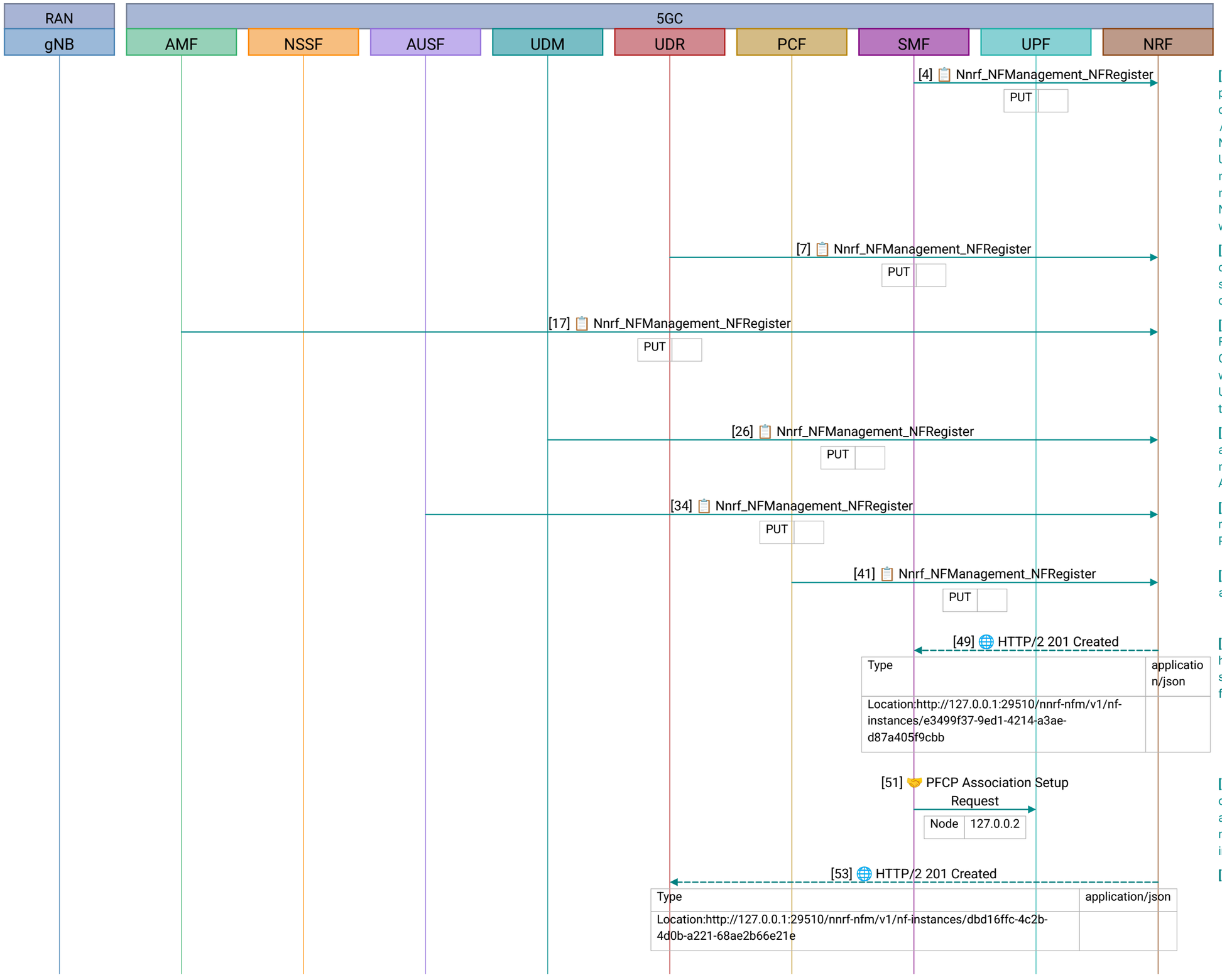
5g-core-registration-pdu-session.annotated



[Frame 4] Phase 1 - core bootstrap. The SMF registers its profile with the NRF (Network Repository Function), the core's directory. PUT `/nnrf-nfm/v1/nf-instances/{id}` is Nnrf_NFManagement_NFRegister: the NF picks its own UUID (`e3499f37-...`) and publishes its services (`nsmf-pdusession`, `nsmf-event-exposure`, `nsmf-oam`) and the slices and DNNs (Data Network Names) it serves: S-NSSAI `1/010203` and `1/112233`, each with DNNs `internet` and `iijmobile.biz`.

[Frame 7] The UDR (Unified Data Repository), the subscriber database, registers as `dbd16ffc-...` with the single service `nudr-dr`. It never calls anyone; every arrow into it comes from the UDM or the PCF.

[Frame 17] The AMF (Access and Mobility Management Function) registers as `7f4ddbaa-...`. Its profile lists two GUAMIs (Globally Unique AMF Identifiers): PLMN 460/00 with AMF ID `cafe00`, and 460/11 with `cafe11`. Keep this UUID in mind: the SMF asks for it by name in frame 775, and the AMF deletes it at shutdown.

[Frame 26] The UDM (Unified Data Management) registers as `688e8bec-...` with five services. Three are used later: `nudm-ueau` (authentication vectors), `nudm-uecm` (which AMF serves the UE) and `nudm-sdm` (subscription data).

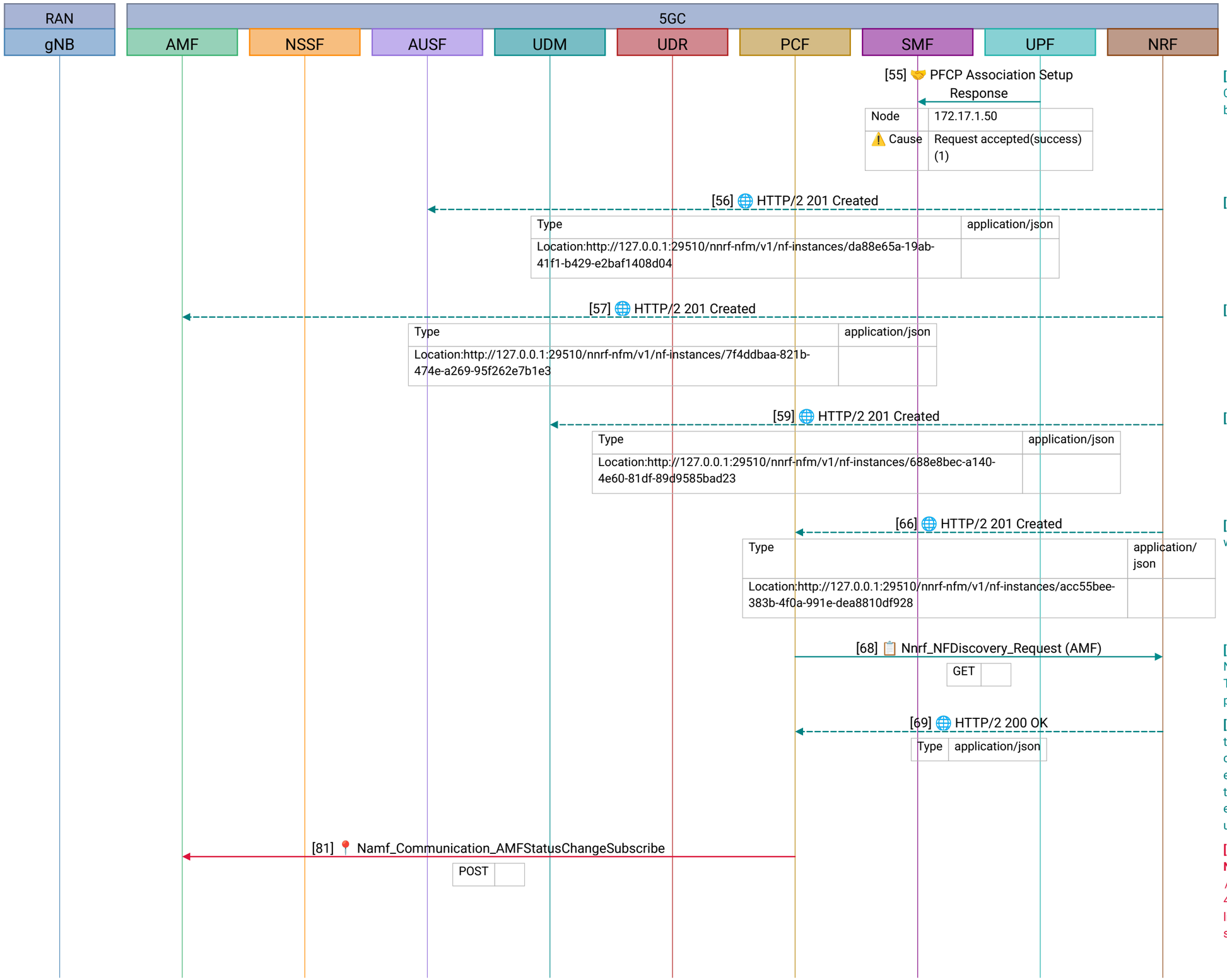
[Frame 34] The AUSF (Authentication Server Function) registers as `da88e65a-...` with `nausf-auth`, serving PLMNs 460/00 and 460/11.

[Frame 41] The PCF (Policy Control Function) registers as `acc55bee-...` with its policy services.

[Frame 49] `201 Created` for the SMF. The `Location` header echoes the profile's URI. The six registrations run on six separate TCP connections, so their answers interleave freely.

[Frame 51] N4 association. The SMF (node ID `127.0.0.2`) opens a PFCP (Packet Forwarding Control Protocol) association with the UPF (User Plane Function). This is node-level, done once; every later per-UE PFCP session rides inside it.

[Frame 53] `201 Created` for the UDR.



[Frame 55] The UPF (node ID `172.17.1.50`) accepts: `Cause: Request accepted`. The N4 control channel is up before any subscriber exists.

[Frame 56] `201 Created` for the AUSF.

[Frame 57] `201 Created` for the AMF.

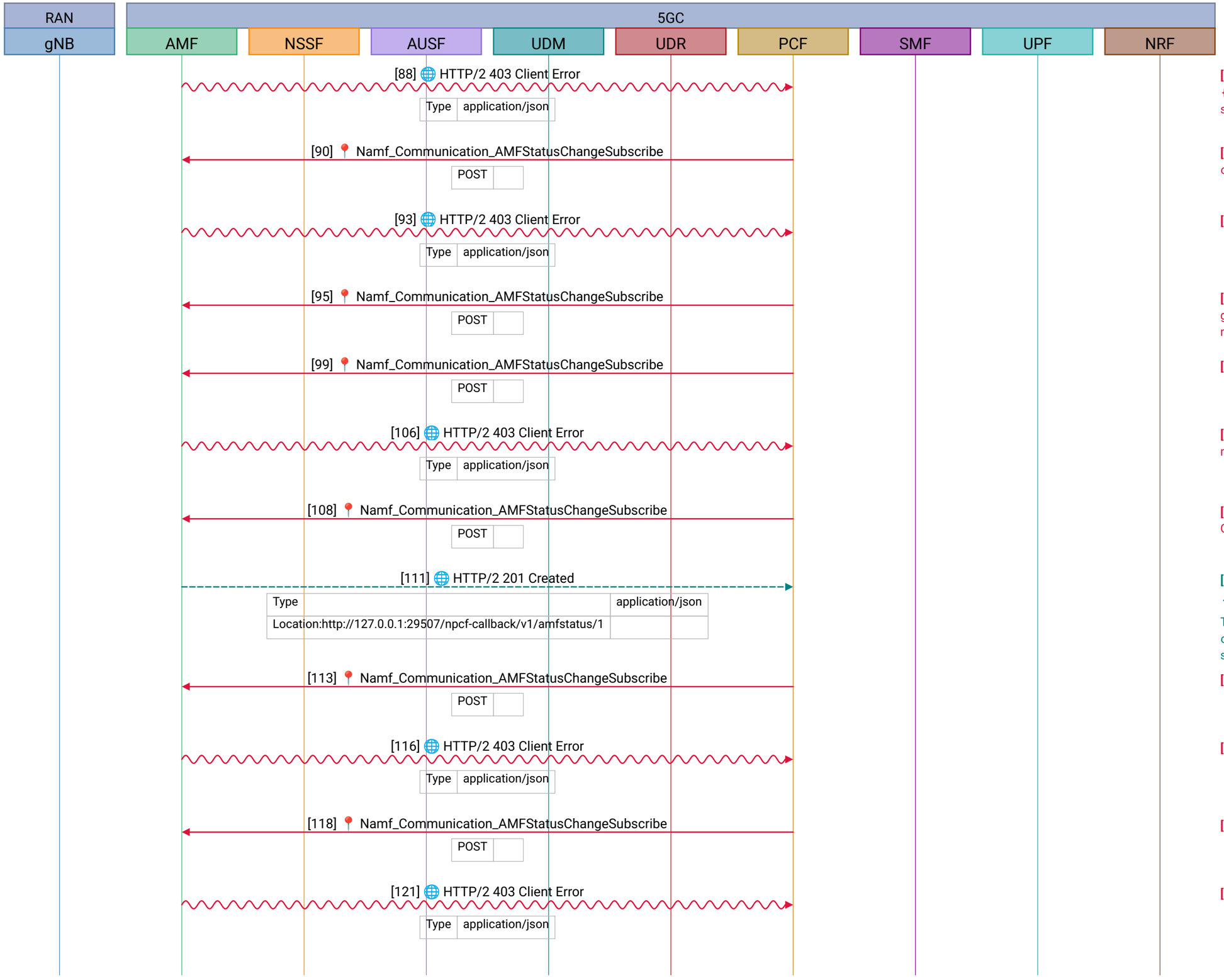
[Frame 59] `201 Created` for the UDM.

