Réseau de Signalisation 5GC

EFORT
http://www.efort.com

1. Introduction

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 cœur mobile 5G et SEPP (Security Edge Protection Proxy) pour le routage entre un réseau mobile 5G et les réseaux 5G externes dans le contexte du roaming.
Le but de ce tutoriel est de présenter le réseau de signalisation 5GC.

2. Service NF

Dans le système 5G, il est prévu que les fonctions de réseau (NF, Network Function) 5G du plan contrôle présentent leur fonctionnalité via une interface basée sur le service.
Les NFs 5G sont décrites dans un autre tutoriel EFORT :
http://efort.com/r_tutoriels/RESEAU_COEUR_5G_EFORT.pdf
Les NFs (Network Functions) peuvent offrir différentes capacités de service et par conséquent, différents services NF à des consommateurs distincts via leur interface de service. Chacun des services NF offert par une fonction de réseau doit être autonome, et indépendante des autres services NF offerts par la même fonction réseau par exemple pour la scalabilité.
Chaque service NF doit être accessible par le moyen d'une interface ou API. Une interface consiste en une ou plusieurs opérations.
Il existe deux opérations élémentaires afin que les NF fournissent leurs services via une interface basée sur le service:

- "Request-response": Une NF_A du plan contrôle (NF Service Consumer) demande à une NF_B du plan de contrôle (NF Service Producer) de fournir un certain service NF, qui peut consister en une action et / ou une demande d 'information. La réponse NF_B fournit les résultats du service NF en fonction des informations fournies par NF_A dans sa demande. Afin de répondre à la demande, NF_B peut à son tour consommer le service NF d'autres NFs. Dans le mécanisme de demande-réponse, la communication est un à un entre deux NF (consommateur et producteur) et une réponse ponctuelle du producteur à une demande du consommateur est attendue dans un certain délai.
- "Subscribe-Notify": Une NF_A du plan contrôle (NF Service Consumer) souscrit auprès service NF offert par une autre NF_B du plan contrôle (NF Service Producer). NF_B notifie les résultats de ce service NF aux NF (s) intéressés qui ont souscrit à ce service NF. La demande de souscription du consommateur peut inclure une demande de notification pour des mises à jour périodiques ou une notification déclenchée par certains événements (par exemple, les informations demandées sont modifiées, atteinte de certains seuils, etc.). Ce mécanisme prend également en compte le cas où les NF (NF_B) sont souscripteurs à certaines notifications implicitement, sans demande de souscription explicite.

Toutes les opérations sont basées sur le protocole HTTP/2. La requête peut être GET (interrogation), POST (création ou interrogation), PUT (création ou modification totale),

PATCH (modification partielle) ou DELETE (suppression). Les réponses sont les réponses HTTP. La souscription et la notification sont des requêtes POST.

