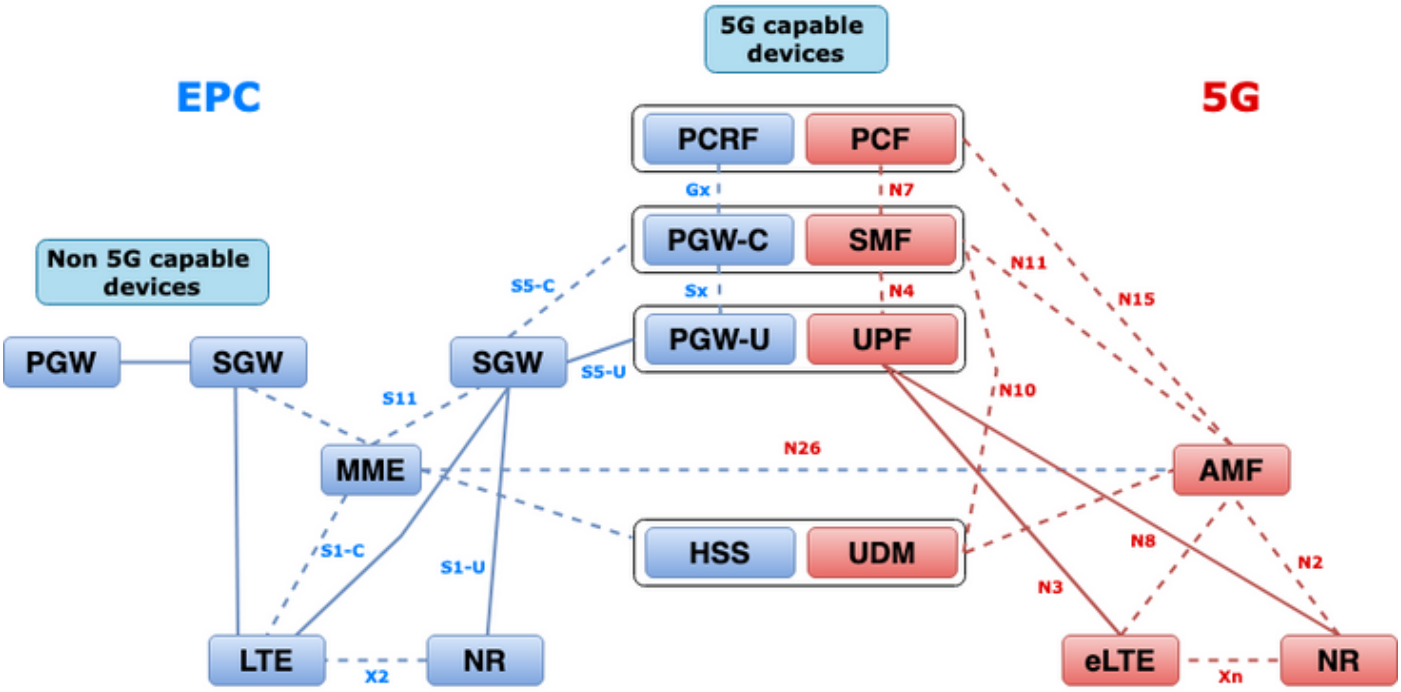
Dépannage des problèmes d'abonnés sur SMF/UPF

Contenu

Introduction

Ce document décrit les commandes CLI utilisées pour les problèmes d'abonnés sur SMF/UPF. Il inclut également des filtres Wireshark pour l'analyse de flux d'appels 5G.

1. Architecture d'interréseau 4G/5G



2. Architecture de base 5G (basée sur les services)

Le modèle de conception architecturale REST a été adopté par 3GPP pour prendre en charge la communication entre les applications et fonctions distribuées sur le coeur 5G.

REST s'appuie sur les protocoles de normes HTTP ou HTTPS pour transmettre des appels entre des entités, et à l'intérieur de cela utilise des identificateurs d'URL uniques, soit un verbe, soit un nom. Les méthodes HTTP ou verbes spécifiés pour REST sont les suivants :

- GET : Récupère la ressource adressée par l'URI dans la demande
- POST: Demande au serveur de créer une nouvelle ressource
- PUT: Remplace (complètement) la ressource adressée par l'URI par la charge utile (format JSON) de la demande
- PATCH : Met à jour une ressource (partiellement)
- DELETE : Supprime la ressource adressée par l'URI dans la demande

Architecture basée sur les services (SBA) : Architecture système dans laquelle les fonctions réseau (NF) assurent la fonctionnalité du système. Fournit des services aux NF autorisés qui consomment leurs services.

Service NF : Un service NF est un type de capacité exposé par un NF (NF Service Producer) à d'autres NF autorisés (NF Service Consumer) via une interface basée sur les services.

