Non-IP Data Delivery (NIDD) dans le Système 5G

EFORT
http://www.efort.fr

NIDD (Non IP Data Delivery) est une nouvelle technologie qui permet aux devices IoT d'échanger (émettre/recevoir) des données via une connexion de données mobile sans leur attribuer d'adresse IP. NIDD fait référence à un mécanisme de communication utilisé dans les réseaux cellulaires adaptés à l'IoT 4G et 5G pour transmettre des données non IP (Internet Protocol). Dans les réseaux cellulaires traditionnels, IP est le principal protocole utilisé pour la communication de données. Il existe cependant des cas où des petits volumes de données doivent être transmis de manière efficace et sécurisée, par exemple pour des applications ou des services spécifiques, notamment pour des devices disposant de peu de ressources (CPU, RAM, débit de connectivité, etc) tels que les capteurs et compteurs IoT. Par exemple, un compteur d'énergie émet quelques dizaines d'octets périodiquement, typiquement à chaque heure, une poubelle connectée envoie quelques octets toutes les 15 mns, etc. Le fait de ne pas disposer d'adresse IP rend la communication plus sécurisée car le device n'est pas visible de l'Internet. Par ailleurs le non-IP permet de ne pas rajouter aux données utiles les en-têtes TCP/IP ou UDP/IP consommateurs en ressources.

NIDD fournit une méthode alternative pour transmettre des données non IP sur les réseaux cellulaires 4G et 5G. Il existe des protocoles applicatifs normalisés qui fonctionnent sans la pile protocolaire TCP/IP ou UDP/IP et donc adaptés aux échanges non-IP, tels que CoAP (Constrained Application Protocol) défini dans le RFC 7252 et MQTT-SN (Message Queue Telemetry Transport for Sensor Networks) défini par OASIS OPEN.

NIDD complémente donc les communications IP dans les réseaux mobiles 4G et 5G pour disposer d'un mécanisme spécialisé pour gérer des données non IP, offrant flexibilité, sécurité et efficacité pour certains types d'applications ou de services notamment IoT.

Le but de ce tutoriel est de présenter NIDD dans le contexte du réseau système 5G. NIDD est aussi applicable au réseau 4G.

1. Pourquoi NIDD ?

NIDD (Non IP Data Delivery) permet aux devices IoT de transmettre des données sans disposer d 'adresse IP.

Cela présente deux avantages :

- Une meilleure sécurité en n'utilisant pas d'adresse IP pour la transmission des données. Ainsi le device n'est pas accessible via Internet.
- Une meilleure efficacité en n'ajoutant pas les en-têtes TCP/IP ou UDP/IP au données utiles. Un grand nombre de devices IoT comme les capteurs et les compteurs disposent de peu de ressources. On dit qu'ils disposent de moins de tout : moins de mémoire, moins de puissance de traitement, moins de bande passante, etc., et bien sûr, moins d'énergie disponible.

Un message NIDD est par définition de petite taille mais peut dans certains cas être de grande taille. Tout message NIDD est échangé via le protocole NAS (Non Access Stratum) entre l'UE et le réseau cœur data mobile 4G et 5G. Ces messages NAS s'appellent DoNAS (Data over NAS). en 4G, les échanges DoNAS ont lieu entre l'UE et le MME. En 5G SA, les échanges DoNAS ont lieu entre l'UE et la SMF via l'AMF. La taille maximum d'un message

NAS est de 1500 octets. C'est alors à la couche application présente dans l'UE de fragmenter/réassembler le message d'application NIDD si ce dernier a une taille supérieure à 1500 octets.

NIDD est un service de transfert de données bidirectionnel qui permet l'échange de données non-IP entre un device IoT et un serveur d'application appelé AF (Application Function).

Si le device n'est pas joignable et qu'un message de données entrant est reçu, le stockage et le transfert s'appliquent.

Le support NIDD fait partie des optimisations des réseaux 4G et 5G pour s'adapter aux contraintes des devices IoT. En 4G, NB-IoT (Narrowband IoT) propose le service NIDD. En 5G SA, mMTC (Massive Machine Type Communication) le propose. Dans le contexte 5G SA, l'UE doit établir une session PDU de type «Unstructured» pour échanger des données non-IP.