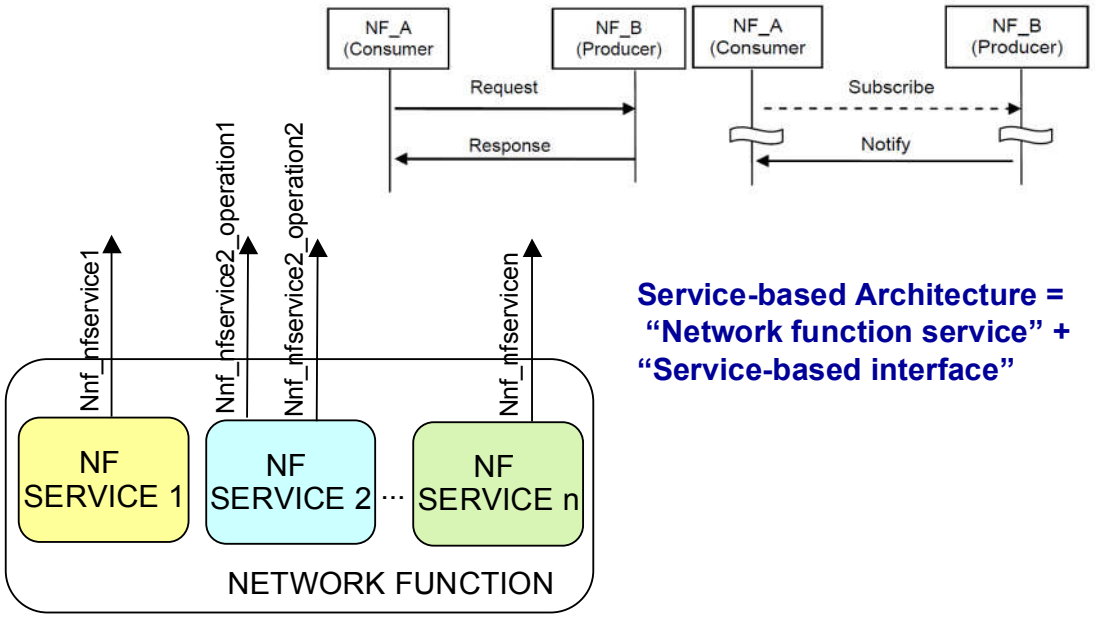


Figure 1: Service NF

3. Communication directe versus communication indirecte

Il existe quatre options de communication qui peuvent toutes coexister au sein d'un même réseau 5GC.
Un service NF est un type de capacité de service exposé par une NF (Producteur de service NF) à une autre NF (Consommateur de service NF) autorisé via une interface de service.
Une fonction de réseau (NF) peut exposer un ou plusieurs services NF.
Les procédures système 5G peuvent être décrites par une séquence d'invocations de services NF. Les NFs consommateur et producteur peuvent communiquer directement entre, ou indirectement via un SCP. Les communications directes et indirectes sont illustrées à la Figure 2. Le fait que le consommateur de service NF utilise la communication directe ou indirecte à l'aide d'un SCP est basé sur la configuration du consommateur de service NF.
Dans la communication directe, le consommateur de service NF effectue la découverte du producteur de service NF cible par configuration locale ou via NRF. Ce consommateur communique directement avec le producteur cible de service NF.
Dans la communication indirecte, le consommateur de service NF communique avec le producteur de service NF cible via un proxy SCP. Le consommateur de service NF peut être configuré pour effectuer directement la découverte du producteur de service NF cible ou déléguer la découverte du producteur de service NF cible au SCP utilisé pour la communication indirecte. Dans ce dernier cas, le SCP utilise les critères de recherche fournis par le consommateur de service NF pour effectuer la découverte et / ou la sélection du producteur de service NF cible. L'adresse SCP peut être configurée localement dans le consommateur du service NF.

- Option A - Communication directe sans interaction NRF (NF Repository Function): Ni NRF ni SCP ne sont utilisés. Les consommateurs sont configurés avec les "profils NF" des producteurs et communiquent directement avec le producteur de leur choix.
- Option B - Communication directe avec interaction NRF: les consommateurs effectuent une découverte en interrogeant la fonction NRF. En fonction du résultat de la découverte, le consommateur effectue la sélection. Le consommateur envoie la demande au producteur sélectionné.

- Option C - Communication indirecte sans découverte déléguée : les consommateurs effectuent la découverte en interrogeant la fonction NRF. En fonction du résultat de la découverte, le consommateur sélectionne une instance NF d'un ensemble d'instances de Service NF. Le consommateur envoie la demande au SCP contenant l'adresse du producteur de service sélectionné pointant vers une instance de service NF ou un ensemble d'instances de service NF. Dans ce dernier cas, le SCP sélectionne une instance de service NF. Si possible, le SCP interagit avec la NRF pour obtenir des paramètres de sélection tels que l'emplacement, la capacité, la charge, etc. Le SCP achemine la demande à l'instance de producteur de service NF sélectionnée.
- Option D - Communication indirecte avec la découverte déléguée: les consommateurs ne font aucune découverte ou sélection. Le consommateur ajoute à la demande de service les paramètres de découverte et de sélection nécessaires pour trouver un producteur approprié présents dans un header dans la requête HTTP/2 appelé +3gpp-Sbi-Discovery. Le SCP utilise les paramètres de découverte et de sélection dans la requête reçue de la NF consommateur pour interroger la NRF, obtenir les profils des instances NF producteur candidates et acheminer la demande à une instance de producteur appropriée.