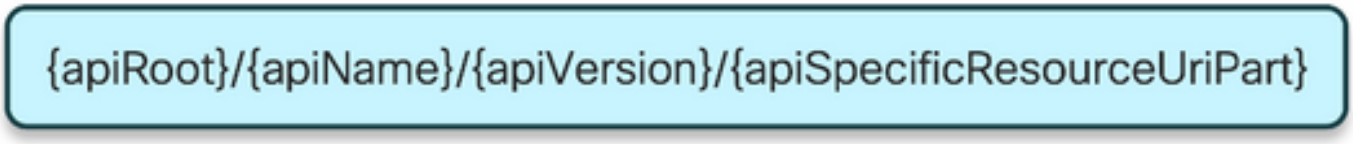
Interface basée sur les services (SBI) : Une interface basée sur les services représente la manière dont l'ensemble de services est fourni ou exposé par un NF donné. Il s'agit de l'interface dans laquelle les opérations de service NF sont appelées. Namf, Nsmf, Nudm, Nnrf, Nnssf, Nausf, Nnef, Nsmsf, etc.

Les interfaces basées sur les services (SBI) utilisent le protocole HTTP/2 sur TCP pour la communication entre les services NF, tel que défini par 3GPP. Le protocole TCP fournit des mécanismes de contrôle de congestion au niveau du transport, comme spécifié dans le document IETF RFC 5681, qui peuvent être utilisés pour le contrôle de congestion entre deux points

d'extrémité TCP (saut par saut). HTTP/2 fournit également des mécanismes de contrôle de flux et des limitations de la concurrence de flux, comme spécifié dans IETF RFC 7540, qui peuvent être configurés pour le contrôle de congestion au niveau de la connexion.

3. Identificateur de ressource unique

Un service NF 5G peut inclure plusieurs ressources accessibles. Un URI (Uniform Resource Identifier) est une chaîne de caractères qui identifie une ressource particulière.



- apiRoot est une concaténation de http:// ou https://, associée à une autorité (port hôte et port facultatif) et une chaîne de caractères spécifique au déploiement en option.
- apiName indique généralement le service appelé par l'API.
- apiVersion est le numéro de version de l'API.
- apiSpecificResourceUriPart indique la ressource spécifique que l'API est conçue pour accéder/manipuler.

4. Fonction de gestion de session (SMF)

La fonction de gestion de session (SMF) de Cisco est l'une des fonctions de réseau du plan de contrôle (NF) du réseau principal 5G (5GC). Le SMF est responsable de la gestion des sessions avec les fonctions individuelles prises en charge pour chaque session.

SMF prend en charge la gestion des sessions (établissement, modification, publication), l'allocation et la gestion des adresses IP de l'UE, les fonctions DHCP, la terminaison de la signalisation NAS liée à la gestion des sessions, la notification des données DL et la configuration de la direction du trafic pour UPF pour un routage approprié du trafic. (AMF dispose d'une partie des fonctionnalités MME et PGW du monde EPC).

5. Fonction du plan utilisateur

La fonction de plan d'utilisateur (UPF) est l'une des fonctions réseau (NF) du réseau principal 5G (5GC). L'UPF est responsable du routage et du transfert des paquets, de l'inspection des paquets, de la gestion de la QoS et de la session PDU externe pour l'interconnexion des réseaux de données (DN), dans l'architecture 5G.

UPF est une fonction de réseau virtuel (VNF) distincte qui offre un moteur de transfert hautes performances pour le trafic utilisateur. Grâce à la technologie VPP (Vector Packet Processing), l'UPF assure un transfert de paquets ultra-rapide tout en conservant la compatibilité avec toutes les fonctionnalités du plan utilisateur.

6. Commandes CLI SMF

6.1. Vérifier si l'abonné spécifique est joint

```
[smf/data] smf# show subscriber namespace smf supi imsi-123969789012404 gr-instance 1
subscriber-details
{
 "subResponses": [
   [
     "roaming-status:visitor-lbo",
     "ue-type:nr-capable",
     "supi:imsi-123969789012404",
     "gpsi:msisdn-22331010101010",
     "pei:imei-123456789012381",
     "psid:1",
     "dnn:testing.com",
     "emergency:false",
     "rat:nr",
     "access:3gpp access",
     "connectivity:5g",
     "udm-uecm:10.10.10.215",
     "udm-sdm:10.10.10.215",
     "auth-status:unauthenticated",
     "pcfGroupId:PCF-dnn=testing.com;",
     "policy:2",
     "pcf:10.10.10.216",
     "upf:10.10.10.150",
     "upfEpKey:10.10.10.150:20.20.20.202",
     "ipv4-addr:pool1/172.16.0.3",
     "ipv4-pool:pool1",
     "ipv4-range:pool1/172.16.0.1",
     "ipv4-startrange:pool1/172.16.0.1",
     "ipv6-pfx:pool1/2001:db0:0:2::",
     "ipv6-pool:pool1",
     "ipv6-range:pool1/2001:db0::",
     "ipv6-startrange:pool1/2001:db0::",
     "id-index:1:0:32768",
     "id-value:2/3",
     "amf:10.10.10.217",
     "peerGtpuEpKey:10.10.10.150:20.0.0.1",
     "namespace:smf",
     "nf-service:smf"
   ]
 ]
}
```

Note: Si la fonctionnalité de redondance GEO (GR) est activée, vous devez vérifier à quelle instance GR l'abonné est connecté.

