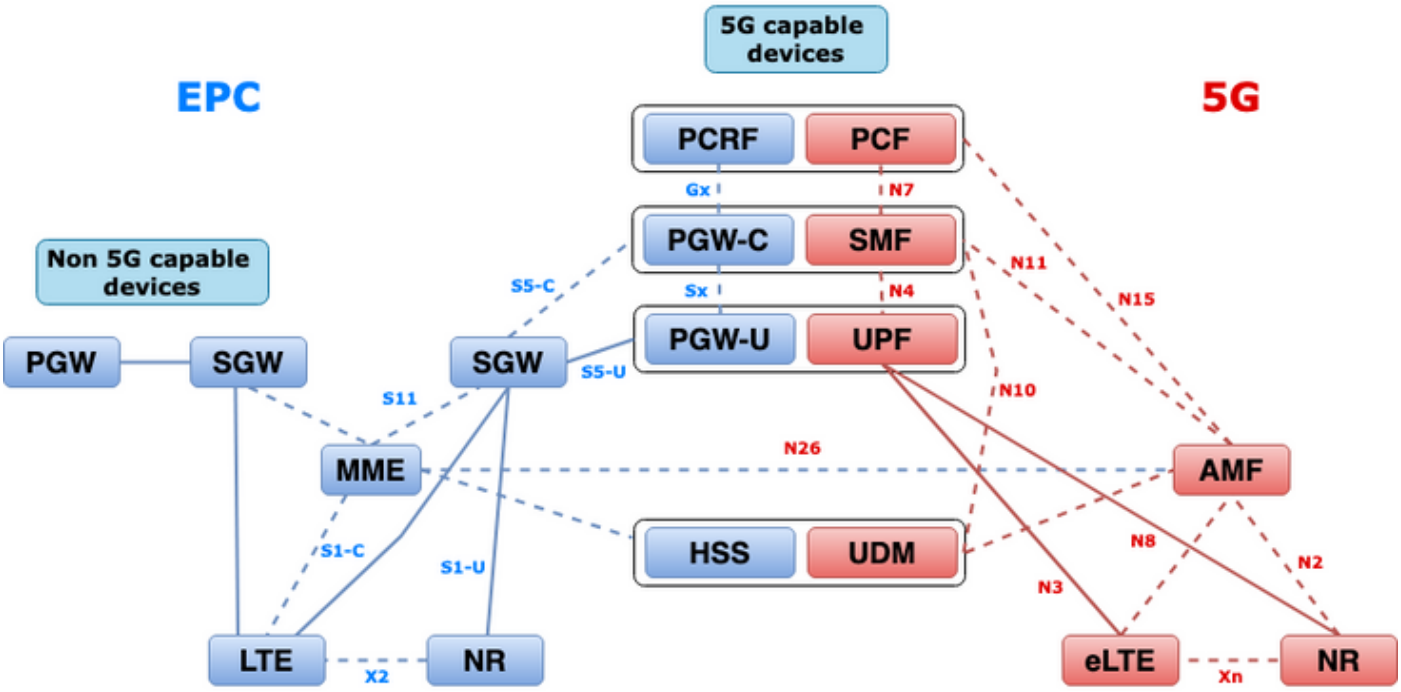
Troubleshoot Subscriber Issues on SMF/UPF

Contents

Introduction

This document describes CLI commands used for subscriber issues on SMF/UPF. Also, it includes Wireshark filters for 5G call flow analysis.

1. 4G/5G Internetwork Architecture



2. 5G Core (Service Based) Architecture

The Representational State Transfer (REST) architectural design model was adopted by 3GPP to support the communication between the distributed applications and functions on the 5G Core.

REST relies on standards protocols HTTP or HTTPS to transmit calls between entities, and within that leverages unique URL identifiers, either a verb or a noun. The specified HTTP methods or verbs for REST are as follows:

- GET: Retrieves the resource addressed by the URI within the request
- POST: Requests the server to create a new resource
- PUT: Replaces (completely) the resource addressed by the URI with the payload (JSON format) of the request
- PATCH: Updates a resource (partially)
- DELETE: Deletes the resource addressed by the URI in the request

Service Based Architecture (SBA): A system architecture in which system functionality is achieved by Network Functions (NFs). Provides services to authorized NFs who consume their services.

NF service: A NF service is one type of capability exposed by an NF (NF Service Producer) to other authorized NF (NF Service Consumer) through a service-based interface.

Service Based Interface (SBI): A service-based interface represents how the set of services is provided or exposed by a given NF. This is the interface where the NF service operations are invoked. Namf, Nsmf, Nudm, Nnrf, Nnssf, Nausf, Nnef, Nsmsf, and so on.

The Service Based Interfaces (SBI) use HTTP/2 protocol over TCP for communication between the NF Services as defined by 3GPP. TCP provides transport-level congestion control mechanisms as specified in IETF RFC 5681, which can be used for congestion control between two TCP endpoints (that is hop by hop). HTTP/2 also provides flow control mechanisms and limitations of stream concurrency, as specified in IETF RFC 7540, that can be configured for connection-level congestion control.

