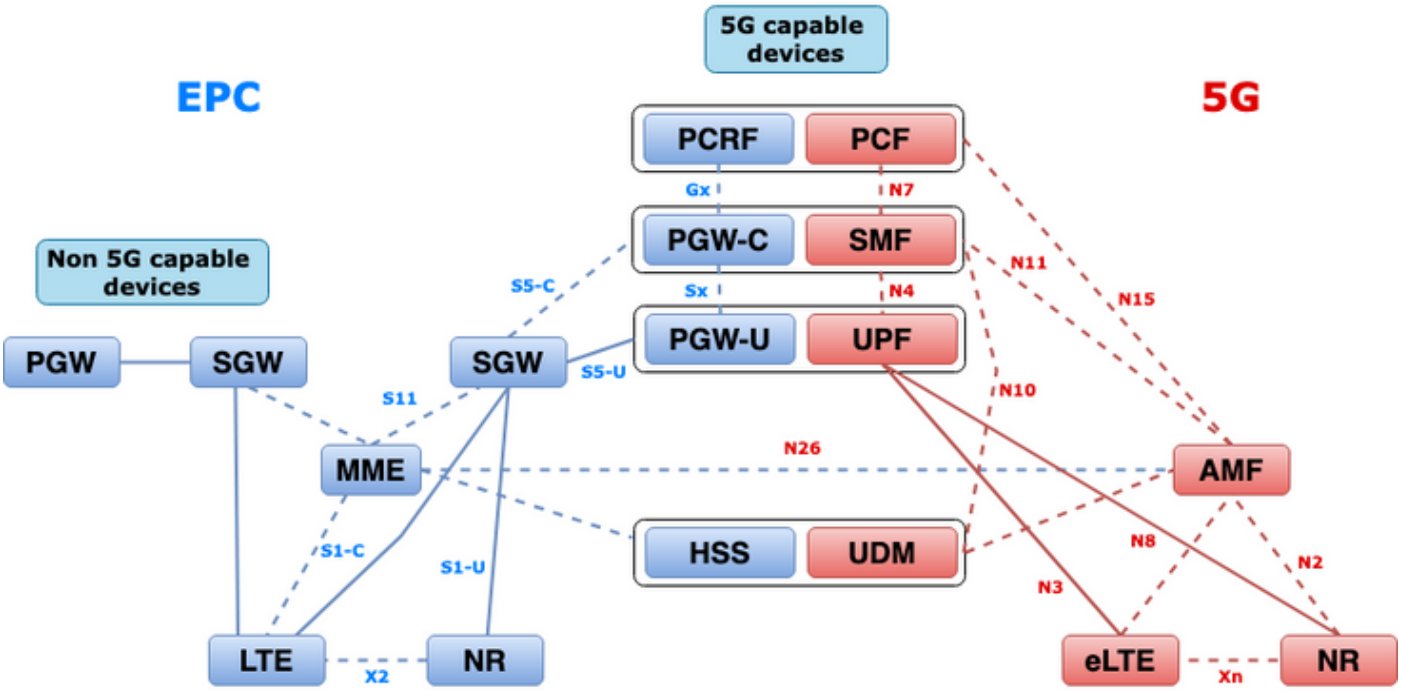
Risoluzione dei problemi del sottoscrittore su SMF/UPF

Sommario

Introduzione

Questo documento descrive i comandi CLI usati per i problemi dei sottoscrittori su SMF/UPF. Include anche filtri Wireshark per l'analisi del flusso di chiamata 5G.

1. Architettura di interrete 4G/5G



2. Architettura di base 5G (basata su servizi)

Il modello di progettazione architetturale REST (Representative State Transfer) è stato adottato da 3GPP per supportare la comunicazione tra le applicazioni e le funzioni distribuite sul 5G Core.

Il servizio REST si basa sui protocolli standard HTTP o HTTPS per trasmettere le chiamate tra entità e all'interno di tali protocolli utilizza identificatori URL univoci, sia verbi che sostantivi. Di seguito sono riportati i metodi o i verbi HTTP specificati per REST:

- SCARICA: Recupera la risorsa indirizzata dall'URI all'interno della richiesta
- POST: Richiede al server di creare una nuova risorsa
- PUT: Sostituisce (completamente) la risorsa indirizzata dall'URI con il payload (formato JSON) della richiesta
- PATCH: Aggiorna una risorsa (parzialmente)
- ELIMINA: Elimina la risorsa indirizzata dall'URI nella richiesta

SBA (Service Based Architecture): Architettura di sistema in cui la funzionalità di sistema viene realizzata dalle funzioni di rete (NF, Network Functions). Fornisce servizi a NF autorizzati che utilizzano i propri servizi.