Au niveau applicatif, le device doit émettre des messages ne nécessitant pas de pile protocolaire TCP/IP ou UDP/IP. Parmi les protocoles ne nécessitant pas un transport IP figurent différents protocoles connus du monde IoT dont :

- CoAP (Constrainted Application Protocol) spécifié dans le RFC 7252. CoAP est la version lightweight du protocole HTTP, ce dernier nécessitant un transport TCP/IP.
- MQTT - SN (Message Queue Telemetry Transport for Sensor Networks) spécifié par OASIS OPEN. MQTT-SN est la version lightweight du protocole MQTT, ce dernier nécessitant un transport TCP/IP.

L'échange des données NIDD entre l'UE et l'AF est réalisé via deux méthodes possibles :

- Livraison en utilisant la NEF
- Livraison en utilisant un tunnel N6 point à point (PtP) entre UPF et AF. IL s'agit généralement d'un tunnel UDP/IP.

2. Livraison NIDD via NEF sans roaming

La figure 1 présente l'architecture pour la livraison NIDD via la NEF sans situation de roaming. NIDD via NEF nécessite une session PDU sur le plan de contrôle. La session PDU est établie entre l'UE et la NEF via l'AMF et la SMF. Le trafic NIDD est échangé en utilisant DoNAS (Data over NAS) entre l'UE et la SMF via l'AMF (données échangées sur le plan contrôle), puis via l'interface N11 entre AMF et SMF, puis via l'interface N29 entre SMF et NEF et enfin via l'interface N33 entre NEF et AF (voir TS 23.502 clause 4.25). Les interfaces N11, N29 et N33 sont basées sur le protocole HTTP/2.

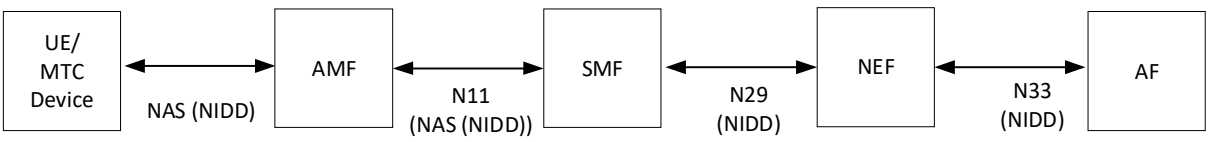

Figure 1 : Livraison NIDD via NEF sans roaming

Le call flow pour l'établissement de la session PDU de type «Unstructured» pour l'échange des données NIDD via la NEF est décrit à la figure 2.

La procédure d'établissement d'une session PDU de type «Unstructured» pour NIDD utilisant la NEF comprend les étapes suivantes :

1. L'UE envoie un message NAS PDU Session Establishment Request pour demander l'établissement de session PDU. Le message NAS contient entre autres le nom du DNN, le nom du S-NSSAI, et le type de session PDU, ici «Unstructured».

2. et 3. L'AMF détermine si la session PDU utilise Data over NAS (DoNAS) pour transférer les données. Si la session PDU utilise DoNAS, l'AMF sélectionne une SMF qui prend en charge les données DoNAS pour le DNN et S-NSSAI demandés. L'AMF conserve l'association entre PDU Session ID et SMF ID que l'AMF a sélectionné pour prendre en charge l'établissement de la session PDU «Unstructured»..

L'AMF invoque la requête Nsmf_PDUSession_CreateSMContext Request (Commande HTTP/2 POST) comprenant le DNN, le S-NSSAI et le PDU Session ID. Cette requête contient le message NAS PDU Session Establishment Request émis par l'UE que la SMF doit traiter. L'AMF indique également à la SMF si la session PDU utilise DoNAS pour transférer les données. La SMF répond via Nsmf_PDUSession_CreateSMContext Response.

