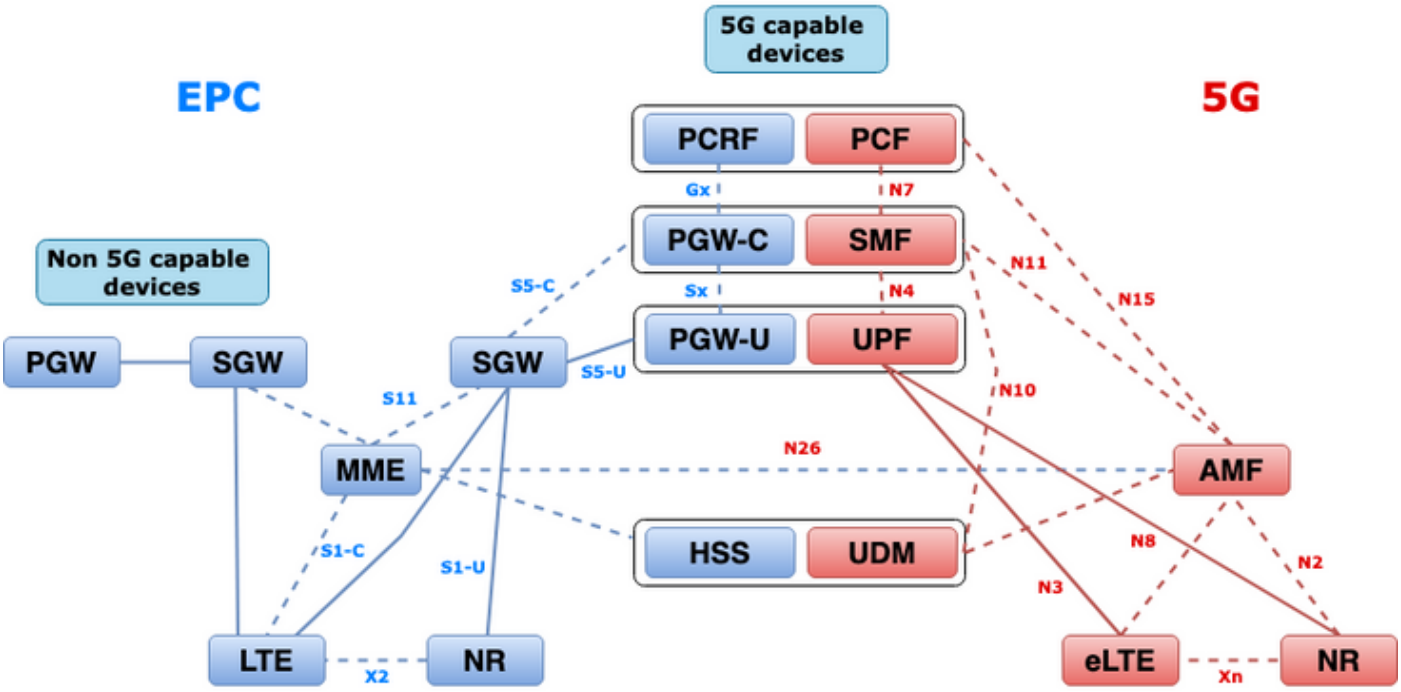
Fehlerbehebung bei Teilnehmerproblemen mit SMF/UPF

Inhalt

Einleitung

In diesem Dokument werden CLI-Befehle für Teilnehmerprobleme bei SMF/UPF beschrieben. Darüber hinaus enthält es Wireshark-Filter für 5G-Anrufflussanalysen.

1. 4G/5G Internetwork Architecture



2. 5G Core (servicebasierte) Architektur

Das Representational State Transfer (REST)-Architekturdesign-Modell wurde von 3GPP eingeführt, um die Kommunikation zwischen den verteilten Anwendungen und Funktionen auf dem 5G-Core zu unterstützen.

REST verwendet die Standardprotokolle HTTP oder HTTPS, um Anrufe zwischen Entitäten zu übertragen. In diesem Fall werden eindeutige URL-IDs verwendet, entweder ein Verb oder ein Substantiv. Die angegebenen HTTP-Methoden oder -Verben für REST sind wie folgt:

- GET: Ruft die vom URI in der Anforderung adressierte Ressource ab
- POST: fordert den Server auf, eine neue Ressource zu erstellen
- PUT: Ersetzt (vollständig) die vom URI adressierte Ressource durch die Payload (JSON-Format) der Anforderung
- PATCH: Aktualisiert eine Ressource (teilweise)
- LÖSCHEN: Löscht die vom URI in der Anforderung adressierte Ressource

Service Based Architecture (SBA): Eine Systemarchitektur, in der die Systemfunktionalität durch Netzwerkfunktionen (NFs) erreicht wird. Stellt Services für autorisierte NFs bereit, die ihre Services nutzen.

NF-Service: Ein NF-Dienst ist ein Funktionstyp, der von einem NF (NF Service Producer) anderen autorisierten NF (NF Service Consumer) über eine servicebasierte Schnittstelle verfügbar gemacht wird.

