5G selected Architecture Themes on 5G New Services Capabilities

to

CNCF TUG

Ike Alisson

LF Edge Akraino TSC member and Documentation Sub-committee TSC Chair

2021-10-04

Rev PA8

Table of Contents

5G White Paper

By NGMN Alliance

Version:	1.0
Date:	17-February-2015
Document Type:	Final Deliverable (Approved)
Confidentiality Class:	P - Public

Project:	NGMN 5G Initiative
Editor / Submitter:	Rachid El Hattachi/ Javan Erfanian
Contributors:	5G Initiative Team
Approved by / Date:	NGMN Board/ 17th of February 2015

1. "5G Network Mobility at "Cell" & "Cloud" Edge - NGMN WP Feb 2015 - 2

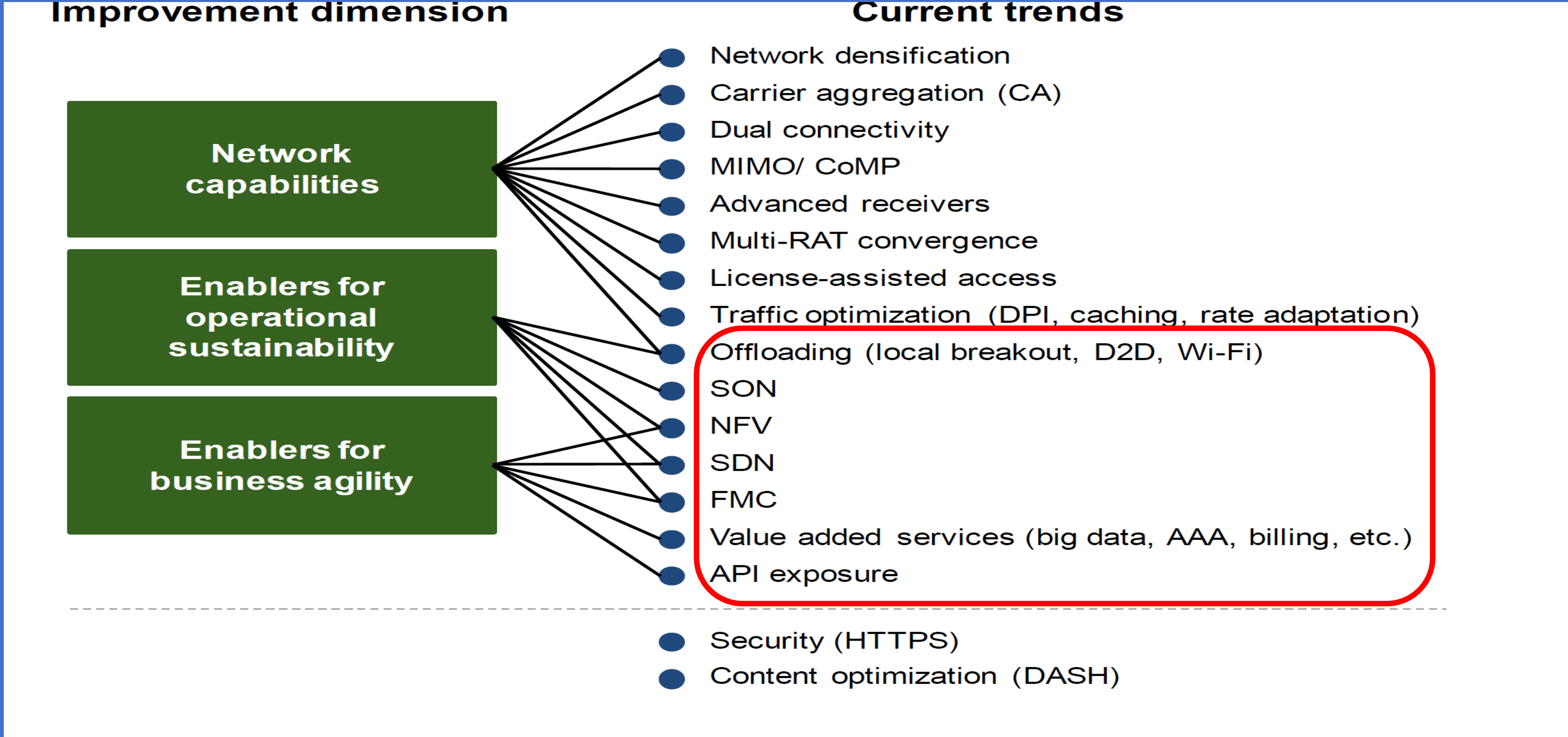


Figure 6: Ongoing technology trends

1. "5G Network Mobility at "Cell" & "Cloud" Edge - NGMN WP Feb 2015 - 3

Radio	Network	Operations & Management
		

Radio

Leverage spectrum
- Exploit higher frequencies and unlicensed spectrum
- C/U-path split, UL/DL split, multiple connectivity

Enable cost-effective dense deployments
- Integrate third party/user deployments
- Automate configuration, optimization and healing
- Enhance multi-RAT coordination
- Support multi-operator/shared use of infrastructure

Coordinate and cancel interference
- Build-in massive MIMO and CoMP
- Exploit controlled non-orthogonal interference

Support dynamic radio topology
- Moving cells, relays, hubs, C-RAN, D-RAN
- D2D (e.g., for latency, disaster relief)

Network

Create common composable core
- Minimize number of entities and functionalities
- C/U-function split, lean protocol stack
- No mandatory U-plane functions
- Minimize legacy interworking
- RAT-agnostic core
- Fixed and mobile convergence

Operations & Management

Simplify operations and management
- Automation and self-healing
- Probeless monitoring
- Collaborative management
- Integrated OAM functionality
- Carrier-grade network cloud orchestration

Embrace flexible functions and capabilities
- Network slicing
- Function variance
- Flexible function/service/application allocation
- Leverage NFV/SDN
- State-disintegrated functions
- Graceful degradation

Support new value creation
- Exploit big data and context awareness
- Expose radio and network APIs
- Facilitate XaaS

Build in security and privacy
- Extend C-plane security (e.g., HetNets)
- Ensure location privacy and identity protection from (unlawful) disclosure