[Frame 66] `201 Created` for the PCF. Six NFs registered within 36 ms.

[Frame 68] The PCF looks for AMFs. Nnrf_NFDiscovery_Request with `target-nf-type=AMF`. The PCF wants to be told if an AMF fails, so it can clean up policies.

[Frame 69] The NRF returns **30 AMF profiles,** not one. Only the last is the AMF that registered in frame 17; the other 29 carry other instance IDs and other PLMNs (460/00, 460/11, even 208/93). They are leftovers from earlier runs of this lab that the NRF never removed. The PCF now subscribes to each profile's GUAMI list in turn, and that explains everything up to frame 181.

[Frame 81] Namf_Communication_AMFStatusChangeSubscribe. POST `/namf-comm/v1/subscriptions` naming GUAMI `460/11` + `cafe00`, taken from the first stale profile. The live AMF serves `460/00` + `cafe00` and `460/11` + `cafe11`, so this GUAMI crosses the two.



[Frame 88] ❌ `403 Forbidden`, body `{"cause":"UNSPECIFIED"}`. The AMF refuses a subscription for a GUAMI it does not serve.

[Frame 90] Second stale profile, same GUAMI `460/11` + `cafe00`.

[Frame 93] ❌ `403` again.

[Frame 95] Third stale profile, same GUAMI. This request gets no answer on this TCP connection; the PCF moves to a new connection.

[Frame 99] The same request again on the new connection.

[Frame 106] ❌ `403`. The transport changed; the GUAMI did not.

[Frame 108] The fourth profile names `460/00` + `cafe00`, a GUAMI the AMF really serves.

[Frame 111] ✅ `201 Created`, subscription `.../amfstatus/1`.

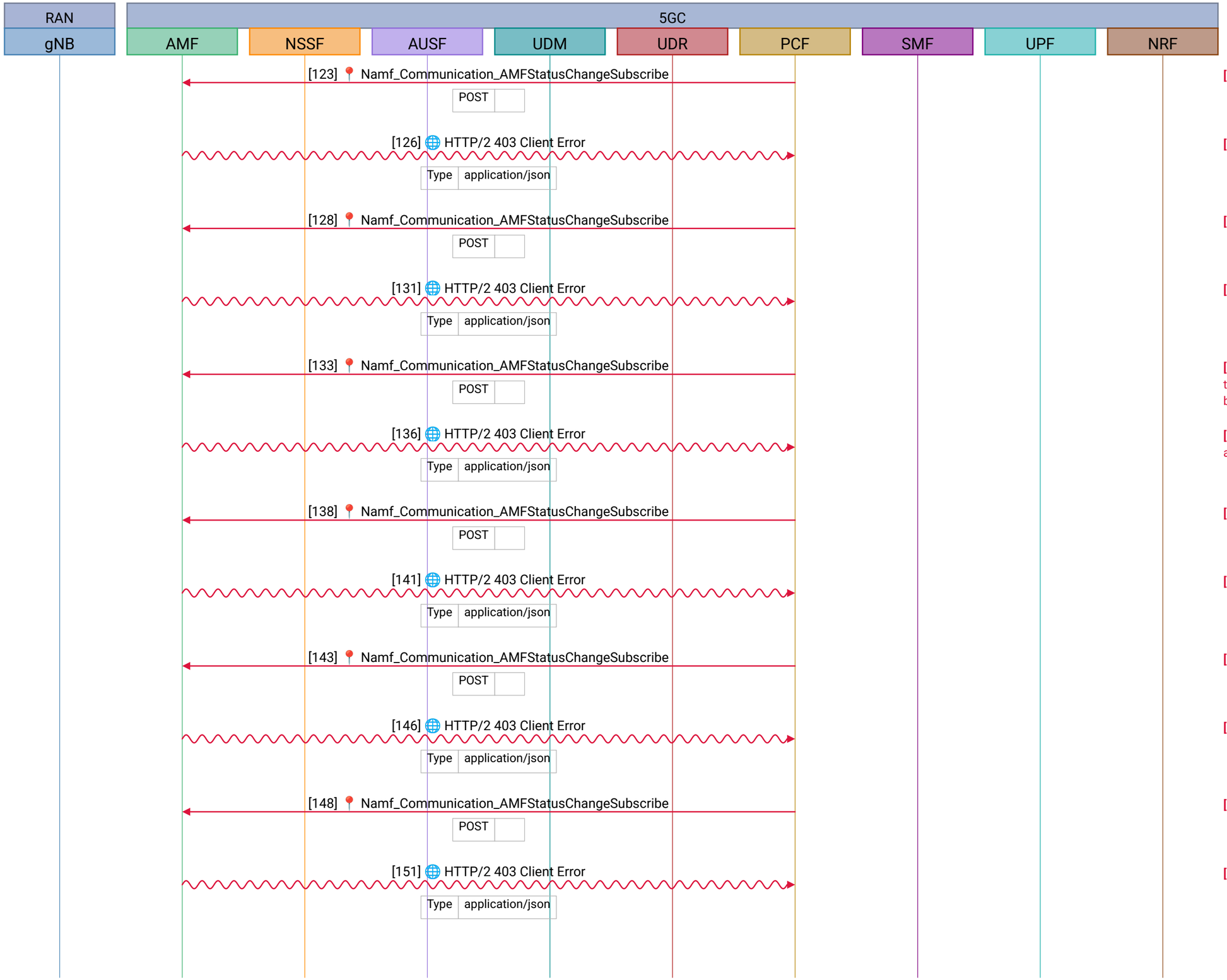
The next 13 profiles in the list carry the same `460/00` + `cafe00`. The PCF sends nothing for them: it appears to skip a GUAMI list it has already subscribed to.

[Frame 113] Next profile: `460/11` + `cafe00` again.

[Frame 116] ❌ `403`.

[Frame 118] `460/11` + `cafe00`.

[Frame 121] ❌ `403`.



[Frame 123] `460/11` + `cafe00`.

[Frame 126] ❌ `403`.

[Frame 128] `460/11` + `cafe00`.

[Frame 131] ❌ `403`.

[Frame 133] GUAMI `208/93` + `cafe00`. PLMN 208/93 is the one free5GC's sample configuration ships with, left behind by an older run.

[Frame 136] ❌ `403`. However wrong the GUAMI, the answer is the same.

[Frame 138] `460/11` + `cafe00`.

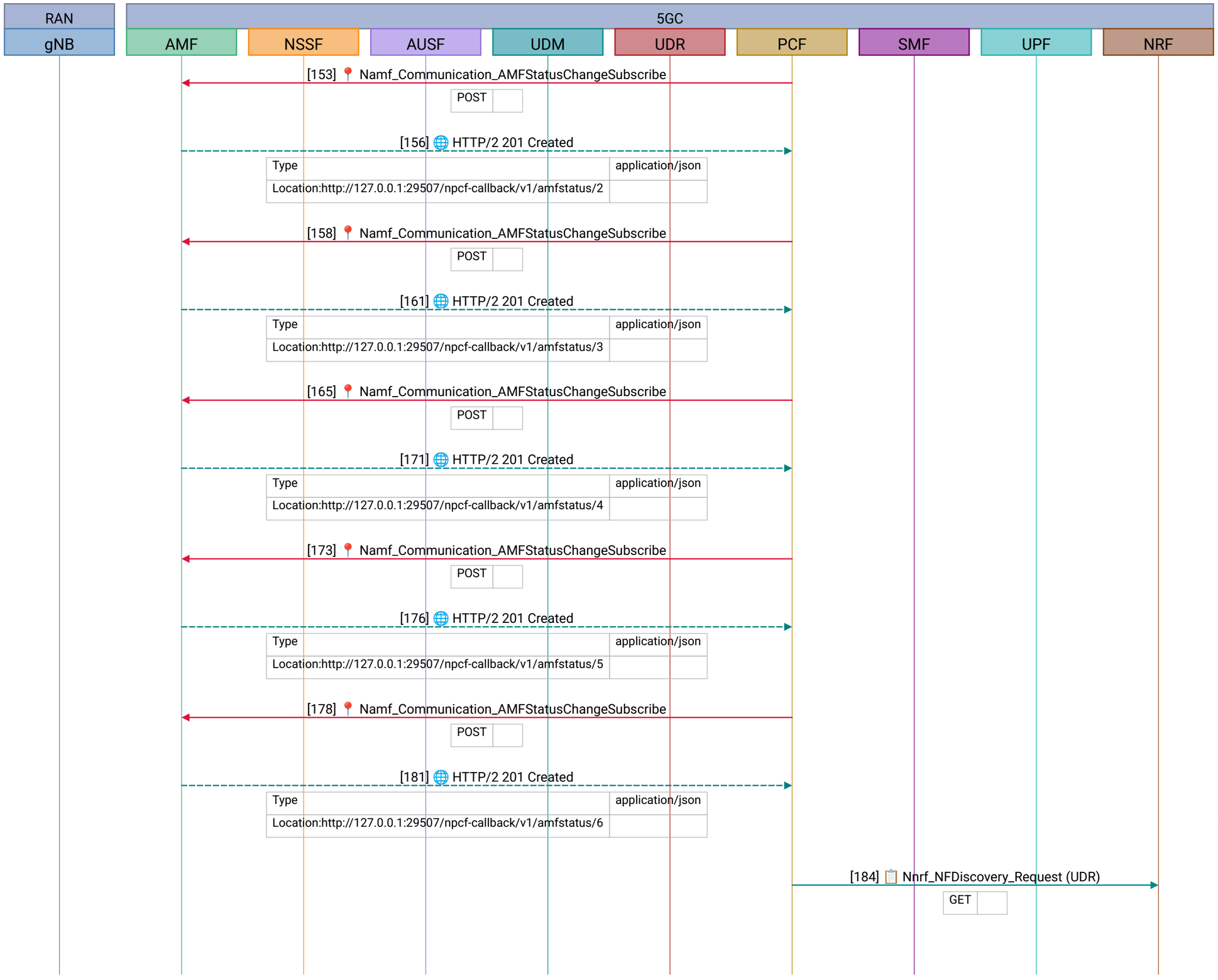
[Frame 141] ❌ `403`.

[Frame 143] `460/11` + `cafe00`.

[Frame 146] ❌ `403`.

[Frame 148] `460/11` + `cafe00`.

[Frame 151] ❌ `403`, the eleventh refusal.



[Frame 153] A two-entry list: `460/00` + `cafe00` (served) and `460/00` + `cafe11` (not served: `cafe11` belongs to 460/11).