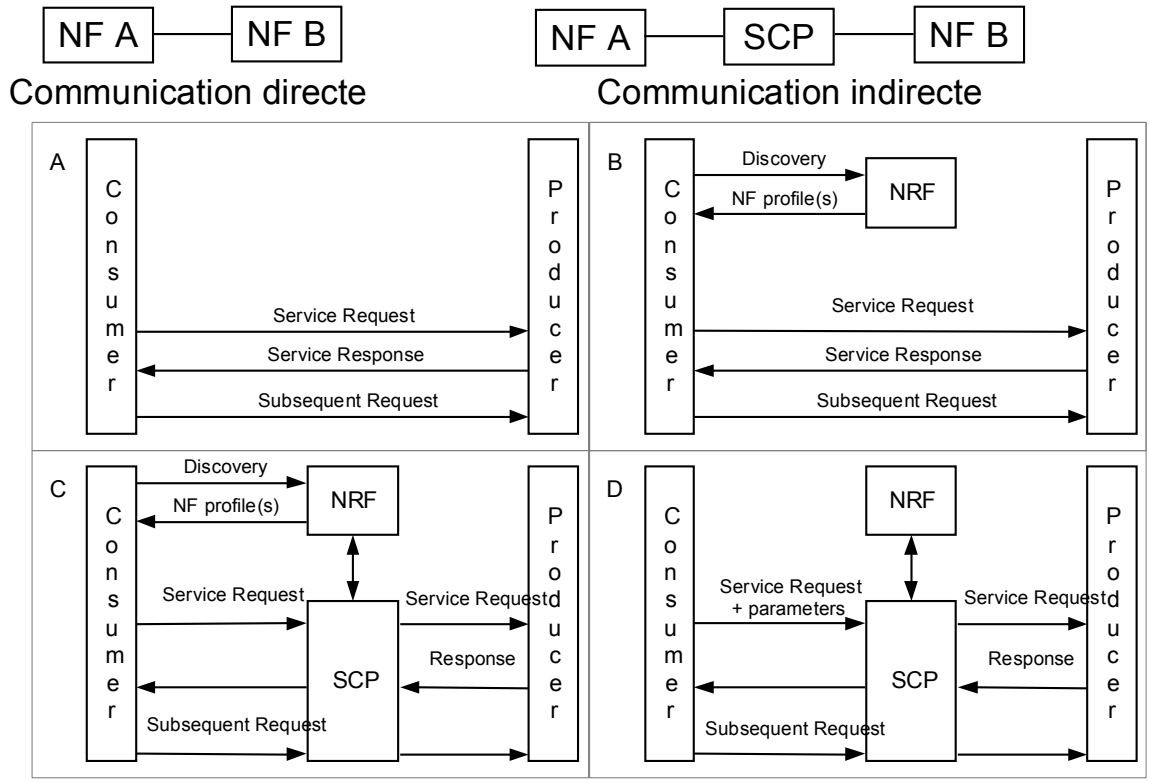


Figure 2 : Communication directe versus communication indirecte

4. NRF et ses services

Dans les réseaux de signalisation SS7, SIGTRAN et DIAMETER, les tables de routage de signalisation présentes dans les fonctions réseau (SP, Signaling Point) et dans les fonctions de routage de signalisation STP/IP STP/DRA sont préconfigurées.
Dans le contexte 5GC, les instances de fonction réseau sont créées, modifiées et supprimées dynamiquement. Le routage est donc dynamique. C'est la fonction NRF (NF Repository Function) qui est mise à jour par les instances de fonction réseau et qui dispose de l'image du réseau 5GC en terme de ses instances de fonction réseau, des services NF qu'elles proposent, des autorisations pour l'usage de ses services NF et et leur état à un instant donné. Avec la communication directe option B, et la communication indirecte option