4. et 5. La SMF s'enregistre auprès de l'UDM et obtient les données de souscription SM (Session Management) pour le SUPI, DNN et S-NSSAI correspondants. Si les données de souscription SM comprennent une indication «Invoke NEF Selection» pour le DNN et le S-NSSAI indiqués par l'UE, la SMF doit impliquer une NEF. La SMF sélectionne la NEF sur la base des données de souscription SM pour le DNN et le S-NSSAI indiqués par l'UE. La SMF configure la NEF pour le transfert de données NIDD.

6. et 7. La SMF envoie un message Namf_Communication_N1N2MessageTransfer Request correspondant à une acceptation d'établissement de session PDU indiquant que les données DoNAS sont activées pour cette session PDU.. Ce message contient le message NAS PDU Session Establishment Accept à l'AMF qui le relaie à l'UE.

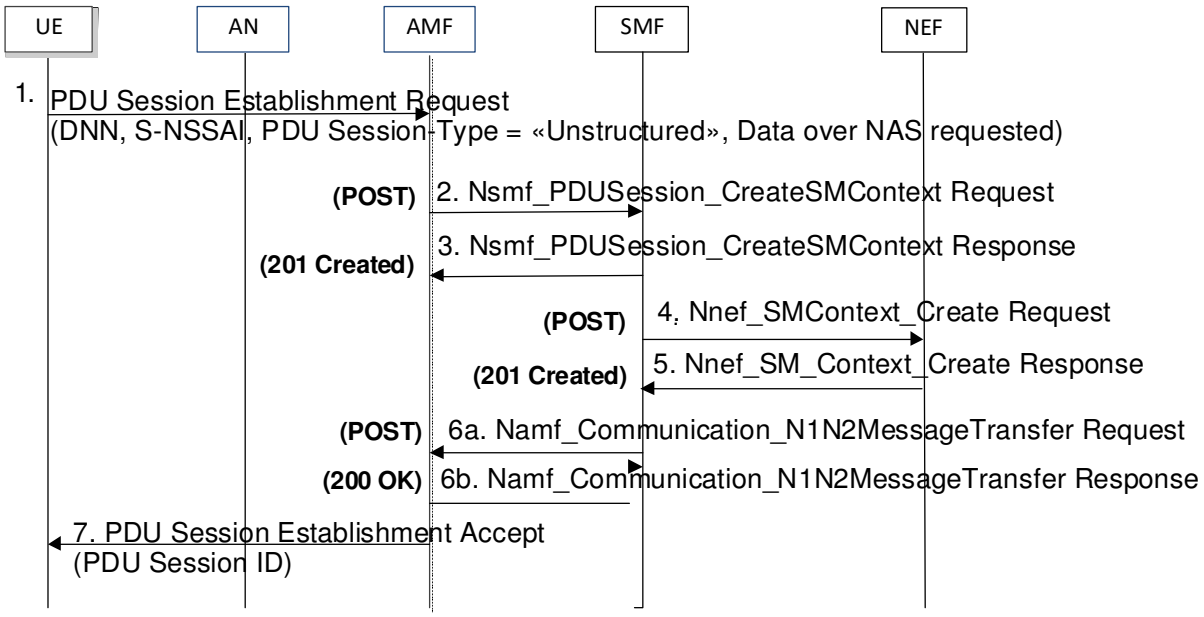

Figure 2 : Etablissement de Session PDU de type « Unstructured » pour l'échange de données NIDD via la NEF

Le call flow pour l'envoi des données NIDD via la NEF est décrit à la figure 3.

L'UE utilise DoNAS et envoie un message NAS SM protégé contenant le message NIDD et le PDU Session ID correspondant au numéro de session PDU dans laquelle est envoyée le

message NIDD, un UE pouvant disposer de plusieurs sessions PDU actives simultanément. «Protégé» signifie que le message a été chiffré et son intégrité protégée.

2. L'AMF vérifie l'intégrité du message DoNAS provenant de l'UE et déchiffre les données contenues.

3 et 4. L'AMF transmet les données à la SMF qui gère la session PDU identifiée par PDU Session ID, contenu dans le message de transport NAS.

5., 6., 7. et 8. La fonction SMF transmet les données à la fonction NEF. La NEF les transmet à l'AF.