Figure 7: 5G design principles

1. "5G Network Mobility at "Cell" & "Cloud" Edge - NGMN WP Feb 2015 - 4

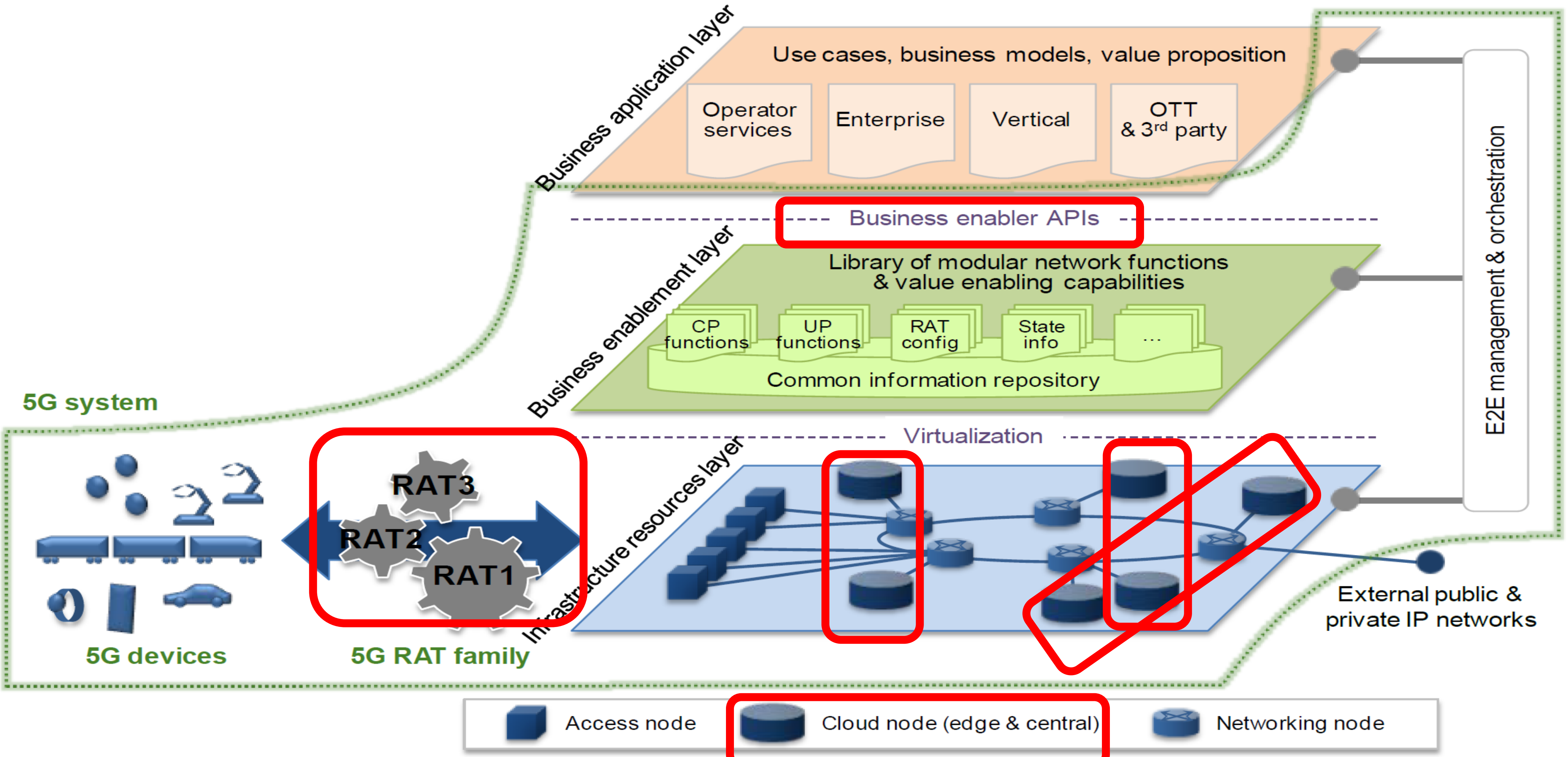


Figure 8: 5G Architecture

1. "5G Network Mobility at "Cell" & "Cloud" Edge - NGMN WP Feb 2015 - 5

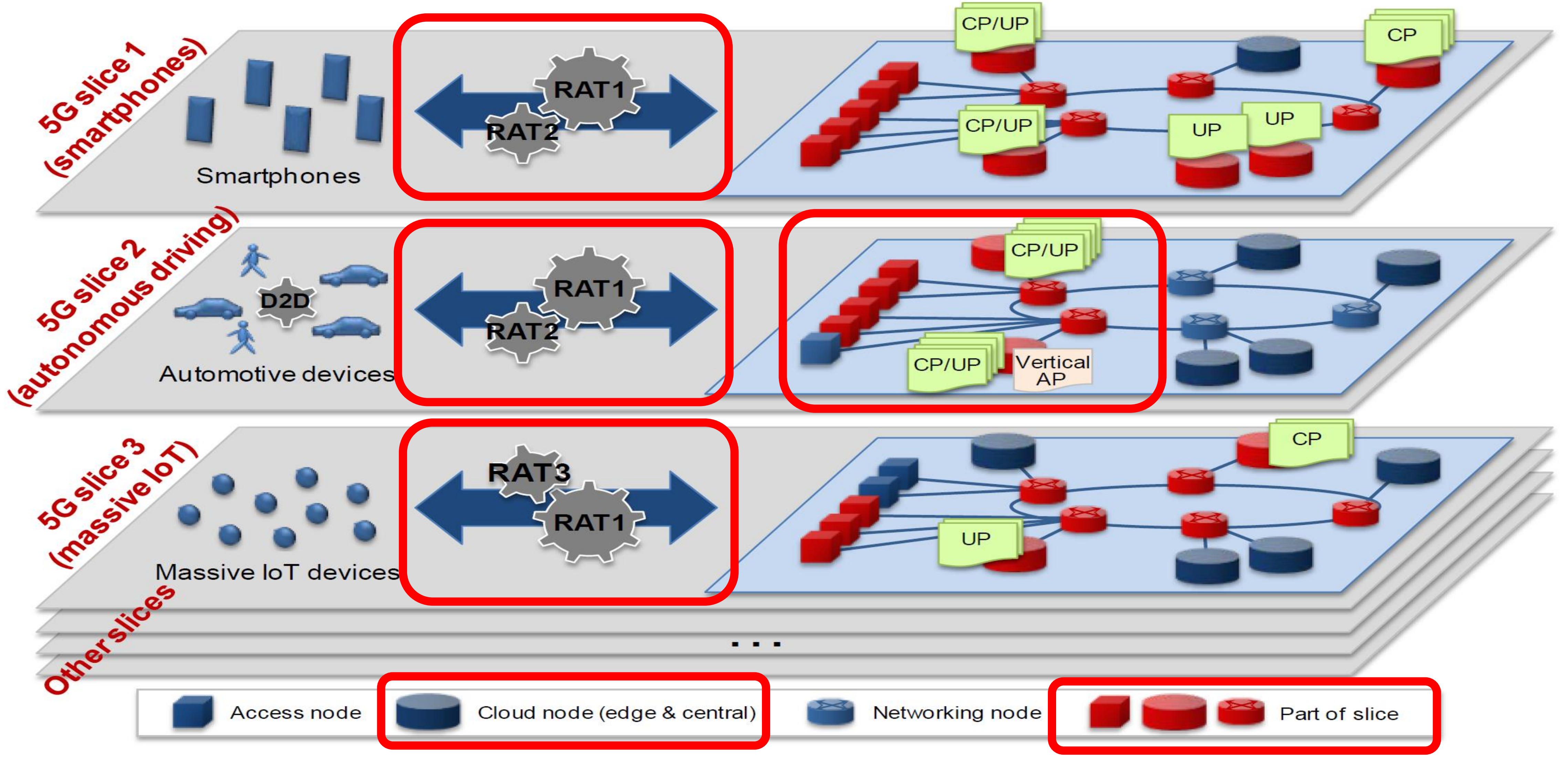


Figure 9: 5G network slices implemented on the same infrastructure

1. "5G Network Mobility at "Cell" & "Cloud" Edge - NGMN WP Feb 2015 - 6

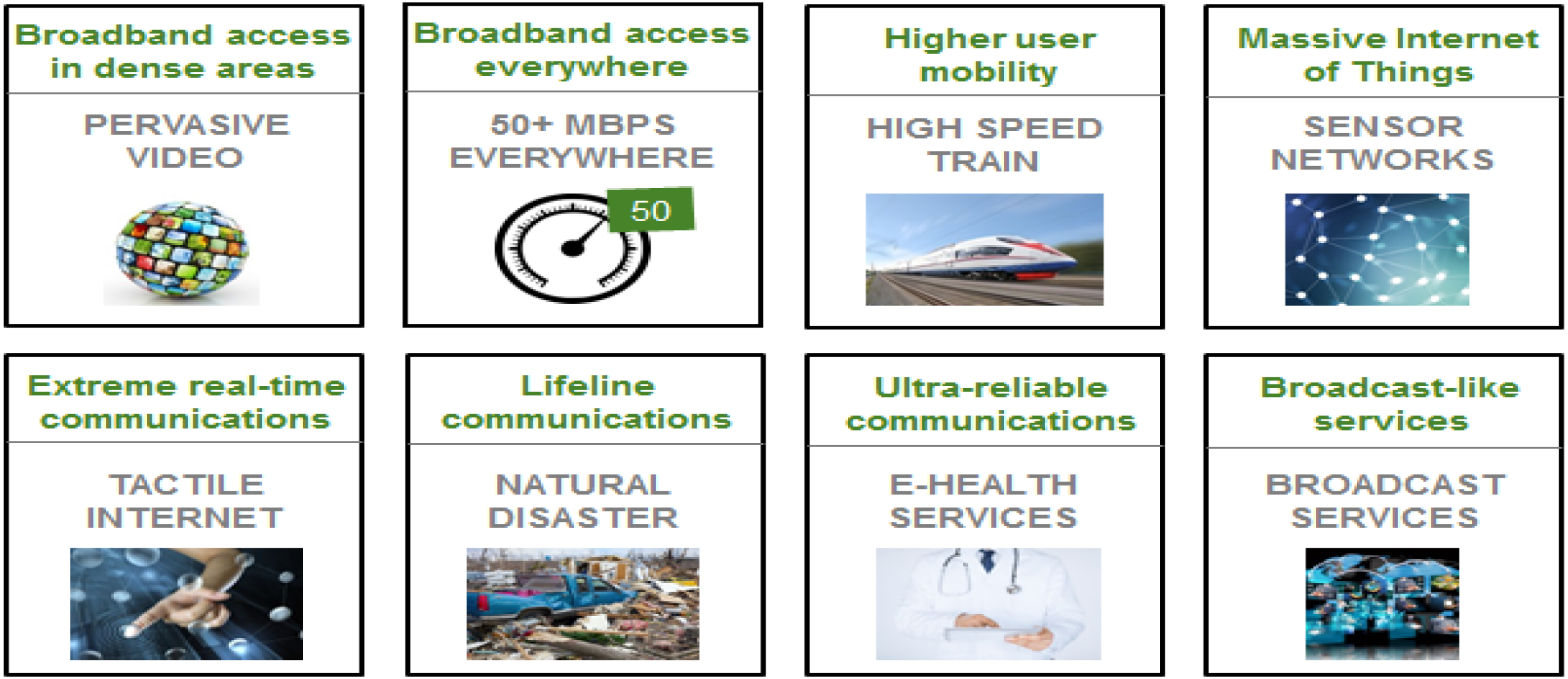


Figure 1: 5G use case families and related examples

1. "5G Network Mobility at "Cell" & "Cloud" Edge - NGMN WP Feb 2015 - 7

Role	Business Models	
Asset Provider	**XaaS: IaaS, NaaS, PaaS** Ability to offer to and operate for a 3rd party provider different network infrastructure capabilities (Infrastructure, Platform, Network) as a Service.	**Network Sharing** Ability to share Network infrastructure between two or more Operators based on static or dynamic policies (e.g. congestion/excess capacity policies)
Connectivity Provider	**Basic Connectivity** Best effort IP connectivity in retail (consumer/business) & wholesale/MVNO	**Enhanced Connectivity** IP connectivity with differentiated feature set (QoS, zero rating, latency, etc..) and enhanced configurability of the different connectivity characteristics.
Partner Service Provider	**Operator Offer Enriched by Partner** Operator offering to its end customers, based on operator capabilities (connectivity, context, identity etc.) enriched by partner capabilities (content, application, etc..)	**Partner Offer Enriched by Operator** Partner offer to its end customers enriched by operator network and other value creation capabilities (connectivity, context, identity etc.)

Figure 2: 5G Business models - Examples

1. "5G Network Mobility at "Cell" & "Cloud" Edge - NGMN WP Feb 2015 - 8

5G

4.1.5 User Experience KPI's

Table 1: User Experience Requirements

Use case category	User Experienced Data Rate	E2E Latency	Mobility
Broadband access in dense areas	DL: 300 Mbps UL: 50 Mbps	10 ms	On demand, 0-100 km/h
Indoor ultra-high broadband access	DL: 1 Gbps, UL: 500 Mbps	10 ms	Pedestrian
Broadband access in a crowd	DL: 25 Mbps UL: 50 Mbps	10 ms	Pedestrian
50+ Mbps everywhere	DL: 50 Mbps UL: 25 Mbps	10 ms	0-120 km/h
Ultra-low cost broadband access for low ARPU areas	DL: 10 Mbps UL: 10 Mbps	50 ms	on demand: 0-50 km/h
Mobile broadband in vehicles (cars, trains)	DL: 50 Mbps UL: 25 Mbps	10 ms	On demand, up to 500 km/h
Airplanes connectivity	DL: 15 Mbps per user UL: 7.5 Mbps per user	10 ms	Up to 1000 km/h
Massive low-cost/long-range/low-power MTC	Low (typically 1-100 kbps)	Seconds to hours	on demand: 0-500 km/h
Broadband MTC	See the requirements for the Broadband access in dense areas and 50+Mbps everywhere categories		
Ultra-low latency	DL: 50 Mbps UL: 25 Mbps	<1 ms	Pedestrian
Resilience and traffic surge	DL: 0.1-1 Mbps UL: 0.1-1 Mbps	Regular communication: not critical	0-120 km/h
Ultra-high reliability & Ultra-low latency	DL: From 50 kbps to 10 Mbps; UL: From a few bps to 10 Mbps	1 ms	on demand: 0-500 km/h
Ultra-high availability & reliability	DL: 10 Mbps UL: 10 Mbps	10 ms	On demand, 0-500 km/h
Broadcast like services	DL: Up to 200 Mbps UL: Modest (e.g. 500 kbps)	<100 ms	on demand: 0-500 km/h

2. ETSI MEC re-named in March 2017 & 3GPP 5G NSA Rel. 15 Mobility - 1

ETSI Multi-access Edge Computing (MEC) starts 2nd Phase & Renews Leadership Team

*Sophia Antipolis, **28 March 2017***

https://www.etsi.org/newsroom/news/1180-2017-03-news-etsi-multi-access-edge-computing-starts-second-phase-and-renews-leadership-team

ETSI's MEC ISG has

1. **Renamed MEC** to **Multi-access Edge Computing** to better reflect Non-Cellular Operators' Requirements.