C, l'instance NF consommateur découvre auprès de la NRF qui sont les instances NF producteur candidates pour router une opération de service. Avec la communication indirecte option D, l'instance NF consommateur délègue au SCP la découverte des instances NF producteur candidates afin de router l'opération de service.
La NRF via son interface de service Nnrf offre donc deux services NF à toutes les instances NF de tout type de NF: Nnrf_NFManagement et Nnrf_NFDiscovery.

Une instance NF doit pouvoir via le service NF Nnrf_NFManagement de la NRF :
• enregistrer auprès de la NRF le profil de l'instance NF et des instances de service NF pris en charge;
• mettre à jour auprès de la NRF le profil qu 'elle a enregistré sur la NRF,
• désenregistrer son profil auprès de la NRF si l'instance NF doit être supprimée dans le 5GC;
Le premier call flow indique un exemple de procédure d'enregistrement NF en utilisant le service NF Nnrf_NFManagement.
1. Une nouvelle instance de NF_A (e.g., instance de SMF) est déployée dans le plan de contrôle du réseau coeur 5G. L'instance de NF_A enregistre son profil incluant le profil de chacun de ses services NF auprès de la NRF.
2. La NRF stocke le profil de cette instance de NF_A.
3. La NRF confirme l'enregistrement.
Le second call flow décrit la procédure de découverte NF dans un réseau cœur 5G en utilisant le service NF NnrfDiscovery proposé par la NRF :
1. Suite à l'enregistrement de l 'usager au 5GC, une instance de NF_A (e.g., AMF, Core Access *and* Mobilit*y* Management. Function) doit accéder aux services fournis par la NF_B (e.g., AUSF, Authentification Server Function). L 'instance de NF_A émet une demande de découverte NF comprenant le type de NF cible, e.g., NF_B, le service NF cible, et les critères de recherche supplémentaires liés au service, e.g., type d'authentification dans le cas où NF_B est une NF d 'authentification et gère un type particulier de méthode d'authentification.
2. La NRF vérifie si NF_A est autorisée à accéder au service NF demandé de NF_B sur la base de la liste des autorisations NF.
3. Si la demande est autorisée, la NRF retourne les profils des instances de NF_B candidates. L'instance de NF_A sélectionne une instance de NF_B appropriée pour accéder à son service, e.g., sur la base de la charge de ces instances de NF_B (la charge fait partie du profil d 'une instance NF).
4. L 'instance de NF_A accède à l'instance de NF_B via un des services NF pris en charge par l 'instance de NF_B.
Ces calls flows ont considéré une communication directe. Dans le cas d'une communication indirecte, le SCP est présent sur tous les échanges entre NFs.

