

5G 오픈소스 프로젝트 기반 테스트베드 구축 및 활용

2021. 06. 03.

1. 5G 오픈소스 프로젝트 필요성 및 활용

2. 5G 오픈소스 프로젝트 소개

- srsRAN
- Free5GC
- OpenAirInterface (OAI)
- Open5GS
- UERANSIM

3. 5G Stand Alone (SA) 테스트베드 구축 및 활용

- Open5GS + UERANSIM
- Radio Resource Control (RRC)
- Non Access Stratum (NAS)
- Protocol Data Unit (PDU)
- RRC State Transition

필요성

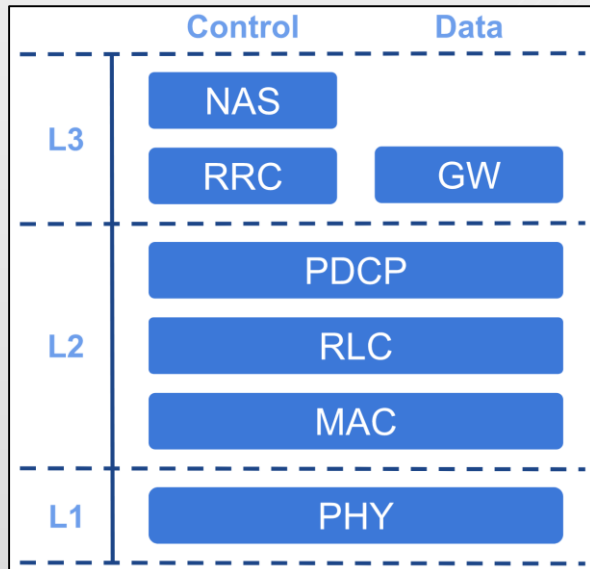
- 5G 보안 취약점 분석 및 검증을 위한 연구 환경 필요
- 5G 프로토콜 스택을 포함하는 상용 장비로 연구 환경을 구축하는 것은 많은 어려움이 수반됨
- 취약점 검증을 위해 코드 수정, 설정 변경 등이 자유로운 연구 환경 필요
- 5G 네트워크에서의 각종 데이터 수집을 위해 유연한 연구 환경 필요

활용

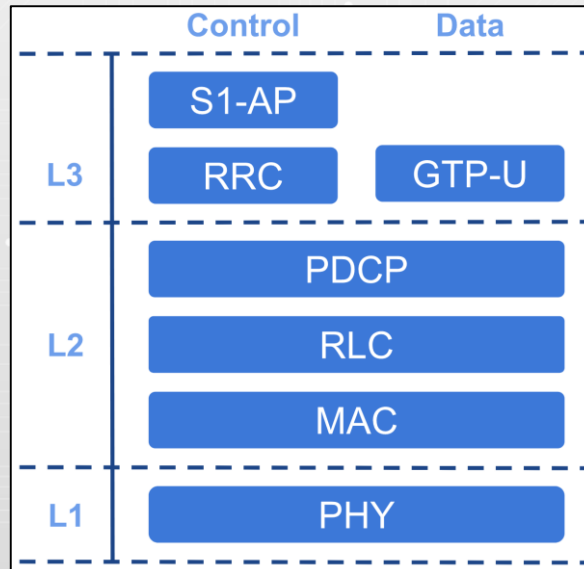
- RAN 구간 (UE \leftrightarrow gNB) 을 비롯하여 N2, N3 등의 인터페이스에 대한 5G 시그널링 및 사용자 데이터 수집
- Man in the Middle, Fake gNB 등의 상황을 구성하여 RAN 영역에서의 다양한 취약점 검증

srsRAN

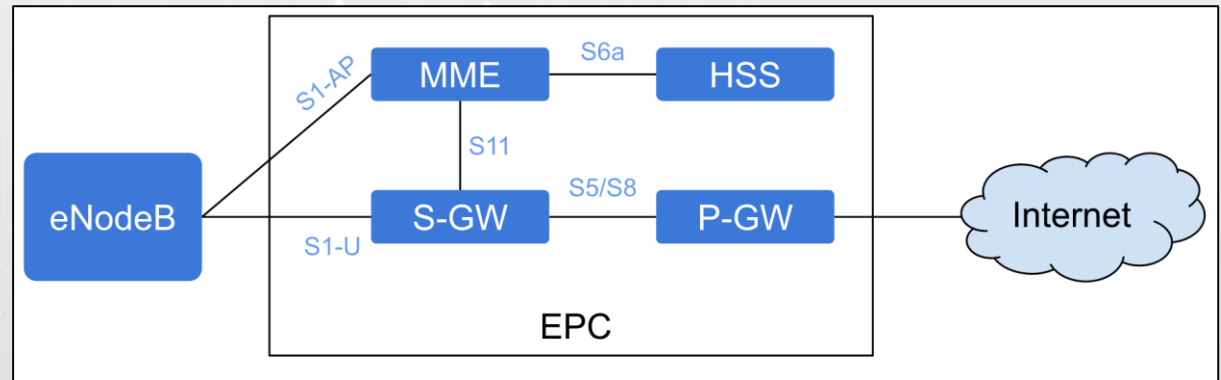
- Full-stack 5G NSA UE, Full-stack 4G eNodeB, Light-weight 4G EPC 지원
- 5G SA UE 향후 개발 예정
- 2021년 3분기에 5G NSA eNodeB/gNodeB 배포 예정
- srsUE는 PHY 레이어를 포함하기 때문에 SDR 장비를 이용하여 무선 신호 송수신 가능