2. **A New Leadership** Team: Alex Reznik new Chair

3. A **New Scope** to address:
   - **multiple MEC Hosts**
   - **different Networks**
   - **Edge Applications in a Collaborative Manner.**

2. ETSI MEC re-named in March 2017 & 3GPP 5G NSA Rel. 15 Mobility - 2

1. **’Mobility” Paterns Re-defined/Diversified - UEs categorized/defined as:**
    1. **Stationary** during their entire usable life (e.g., sensors embedded in infrastructure)
    2. **Nomadic during Active Periods**, but Stationary **between activations** (e.g., Fixed Access)
    3. **Mobile within a Constrained & Well-Defined Space/Area**
       (**Spatially Restricted** e.g., in a Factory or Stadion or Airport),
    4. **Fully Mobile (WAN)**.

IP Anchor Node & UE - Relay - deployed at the "Edge" for
- 5G Network Traffic offloading onto traditional IP Routing Networks

- as UE moves, changing the **IP Anchor Node** needed in order to reduce
    - IP Traffic Load,
    - End-to-End latency
    - Better User Experience

- Seamless access to both 3PGG and non - 3GPP Network Access Technology
(e.g WiFi, Bluetooth, Ethernet &..)

- Dynamic Subscriber Management via
  GSMA Standardised eUICC OTA Platform (SM-DP & SM-SR Platform)

5GS Network Capabilities (UPF) & MEC Integration

1. MEC & the **local UPF collocated with the eNB/gNB Base Station**
2. MEC collocated with **a Transmission Node, possibly with a local UPF**
3. MEC & the **local UPF collocated with a Network Aggregation Point**
4. MEC collocated with the **CN Functions (i.e. in the same DC)**

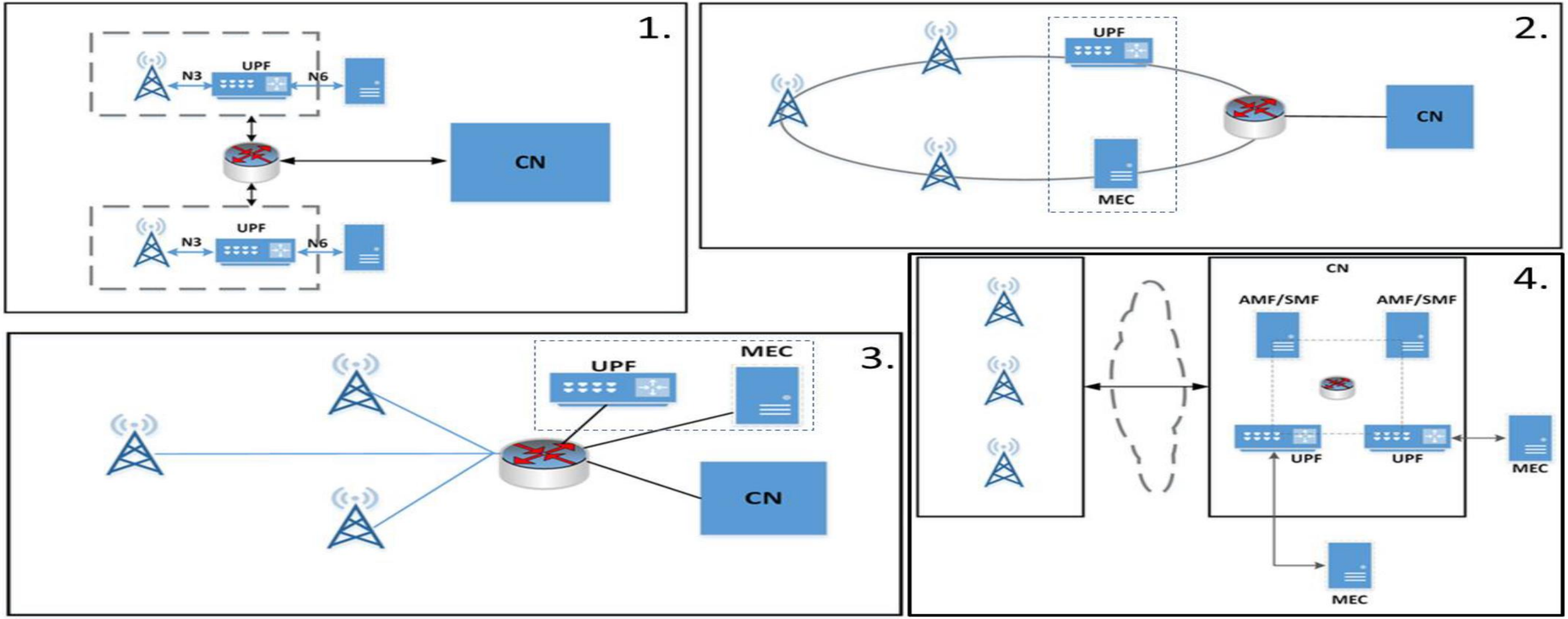
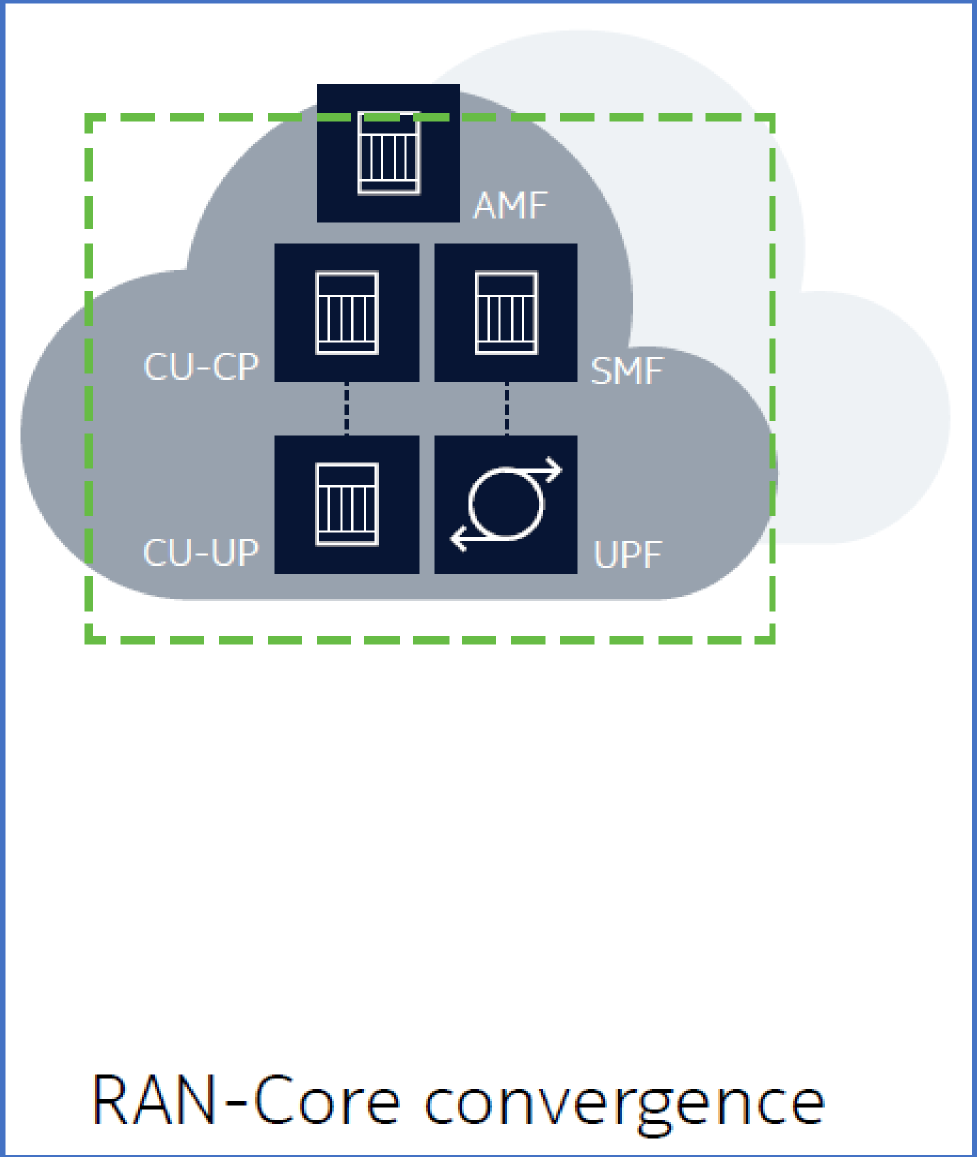
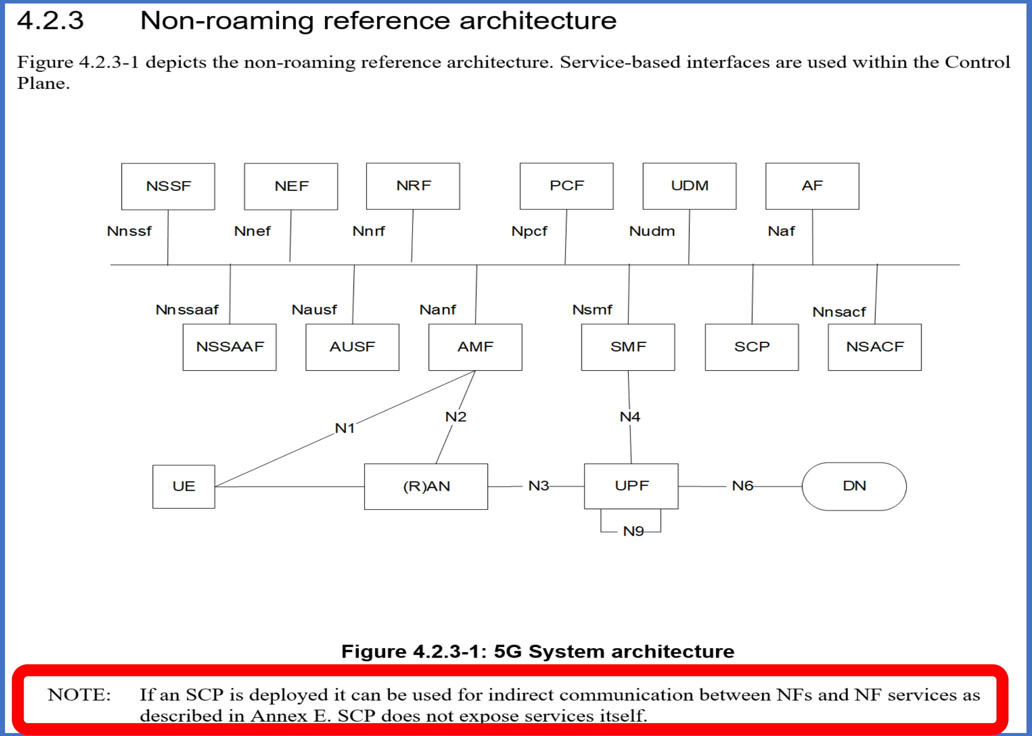


