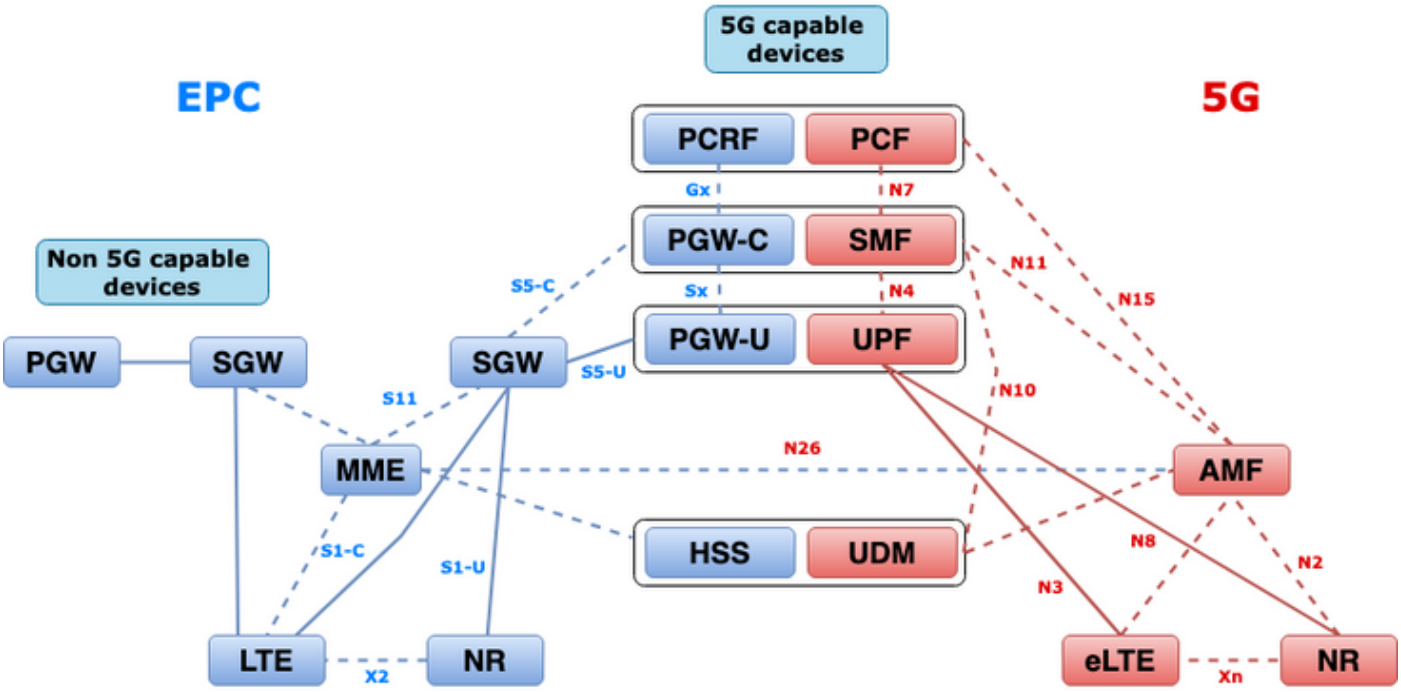
Solucionar problemas do assinante em SMF/UPF

Contents

Introduction

Este documento descreve os comandos CLI usados para problemas do assinante em SMF/UPF. Além disso, inclui filtros do Wireshark para análise de fluxo de chamadas 5G.

1. Arquitetura de internetwork 4G/5G



2. Arquitetura de núcleo 5G (baseada em serviços)

O modelo de projeto de arquitetura REST (Representational State Transfer) foi adotado pela 3GPP para suportar a comunicação entre os aplicativos distribuídos e as funções no núcleo 5G.

O REST depende dos protocolos padrão HTTP ou HTTPS para transmitir chamadas entre entidades, e dentro disso aproveita identificadores de URL exclusivos, seja um verbo ou um nome. Os métodos ou verbos HTTP especificados para REST são os seguintes:

- GET: Recupera o recurso endereçado pelo URI na solicitação
- POST: Solicita ao servidor que crie um novo recurso
- PUT: Substitui (completamente) o recurso endereçado pelo URI pelo payload (formato JSON) da solicitação
- PATCH: Atualiza um recurso (parcialmente)
- DELETE: Exclui o recurso endereçado pelo URI na solicitação

Arquitetura baseada em serviços (SBA): Uma arquitetura de sistema na qual a funcionalidade do sistema é obtida pelas funções de rede (NFs). Fornece serviços para NFs autorizadas que consomem seus serviços.

