - 1.4. V2X versus 802.11P
   - 1.5. Spectre pour les services V2X
   - 1.6. Améliorations 3GPP pour le support eV2X
     - 1.6.1. eV2X versus V2X
   - 1.7. Services de communication Vehicle-to-everything (eV2X)
     - 1.7.1. Vehicle platooning (échange d'information entre le groupe de véhicules voyageant ensemble)
     - 1.7.2. Advanced driving (conduite semi ou totalement automatique)
     - 1.7.3. Extended sensors (échange d'information collectées par des capteurs entre véhicules, mobiles des piétons et serveurs d'application V2X)
     - 1.7.4. Remote driving (contrôle à distance du véhicule par un conducteurs ou une application V2X)

2. Architecture pour les services V2X
   - 2.1. Communication V2X basée sur PC5
   - 2.2. Communication V2X basé sur LTE-Uu
   - 2.3. Architecture V2X basée sur PC5 et LTE-Uu
     - 2.3.1. V2X Application Server
     - 2.3.2. V2X Control Function
     - 2.3.3. V2X Application
     - 2.3.4. Interfaces V1, V2, V3, V4, V5, LTE-Uu et PC5
   - 2.4. Provisioning des policies/paramètres pour les communications V2X sur l'UE via PC5 et LTE-Uu
   - 2.5. Transmission/Réception des messages V2X via PC5 et LTE-Uu
   - 2.6. Call flows pour les procédures associées

3. Architecture pour les services eV2X
   3.1. Communication eV2X basée sur PC5
   3.2. Communication eV2X basé sur NG-Uu
   3.3. Provisioning de service sur l'UE pour les communications eV2X via PC5 et NG-Uu
   3.4. Impacts eV2X sur les procédures 5GC
      3.4.1. Procédure d'nregistrement de l'UE
      3.4.2. Procédure Service Request de l'UE
      3.4.3. Procédure de Handover N2
      3.4.4. Procédure de Handover Xn
      3.4.5. Impacts sur les entités et interfaces existantes

4. Slice uRLLC
   4.1. Eléments clé pour satisfaire les exigences uRLLC sur la latence, la gigue et la fiabilité
   4.2. Minimisation de la mobilité de l'UE sur la latence et la gigue entre le réseau d'accès et le réseau cœur et dans le réseau cœur
   4.3. Transmission plus fiable que celle d'un seul tunnel du plan usager sur les interfaces N3 et N9 dans le plan usager
   4.4. Supervision de la QoS des QoS flows avec les exigences uRLLC
   4.5. Impacts sur policy control et charging control

Authentification dans les réseaux 4G, 5G et les services VoLTE/VoWiFi/VoNR

Durée : 2 jours

Objectifs : Comprendre l'authentification mobile et son application aux réseaux 4G et 5G et aux services VoLTE/VoWiFi/VoNR

Public : Ingénieurs télécom et réseau, Architectes réseau, Consultants réseaux et télécom

Pré-requis : Connaissance des réseaux mobiles 4G et 5G

Le but de cette formation est de :
- Présenter les différentes identités utilisées pour les authentifications 4G et 5G
- Décrire les données de souscription présentes dans l'UDR pour l'authentification
- Présenter les procédures d'authentification et d'agrément de clé dans les réseaux mobiles 4G/5G depuis un accès cellulaire ou accès WiFi et dans les services VoLTE/VoWiFi/VoNR

1. Authentification Mobile 4G/5G
   1.1. Principes
   1.2. Données de souscription dans l'UDR pour l'authentification

2. Authentification 4G avec accès LTE
   2.1. Identités
   2.2. Authentication and Key Agreement (AKA)
   2.3. Clés K_{ASME}, K_{NASenc}, K_{NASint}, K_{eNB}, K_{Upenc}, K_{RRCenc}, K_{RRCint}
   2.4. Vecteur d'authentification LTE : RAND, XRES, AUTN, K_{ASME}
   2.5. Procédure d'authentification avec UE, MME et HSS
   2.6. Dérivation de clés pour le chiffrement et la protection de l'intégrité
   2.7. Chiffrement et protection de l'intégrité des signalisation RRC et NAS
   2.8. Chiffrement du plan usager

3. Authentification 4G avec accès WiFi
   3.1. Identités
   3.2. AKA et AKA'
   3.3. Algorithme EAP
   3.4. Vecteur d'authentification EAP-AKA/EAP-AKA'
   3.5. Clé MSK et dérivation de clés pour le chiffrement et la protection de l'intégrité
   3.6. Procédure d'authentification entre UE et AAA Server via ePDG et obtention des vecteurs d'authentification par le AAA Server auprès du HSS

4. Authentification primaire 5G avec accès cellulaire
   4.1. Identités
   4.2. Architecture d'authentification
      4.2.1. SEAF, AUSF et ARPF
      4.2.2. SIDF

4.3. 5G-AKA
4.4. Vecteur 5G HE AV (RAND, AUTN, XRES*, KAUSF) et vecteur 5G SE AV (RAND, AUTN, HXRES*)
4.5. Dérivation de clés de chiffrement et de protection d'intégrité
4.6. Procédure d'authentification 5G-AKA avec UE, AMF/SEAF, AUSF et UDM/ARPF
4.7. Chiffrement et protection de l'intégrité des signalisation RRC et NAS
4.8. Chiffrement et protection de l'intégrité du plan usager

5. Authentification primaire 5G avec accès WiFi
   5.1. Identités
   5.2. Architecture d'authentification
      5.2.1. SEAF, AUSF et ARPF
      5.2.2. SIDF
   5.3. EAP-AKA'
   5.4. Vecteur EAP-AKA'
   5.5. Dérivation de clés de chiffrement et de protection d'intégrité
   5.6. Procédure d'authentification EAP-AKA' avec UE, AMF/SEAF, AUSF et UDM/ARPF

6. Authentification primaire 5G via EAP-TLS, e.g., pour les devices IoT
   6.1. Identités
   6.2. Architecture d'authentification
      6.2.1. SEAF et AUSF
      6.2.2. SIDF
   6.3. EAP-TLS
   6.4. Certificats client et serveur
   6.5. Dérivation de clés de chiffrement et de protection d'intégrité
   6.6. Procédure d'authentification EAP-TLS avec UE, AMF/SEAF et AUSF

7. Authentification spécifique au slice de réseau
   7.1. Définition du slice de réseau
   7.2. Identités
   7.3. Architecture d'authentification
      7.3.1. AMF, NSS-AAF, AAA Server, AAA Proxy, 3rd Party AAA Server
   7.4. EAP
   7.5. Procédure d'authentification/ré-authentification EAP pour l'accès au slice avec UE, AMF, NSS-AAF et AAA Server

8. Authentification secondaire lors de l'établissement d'une session PDU dans un slice de réseau
   8.1. Identités
   8.2. Architecture d'authentification
      8.2.1. SMF, DN-AAA Server
   8.3. EAP
   8.4. Procedure d'établissement d'une session PDU
   8.5. Procédure d'authentification EAP pour l'établissement d'une session PDU dans un slice de réseau avec UE, SMF, DN-AAA Server
   8.6. Procédure de ré-authentification

9. Authentification VoLTE/VoWiFi/VoNR
   - 9.1. Authentification USIM et Authentification ISIM
   - 9.2. Identités
   - 9.3. AKA
   - 9.4. Vecteur d’authentification VoLTE/VoWiFi/VoNR (RAND, AUTN, XRES, CK, IK)
     - 9.4.1. Cas USIM
     - 9.4.2. Cas ISIM
   - 9.5. Utilisation CK et IK sur tunnel IPSec entre UE et P-CSCF

Comprendre la voix sur IP dans le contexte de la 5G SA

Durée : 2 jours

Objectifs : Comprendre la voix sur IP dans le contexte de la 5G en mode SA avec les variantes VoNR, VoeLTE, EPS Fallback et RAT Fallback

Pré-requis : Connaissance de la VoLTE et de la VoWiFi

Public : Ingénieur télécom, architecte telecom, chef de projet telecom

Au début du déploiement de la 5G en mode SA, Evolved Packet System Fallback (EPS FB) sera la première solution pour le service voix à être déployée pour réutiliser le service VoLTE. Elle nécessite une couverture LTE, là où est déployée la couverture 5G en mode SA. Tout comme Circuit Switched Fallback (CSFB) a été introduit au début de la LTE pour offrir un service voix circuit avant l'arrivée de la VoLTE, l'EPS FB est une solution initiale pour offrir la voix via la 5G en mode SA avant l'arrivée de la VoNR. Mais la solution long terme pour la voix avec la 5G en mode SA est la VoNR pour unifier les services voix et data avec la 5G en mode SA.

Indépendamment de VoNR et EPS FB offerts par le mode 5G SA, il est possible de considérer VoeLTE où la voix est prise en charge par un accès 4G connecté à un cœur de réseau 5G et l 'IMS ainsi que RAT Fallback ou la session voix est transférée de l'accès 5G à l'accès 4G où les deux radios sont connectées au même réseau cœur 5GC.

Le but de cette formation est de présenter la Vo5G avec VoNR, VoeLTE, EPS FB et RAT Fallback.

1. 5G CN et service voix sur IMS
   - 1.1. Introduction au 5G CN
   - 1.2. Configuration des DNN IMS et SOS, S-NSSAI et Mode SSC
   - 1.3. UE Route Selection Policy pour IMS
   - 1.4. Etablissement de session PDU pour le DNN IMS et SOS
   - 1.5. Roaming LBO et N9HR
   - 1.6. Contraintes sur l'Interfonctionnement 5GC/EPC pour le service voix

2. 5G NSA et VoLTE
   - 2.1. Configuration de l'option 3X
   - 2.2. Option 3X et VoLTE

3. Solutions pour la VoIP dans le contexte 5G SA
   - 3.1.1. Vo5G
     - 3.1.1.1. Négociation entre UE et réseau pour utiliser Vo5G
     - 3.1.1.2. Architecture
     - 3.1.1.3. Procédure d'enregistrement
     - 3.1.1.4. Procédure d'établissement d'appel
     - 3.1.1.5. Interfonctionnement 5GS/EPS pour l'EPS Fallback

3.1.1.6. RAT Fallback
3.1.1.7. Handover versus Redirection
3.1.1.8. Emergency Services Fallback
3.1.1.9. Codecs audio et vidéo pour la Vo5G
3.1.2. VoNR
3.1.3. Comparaison entre VoNR, VoeLTE, EPSFB et RAT Fallback

4. Evolutions des interfaces DIAMETER Cx, Sh, Rx vers des interfaces de service basées sur le protocole HTTP/2
   4.1. De Cx et Sh à Nhss_ims
      4.1.1. API Nhss_imsUEContextManagement
      4.1.2. API Nhss_imsUESuscriberDataManagement
      4.1.3. Nhss_imsUEAuthentication
   4.2. De Rx à Nbsf et Npcf

5. Procédures VoNR
   5.1.1. Enregistrement/Réenregistrement/Désenregistrement
   5.1.2. Authentification VoNR (versus Authentification VoLTE)
   5.1.3. Etablissement de session
   5.1.4. 5G-SRVCC
   5.1.5. T-ADS
   5.1.6. Restauration S-CSCF
   5.1.7. Restauration P-CSCF

6. Services Vo5G
   6.1. Call composer
   6.2. USSI (Unstructured Supplementary Service Data using IMS)
   6.3. NG eCall

7. Policy Control pour la VoNR
   7.1.1. Bidding de session via la fonction BSF
   7.1.2. Réservation des ressources pour la session VoIP via la fonction PCF
      7.1.2.1. QoS Flows pour SIP, RTP audio et RTP video (ViNR)

8. Interception légale pour la VoNR
   8.1.1. Nouvelle architecture LI pour la 5G et pour l'IMS
   8.1.2. Interception légale de la cible et du non-local-ID
   8.1.3. de LI S8HR à LI N9HR

9. Evolutions des headers SIP incluant des informations d'accès pour la VoNR, e.g., P-A-N-I.

Le Réseau et les Services 5G et Impacts sur le SI

Durée : 2 jours

Objectifs :

- **Présenter l'évolution vers la 5G, les familles d'usage de la 5G, l'architecture du système 5G. Décrire le principe de slice de réseau qui est un « Network As A Service » et sa gestion.**
- **Présenter les plate-formes de service 5G notamment Policy and Charging Control (PCC) et NEF (Network Exposure Function).**
- **Décrire le modèle de données 5G avec les données de souscription, les données de policing et les données d'application.**
- **Montrer l'impact de la 5G sur le SI.**

Prérequis : Connaissance minimum du réseau mobile 4G et du protocole IP

Public : Ingénieurs télécom, Consultants réseaux et télécom, Architectes réseau et télécom, Architectes SI

L'utilisation d'un mobile et de ses applications est désormais fermement ancrée dans le quotidien : les appareils portables connectés sont de plus en plus performants : ils remplacent bien souvent le téléphone fixe, l'appareil photo, voire l'ordinateur et même le téléviseur. Le volume de données échangées sur les réseaux mobiles n'arrête pas de doubler d'une année à l'autre et dans les 5 ans à venir, il aura été multiplié par 10 par rapport à l'utilisation actuelle. De nouvelles solutions doivent donc être trouvées afin de pouvoir répondre à cette demande et d'optimiser l'utilisation des ressources. L'augmentation du nombre d'applications, leur diversification ainsi que l'amélioration de la qualité des réseaux mobiles ont conduit à l'augmentation de la demande, à l'apparition de nouveaux usages et de nouveaux utilisateurs. La 5G se situe au carrefour de ces nouveaux usages ; elle ambitionne de répondre mieux et simultanément à cette grande variété de besoins et ces nouvelles demandes, via une technologie unifiée qui prend en compte, dès sa conception, cette diversité. La 5G définit trois grandes famille d'usage avec leurs exigences respectives et potentiellement incompatibles entre elles:
1. mMTC – Massive Machine Type Communications : communications entre une grande quantité d'objets avec des besoins de qualité de service variés. L'objectif de cette catégorie est de répondre à l'augmentation exponentielle de la densité d'objets connectés ;
2. eMBB – Enhanced Mobile Broadband : connexion en ultra haut débit en outdoor et en indoor avec uniformité de la qualité de service, même en bordure de cellule ;
3. uRLLC – Ultra-reliable and Low Latency Communications : communications ultra-fiables pour les besoins critiques avec une très faible latence, pour une réactivité accrue.