<srsUE Architecture>

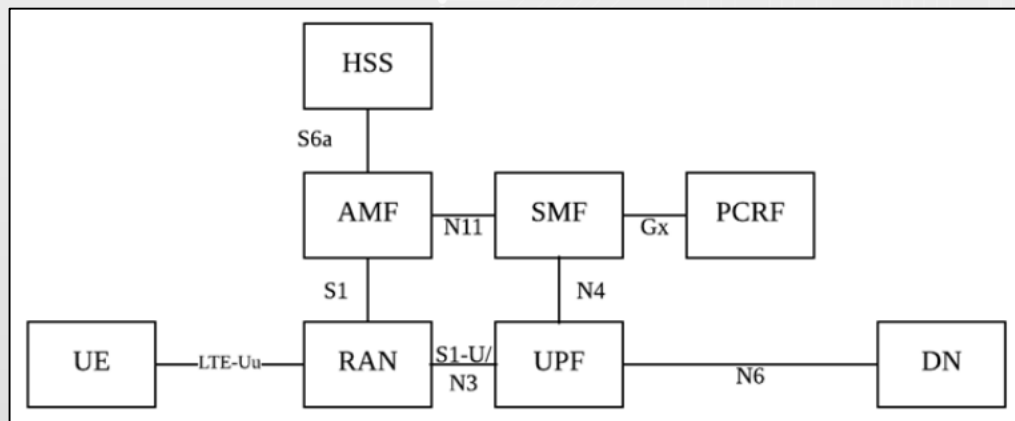


<eNodeB Architecture>

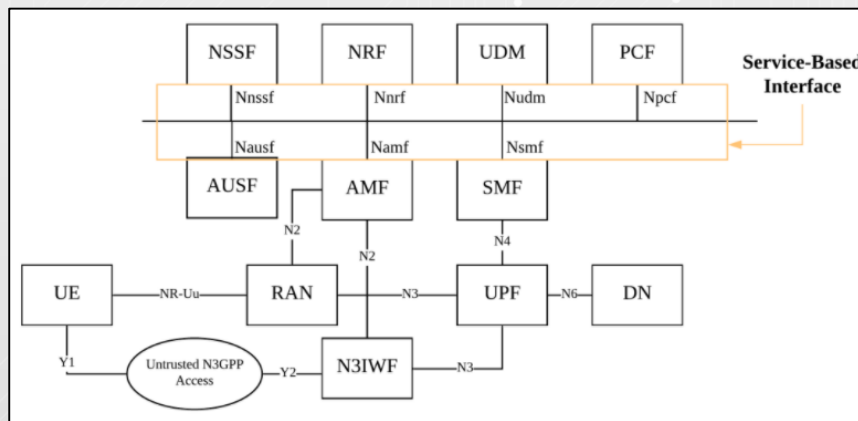


<EPC Architecture>

- 3GPP Release 15 기반의 5G Core 오픈소스 프로젝트
- 2019년 1월부터, 3단계의 로드맵을 거쳐 2020년 4월 Full operational 5G Core 배포
- 3단계 배포 이후에도 최근(2021년 2월)까지 꾸준히 기능 추가와 버그 패치 등이 이루어짐



<Stage 1 Architecture>



<Stage2 Architecture>

5G Orchestrator

+

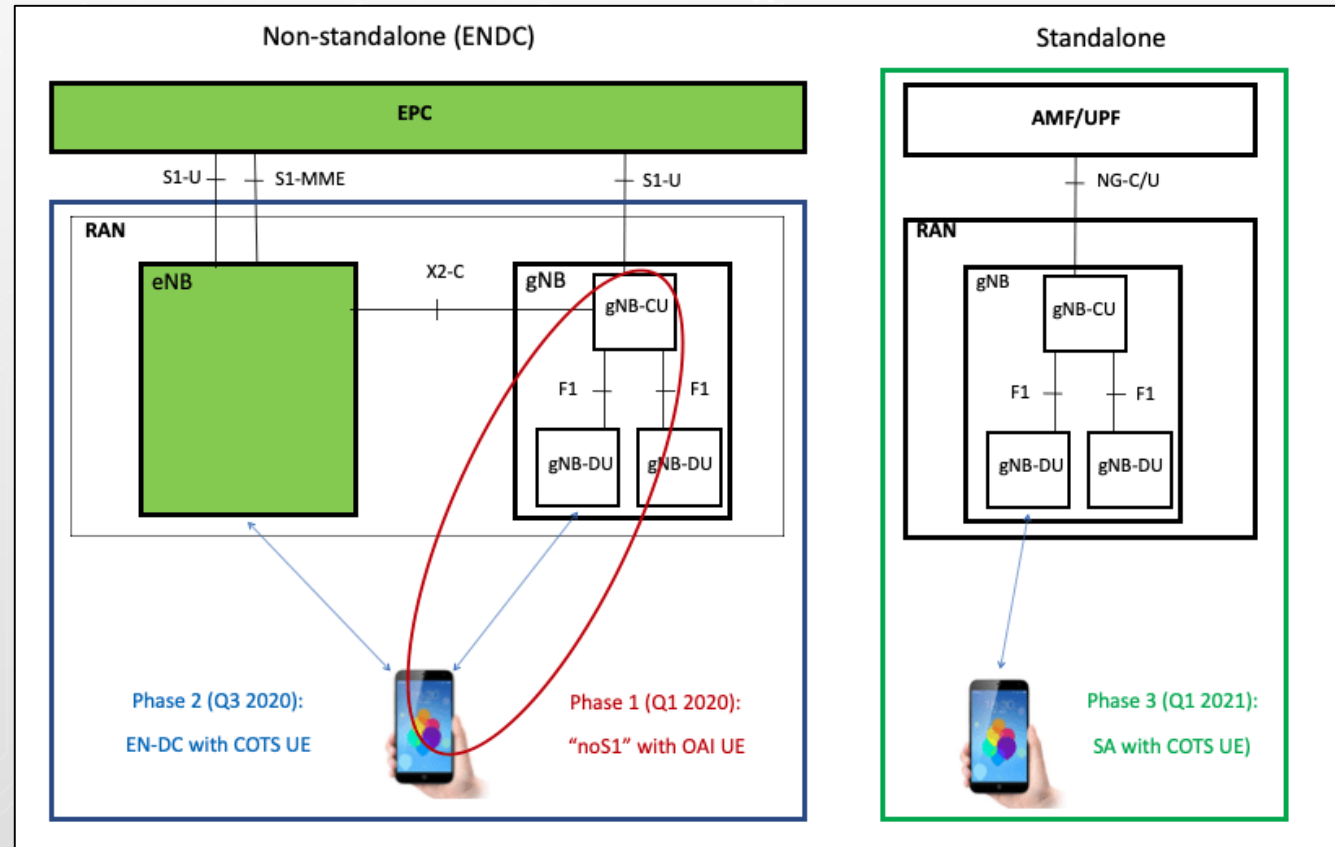
Non-mobile Access Network (N3IWF)