Servizio NF: Un servizio NF è un tipo di funzionalità esposta da un NF (NF Service Producer) ad altri NF (NF Service Consumer) autorizzati tramite un'interfaccia basata su servizi.

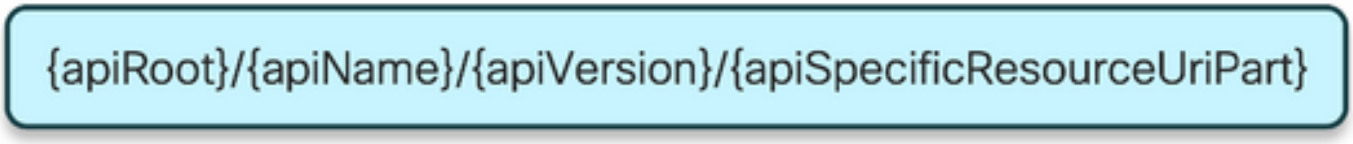
Service Based Interface (SBI): Un'interfaccia basata su servizi rappresenta il modo in cui l'insieme di servizi viene fornito o esposto da un determinato NF. Si tratta dell'interfaccia in cui vengono richiamate le operazioni del servizio NF. Namf, Nsmf, Nudm, Nnrf, Nnssf, Nausf, Nnef, Nsmsf e così via.

Le interfacce SBI (Service Based Interfaces) utilizzano il protocollo HTTP/2 su TCP per la comunicazione tra i servizi NF, come definito da 3GPP. Il protocollo TCP fornisce meccanismi di controllo della congestione a livello di trasporto, come specificato nella RFC 5681 dell'IETF, che possono essere utilizzati per il controllo della congestione tra due endpoint TCP (hop per hop).

HTTP/2 fornisce inoltre meccanismi di controllo del flusso e limitazioni della congestione del flusso, come specificato nella RFC 7540 dell'IETF, che può essere configurata per il controllo della congestione a livello di connessione.

3. Uniform Resource Identifier

Un servizio NF 5G può includere più risorse accessibili. Un URI (Uniform Resource Identifier) è una stringa di caratteri che identifica una particolare risorsa.



- apiRoot è una concatenazione di http:// o https://, associata a un'autorità (host e porta opzionale) e a una stringa opzionale specifica per la distribuzione.
- apiName in genere indica il servizio richiamato dall'API.
- apiVersion è il numero di versione dell'API.
- apiSpecificResourceUriPart indica la risorsa specifica a cui l'API è progettata per accedere/modificare.

4. Funzione di gestione delle sessioni (SMF)

La funzione SMF (Cisco Session Management Function) è una delle funzioni NF (Control Plane Network Functions) della rete principale 5G (5GC). L'SMF è responsabile della gestione delle sessioni con le singole funzioni supportate per ogni sessione.

SMF supporta la gestione delle sessioni (creazione delle sessioni, modifica, rilascio), l'allocazione e la gestione degli indirizzi IP UE, le funzioni DHCP, la terminazione della segnalazione NAS relativa alla gestione delle sessioni, la notifica dei dati DL e la configurazione della direzione del traffico per UPF per il routing del traffico corretto. (AMF fa parte delle funzionalità MME e PGW dell'EPC).

5. Funzione piano utente

La funzione User Plane (UPF) è una delle funzioni di rete (NF) della rete principale 5G (5GC). L'UPF è responsabile del routing e dell'inoltro dei pacchetti, dell'ispezione dei pacchetti, della gestione QoS e della sessione PDU esterna per l'interconnessione delle reti di dati (DN), nell'architettura 5G.

UPF è una funzione di rete virtuale (VNF, Virtual Network Function) distinta che offre un motore di inoltro ad alte prestazioni per il traffico degli utenti. Con la tecnologia Vector Packet Processing (VPP), l'UPF realizza l'inoltro ultra-rapido dei pacchetti mantenendo la compatibilità con tutte le funzionalità dell'aereo utente.

6. Comandi CLI di SMF

6.1. Verificare se il destinatario specifico è collegato

```
[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"
   ]
 ]
}
```

Nota: Se è abilitata la funzione di ridondanza geografica (GR), è necessario controllare a quale istanza GR è collegato il sottoscrittore.