[Frame 156] ✅ `201 Created, .../amfstatus/2.` The response body lists only `460/00` + `cafe00`: the AMF accepted the subscription for the GUAMI it serves and dropped the other.

[Frame 158] The same two-entry list from the next stale profile.

[Frame 161] ✅ `201, .../amfstatus/3,` again echoing only `460/00` + `cafe00.`

[Frame 165] The same list, on a third TCP connection.

[Frame 171] ✅ `201, .../amfstatus/4.`

[Frame 173] The same list once more.

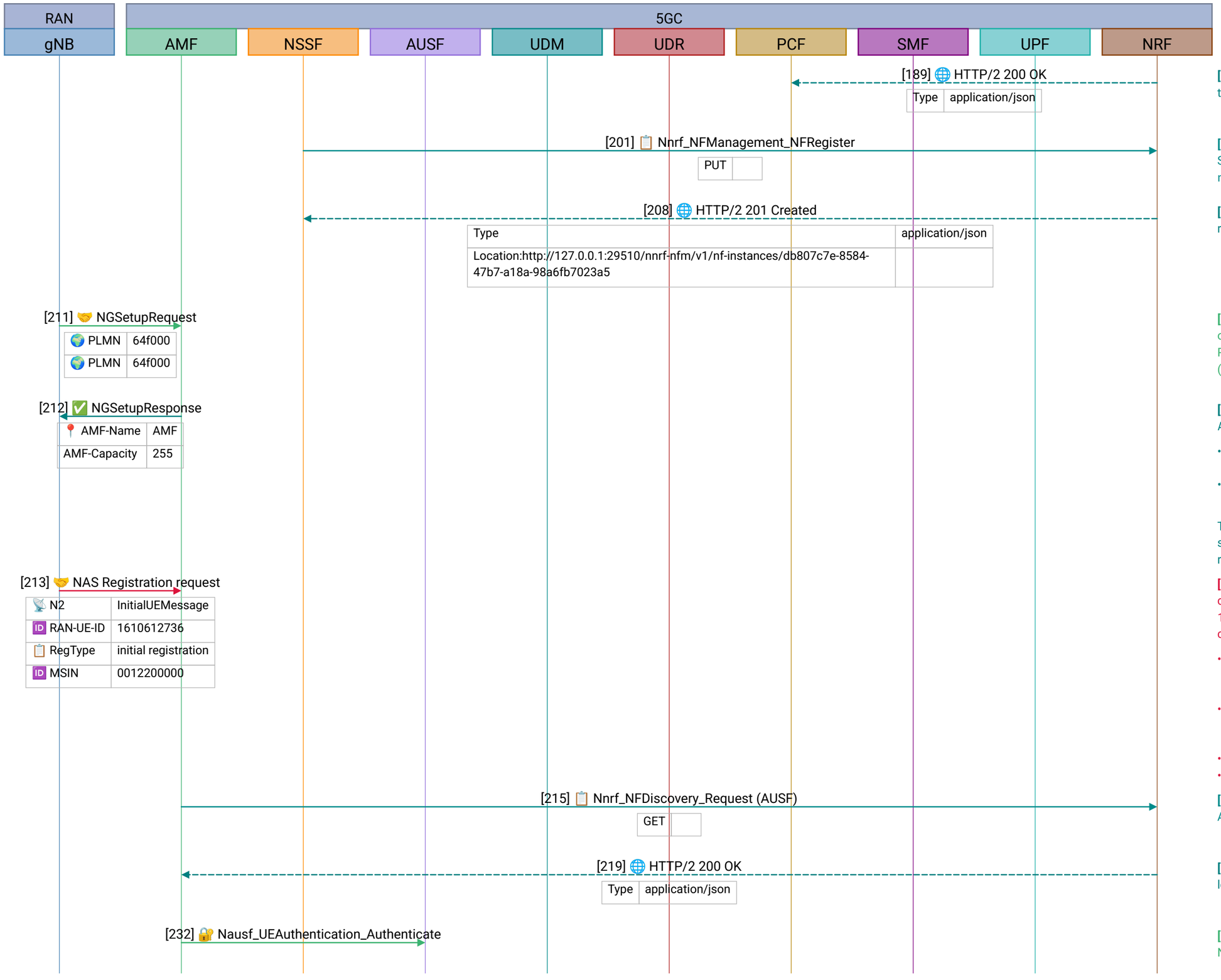
[Frame 176] ✅ `201, .../amfstatus/5.`

[Frame 178] The last profile, the live AMF: `460/00` + `cafe00` and `460/11` + `cafe11,` both served.

[Frame 181] ✅ `201, .../amfstatus/6,` and this time the body echoes both GUAMIs.

Tally: 18 requests, 11 refused, 1 unanswered, 6 accepted. Six subscriptions on one AMF mean six identical notifications when it stops (frames 851 to 874).

[Frame 184] The PCF discovers the UDR (`service-names=nudr-dr).` The NRF returns 123 UDR profiles; again the live one is last.



[Frame 189] Discovery result. The core is up, 119 ms after the first registration.

[Frame 201] About 2 s later the NSSF (Network Slice Selection Function) registers as `db807c7e-...` with `nnssf-nsselection` and `nnssf-nssaiavailability`.

[Frame 208] `201 Created` for the NSSF. All seven NFs are registered.

[Frame 211] Phase 2 - the gNB connects. 13 s later the gNB opens N2 over SCTP with **NG Setup Request:** gNB ID 0, PLMN `64f000` (MCC 460, MNC 00), tracking area code (TAC) 1, slices SST 1, 2 and 3.

[Frame 212] NG Setup Response. The AMF names itself `AMF`, relative capacity 255, and lists its served GUAMIs:

- 460/00: region `0xCA`, set 1016, pointer 0 -> AMF ID `cafe00`
- 460/11: region `0xCA`, set 1016, pointer 17 -> AMF ID `cafe11`

These two are the whole served set, which is why every subscription in phase 1 that named another GUAMI was refused. N2 is up.

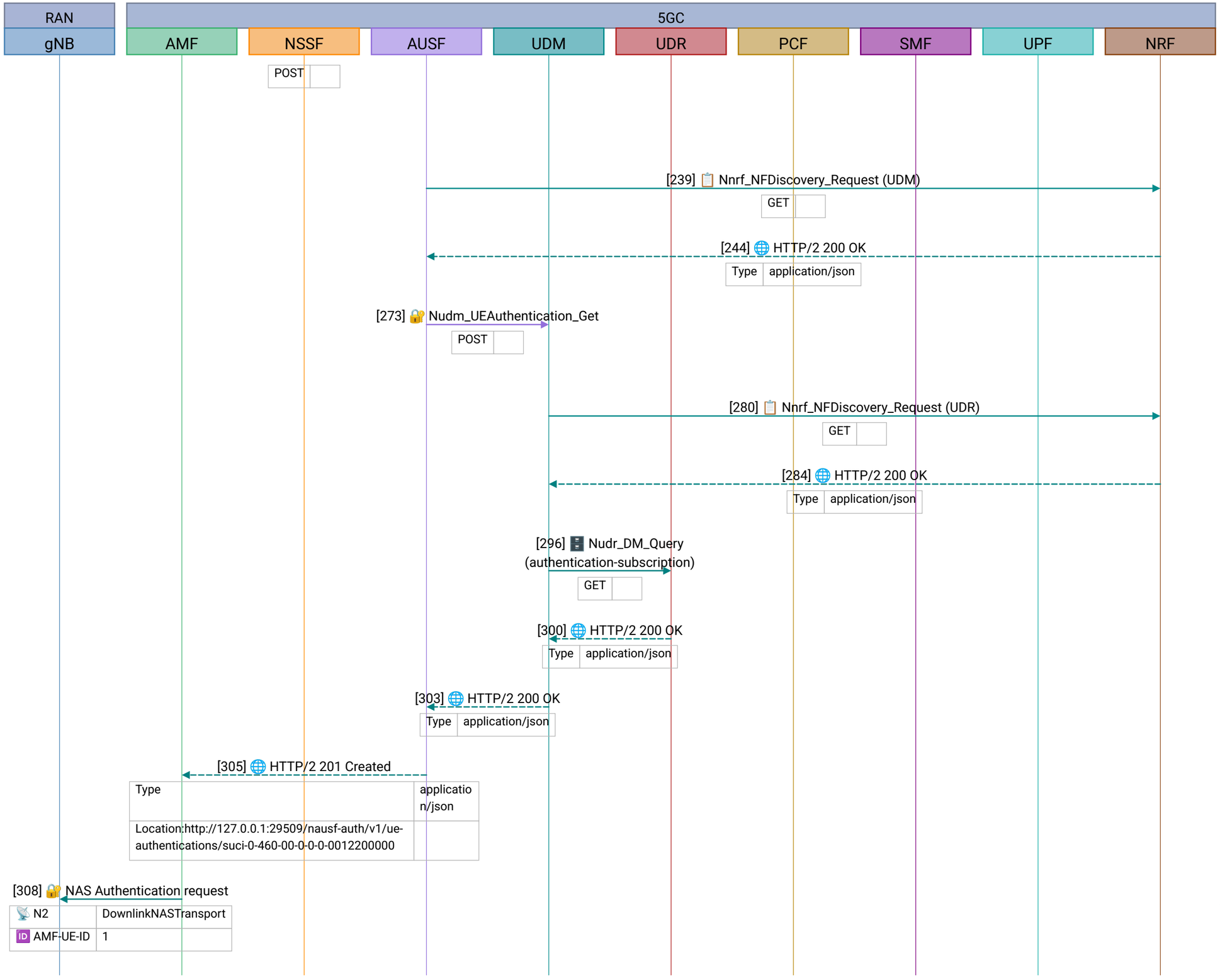
[Frame 213] Phase 3 - registration. Initial UE Message carrying a NAS **Registration Request,** RAN-UE-NGAP-ID `1610612736`, RRC establishment cause `mo-Signalling`, cell 1 in TAC 1.

- Registration type: initial, with the **Follow-On Request** bit set: the UE has more to send (a PDU session request, frame 616).
- Identity: SUCI (Subscription Concealed Identifier) with the **null protection scheme,** so the MSIN `0012200000` travels in clear. SUCI concealment is switched off.
- ngKSI 7: the UE holds no security context yet.
- UE security capabilities: 5G-EA0 to EA3 and 5G-IA0 to IA3.

[Frame 215] To authenticate the UE, the AMF needs an AUSF: Nnrf_NFDiscovery_Request (AUSF).

[Frame 219] 123 AUSF profiles come back. With a list that long, this discovery takes 37 ms.

[Frame 232] 5G-AKA starts.
Nausf_UEAuthentication_Authenticate with `supiOrSuci`:



`suci-0-460-00-0-0-0-0012200000` and `servingNetworkName: 5G:mnc000.mcc460.3gppnetwork.org`. The serving network name is bound into the key derivation, so an authentication vector made for one network cannot be replayed in another.

[Frame 239] The AUSF cannot compute vectors itself; the UDM holds the subscriber's long-term key. AUSF discovers a UDM offering `nudm-ueau`.

[Frame 244] Discovery result (125 UDM profiles).

[Frame 273] Nudm_UEAuthentication_Get: `POST .../suci-.../security-information/generate-auth-data`. The UDM de-conceals the SUCI to the SUPI (Subscription Permanent Identifier), trivially here because of the null scheme.

[Frame 280] The UDM discovers the UDR.

[Frame 284] Discovery result.

