Exploring gnb_zmq_ngap.pcap

gNB | AMF

📁 **gnb_zmq_ngap.pcap**

🤝 NGSetupRequest

🌍 PLMN	00f110
📡 gNB-Name	srsgnb01
🌍 PLMN	00f110

💡 [Frame 1] NGAP NG Setup — gNB and AMF exchange supported PLMN/TAI/slices over the N2 interface after the transport association comes up

✅ NGSetupResponse

📍 AMF-Name	open5gs-amf0
AMF-Capacity	255

💡 [Frame 2] NGAP NG Setup — gNB and AMF exchange supported PLMN/TAI/slices over the N2 interface after the transport association comes up

🤝 InitialUEMessage, Registration request

🆔 RAN-UE-ID	0
📋 RegType	initial registration
🆔 MSIN	9123456799
📡 RRCEstablishmentCause	mo-Signalling

💡 [Frame 3] 5GMM Registration Request — UE starts 5G registration via gNB; AMF receives SUCI/5G-GUTI and requested NSSAI, then selects AUSF/UDM to authenticate the subscriber

🔐 DownlinkNASTransport, Authentication request

🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0

💡 [Frame 4] 5G-AKA/EAP-AKA' Challenge — AMF (via AUSF) delivers authentication vector to the UE; UE returns RES* to prove knowledge of the long-term key K

🔑 UplinkNASTransport, Authentication response

🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0

💡 [Frame 5] 5G-AKA Response — UE returns RES* computed from RAND/AUTN; AUSF compares it to HXRES* to confirm the UE knows the long-term key and finishes primary authentication

🔐 DownlinkNASTransport, Security mode command

🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0
🔐 Cipher	5G-EA0 (null ciphering algorithm)
🔐 Integrity	128-5G-IA2

💡 [Frame 6] NAS Security Mode Command — AMF selects 5G-NEA/5G-NIA ciphering and integrity algorithms and activates NAS security using keys derived from KAMF

🤝 InitialUEMessage, Registration request

🆔 RAN-UE-ID	0
📋 RegType	initial registration
🆔 MSIN	9123456799

💡 [Frame 7] 5GMM Registration Request — UE starts 5G registration via gNB; AMF receives SUCI/5G-GUTI and requested NSSAI, then selects AUSF/UDM to authenticate the subscriber

✅ DownlinkNASTransport, Registration accept

🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0

💡 [Frame 8] 5GMM Registration Accept — AMF confirms registration and assigns 5G-GUTI, allowed NSSAI and configured NSSAI to the UE

✅ InitialContextSetupResponse

🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0

💡 [Frame 9] NGAP Initial Context Setup — AMF instructs gNB to establish the UE's AS security context and radio bearers; security keys and UE capabilities are delivered after successful NAS authentication

✅ UplinkNASTransport, Registration complete

🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0

💡 [Frame 10] 5GMM Registration Complete — UE acknowledges the new 5G-GUTI assignment, concluding the registration procedure on the NAS layer

🎬 UplinkNASTransport, PDU session establishment request

🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0

💡 [Frame 11] 5GSM PDU Session Establishment Request — UE asks SMF (via AMF) for a PDU session to a DNN; SMF selects UPF and allocates UE IP and N4 tunnels

🔒⬇️ DownlinkNASTransport (ciphered)