Le but de cette formation est de décrire le réseau 5G dans son ensemble via les familles d'usage qu'il adresse, via les KPIs attendus, son architecture de réseau de

bout en bout, avec notamment une architecture de réseau basée sur le service pour plus de flexibilité et d'évolutivité. Le concept de slice de réseau pour le marché entreprise qui représente un « network as a service » est développé. Les services PCC (Policy and Charging Control) et les APs de service exposées au monde externe via une network exposure function sont décrits.
Le modèle de données 5G associé au client avec notamment les données de souscription, les données de policing, les données structurées pour exposition et les données d'application est développé.

Par ailleurs, cette formation introduit l'impact de la 5G sur le SI avec la compréhension du provisionning de l'usager et des slices de réseau 5G, la gestion de la QoS des sessions de données, et du policy control et de la taxation.

1. De la 4G à la 5G

2. Familles d'usage de la 5G
   - 2.1. eMBB - Enhanced Mobile Broadband
   - 2.2. mMTC - Massive Machine Type Communications
   - 2.3. uRLLC - Ultra-reliable and Low Latency Communications
   - 2.4. Catalogue de slices notamment pour le marché entreprise

3. KPIs 5G

4. Architecture 5GS (5G System)
   - 4.1. Concepts et principes sous-jacents à l'architecture 5GC
   - 4.2. Architecture du réseau d'accès 5G RAN
   - 4.3. Architecture du réseau coeur 5G (5GC, 5G Core)
   - 4.4. Fonctions de réseau 5GS (5G RAN + 5GC)
   - 4.5. Les interfaces de service : API REST/HTTP pour la communication entre fonctions du plan contrôle du réseau 5G
   - 4.6. Relations entre 5G, SDN, NFV et le cadre de gestion NFV pour la mise en œuvre du réseau 5G

5. Identités 5G
   - 5.1. SUPI versus IMSI
   - 5.2. GPSI versus MSISDN
   - 5.3. PEI versus IMEI
   - 5.4. SUCI
   - 5.5. Identités de groupe :
     - 5.5.1. Identité de groupe externe
     - 5.5.2. Identité de groupe interne

6. Slices de réseau
   - 6.1. Fonctions communes aux différents slices de réseau
   - 6.2. Fonctions spécifiques à chaque slice de réseau
   - 6.3. Configuration d'une instance de slice de réseau pour un client donné.
   - 6.4. Caractéristiques du slice
   - 6.5. Exemples de slices de réseau,
     - 6.5.1. Slice eMBB
     - 6.5.2. Slice mMTC

6.5.3. Slice uRLLC

7. Modèle de données relatif à la souscription 5G
   7.1. Données de souscription
      7.1.1. Données de gestion de mobilité
      7.1.2. Données de gestion de session
      7.1.3. Données de gestion de SMS
   7.2. Données de policing
      7.2.1. Politiques de QoS et de gating
      7.2.2. Politiques de traffic steering
      7.2.3. Politiques de gestion de mobilité
      7.2.4. Politiques de sélection de réseau accès
   7.3. Données structurées pour exposition
   7.4. Données d'application

8. Procédures 5G
   8.1. Enregistrement/désenregistrement
   8.2. Etablissement de session PDU IPv4, IPv6, Ethernet et non-structurée

9. Voix sur IP sur la 5G avec IMS

10. Provisioning dans la 5G
   10.1. Provisioning de l'UE
      10.1.1. Provisioning du modèle de données relatif à la 5G dans l'UDR
   10.2. Provisioning de slice de réseau

11. Gestion des performances de la 5G
   11.1. Modèle de QoS 5G
   11.2. Mise en œuvre et gestion de la QoS pour les sessions PDU et les flux de service

12. Policy control et taxation dans la 5G (PCC)
   12.1. Policy control ou l'intelligence du réseau 5G
   12.2. Nouveaux scénarii PCC par rapport à ceux de la 4G
   12.3. Architecture PCC
   12.4. Règles PCC
      12.4.1. Politiques de mobility management
      12.4.2. Politiques de session management
      12.4.3. Politiques de traffic steering
      12.4.4. Politiques de access network discovery and selection

Réseau d'accès et nouvelle Radio 5G NR

Durée : 2 jours

Objectifs : Comprendre le réseau d'accès et la radio 5G

Pré-requis : Connaissance de base sur les réseaux mobiles

Public : Ingénieurs Télécom, Architectes Réseau, Consultants Télécom

En décembre 2017, une première étape de normalisation 5G a été franchie : le 3GPP a annoncé la sortie des premières spécifications techniques pour cette 5G dite NR (NR pour New Radio). Sans prétendre être la 5G finale, cette première mouture est une étape essentielle avant la 5G Phase 1 prévue pour fin 2018 et complétée en 2020 par une Phase 2.

Cette formation 5G NR est une étape cruciale qui détermine le cadre global et les briques élémentaires pour cette future génération aussi bien d'un point de vue architectural que procédural. Cette étape se propose d'exploiter les réseaux 4G actuels en augmentant leurs débits et en réduisant leur latence par l'usage d'une évolution dite eMBB (Enhanced Mobile Broadband) de l'interface radio tout en anticipant les futures évolutions nécessaires pour répondre aux challenges mMTC (M2M/IoT) et URLLC (eV2X).

Cette 5G de transition, appelée aussi 5G NR Non Standalone (NSA) prépare l'avènement de la future 5G NR Standalone (SA) prévue en phase 1 qui s'annonce déjà comme une « vraie 5G ». C'est sur cette base, que des essais grandeur nature (JO d'Hiver en Corée) voire des déploiements pré-commerciaux vont pouvoir être lancés par les constructeurs et les opérateurs.

C'est toute la dimension radio qui sera abordée dans cette formation. Bien évidement l'interface radio y sera largement évoquée. On présentera les nouveautés 5G en regard du socle 4G sur lesquelles elles reposent. Les aspects architecture, protocoles et procédures de ce nouveau RAN seront bien évidemment traités.

1. Introduction
   1.1. Brefs rappels 2G & 3G
   1.2. La genèse de la 5G : perspectives économiques, performances attendues, services 5G espérés, des trials à la standardisation 3GPP, calendrier de la standardisation

2. De l'E-UTRAN (4G) au NG-RAN (5G)
   2.1. Eléments d'architecture 4G
   2.2. Equipements, Interfaces et Protocoles 5G : gNB, interfaces Xn, NG & radio, protocoles NG-AP, Xn-AP & radio, Cloud RAN (CU/DU, options de split, eCPRI)
   2.3. Interaction avec le cœur de réseau : concept NSA/SA, protocole NAS

3. Interface Radio

3.1. Canaux Physiques:
  3.1.1. Des fréquences pour la 5G,
  3.1.2. Numérologie et structure : de l'OFDM 4G & l'OFDM 5G, modulations, trame & slot, FDD/TDD, BWP
  3.1.3. Canaux DL : Rappels 4G, PSS, SSS, PBCH, PDCCH, PDSCH, CSI-RS, DM-RS, PT-RS
  3.1.4. Canaux UL : Rappels 4G, PUSCH, PUCCH, PRACH, SRS, DM-RS
3.2. Eléments connexes :
  3.2.1. Codage Canal : évolutions HARQ, du Turbo Coding au LDPC/Polar Code
  3.2.2. Link Adaptation: AMC, Power Control, CQI, Scheduling, BWP
  3.2.3. Protocoles : MAC, RLC, PDCP, SDAP, RRC
  3.2.4. MIMO 5G : SU-MIMO, MU-MIMO & Beamforming
  3.2.5. Carrier Aggregation & Dual Connectivity
3.3. Aspects Backhauling : self-Backhauling

4. Procédures Radio
4.1. Gestion de la Connection Radio :
  4.1.1. Synchronisation et sélection des cellules
  4.1.2. Aspects RACH
  4.1.3. Etats de connection RRC
  4.1.4. Aspects DRX
  4.1.5. Aspects SysInfo
  4.1.6. Power control
  4.1.7. Timing Advance
4.2. Gestion du trafic :
  4.2.1. Processus d'allocation des ressources
  4.2.2. Radio Bearer : concept,
  4.2.3. QoS & 5G : du QCI 4G au 5QI 5G, procédures associées
4.3. Gestion de la mobilité :
  4.3.1. Selection & re-selection de cellule
  4.3.2. Mécanismes de Handover : gestion des mesures, procédures de handover
  4.3.3. Procédures de paging
4.4. Eléments connexes :
  4.4.1. Identités : UE et Eléments du Réseau
  4.4.2. Aspects Slicing
  4.4.3. Du SON 4G au SON 5G
  4.4.4. Du RAN Sharing 4G au RAN Sharing 5G

5. Evolutions 5G NR Phase 2 :
5.1. Vers une OFDM plus filtrée : FBMC, F-OFDM ?
5.2. Optimisations mMTC :
  5.2.1. NOMA
  5.2.2. SCMA
  5.2.3. Du LTE-M/NB-IoT 4G au 5G-IoT
5.3. Optimisations URLLC :

Comprendre le système 5G de bout en bout

Durée : 2 jours

Objectifs : Comprendre le système 5G (5GS) de bout en bout, l'architecture 5GS avec le réseau d'accès, le réseau cœur et les plate-formes de services, les procédures 5GS, les interfaces de services 5GS, les protocoles utilisés sur le plan contrôle et le plan usager et l'interfonctionnement avec la 4G

Pré-requis : Connaissance de base sur les réseaux mobiles

Public : Ingénieurs Télécom, Architectes Réseau, Consultants Télécom

Le but de cette formation est de présenter le réseau 5G de bout en bout :

- Le réseau cœur 5GC prenant en charge la radio LTE, la radio WiFi et la nouvelle radio 5G
- Les fonctions réseau du système 5G
- Le slicing de réseau 5G
- L'interfonctionnement entre 5G et 4G
- Les procédures 5G (Enregistrement/désenregistrement de l'UE, établissement de session PDU, etc).

1. Le système 5G (5GS) de bout en bout
   - 1.1. Le but de la 5G
   - 1.2. Les slices de réseau 5G : eMBB, mMTC et uRLLC
   - 1.3. Le réseau d'accès NR
     - 1.3.1. Les fonctions du réseau d'accès 5G : gNB et Security Gateway
       - 1.3.1.1. gNB
         - 1.3.1.1.1. RU
         - 1.3.1.1.2. DU
         - 1.3.1.1.3. CU-CP
         - 1.3.1.1.4. CU-UP
         - 1.3.1.1.5. Interfaces entre fonctions
       - 1.3.1.2. Cloud RAN
       - 1.3.1.3. Virtual RAN
       - 1.3.1.4. Open RAN
       - 1.3.1.5. Déploiement désagrégé du gNB
     - 1.3.2. Les bandes de fréquences 5G
       - 1.3.2.1. Bandes basses et cas d'usage
       - 1.3.2.2. Bandes moyennes et cas d'usage
       - 1.3.2.3. Bandes hautes et cas d'usage
   - 1.4. Le réseau cœur 5GC plan contrôle
     - 1.4.1. Les fonctions réseau (NF, Network Function)
     - 1.4.2. L'architecture de service 5GC
     - 1.4.3. Les interfaces de service des NFs

1.4.4. Mapping entre fonctions réseau 4G et fonctions réseau 5G
1.4.5. NFs stateful versus NFs stateless pour une meilleure résilience
1.5. Le réseau cœur 5GC plan usager
1.5.1. Types de session PDU : IPv4, IPv6, Ethernet, Unstructured (Non-IP)
1.5.2. Mode SSC (Session and Service Continuity) : SSC1, SSC2 et SCC3
1.5.3. Uplink Classifier (UC) et Branching Point (BP) pour la mise en œuvre d'un plan usager flexible

2. Procédures 5GS
2.1. Protocole NAS afin que l'UE puisse invoquer les procédures de service
2.2. Procédure d'enregistrement
2.3. Procédure de mise à jour de TA
2.4. Procédure de désenregistrement par l'UE et par le réseau
2.5. Procédure de relocalisation d'AMF
2.6. Procédure d'établissement de session PDU
2.7. Procédure Service Request initiée par l'UE pour l'envoi des données
2.8. Procédure Service Request initiée par l'UE pour la réception des données

3. Interfonctionnnement 5GC/EPC

4. Network slicing ou comment créer des réseaux personnalisés afin d'offrir une solution optimisée pour des scénarii associés à différents marchés, e.g., en terme de fonctionnalité, performance et isolation
4.1. Terminologie et définitions
4.2. Fonctions de réseau communes et fonctions de réseau spécifiques à une instance de slice de réseau
4.3. Caractérisation d'une instance de slice de réseau avec NG.116
4.4. Création, modification et suppression d'une instance de slice de réseau
4.5. Exemples de slices eMBB, mMTC et uRRLC
4.6. Support de slice de réseau en roaming
4.7. Association d'un UE à ses slices de réseau
4.8. Sélection et association d'une session PDU à une instance de slice de réseau
4.9. Mesure de KPIs radio, cœur de réseau et de bout en bout par instance de slice de réseau

Comprendre à un haut niveau le nouveau réseau 5G

Durée : 1 jour

Objectifs : Comprendre à un haut niveau les évolutions du réseau mobile vers la 5G pour mieux appréhender l'écosystème 5G de bout en bout (Accès, Réseau, Services et SI)

Pré-requis : Connaissance de base sur les réseaux mobiles

Public : Manager réseau et SI, Architecture réseau technique et SI 5G

Le but de cette formation est d'introduire le réseau et les services 5G, notamment :