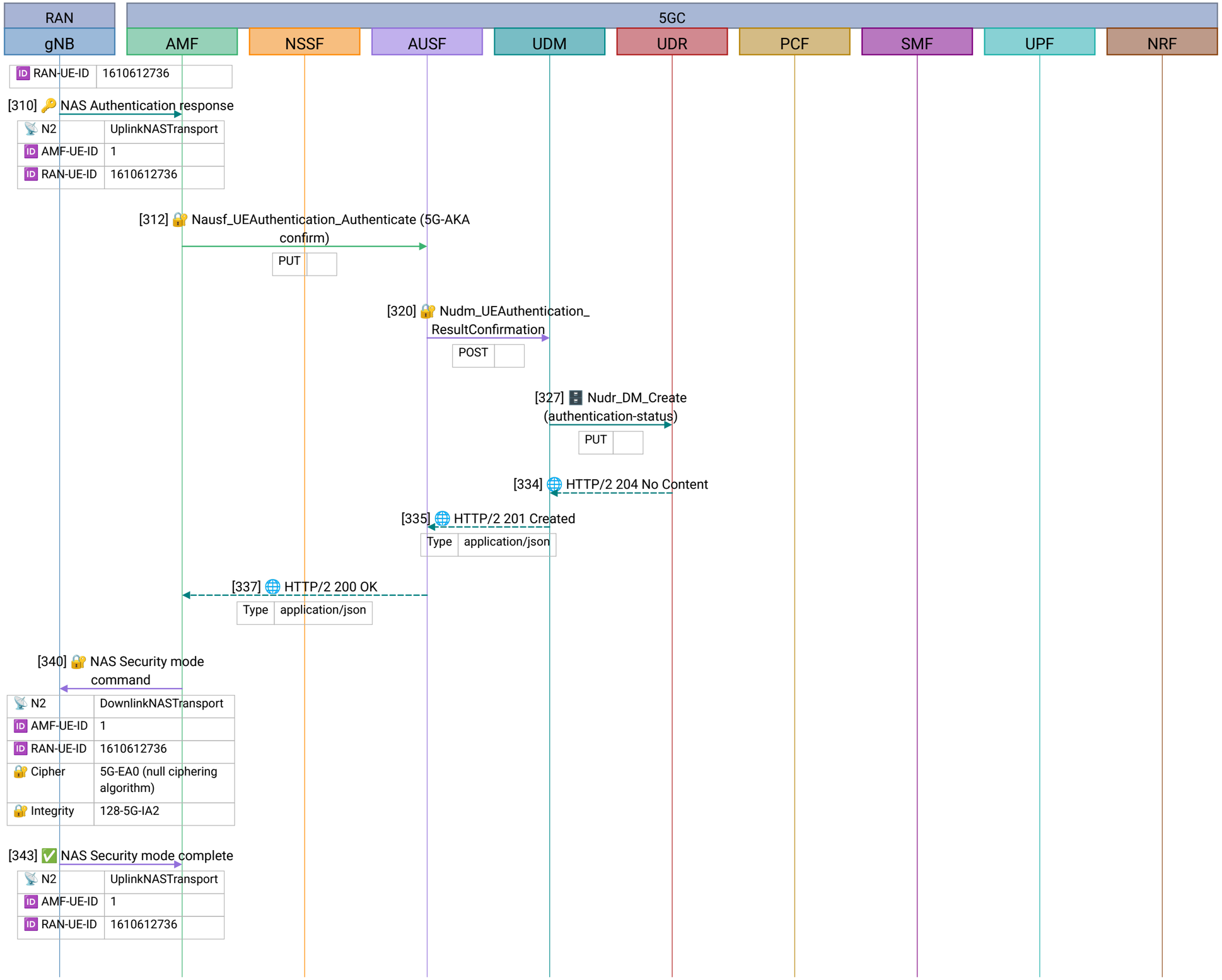
[Frame 296] Nudr_DM_Query for the subscriber's `authentication-subscription`. The URI now carries the plain SUPI `imsi-460000012200000`.

[Frame 300] The UDR returns the credentials; the UDM computes the vector.

[Frame 303] The UDM returns the home-network vector to the AUSF: `RAND`, `AUTN`, `XRES*`, `K_AUSF` and the SUPI.

[Frame 305] `201 Created` to the AMF with `RAND`, `AUTN` and **`HXRES*`**, a hash of the expected response. The AUSF keeps `XRES*` and the SUPI. The serving network can pre-check the UE's answer, but only the home network can confirm it.

[Frame 308] NAS **Authentication Request** in Downlink NAS Transport: ngKSI 0, ABBA `0000`, RAND `07d1...8194`, AUTN `db12...3bcb`. The AMF assigns AMF-UE-NGAP-ID 1 here.



[Frame 310] NAS **Authentication Response** with `RES* 1573d7ca....` The UE checked `AUTN`, which proves the network knows its key, and computed `RES*`. Round trip: 2 ms.

[Frame 312] Nausf_UEAuthentication_Authenticate, confirmation step: PUT `.../5g-aka-confirmation` with `resStar`. The AMF has matched the hash of `RES*` against `HXRES*`; now the AUSF compares `RES*` with `XRES*`. They are equal.

[Frame 320] Nudm_UEAuthentication_ResultConfirmation: the AUSF tells the UDM the UE was authenticated.

[Frame 327] The UDM stores the authentication status in the UDR (Nudr_DM_Create, `authentication-status`).

[Frame 334] `204 No Content:` stored.

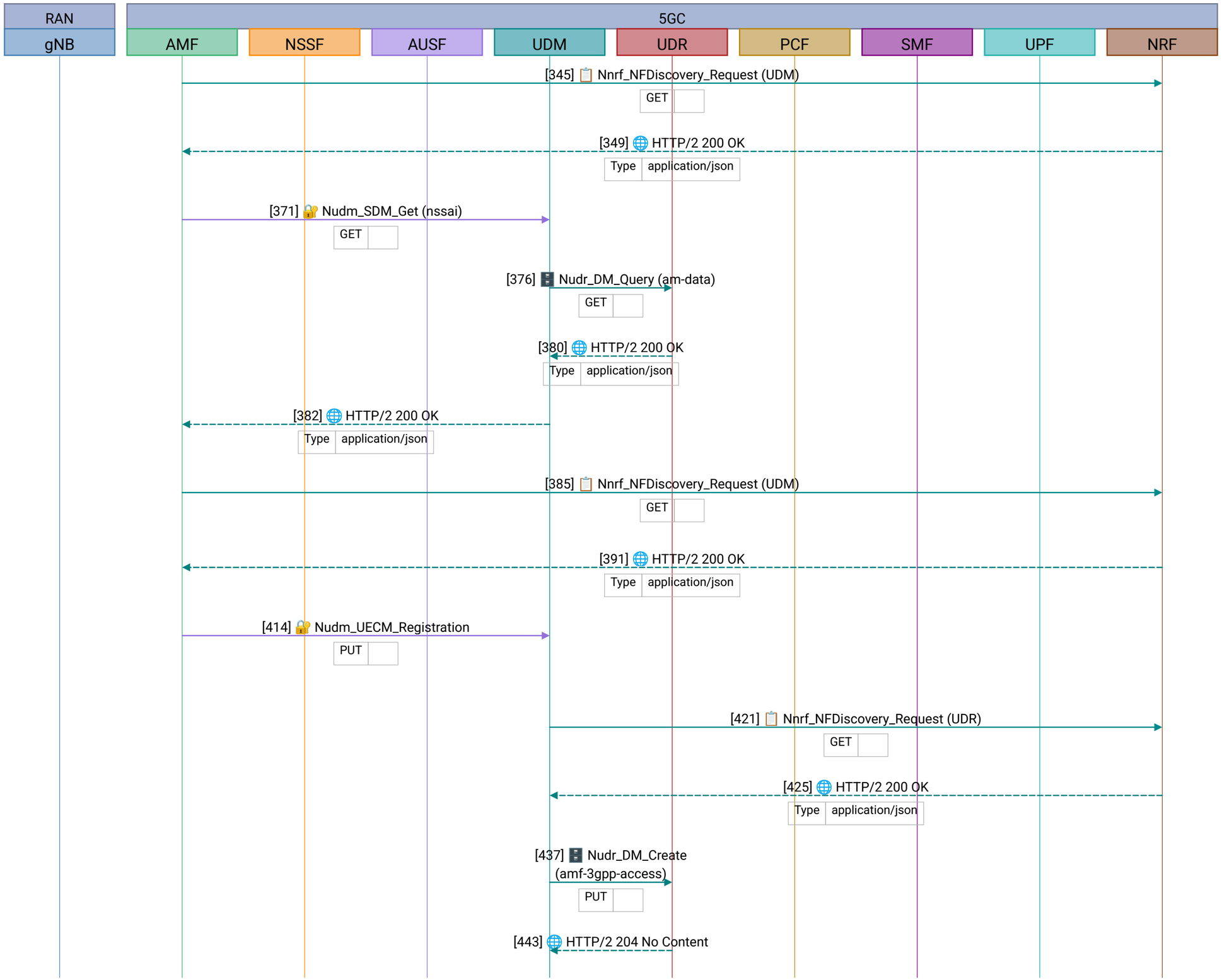
[Frame 335] `201 Created:` the authentication event is recorded.

[Frame 337] ✅ `200 OK, authResult: AUTHENTICATION_SUCCESS`. Only now does the AMF receive the **SUPI** and **K_SEAF**, the anchor key from which the AMF derives its NAS keys.

[Frame 340] Security Mode Command (security header type 3: integrity protected with the new context). The AMF selects **5G-EA0 (null ciphering)** and **128-5G-IA2** integrity, replays the UE's security capabilities, and requests the IMEISV.

The UE supports EA1 to EA3, so encryption was available and not chosen. That is why every later NAS message decodes in full here; it is a lab setting.

[Frame 343] Security Mode Complete (header type 4: integrity protected and ciphered with the new context, the cipher being null). It carries the IMEISV and, in the NAS message container, the complete Registration Request again, so the AMF can check that the unprotected copy in frame 213 was not altered.



[Frame 345] Phase 4 - subscription data. With the SUPI known, the AMF discovers the UDM for this subscriber (`supi=imsi-...`).

[Frame 349] Discovery result.

[Frame 371] Nudm_SDM_Get (`nssai`) : which slices may this subscriber use?

[Frame 376] The UDM reads `am-data` from the UDR.

[Frame 380] UDR response.

[Frame 382] Subscribed S-NSSAIs: `1/010203` and `1/112233` , both marked default.

[Frame 385] The AMF runs the same UDM discovery again rather than reusing the result. free5GC repeats discovery before many calls, which is one reason this capture holds so many NRF round trips.

[Frame 391] Discovery result.

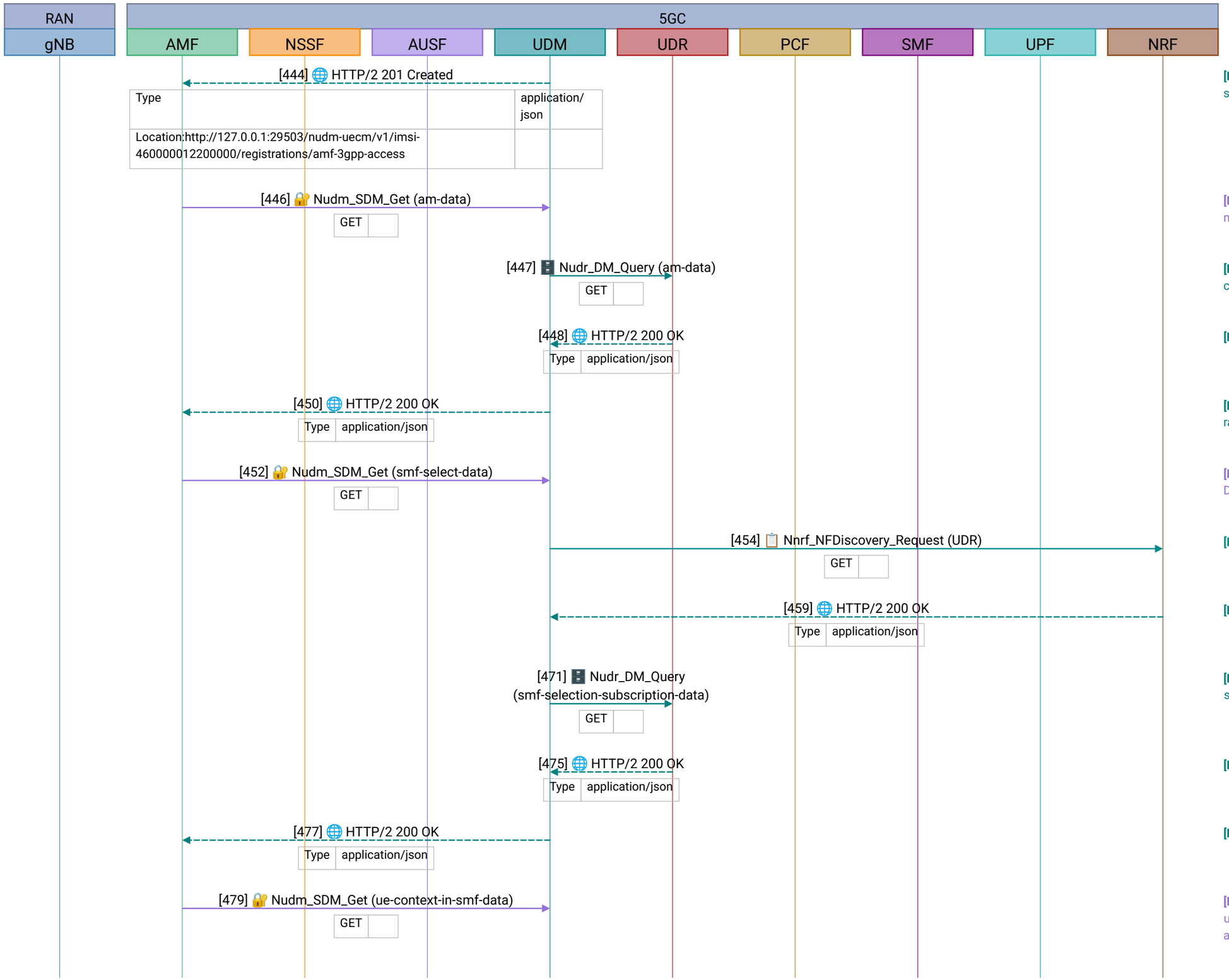
[Frame 414] Nudm_UECM_Registration. PUT `.../registrations/amf-3gpp-access` : this AMF (`7f4ddbaa-...` , GUAMI 460/00 + cafe00) records itself as the subscriber's serving AMF for 3GPP access. Other NFs find the UE's AMF through this record.