Serviço NF: Um serviço de NF é um tipo de recurso exposto por um NF (NF Service Producer) a outra NF autorizada (NF Service Consumer) através de uma interface baseada em serviço.

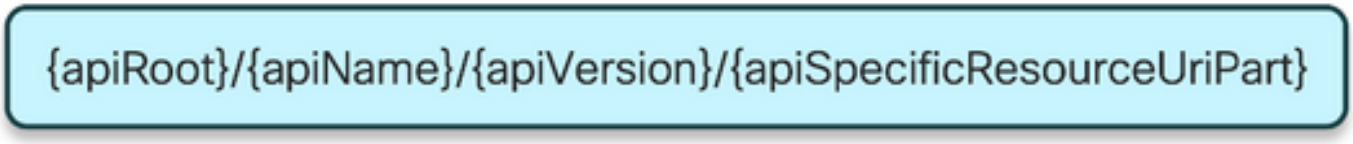
Interface baseada em serviços (SBI): Uma interface baseada em serviços representa como o conjunto de serviços é fornecido ou exposto por uma determinada NF. Esta é a interface onde as operações de serviço NF são chamadas. Namf, Nsmf, Nudm, Nnrf, Nnssf, Nausf, Nnef, Nsmsf, etc.

As Interfaces Baseadas em Serviço (SBI - Service Based Interfaces) usam o protocolo HTTP/2 sobre TCP para comunicação entre os Serviços NF, conforme definido por 3GPP. O TCP fornece mecanismos de controle de congestionamento no nível de transporte conforme especificado no IETF RFC 5681, que podem ser usados para controle de congestionamento entre dois pontos de

extremidade TCP (ou seja, salto por salto). O HTTP/2 também fornece mecanismos de controle de fluxo e limitações de simultaneidade de fluxo, conforme especificado no IETF RFC 7540, que podem ser configurados para controle de congestionamento no nível de conexão.

3. Uniform Resource Identifier

Um serviço NF 5G pode incluir vários recursos que podem ser acessados. Um Uniform Resource Identifier (URI) é uma sequência de caracteres que identifica um recurso específico.



- apiRoot é uma concatenação de http:// ou https://, juntamente com uma autoridade (host e porta opcional) e uma string opcional específica de implantação.
- apiName normalmente indica o serviço chamado pela API.
- apiVersion é o número da versão da API.
- apiSpecificResourceUriPart denota o recurso específico que a API foi projetada para acessar/manipular.

4. Função de gerenciamento de sessão (SMF)

A Cisco Session Management Function (SMF) é uma das funções de rede do plano de controle (NF) da rede central 5G (5GC). O SMF é responsável pelo gerenciamento de sessões com as funções individuais suportadas por sessão.

O SMF suporta gerenciamento de sessão (estabelecimento de sessão, modificação, versão), alocação e gerenciamento de endereços IP UE, funções DHCP, terminação da sinalização NAS relacionada ao gerenciamento de sessão, notificação de dados DL e configuração de direcionamento de tráfego para UPF para roteamento de tráfego apropriado. (A AMF tem parte da funcionalidade MME e PGW do mundo do EPC).

5. Função de plano do usuário

A UPF (User Plane Function - Função do plano do usuário) é uma das funções de rede (NFs) da rede central 5G (5GC). O UPF é responsável pelo roteamento e encaminhamento de pacotes, inspeção de pacotes, tratamento de QoS e sessão de PDU externa para interconexão de redes de dados (DN), na arquitetura 5G.

O UPF é uma função de rede virtual (VNF) distinta que oferece um mecanismo de encaminhamento de alto desempenho para o tráfego do usuário. Com a tecnologia VPP (Vetor Packet Processing, processamento de pacote vetorial), o UPF consegue o encaminhamento de pacotes ultrarrápido, mantendo a compatibilidade com toda a funcionalidade do plano do usuário.