3. Uniform Resource Identifier

A 5G NF service can include multiple resources which can be accessed. A Uniform Resource Identifier (URI) is a string of characters that identify a particular resource.

- apiRoot is a concatenation of http:// or https://, coupled with an authority (host and optional port) and an optional deployment-specific string.
- apiName typically denotes the service invoked by the API.
- apiVersion is the version number of the API.
- apiSpecificResourceUriPart denotes the specific resource that the API is designed to access/manipulate.

4. Session Management Function (SMF)

The Cisco Session Management Function (SMF) is one of the Control Plane Network Functions (NF) of the 5G core network (5GC). The SMF is responsible for the session management with the supported individual functions on a per-session basis.

SMF supports session management (session establishment, modification, release), UE IP address allocation and management, DHCP functions, termination of NAS signaling related to session management, DL data notification, and traffic steering configuration for UPF for proper traffic routing. (AMF has part of the MME and PGW functionality from the EPC world).

5. User Plane Function

The User Plane Function (UPF) is one of the network functions (NFs) of the 5G core network (5GC). The UPF is responsible for packet routing and forwarding, packet inspection, QoS handling, and external PDU session for interconnecting Data Networks (DN), in the 5G architecture.

UPF is a distinct Virtual Network Function (VNF) that offers a high-performance forwarding engine for user traffic. With Vector Packet Processing (VPP) technology, the UPF achieves ultra-fast packet forwarding while retaining compatibility with all the user plane functionality.

6. SMF CLI Commands

6.1. Check if the Specific Subscriber is Attached

```
[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: If you have GEO Redundancy (GR) feature enabled, you need to check to which GR instance the subscriber is attached to.

6.2. Identify Peer IP Addresses, and their 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. Identify UPF IP Address

Get the UPF IP from “show subscriber namespace smf supi imsi-xxxxxxxxxxxxxxx”, and then filter this particular IP Address from the configuration to confirm the node-id:

```
[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 Filter DNN for a Specific Subscriber

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

6.5. Enable Monitor Subscriber

```
[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: Enter Ctrl+C to stop the capture.

7. UPF CLI commands

7.1. Identify Called for a Specific Subscriber

```
[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. Get Subscriber-Level Information (like ruledefs, 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**: For this example, we used 01317b22 as callid. However, you need to use the callid based on the output you get from step 7.1.

7.3. Enable Monitor Subscriber

```
[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: Enable the necessary options based on the subscriber issue (the most common are A, X, Y, 19, 26, 34, 35, and 37, 40, 88, 89 for VoLTE call plus verbosity 5). Enter Q to stop the monitor subscriber.

7.4. Get Slow path/vpp PCAPs for Specific Subscriber

```
[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: Monitor subscriber can be enabled with Option V in order to generate the slow path/vpp PCAPs. Download the slow path/vpp PCAPs from “dir /hd-raid/records/hexdump”.

8. Useful Filters on Wireshark per SBI Interface

8.1. NG Application Protocol (NGAP)

NG Application Protocol (NGAP) provides the control plane signaling between the NG-RAN node and the Access and Mobility Management Function (AMF). Here you have some useful Wireshark filters for NG Application Protocol:

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

8.2. NRF Interface

NF Repository function (NRF) supports service discovery function and maintains NF profile and available NF instances. (not present in the EPC world). Here you have some useful Wireshark filters for the NRF interface:

```
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 Registration/Subscription (N10 Interface)

Unified Data Management (UDM) supports the generation of Authentication and Key Agreement (AKA) credentials, user identification handling, access authorization, and subscription management. (part of HSS functionality from EPC world). Here you have some useful Wireshark filters for the N10 interface:

```
## 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 Interface)

Access and Mobility Management Function (AMF) supports termination of NAS signaling, NAS ciphering & integrity protection, registration management, connection management, mobility management, access authentication and authorization, and security context management. (AMF has part of the MME functionality from the EPC world). Here you have some useful Wireshark filters for the N11 interface:

```
## 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 Interface)

Policy Control Function (PCF) supports a unified policy framework, providing policy rules to CP functions, and access to subscription information for policy decisions in UDR. (PCF has part of the PCRF functionality from the EPC world) Authentication Server Function (AUSF) acts as an authentication server (part of HSS from the EPC world). Here you have some useful Wireshark filters for the N7 interface:

```
### 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 Interface)

Charging Function (CHF) is a 5G SA core network function, and it supports 3GPP Converged Charging System functionality. CHF supports online and offline charging feature for multiple services, including 5G and 4G core integration. Here you have some useful Wireshark filters for the N40 interface:

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

8.7. Additional Useful Filters like Code Errors, and 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**: Take into account that in order to visualize the HTTP2 protocol, you need to decode the port number accordingly on Wireshark from **Analyze**. Select **Decode** as an option.

```
Field      Value            Type             Default              Current

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

File Name	Proposed alt-text
diagram_internetworking.png	4G/5G Internetworking Architecture
uri.png	Uniform Resource Identifier