Figure 3. Examples of the physical deployment of MEC.

2. RAN Core Convergence via CUPS implementation





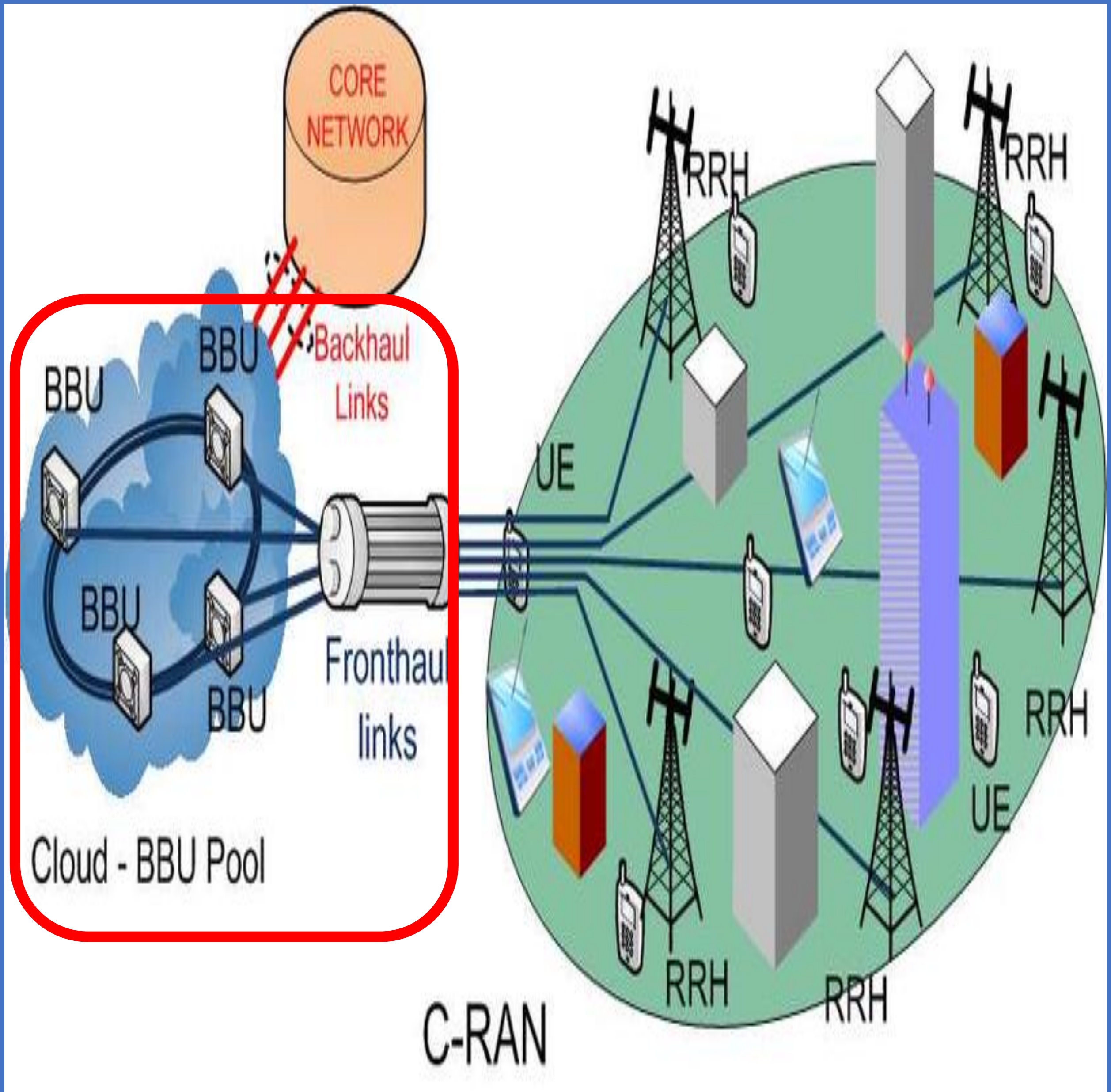
4.2.3 Non-roaming reference architecture

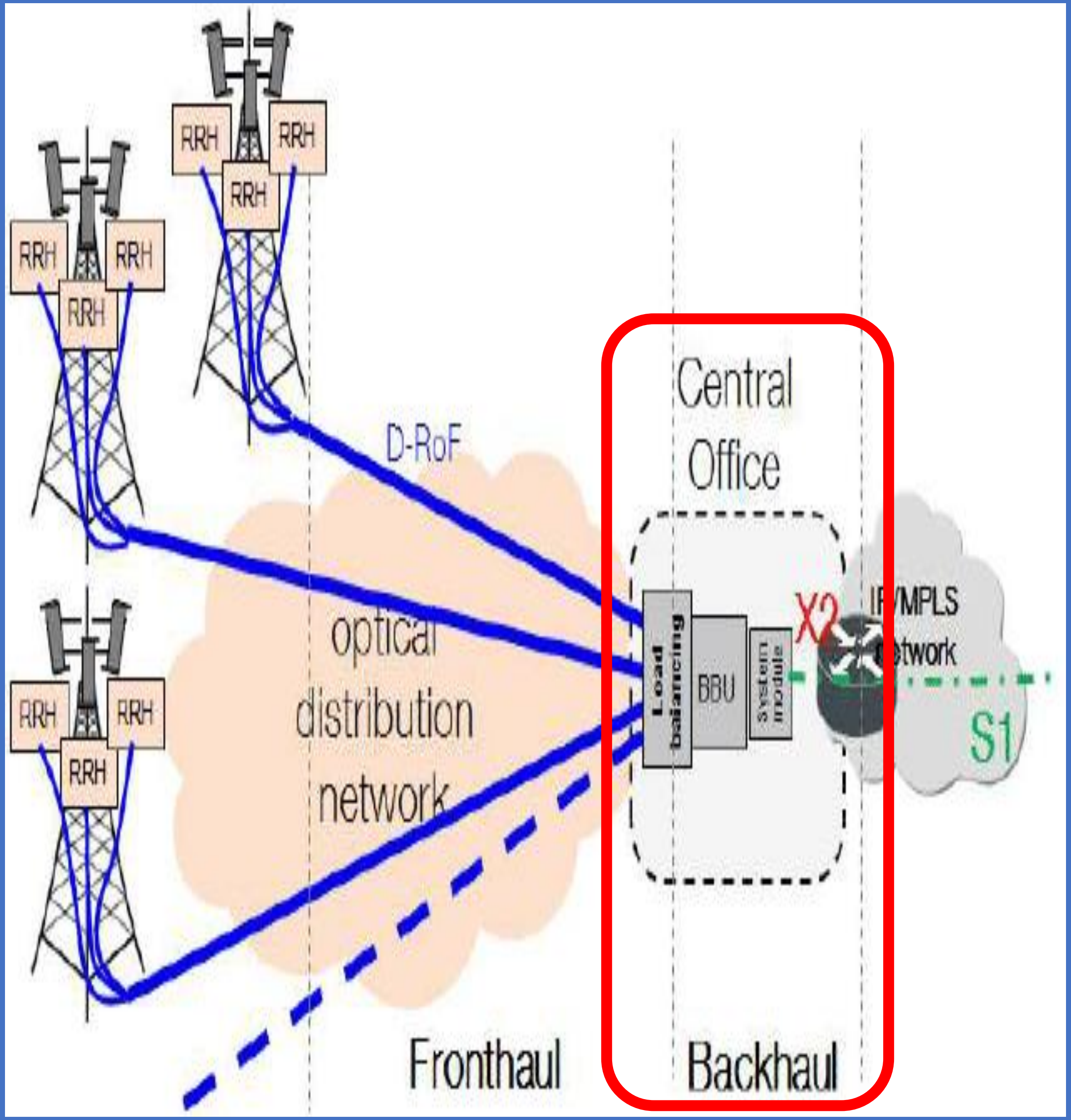
Figure 4.2.3-1 depicts the non-roaming reference architecture. Service-based interfaces are used within the Control Plane.

Figure 4.2.3-1: 5G System architecture

NOTE: If an SCP is deployed it can be used for indirect communication between NFs and NF services as described in Annex E. SCP does not expose services itself.