- Le réseau d'accès 5G avec la nouvelle radio NR
- Le réseau coeur 5GC prenant en charge la radio WiFi, la nouvelle radio 5G et les accès filaires.
- Les fonctions réseau du réseau 5G
- Le slicing de réseau dans le réseau 5G notamment les slices pour Enhanced Mobile Broadband (eMBB), Massive IoT (mMTC) et Ultra Reliable and Low Latency Communication (uRLLC)
- Les services 5G notamment les services PCC (Policy and Charging Control) et les services via la NEF (Network Exposure Function)
- Les impacts SI de la 5G

1. De la 4G à la 5G

2. La technologie radio 5G (NR, New Radio) et le réseau d'accès 5G
   2.1. 5G NSA (Non Stand Alone)
   2.2. 5G SA (Stand Alone)
   2.3. Avantages du mode SA par rapport au mode NSA
   2.4. La 5G pour le mobile d'une part et le fixe d'autre part (FWA, Fixed Wireless Access et WWC, Wireless Wireless Convergence)

3. Le réseau cœur 5GC et la prise en charge des radios NR, WiFi et Accès Fixes

4. Les fonctions réseau du réseau 5G

5. Le réseau de signalisation 5GC basé sur des proxys HTTP2

6. Le slicing de réseau dans le réseau 5G : Network as a Service
   6.1. Exemples d'instances de slices de réseau
   6.2. Les grands domaines d'application pour le business du slicing

7. L'évolution de PCC (Policy and Charging Control) dans le contexte de la 5G

8. API de Service exposée au monde externe via la NEF (Network Exposure Function)

9. Impacts de la 5G sur le système d’information (SI)

MCX : MCPTT, MCVideo, MCData

Durée : 3 jours

Objectifs : Comprendre les services MCX, à savoir MCPTT audio, MCVideo et MCData

Pré-requis : Connaissance minimum du réseau cœur 4G

Public: Ingénieur télécom, architecte telecom, chef de projet telecom

La réalisation d'un système de télécommunication critique passe par l'acquisition de trois éléments fondamentaux qui forment le cœur technique de l'infrastructure de communication critique :
• une capacité d'accès à la couverture radio 4G (puis 5G) et aux services de téléphonie et d'internet auprès de quelques opérateurs de réseaux mobiles ;
• l'acquisition des capacités techniques d'un opérateur de réseau mobile virtuel (MVNO) à savoir un « cœur » de réseau télécom, un système d'information de gestion du réseau privé et de ses abonnés, un centre d'opération du réseau et de service, une offre de terminaux mobiles ;
• l'acquisition d'une capacité à délivrer des services applicatifs de communications pour missions critiques (MCx), permettant d'organiser des communications multimédias de groupe au profit des abonnés de l'infrastructure de communication critique en bénéficiant d'une qualité de service (QoS) avec priorité et préemption dans les réseaux aujourd'hui 4G et demain 5G.

Le but de cette formation est de présenter les services MCX notamment MCPTT pour l'audio, MCVideo et MCData.

1. Mission Critical Communications (MCX)
   - 1.1. Technologie Tetra existante pour la prise en charge des communications critiques dans le contexte d'un réseau privé
   - 1.2. Place de MCX dans la PMR (Private Mobile Communication)
   - 1.3. Réseau privé 4G/5G pour MCX versus réseau public 4G/5G traditionnel
   - 1.4. QoS 4G MCX versus QoS 4G traditionnelle
   - 1.5. Configuration du réseau 4G pour MCX

2. L'architecture MCX
   - 2.1. MCX Server (MCPTT server, MCVideo server, MCData server)
     - 2.1.1. Participating Function
     - 2.1.2. Controlling Function
     - 2.1.3. Non-Controlling Function
   - 2.2. Identity Management Server
   - 2.3. Configuration Management Server
   - 2.4. Key Management Server
   - 2.5. Group Management Server
   - 2.6. Location Management Server

2.7. Recording Server
2.8. MC Gateway Server pour l'interconnexion entre systèmes MCX
2.9. MCX Database

3. Procédure d'enregistrement MCPTT
   3.1. Identité MC
   3.2. Identité MCPTT
   3.3. Identité SIP (i.e., IMPU) versus identité MCPTT
   3.4. MCPPT Client ID
   3.5. Enregistrement SIP/IMS versus enregistrement MCPTT

4. MCPTT
   4.1. Interfaces entre le client MCPTT et le serveur MCPTT
   4.2. Appel MCPTT privé
   4.3. Appel MCPTT de groupe
   4.4. Appel MCPTT de groupe broadcast
   4.5. Appel MCPTT d'urgence ou de groupe d'urgence
   4.6. Appel MCPTT de groupe danger imminent
   4.7. Appel MCPTT pré-établi versus appel à la demande
   4.8. Appel MCPTT automatique versus appel manuel
   4.9. Floor Control pour la gestion du jeton de parole
   4.10. SIP, RTP et RTCP pour la mise en œuvre des communications MCPTT
   4.11. QoS pour les sessions MCPTT
   4.12. Interface Rx pour la mise en œuvre dynamique des dedicated bearers pour la voix

5. MCData
   5.1. Interfaces entre le client MCData et le serveur MCData
   5.2. Protocole de signalisation pour supporter les services MCData
   5.3. Protocole média pour supporter les services MCData
   5.4. SDS
      5.4.1. Standalone Short Data Service (SDS) one-to-one et de groupe via le plan SIP
      5.4.2. Standalone SDS one-to-one et de groupe via le plan média
         5.4.2.1. Protocole MSRP pour l'échange des SDS sur le plan média
      5.4.3. Session SDS one-to-one et session SDS de groupe
      5.4.4. Notifications de livraison et de lecture
   5.5. FD
      5.5.1. File Distribution (FD) one-to-one et groupe via http
      5.5.2. FD one-to-one et groupe via le plan média
   5.6. Data Streaming
   5.7. IP Connectivity
   5.8. QoS associées aux services MCData
   5.9. Interface Rx pour la mise en œuvre dynamique des dedicated bearers pour les données

6. MCVideo
   6.1. Interfaces entre le client MCVideo et le serveur MCVideo
   6.2. Appel MCVideo privé

6.3. Appel MCVideo de groupe
6.4. Appel MCVideo de groupe broadcast
6.5. Appel MCVideo privé et de groupe urgence
6.6. Appel MCVideo de groupe danger imminent
6.7. Video Pull
6.8. Video Push
6.9. Protocole Transmission Control pour la gestion du droit de parole
6.10. SIP, RTP et RTCP pour la mise en œuvre des communcations MCVideo
6.11. QoS associées aux services MCVideo
6.12. Interface Rx pour la mise en œuvre dynamique des dedicated bearers pour la vidéo

Réseau cœur paquet 5G : 5GC

Durée : 4 jours

Objectifs : Comprendre le réseau cœur paquet mobile 5GC

Prérequis : Connaissance des réseaux cœur paquet mobiles GPRS et ePC

Public : Ingénieurs télécom, Architectes télécom, Consultants télécom, ingénieur cœur de réseau

Le but de cette formation est de présenter le réseau coeur paquet mobile 5G appelé 5GC (5G Core) , notamment:

- Le réseau cœur 5GC prenant en charge la radio LTE, la radio WiFi et la nouvelle radio 5G
- Les fonctions réseau du réseau coeur 5G (5GC)
- Le réseau de signalisation basé sur des proxy HTTP pour le routage des opérations de service HTTP2 internes et externes (roaming)
- Le slicing de réseau dans le réseau coeur 5C
- L'interfonctionnement entre 5GC et ePC
- Le Policy and Charging Control dans le 5GC
- L'exposition de services réseau au monde externe via la NEF (Network Exposure Function)
- Les procédures de service 5GC (Enregistrement/désenregistrement de l'UE, établissement de session PDU, etc).
- La voix sur IP dans le contexte 5G

1. Evolution du réseau ePC pour l'interfonctionnement avec le nouveau réseau 5G
   1.1. Réseau d'accès 4G : LTE, LTE-Advanced, LTE-Advanced-Pro
   1.2. Réseau Coeur ePC et Architecture CUPS (Control and User Plane Separation)
      1.2.1. Décomposition SGW/PGW : SGW-C/PGW-C et SGW-U/PGW-U
   1.3. LTE pour l'IoT : LTE-M et NB-IoT

2. Réseau cœur 5G (5GC)
   2.1. Support des RAT NR, LTE et WiFi
   2.2. Fonctions réseau 5GC
      2.2.1. Authentication Server Function (AUSF)
      2.2.2. Core Access and Mobility Management Function (AMF)
      2.2.3. Session Management Function (SMF)
      2.2.4. Network Exposure Function (NEF)
      2.2.5. NF Repository Function (NRF)
      2.2.6. Policy Control function (PCF)
      2.2.7. User Data Repository (UDR)
      2.2.8. Unified Data Management (UDM)
      2.2.9. Network Slice Selection Function (NSSF)
      2.2.10. User plane Function (UPF)

2.2.11. Application Function (AF)
2.2.12. Unstructured Data Server Function (UDSF)
2.2.13. Binding Support Function (BSF)
2.2.14. Service Communication Proxy (SCP)
2.2.15. Security Edge Protection Proxy (SEPP)
2.2.16. Network Data Analytics Function (NWDAF)
2.2.17. Charging Function (CHF)
2.3. Interfaces point à point et interfaces de service
2.4. Principe d'API REST
2.5. Architecture de roaming 5GC : Local Breakout et Home Routed
2.6. Session PDU
2.7. QoS 5GC
2.8. Procédures 5GC
2.8.1. Procédure d'enregistrement
2.8.2. Procédure d'établissement de session PDU
2.8.3. Procédure Service Request initiée par l'UE
2.8.4. Procédure Service Request initiée par le réseau
2.9. Interfonctionnnement avec l'ePC
2.9.1. Enregistrement unique
2.9.2. Double enregistrement
2.10. SMS avec NAS 5GC

3. Réseau de signalisation 5GC
3.1. Mode quasi-associé pour le plan de contrôle du réseau 5GC avec SCP
3.1.1. Routing
3.1.2. Lod balancing
3.1.3. Congestion control
3.2. Session binding et BSF
3.3. Roaming et Security Edge Protection Proxy (SEPP)
3.3.1. Firewalling
3.3.2. Topology hiding
3.4. Relation entre SEPP et NRF
3.5. Scénarii de routage

4. Network slicing ou comment créer des réseaux personnalisés afin d'offrir une solution optimisée pour des scénarii associés à différents marchés, e.g., en terme de fonctionnalité, performance et isolation
4.1. Terminologie et définitions
4.2. Architecture Coeur de réseau de slice de réseau
4.3. Fonctions de réseau communes et fonction de réseau spécifiques à une instance de slice de réseau
4.4. Création, modification et suppression d'une instance de slice de réseau
4.5. Support de slice de réseau en roaming
4.6. Sélection et association d'une session PDU à une instance de slice de réseau
4.7. Domaines d'application pour le slicing 5G

5. Policy control et taxation dans la 5G (PCC)
5.1. Policy control ou l'intelligence du réseau 5G

5.2. Nouveaux scénarii PCC par rapport à ceux de la 4G
5.3. Architecture PCC : SMF, AMF, PCF, NWDA, Charging System, NEF, AF
5.4. Nouvelles interfaces de service pour PCC
5.5. Règles PCC
5.5.1. Règles de mobility management et règles d'UE
5.5.2. Règles de session management
5.5.2.1. Règles de gestion de QoS
5.5.2.2. Règles de background data transfer
5.5.2.3. Règles de traffic influence
5.5.2.4. Règles de traffic steering

6. Network Exposure dans la 5G
6.1. Architecture NEF (Network Exposure Function) et interfaces de service
6.2. Exposition de capacité de souscription/notification à des événements de réseau au monde externe et au monde interne
6.3. Exposition de capacité de provisioning aux fonctions externes
6.4. Exposition de capacités PCC à des fonctions externes
6.5. Exposition de capacités internes du cœur de réseau pour l'analytique
6.6. Exposition de capacité de service de device triggering

7. Voix sur IP sur 5G : VoNR
7.1. Architecture IMS pour VoNR
7.2. RAT Fallback
7.3. EPS Fallback
7.4. Emergency Services Fallback

Réseau de signalisation HTTP2 pour le réseau 5GC

Durée : 3 jours

Objectifs du séminaire : Comprendre l'architecture de signalisation associée au plan contrôle du réseau 5GC. Comprendre les protocoles NAS 5G et les services associés.

Pré-requis : Connaissance des réseaux de signalisation des réseaux mobiles

Public : Ingénieurs télécom, Consultants réseaux et télécom, Architectes réseau et services télécom, responsables télécom, ingénieurs avant-vente

L'introduction du réseau 5G fait apparaître un nouveau protocole de signalisation utilisé par les fonctions du plan contrôle du réseau coeur 5G, à savoir HTTP2 (HyperText Transfer Protocol version 2). Comme avec les réseaux coeur 2G/3G qui utilisent un réseau de signalisation SS7/SIGTRAN et le réseau coeur 4G qui utilise un réseau de signalisation DIAMETER, il est nécessaire pour le réseau coeur 5G de mettre en œuvre un réseau de signalisation HTTP2/JSON avec des routeurs de signalisation appelés SCP (Service Communication Proxy) pour le routage HTTP/2 interne à un réseau mobile et SEPP (Security Edge Protection Proxy) pour le routage entre un réseau mobile et les réseaux externes dans le contexte du roaming. HTTP/2 hérite du protocole HTTP/1.1 ses méthodes, ses codes de statut, ses headers mais améliore différents aspects du protocole HTTP/1.1 tels que le passage d ’un protocole texte à un protocole binaire, le multiplexage sur une même connexion TCP d ’un grand nombre de requêtes/réponses HTTP avec la priorisation des flux HTTP, la compression des en-têtes HTTP avec la méthode HPACK, le mécanisme de Server Push, etc. L ’échange des données dans les payloads des requêtes et réponses HTTP s ’effectue au format JSON (JavaScript Object Notation) Le but de cette formation est de présenter :

- Le protocole HTTP/1.1 pour comprendre le protocole HTTP/2,
- Les optimisations apportées par le protocole HTTP/2,
- Le réseau coeur 5G et notamment les fonctions de ce réseau qui contribuent au routage de la signalisation HTTP2, notamment, NRF, BSF, NSSF, SCP et SEPP, ainsi que leurs interfaces de service.
- Le routage de la signalisation HTTP/2.