6.2. Identifier les adresses IP homologues et leur état

```
### NRF Peers
[smf/data] smf# show peers all rpc NRF
GR                                                                  POD
CONNECTED       ADDITIONAL  INTERFACE
INSTANCE  ENDPOINT  LOCAL ADDRESS   PEER ADDRESS       DIRECTION  INSTANCE   TYPE  TIME
RPC  DETAILS     NAME
-------------------------------------------------------------------------------------------
-------------------------
1         <none>    192.168.109.94  20.20.20.219:8080  Outbound   rest-ep-0  Rest  21 hours
NRF  <none>      nrf

### AMF Peers
```

```
[smf/data] smf# show peers all rpc AMF
GR                                                                  POD
CONNECTED       ADDITIONAL  INTERFACE
INSTANCE  ENDPOINT  LOCAL ADDRESS   PEER ADDRESS       DIRECTION  INSTANCE   TYPE  TIME
RPC  DETAILS     NAME
-------------------------------------------------------------------------------------------
-------------------------
1         <none>    192.168.109.94  10.10.10.217:8086  Outbound   rest-ep-0  Rest  21 hours
AMF  <none>      n11

### UDM Peers
[smf/data] smf# show peers all rpc UDM
GR                                                                  POD
CONNECTED       ADDITIONAL  INTERFACE
INSTANCE  ENDPOINT  LOCAL ADDRESS   PEER ADDRESS       DIRECTION  INSTANCE   TYPE  TIME
RPC  DETAILS     NAME
-------------------------------------------------------------------------------------------
-------------------------
1         <none>    192.168.109.94  10.10.10.215:8000  Outbound   rest-ep-0  Rest  21 hours
UDM  <none>      n10

### CHF Peers
[smf/data] smf# show peers all rpc CHF
GR                                                                  POD
CONNECTED       ADDITIONAL  INTERFACE
INSTANCE  ENDPOINT  LOCAL ADDRESS   PEER ADDRESS       DIRECTION  INSTANCE   TYPE  TIME
RPC  DETAILS     NAME
-------------------------------------------------------------------------------------------
-------------------------
1         <none>    192.168.109.94  20.20.20.218:1090  Outbound   rest-ep-0  Rest  21 hours
CHF  <none>      n40

### PCF Peers
[smf/data] smf# show peers all rpc PCF
GR                                                                  POD
CONNECTED       ADDITIONAL  INTERFACE
INSTANCE  ENDPOINT  LOCAL ADDRESS   PEER ADDRESS       DIRECTION  INSTANCE   TYPE  TIME
RPC  DETAILS     NAME
-------------------------------------------------------------------------------------------
-------------------------
1         <none>    192.168.109.94  10.10.10.216:8080  Outbound   rest-ep-0  Rest  19 hours
PCF  <none>      n7
```

6.3. Identifier l'adresse IP UPF

Obtenez l'adresse IP UPF à partir de “ show subscribe namespace smf supi imsi-xxxxxxxxxxxxxxx ”, puis filtrez cette adresse IP particulière à partir de la configuration pour confirmer l'ID de noeud :

```
[smf/data] smf# show subscriber namespace smf supi imsi-123969789012404 gr-instance 1 | include
"upf:"
     "upf:10.10.10.150",

[smf/data] smf# show running-config profile network-element upf n4-peer-address ipv4
10.10.10.150
profile network-element upf upf1
 node-id           n4-peer-NAME
 n4-peer-address ipv4 10.10.10.150
 n4-peer-port      8805
 upf-group-profile upf-group1
```

```
 dnn-list          [ testing.com ]
 capacity          10
 priority          1
exit
```

6.4 Filtrer DNN pour un abonné spécifique

```
[smf/data] smf# show subscriber namespace smf supi imsi-123969789012404 gr-instance 1 | include
"dnn:"
     "dnn:testing.com",
```