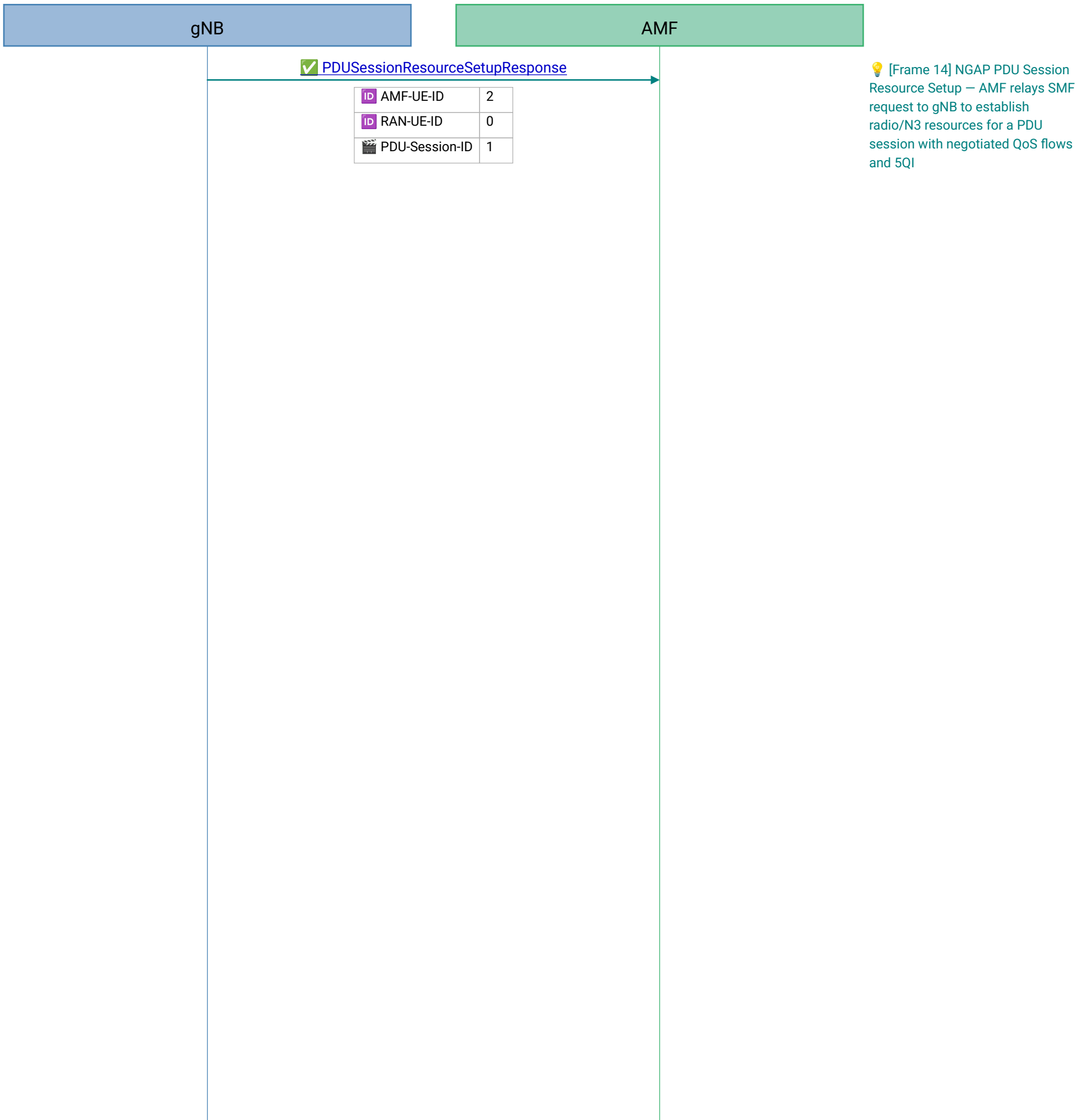
🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0
🛡️ Sec	Integrity protected and ciphered
🔏 MAC	0x1ae973b1
🔢 Seq	2
🛡️ Sec	Plain NAS message, not security protected

💡 [Frame 12] NGAP Downlink NAS Transport — AMF sends a NAS PDU to the UE via gNB over N2 (e.g. Authentication Request, Security Mode Command, Registration Accept). After Security Mode Complete, NAS messages are ciphered and the inner message type is opaque to the dissector — the security header, MAC and sequence number are still visible

✅ DownlinkNASTransport, PDU session establishment accept

🆔 AMF-UE-ID	2
🆔 RAN-UE-ID	0
🎬 PDU-Session-ID	1

💡 [Frame 13] 5GSM PDU Session Establishment Accept — SMF assigns UE IP, QoS rules, and S-NSSAI; user plane via UPF is ready so the UE can send data on this DNN


gNB
AMF
✅ PDUSessionResourceSetupResponse
ID AMF-UE-ID 2
ID RAN-UE-ID 0
PDU-Session-ID 1
💡 [Frame 14] NGAP PDU Session Resource Setup — AMF relays SMF request to gNB to establish radio/N3 resources for a PDU session with negotiated QoS flows and 5QI