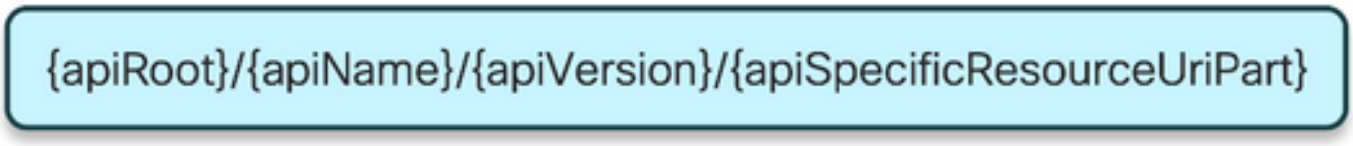
Service Based Interface (SBI): Eine servicebasierte Schnittstelle stellt dar, wie der Satz von Diensten von einer bestimmten NF bereitgestellt oder verfügbar gemacht wird. Dies ist die Schnittstelle, an der die NF-Dienstvorgänge aufgerufen werden. Namf, NSMF, Nudm, NNRF, NNSSF, NAUSF, NSMSF usw.

Die Service Based Interfaces (SBI) verwenden HTTP/2 Protocol over TCP für die Kommunikation zwischen den NF Services gemäß 3GPP. TCP stellt Überlastungskontrollmechanismen auf

Transportebene bereit, wie in IETF RFC 5681 angegeben, die für die Überlastungskontrolle zwischen zwei TCP-Endpunkten (Hop-by-Hop) verwendet werden können. HTTP/2 bietet außerdem Datenflusskontrollmechanismen und Einschränkungen der Parallelität von Streams, wie in IETF RFC 7540 angegeben, die für die Überlastungssteuerung auf Verbindungsebene konfiguriert werden können.

3. Einheitliche Ressourcenkennung

Ein 5G NF-Dienst kann mehrere Ressourcen enthalten, auf die zugegriffen werden kann. Ein URI (Uniform Resource Identifier) ist eine Zeichenfolge von Zeichen, die eine bestimmte Ressource identifizieren.



- apiRoot ist eine Verkettung von http:// oder https://, gekoppelt mit einer Authority (Host und optionaler Port) und einer optionalen bereitstellungsspezifischen Zeichenfolge.
- apiName bezeichnet in der Regel den Dienst, der von der API aufgerufen wird.
- apiVersion ist die Versionsnummer der API.
- apiSpecificResourceUriPart gibt die spezifische Ressource an, auf die die API zugreifen und die sie bearbeiten soll.

4. Session Management-Funktion (SMF)

Die Cisco Session Management Function (SMF) ist eine der Steuerungsebenen-Netzwerkfunktionen (NF) des 5G-Core-Netzwerks (5GC). Der SMF ist für das Sitzungsmanagement mit den unterstützten Einzelfunktionen pro Sitzung verantwortlich.

SMF unterstützt Sitzungsmanagement (Sitzungserstellung, Änderung, Freigabe), UE-IP-Adresszuweisung und -verwaltung, DHCP-Funktionen, Beendigung der NAS-Signalisierung im Zusammenhang mit Sitzungsmanagement, DL-Datenbenachrichtigung und Konfiguration der Datenverkehrssteuerung für UPF für eine ordnungsgemäße Datenverkehrsweiterleitung. (AMF ist Teil der MME- und PGW-Funktionalität der EPC-Welt).

5. Funktion der Benutzerebene

Die User Plane Function (UPF) ist eine der Netzwerkfunktionen (NFs) des 5G-Core-Netzwerks (5GC). Die UPF ist für Paketrouting und -weiterleitung, Paketprüfung, QoS-Verarbeitung und externe PDU-Sitzungen zur Verbindung von Data Networks (DN) in der 5G-Architektur verantwortlich.

UPF ist eine eigenständige Virtual Network Function (VNF), die eine leistungsstarke Weiterleitungs-Engine für Benutzerdatenverkehr bereitstellt. Mit der VPP-Technologie (Vector Packet Processing) erreicht die UPF eine extrem schnelle Paketweiterleitung, ohne dabei die Kompatibilität mit allen Funktionen auf Benutzerebene zu beeinträchtigen.

6. SMF CLI-Befehle

6.1. Überprüfen Sie, ob der jeweilige Teilnehmer angeschlossen ist.

```
[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"
   ]
 ]
}
```

Anmerkung: Wenn die GEO Redundancy (GR)-Funktion aktiviert ist, müssen Sie überprüfen, mit welcher GR-Instanz der Abonnent verbunden ist.