6.5. Activer l'abonné Monitor

```
[smf/data] smf# monitor subscriber supi imsi-123969789012404 gr-instance 1 nf-service smf
capture-duration 3600 internal-messages yes
supi: imsi-123969789012404
captureDuraiton: 3600
enableInternalMsg: true
enableTxnLog: false
namespace(deprecated. Use nf-service instead.): none
nf-service: smf
gr-instance: 1
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                Dload  Upload   Total   Spent    Left  Speed
100   305  100   103  100   202   3678   7214 --:--:-- --:--:-- --:--:-- 11296
Command: --header Content-type:application/json --request POST --data
{"commandname":"mon_sub","parameters":{"supi":"imsi-
123969789012404","duration":3600,"enableTxnLog":false,"enableInternalMsg":true,"action":"start",
"namespace":"none","nf-service":"smf","grInstance":1}} http://oam-pod:8879/commands
Result start mon_sub, fileName ->logs/monsublogs/smf.imsi-123969789012404_TS_2022-05-
24T18:27:21.343004358.txt
Starting to tail the monsub messages from file: logs/monsublogs/smf.imsi-
123969789012404_TS_2022-05-24T18:27:21.343004358.txt
Defaulting container name to oam-pod.
Use 'kubectl describe pod/oam-pod-0 -n cn-data' to see all of the containers in this pod.
```

Note: Appuyez sur Ctrl+C pour arrêter la capture.

7. Commandes CLI UPF

7.1. Identifier l'appel d'un abonné spécifique

```
[local]saegw-up1# show subscriber imsi 123969789012404
+-----Access  (S) - pdsn-simple-ip     (M) - pdsn-mobile-ip  (H) - ha-mobile-ip
|     Type:   (P) - ggsn-pdp-type-ppp  (h) - ha-ipsec        (N) - lns-l2tp
|             (I) - ggsn-pdp-type-ipv4                       (G) - IPSG
|             (V) - ggsn-pdp-type-ipv6                       (C) - cscf-sip
|             (z) - ggsn-pdp-type-ipv4v6                     (A) - X2GW
|             (R) - sgw-gtp-ipv4       (O) - sgw-gtp-ipv6    (Q) - sgw-gtp-ipv4-ipv6
|             (W) - pgw-gtp-ipv4       (Y) - pgw-gtp-ipv6    (Z) - pgw-gtp-ipv4-ipv6
|             (B) - pgw-gtp-non-ip     (J) - sgw-gtp-non-ip
|             (@) - saegw-gtp-ipv4     (#) - saegw-gtp-ipv6  ($) - saegw-gtp-ipv4-ipv6
|             (&) - samog-ip           (^) - cgw-gtp-ipv6    (*) - cgw-gtp-ipv4-ipv6
|             (p) - sgsn-pdp-type-ppp  (s) - sgsn            (4) - sgsn-pdp-type-ip
|             (6) - sgsn-pdp-type-ipv6 (2) - sgsn-pdp-type-ipv4-ipv6
|             (L) - pdif-simple-ip     (K) - pdif-mobile-ip  (o) - femto-ip
|             (F) - standalone-fa
```

```
|             (e) - ggsn-mbms-ue       (U) - pdg-ipsec-ipv4
|             (E) - ha-mobile-ipv6     (T) - pdg-ssl         (v) - pdg-ipsec-ipv6
|             (f) - hnbgw-hnb          (g) - hnbgw-iu        (x) - s1-mme
|                                      (k) - PCC
|             (X) - HSGW               (n) - ePDG            (t) - henbgw-ue
|             (m) - henbgw-henb        (q) - wsg-simple-ip   (r) - samog-pmip
|             (D) - bng-simple-ip      (l) - pgw-pmip        (3) - GILAN
|             (y) - User-Plane         (u) - Unknown
|             (+) - samog-eogre        (%) - eMBMS-ipv4      (!) - eMBMS-ipv6
|
|+----Access  (X) - CDMA 1xRTT         (E) - GPRS GERAN      (I) - IP
||    Tech:   (D) - CDMA EV-DO         (U) - WCDMA UTRAN     (W) - Wireless LAN
||            (A) - CDMA EV-DO REVA    (G) - GPRS Other      (M) - WiMax
||            (C) - CDMA Other         (J) - GAN             (O) - Femto IPSec
||            (P) - PDIF               (S) - HSPA            (L) - eHRPD
||            (T) - eUTRAN             (B) - PPPoE           (F) - FEMTO UTRAN
||            (N) - NB-IoT             (Q) - WSG             (.) - Other/Unknown
||
||+---Call    (C) - Connected          (c) - Connecting
|||   State:  (d) - Disconnecting      (u) - Unknown
|||           (r) - CSCF-Registering   (R) - CSCF-Registered
|||           (U) - CSCF-Unregistered
|||
|||+--Access  (A) - Attached           (N) - Not Attached
||||  CSCF    (.) - Not Applicable
||||  Status:
||||
||||+-Link    (A) - Online/Active      (D) - Dormant/Idle
||||| Status:
|||||
|||||+Network (I) - IP                 (M) - Mobile-IP         (L) - L2TP
||||||Type:   (P) - Proxy-Mobile-IP    (i) - IP-in-IP          (G) - GRE
||||||        (V) - IPv6-in-IPv4       (S) - IPSEC             (C) - GTP
||||||        (A) - R4 (IP-GRE)        (T) - IPv6              (u) - Unknown
||||||        (W) - PMIPv6(IPv4)       (Y) - PMIPv6(IPv4+IPv6) (R) - IPv4+IPv6
||||||        (v) - PMIPv6(IPv6)       (/) - GTPv1(For SAMOG)  (+) - GTPv2(For SAMOG)
||||||        (N) - NON-IP             (x) - UDP-IPv4          (X) - UDP-IPv6
||||||
||||||
vvvvvv CALLID   MSID            USERNAME              IP                            TIME-IDLE
------ -------- --------------- --------------------- ----------------------------- ---------
y.C.AI 01317b22 123969789012404 -                     2001:db0:0:3:0:1:317b:2201,172.16.0.4
00h00m00s
```