[Frame 421] The UDM discovers the UDR.

[Frame 425] Discovery result.

[Frame 437] Nudr_DM_Create (`amf-3gpp-access`) : the serving-AMF record is written.

[Frame 443] `204 No Content` .



[Frame 444] `201 Created`. This AMF is now the registered serving AMF.

[Frame 446] Nudm_SDM_Get (`am-data`): access and mobility subscription data.

[Frame 447] The UDM reads it from the UDR on the connection it opened in frame 437, with no new discovery.

[Frame 448] UDR response.

[Frame 450] Subscribed UE-AMBR (aggregate maximum bit rate) 1000 kbps each way, MSISDN `0900000000`.

[Frame 452] Nudm_SDM_Get (`smf-select-data`): which DNNs per slice, used later to choose an SMF.

[Frame 454] The UDM discovers the UDR.

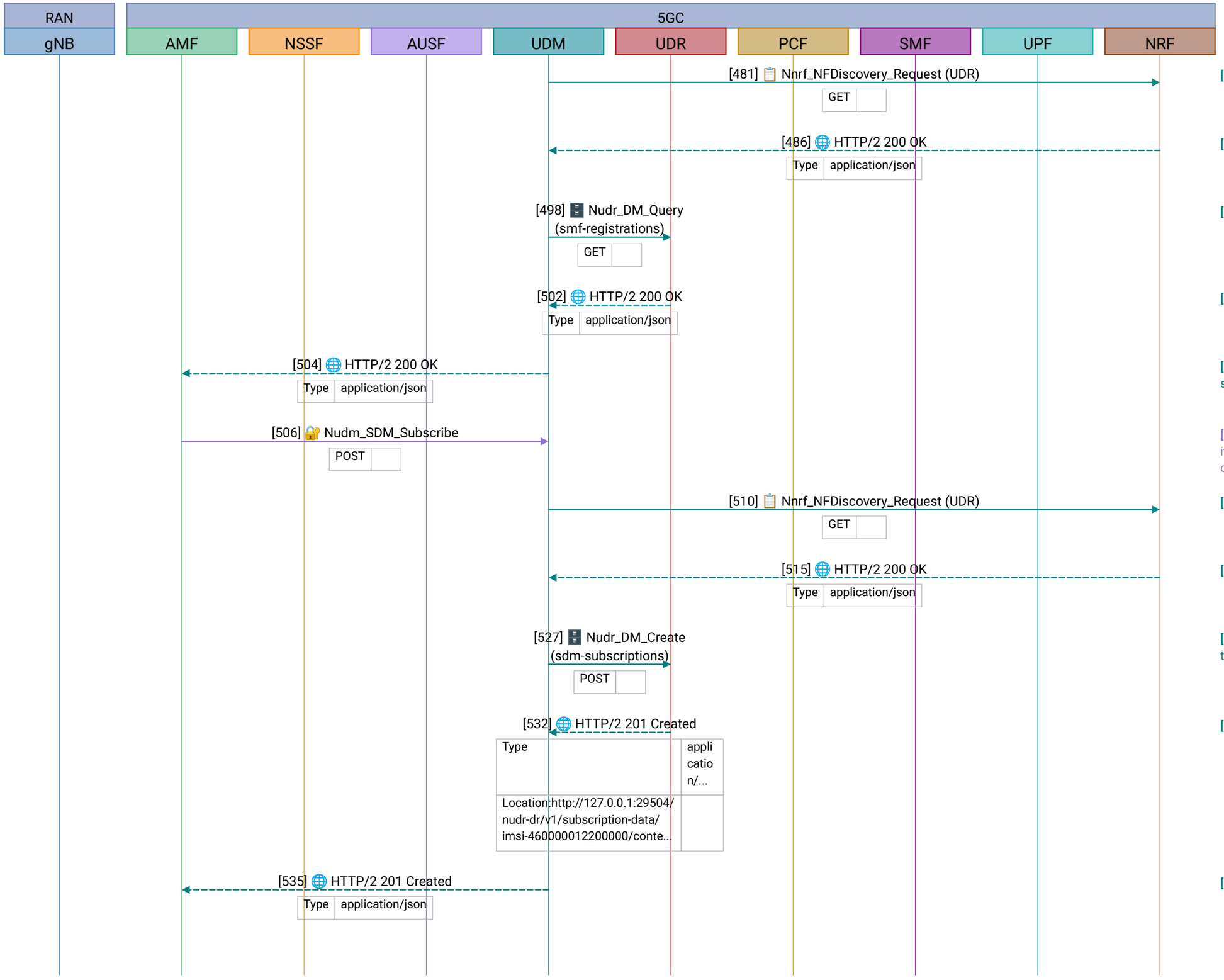
[Frame 459] Discovery result.

[Frame 471] Nudr_DM_Query (`smf-selection-subscription-data`).

[Frame 475] UDR response.

[Frame 477] Both slices allow DNN `internet`.

[Frame 479] Nudm_SDM_Get (`ue-context-in-smf-data`): does the subscriber already have PDU sessions on some SMF?



[Frame 481] The UDM discovers the UDR.

[Frame 486] Discovery result.

[Frame 498] Nudr_DM_Query (`smf-registrations`).

[Frame 502] The UDR returns no SMF registrations.

[Frame 504] The UDM relays an empty object: no existing sessions.

[Frame 506] Nudm_SDM_Subscribe: the AMF asks to be told if this subscriber's data changes, so a later provisioning change reaches it without a new registration.

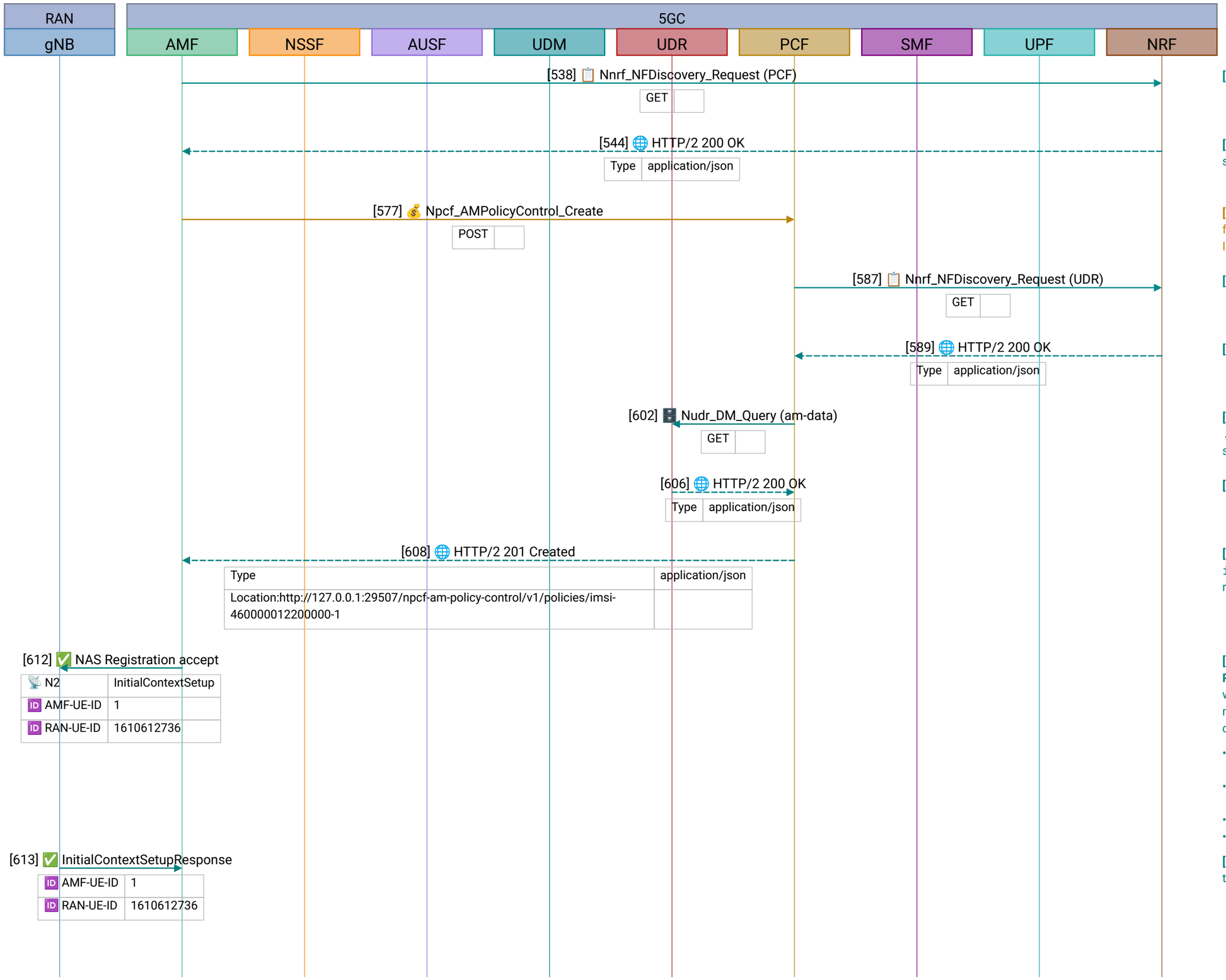
[Frame 510] The UDM discovers the UDR.

[Frame 515] Discovery result.

[Frame 527] Nudr_DM_Create (`sdm-subscriptions`): the UDM stores the subscription.

[Frame 532] `201 Created`, subscription ID 1.

[Frame 535] `201 Created` to the AMF.



[Frame 538] The AMF discovers a PCF for this SUPI.

[Frame 544] Discovery result: the same PCF whose subscriptions this AMF refused eleven times in phase 1.

[Frame 577] Npcf_AMPolicyControl_Create: the AMF asks for access and mobility policy, sending the SUPI, MSISDN, IMEISV, GUAMI and serving PLMN.

[Frame 587] The PCF discovers the UDR.

[Frame 589] Discovery result.

[Frame 602] Nudr_DM_Query (`policy-data .../am-data)` : policy data lives in the same UDR under a separate `policy-data` tree.