6.2. Identifizieren von Peer-IP-Adressen und deren 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. UPF-IP-Adresse identifizieren

Rufen Sie die UPF-IP aus "show Subscriber namespace smf supi imsi-xxxxxxxxxxxxx" ab, und filtern Sie diese spezielle IP-Adresse aus der Konfiguration, um die Knoten-ID zu bestätigen:

```
[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 Filtern von DNN für einen bestimmten Kunden

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

6.5. Monitor-Subscriber aktivieren

```
[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.
```

Anmerkung: Geben Sie Strg+C ein, um die Erfassung zu stoppen.

7. UPF CLI-Befehle

7.1. Angerufene für einen bestimmten Kunden identifizieren

```
[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. Abrufen von Informationen auf Teilnehmerebene (z. B. RegelnDefs, 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
```

Anmerkung: In diesem Beispiel wurde 01317b22 als "callid" verwendet. Sie müssen jedoch den berechneten Wert basierend auf der Ausgabe verwenden, die Sie aus Schritt 7.1 erhalten.

7.3. Monitor-Subscriber aktivieren

```
[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) ***
```

Anmerkung: Aktivieren Sie die erforderlichen Optionen basierend auf dem Teilnehmerproblem (die häufigsten sind A, X, Y, 19, 26, 34, 35 und 37, 40, 88, 89 für VoLTE-Anruf plus Ausführlichkeit 5). Geben Sie Q ein, um den Monitorteilnehmer zu stoppen.

7.4. Langsamer Pfad/VPP-PCAPs für bestimmte Teilnehmer abrufen

```
[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
```

Anmerkung: Monitor-Subscriber können mit Option V aktiviert werden, um langsame Pfad-/VPP-PCAPs zu generieren. Laden Sie die slow path/vpp PCAPs von "dir /hd-raid/record/hexdump" herunter.

8. Nützliche Filter auf Wireshark pro SBI-Schnittstelle

8.1. NG Application Protocol (NGAP)

NG Application Protocol (NGAP) stellt die Signalisierung auf Kontrollebene zwischen dem NG-RAN-Knoten und der Access and Mobility Management Function (AMF) bereit. Hier finden Sie einige nützliche Wireshark-Filter für NG-Anwendungsprotokolle:

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

8.2. NRF-Schnittstelle

Die NF Repository-Funktion (NRF) unterstützt die Diensterkennungsfunktion und verwaltet das NF-Profil und die verfügbaren NF-Instanzen. (in der EPC-Welt nicht vorhanden). Hier finden Sie einige nützliche Wireshark-Filter für die NRF-Schnittstelle:

```
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. UDM-Registrierung/-Abonnement (N10-Schnittstelle)

Unified Data Management (UDM) unterstützt die Generierung von Authentifizierungs- und Key Agreement (AKA)-Anmeldeinformationen, die Bearbeitung von Benutzeridentifizierungen, die Zugriffsautorisierung und das Abonnementmanagement. (Teil der HSS-Funktionalität aus der EPC-Welt). Hier finden Sie einige nützliche Wireshark-Filter für die N10-Schnittstelle:

```
## 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 (N11-Schnittstelle)

Die Access and Mobility Management Function (AMF) unterstützt die Terminierung von NAS-Signalisierung, NAS-Verschlüsselung und -Integritätsschutz, Registrierungsmanagement, Verbindungsmanagement, Mobilitätsmanagement, Zugriffsauthentifizierung und -autorisierung sowie das Management von Sicherheitskontexten. (AMF ist Teil der MME-Funktionalität aus der EPC-Welt.) Hier finden Sie einige nützliche Wireshark-Filter für die N11-Schnittstelle:

```
## 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 (N7-Schnittstelle)

Policy Control Function (PCF) unterstützt ein einheitliches Richtlinien-Framework, das Richtlinienregeln für CP-Funktionen bereitstellt und Zugriff auf Abonnementinformationen für Richtlinienentscheidungen im UDR bietet. (PCF ist Teil der PCRF-Funktionalität der EPC-Welt) Die Authentifizierungsserver-Funktion (AUSF) fungiert als Authentifizierungsserver (Teil des HSS aus der EPC-Welt). Hier finden Sie einige nützliche Wireshark-Filter für die N7-Schnittstelle:

```
### 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 (N40-Schnittstelle)

Charging Function (CHF) ist eine 5-G-SA-Core-Netzwerkfunktion und unterstützt die Funktion des konvergenten 3GPP-Charging-Systems. CHF unterstützt die Online- und Offline-Gebührenfunktion für mehrere Services, einschließlich 5G- und 4G-Core-Integration. Hier finden Sie einige nützliche Wireshark-Filter für die N40-Schnittstelle:

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

8.7. Zusätzliche nützliche Filter wie Codefehler und 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
```

Anmerkung: Beachten Sie, dass Sie zur Visualisierung des HTTP2-Protokolls die Portnummer in Wireshark aus **Analyze** decodieren müssen. Wählen Sie als Option **Decode** aus.

```
Field      Value            Type             Default              Current

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

Dateiname	Vorgeschlagener alt-text
diagramm_internetworking.png	4G/5G Internetworking-Architektur
uri.png	Einheitliche Ressourcenkennung