7.2. Obtenir des informations de niveau abonné (comme les règles, pdr, far, qer, urr)

```
show subs user-plane-only full callid 01317b22
show subs data-rate call 01317b22
show subscribers user-plane-only callid 01317b22 pdr full all
show subscribers user-plane-only callid 01317b22 far full all
show subscribers user-plane-only callid 01317b22 qer full all
show subscribers user-plane-only callid0 1317b22 urr full all
```

> **Note**: Pour cet exemple, nous avons utilisé 01317b22 comme nom. Cependant, vous devez utiliser le callid en fonction du résultat obtenu à l'étape 7.1.

7.3. Activer l'abonné Monitor

```
[local]saegw-up1# monitor subscriber imsi 123969789012404
-------------------------------------------------------------------------------
Matching Call Found:
-------------------------------------------------------------------------------
 MSID/IMSI   : 123969789012404            Callid      : 01317b22
 IMEI        : 123456789012381            MSISDN      : 22331010101010
 Username    : n/a                        SessionType : uplane-ipv4v6
 Status      : Active                     Service Name: upf
 Src Context : up                         Dest Context: ISP
-------------------------------------------------------------------------------
C - Control Events  (ON )      11 - PPP         (ON )  21 - L2TP        (ON )
D - Data Events     (ON )      12 - A11         (ON )  22 - L2TPMGR     (OFF)
E - EventID Info    (ON )      13 - RADIUS Auth (ON )  23 - L2TP Data   (OFF)
I - Inbound Events  (ON )      14 - RADIUS Acct (ON )  24 - GTPC        (ON )
O - Outbound Events (ON )      15 - Mobile IPv4 (ON )  25 - TACACS  (ON )
S - Sender Info     (OFF)      16 - A11MGR      (OFF)  26 - GTPU        (OFF)
T - Timestamps      (ON )      17 - SESSMGR     (ON )  27 - GTPP        (ON )
X - PDU Hexdump     (OFF)      18 - A10         (OFF)  28 - DHCP        (ON )
A - PDU Hex/Ascii   (OFF)      19 - User L3     (OFF)  29 - CDR         (ON )
+/- Verbosity Level (  1)      31 - Radius COA  (ON )  30 - DHCPV6      (ON )
L - Limit Context   (OFF)      32 - MIP Tunnel  (ON )  53 - SCCP        (OFF)
M - Match Newcalls  (ON )      33 - L3 Tunnel   (OFF)  54 - TCAP        (OFF)
R - RADIUS Dict: (no-override) 34 - CSS Data    (OFF)  55 - MAP         (ON )
G - GTPP Dict: (no-override)   35 - CSS Signal  (OFF)  56 - RANAP       (OFF)
Y - Multi-Call Trace (OFF)     36 - EC Diameter (ON )  57 - GMM         (ON )
H - Display ethernet (OFF)     37 - SIP (IMS)   (OFF)  58 - GPRS-NS     (OFF)
                        39 - LMISF (OFF)
U - Mon Display     (ON )      40 - IPSec IKEv2 (OFF)  59 - BSSGP       (OFF)
V - PCAP Hexdump     (OFF)     41 - IPSG RADIUS (ON )  60 - CAP         (ON )
F - Packet Capture: (Full Pkt) 42 - ROHC        (OFF)  64 - LLC         (OFF)
/ - Priority        (  0)      43 - WiMAX R6    (ON )  65 - SNDCP       (OFF)
N - MEH Header      (OFF)      44 - WiMAX Data  (OFF)  66 - BSSAP+      (OFF)
W - UP PCAP Trace   (ON )      45 - SRP         (OFF)  67 - SMS         (OFF)
                               68 - OpenFlow(ON )
                              46 - BCMCS SERV AUTH(OFF)
                              47 - RSVP        (ON )
                              48 - Mobile IPv6 (ON )  69 - X2AP        (ON )
                                                   77 - ICAP/UIDH   (ON )
                              50 - STUN (IMS)  (OFF)  78 - Micro-Tunnel(ON )
                              51 - SCTP        (OFF)
                              72 - HNBAP       (ON )  79 - ALCAP       (ON )
                              73 - RUA         (ON )  80 - SSL         (ON )
                              74 - EGTPC       (ON )
                              75 - App Specific Diameter  (OFF)
                              81 - S1-AP       (ON )  82 - NAS         (ON )
                              83 - LDAP        (ON )  84 - SGS         (ON )
                              85 - AAL2        (ON )  86 - S102         (ON )
                              87 - PPPOE  (ON )
                              88 - RTP(IMS)    (OFF)  89 - RTCP(IMS)   (OFF)
                              91 - NPDB(IMS)  (OFF)
                              92 - SABP  (ON )
                              94 - SLS   (ON )
                              96 - SBc-AP  (ON )
                              97 - M3AP    (ON )
                              49 - PFCP    (ON )
                              76 - NSH    (ON )
 (Q)uit,   <ESC> Prev Menu,   <SPACE> Pause,   <ENTER> Re-Display Options
*** User L3 PDU Decodes (ON ) ***
*** GTPU PDU Decodes (ON ) ***
*** CSS Data Decodes (ON ) ***
*** CSS Signaling (ON ) ***
*** session initiation protocol (SIP) decodes (ON ) ***
*** IPSEC IKE Subscriber (ON ) ***
*** Real Time Transport Protocol(RTP) decodes (ON ) ***
```

```
*** Real Time Transport Control Protocol(RTCP) decodes (ON ) ***
*** PDU Hex+Ascii dump (ON ) ***
*** PDU Hexdump (ON ) ***
*** Multi-Call Trace (ON ) ***
*** Verbosity Level (  2) ***
*** Verbosity Level (  3) ***
*** Verbosity Level (  4) ***
*** Verbosity Level (  5) ***
```