6.2. Identificazione degli indirizzi IP peer e relativo stato

```
### 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. Identificazione dell'indirizzo IP UPF

Ottenere l'indirizzo IP UPF da "show subscriber namespace smf supi imsi-xxxxxxxxxxx", quindi filtrare questo particolare indirizzo IP dalla configurazione per confermare l'ID del nodo:

```
[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 Filtra DNN per un utente specifico

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

6.5. Abilita Sottoscrittore di monitoraggio

```
[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.
```

Nota: Immettere Ctrl+C per interrompere l'acquisizione.

7. Comandi UPF CLI

7.1. Identificare l'utente chiamato per un determinato utente

```
[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. Ottieni informazioni a livello di utente (ad esempio, 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
```

> **Nota:** In questo esempio è stato utilizzato 01317b22 come callid. Tuttavia, è necessario utilizzare il callid in base all'output ottenuto dal passaggio 7.1.

7.3. Abilita Sottoscrittore di monitoraggio

```
[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) ***
```

Nota: Abilitare le opzioni necessarie in base al problema dell'abbonato (le più comuni sono A, X, Y, 19, 26, 34, 35 e 37, 40, 88, 89 per la chiamata VoLTE più il livello di dettaglio 5). Immettere Q per arrestare il destinatario predefinito del monitoraggio.

7.4. Ottieni PCAP di percorso lento/vpp per un sottoscrittore specifico

```
[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
```

Nota: Il sottoscrittore di monitoraggio può essere abilitato con l'opzione V per generare i PCAP vpp e il percorso lento. Scaricare i PCAP vpp e slow path da dir /hd-raid/records/hexdump.

8. Filtri utili su Wireshark per interfaccia SBI

8.1. Protocollo di applicazione NG (NGAP)

Il protocollo NGAP (NG Application Protocol) fornisce la segnalazione del control plane tra il nodo NG-RAN e la funzione di gestione degli accessi e della mobilità (AMF). Di seguito sono riportati alcuni utili filtri Wireshark per il protocollo applicativo NG:

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

8.2. Interfaccia NRF

La funzione NF Repository (NRF) supporta la funzione Service Discovery e mantiene il profilo NF e le istanze NF disponibili. (non presente nel mondo dell'EPC). Di seguito sono riportati alcuni utili filtri Wireshark per l'interfaccia 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. Registrazione/sottoscrizione UDM (interfaccia N10)

Unified Data Management (UDM) supporta la generazione di credenziali di autenticazione e di accordo chiave (AKA), la gestione dell'identificazione utente, l'autorizzazione di accesso e la gestione delle sottoscrizioni. (parte della funzionalità HSS di EPC world). Ecco alcuni utili filtri Wireshark per l'interfaccia 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 (interfaccia N11)

La funzione di gestione degli accessi e della mobilità (AMF) supporta la terminazione della segnalazione NAS, la cifratura NAS e la protezione dell'integrità, la gestione della registrazione, la gestione delle connessioni, la gestione della mobilità, l'autenticazione e l'autorizzazione degli accessi e la gestione del contesto di sicurezza. (l'AMF fa parte delle funzionalità dell'MME dell'EPC). Ecco alcuni utili filtri Wireshark per l'interfaccia 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 (interfaccia N7)

La funzione PCF (Policy Control Function) supporta un quadro di regole unificato che fornisce regole di policy alle funzioni CP e l'accesso alle informazioni di sottoscrizione per le decisioni di policy in UDR (PCF fa parte della funzionalità PCRF del mondo EPC) La funzione AUSF (Authentication Server Function) funge da server di autenticazione (parte di HSS del mondo EPC). Di seguito sono riportati alcuni utili filtri Wireshark per l'interfaccia 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 (interfaccia N40)

La funzione di ricarica (CHF) è una funzione di rete di base 5G SA e supporta la funzionalità del sistema di ricarica convergente 3GPP. CHF supporta la funzione di ricarica online e offline per diversi servizi, tra cui l'integrazione di base 5G e 4G. Qui sono disponibili alcuni utili filtri Wireshark per l'interfaccia N40:

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

8.7. Filtri utili aggiuntivi come errori di codice 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
```

> **Nota:** Tenere presente che per visualizzare il protocollo HTTP2, è necessario decodificare il numero di porta di conseguenza su Wireshark da **Analyze**. Selezionare **Decodifica** come opzione.

```
Field      Value            Type             Default               Current

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

Nome file	Testo alternativo proposto
diagram_internetworking.png	Architettura di internetworking 4G/5G
uri.png	Uniform Resource Identifier