UP Link Classifier (ULCL)

<Stage3>

OpenAirInterface (OAI) – 5G RAN

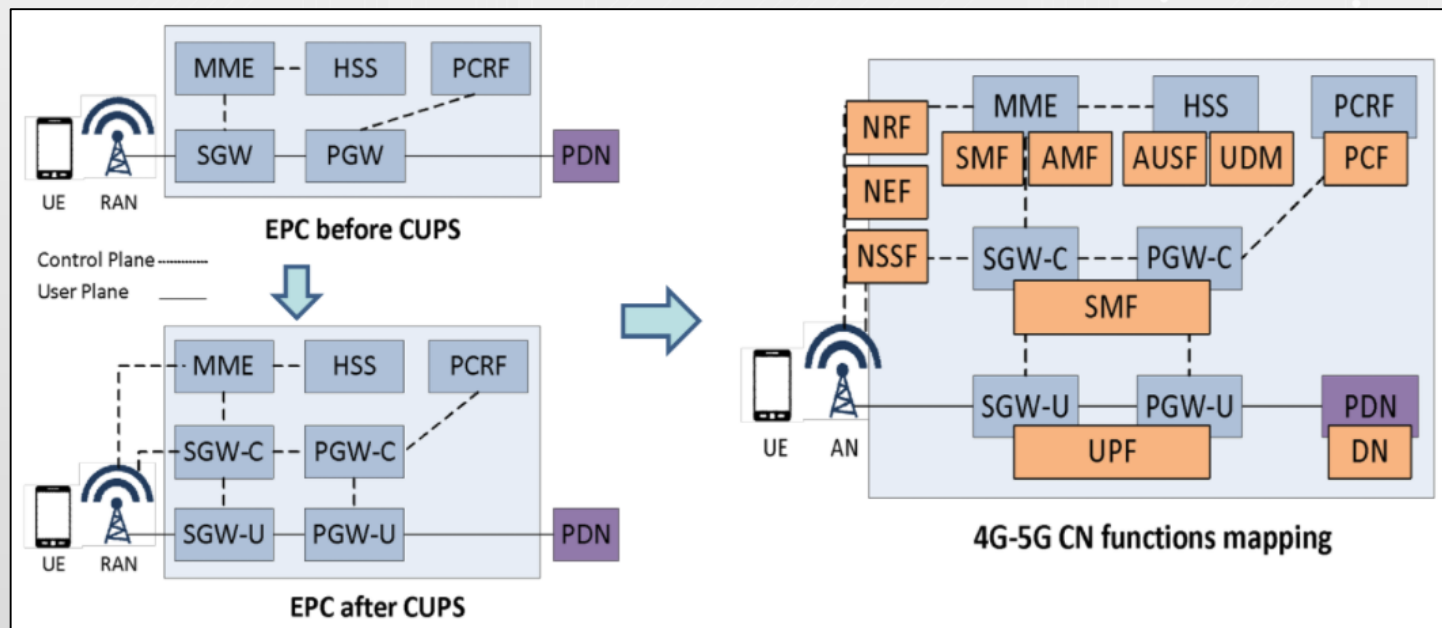
- 2020년 2단계의 개발을 통해 NSA RAN을 배포
- 2021년 중으로 SA RAN이 배포될 예정
 - Non Stand-Alone gNB software stack
 - Stand-Alone gNB software stack
 - 5G UE software stack
 - RAN Intelligent Controller (RIC) interfaces