1. Architecture 5GC
   1.1. Plan Contrôle 5GC
      1.1.1. Fonctions du plan contrôle
      1.1.2. Fonctions communes
      1.1.3. Fonctions spécifiques à un slice de réseau
      1.1.4. Architecture du plan contrôle basée sur le service

1.1.5. Interface de service
1.1.5.1. NF service
1.1.5.2. Opération de service
1.1.6. Fonctions du plan contrôle contribuant au routage du trafic HTTP2 : NSSF, NRF, BSF, SCP, SEPP, NEF
1.2. Plan usager 5GC

2. Protocole HTTP2
2.1. Protocole HTTP/1.1 : Méthodes, code de statut, Headers
2.2. Principes HTTP/2 : Message, Trame et Stream
2.3. Le format binaire
2.4. Multiplexage de flux
2.5. Priorités et dépendances
2.6. Compression d'en-tête : HPACK
2.6.1. Table statique
2.6.2. Table dynamique
2.6.3. Encodage Huffman
2.6.4. 2.5. Server push
2.7. HTTP2 et TLS
2.8. JSON

3. API REST
3.1. Principes REST
3.2. Contraintes REST
3.3. Exemples d'APIS de service dans le contexte 5GC relatives aux fonctions de routage
3.4. API de service de la NRF
3.5. API de service de la BSF
3.6. API de service de la NSSF

4. Architecture du réseau de signalisation HTTP2
4.1. Mode de communication
4.1.1. Communication directe avec et sans interaction avec NRF
4.1.2. Communication indirecte avec et sans délégation de découverte
4.2. Entité SCP (Service Communication Proxy) pour le routage de la signalisation HTTP2 interne à un réseau mobile
4.3. Entité SEPP (Security Edge Protection Proxy) pour le routage HTTP2 entre un réseau mobile et les réseau externes (dans le contexte du roaming)
4.4. Entité NRF pour les données de routage
4.5. Fonctions SCP : Routage, partage de charge et contrôle de congestion
4.6. Fonctions additionnelles SEPP : Masquage de la topologie et firewalling
4.7. Entité BSF et session binding
4.8. SCP/SEPP/SBF et Agent DIAMETER (DEA/DRA) combinés pour l'interfonctionnement 5GC/EPC

5. Procédures 5GS et HTTP2
5.1. Enregistrement/Désenregistrement

5.2. Mise à jour de localisation
5.3. Etablissement de session PDU
5.4. Service Request

6. Protocole NAS N1
   6.1. Identités NAS
   6.2. NAS 5GMM, NAS 5GSM, NAS 5GSMS
   6.3. Sécurité NAS
   6.4. NAS 5GMM
   6.5. NAS 5GSM
   6.6. NAS SMS

Technologies pour l'appel d'urgence : VoLTE, CSFB, Emergency Service Fallback, VoNR, VoWiFi, eCall, NG eCall

Objectifs : Comprendre la mise en œuvre du service d'appel d'urgence avec les différentes technologies suivantes : VoLTE, Circuit Switched Fallback (CSFB), VoNR, Emergency Service Fallback, VoWiFi ; comprendre la mise en œuvre du service eCall et NG-eCall (eCall avec l'IMS).

Pré-requis : Connaissance des principes de la « Voix sur IP », de SIP, RTP et du monde des mobiles

Public : Ingénieurs télécom plutôt orientés cœur de réseau, Consultants réseaux et télécom, Architectes réseau et services télécom, responsables télécom, chefs de projet télécom

L'IMS (IP Multimedia Subsystem) existe en tant qu'architecture pour offrir des services multimédia sur IP depuis un certain nombre d'années et de nombreux fournisseurs d'infrastructures ont investi de manière importante dans le développement de leurs produits et solutions IMS. La plate-forme IMS a un grand nombre de domaines d'application qui lui permettent de toujours projeter dans le futur : L'IMS offre aujourd'hui la téléphonie fixe résidentielle, la téléphoniqe fixe d'entreprise (IP Centrex, SIP Trunking), la téléphonie sur IP mobile (VoLTE, VoNR, VoWiFi, EPS Fallback).

Le but de ce cours est de présenter l'IMS, de décrire la téléphonie sur IP avec l'IMS et de se focaliser sur tous les scénarios d'appel d'urgence avec l'IMS.

1. LTE + ePC = EPS
   - 1.1. Définition et Architecture EPS de Haut Niveau
   - 1.2. Gestion de la Mobilité EPS
     - 1.2.1. Attachement normal
     - 1.2.2. Attachement d'urgence
   - 1.3. Gestion de Session EPS
     - 1.3.1. Etablissement des default bearers Internet, IMS et SOS
     - 1.3.2. Etablissement de dedicated bearer IMS et SOS pour la VoLTE
   - 1.4. Roaming EPS
     - 1.4.1. Mode Home routed pour l'APN Internet et l'APN IMS
     - 1.4.2. Mode Local Breakout pour l'APN SOS
   - 1.5. QoS EPS pour l'APN Internet, l'APN IMS et l'APN SOS
   - 1.6. Les services du domaine CS sur l'EPS : CS Fallback (CSFB)
     - 1.6.1. Appel voix et appel d'urgence en CSFB

2. NR + 5GC = 5GS
   - 2.1. Définition et Architecture 5GS de Haut Niveau
   - 2.2. Gestion de la Mobilité 5GS
     - 2.2.1. Enregistrement normal

- 2.2.2. Enregistrement d'urgence
- 2.3. Gestion de Session 5GS
  - 2.3.1. Etablissement de Sessions PDU Internet, IMS et SOS
- 2.4. Roaming 5GS
  - 2.4.1. Mode Home routed pour le DNN Internet et le DNN IMS
  - 2.4.2. Mode Local Breakout pour le DNN SOS
- 2.5. QoS 5GS pour le DNN Internet, le DNN IMS et le DNN SOS

3. Architecture IMS
   - 3.1. CSCF : P-CSCF, I-CSCF, S-CSCF pour le contrôle des sessions multimédia
   - 3.2. IMS-MGW, MGCF, BGCF, T-SGW pour l'interfonctionnement avec le domaine circuit (RTC, GSM)
   - 3.3. Base de données HSS, SLF et proxy agent DIAMETER pour la gestion de la mobilité de l'usager
   - 3.4. PCRF pour le policy control
   - 3.5. IMS-ALG, IMS-AGW, IBCF, TrGW pour le bearer control
   - 3.6. AS, MRF et SCIM pour l'exécution des services, la livraison des flux média et la gestion de l'interaction de services respectivement
   - 3.7. ATCF et ATGw pour le traitement SR-VCC
   - 3.8. E-CSCF et LRF pour les sessions d'urgence
   - 3.9. DNS et ENUM pour l'interfonctionnement entre réseaux IMS

4. AML : Advanced Mobile Location
   - 4.1. Objectifs d'AML
   - 4.2. Architecture AML
   - 4.3. Transport AML par SMS en 2G/3G/4G/5G
   - 4.4. Transport AML par HTTP PUSH en 2G/3G/4G/5G
   - 4.5. Transport AML par SIP INVITE en 4G/5G

5. Procédures IMS: Enregistrement/Désenregistrement
   - 5.1. Identités IMS depuis un accès large bande fixe
   - 5.2. Identités IMS depuis l'accès mobile (VoLTE/VoWiFi/VoNR/EPS Fallback)
     - 5.2.1. Identité sans module ISIM sur l'UICC
     - 5.2.2. Identités avec module ISIM sur l'UICC
   - 5.3. Enregistrement depuis l'accès EPS
     - 5.3.1. Enregistrement depuis le réseau nominal
     - 5.3.2. Enregistrement depuis un réseau visité (S8HR pour les appels normaux et LBO pour l'appel d'urgence)
   - 5.4. Enregistrement depuis l'accès 5GS
     - 5.4.1. Enregistrement depuis le réseau nominal
     - 5.4.2. Enregistrement depuis un réseau visité (N9HR pour les appels normaux et LBO pour l'appel d'urgence)

6. Procédures IMS: Contrôle de session
   - 6.1. Etablissement de session depuis un accès large bande fixe
   - 6.2. Etablissement de session voix sur IP sur LTE
   - 6.3. Etablissement de session voix sur IP sur WiFi
   - 6.4. Call flows associés

6.4.1. Session de VoLTE à Voix sur IP
6.4.2. Session de VoLTE à CS

7. Procédures IMS : Session d'urgence
   7.1. Architecture de session d'urgence : P-CSCF, E-CSCF, LRF, PSAP
   7.2. Traitement des appels au 112
   7.3. Traitement des appels au 15, 17, 18
   7.4. eSR-VCC pendant l'appel d'urgence en VoLTE
   7.5. Appel d'urgence en VoWiFi

8. SMS avec IMS
   8.1. Architecture de service SMS avec IMS
      8.1.1. IP-SM-GW AS
      8.1.2. HLR
      8.1.3. HSS
      8.1.4. SMSC
   8.2. Scénarii d'envoi et de réception de SMS
   8.3. SMS d'urgence
   8.4. Alerte aux populations : FR-Alert
      8.4.1. Approche cell broadcast
      8.4.2. Approche Location based SMS

9. SR-VCC (Single Radio Voice Call Continuity) pour garantir la continuité de la session voix entre LTE+ePC/IMS et 2G/3G R4
   9.1. Architecture SR-VCC
   9.2. Architecture Emergency SR-VCC
   9.3. Scénarios SRVCC

10. Vo5G
   10.1. Architectures Vo5G
      10.1.1. VoNR
      10.1.2. EPS Fallback (EPSFB)
      10.1.3. VoeLTE
      10.1.4. RAT Fallback
   10.2. Call flows associés
   10.3. Architecture d'appel l'urgence Vo5G
      10.3.1. VoNR
      10.3.2. Emergency Service Fallback
   10.4. Call flow d'appel d'urgence en VoNR
   10.5. Call flow d'appel d'urgence en Emergency Service Dallback

11. eCall et NG eCall
   11.1. Objectifs d'eCall
   11.2. Exigences eCall
   11.3. Etablissement d'appel eCall
   11.4. Minimum Set of Data (MSD) échangées Durant l'eCall
   11.5. Points faibles d'eCall

Les Architectures de Services Mobiles 5G SA : SMS, PWS, NEF, LCS, eMBMS, Edge Computing, 5GMS, MDT

Durée : 3 jours

Objectifs du séminaire : Comprendre les architectures de services dans le réseau 5GS : Messaging (SMS), Localisation (LB-SMS, CBS, LCS, MDT), diffusion (eMBMS), streaming (5GMS), services NEF et Edge Computing

Pré-requis : Connaissance minimum du réseau 5G SA appelé 5GS (5G System)

Public : Ingénieurs télécom et réseau, Architectes réseau, Consultants réseaux et télécom

Le réseau mobile 5G en mode SA s'appelle 5GS (5GS Packet system). Il est constitué d'un nouveau réseau d'accès appelé NR (New Radio) et d'un nouveau réseau cœur appelé 5GC (5G Core) tout IP. Indépendamment des services IP tels que la VoNR ou RCS mis en œuvre via des plates-formes de service IP de type IMS et accédées via le 5GS, le réseau 5GS lui-même offre des services aux clients 5G. Ces services sont décrits dans cette formation :

- Le service SMS : Alors que le SMS peut être mis en œuvre via le domaine l'IMS, il est possible d'émettre et recevoir des SMS via le réseau 5GS directement. Une architecture de service SMS in 5GS permet d'offrir le service. La formation décrit les différentes architecture SMS pour le 5GS.
- Les architectures pour l'alerte aux populations en 5G : Cell Broadcast et Location-based SMS. Le service Cell Broadcast (CBS) permet la diffusion d'un certain nombre de messages non acquittés à tous les récepteurs dans une région donnée appelée Cell Broadcast Areas. Ce service permet notamment la fonction de protection des populations en intégrant une capacité à avertir les populations de tout événement de sécurité civile : catastrophes naturelles (e.g., inondations, séisme, tsunami), technologiques (e.g., accident industriel), outre les attentats terroristes. Une alternation au CBS et le LB-SMS (Location-based SMS) qui permet dde délivrer un SMS en point à point à tous les usagers se trouvant dans la zone de diffusion.
- Le service de localisation (LCS) permettant de fournir la localisation de l'usager 5GS soit de base via l'information Cell ID qui correspond à l'identité de la cellule qui prend en charge l'UE, soit très précise avec des techniques telles que E-CellID (Enhanced Cell ID), OTDOA (Observed Time Difference of Arrival) et A-GNSS (Assisted Global Navigation Satellite Systems). Une architecture de service LCS dans le réseau 5GS est requise pour offrir ce service.
- Les services NEF (Network Expoisure Function) qui correspondent à des services du réseau 5G qui sont exposées au monde externe qui peut les invoquer via des APIs. Parmi ces services figurent des services de policy and charging control,

services de provisioninig, services de souscription/notification à des événements réseau, etc.

