

SMF/UPF에서 가입자 문제 해결

목차

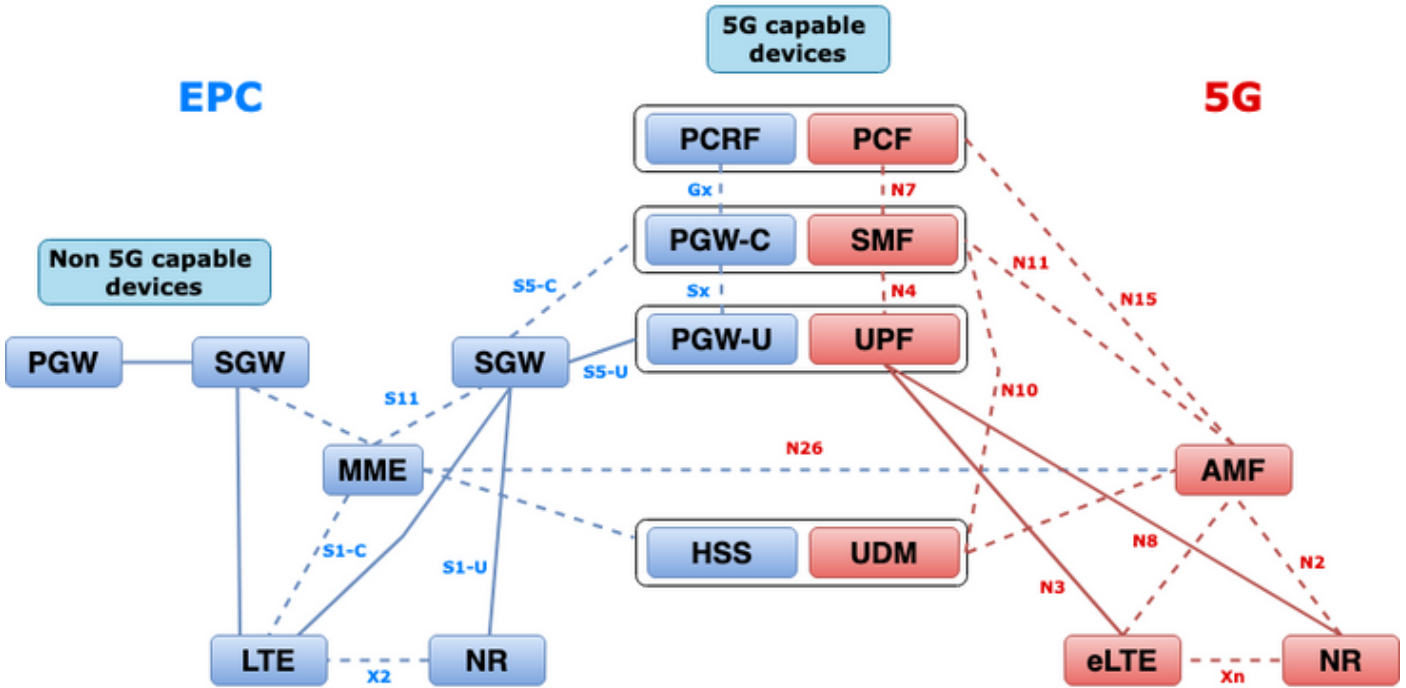
소개

1. 4G/5G 네트워크 간 아키텍처
2. 5G 코어(서비스 기반) 아키텍처
3. 균일 리소스 식별자
4. 세션 관리 기능(SMF)
5. 사용자 평면 기능
6. SMF CLI 명령
 - 6.1. 특정 가입자가 연결되어 있는지 확인
 - 6.2. 피어 IP 주소 및 상태 확인
 - 6.3. UPF IP 주소 식별
 - 6.4. 특정 가입자에 대한 DNN 필터링
 - 6.5. 모니터 가입자 활성화
7. UPF CLI 명령
 - 7.1. 특정 가입자에 대해 호출된 정보 확인
 - 7.2. 가입자 레벨 정보 가져오기(예: ruledefs, pdr, far, qer, urr)
 - 7.3. 모니터 가입자 활성화
 - 7.4. 특정 가입자에 대한 느린 경로/vpp PCAP 가져오기
8. SBI 인터페이스당 Wireshark의 유용한 필터
 - 8.1. NGAP(NG 애플리케이션 프로토콜)
 - 8.2. NRF 인터페이스
 - 8.3. UDM 등록/등록(N10 인터페이스)
 - 8.4. AMF(N11 인터페이스)
 - 8.5. PCF(N7 인터페이스)
 - 8.6. CHF(N40 인터페이스)
 - 8.7. 코드 오류 및 RST STREAM과 같은 추가적인 유용한 필터

소개

이 문서에서는 SMF/UPF의 가입자 문제에 사용되는 CLI 명령에 대해 설명합니다. 또한 5G 통화 흐름 분석을 위한 Wireshark 필터가 포함되어 있습니다.

1. 4G/5G 네트워크 간 아키텍처



2. 5G 코어(서비스 기반) 아키텍처

3GPP는 REST(Representational State Transfer) 아키텍처 설계 모델을 채택하여 5G 코어의 분산 애플리케이션과 기능 간의 통신을 지원합니다.

REST는 표준 프로토콜 HTTP 또는 HTTPS를 사용하여 엔티티 간에 통화를 전송하고, 이 프로토콜 내에서 동사나 명사 같은 고유한 URL 식별자를 활용합니다. REST에 대해 지정된 HTTP 메서드 또는 동사는 다음과 같습니다.

- 목표: 요청 내 URI에서 지정한 리소스를 검색합니다.
- POST: 서버에 새 리소스를 만들도록 요청