<OAI RAN 개발 계획>

OpenAirInterface (OAI) – 5G CORE

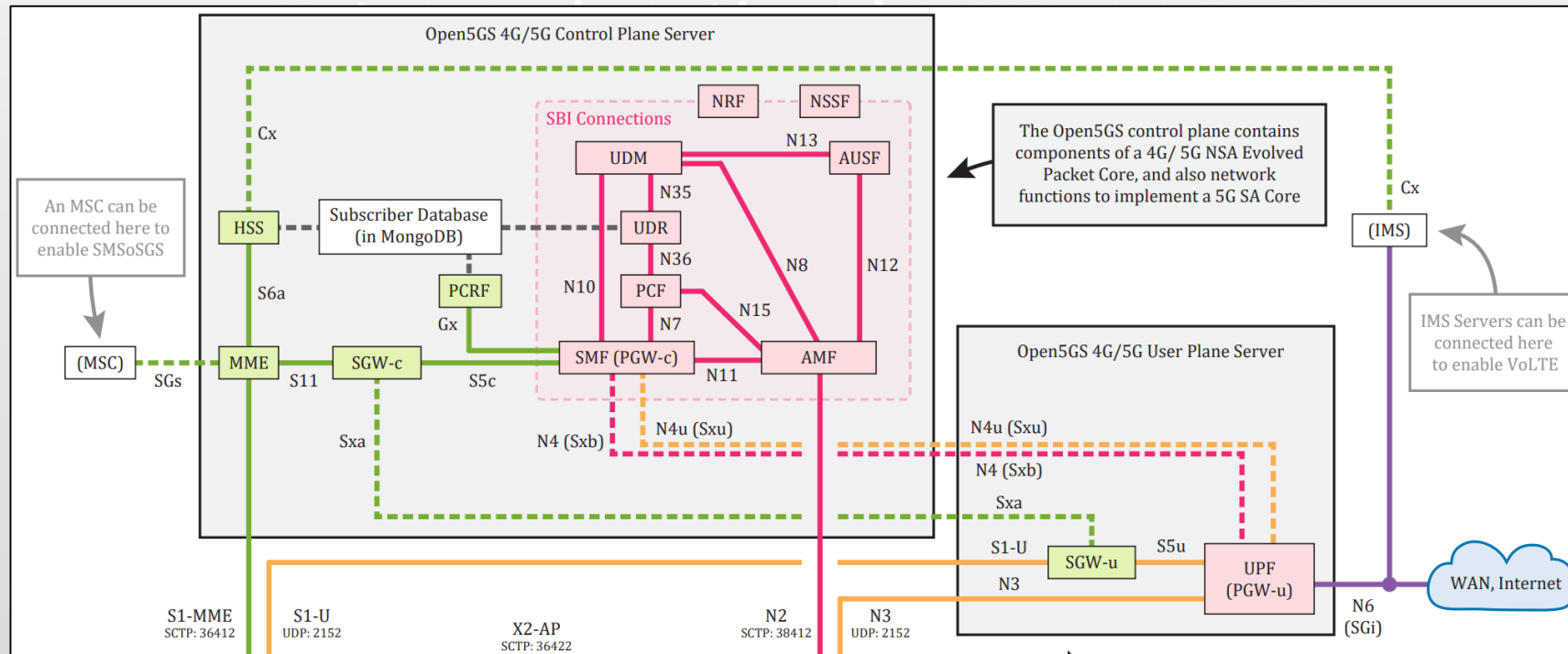
- 3단계의 개발 계획을 바탕으로 5G Core 오픈소스를 개발 중
- 1단계는 우분투에서 동작하는 docker 컨테이너 기반의 AMF, SMF, UPF를 개발 (완료)
- 2단계는 1단계에서 개발된 function들에 기능을 추가하고 UDM, AUSF 개발 예정
- 3단계는 Full SA 5G Core 개발 예정



<5G Core Architecture>

Open5GS

- 3GPP Release 16 기반의 5G Core 오픈소스 프로젝트이며 NSA와 SA를 모두 지원
- RAN 오픈소스 프로젝트(UERANSIM)와의 연동에 대한 튜토리얼 제공
- Ubuntu/CentOS/Fedora/FreeBSD/MacOSX 등 다양한 플랫폼에서의 빌드 매뉴얼 제공