- Le service Evolved Multimedia Broadcast Multicast Service (E-MBMS) : L'architecture de service E-MBMS (Multimedia Broadcast MultiCast Service) permet de transmettre simultanément le même flux à tous les utilisateurs qui le souhaitent en utilisant le transport multicast dans le réseau cœur et un seul canal radio multicast.
- L'edge computing est un mode du traitement de données qui vise à effectuer les opérations au plus proche de la source des données. Les calculs prennent place à la périphérie du réseau ce qui diminue les temps de latence. L'edge computing implique donc une infrastructure locale sous forme de edge data centers. Une architectures Edge Computing 3GPP dans le 5GS est nécessaire pour offrir la fonctionnalité ; elle s'appuie sur les enablers offerts par le 5GS.
- 5G Media Streaming (5GMS) permet aux application providers souhaitant offrir des services de streaming en 5G d'utiliser les enablers 5G pour délivrer des services de qualité : edge computing, eMBMS, streaming session with QoS, etc. Une architecture 5GMS a été intégrée dans le 5GS.
- Minimization of drive tests : Grace cette fonctionnalité, les terminaux peuvent, sur demande du réseau, remonter des indicateurs de qualité radio (couverture, qualité de service selon le service) associés à l'information de géo-localisation (localisation où la mesure a été effectuée). Une exploitation efficace de ces mesures permettrait une gestion plus fine et plus personnalisée des ressources radio.

1. Architectures de service SMS pour un client 5GS
   - 1.1. SMS in 5GS
     - 1.1.1. Entités : AMF, SMSF, UDM/UDR, SMSC
     - 1.1.2. Interfaces Namf, Nsmsf, Nudm
     - 1.1.3. Interface MAP E ou DIAMETER SGd du SMSC
     - 1.1.4. Enregistrement au 5GS et assignation de la SMSF
     - 1.1.5. Envoi de SMS
     - 1.1.6. Réception de SMS
     - 1.1.7. Traitement d'erreur
     - 1.1.8. Données du profil de l'usager 5GS relatives à SMS in MME
   - 1.2. Architecture SMS over IP
     - 1.2.1. Envoi de SMS
     - 1.2.2. Réception de SMS

2. Public Warning System (PWS)
   - 2.1. CBS (Cell Broadcast Service) pour PWS
     - 2.1.1. Architecture CBS dans le 5GS
       - 2.1.1.1. CBE
       - 2.1.1.2. CBC/CBCF
       - 2.1.1.3. AMF
       - 2.1.1.4. gNB
       - 2.1.1.5. PWS-IWF
       - 2.1.1.6. Interfaces SBc, N50, N2

2.1.2. Format de message CBS entre CBCF et AMF et entre AMF et gNB
2.1.3. Formation de message SIB12 entre gNB et UE
2.1.4. Envoi de message CBS et call flow associé
2.2. LB-SMS (Location-Based SMS) pour PWS
2.2.1. Architecture
2.2.1.1. Base de données de localisation passive
2.2.1.2. Passerelle d'alerte
2.2.1.3. SMSC
2.2.1.4. Envoi de message LB-SMS et call flow associé
2.3. Différences entre CBS et LB-SMS

3. Architecture de service LCS (Location based Services)
3.1. Applications de localisation
3.2. Entités : GMLC, LMF, UDM, AMF, PPR
3.3. Interfaces : NL6, NL2, NL6
3.4. Protocole LPP entre UE et LMF
3.5. Protocole LPPa entre gNB et LMF
3.6. API entre les applications externes et le réseau mobile (i.e., GMLC) : MLP
3.7. Méthodes de localisation
3.7.1. Méthode basée sur le plan usager
3.7.2. Méthode basée sur le plan de contrôle
3.8. Techniques de localisation
3.8.1. Cell ID
3.8.2. Enhanced Cell ID
3.8.3. OTDOA
3.8.4. UTDOA
3.8.5. A-GNSS
3.9. Call flows de bout en bout pour les services de localisation
3.10. MT-LR
3.11. NI-LR
3.12. MO-LR

4. NEF : Network Exposure Function
4.1. Service de souscription/Notification à des évènements réseau standard
4.2. Service de provisioning (trafic influence, gestion des PFDs, gestion de l'economie d'énergie pour des devices IoT, etc)
4.3. Services PCC (background data transfer, AF session with QoS, etc.)
4.4. Service de device triggering
4.5. Services de livraison de données non-IP (données unstructured)

5. E-MBMS : Evolved Multimedia Broadcast Multicast Service
5.1. Applications nécessitant le mode broadcast ou multicast
5.2. Entités de l'architecture E-MBMS : BM-SC, MBMS GW, AMF, MCE, gNB
5.3. Interfaces
5.3.1. SGmb, SGi-mb, M1, M2, M3
5.4. E-MBMS User Services
5.4.1. Procédures de livraison associées

5.5. E-MBMS Bearer Services
5.5.1. Session Start
5.5.2. Session Stop
5.5.3. Session Update

6. Edge Computing dans le 5GS
6.1. Définition de l'edge computing
6.2. Avantages de l'Edge Computing
6.3. Domaines d'application de l'Edge Computing
6.4. Device edge computing aware versus Device edge computing unaware
6.5. Mobilité Edge Computing versus mobilité radiomobile
6.6. Acteurs de l'edge computing
6.6.1. ASP : Application Service Provider
6.6.2. ECSP : Edge Computing Service Provider
6.6.3. CSP : Communications Service Provider
6.6.4. Fonctions prises en charge par chaque acteur dans l'architecture edge computing
6.7. Architecture Edge Computing 3GPP
6.7.1. Fonctionnalités EDGEAPP (Architecture for enabling Edge Applications)
6.7.2. AC (Application Client)
6.7.3. EEC (Edge Enabler Client)
6.7.4. EES (Edge Enabler Server)
6.7.5. EAS (Edge Application Server)
6.7.6. ECS (Edge Configuration Server)
6.7.7. Interfaces EDGE entre les entités de l'architecture : EDGE 1 à EDGE 9
6.8. Identités Edge Computing
6.9. Modèles de déploiement possibles de l'architecture Edge Computing 3GPP
6.10. Procédures Edge Computing 3GPP
6.10.1. Enregistrement
6.10.2. Découverte des EAS
6.10.3. Scénarios d'Application Context Relocation (ACR)
6.10.4. APIs exposées par le réseau 5G SA via la NEF ou la PCF à l'architecture Edge Computing 3GPP et procédures associées
6.10.5. API AF Traffic Influence
6.10.6. API UE Location
6.10.7. API UE Identifier
6.10.8. AF Session With QoS
6.10.9. API UE Expected Behavior

7. 5GMS (5G Media Streaming)
7.1. Streaming dans le contexte 5GS
7.2. Architecture 5GMS
7.2.1. 5GMS Client
7.2.1.1. Media Session Handler
7.2.1.2. Media Streamer
7.2.2. 5GMS AF

7.2.3. 5GMS AS
7.2.4. Interface entre les composants de l’architecture
7.3. Architecture 5GMSd
7.4. Architecture 5GMSu
7.5. Intrégration d’Edge Computing dans 5GMS
7.6. Intégration d’eMBMS dans 5GMS
7.7. Procédure 5GMS
7.7.1. Configuration du 5GMS Client avec les informations d’accès au service
7.7.2. Consumption reporting
7.7.3. Metrics reporting
7.7.4. Policy invocation
7.7.5. Network assistance

8. Minimization of Drive Test (MDT)
8.1. Avantages de MDT
8.2. Signaling-based MDT versus Management-based MDT
8.3. Architecture Signaling-based MDT
8.4. Architecture Management-based MDT
8.5. Types de MDT
8.5.1. Immediate MDT
8.5.2. Logged MDT
8.5.3. Accessibility MDT
8.6. Architecture de collecte MDT
8.7. Paramètres mesurés pour les immediate MDTs :
8.7.1. RSRP, RSRQ, Power Headroom
8.7.2. Data volume, throughput, delay, loss
8.8. Paramètres mesurés pour les Logged MDTs :
8.8.1. RSRP, RSRQ

Les Réseaux Privés 5G

Durée : 2 jours

Objectifs : Comprendre les réseaux privés 5G, leurs spécificités, les modèles de déploiement possibles et des exemples de déploiement.

Pré-requis : Connaissance minimum du réseau 5G

Public : Ingénieur télécom, architecte telecom, chef de projet telecom

Les réseaux privés 5G sont des réseaux de communication basés sur la technologie 5G qui sont spécifiquement déployés et exploités pour une utilisation privée par une organisation ou une entreprise, plutôt que pour une utilisation publique. Ces réseaux privés permettent aux organisations de disposer de leur propre infrastructure de communication 5G hautement performante et sécurisée pour répondre à leurs besoins spécifiques. Le but de cette formation est de présenter tous les aspects relatifs aux réseaux privés 5G afin de comprendre les réseaux privés 5G de bout en bout. La formation présente en particulier la technologie 5G, les modèles de déploiement possible pour les réseaux privés 5G, les optimisations définies pour les réseaux privés 5G en fonction des cas d'usage. La formation présente aussi des exemples de déploiement de réseaux privés 5G.

1. Introduction
   - 1.1. Rappels sur l'évolution des réseaux radio mobiles depuis la 2G jusqu'à la 5G
   - 1.2. Concepts de réseaux privés :
     - 1.2.1. Principes
     - 1.2.2. Avantages/inconvénients
     - 1.2.3. Difficultés à venir
     - 1.2.4. Acteurs potentiels ciblés
     - 1.2.5. Stratégies et option de déploiement possibles
     - 1.2.6. Liens avec les réseaux grand public
     - 1.2.7. Rôle du 3GPP
     - 1.2.8. Statut actuel

2. Focus 5G :
   - 2.1. Genèse de la 5G
   - 2.2. Quels services pour la 5G ? (eMBB / mMTC/uRLLC)
   - 2.3. Aspects Radio : fréquences, architecture RAN, interface radio, protocoles, interfaces et principales procédures
   - 2.4. Aspects Core Network : lien avec le RAN, architecture CN, protocoles, interfaces et principales procédures, gestion de la mobilité (handover & roaming), des sessions et de la sécurité, focus SDN/NFV, Slicing et MEC, optimisations spécifiques pour l'uRLLC

3. Réseaux Privés 5G :

3.1. Modèles de déploiement possibles :
  3.1.1. SNPN : Standalone Non-Public Network
  3.1.2. PNI-NPN : Public Network Integrated – Non Public Network
  3.1.3. 5G Hybrid Private Network Architecture
  3.1.4. 5G Virtual Private Network Architecture
3.2. Aspects fréquences :
  3.2.1. Bandes licenciées, licenciées partagées ou sans licence
  3.2.2. Optimisation 5G pour un usage sur des bandes sans licences
  3.2.3. Concurrence avec le modèle WiFi
3.3. Optimisations 5G spécifiques à certains scénarios fortement liés aux réseaux privés :
  3.3.1. Aspects Identification, Authentification et Sécurité
  3.3.2. Aspects Mobilité : roaming/handover public-privé, privé-privé
  3.3.3. Aspects MCX (Mission Critical Voice, Video & Data)
  3.3.4. Aspects V2X (Vehicular to Everything)
  3.3.5. Aspects TSN (Time Sensitive Network)
  3.3.6. Aspects UAV (Unmanned Aerial Vehicle)

4. Exemples de déploiement de réseaux privés : architecture, services et exemple d'implémentations
  4.1. Réseau pour assurer des missions critiques (Public Safety)
  4.2. Réseau pour le ferroviaire (Train/Metro)
  4.3. Réseau pour les véhicules routiers (Ville/Autoroute) ou volants (Drones)
  4.4. Réseau dans les usines intelligentes et les ports communicants

Découvrir la Virtualisation/Conteneurisation de réseau et de service, SDN et NFV

Objectifs : Comprendre la mise en oeuvre de la virtualisation/conteneurisation dans l'infrastructure des télécommunications. Comprendre la notion de Network Function Virtualization (NFV). Appréhender la notion de Software Defined Network (SDN) et de réseau programmable, et leur application dans le contrôle des infrastructures réseau virtualisées.

Pré-requis : Aucune connaissance particulière

Public : Ingénieurs télécom et SI, Architectes télécom et SI, Consultants télécom, ingénieurs avant-vente

Les technologies SDN (Software Defined Networks) et NFV (Network Functions Virtualisation) devraient révolutionner à terme les architectures des réseaux des opérateurs, et permettre de déployer des nouveaux services de manière beaucoup plus rapide et avec des coûts significativement réduits. Elles changeront complètement l'écosystème des infrastructures de Télécommunication dans les années à venir, notamment avec l'arrivée du réseau 5G dont le réseau d'accès et le réseau cœur sont complétement conçus sur la base des technologies SDN et NFV. De quoi s'agit-il? La Virtualisation des Fonctions Réseau (NFV en anglais) est un élément déterminant pour optimiser l'utilisation des ressources du réseau en « virtualisant » des fonctions habituellement mises en œuvre dans le matériel propriétaire, réduisant ainsi pour les opérateurs les coûts d'investissement et d'exploitation. La solution NFV est basée sur le principe de séparation entre une couche matérielle banalisée et standardisée de type « Data Center » et une couche logicielle applicative implantant des fonctions nécessaires au fonctionnement du réseau d'un opérateur (services de la couche 4 à la couche 7 tes que firewall, NAT, Load balancer, système d'inspection de paquets, etc). Les architectures de matériel de routage et switching IP évoluent en parallèle suivant la standardisation poussée par l'ONF (Open Networking Foundation) appelée SDN (Software Defined Networking), visant à séparer la couche de transport IP et la couche de contrôle du routage IP, avec la mise en place d'un protocole « ouvert » appelé Openflow, permettant à la couche de contrôle d'inter-opérer avec des matériels de constructeurs différents. Le SDN est donc complémentaire de la technologie NFV et permet de mettre en place des solutions purement logicielles rendant possible le contrôle d'un réseau soit d'entreprise, soit d'opérateur. Le but de cette formation est de décrire la virtualisation/conteneurisation de réseau et de service, les nouveaux concepts pour y parvenir tels que NFV et SDN avec leurs composants clés ainsi que les stratégies des principaux acteurs du monde des réseaux de télécommunication. SDN et NFV sont appliqués au réseau ePC, au réseau 5GC, au RAN, ainsi qu 'au chaînage de service.