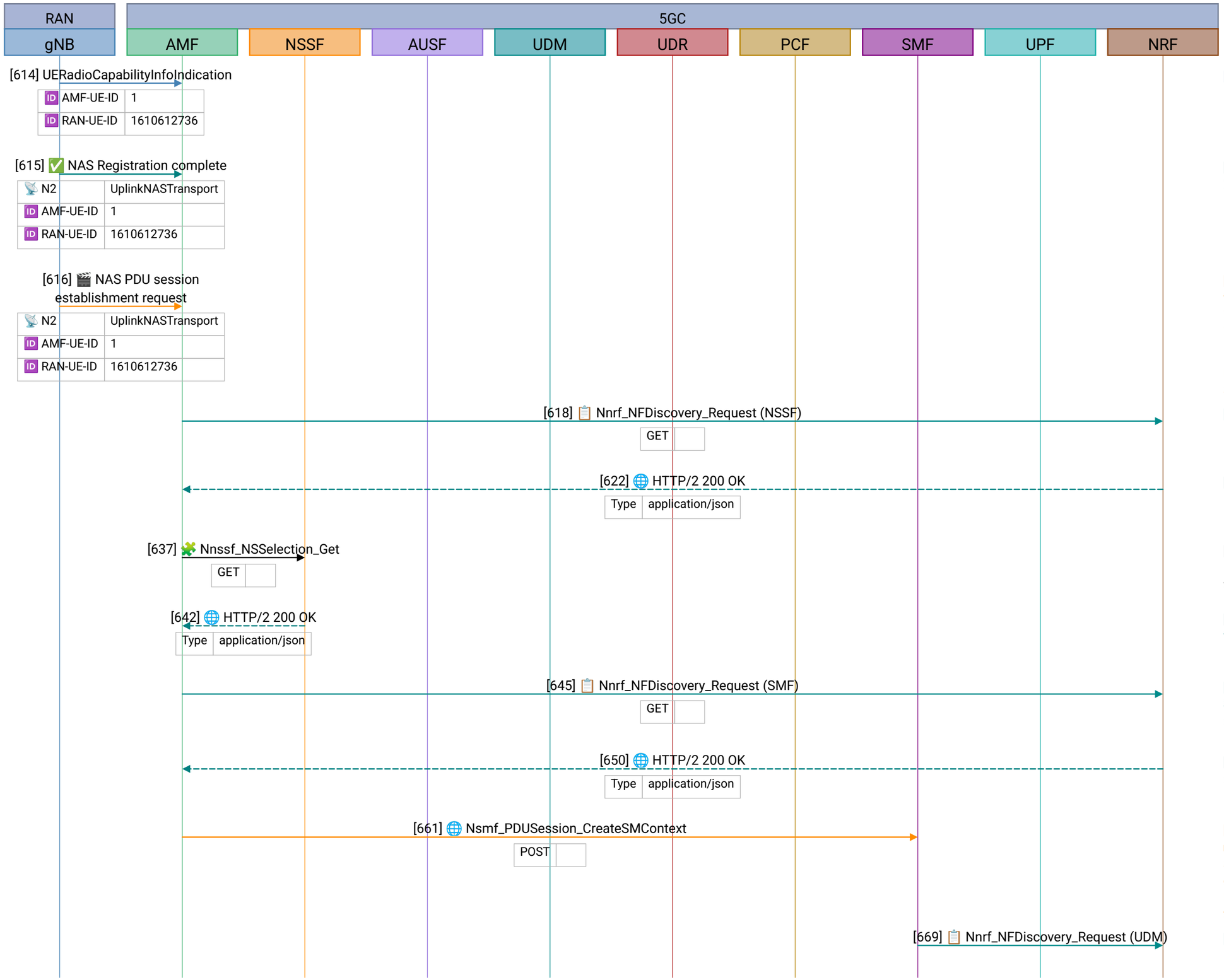
[Frame 606] UDR response: subscriber category `free5gc.`

[Frame 608] `201 Created,` policy `imsi-460000012200000-1.` The AMF deletes exactly this resource at shutdown (frame 843).

[Frame 612] Phase 5 - registration accepted. NAS **Registration Accept** inside an **Initial Context Setup Request,** which also gives the gNB the UE's security context. The NAS message is integrity protected (sequence number 1) and carries:

- 5G-GUTI: 460/00, region 202, set 1016, pointer 0, 5G-TMSI 1
- Equivalent PLMNs 460/00 and 460/11; tracking area list TAC 1
- Allowed NSSAI `1/010203` and `1/112233`
- T3512 (periodic registration) 60 min, T3502 12 min

[Frame 613] Initial Context Setup Response: the gNB holds the UE context, 665 ms after the Initial UE Message.



[Frame 614] UE Radio Capability Info Indication: the gNB hands the AMF the UE's radio capabilities to store.

[Frame 615] NAS **Registration Complete:** the UE accepts the 5G-GUTI. The UE is registered.

[Frame 616] Phase 6 - PDU session. The follow-on request from frame 213 is used now. A **UL NAS Transport** carries a 5GSM **PDU Session Establishment Request:** PDU session ID 5, PTI 1, IPv4, SSC mode 1. The outer 5GMM message adds request type `initial request` and DNN `internet`.

It carries **no S-NSSAI,** so the AMF picks the slice from the subscription; it chooses `1/112233`.

[Frame 618] The AMF discovers the NSSF.

[Frame 622] Discovery result.

[Frame 637] Nnssf_NSSelection_Get with `sNssai {sst 1, sd 112233}` and `roamingIndication NON_ROAMING`: which network slice instance serves this session?

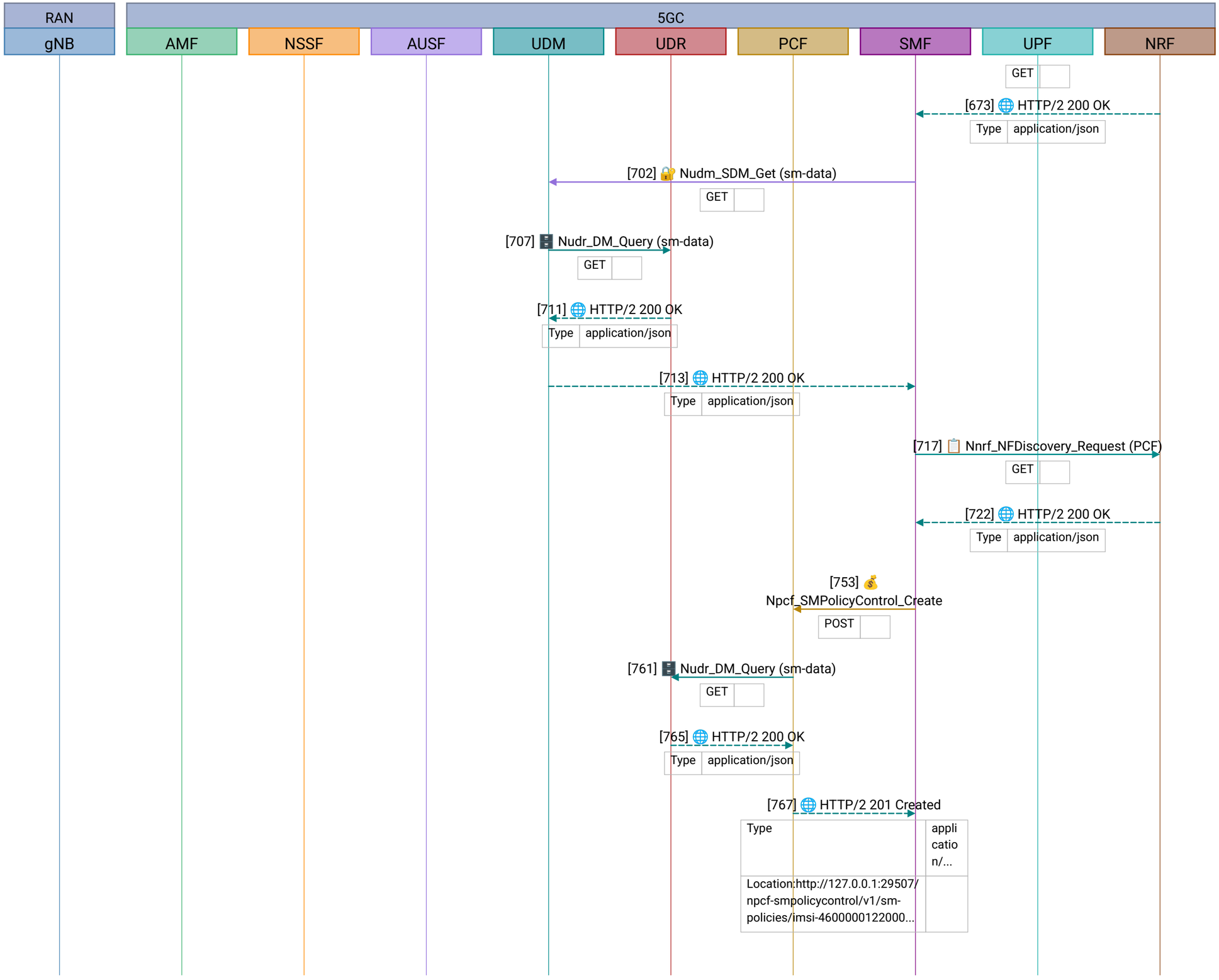
[Frame 642] Slice instance `nsiId 23,` with the NRF to use for it.

[Frame 645] The most specific discovery in the capture: an SMF with `dnn=internet, service-names=nsmf-pdusession,` S-NSSAI `1/112233,` PLMN 460/00.

[Frame 650] 33 SMF profiles match; the live SMF (`e3499f37-...`) is last.

[Frame 661] Nsmf_PDUSession_CreateSMContext. A `multipart/related` POST: one JSON part (SUPI, PDU session ID 5, DNN, S-NSSAI, serving AMF, GUAMI, a status callback URI) and one binary part, the UE's NAS PDU Session Establishment Request. The AMF forwards 5GSM messages without interpreting them; the SMF reads them.

[Frame 669] The SMF discovers the UDM.



[Frame 673] Discovery result.

[Frame 702] Nudm_SDM_Get (`sm-data`) for DNN `internet` on slice `1/112233` .

[Frame 707] The UDM reads `sm-data` from the UDR.

[Frame 711] UDR response.

[Frame 713] Session subscription: IPv4 only, SSC modes 1 to 3 (default 1), default QoS 5QI 9 with ARP priority 8, session-AMBR **1000 kbps** each way.

[Frame 717] The SMF discovers the PCF.