Note: Activez les options nécessaires en fonction du problème de l'abonné (les plus courantes sont A, X, Y, 19, 26, 34, 35, et 37, 40, 88, 89 pour les appels VoLTE plus verbosity 5). Saisissez Q pour arrêter l'abonné du moniteur.

7.4. Obtenir des PCAP chemin lent/vpp pour un abonné spécifique

```
[local]saegw-up1# monitor subscriber imsi 123969789012404
-------------------------------------------------------------------------
Matching Call Found:
-------------------------------------------------------------------------
 MSID/IMSI   : 123969789012404            Callid      : 01317b22
 IMEI        : 123456789012381            MSISDN      : 22331010101010
 Username    : n/a                        SessionType : uplane-ipv4v6
 Status      : Active                     Service Name: upf
 Src Context : up                         Dest Context: ISP
-------------------------------------------------------------------------
C - Control Events  (ON )      11 - PPP         (ON )  21 - L2TP        (ON )
D - Data Events     (ON )      12 - A11         (ON )  22 - L2TPMGR     (OFF)
E - EventID Info    (ON )      13 - RADIUS Auth (ON )  23 - L2TP Data   (OFF)
I - Inbound Events  (ON )      14 - RADIUS Acct (ON )  24 - GTPC        (ON )
O - Outbound Events (ON )      15 - Mobile IPv4 (ON )  25 - TACACS  (ON )
S - Sender Info     (OFF)      16 - A11MGR      (OFF)  26 - GTPU        (OFF)
T - Timestamps      (ON )      17 - SESSMGR     (ON )  27 - GTPP        (ON )
X - PDU Hexdump     (OFF)      18 - A10         (OFF)  28 - DHCP        (ON )
A - PDU Hex/Ascii   (OFF)      19 - User L3     (OFF)  29 - CDR         (ON )
+/- Verbosity Level (  1)      31 - Radius COA  (ON )  30 - DHCPV6      (ON )
L - Limit Context   (OFF)      32 - MIP Tunnel  (ON )  53 - SCCP        (OFF)
M - Match Newcalls  (ON )      33 - L3 Tunnel   (OFF)  54 - TCAP        (OFF)
R - RADIUS Dict: (no-override) 34 - CSS Data    (OFF)  55 - MAP         (ON )
G - GTPP Dict: (no-override)   35 - CSS Signal  (OFF)  56 - RANAP       (OFF)
Y - Multi-Call Trace (OFF)     36 - EC Diameter (ON )  57 - GMM         (ON )
H - Display ethernet (OFF)     37 - SIP (IMS)   (OFF)  58 - GPRS-NS     (OFF)
                       39 - LMISF (OFF)
U - Mon Display     (ON )      40 - IPSec IKEv2 (OFF)  59 - BSSGP       (OFF)
V - PCAP Hexdump    (ON)      41 - IPSG RADIUS (ON )  60 - CAP         (ON )
F - Packet Capture: (Full Pkt) 42 - ROHC        (OFF)  64 - LLC         (OFF)
/ - Priority        (  0)      43 - WiMAX R6    (ON )  65 - SNDCP       (OFF)
N - MEH Header      (OFF)      44 - WiMAX Data  (OFF)  66 - BSSAP+      (OFF)
W - UP PCAP Trace   (ON )      45 - SRP         (OFF)  67 - SMS         (OFF)
                               68 - OpenFlow(ON )
                              46 - BCMCS SERV AUTH(OFF)
                              47 - RSVP        (ON )
                              48 - Mobile IPv6 (ON )  69 - X2AP        (ON )
                                                  77 - ICAP/UIDH   (ON )
                              50 - STUN (IMS)  (OFF)  78 - Micro-Tunnel(ON )
                              51 - SCTP        (OFF)
                              72 - HNBAP       (ON )  79 - ALCAP       (ON )
                              73 - RUA         (ON )  80 - SSL         (ON )
                              74 - EGTPC       (ON )
                              75 - App Specific Diameter  (OFF)
                              81 - S1-AP       (ON )  82 - NAS         (ON )
```

```
                              83 - LDAP        (ON )  84 - SGS         (ON )
                              85 - AAL2        (ON )  86 - S102         (ON )
                              87 - PPPOE  (ON )
                              88 - RTP(IMS)    (OFF)  89 - RTCP(IMS)   (OFF)
                              91 - NPDB(IMS)  (OFF)
                              92 - SABP  (ON )
                              94 - SLS   (ON )
                              96 - SBc-AP  (ON )
                              97 - M3AP    (ON )
                              49 - PFCP    (ON )
                              76 - NSH    (ON )
 (Q)uit,   <ESC> Prev Menu,   <SPACE> Pause,   <ENTER> Re-Display Options
```