1. Virtualisation
   1.1. Une définition
   1.2. Quoi virtualiser ?

1.3. Architecture générique de virtualisation
1.4. Virtualisation de serveur
  1.4.1. Architecture de serveur virtualisé
1.5. Hyperviseur
  1.5.1. Types d'hyperviseur : Types 1 et 2
  1.5.2. Fonctions de l'hyperviseur
  1.5.3. Exemples d'hyperviseur de type 1 et 2
1.6. Para virtualisation
1.7. Conteneurisation
  1.7.1. Conteneurisation versus virtualisation
  1.7.2. Couches de conteneurisation : LXC, LXD, Docker
  1.7.3. Kubernetes : Orchestration d'applications conteneurisées
    1.7.3.1. Cluster, Master et Node Kubernetes
    1.7.3.2. Objets Kubernetes : Pod, Service, Replicat-Set, Deployment
    1.7.3.3. Fichier déclaratif pour le déploiement et la gestion automatisée d'application conteneurisée
1.8. Virtualisation de réseau
  1.8.1. VLAN
  1.8.2. VxLAN

2. SDN : Software Defined Network
  2.1. Pourquoi SDN ?
  2.2. Architecture du SDN
    2.2.1. Caractéristiques du SDN
      2.2.1.1. Séparation des plans contrôle et données
      2.2.1.2. Virtualisation et automatisation du réseau
      2.2.1.3. Ouverture via des interfaces et APIs standard
    2.2.2. Architectures SDN : Raisons de leur succès et exemples d'applications
  2.3. Les opérations du SDN
  2.4. Les composants du SDN
    2.4.1. Le contrôleur
      2.4.1.1. Modules du contrôleur
      2.4.1.2. Interfaces du contrôleur
    2.4.2. Les commutateurs
      2.4.2.1. Commutateur logiciel SDN
      2.4.2.2. Commutateur matériel SDN
    2.4.3. Les Applications
    2.4.4. Les interfaces SDN et les protocoles/APIs associés
      2.4.4.1. Southbound API
      2.4.4.2. Northbound API
      2.4.4.3. Westbound/Eastbound API
  2.5. Exemple de solutions SDN

3. Openflow en tant que southbound API
  3.1. But d'Openflow
  3.2. Structure d'un commutateur Openflow
  3.3. Tables OpenFlow : Table de flux, table de métrage, table de groupe
  3.4. Pipeline Openflow
  3.5. Protocole Openflow
    3.5.1. Messages Controleur-à-Switch

- 3.5.2. Messages symétriques
- 3.5.3. Messages asynchrones
- 3.6. Call flows OpenFlow

4. Applications SDN
   - 4.1. Chainage de service dynamique pour le traffic steering : SGi-LAN
   - 4.2. SD-WAN
   - 4.3. SDN Overlay pour la configuration automatique de VLAN/VxLAN dans les data centers virtualisés
   - 4.4. SDN dans la 5G
   - 4.5. SDN pour l'ouverture des middles boxes

5. NFV : Network Function Virualization
   - 5.1. Définition
   - 5.2. Fonctions réseau candidates pour la virtualisation
   - 5.3. NFV et le chainage de service
   - 5.4. Architecture de référence NFV
     - 5.4.1. NFVI et relation avec OPNFV
     - 5.4.2. MANO
     - 5.4.3. VNF/EMS
     - 5.4.4. OSS/BSS
     - 5.4.5. Interfaces de l'architecture NFV
   - 5.5. MANO : Management and Orchestration
     - 5.5.1. NFVO
     - 5.5.2. VNFM
     - 5.5.3. VIM
     - 5.5.4. Repositories : VNF catalog, Network services, NFV instances, NFVI resources
     - 5.5.5. ONAP et OSM pour la mise en œuvre de MANO
   - 5.6. Instanciation et terminaison de VNF
   - 5.7. Exemple d'architectures virtualisées
     - 5.7.1. vEPC
     - 5.7.2. vIMS
     - 5.7.3. Livebox virtualisée
     - 5.7.4. vRAN
   - 5.8. Relation entre SDN et NFV

6. 5G, SDN et NFV
   - 6.1. Réseau accès 5G et Cloud RAN
   - 6.2. Architecture du réseau cœur 5G
   - 6.3. Slices de réseau 5G
   - 6.4. Réseau cœur 5G et SDN
   - 6.5. Réseau cœur 5G et NFV

APIs de la NEF et leur mise en œuvre

Objectifs : Comprendre les APIs de la NEF et leur mise en œuvre. Comprendre les call flows de chacun des APIs

Pré-requis : Connaissance minimum des réseaux cœur mobile 4G, 5G NSA et 5G SA

Public : Ingénieurs télécom, Consultants réseaux et télécom, Architectes réseau et services télécom, responsables télécom

La Network Exposure Function (NEF) est un composant clé de l'architecture 5G SA . Elle permet aux applications externes (AF - Application Function) d'accéder de manière sécurisée aux capacités du réseau mobile 5G SA via des interfaces normalisées. Les API exposées par la NEF facilitent l'innovation, la personnalisation des services et la monétisation des fonctionnalités réseau.

1. Network Exposure Function dans le réseau 5GS
   - 1.1. Fonctions de la NEF
   - 1.2. Architecture de la NEF
   - 1.3. NEF versus SCEF
   - 1.4. NEF/SCEF combinées
   - 1.5. Identités de l'UE ou d'un groupe d'UE pour invoquer les APIs de la NEF
   - 1.6. Familles d'APIs de la NEF
     - 1.6.1. API de provisioning
     - 1.6.2. API de policy and Charging
     - 1.6.3. API de monitoring
     - 1.6.4. APIs de Non IP Data Delivery
     - 1.6.5. etc.
     - 1.6.6. APIs communes à la SCEF et à la NEF
     - 1.6.7. APIs spécifiques à la NEF

2. APIs de la NEF exposées vers les AFs externes
   - 2.1. API Event Monitoring permettant à l'AF de souscrire et être notifié du changement d'état d'un UE ou d'un groupe d'UEs (15 événements sont proposés)
   - 2.2. API Device Triggering permettant à une AF de délivrer un message à un UE ou un groupe d'UEs.
   - 2.3. API Background Data Transfer Policy Negotiation permmetant à l'AF de négocier une politique de transfert de données pour un groupes de devices.
   - 2.4. API Traffic Influence permettant à l'AF d'influencer le choix de l'UPF qui prend en charge le trafic d'un UE.
   - 2.5. API Network Configuration Parameter Provisioning pour configurer des paramètres liés à l'économie d'énergie d'un device IoT.
   - 2.6. API AF Session With QoS permettant à une AF de demander une QoS pour un flux échangé entre l'AF et un UE.

2.7. API MSISDN-less Mobile Originated SMS permettant à un UE d'émettre un SMS à une AF sans que l'UE n'ait de MSISDN.
2.8. API NIDD pour permettre à un device d'échanger des données avec une AF via une session PDU Non-IP (i.e., unstructured).
2.9. API Analytics Information Exposure permettant à une AF d'obtenir des données d'analytics concernant un slice donné ou concernant des UEs (données de mobilité, de connectivité, etc).
2.10. API 5G LAN Parameter permettant à l'AF de créer, modifier, supprimer des groupes. Cela permet ensuit d'invoquer les APIs de la NEF pour des groupes de devices.
2.11. API SliceParamProvision pour permettre à l'AF de configurer des paramètres d'une instance de slice de réseau.
2.12. API UeAddress pour permettre à une AF de récupérer l'adresse IP assignée à un UE.
2.13. API UE ID retrieval permettant à l'AF d'obtenir le SUPI ou le GPSI d'un UE à partir de son adresse IPv4 et d'un numéro de port publics ou à partir d'une adresse IPv6.
2.14. API Service Specific Parameter Provisioning permettant à une AF de configurer des données de services relatives à un UE telles que l'URSP.
2.15. API Mobile Originated Location Request permettant à la NEF de notifier la localisation de l'UE fournie par le GMLC à l'AF.
2.16. API AM Policy Authorization permettant à l'AF de configurer une AM policy applicable à un UE. Cette AM policy est relayer par la NEF à la PCF et de la PCF à l'AMF afin que l'AMF puisse l'appliquer.
2.17. Autres APIs

3. APIs de la NEF exposées vers les fonctions réseau (NF) internes
   3.1. API de la NEF utilisée par la SMF pour NIDD : API Nnef_SMContext
   3.2. API de la NEF utilisée par le SMSC pour MSISDN-less SMS : API Nnef_SMService
   3.3. API de la NEF utilisée par NWDAF ou LMF pour souscrire aux changements d'état de l'UE : API Nnef_EventExposure
   3.4. API de la NEF utilisée par le GMLC pour obtenir le SUPI de l'UE à partir du GPSI ou de l'adresse IP de l'UE : API Nnef_UEId

4. Modèle de données de l'usager présentes dans l'UDR manipulées par la NEF
   4.1. Subscription data
   4.2. Policy data
   4.3. Structured data for exposure
   4.4. Application data
      4.4.1. AccessAndMobilityData
      4.4.2. PduSessionManagementData

APIs CAMARA et leur mise en œuvre

Objectifs : Comprendre les APIs CAMARA et leur mise en œuvre. Comprendre les call flows de chacun des APIs

Pré-requis : Connaissance minimum des réseaux cœur mobile 4G, 5G NSA et 5G SA

Public : Ingénieurs télécom, Consultants réseaux et télécom, Architectes réseau et services télécom, responsables télécom

Le secteur des télécommunications mobiles est à l'aube d'une mutation majeure, motivée par plusieurs facteurs, à la fois opportunistes et contextuels. Dans le contexte technologique global, la virtualisation de l'infrastructure réseau ouvre la voie à une approche plus dynamique et agile des fonctions réseau, implémentées sous la forme de logiciels. Parallèlement, les secteurs du logiciel et de l'IT connaissent leur propre transformation avec l'essor du cloud, la conteneurisation des charges utiles et la décomposition fonctionnelle d'applications monolithiques en services modulaires. La convergence de ces deux mondes n'était qu'une question de temps, créant ainsi une formidable opportunité pour le secteur des télécommunications d'adopter de nouveaux modèles de livraison de services et de business associés.

Conceptuellement, les réseaux programmables existent depuis un certain temps, mais ce n'est qu'aujourd'hui que les avantages de la programmabilité peuvent être concrétisés par les fournisseurs de services de communication grâce à une architecture orientée services (aaS). Tout comme pour l'IT as a Service, le service en tant que service dans le domaine mobile repose sur la capacité à masquer la mise en œuvre et la complexité des services réseau derrière un « contrat » programmatique sous la forme d'une interface de programmation d'applications (API). Pour intégrer les APIs aux services réseau, il est impératif que les opérateurs fournissent aux développeurs d'applications un cadre de type « franchise » où, quel que soit l 'opérateur, ils peuvent compter sur les mêmes fonctionnalités, conformes à un ensemble uniforme de normes, de spécifications et de processus. Conformément au principe Triple S (Sécurité, Simplicité et Scalabilité), les services réseau et leurs API réseau correspondantes doivent être sécurisés et préserver la confidentialité des utilisateurs, simples à utiliser pour les développeurs d'applications non familiarisés avec les protocoles réseau, et être scalable aux besoins des utilisateurs et des opérateurs dans de multiples domaines géographiques et marchés. Des initiatives telles que GSMA Open Gateway, le projet CAMARA de la Fondation Linux et le TM Forum Open Digital Architecture (ODA) collaborent pour établir la franchise d'API réseau de demain.

Les APIs CAMARA proposées ont pour but de masquer la complexité des APIs de réseau proposées par le réseau de télécommunication afin que les APIs soient faciles à utiliser pour les clients n'ayant aucune expertise en télécommunications (API conviviales).

Le but de cette formation et de passer en revue les APIs de service CAMARA, décrire leur objectif, leur structure et montrer comment les mettre en œuvre.

1. Ecosystème CAMARA
   1.1. Utilisateur
   1.2. ASP
   1.3. CSP
   1.4. Agrégateur et Telco Finder
   1.5. Hyperscaler

2. Open Gateway Platform GSMA
   2.1. Architecture de l'Open Gateway Platform
   2.2. APIs
      2.2.1. Northbound APIs = APIs CAMARA
      2.2.2. Southbound APIs
         2.2.2.1. SBI-NR : Network resources API
         2.2.2.2. SBI-CR : Cloud resources API
         2.2.2.3. SBI-CHF : Charging APIs
         2.2.2.4. SBI-OAM : OAM APIs
      2.2.3. West and Eastbound API
   2.3. Compatibilité avec CAPIF (Common API Framework)
   2.4. Compatibilité avec SEAL (Service Enabler Architecture Layer for Verticals)
   2.5. Open Gateway Platform versus NEF/SCEF

3. APIs CAMARA
   3.1. APIs relatives aux informations de devices
      3.1.1. API Device Roaming Status
      3.1.2. API Device Roaming Status Subscriptions
      3.1.3. API Device Reachability Status
      3.1.4. API Device Reachability Status Subscriptions
      3.1.5. API Connected Network Type
      3.1.6. API Connected Network Type Subscriptions
      3.1.7. API Device Identifier
   3.2. APIs relatives aux services de localisation
      3.2.1. API Location Retrieval
      3.2.2. API Location Verification
      3.2.3. API Geofencing Subscriptions
      3.2.4. API Population Density Data
      3.2.5. API Region Device Count
   3.3. APIs relatives à des services de communication
      3.3.1. WebRTC Call Handling
      3.3.2. WebRTC Event Subscription
      3.3.3. WebRTC REgistration
   3.4. APIs relatives à la qualité de communication
      3.4.1. API QoS Profiles
      3.4.2. API Quality on Demand
      3.4.3. API QoD Provisioning
      3.4.4. API Application Profiles

Evolution des Réseaux et Services Mobiles de la 2G à la 5G

Objectifs : Comprendre les réseaux et les services mobiles de bout en bout de la 2G à la 5G.