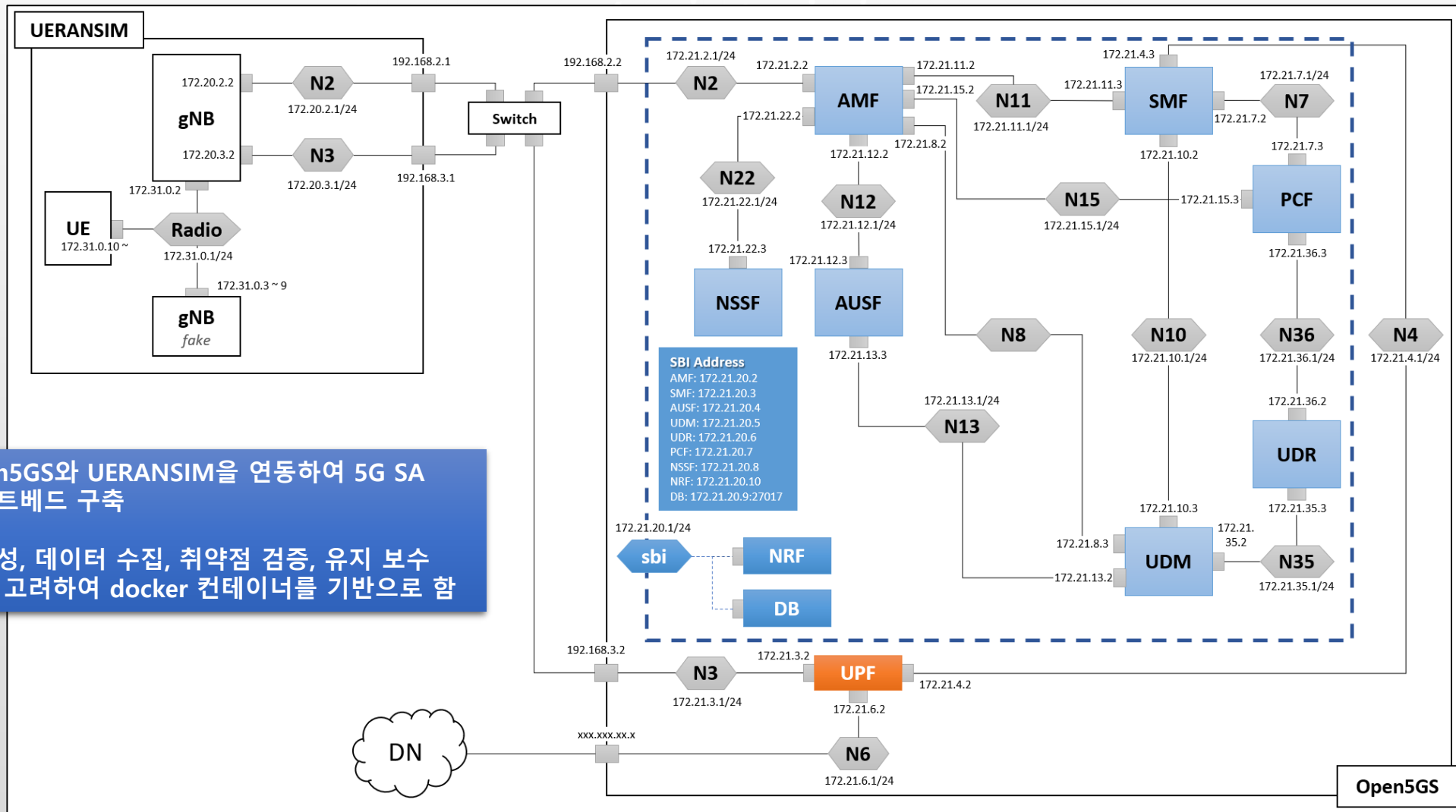


<Open5GS Architecture>

UERANSIM

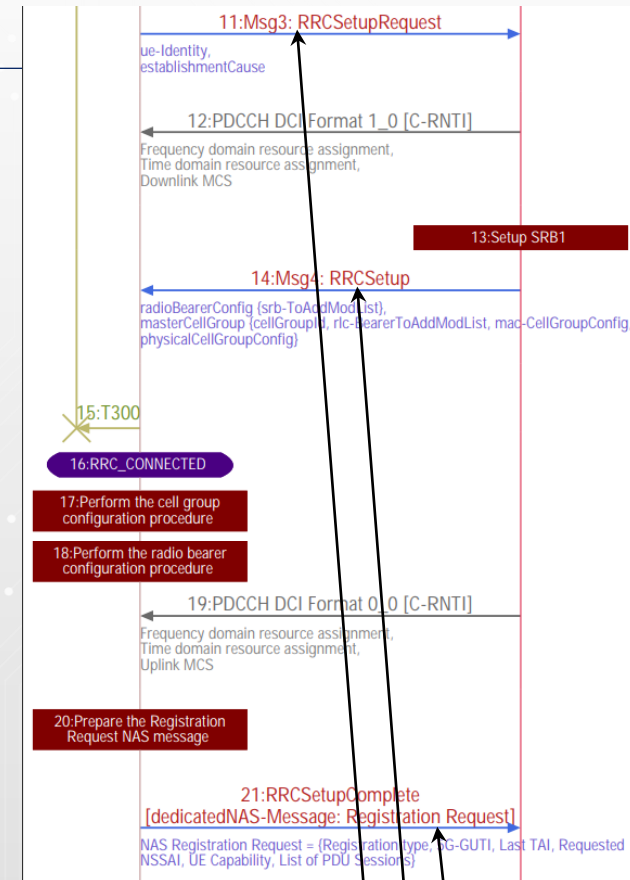
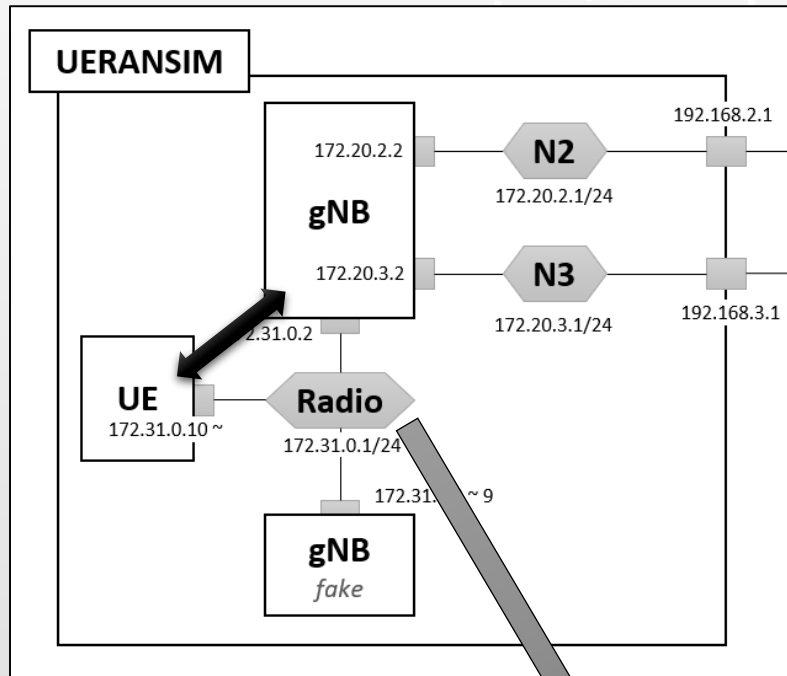
- 3GPP Release 15 기반의 5G RAN 오픈소스 프로젝트이며 SA를 지원
- gNB와 UE간의 인터페이스 뿐 아니라, gNB-AMF/gNB-UPF 인터페이스 지원
- RRC, NAS, NGAP 레이어의 기능들을 지원
- User Plane을 위한 GTP 프로토콜 지원
- deregistration/RRC release/paging/service request/PDU session 제어 등의 기능 지원
- 현재는 PHY 레이어를 제공하지 않기 때문에 SDR 하드웨어를 통한 RAN 구성은 불가능
- 5G Core 오픈소스 프로젝트인 Free5GC, Open5GS와의 연동 튜토리얼 제공

Open5GS + UERANSIM



I 5G Stand-Alone (SA) 테스트베드 구축 및 활용

Radio Resource Control (RRC)

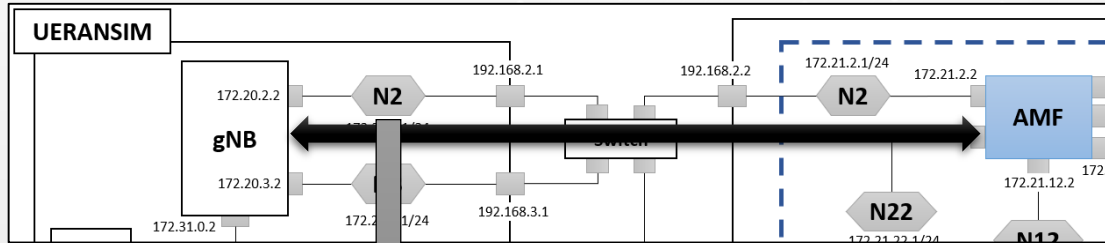


출처: <https://www.eventhelix.com/5g/standalone-access-registration/5g-standalone-access-registration.pdf>