- PUT: URI가 지정한 리소스를 요청의 페이로드(JSON 형식)로 대체(전체)
- 패치: 리소스 업데이트(부분적으로)
- 삭제: 요청에서 URI가 지정한 리소스를 삭제합니다.

SBA(Service Based Architecture): NF(Network Functions)에서 시스템 기능을 구현하는 시스템 아키텍처. 서비스를 사용하는 공인 NF에게 서비스를 제공합니다.

NF 서비스: NF 서비스는 서비스 기반 인터페이스를 통해 NF(NF Service Producer)가 다른 인증된 NF(NF Service Consumer)에 노출하는 기능 중 하나입니다.

SBI(서비스 기반 인터페이스): 서비스 기반 인터페이스는 지정된 NF에서 서비스 집합을 제공하거나 노출하는 방법을 나타냅니다. NF 서비스 작업이 호출되는 인터페이스입니다. Namef, Nsmf, Ndmf, Nrf, Nssf, Nausf, Nnef, Nsmf 등

SBI(Service Based Interfaces)는 3GPP에 의해 정의된 대로 NF 서비스 간 통신에 TCP를 통한 HTTP/2 프로토콜을 사용합니다. TCP는 IETF RFC 5681에 지정된 대로 전송 레벨 혼잡 제어 메커니즘을 제공합니다. 이 메커니즘은 두 TCP 엔드포인트(흡별) 간 혼잡 제어에 사용할 수 있습니다. 또한 HTTP/2는 연결 수준 혼잡 제어를 위해 구성할 수 있는 IETF RFC 7540에 지정된 대로 스트림 동시연결의 제한 및 흐름 제어 메커니즘을 제공합니다.

3. 균일 리소스 식별자

5G NF 서비스에는 액세스할 수 있는 여러 리소스가 포함될 수 있습니다. URI(Uniform Resource Identifier)는 특정 리소스를 식별하는 문자 문자열입니다.

`{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}`

- apiRoot는 http:// 또는 https://의 연결로서 권한(호스트 및 선택적 포트) 및 선택적인 구축별 문자열을 결합합니다.
- apiName은 일반적으로 API에서 호출한 서비스를 나타냅니다.
- apiVersion은 API의 버전 번호입니다.
- apiSpecificResourceUriPart는 API가 액세스/조작하도록 설계된 특정 리소스를 나타냅니다.