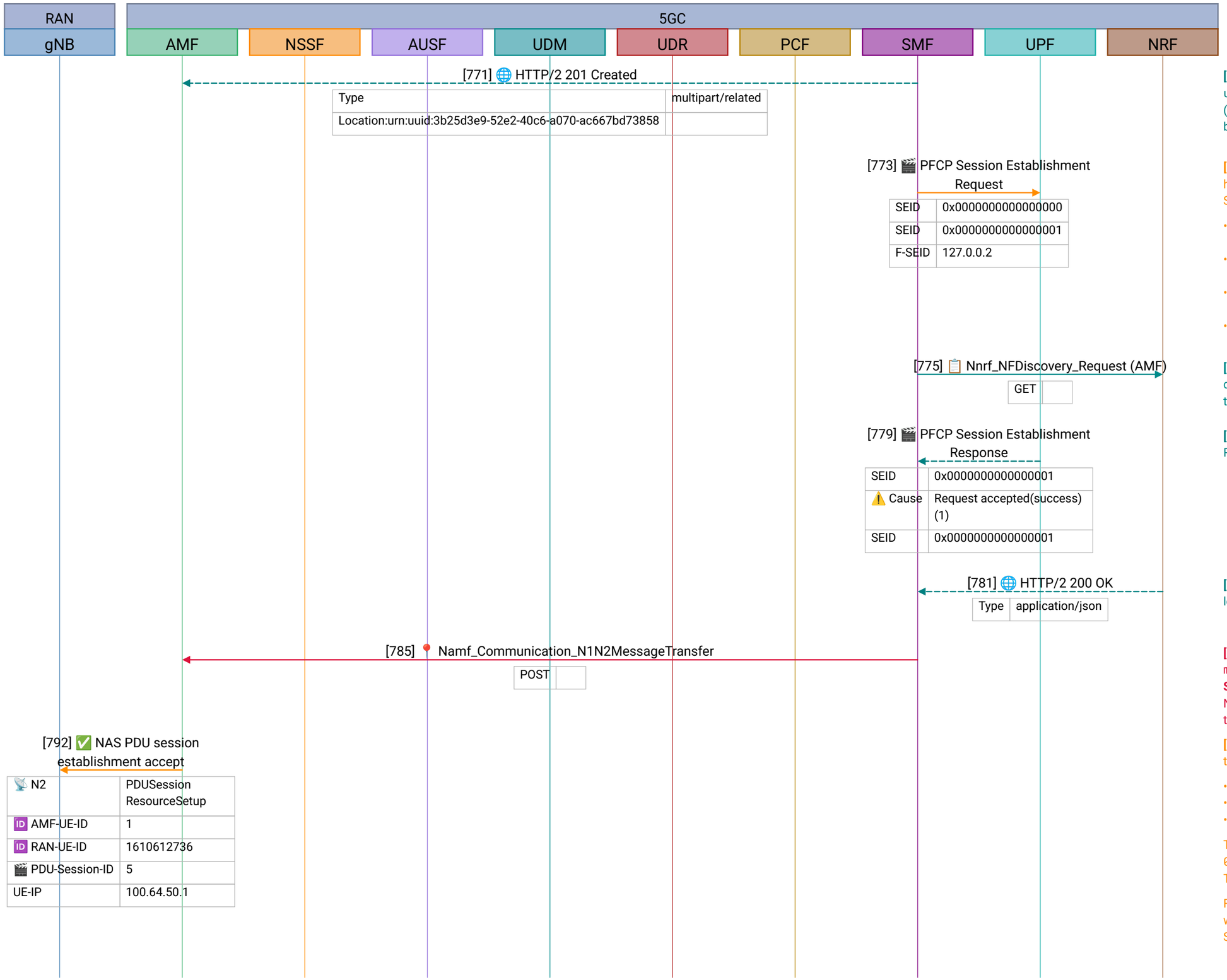
[Frame 722] Discovery result.

[Frame 753] Npcf_SMPolicyControl_Create: the SMF asks for session policy. The request already carries the UE address `100.64.50.1,` so the SMF allocated it before this call.

[Frame 761] The PCF reads the subscriber's SM policy data from the UDR.

[Frame 765] UDR response.

[Frame 767] `201 Created,` policy `imsi-460000012200000-5` (5 is the PDU session ID). Authorized: session-AMBR 1000 kbps, 5QI 9, ARP priority 8.



[Frame 771] `201 Created` for the SM context, `Location: urn:uuid:3b25d3e9-....` Every later call on this session (update, release) uses this reference. The SMF answers before it programs the UPF.

[Frame 773] PFCP Session Establishment Request. The header SEID is 0 because the UPF has no session yet; the SMF offers its own F-SEID `0x1` at `127.0.0.2`.

- PDR 1 (uplink): source Access, F-TEID **TEID 1 at 172.17.1.50,** remove the GTP-U header, apply FAR 1.
- PDR 2 (downlink): source Core, UE IP `100.64.50.1`, apply FAR 2.
- FAR 1: forward, destination interface `Access`. For uplink, TS 29.244 expects `Core`.
- FAR 2: forward, with no tunnel yet: the gNB's downlink TEID is still unknown.

[Frame 775] The SMF needs the AMF that holds this UE, so it discovers by **`target-nf-instance-id=7f4ddbaa-...,`** the UUID from frame 17.

[Frame 779] PFCP Session Establishment Response: `Request accepted`, UPF SEID 1.

[Frame 781] Exactly one profile comes back, in 3 ms; the long lists elsewhere took 20 to 100 ms.

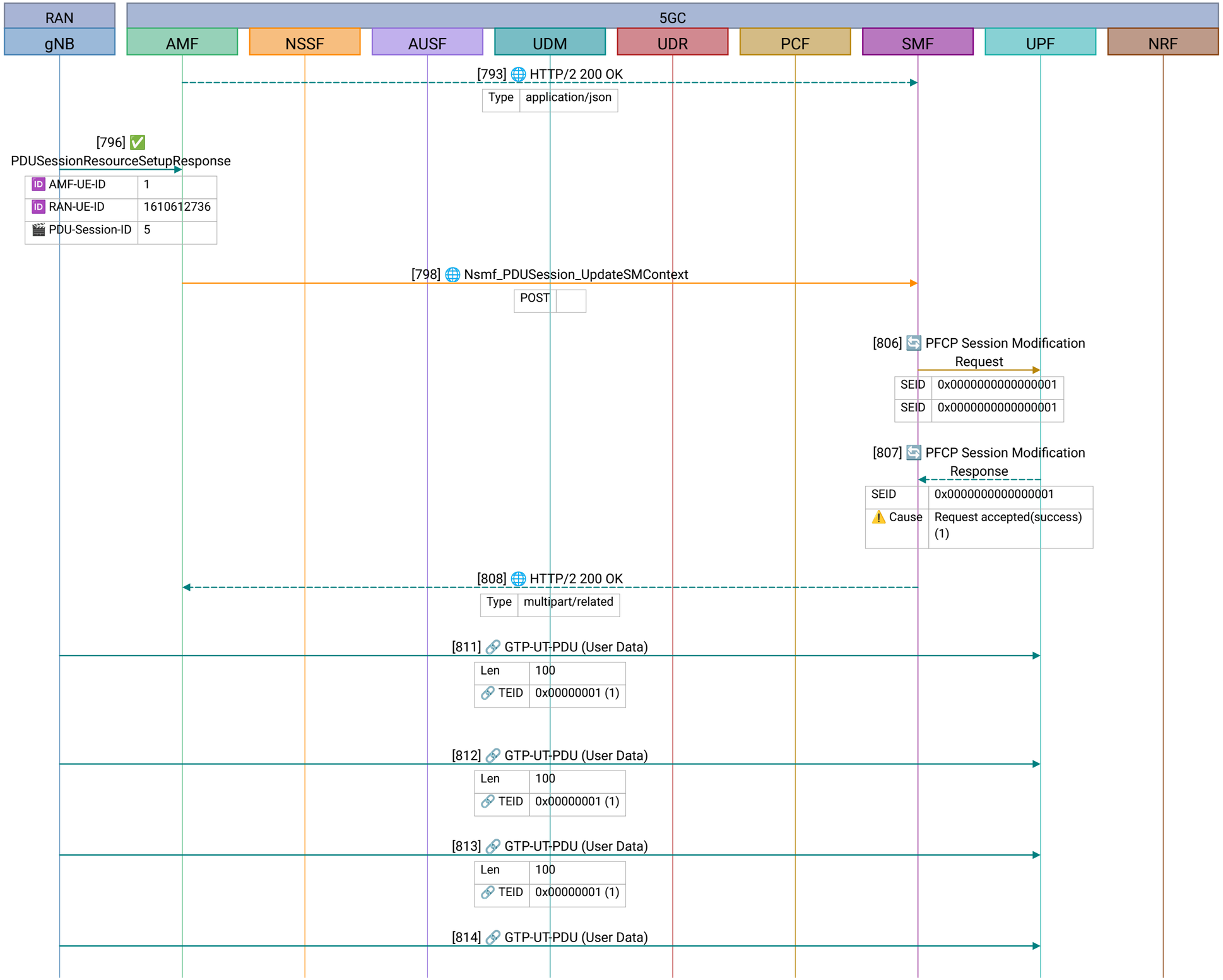
[Frame 785] Namf_Communication_N1N2MessageTransfer, `multipart/related` with two binary parts: the 5GSM **PDU Session Establishment Accept** for the UE (N1) and the NGAP **PDU Session Resource Setup Request Transfer** for the gNB (N2), which holds the UPF's uplink tunnel endpoint.

[Frame 792] PDU Session Resource Setup Request, carrying the NAS **PDU Session Establishment Accept:**

- PDU address **`100.64.50.1,`** IPv4, SSC mode 1
- Default QoS rule 1 on **QFI 9**
- Session-AMBR **59395 kbps** each way

The subscription and policy said 1000 kbps, which is `0x03E8`. `59395` is `0xE803`: the same two bytes swapped. The SMF encoded the value in the wrong byte order.

For the gNB: uplink tunnel **TEID 1 at 172.17.1.50,** QoS flow 9 with 5QI 9 (ARP priority 15, although the policy said 8), S-NSSAI `1/112233`.



[Frame 793] `200 OK, cause: N1_N2_TRANSFER_INITIATED`: the AMF has passed both parts on.

[Frame 796] PDU Session Resource Setup Response: QoS flow 9 is set up and the gNB's downlink tunnel is **TEID 1 at 172.17.1.231.** Both directions use TEID value 1, but they are different endpoints; a TEID only means something with its IP address.

[Frame 798] Nsmf_PDUSession_UpdateSMContext: the AMF relays the gNB's N2 response (and the UE's location) to the SMF.

[Frame 806] PFCP Session Modification Request: update FAR 2 with outer header creation GTP-U/UDP/IPv4, **TEID 1 at 172.17.1.231.** Downlink traffic now has somewhere to go.

[Frame 807] PFCP Session Modification Response: `Request accepted.` The N3 tunnel is complete both ways, 279 ms after the UE asked.

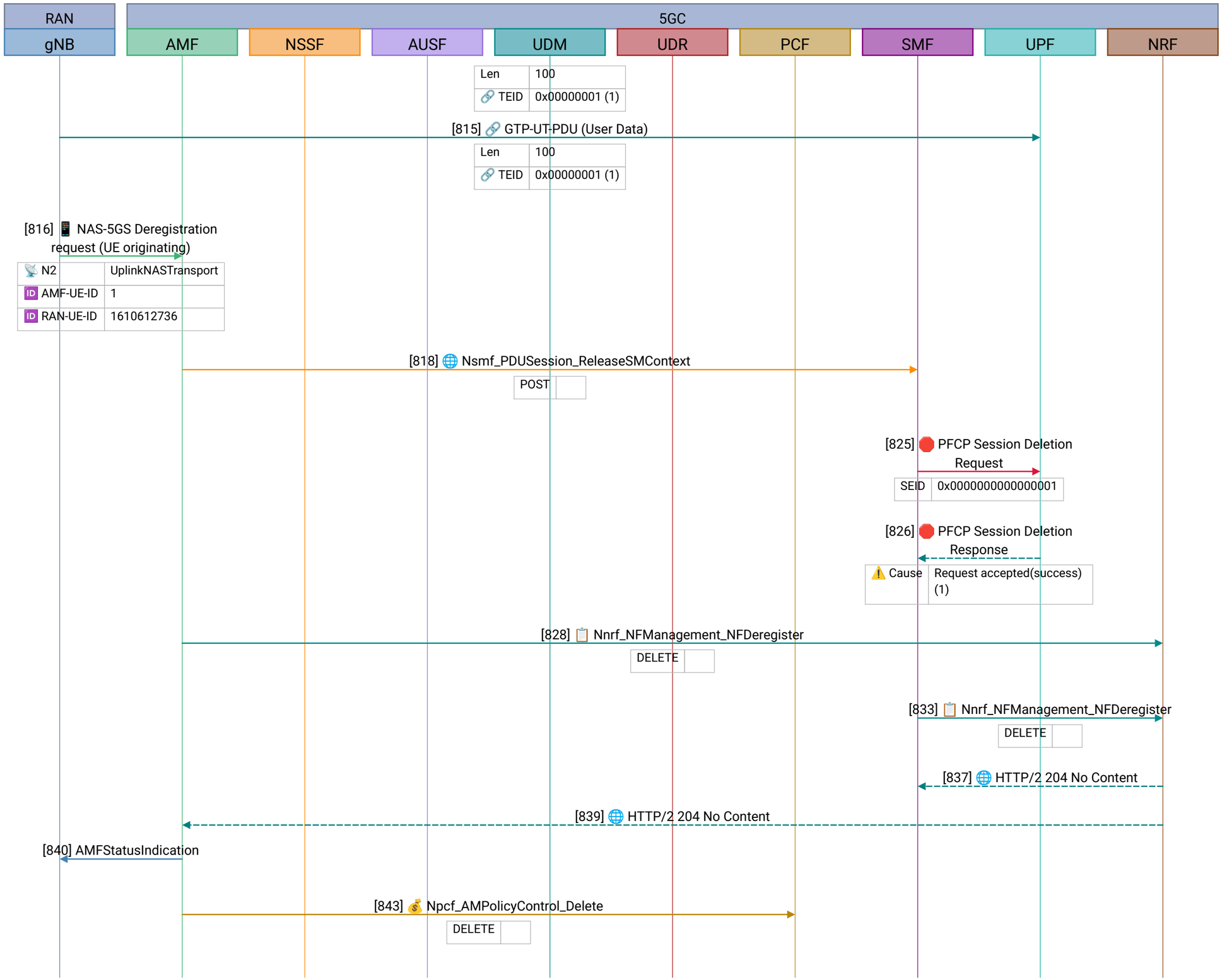
[Frame 808] `200 OK` to the AMF. The control plane is done.