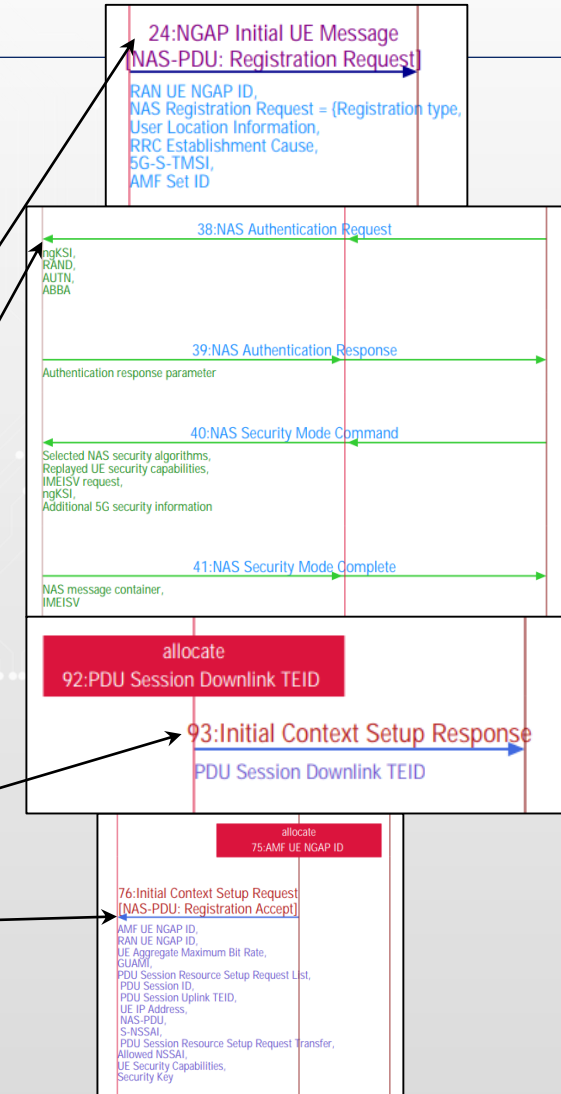
757	2.752515	172.31.0.10	172.31.0.2	NR RRC	74 RRC Setup Request
758	2.752743	172.31.0.2	172.31.0.10	NR RRC	73 RRC Setup
759	3.752989	172.31.0.10	172.31.0.2	NR RRC/NAS-5GS	97 RRC Setup Complete, Registration request

I 5G Stand-Alone (SA) 테스트베드 구축 및 활용

Non Access Stratum (NAS)