4. 세션 관리 기능(SMF)

Cisco SMF(Session Management Function)는 5G 코어 네트워크(5GC)의 NF(Control Plane Network Functions) 중 하나입니다. SMF는 세션별로 지원되는 개별 기능을 사용하여 세션 관리를 담당합니다.

SMF는 적절한 트래픽 라우팅을 위해 세션 관리(세션 설정, 수정, 해제), UE IP 주소 할당 및 관리, DHCP 기능, 세션 관리와 관련된 NAS 신호 처리 종료, DL 데이터 알림, UPF를 위한 트래픽 조정 구성을 지원합니다. (AMF는 EPC 환경에서 MME 및 PGW 기능의 일부를 제공합니다.)

5. 사용자 평면 기능

UPF(User Plane Function)는 5G 코어 네트워크(5GC)의 네트워크 기능(NF) 중 하나입니다. UPF는 5G 아키텍처에서 DN(Data Networks)을 상호 연결하기 위한 패킷 라우팅 및 전달, 패킷 검사, QoS 처리, 외부 PDU 세션을 담당합니다.

UPF는 사용자 트래픽을 위한 고성능 포워딩 엔진을 제공하는 고유한 VNF(Virtual Network Function)입니다. VPP(Vector Packet Processing) 기술을 통해 UPF는 모든 사용자 평면 기능과의 호환성을 유지하면서 매우 빠른 패킷 포워딩을 실현합니다.

6. SMF CLI 명령

6.1. 특정 가입자가 연결되어 있는지 확인

```
[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"
]
]
}

```

참고: GR(GEO Redundancy) 기능이 활성화된 경우 가입자가 연결된 GR 인스턴스를 확인해야 합니다.

6.2. 피어 IP 주소 및 상태 확인

```

### 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 주소 식별

"show subscriber namespace smf supi imsi-xxxxxxxxxxxxx"에서 UPF IP를 가져온 다음 구성에서 이 특정 IP 주소를 필터링하여 node-id를 확인합니다.

```
[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 특정 가입자에 대한 DNN 필터링

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

6.5. 모니터 가입자 활성화

```
[smf/data] smf# monitor subscriber supi imsi-123969789012404 gr-instance 1 nf-service smf
capture-duration 3600 internal-messages yes
supi: imsi-123969789012404
captureDuration: 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.
```

참고: 캡처를 중지하려면 Ctrl+C를 입력합니다.

7. UPF CLI 명령

7.1. 특정 가입자에 대해 호출된 정보 확인

```
[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) - IPSP
| (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) - sl-mme
| (k) - PCC
| (X) - HSGW (n) - ePDG (t) - hnbgw-ue
| (m) - hnbgw-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
||
||
||
||

```

```

vvvvvvv 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. 가입자 레벨 정보 가져오기(예: 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

```

참고: 이 예제에서는 calid로 01317b22를 사용했습니다. 그러나 7.1단계에서 얻은 출력에 따라 called를 사용해야 합니다.

7.3. 모니터 가입자 활성화

```
[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 - All (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 - AllMGR      (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 - IPsec RADIUS (ON )  60 - CAP       (ON )
F - Packet Capture: (Full Pkt) 42 - ROHC        (OFF)  64 - LLC       (OFF)
/ - Priority         ( 0)      43 - WiMAX R6    (ON )  65 - SNDSCP    (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) ***

```

참고: 가입자 문제에 따라 필요한 옵션을 활성화합니다(가장 일반적인 옵션은 A, X, Y, 19, 26, 34, 35, 37, 40, 88, 89, for VoLTE call plus verbosity 5). 모니터 가입자를 중지하려면 Q를 입력합니다.