Si l'on considère que l'UE a utilisé le protocole CoAP pour générer un message applicatif non-IP, ce même message CoAP est relayé par la NEF à l'AF sous forme d'un body dans une requête HTTP/2 POST (message 6 du call flow).

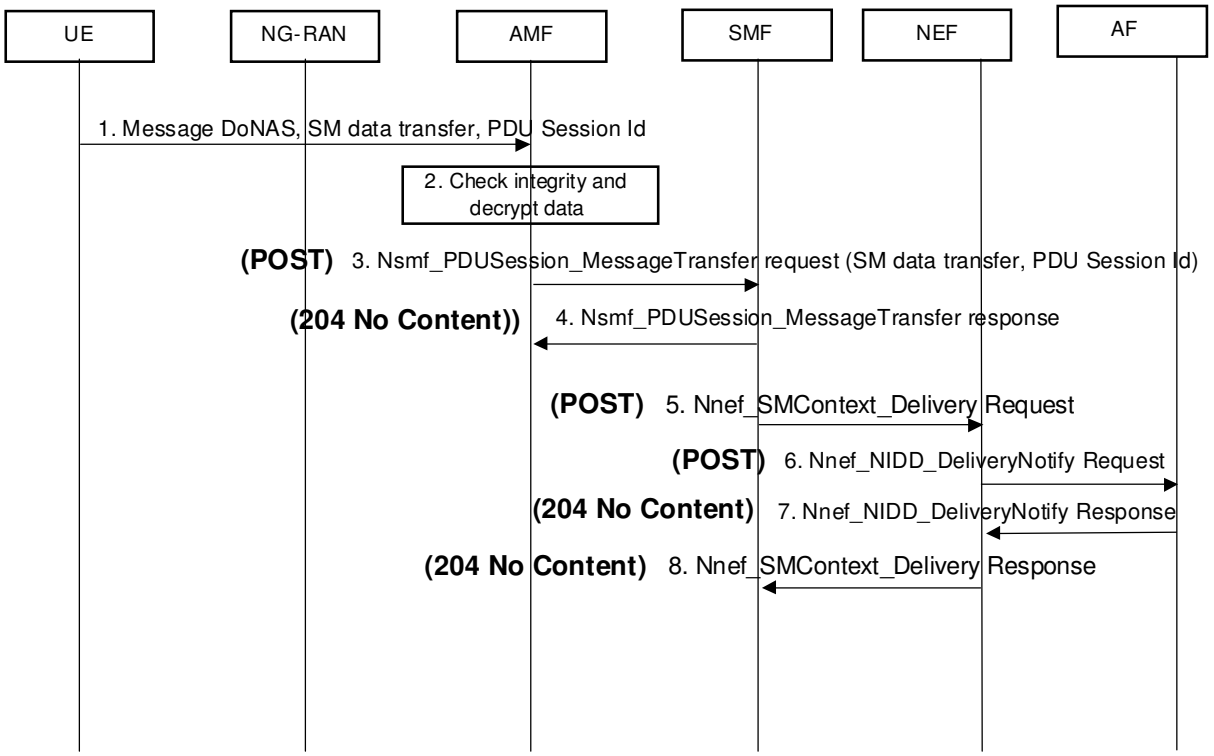

Figure 3 : Envoi de données NIDD par l'UE à l'AF via la NEF

3. Livraison NIDD via UPF et tunnel PtP N6 sans roaming

La figure 4 montre l'architecture pour la livraison NIDD via l'UPF et un tunnel PtP N6 jusqu'à l'AF sans situation de roaming. Le trafic NIDD est échangé en utilisant DoNAS entre l'UE et l'AMF, que l'AMF relaie via l'interface N11 basée sur le protocole HTTP/2 à la SMF. La SMF relaie le trafic NIDD via l'interface N4 basée sur le protocole PFCP à UPF qui le relaie sur le tunnel PtP N6 entre UPF et AF. Le tunnel est généralement un tunnel UDP/IP.