6. Comandos CLI SMF

6.1. Verifique se o assinante específico está conectado

```
[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: Se você tiver o recurso GEO Redundancy (GR) habilitado, precisará verificar a qual instância GR o assinante está conectado.

6.2. Identificar endereços IP de peer e seu status

```
### 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. Identificar endereço IP UPF

Obtenha o IP UPF de "show subscriber namespace smf supi imsi-xxxxxxxxxxxxx" e, em seguida, filtre esse endereço IP específico da configuração para confirmar o ID do nó:

```
[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 Filtrar DNN para um assinante específico

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

6.5. Ativar assinante de 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: Digite Ctrl+C para interromper a captura.

7. Comandos CLI UPF

7.1. Identificar um assinante específico chamado

```
[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. Obter informações de nível de assinante (como regras, 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: Para este exemplo, usamos 01317b22 como chamada. No entanto, você precisa usar a chamada com base na saída obtida da etapa 7.1.

7.3. Ativar assinante de 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: Ative as opções necessárias com base no problema do assinante (as mais comuns são A, X, Y, 19, 26, 34, 35 e 37, 40, 88, 89 para chamada VoLTE mais verbosity 5). Digite Q para interromper o assinante do monitor.

7.4. Obtenha PCAPs de caminho lento/vpp para assinante específico

```
[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: O assinante do monitor pode ser ativado com a Opção V para gerar os PCAPs de caminho lento/vpp. Baixe os PCAPs de caminho lento/vpp de "dir /hd-raid/Records/hexdump".

8. Filtros úteis no Wireshark por interface SBI

8.1. NGAP (NG Application Protocol)

O NG Application Protocol (NGAP) fornece a sinalização do plano de controle entre o nó NG-RAN e a função de gerenciamento de acesso e mobilidade (AMF). Aqui você tem alguns filtros úteis do Wireshark para o NG Application Protocol:

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

8.2. Interface NRF

A função de repositório NF (NRF) suporta a função de descoberta de serviços e mantém o perfil NF e as instâncias NF disponíveis. (não presente no mundo do CEP). Aqui você tem alguns filtros úteis do Wireshark para a 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. Inscrição/assinatura do UDM (Interface N10)

O Unified Data Management (UDM) suporta a geração de credenciais de Autenticação e Acordo Chave (AKA), tratamento de identificação de usuário, autorização de acesso e gerenciamento de assinatura. (parte da funcionalidade HSS do EPC). Aqui você tem alguns filtros úteis do Wireshark para a 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)

A função de gerenciamento de acesso e mobilidade (AMF) suporta terminação de sinalização NAS, criptografia NAS e proteção de integridade, gerenciamento de registro, gerenciamento de conexão, gerenciamento de mobilidade, autenticação e autorização de acesso e gerenciamento de contexto de segurança. (A AMF tem parte da funcionalidade da MME do mundo do EPC). Aqui você tem alguns filtros úteis do Wireshark para a 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)

O Policy Control Function (PCF) suporta uma estrutura de política unificada, fornecendo regras de política para funções do CP e acesso a informações de assinatura para decisões de política no UDR. A função de servidor de autenticação (AUSF) atua como um servidor de autenticação (parte do HSS do mundo do EPC). Aqui você tem alguns filtros úteis do Wireshark para a 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-xxxxxxxxxxxxxx"

## 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)

A CHF (Charging Function, Função de cobrança) é uma função central de rede SA de 5G e suporta a funcionalidade 3GPP de sistema de cobrança convergente. O CHF suporta o recurso de cobrança online e offline para vários serviços, incluindo integração de núcleo 5G e 4G. Aqui você tem alguns filtros úteis do Wireshark para a interface N40:

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

8.7. Filtros úteis adicionais como erros de código e 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 == xxxxxxxxxxxxxx

## 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**: Considere que, para visualizar o protocolo HTTP2, você precisa decodificar o número da porta de acordo com o Wireshark em **Analyze**. Selecione **Decodificar** como uma opção.

```
Field      Value            Type             Default              Current
```

TCP port	<port_number>	Integer, base 10 none	HTTP2

nome do arquivo	Texto alternativo proposto
diagrama_internetworking.png	Arquitetura de interconexão de redes 4G/5G
uri.png	Uniform Resource Identifier