Note: L'abonné de surveillance peut être activé avec l'option V afin de générer les PCAP chemin lent/vpp. Téléchargez les PCAP chemin lent/vpp depuis “ répertoire /hd-raid/records/hexdump ”.

8. Filtres utiles sur Wireshark par interface SBI

8.1. Protocole NGAP (NG Application Protocol)

Le protocole NGAP (NG Application Protocol) fournit la signalisation du plan de contrôle entre le noeud NG-RAN et la fonction AMF (Access and Mobility Management Function). Voici quelques filtres Wireshark utiles pour le protocole d'application NG :

```
ngap.RAN_UE_NGAP_ID == <NGAP_ID>
ngap.procedureCode == 29
ngap.pDUSessionID == 5
```

8.2. Interface NRF

La fonction NRF (NF Repository) prend en charge la fonction de découverte de service et gère le profil NF et les instances NF disponibles. (non présent dans le monde de la CBE). Voici quelques filtres Wireshark utiles pour l'interface NRF :

```
http2.header.value contains "/nnrf-nfm/v1/nf-instances/"
http2.header.value == "/nnrf-nfm/v1/nf-instances/xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
json.value.string == "REGISTERED"
json.value.string == "UNDISCOVERABLE"
```

8.3. Inscription/abonnement UDM (interface N10)

La gestion unifiée des données (UDM) prend en charge la génération d'identifiants d'authentification et d'accord de clé (AKA), la gestion de l'identification des utilisateurs, l'autorisation d'accès et la gestion des abonnements. (partie de la fonctionnalité HSS d'EPC World). Voici quelques filtres Wireshark utiles pour l'interface N10 :

```
## Registration
http2.header.value contains "/nudm-uecm/v1/imsi-" && http2.header.value contains
"/registrations/smf-registrations"

## DELETE Registration
http2.header.value == "DELETE" && http2.header.value contains "/registrations/smf-registrations"
```

```
## Subscription
http2.header.value contains "/nudm-sdm/v2/imsi-" && http2.header.value contains "/sdm-
subscriptions"

## Subscription Fetch
http2.header.value contains "/nudm-sdm/v2/" && http2.header.value contains "/sm-
data?dnn=<dnn_name>&plmn-id="
```