C-RAN


CORE NETWORK
Backhaul Links
BBU
BBU
BBU
BBU
Fronthaul links
Cloud - BBU Pool
UE
RRH
RRH
RRH
UE
RRH
RRH
C-RAN

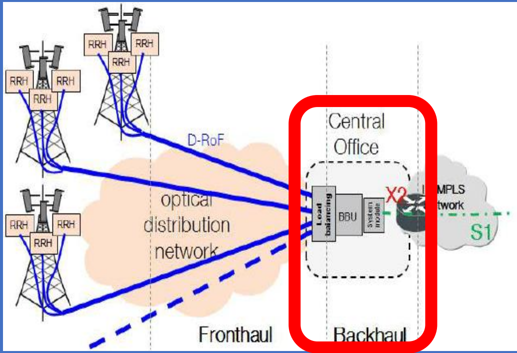

RRH
RRH
RRH
RRH
RRH
RRH
RRH
RRH
RRH
D-RoF
optical distribution network
Central Office
Load balancing
BBU
System module
X2
IP/MPLS network
S1
Fronthaul
Backhaul

3GPP RAN gNB DU and CU Functional Split:

3GPP has also defined a functional split [13] inside the gNB with 2 components: the DU (Distributed Unit) and the CU (Centralized Unit), communicating via a standard interface F1.

The CU can also be split in 2 entities: a CU-C for CP and a CU-U for UP.

This architecture allows for the RAN to be more and more virtualized and a number of functions to run in the Cloud, either close to the Antenna on Edge Location if low latency is being required, or further down in more Centralized Data Centre with different Split Options between Central unit (CU) and Distributed Unit (DU).



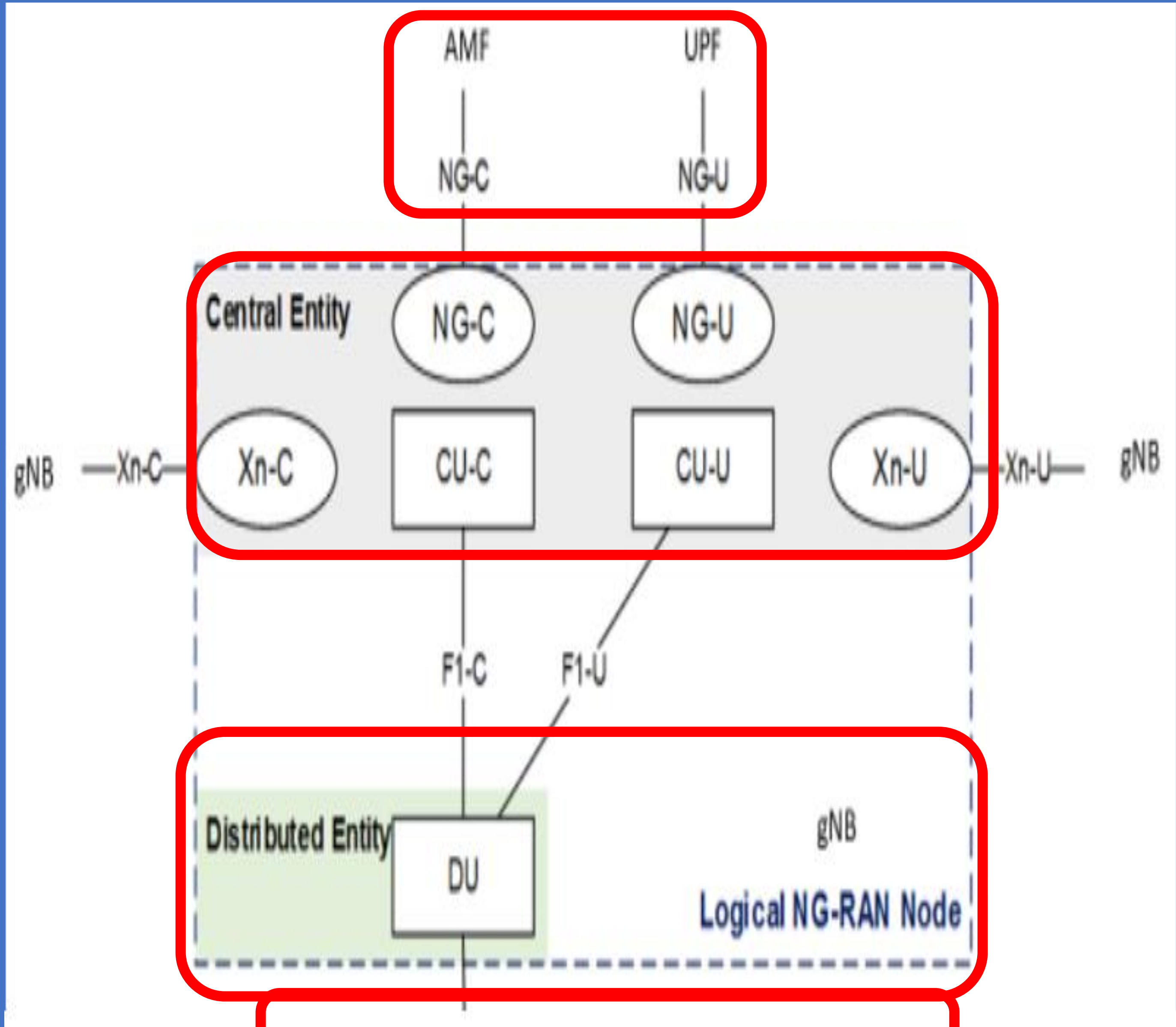


Figure 14: 3GPP DU CU Functional Split

3GPP has defined the Architecture of the 5G Next Generation RAN (NG-RAN) with a Reference Architecture as described below with 2 keys Components:

- A gNB may consist of a gNB-CU and 1 or more gNB-DU(s). A gNB-CU and a gNB-DU is connected via F1 interface.
  One gNB-DU is connected to only one gNB-CU.

- gNB, providing 5G NR User Plane (UP) and Control Plane (CP) protocol terminations towards the UE

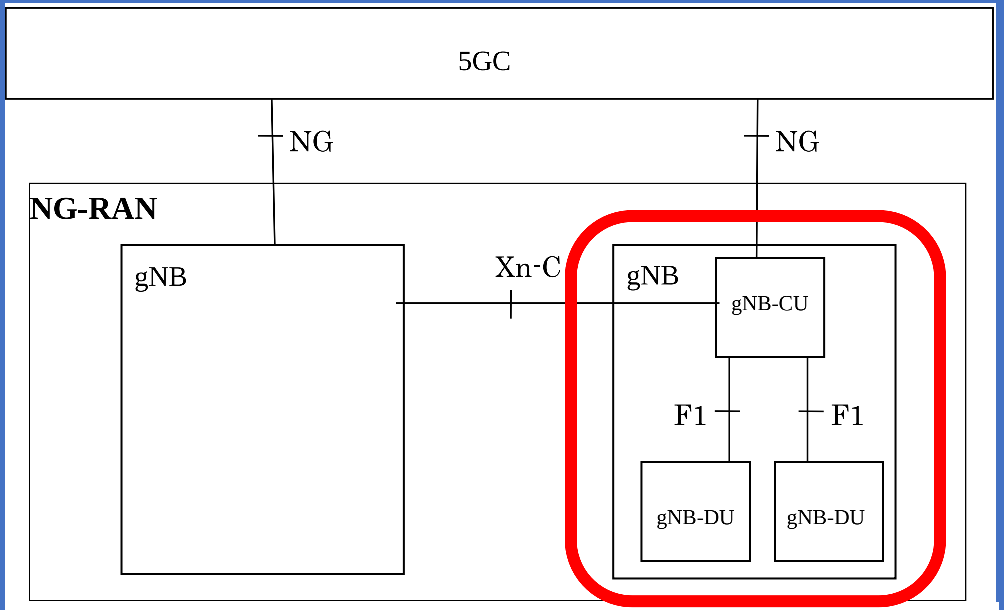


Figure 6.1-1: NG RAN Overall architecture

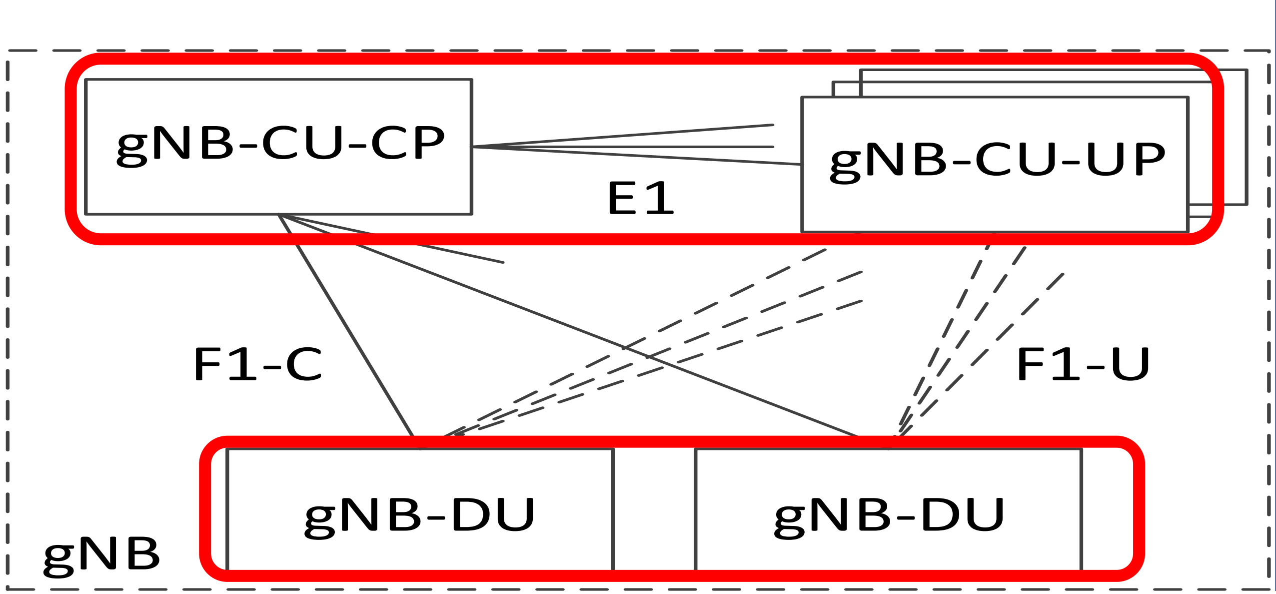


Figure 6.1.2-1. Overall architecture for separation of gNB-CU-CP and gNB-CU-UP

O-RAN ALLIANCE

O-RAN Specifications are built based on the 3GPP Specifications by defining Interface Profiles, Additional New Open Interfaces, and New Nodes, in three (3) RAN Areas: Disaggregation, Automation, and Virtualization.