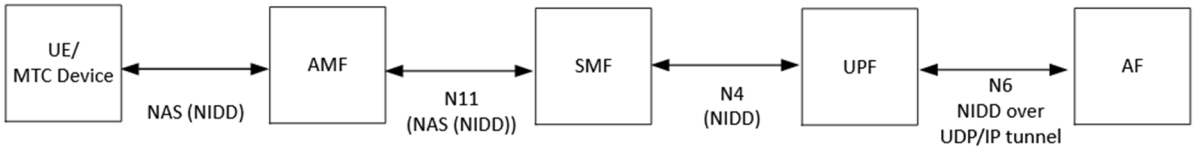

Figure 4 : Livraison NIDD via UPF et tunel Ptp N6 sans roaming

4. Livraison NIDD via NEF avec roaming

En situation de roaming, la session PDU pour la livraison NIDD via la NEF est établie entre l'UE et la NEF via l'AMF visitée (V-AMF), la SMF visitée (V-SMF) et la SMF nominale (H-SMF). Le trafic NIDD est échangé en utilisant DoNAS entre l'UE et l'AMF, puis via l'interface N11 entre AMF et V-SMF, via l'interface N16 entre V-SMF et H-SMF et via l'interface N29 entre SMF et NEF et enfin via l'interface N33 entre NEF et AF. Les interfaces N11, N16, N29 et N33 sont basées sur le protocole HTTP/2. La Figure 5 montre l'architecture pour la livraison NIDD en utilisant la NEF en situation de roaming.

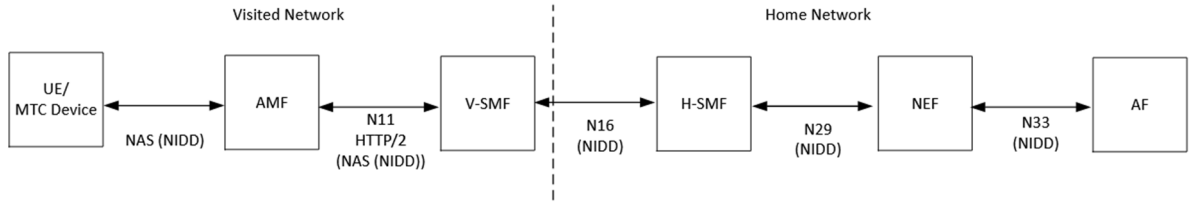

Figure 5 : Livraison NIDD via NEF avec roaming

5. Livraison NIDD via UPF et tunnel PtP N6 avec roaming

En situation de roaming, le trafic NIDD est échangé en utilisant DoNAS entre l' UE et l'AMF, que l'AMF relaie à la V-SMF via l'interface S11. La V-SMF relaie le trafic NIDD via l'interface N4 à la V-UPF. LA V-UPF achemine le trafic NIDD via l'interface N9 à la H-UPF qui enfin délivre ce trafic NIDD via le tunnel PtP N6 à l'AF (Figure 6). L'interface N11 utilise le protocole HTTP/2, N4 utilise le protocole PFCP, N9 fait usage du protocole GTP-U.

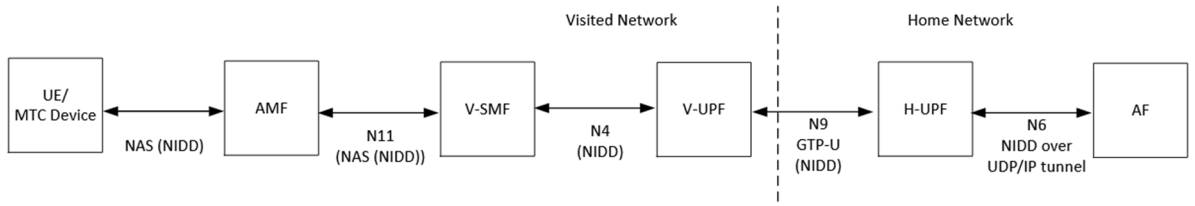

Figure 6 : Livraison NIDD via UPF et tunel Ptp N6 avec roaming

La formation EFORT « mMTC 5G versus LTE-M/NB-IoT 4G» permet de comprendre les évolutions des réseaux 4G et 5G SA pour prendre en charge les spécificités des devices IoT, entre autres NIDD.

https://www.efort.fr/formations-iot-1/-mmtc-5g-versus-lte-m%2Fnb-iot-4g