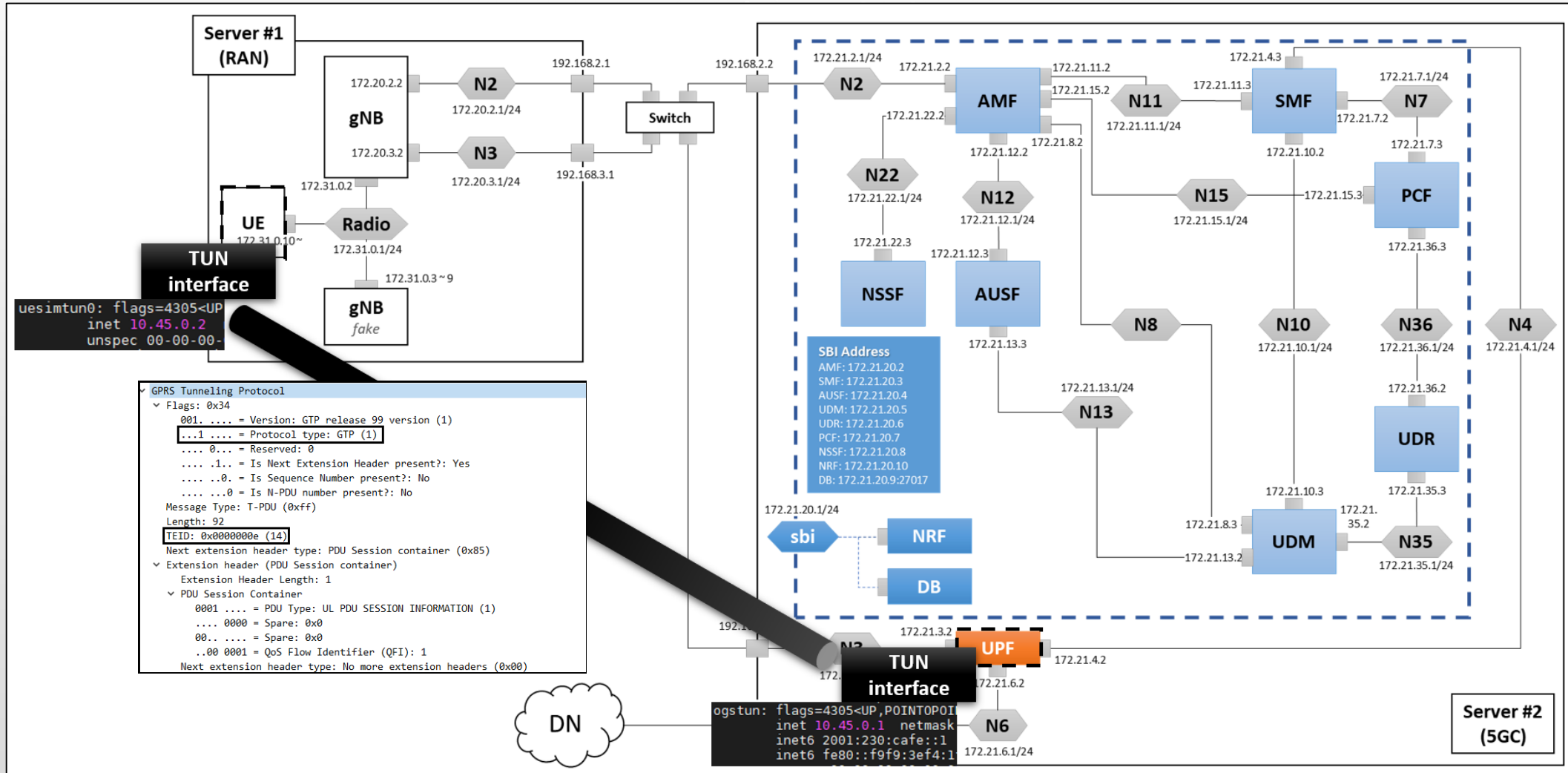
13	11.866056	172.20.2.2	192.168.2.2	NGAP/NAS-5GS	138 InitialUEMessage, Registration request
14	13.522708	192.168.2.2	172.20.2.2	SCTP	98 HEARTBEAT
15	13.522759	172.20.2.2	192.168.2.2	SCTP	98 HEARTBEAT_ACK
16	13.875268	192.168.2.2	172.20.2.2	NGAP/NAS-5GS	146 DownlinkNASTransport, Authentication request
17	14.076187	172.20.2.2	192.168.2.2	SCTP	62 SACK
18	14.876560	172.20.2.2	192.168.2.2	NGAP/NAS-5GS	130 UplinkNASTransport, Authentication response
19	16.883078	192.168.2.2	172.20.2.2	NGAP/NAS-5GS	126 DownlinkNASTransport, Security mode command
20	17.084190	172.20.2.2	192.168.2.2	SCTP	62 SACK
21	17.884484	172.20.2.2	192.168.2.2	NGAP/NAS-5GS	174 UplinkNASTransport
22	19.900086	192.168.2.2	172.20.2.2	NGAP/NAS-5GS	234 InitialContextSetupRequest
23	19.900523	172.20.2.2	192.168.2.2	NGAP	98 InitialContextSetupResponse
24	22.102712	192.168.2.2	172.20.2.2	SCTP	62 SACK
25	22.102782	172.20.2.2	192.168.2.2	NGAP/NAS-5GS	242 UplinkNASTransport
26	24.103777	192.168.2.2	172.20.2.2	NGAP/NAS-5GS	142 DownlinkNASTransport
27	24.119369	192.168.2.2	172.20.2.2	NGAP/NAS-5GS	250 PDUSessionResourceSetupRequest
28	24.119433	172.20.2.2	192.168.2.2	SCTP	62 SACK
29	24.126451	172.20.2.2	192.168.2.2	NGAP	102 PDUSessionResourceSetupResponse
30	26.330676	192.168.2.2	172.20.2.2	SCTP	62 SACK



출처: <https://www.eventhelix.com/5g/standalone-access-registration/5g-standalone-access-registration.pdf>

I 5G Stand-Alone (SA) 테스트베드 구축 및 활용

Protocol Data Unit (PDU)



I 5G Stand-Alone (SA) 테스트베드 구축 및 활용

Protocol Data Unit (PDU)

ping in UE (ICMP)

```
# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=36.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=36.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=36.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=36.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=111 time=35.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=111 time=36.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=111 time=35.9 ms
```

TUN interface in UE (ICMP)

```
root@3d1cc3fd6a5e:/# tcpdump -i uesimtun0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on uesimtun0, link-type RAW (Raw IP), capture size 262144 bytes
09:33:39.419107 IP 10.45.0.2 > 8.8.8.8: ICMP echo request, id 84, seq 72, length 64
09:33:39.455054 IP 8.8.8.8 > 10.45.0.2: ICMP echo reply, id 84, seq 72, length 64
09:33:40.420307 IP 10.45.0.2 > 8.8.8.8: ICMP echo request, id 84, seq 73, length 64
09:33:40.456312 IP 8.8.8.8 > 10.45.0.2: ICMP echo reply, id 84, seq 73, length 64
09:33:41.421524 IP 10.45.0.2 > 8.8.8.8: ICMP echo request, id 84, seq 74, length 64
09:33:41.457479 IP 8.8.8.8 > 10.45.0.2: ICMP echo reply, id 84, seq 74, length 64
09:33:42.422687 IP 10.45.0.2 > 8.8.8.8: ICMP echo request, id 84, seq 75, length 64
09:33:42.458667 IP 8.8.8.8 > 10.45.0.2: ICMP echo reply, id 84, seq 75, length 64
```

N3 Interface (UDP)

```
# tcpdump -i n3_link
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on n3_link, link-type EN10MB (Ethernet), capture size 262144 bytes
18:35:34.564849 IP 192.168.3.1.2152 > 172.21.3.2.2152: UDP, length 100
18:35:34.599392 IP 172.21.3.2.48046 > 192.168.3.1.2152: UDP, length 100
18:35:35.566886 IP 192.168.3.1.2152 > 172.21.3.2.2152: UDP, length 100
18:35:35.601402 IP 172.21.3.2.48046 > 192.168.3.1.2152: UDP, length 100
18:35:36.567952 IP 192.168.3.1.2152 > 172.21.3.2.2152: UDP, length 100
18:35:36.602521 IP 172.21.3.2.48046 > 192.168.3.1.2152: UDP, length 100
```

TUN interface in UPF (ICMP)