[Frame 811] Phase 7 - user plane on N3. GTP-U T-PDU from the gNB to the UPF on **TEID 1,** the uplink endpoint from frame 773, with QFI 9 in the PDU session container. Inside: ICMP Echo Request from `100.64.50.1` to `8.8.8.8`, identifier `0xABCD`, sequence 28653. One second after the session came up.

[Frame 812] Echo Request, sequence 28654, one second later.

[Frame 813] Echo Request, sequence 28655.

[Frame 814] Echo Request, sequence 28656.



[Frame 815] Echo Request, sequence 28657.

No echo reply appears. All five packets are uplink, and no downlink GTP-U follows. The capture cannot say whether the UPF dropped them or the replies never came back; note the uplink FAR's `Access` destination in frame 773.

[Frame 816] Phase 8 - deregistration. 12 s after the last ping, a **UL NAS Transport** carries **Deregistration Request (UE originating):** normal deregistration (not switch-off), 3GPP access, 5G-GUTI with TMSI 1. Because it is not a switch-off, the UE expects a Deregistration Accept.

[Frame 818] Nsmf_PDUSession_ReleaseSMContext for `urn:uuid:3b25d3e9-...`, with an empty JSON body `{}`.

⚠️ The SMF never answers this request in the capture.

[Frame 825] Even so, the SMF tears down the user plane: **PFCP Session Deletion Request** for SEID 1.

[Frame 826] PFCP Session Deletion Response: `Request accepted.` The tunnel is gone 10 ms after the deregistration request. The HTTP/2 response to the AMF still does not come.

[Frame 828] Phase 9 - shutdown. 24 s of silence, and no Deregistration Accept. Then the AMF deletes its own NRF profile (Nnrf_NFManagement_NFDeregister): the AMF is shutting down.

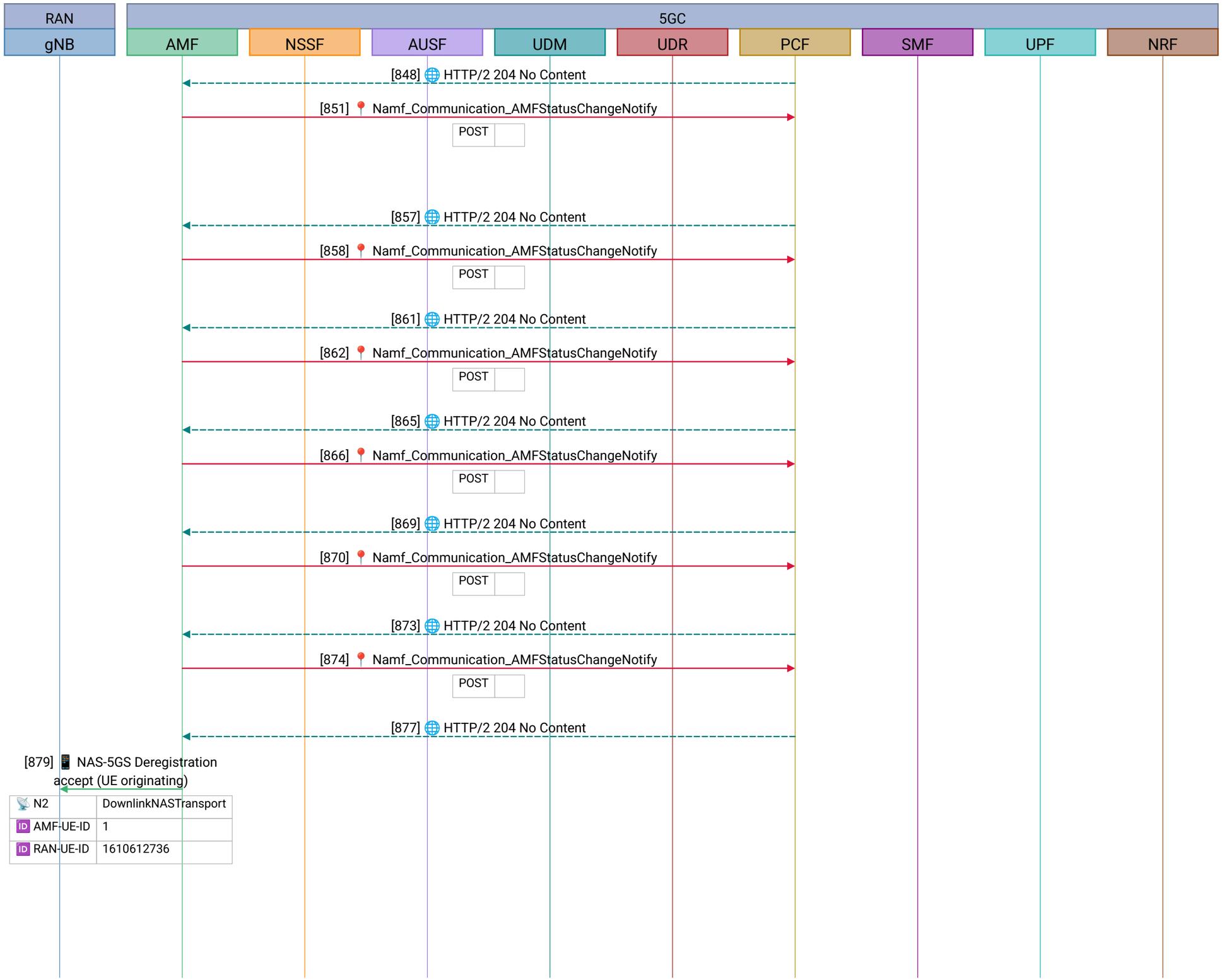
[Frame 833] 2 ms later the SMF deregisters too. The whole core is being stopped.

[Frame 837] `204 No Content` for the SMF, a full second after the request.

[Frame 839] `204 No Content` for the AMF.

[Frame 840] AMF Status Indication to the gNB, listing both GUAMIs as unavailable, so the gNB stops sending new UEs to this AMF.

[Frame 843] Npcf_AMPolicyControl_Delete for policy `imsi-460000012200000-1`, created in frame 608.



[Frame 848] `204 No Content.`

[Frame 851] **Namf_Communication_AMFStatusChangeNotify** to the PCF's callback: `statusChange: AMF_UNAVAILABLE.` Notification 1 of 6, one per subscription accepted in phase 1. The body carries no GUAMI list, so the PCF cannot tell which GUAMI changed.

[Frame 857] `204 No Content.`

[Frame 858] Notification 2 of 6.

[Frame 861] `204.`

[Frame 862] Notification 3 of 6.

[Frame 865] `204.`

[Frame 866] Notification 4 of 6.

[Frame 869] `204.`

[Frame 870] Notification 5 of 6.

[Frame 873] `204.`

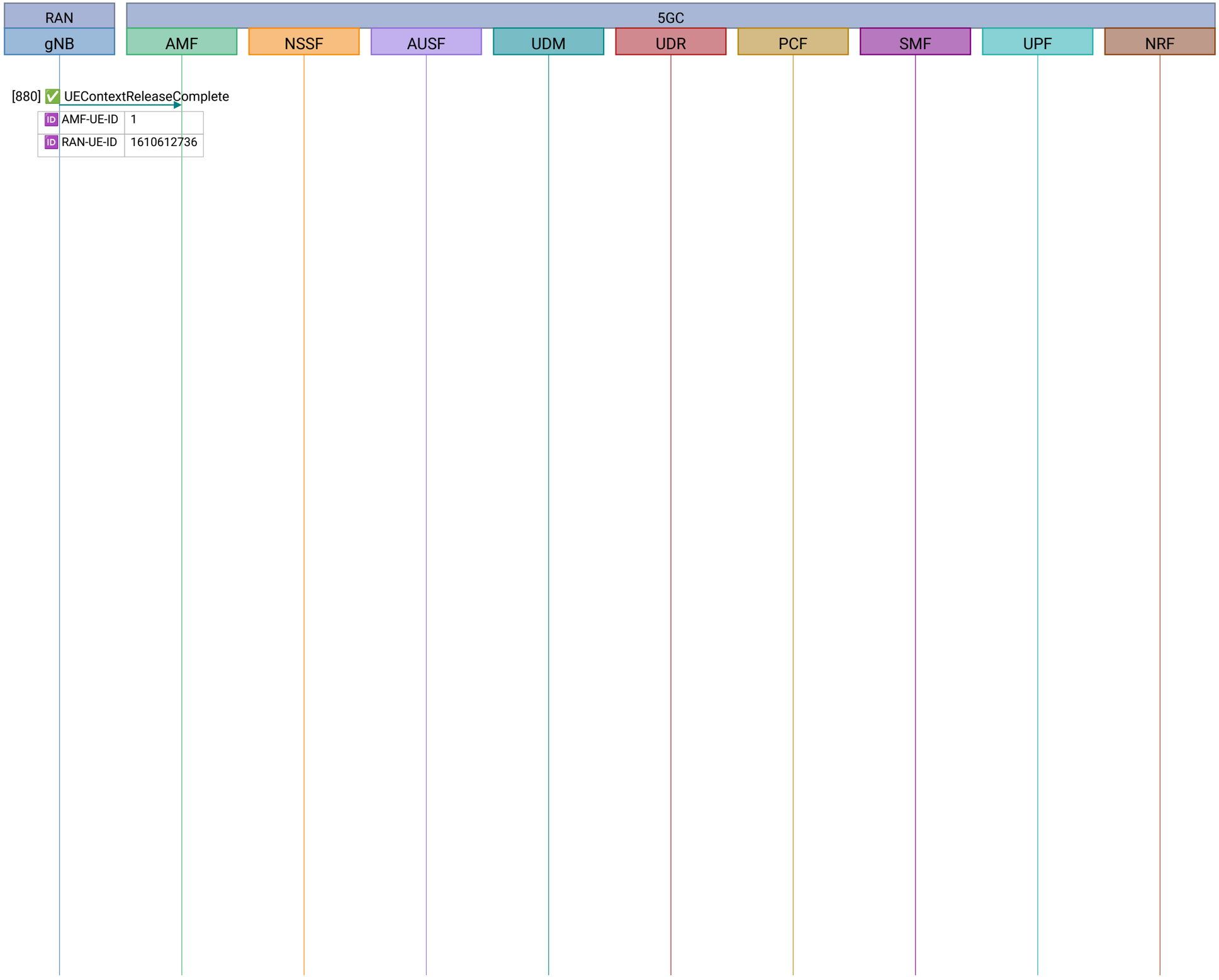
[Frame 874] Notification 6 of 6. Six notifications for one AMF, because the stale NRF profiles produced six subscriptions.

[Frame 877] `204,` the last acknowledgment.

[Frame 879] **Deregistration Accept,** 25 s after the request, sent during the AMF's own shutdown. Per TS 23.502 the AMF sends it after the SM context is released, and the SMF never confirmed that release.

This SCTP packet carries **two** NGAP messages. The arrow shows the first, Downlink NAS Transport with the NAS accept. The second is **UE Context Release Command** with cause `nas: deregister,` which the next message answers.

Never seen in this teardown: Nudm_UECM_Deregistration and Nudm_SDM_Unsubscribe. The UDM still lists this AMF



as serving the UE.

[Frame 880] UE Context Release Complete: the gNB has released the UE. The capture ends here.