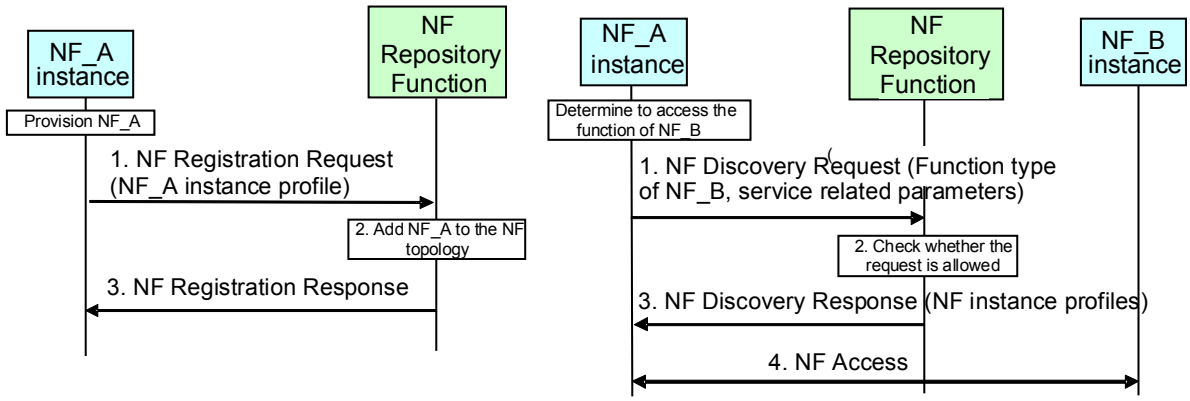


Figure 3 : NRF et ses services NF : Enregistrement NF et découverte NF

5. Communication indirecte avec découverte déléguée (Option D)

Pour illustrer la communication avec découverte déléguée (Option D), considérons le cas où l 'AMF reçoit une demande d 'enregistrement d 'un UE donné. L 'AMF doit interagir avec l 'UDM afin d 'obtenir les données de souscription liées à la gestion de la mobilité de l 'UE (Figure 4).

1. L 'AMF définit les critères de recherche à soumettre à la NRF et les encapsule dans la demande à délivrer à l 'UDM via un header http défini par 3GPP, appelé +3gpp-Sbi-Discovery. L 'AMF relaie au SCP le message à délivrer à l 'UDM.
2. Le SCP utilise les critères de recherche présents dans le header +3gpp-Sbi-Discovery pour interroger la NRF via son service NF Nnrf_NFDiscovery afin d 'obtenir les profils des instances UDM qui incluent les profils de leurs services NF qui correspondent aux critères de recherche.
3. La NRF retourne les profils des instances UDM candidates.
4. Le SCP analyse les profils, notamment les informations relatives à la charge de chaque instance d 'UDM pour choisir l 'instance d 'UDM la plus appropriée.
5. L 'instance d 'UDM retourne la réponse au SCP.
6. Le SCP relaie la réponse au demandeur, i.e., AMF1.

Dans cette configuration, l 'instance AMF dispose uniquement d'une connexion TCP avec chaque SCP avec lesquels elle est mise en relation, afin de communiquer avec un grand nombre d 'instances NF, à savoir, les autres instances d 'AMF, les instances SMF, les instances AUSF, les instances UDM, les instances SMSF, les instances NSSF, les instances NRF, les instances UDSF, etc.

Le SCP dans cette configuration peut effectuer un partage de charge sophistiqué à partir des informations des différents profils que lui a retourné la NRF.

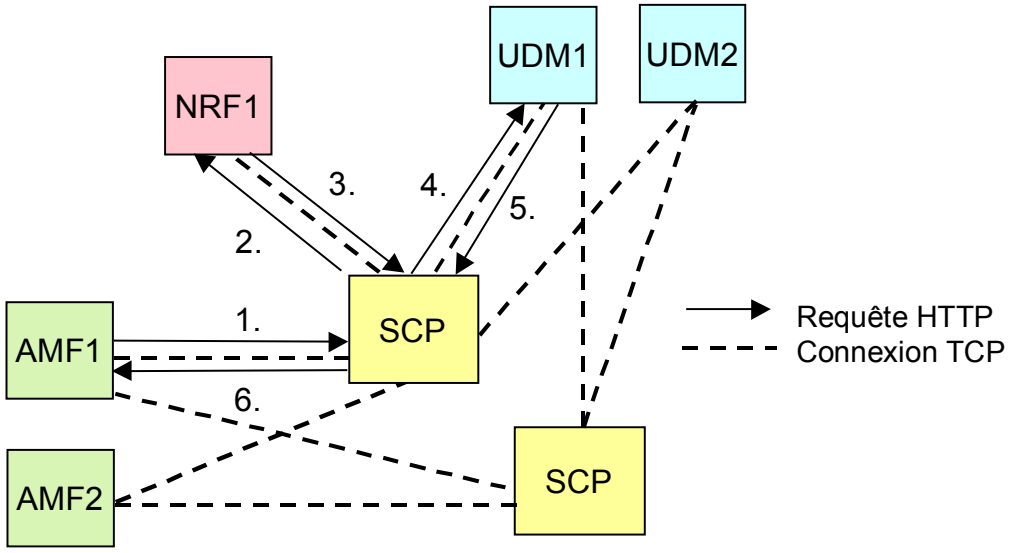


Figure 4 : Communication indirecte entre AMF et UDM avec découverte déléguée (Option D)