Pré-requis : Connaissances générales sur les réseaux mobiles

Public : : Collaborateur amené à appréhender l'architecture et le fonctionnement du réseau mobile.

Depuis les années 1990, les réseaux et services mobiles ont connu une évolution rapide, passant de la 2G, centrée sur la voix et les SMS, à la 3G qui a ouvert la voie à l'Internet mobile. La 4G a ensuite marqué un tournant avec le haut débit mobile et l'essor des usages multimédias. Aujourd'hui, la 5G poursuit cette dynamique en offrant des débits ultra-rapides, une faible latence et une connectivité massive, ouvrant la voie à de nouveaux services comme l'Internet des objets, la réalité augmentée et les applications critiques en temps réel.

Le but de cette formation est de comprendre le réseau et les services mobiles de bout en bout de la 2G à la 5G :

- Connaître l'architecture du réseau mobile (accès et cœur) et les infrastructures de services (Voix, Data) qui sont utilisées
- Comprendre le fonctionnement de l'infrastructure "Réseau": le réseau d'accès 2G à 5G, le RAN Backhaul, le transport backhaul, le réseau cœur 2G à 5G.
- Comprendre les infrastructures de Services Voix et Data utilisées dans le mobile avec une vision de bout en bout.
- Comprendre les différents call flows de bout en bout

1. Réseau mobile
   1.1. 2G
   1.2. 3G/3G+
   1.3. 4G/4G+
   1.4. 5G NSA
   1.5. 5G SA
   1.6. Non Terrestrial Network et le réseau mobile
   1.7. Que se trame-t-il avec la 6G ?

2. Composants des réseaux mobiles
   2.1. Réseau d'accès
   2.2. RAN Backhaul
   2.3. Transport Backhaul
   2.4. Réseau cœur
   2.5. Plate-forme de service
   2.6. Sites radio, agrégation, cœur pour le déploiement du réseau mobile
   2.7. Cloud Telco pour le déploiement des futurs réseau mobiles
   2.8. Virtualisation/Conteunirisation du réseau d'accès, du réseau cœur et des plate-formes de services
   2.9.

3. Réseau d'accès
   3.1. Réseau d'accès 2G : BSS
   3.2. Réseau d'accès 3G : UTRAN
   3.3. Réseau d'accès 4G : eUTRAN
   3.4. Réseau d'accès 5G : NG-RAN
   3.5. 5G NSA
   3.6. 5G SA
   3.7. RAN sharing avec MORAN et MOCN

4. RAN Backhaul (collecte)
   4.1. De la collecte mobile à la collecte unifiée fixe/mobile
      4.1.1. PE d'agrégation
      4.1.2. PE unifié

5. Transport backhaul (agrégation et transport national)
   5.1. Structure du backbone IP
   5.2. Du transport mobile au transport unifié fixe/mobile

6. Réseau cœur
   6.1. Cœur circuit 2G/3G = R4
   6.2. Cœur paquet 2G/3G = GPRS
   6.3. Cœur paquet 4G = EPC pour la 4G et la 5G NSA
   6.4. Cœur paquet 5G = 5GC pour la 5G SA

7. Plate-formes de service
   7.1. SMSC
   7.2. MMSC
   7.3. IMS pour VoLTE/VoWiFI/EPS Fallback et VoNR
   7.4. GMLC pour les services de localisation
   7.5. CBS pour FR-Alert
   7.6. RCS Personne à Personne et RCS Application à Personne
   7.7. MCX pour les communications critiques avec MCPTT, MCVideo et MCData

8. Service voix
   8.1. Voice circuit 2G/3G
   8.2. Circuit Switched Fallback
   8.3. Voice sur IP sur LTE : VoLTE
   8.4. Voix sur IP sur WiFi : VoWiFi
   8.5. Voix sur 5G (Vo5G) : VoNR et EPS Fallback

9. Service de données
   9.1. Contexte PDP 2G/3G
   9.2. Default et Dedicated bearer 4G
   9.3. Session PDU 5G SA
      9.3.1. Session PDU IP
      9.3.2. Session PDU Ethernet
      9.3.3. Session PDU Unstructured (Non-IP)

10. Procédures mobiles de bout en bout
    10.1. Attachement au réseau circuit 2G/3G

- 10.2. Etablissement d'appel circuit 2G/3G
- 10.3. Envoi/réception de SMS dans le domaine circuit 2G/3G
- 10.4. Attachement au réseau paquet 2G/3G (GPRS)
- 10.5. Etablissement de contexte PDP dans le domaine paquet 2G/3G et notation d'APN
- 10.6. Attachement au réseau paquet 4G EPC
- 10.7. Etablissement de default bearer dans le domaine paquet EPC
- 10.8. Enregistrement au réseau paquet 5GC
- 10.9. Etablissement de session PDU dans le domaine paquet 5GC
- 10.10. Ré-établissement du RAB (Radio Access Bearer) dans les différents réseaux mobiles

11. Policy and Charging Control (PCC) dans le domaine paquet mobile
    - 11.1. Principes du policy control appliqué à la connexion data mobile
        - 11.1.1. Identification des flux
        - 11.1.2. Blocage/autorisation des flux
        - 11.1.3. Dégradation de la QoS des flux
    - 11.2. Principes du charging control
        - 11.2.1. Taxation des flux en online charging
        - 11.2.2. Taxation des flux en offline charging
    - 11.3. Scénarios PCC
        - 11.3.1. Faire use, forfait bloqué, prépayé
        - 11.3.2. Pass data roaming international, anti bill shock, turbo button, etc.

12. Mobilités
    - 12.1. Mobilité dans l'état IDLE et mobilité dans l'état CONNECTED
    - 12.2. Mobilité 2G
    - 12.3. Mobilité 3G
    - 12.4. Mobilité 4G
    - 12.5. Mobilité 5G NSA
    - 12.6. Mobilité 5G SA
    - 12.7. Mobilité 4G/3G
    - 12.8. Mobilité 5G SA/4G

13. Roaming mobile
    - 13.1. Accords de roaming bilatéral et multilatéral
    - 13.2. Roaming Hub versus Roaming sponsor
    - 13.3. Structure des réseaux mobiles en situation de roaming (roamer-in et roamer-out)
    - 13.4. Types d'accord de roaming
        - 13.4.1. Roaming GSM
        - 13.4.2. Roaming GPRS
        - 13.4.3. Roaming 4G
        - 13.4.4. Roaming LTE
        - 13.4.5. Roaming VoLTE
        - 13.4.6. Roaming 5G NSA
        - 13.4.7. Roaming 5G SA
        - 13.4.8. Roaming Vo5G

Services de Localisation 4G/5G

Durée : 1 à 2 jours

Objectifs : Comprendre la localisation mobile 4G/5G à travers son architecture, les méthodes de localisation et les call flows et scénarios associés.

Pré-requis : Connaissance minimum des réseaux cœur mobile 4G et 5G SA

Public : Ingénieurs télécom, Consultants réseaux et télécom, Architectes réseau et services télécom, responsables télécom

La localisation des terminaux mobiles constitue aujourd'hui un enjeu stratégique majeur pour les réseaux 4G et 5G. Elle est au cœur de nombreux services commerciaux (applications LBS, services contextuels, géofencing, analytics), mais également de services réglementaires et de sécurité publique, tels que l'interception légale ou les services d'urgence.

Les réseaux mobiles modernes mettent en œuvre un ensemble complexe de fonctions réseau, d'interfaces normalisées et de protocoles de signalisation, permettant de déterminer la position d'un terminal avec des niveaux de précision variables, depuis la simple localisation cellulaire jusqu'aux méthodes avancées basées sur le temps, l'angle ou des approches hybrides.

Cette formation a pour objectif de fournir une vision complète et opérationnelle des mécanismes de localisation dans les réseaux LTE (4G) et 5G, depuis les principes fondamentaux de mobilité jusqu'aux architectures de localisation, aux procédures C-Plane et U-Plane, et aux méthodes de positionnement radio.

Une attention particulière est portée à l'évolution vers la 5G Standalone, à l'exposition des capacités de localisation via des APIs normalisées (CAMARA, NEF/SCEF), ainsi qu'aux usages concrets de la localisation dans les services numériques actuels.

À l'issue de cette formation, les participants disposeront d'une compréhension claire des architectures, protocoles, interfaces et méthodes de localisation, leur permettant d'analyser, concevoir ou exploiter des services LBS dans les réseaux mobiles 4G et 5G.

1. Fonctionnement du réseau mobile et principes de localisation
   1.1. Localisation dans l'état IDLE : TAI (Tracking Area Identity)
   1.2. Localisation dans l'état CONNECTED : Cell-ID

2. Architecture de localization
   2.1. 4G : MME, E-SMLC, HSS
   2.2. 5G : AMF, LMF, UDM
   2.3. GMLC, PPR, LRF, SLP

2.4. Interfaces 4G : SLh, SLg, LPP, LPPa
2.5. Interface 5G SA : Nlmf, Nudm, Namf, LPP, NRPPa

3. APIs de service et exposition de la localisation
   3.1. Interface Le : Protocole MLP
   3.2. APIs CAMARA
      3.2.1. API Location Retrieval
      3.2.2. API Location Verification
      3.2.3. API Geofencing Subscriptions
      3.2.4. API Population Density Data
      3.2.5. API Region Device Count
      3.2.6. APIs NEF/SCEF

4. Procédure de Localisation Plan Contrôle (C-Plane)
   4.1. MT-LR (Mobile Terminated Location Request) pour les services commerciaux
   4.2. MT-LR (Mobile Terminated Location Request) pour les services réglementaires
   4.3. MO-LR (Mobile Originated Location Request)
   4.4. NI-LR (Network Induced Location Request)

5. Procédure de Localisation Plan Usager (U-Plane)
   5.1. Protocole ULP (UserPlane Location Protocol)
   5.2. Protocole de positionnement LPP/LPPe
   5.3. Localisation WiFi, GNSS, A-GNSS

6. Méthodes de localisation cellulaire
   6.1. 4G
      6.1.1. E-CID (Enhanced Cell ID)
      6.1.2. OTDOA (Observed Time Difference Of Arrival)
      6.1.3. UTDOA (Uplink Time Difference Of Arrival)
   6.2. 5G
      6.2.1. NR-OTDOA
      6.2.2. NR-E-CID
      6.2.3. NR-UTDOA
      6.2.4. Angle-based positioning
      6.2.5. Multi-RTT (Round Trip Time)
      6.2.6. Méthodes hybrides

7. Interfaces et flux de localization
   7.1. Interfaces radio
   7.2. Interfaces cœur de réseau
   7.3. Interfaces northbound (services / APIs)

Sécurité 4G/5G

Durée : 3 jours

Objectifs : Comprendre l'architecture, les mécanismes de sécurité, les procédures d'authentification, de chiffrement et de protection des réseaux mobiles 4G, IMS et 5G SA, afin d'identifier, prévenir et mitiger les menaces et fraudes dans un environnement opérateur.

Public : Ingénieurs télécom et réseau, Architectes réseau, Consultants réseaux et télécom, Consultant sécurité, Chef de projet sécurité mobile

Pré-requis : Connaissance minimum des réseaux mobiles notamment réseau 4G

A l'issue de ce séminaire, les participants seront en mesure de :
- décrire les architectures des réseaux et des services mobiles, notamment 4G paquet, 5G NSA paquet, 5G SA paquet et IMS ;
- comprendre les mécanismes d'authentification, de chiffrement et de protection de l'intégrité dans les réseaux mobiles, ainsi que leur application aux services de téléphonie et de données mobiles ;
- comprendre les mécanismes de sécurité du plan de contrôle, basés sur DIAMETER (4G et 5G NSA) et HTTP/2 (5G SA) ;
- comprendre les principes de sécurité du plan usager ;
- identifier les principaux scénarios d'attaques et de fraudes dans les réseaux mobiles et les moyens de prévention et de mitigation associés.