7.4. 특정 가입자에 대한 느린 경로/vpp PCAP 가져오기

```
[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 - All          (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 - AllMGR      (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 - IPsec RADIUS (ON )  60 - CAP          (ON )
F - Packet Capture: (Full Pkt) 42 - ROHC        (OFF)  64 - LLC          (OFF)
/ - Priority ( 0)            43 - WiMAX R6    (ON )  65 - SNDSCP       (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
```

참고: 느린 경로/vpp PCAP를 생성하려면 옵션 V를 사용하여 모니터 가입자를 활성화할 수 있습니다. "dir /hd-raid/records/hexdump"에서 느린 경로/vpp PCAP를 다운로드합니다.

8. SBI 인터페이스당 Wireshark의 유용한 필터

8.1 NGAP(NG 애플리케이션 프로토콜)

NGAP(NG Application Protocol)는 NG-RAN 노드와 AMF(Access and Mobility Management Function) 간의 컨트롤 플레인 신호를 제공합니다. NG 애플리케이션 프로토콜에 유용한 Wireshark 필터가 있습니다.

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

8.2. NRF 인터페이스

NF 저장소 기능(NRF)은 서비스 검색 기능을 지원하고 NF 프로필 및 사용 가능한 NF 인스턴스를 유지 관리합니다. (EPC 세계에는 없음) 다음은 NRF 인터페이스에 유용한 Wireshark 필터입니다.

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

8.3 UDM 등록/등록(N10 인터페이스)

UDM(Unified Data Management)은 AKA(Authentication and Key Agreement) 자격 증명 생성, 사용자 식별 처리, 액세스 권한 부여 및 구독 관리를 지원합니다. (EPC 환경에서 HSS 기능의 일부) 다음은 N10 인터페이스에 유용한 Wireshark 필터입니다.

```
## 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 인터페이스)

AMF(Access and Mobility Management Function)는 NAS 시그널링 종료, NAS 암호화 및 무결성 보호, 등록 관리, 연결 관리, 모빌리티 관리, 액세스 인증 및 권한 부여, 보안 컨텍스트 관리를 지원합니다. (AMF는 EPC 세계의 MME 기능에 포함되어 있습니다.) 다음은 N11 인터페이스에 유용한 Wireshark 필터입니다.

```
## 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-xxxxxxxxxxxxxxxx/assign-ebi"
http2.header.value == "/namf-comm/v1/ue-contexts/imsi-xxxxxxxxxxxxxxxx/n1-n2-messages"

```

8.5. PCF(N7 인터페이스)

PCF(Policy Control Function)는 통합 정책 프레임워크를 지원하며, CP 기능에 정책 규칙을 제공하고, UDR에서 정책 결정을 위한 등록 정보에 액세스합니다. PCF는 EPC(PCRF) 기능의 일부를 가집니다. AUSF(Authentication Server Function)는 인증 서버(EPC 세계에서 HSS의 일부) 역할을 합니다. 다음은 N7 인터페이스에 대한 몇 가지 유용한 Wireshark 필터입니다.

```

### 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-xxxxxxxxxxxxxxxx"

## 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 인터페이스)

CHF(Charging Function)는 5G SA 코어 네트워크 기능이며 3GPP 통합 충전 시스템 기능을 지원합니다. CHF는 5G 및 4G 코어 통합을 포함하여 여러 서비스에 대한 온라인 및 오프라인 충전 기능을 지원합니다. 다음은 N40 인터페이스에 유용한 Wireshark 필터입니다.

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

8.7. 코드 오류 및 RST_STREAM과 같은 추가적인 유용한 필터

```
## 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 == xxxxxxxxxxxxxxxxx

## 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
```

참고: HTTP2 프로토콜을 시각화하기 위해 Analyze(분석)의 Wireshark에 따라 포트 번호를 디코딩해야 한다는 점을 고려하십시오. 옵션으로 디코딩을 선택합니다.

Field	Value	Type	Default	Current
TCP port	<port_number>	Integer, base 10	none	HTTP2
파일 이름	다이어그램_인터넷워킹.png			제안된 대체 텍스트
uri.png				4G/5G 인터넷워킹 아키텍처
				균일 리소스 식별자