6. Fonctions de routage de signalisation

Plusieurs fonctions contribuent au routage des opérations HTTP/2 (Figure 5):

• La fonction SCP qui permet le routage indirect d 'opérations HTTP/2 entre consommateurs et producteurs de service NF dans un réseau cœur 5G donné.

• La fonction SEPP qui permet le routage d 'opérations HTTP/2 entre consommateurs et producteurs de service NF présents dans des réseaux 5GC distincts, lorsqu'il s'agit de situation de roaming.

• La fonction NEF qui sert de broker de service entre des serveurs d ’application d ’entreprise externes et les fonctions du réseau cœur 5GC (e.g., AMF, PCF, SMF, etc).
• La fonction BSF qui permet de mettre en œuvre le binding de service. C ’est cette fonction qui permet à une fonction AF d ’acheminer ses opérations de service HTTP/2 à la fonction PCF adéquate.
• La fonction NRF qui permet à partir de critères de sélection d ’identifier les instances de fonction de réseau producteur et retourner ces informations aux instances de fonction de réseau consommateur.
• La fonction NSSF qui permet d ’identifier une instance de fonction AMF appropriée pour prendre en charge un UE en fonction de l’ensemble des slides souscrits pour l’usager associé.

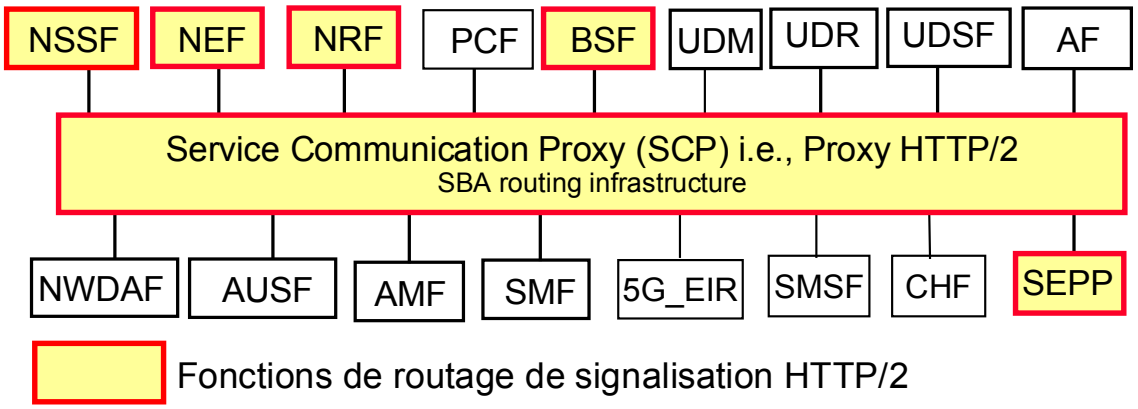
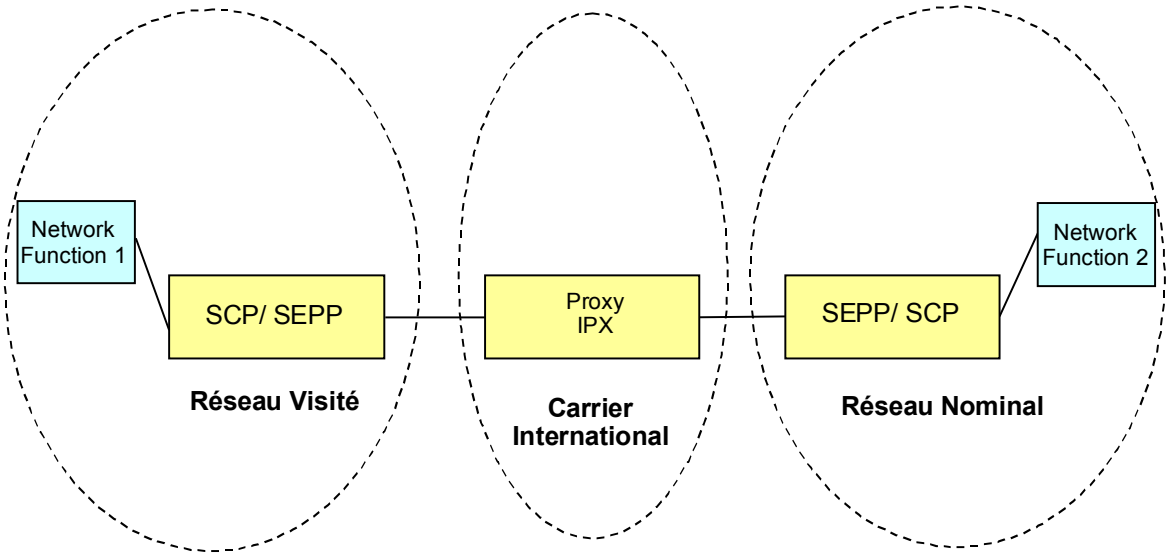