1. Architecture 4G et sécurité
   - 1.1. Architecture du réseau d'accès E-UTRAN et du réseau cœur EPC
   - 1.2. SeGW pour sécuriser les échanges entre réseau accès E-UTRAN et cœur de réseau EPC et entre entités du réseau accès
     - 1.2.1. Authentification des eNodeB
     - 1.2.2. Chiffrement des communications entre E-UTRAN et EPC (Interfaces OAM, S1, X2) via tunnel(s) IPSec
     - 1.2.3. Isolement de l'EPC contre les intrusions venant du réseau d'accès.
   - 1.3. Authentification LTE
     - 1.3.1. Authentication and Key Agreement (AKA)
     - 1.3.2. Clés K_{ASME}, K_{NASenc}, K_{NASint}, K_{eNB}, K_{Upenc}, K_{RRCenc}, K_{RRCint}
     - 1.3.3. Vecteur d'authentification LTE : RAND, XRES, AUTN, K_{ASME}
     - 1.3.4. Algorithmes de chiffrement et de protection de l'intégrité
     - 1.3.5. Chiffrement et protection de l'intégrité du trafic RRC
     - 1.3.6. Chiffrement et protection de l'intégrité du trafic NAS
     - 1.3.7. Chiffrement du trafic du plan usager
   - 1.4. Sécurité de la signalisation DIAMETER
     - 1.4.1. Masquage de la topologie
     - 1.4.2. Contrôle d'admission (Filtrage des messages DIAMETER) pour uniquement traiter les messages autorisés
     - 1.4.3. Catégories de filtrage DIAMETER

1.4.3.1. Catégorie 0 : Filtrage DIAMETER à un bas niveau, e.g., Host-IP-Address, Origin-Host, Origin-Realm, Destination-Realm pour l'anti-spoofing
1.4.3.2. Catégorie 1 : Filtrage DIAMETER sur la base des champs d'en-tête de commande DIAMETER, i.e., Application-ID et Command-Code pour détecter le mauvais usage des applications
1.4.3.3. Catégorie 2 : Filtrage sur la base des AVPs, e.g., User-Name afin de n'autoriser que les messages nécessaires sur chaque interface DIAMETER
1.4.4. Attaques possibles DIAMETER
1.4.5. Fraudes possibles DIAMETER
1.5. Sécurité du plan de transport GTP-U
1.6. Sécurité WiFi connecté à l'EPC pour le service VoWiFi
1.6.1. Architecture WiFi connectée à l'EPC
1.6.1.1. ePDG
1.6.1.2. 3GPP AAA Server
1.6.1.3. Authentification d'accès (par le hotspot WiFi) et authentification réseau (par le 3GPP AAA Server) de l'UE
1.6.1.4. Tunnel IPSec entre l'UE et l'ePDG
1.7. Interception légale 4G

2. Sécurité IMS pour VoLTE, VoWiFi et Vo5G (EPS Fallback et VoNR)
2.1. Architecture de réseau et de service IMS
2.2. Protocole SIP et problèmes de sécurité liés au protocole
2.2.1. SIP INVITE flooding, REGISTER hijacking, SIP header spoofing, SIP replay
2.3. Enregistrement au réseau IMS (procédure d'enregistrement SIP)
2.4. Procédure d'authentification pour un client IMS pour les scénarios suivants:
2.4.1. Client IMS ayant une carte USIM et le module ISIM (IMS SIM Module)
2.4.2. Client IMS ayant une carte USIM sans module ISM
2.4.3. Authentification AKA 3G, AKA IMS pour l'authentification au monde IMS
2.5. Tunnel IPSec entre l'UE et le P-CSCF (premier point d'entrée IMS) pour sécuriser le trafic de signalisation SIP ou transport TLS
2.5.1. Chiffrement et protection de l'intégrité du trafic SIP sans roaming
2.5.2. Protection de l'intégrité en cas de roaming
2.6. Résilience, redondance et restauration des CSCF
2.6.1. Restauration P- CSCF
2.6.2. Restauration S-CSCF
2.6.3. Stateless I-CSCF
2.7. Interception légale IMS
2.7.1. BBIFF et LMISF dans le réseau visité pour l'interception légale dans le pays visité
2.7.2. IMS dans le réseau nominal pour l'interception dans le pays nominal
2.8. STIR/SHAKEN pour la lutte contre l'usurpation d'identité d'appelant (caller ID spoofing)
2.8.1. STIR
2.8.2. SHAKEN

3. Architecture 5G SA et sécurité

3.1. Architecture du réseau d'accès 5G-RAN et du réseau cœur 5GC
3.2. Principes de sécurité 5G (3GPP TS 33.501)
3.3. SeGW pour sécuriser les échanges entre réseau accès 5G-RAN et 5GC
3.4. Authentification primaire 5G SA
  3.4.1. Architecture d'authentification
    3.4.1.1. SEAF, AUSF et UDM/ARPF
  3.4.2. SUCI versus SUPI
  3.4.3. 5G-AKA
  3.4.4. Vecteur 5G HE AV (RAND, AUTN, XRES*, KAUSF) et vecteur 5G SE AV (RAND, AUTN, HXRES*)
  3.4.5. Dérivation de clés de chiffrement et de protection d'intégrité : K_{AUSF}, K_{SEAF}, K_{AMF}, K_{NASenc}, K_{NASint}, K_{gNB}, K_{UPenc}, K_{UPint}, K_{RRCenc}, K_{RRCint}
3.5. Procédure d'authentification 5G-AKA avec UE, AMF/SEAF, AUSF et UDM/ARPF
3.6. Chiffrement et protection de l'intégrite 5G SA
  3.6.1. Algorithmes de chiffrement et de protection de l'intégrité
  3.6.2. Chiffrement et protection de l'intégrité du trafic RRC
  3.6.3. Chiffrement et protection de l'intégrité du trafic NAS
  3.6.4. Chiffrement et protection de l'intégrité du trafic du plan usager
3.7. Authentification secondaire 5G SA
  3.7.1. Authentification spécifique au slice de réseau
  3.7.2. Définition du slice de réseau
  3.7.3. Identités
  3.7.4. Architecture d'authentification
    3.7.4.1. AMF, NSS-AAF, AAA Server, AAA Proxy, 3rd Party AAA Server
  3.7.5. EAP
  3.7.6. Procédure d'authentification/ré-authentification EAP pour l'accès au slice avec UE, AMF, NSS-AAF et AAA Server
3.8. Echanges HTTP/2 entre NF du réseau cœur 5G
  3.8.1. Chiffrement et protection de l'intégrité du trafic HTTP/2 entre NFs du plan contrôle
  3.8.2. Jeton d'accès par la NRF pour les interactions entre les NFs du plan contrôle du réseau cœur 5G
3.9. Proxy HTTP/2 (SCP, Service Communication Proxy) pour le routage HTTP/2 entre NFs.
3.10. Proxy HTTP/2 (SEPP, Security Edge Protection Proxy) pour le routage HTTP/2 entre NFs de différents réseaux
  3.10.1. Masquage de la topologie
  3.10.2. Firewalling
  3.10.3. TLS entre SEPPs directement interconnectés
  3.10.4. TLS ou PRINS (PRotocol for N32 INterconnect Security) entre SEPPs interconnectés via des carriers internationaux et leurs IPX Proxy
3.11. Interception légale 5G SA

4. Conclusion

Evolution des Réseaux et Services Mobiles de la 2G à la 5G

Durée : 5 jours

Objectifs : Le but de cette formation est de comprendre le réseau et les services mobiles de bout en bout de la 2G à la 5G.

· Connaître l'architecture du réseau mobile (accès et cœur) et les infrastructures de services (Voix, Data) qui sont utilisées

· Comprendre le fonctionnement de l'infrastructure "Réseau": le réseau d'accès 2G à 5G, le RAN Backhaul, le transport backhaul, le réseau cœur 2G à 5G.

· Comprendre les infrastructures de Services Voix et Data utilisées dans le mobile avec une vision de bout en bout.

Pre-requis : Connaissances de base sur les réseaux de télécommunications

Public : Collaborateur amené à appréhender l'architecture et le fonctionnement du réseau mobile.

Depuis les années 1990, les réseaux et services mobiles ont connu une évolution rapide, passant de la 2G, centrée sur la voix et les SMS, à la 3G qui a ouvert la voie à l'Internet mobile. La 4G a ensuite marqué un tournant avec le haut débit mobile et l'essor des usages multimédias. Aujourd'hui, la 5G poursuit cette dynamique en offrant des débits ultra-rapides, une faible latence et une connectivité massive, ouvrant la voie à de nouveaux services comme l'Internet des objets, la réalité augmentée et les applications critiques en temps réel.

Le but de cette formation est de comprendre le réseau et les services mobiles de bout en bout de la 2G à la 5G :

• Connaître l'architecture du réseau mobile (accès et cœur) et les infrastructures de services (Voix, Data) qui sont utilisées

• Comprendre le fonctionnement de l'infrastructure "Réseau": le réseau d'accès 2G à 5G, le RAN Backhaul, le transport backhaul, le réseau cœur 2G à 5G.

• Comprendre les infrastructures de Services Voix et Data utilisées dans le mobile avec une vision de bout en bout.

• Les mécanismes de sécurité mis en œuvre dans les réseaux 2G à 5G : authentification, chiffrement, protection de l'intégrité, firewalling dans les réseaux de signalisation SS7/SIGTRAN/DIAMETER/HTTP2

• Comprendre les différents call flows de bout en bout

1. Réseau mobile

1.1. 2G
1.2. 3G/3G+
1.3. 4G/4G+
1.4. 5G NSA
1.5. 5G SA
1.6. Non Terrestrial Network et le réseau mobile
1.7. Que se trame-t-il avec la 6G ?

2. Composants des réseaux mobiles
   2.1. Réseau d'accès
   2.2. RAN Backhaul
   2.3. Transport Backhaul
   2.4. Réseau cœur
   2.5. Plate-forme de service
   2.6. Sites radio, agrégation, cœur pour le déploiement du réseau mobile
   2.7. Cloud Telco pour le déploiement des futurs réseau mobiles
   2.8. Virtualisation/Conteunirisation du réseau d'accès, du réseau cœur et des plate-formes de services

3. Réseau d'accès
   3.1. Réseau d'accès 2G : GERAN
   3.2. Réseau d'accès 3G : UTRAN
   3.3. Réseau d'accès 4G : E-UTRAN
   3.4. Réseau d'accès 5G : NG-RAN
   3.5. 5G NSA
   3.6. 5G SA
   3.7. RAN sharing avec MORAN et MOCN

4. RAN Backhaul (collecte)
   4.1. De la collecte mobile à la collecte unifiée fixe/mobile
      4.1.1. PE d'agrégation
      4.1.2. PE unifié

5. Transport backhaul (agrégation et transport national)
   5.1. Structure du backbone IP
   5.2. Du transport mobile au transport unifié fixe/mobile

6. Réseau cœur
   6.1. Cœur circuit 2G/3G = R4
   6.2. Cœur paquet 2G/3G = GPRS
   6.3. Cœur paquet 4G = EPC pour la 4G et la 5G NSA
   6.4. Cœur paquet 5G = 5GC pour la 5G SA

7. Plate-formes de service
   7.1. SMSC
   7.2. MMSC
   7.3. IMS pour VoLTE/VoWiFI/EPS Fallback et VoNR

7.4. GMLC pour les services de localisation
7.5. CBS pour FR-Alert
7.6. RCS Personne à Personne et RCS Application à Personne
7.7. MCX pour les communications critiques avec MCPTT, MCVideo et MCData

8. Service voix
   8.1. Voice circuit 2G/3G
   8.2. Circuit Switched Fallback
   8.3. Voice sur IP sur LTE : VoLTE
   8.4. Voix sur IP sur WiFi : VoWiFi
   8.5. Voix sur 5G (Vo5G) : VoNR et EPS Fallback

9. Service de données
   9.1. Contexte PDP 2G/3G
   9.2. Default et Dedicated bearer 4G
   9.3. Session PDU 5G SA
      9.3.1. Session PDU IP
      9.3.2. Session PDU Ethernet
      9.3.3. Session PDU Unstructured (Non-IP)

10. Procédures mobiles de bout en bout
   10.1. Attachement au réseau circuit 2G/3G
   10.2. Etablissement d'appel circuit 2G/3G
   10.3. Envoi/réception de SMS dans le domaine circuit 2G/3G
   10.4. Attachement au réseau paquet 2G/3G (GPRS)
   10.5. Etablissement de contexte PDP dans le domaine paquet 2G/3G et notation d'APN
   10.6. Attachement au réseau paquet 4G EPC
   10.7. Etablissement de default bearer dans le domaine paquet EPC
   10.8. Enregistrement au réseau paquet 5GC
   10.9. Etablissement de session PDU dans le domaine paquet 5GC
   10.10. Ré-établissement du RAB (Radio Access Bearer) dans les différents réseaux mobiles

11. Policy and Charging Control (PCC) dans le domaine paquet mobile
   11.1. Principes du policy control appliqué à la connexion data mobile
      11.1.1. Identification des flux
      11.1.2. Blocage/autorisation des flux
      11.1.3. Dégradation de la QoS des flux
   11.2. Principes du charging control
      11.2.1. Taxation des flux en online charging
      11.2.2. Taxation des flux en offline charging
   11.3. Scénarios PCC
      11.3.1. Faire use, forfait bloqué, prépayé
      11.3.2. Pass data roaming international, anti bill shock, turbo button, etc.

12. Mobilités

12.1. Mobilité dans l'état IDLE et mobilité dans l'état CONNECTED
12.2. Mobilité 2G
12.3. Mobilité 3G
12.4. Mobilité 4G
12.5. Mobilité 5G NSA
12.6. Mobilité 5G SA
12.7. Mobilité 4G/3G
12.8. Mobilité 5G SA/4G

13. Roaming mobile
    13.1. Accords de roaming bilatéral et multilatéral
    13.2. Roaming Hub versus Roaming sponsor
    13.3. Structure des réseaux mobiles en situation de roaming (roamer-in et roamer-out)
    13.4. Types d'accord de roaming
        13.4.1. Roaming GSM
        13.4.2. Roaming GPRS
        13.4.3. Roaming 4G
        13.4.4. Roaming LTE
        13.4.5. Roaming VoLTE
        13.4.6. Roaming 5G NSA
        13.4.7. Roaming 5G SA
        13.4.8. Roaming Vo5G

14. Sécurité mobile
    14.1. Authentification 2G : A3/A5
    14.2. Authentification 3G à 5G SA : AKA
    14.3. Chiffrement de la signalisation et du plan usager en 2G/3G/4G/5G NSA/5G SA
    14.4. Protection de l'intégrité de la signalisation en 3G/4G/5G NSA/5G SA et du plan usager en 5G SA
    14.5. Sécurité IMS
        14.5.1. Authentification IMS
        14.5.2. Chiffrement et protection de l'intégrité du trafic SIP dans l'IMS.
        14.5.3. Résilience, redondance et restauration des CSCF
            14.5.3.1. Restauration P- CSCF
            14.5.3.2. Restauration S-CSCF
            14.5.3.3. Stateless I-CSCF
    14.6. Sécurité de la signalisation MAP 2G/3G
        14.6.1. Contrôle d'admission (Filtrage des messages MAP) pour uniquement traiter les messages autorisés
        14.6.2. Catégories de filtrage MAP
    14.7. Sécurité de la signalisation DIAMETER 4G/5G NSA
        14.7.1. Masquage de la topologie
        14.7.2. Contrôle d'admission (Filtrage des messages DIAMETER) pour uniquement traiter les messages autorisés
        14.7.3. Catégories de filtrage DIAMETER

14.8. Chiffrement de la signalisation HTTP/2 via SCTP de proche en proche en 5G SA