One of the Key New Interfaces standardized by O-RAN is Open Interface of Fronthaul (FH), connection between RU (Radio Unit) and DU (Distributed Unit).

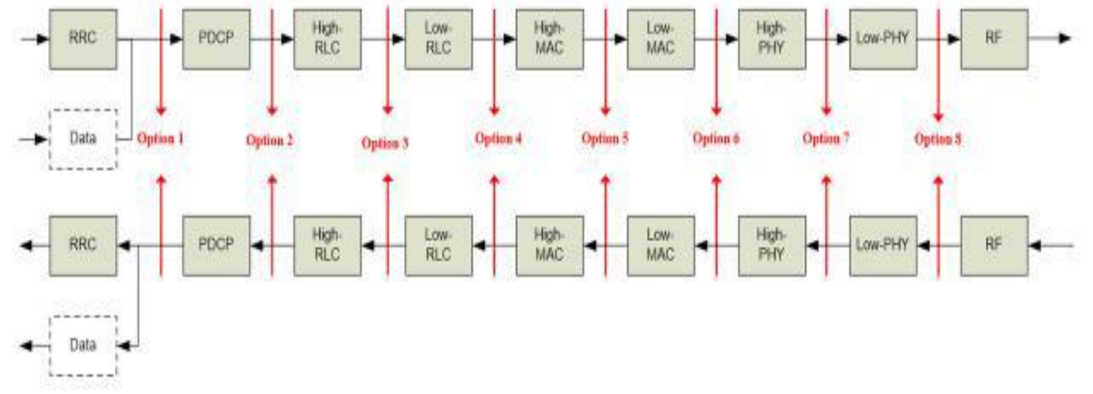


Figure 15: RAN Split Option

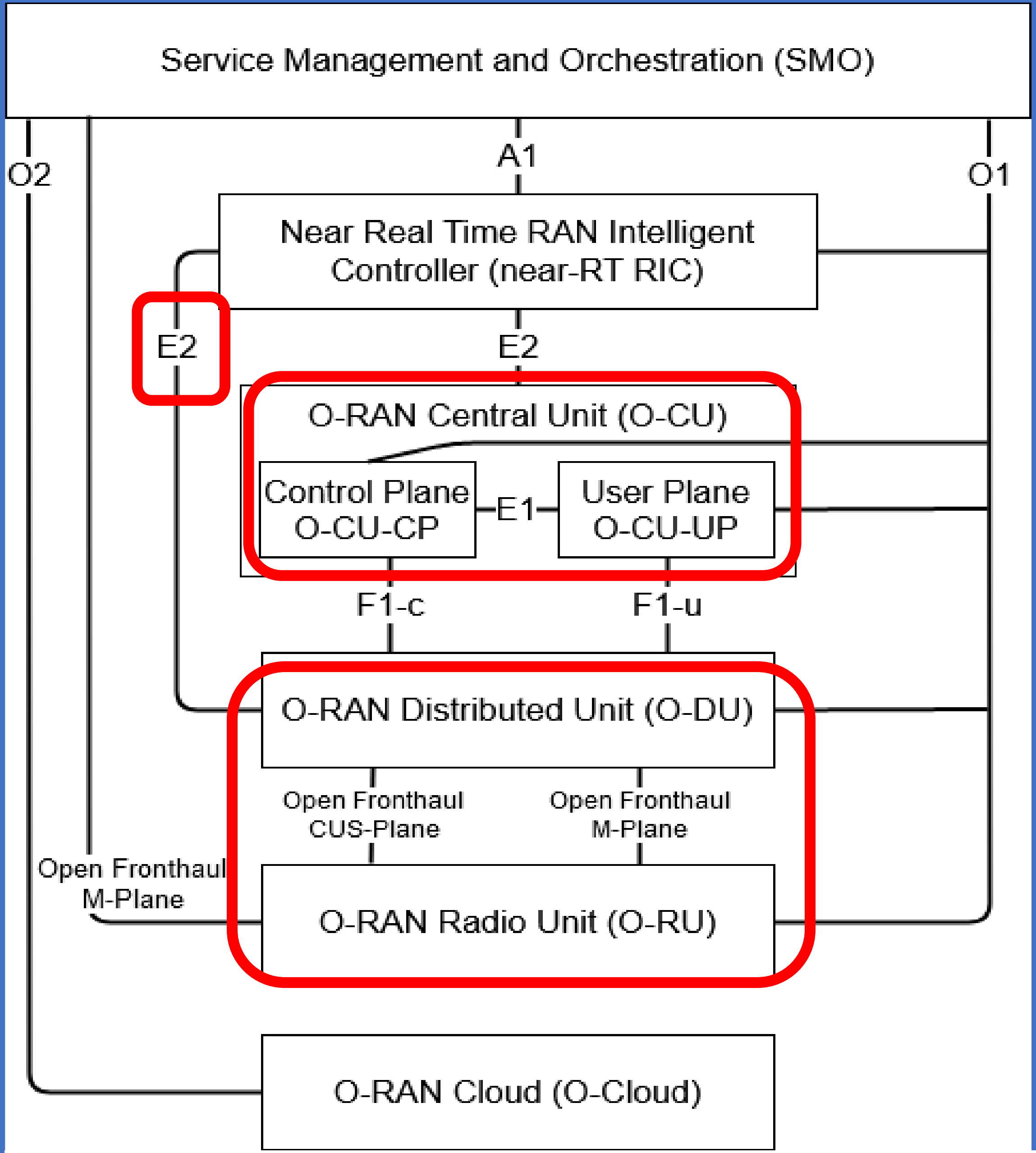


Figure 16: Logical architecture of O-RAN

O-RAN Alliance Control Loops: Non/Near/Real-time Control Loops

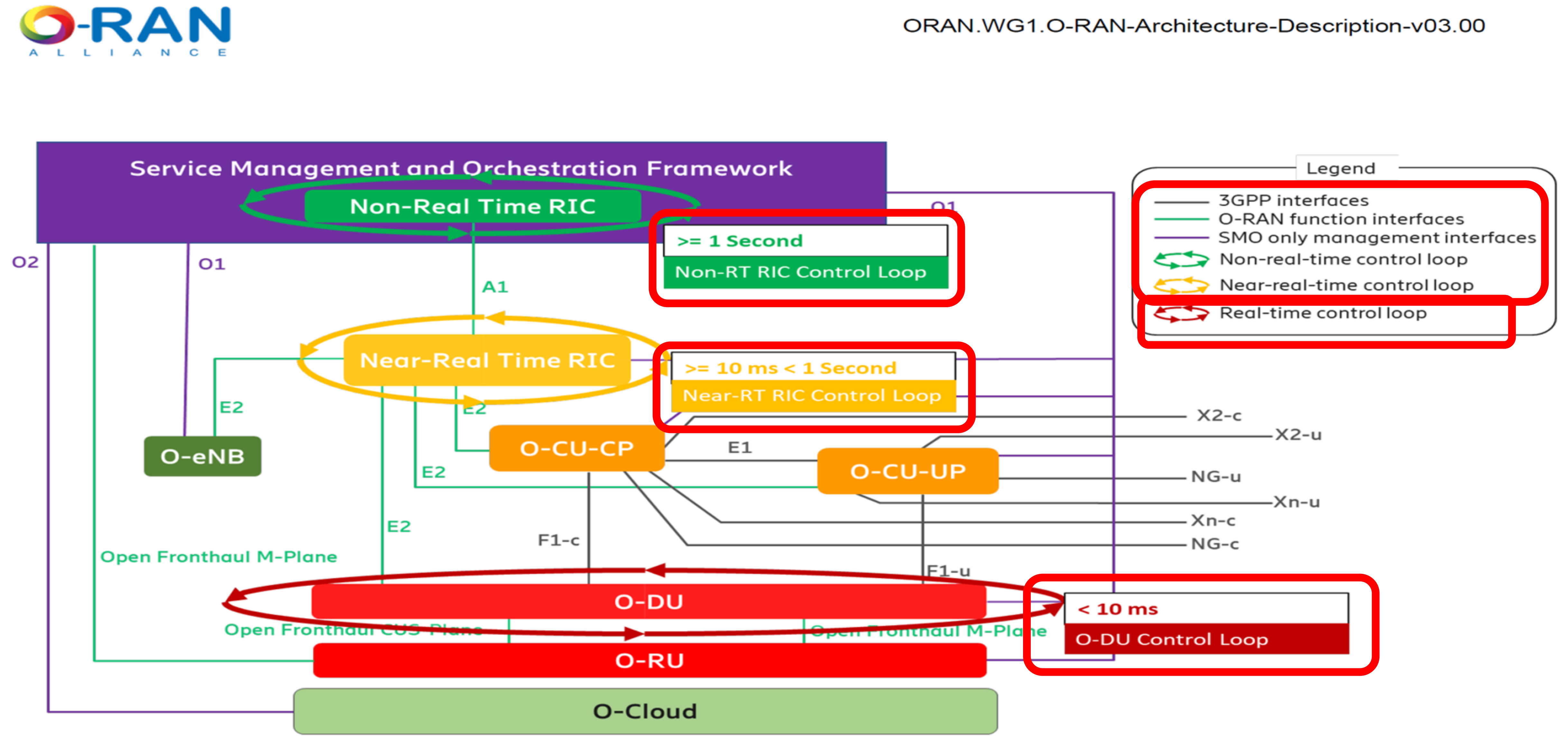
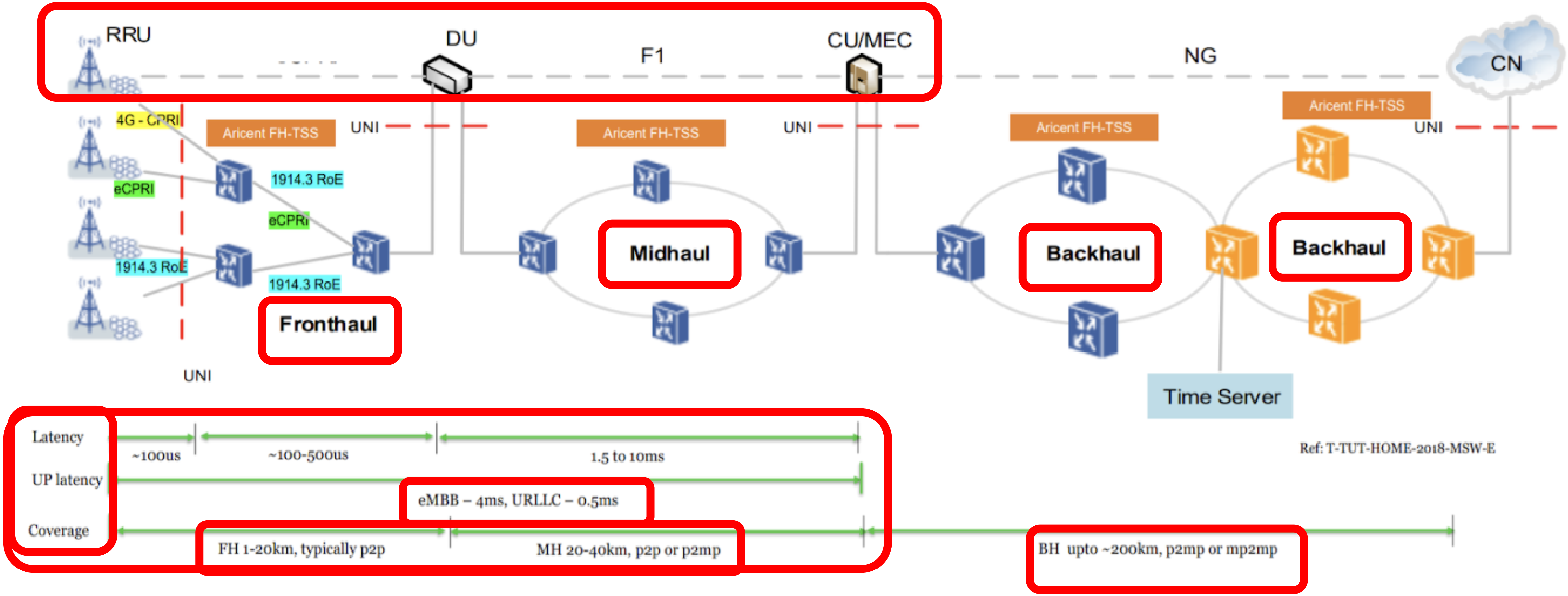