Figure 5 : Fonctions impliquées dans le routage de la signalisation HTTP/2

La fonction SCP (Service Communication Proxy) supporte les fonctionnalités suivantes :
- Routage des opérations de service entre NF consommateur et NF fournisseur
- Partage de charge entre différentes destinations possibles
- Contrôle de congestion en identifiant et en routant le trafic prioritaire et en rejetant le trafic de basse priorité.

La fonction SEPP (Security Edge Protection Proxy) qui représente une fonction proxy à l ’interface entre le réseau interne et les réseaux externes pour le roaming supporte les fonctionnalités additionnelles suivantes à celles d’un SCP :
- Masquage de la topologie pour sécuriser le plan de contrôle 5G d ’un opérateur 5G vis à vis du monde externe.
- Firewalling HTTP/2 pour filtrer tout le trafic HTTP/2 plan de contrôle entrant et sortant du réseau 5GC d ’un opérateur.

Les SEPPs (Security Edge Protection Proxy) représentent les éléments d’interfonctionnement entre réseaux au même titre que les agents DIAMETER (DEAs) et les STPs SS7/SIGTRAN, Par ailleurs les carriers internationaux disposent de leurs proxy HTTP appelés Proxy IPX (IP eXchange) (Figure 6).



SEPP : Security Edge Protection Proxy
IPX : IP eXchange Network

Figure 6 : Architecture de signalisation HTTP/2 dans le contexte du roaming

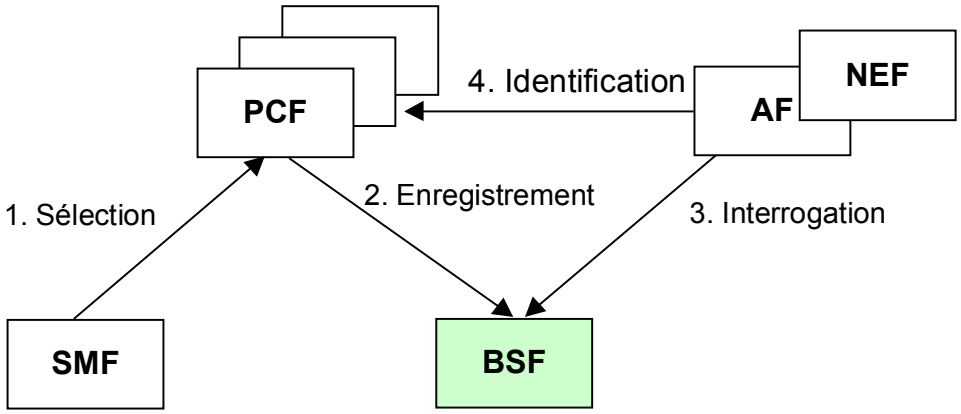
7. BSF et ses services

Une fonctionnalité réseau supplémentaire est généralement nécessaire lorsque la VoIP doit être déployée dans un réseau mobile. Cela couvre le scénario selon lequel plusieurs PCFs sont utilisées dans le réseau 5GC. La PCF doit servir une session de données spécifique et est sélectionnée par la SMF, généralement après avoir interrogé la NRF. Cela signifie que différentes sessions de données peuvent être prises en charge par différentes PCF (ainsi que différentes SMF). Pour qu'une application externe directement ou via la NEF puisse localiser la PCF spécifique qui prend en charge une session de données spécifique à un UE, elle interroge une fonction réseau distincte qui a pour rôle de tenir des registres des sessions prises en charge par les PCFs. Cette fonction réseau est appelée Binding Support Function (BSF). La BSF offre d ’une part des services aux PCF pour enregistrer et désenregistrer des informations sur les sessions de données et d ’autre part des services aux AF et NEF pour obtenir de la BSF les informations sur la PCF qui prend en charge une session de données spécifique.