8.4. AMF (interface N11)

La fonction AMF (Access and Mobility Management Function) prend en charge la terminaison de la signalisation NAS, le chiffrement NAS et la protection de l'intégrité, la gestion des enregistrements, la gestion des connexions, la gestion de la mobilité, l'authentification et l'autorisation d'accès, ainsi que la gestion du contexte de sécurité. (AMF possède une partie de la fonctionnalité MME du monde EPC). Voici quelques filtres Wireshark utiles pour l'interface N11 :

```
## Filter all SM-Context packages
http2.header.value contains "/nsmf-pdusession/v1/sm-contexts"

## Filter SM-Context Release
http2.header.value contains "/nsmf-pdusession/v1/sm-contexts" && http2.header.value contains
"/release"

## Filter SM-Context Retrieve
http2.header.value contains "/nsmf-pdusession/v1/sm-contexts" && http2.header.value contains
"/retrieve"

## Filter SM-Context Modify
http2.header.value contains "/nsmf-pdusession/v1/sm-contexts" && http2.header.value contains
"/modify"

## Filter all UE-Context packages
http2.header.value contains "/namf-comm/v1/ue-contexts/imsi-"

## Filter all UE-Context Assign-EBi
http2.header.value contains "/namf-comm/v1/ue-contexts/imsi-" && http2.header.value contains
"/assign-ebi"

## Filter all UE-Context N1N2-Message
http2.header.value contains "/namf-comm/v1/ue-contexts/imsi-" && http2.header.value contains
"/n1-n2-message"

## Filter all UE-Context Assign-EBi/N1N2-Message for specific SUPI
http2.header.value == "/namf-comm/v1/ue-contexts/imsi-xxxxxxxxxxxxxxx/assign-ebi"
http2.header.value == "/namf-comm/v1/ue-contexts/imsi-xxxxxxxxxxxxxxx/n1-n2-messages"
```

8.5. PCF (interface N7)

La fonction PCF (Policy Control Function) prend en charge un cadre de stratégie unifié, fournissant des règles de stratégie aux fonctions CP et l'accès aux informations d'abonnement pour les décisions de stratégie dans UDR. (PCF possède une partie de la fonctionnalité PCRF du monde EPC) Authentication Server Function (AUSF) agit en tant que serveur d'authentification (partie de HSS du monde EPC). Voici quelques filtres Wireshark utiles pour l'interface N7 :

```
### Filter all SM-Policy packages
http2.header.value contains "/npcf-smpolicycontrol"

## Filter SM-Policy Create Request
http2.header.value == "/npcf-smpolicycontrol/v1/sm-policies"
```

```
## Filter all SM-Policy from specific SUPI
http2.header.value contains "/npcf-smpolicycontrol/v1/sm-policies" && http2.header.value
contains "imsi-xxxxxxxxxxxxxxx"

## Filter SM-Policy Update
http2.header.value contains "/npcf-smpolicycontrol/v1/sm-policies/ism.5.imsi-" &&
http2.header.value contains "/update"

#### Filter SM-Policy Delete
http2.header.value contains "/npcf-smpolicycontrol/v1/sm-policies/ism.5.imsi-" &&
http2.header.value contains "/delete"

#### Filter SM-Policy Update Notification
http2.header.value contains "smPoliciesUpdateNotification"
```

8.6. CHF (interface N40)

La fonction de charge (CHF) est une fonction réseau de base de la SA 5G et prend en charge la fonctionnalité de système de charge convergé 3GPP. CHF prend en charge la fonction de facturation en ligne et hors ligne pour plusieurs services, notamment l'intégration de coeur 5G et 4G. Voici quelques filtres Wireshark utiles pour l'interface N40 :

```
http2.header.value == "/nchf-convergedcharging/v2/chargingdata/"
http2.header.value contains "/nchf-convergedcharging/"
```

8.7. Filtres supplémentaires utiles tels que les erreurs de code et RST_STREAM

```
## PDU session establishment accept
nas_5gs.sm.message_type == 0xc2

## PDU session establishment reject
nas_5gs.sm.message_type == 0xc3

## GTPv2 (filter specific IMSI)
e212.imsi == xxxxxxxxxxxxxxx

## GTPv2 (S5/S8 interface type)
gtpv2.f_teid_interface_type == 6

## GTPv2 (S2b ePDG interface type)
gtpv2.f_teid_interface_type == 30

## Search for Specific Errors
http2.header.value == 400
http2.header.value == 404
http2.header.value == 413
http2.header.value == 410
http2.header.value == 409
http2.header.value == 500
json.value.string == CONTEXT_NOT_FOUND
json.value.string == USER_NOT_FOUND

## RST_STREAM
http2.rst_stream.error
```

> **Note**: Tenez compte que pour visualiser le protocole HTTP2, vous devez décoder le numéro de port en conséquence sur Wireshark à partir de **Analyze**. Sélectionnez **Décoder** comme option.

```
Field      Value            Type             Default               Current

TCP port   <port_number>    Integer, base 10 none                  HTTP2
```

Nom de fichier	Texte alternatif proposé
diagramme_interréseau.png	Architecture d'interconnexion de réseaux 4G/5G
uri.png	Identificateur de ressource unique