Figure 4.2-1: O-RAN Control Loops

RAN Latency and Distance in FH, MH, BH



- ✓ Fronthaul – Network between RRU/RU (Remote Unit) and DU (Distributed Unit) – can be CPRI or eCPRI or IEEE 1914.3
- ✓ Midhaul – Network between DU and CU (Centralized Unit) – "F interface"
- ✓ Backhaul – Network between CU and 5G NGC (and EPC)

Source: Altran (Aricent)

1. 3GPP 5G System Idle Inactive Connected

Figure 4.2.1-1 not only provides an overview of the RRC states in E-UTRA/EPC, but also illustrates the Mobility support between E-UTRA/EPC, UTRAN and GERAN.

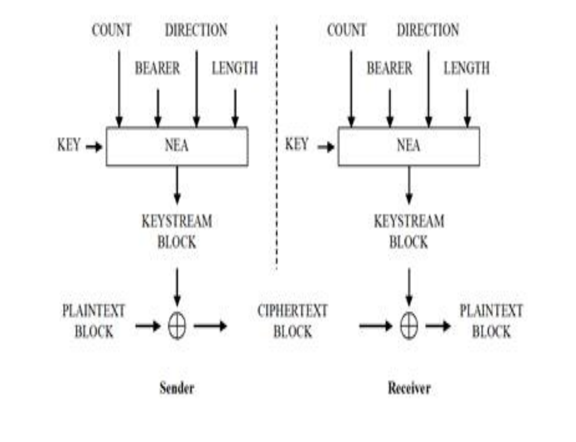


Figure D.2.1.1-1: Ciphering of data

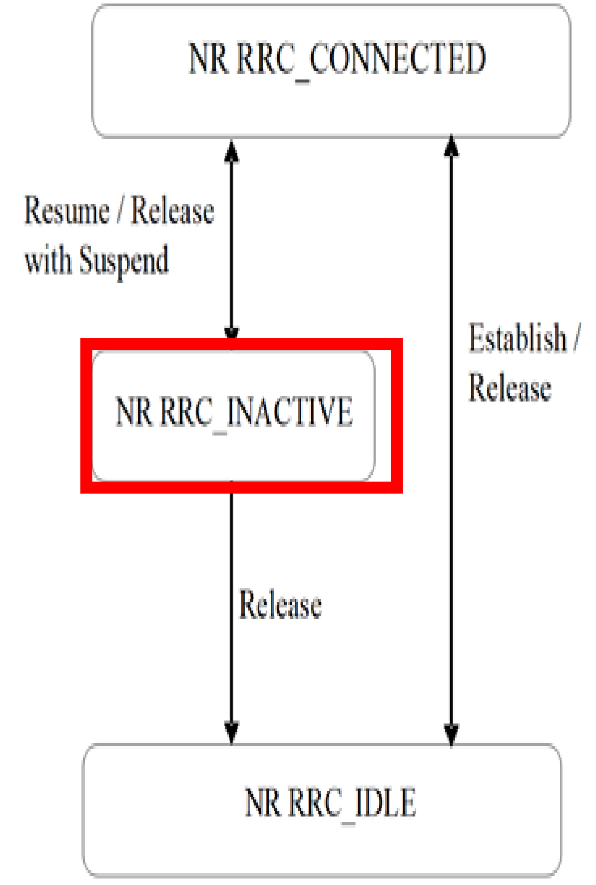


Figure 4.2.1-1: UE state machine and state transitions in NR

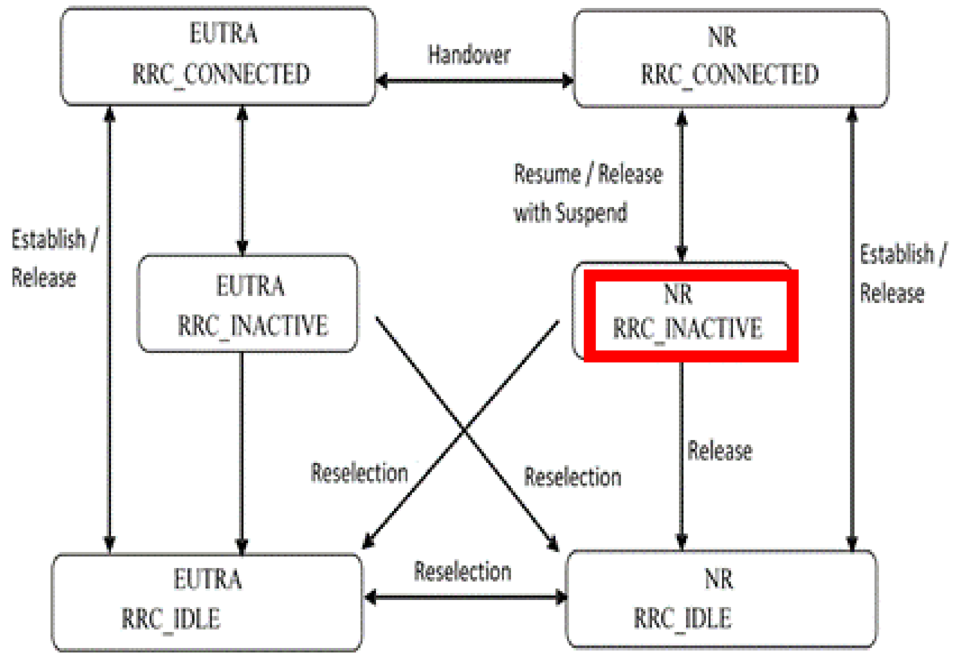


Figure 4.2.1-2: UE state machine and state transitions between NR/5GC, E-UTRA/EPC and E-UTRA/5GC

1. 3GPP 5G System Idle Inactive Connected States

Figure 4.2.1-3 not only provides an overview of the RRC states in E-UTRA/5GC, but also illustrates the mobility support between E-UTRA/5GC, UTRAN and GERAN.

UE states and state transitions including inter RAT

A UE is in RRC_CONNECTED when an RRC connection has been established or in RRC_INACTIVE (if the UE is connected to 5GC) when RRC connection is suspended. If this is not the case, i.e. no RRC connection is established, the UE is in RRC_IDLE state. The RRC states can further be characterised as follows:

RRC_INACTIVE:

- A UE specific DRX may be configured by upper layers or by RRC layer;

- A RAN-based Notification Area (RNA) is configured by RRC layer;

- The UE stores the UE Inactive AS Context;

- The UE:

- Applies RRC_IDLE procedures unless specified otherwise;

- **Monitors a Paging channel for CN Paging using 5G-S-TMSI and RAN paging using fullI-RNTI;**

- Performs periodic RAN-based Notification Area (RNA) update;

- Performs RAN-based notification area update when moving out of the configured RAN-based notification area.