La BSF présente les caractéristiques suivantes :

- La BSF stocke des informations sur l'identité de l'usager, le DNN, l'adresse ou les adresses UE (IP ou Ethernet), les informations DN (e.g.,, S-NSSAI) et l'adresse de la PCF sélectionnée pour une certaine session PDU. Ces informations peuvent être stockées dans l'UDR en tant que données structurées ou en interne dans la BSF.
- La PCF enregistre, met à jour et supprime les informations de binding auprès de la BSF en utilisant les opérations du service du service NF Nbsf_Management de l ’interface de service de la BSF.
- La PCF s'assure que les informations de binding sont mises à jour chaque fois qu'une adresse IP est allouée, modifiée ou désallouée à la session PDU. Pour l ’obtention des informations de binding, toute NF, telle que NEF ou AF, qui doit découvrir la PCF sélectionnée pour le tuple (adresse UE, DNN, S-NSSAI, SUPI, GPSI) (ou pour un sous-ensemble de ce tuple) utilise l ’opération de service de découverte de service du service NF Nbsf_Management de l’interface de service de la BSF.

Pour montrer le fonctionnement de la BSF, considérons l'exemple suivant (Figure 7) :

1. Lorsqu'une session PDU est établie, la fonction SMF gérant cette session PDU interroge une PCF pour obtenir des règles PCC. Si l'on considère une communication indirecte, la demande de la SMF est routée par la fonction SCP une instance de fonction PCF.
2. La PCF sélectionnée par le SCP met à jour la BSF avec les informations de binding de session.
3. L'AF ou la NEF interroge la BSF pour obtenir l'adresse le la PCF à invoquer. C 'est la fonction BSF qui identifie l 'instance PCF adéquate car elle dispose des informations de la session mises à jour par l 'instance de fonction PCF.
4. Lorsque l 'AF reçoit les informations, elle peut alors délivrer sa demande de service à l 'instance PCF adéquate. La fonction SCP est présente sur tous les échanges entre AF et BSF ainsi qu 'entre AF et PCF si la communication est indirecte. La fonction SCP peut être co-localisée avec la fonction BSF.



5. Figure 7 : Fonction BSF et ses interactions

3GPP TS 29.510, 5G System; Network function repository services; Stage 3
3GPP TS 29.521, 5G System; Binding Support Management Service; Stage 3

La formation EFORT «Réseau de Signalisation HTTP/2 dans le 5GC» décrit l'architecture de signalisation associée au plan contrôle du réseau 5GC et le protocole HTTP/2 utilisé dans ce contexte.
http://www.efort.com/index.php?PageID=21&l=fr&f_id=203&imageField.x=8&imageField.y=5