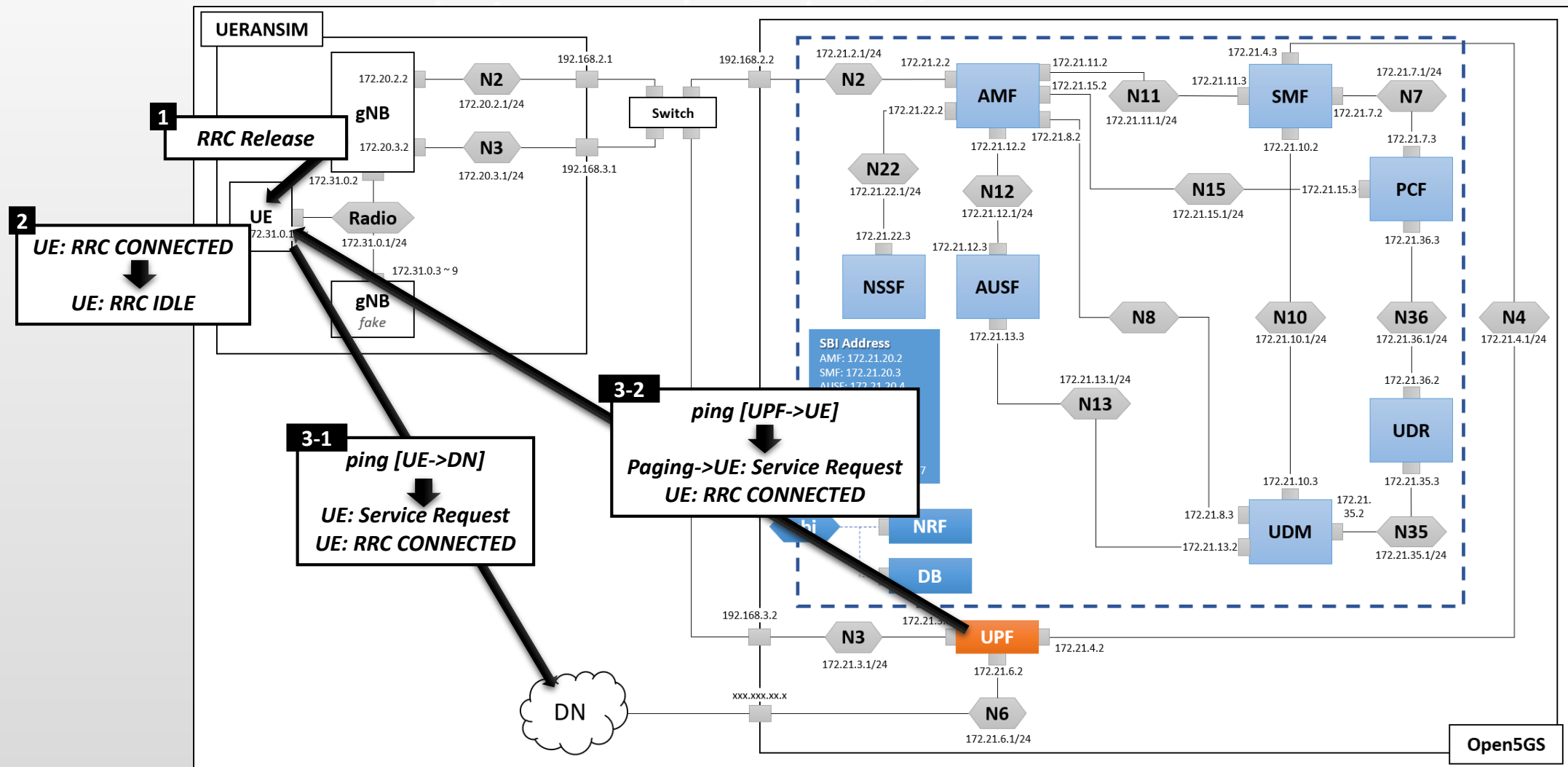
```
root@3f456c431386:~/upf# tcpdump -i ogstun -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ogstun, link-type RAW (Raw IP), capture size 262144 bytes
09:38:06.772817 IP 10.45.0.2 > 8.8.8.8: ICMP echo request, id 84, seq 339, length 64
09:38:06.807100 IP 8.8.8.8 > 10.45.0.2: ICMP echo reply, id 84, seq 339, length 64
09:38:07.774848 IP 10.45.0.2 > 8.8.8.8: ICMP echo request, id 84, seq 340, length 64
09:38:07.809090 IP 8.8.8.8 > 10.45.0.2: ICMP echo reply, id 84, seq 340, length 64
09:38:08.776811 IP 10.45.0.2 > 8.8.8.8: ICMP echo request, id 84, seq 341, length 64
09:38:08.811025 IP 8.8.8.8 > 10.45.0.2: ICMP echo reply, id 84, seq 341, length 64
```

N6 Interface (ICMP)

```
# tcpdump -i n6_link -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on n6_link, link-type EN10MB (Ethernet), capture size 262144 bytes
18:42:03.583144 IP 172.21.6.2 > 8.8.8.8: ICMP echo request, id 98, seq 19, length 64
18:42:03.617307 IP 8.8.8.8 > 172.21.6.2: ICMP echo reply, id 98, seq 19, length 64
18:42:04.584299 IP 172.21.6.2 > 8.8.8.8: ICMP echo request, id 98, seq 20, length 64
18:42:04.618545 IP 8.8.8.8 > 172.21.6.2: ICMP echo reply, id 98, seq 20, length 64
18:42:05.585471 IP 172.21.6.2 > 8.8.8.8: ICMP echo request, id 98, seq 21, length 64
18:42:05.619662 IP 8.8.8.8 > 172.21.6.2: ICMP echo reply, id 98, seq 21, length 64
```

I 5G Stand-Alone (SA) 테스트베드 구축 및 활용

RRC State Transition



감사합니다

National AI Research Institute - Making a Better Tomorrow

ETRI

한국 전자통신연구원