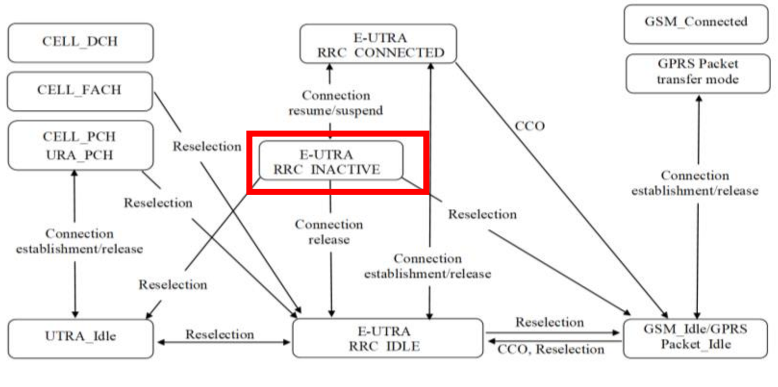


Figure 4.2.1-3: E-UTRA/5GC states and inter RAT mobility procedures, 3GPP

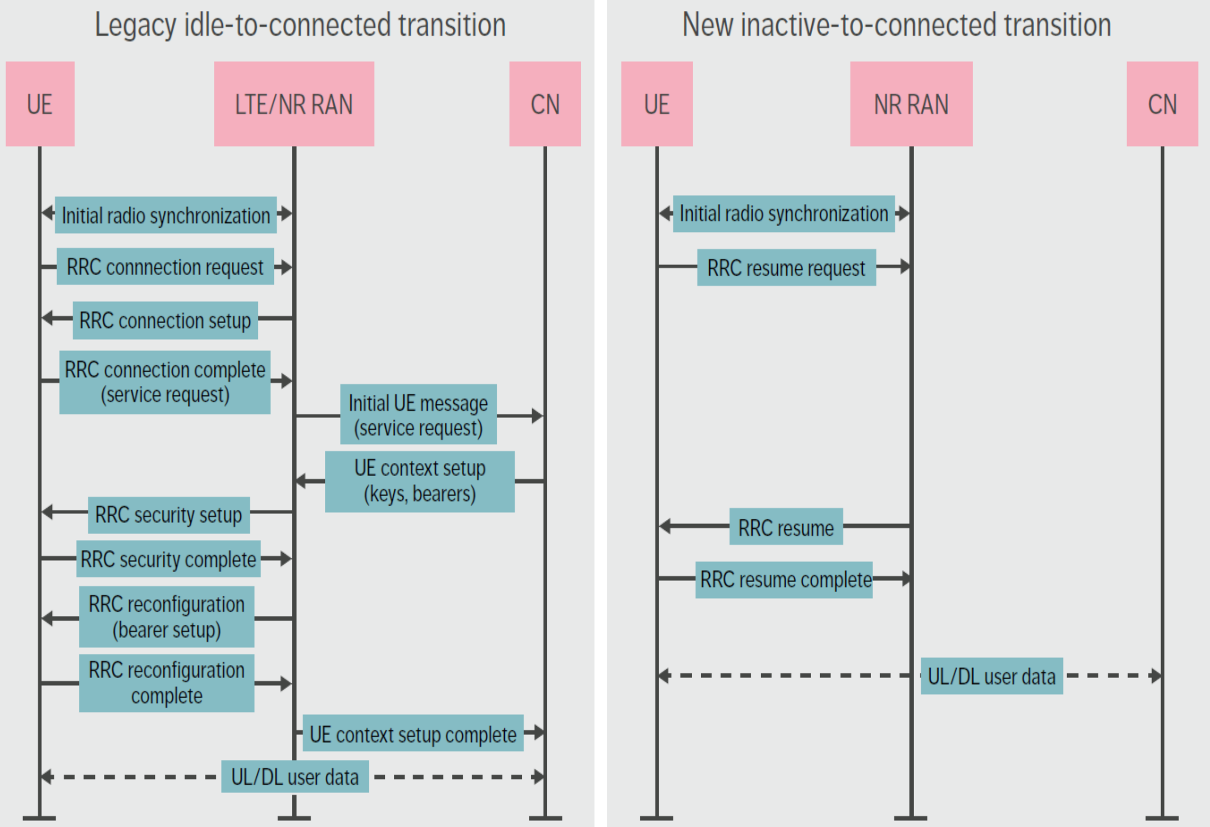


Figure 2 Comparison of Signalling involved in Legacy Idle-to-Connected transition (Left) versus Inactive-to-Connected Transition (Right)

UE Route Selection Policy (URSP)

The URSP is defined and is a set of one or more URSP rules, where a URSP rule is composed of:

a) A precedence value of the URSP rule identifying the precedence of the URSP rule among all the existing URSP rules;

b) A traffic descriptor, including either:

1) match-all traffic descriptor; or

2) at least one of the following components:

A) one or more application identifiers;

B) one or more IP 3 tuples i.e. the destination IP address, the destination port number, and the protocol in use above the IP;

C) one or more non-IP descriptors, i.e. destination information of non-IP traffic;

D) one or more DNNs;

E) one or more connection capabilities; and

F) one or more domain descriptors, i.e. destination FQDN(s) or a regular expression as a domain name matching criteria; and

c) one or more route selection descriptors each consisting of a precedence value of the route selection descriptor and either

1) one PDU session type and, optionally, one or more of the followings:

A) SSC mode;

B) 1 or more S-NSSAIs;

C) 1 or more DNNs;

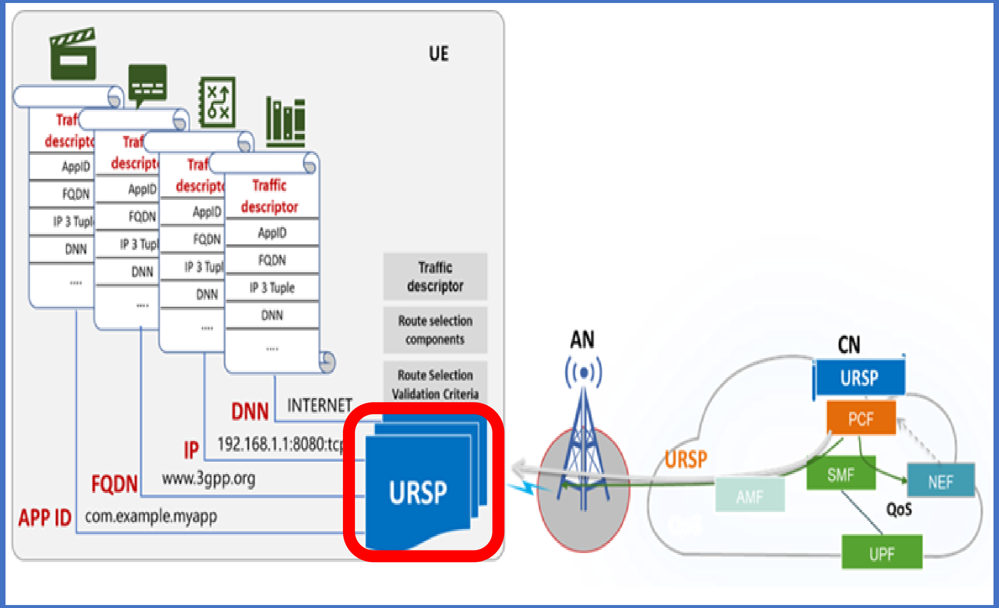
D) Void;

E) preferred Access Type;

F) Multi-Access Preference;

G) a Time Window; and

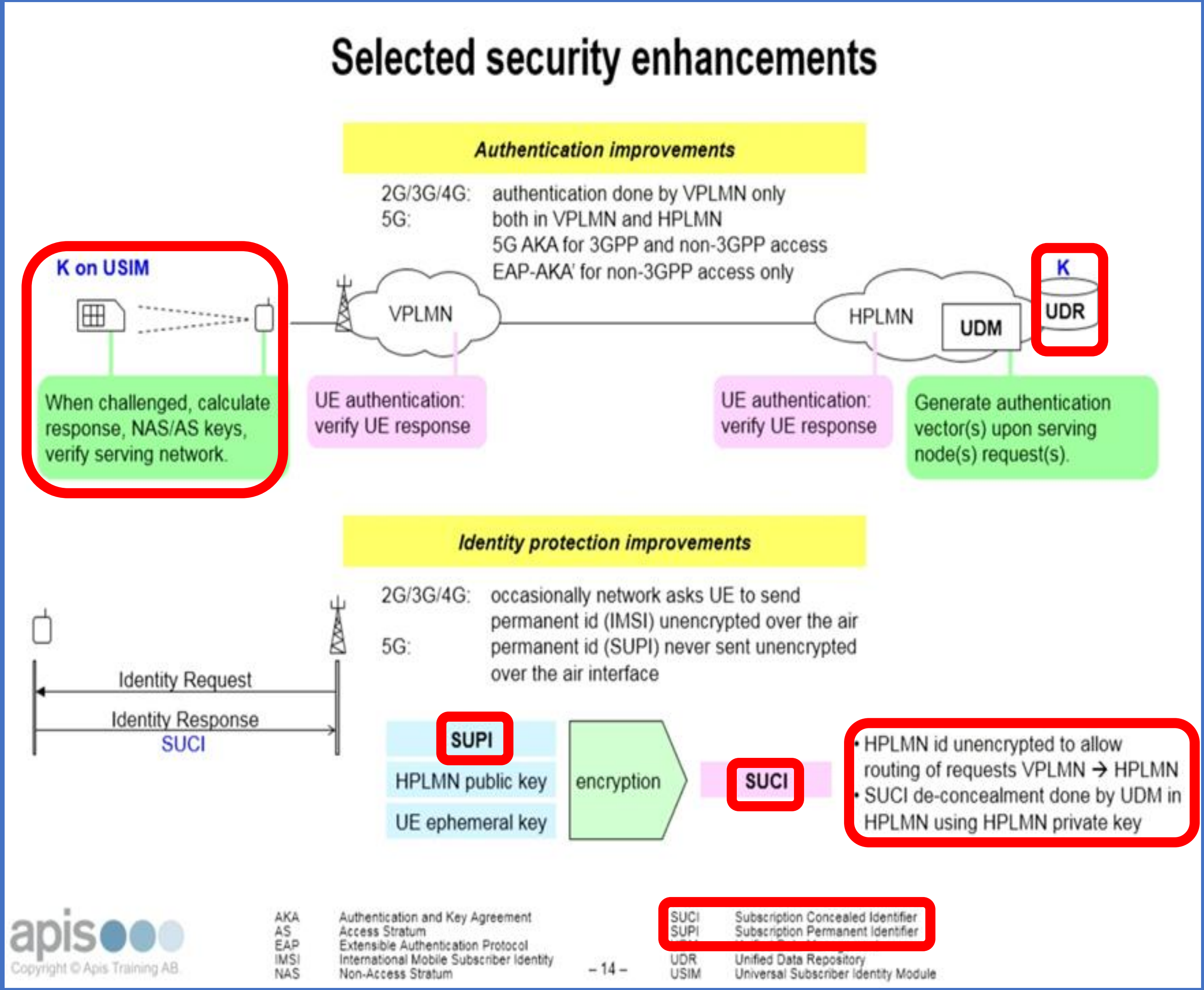
H) Location Criteria;

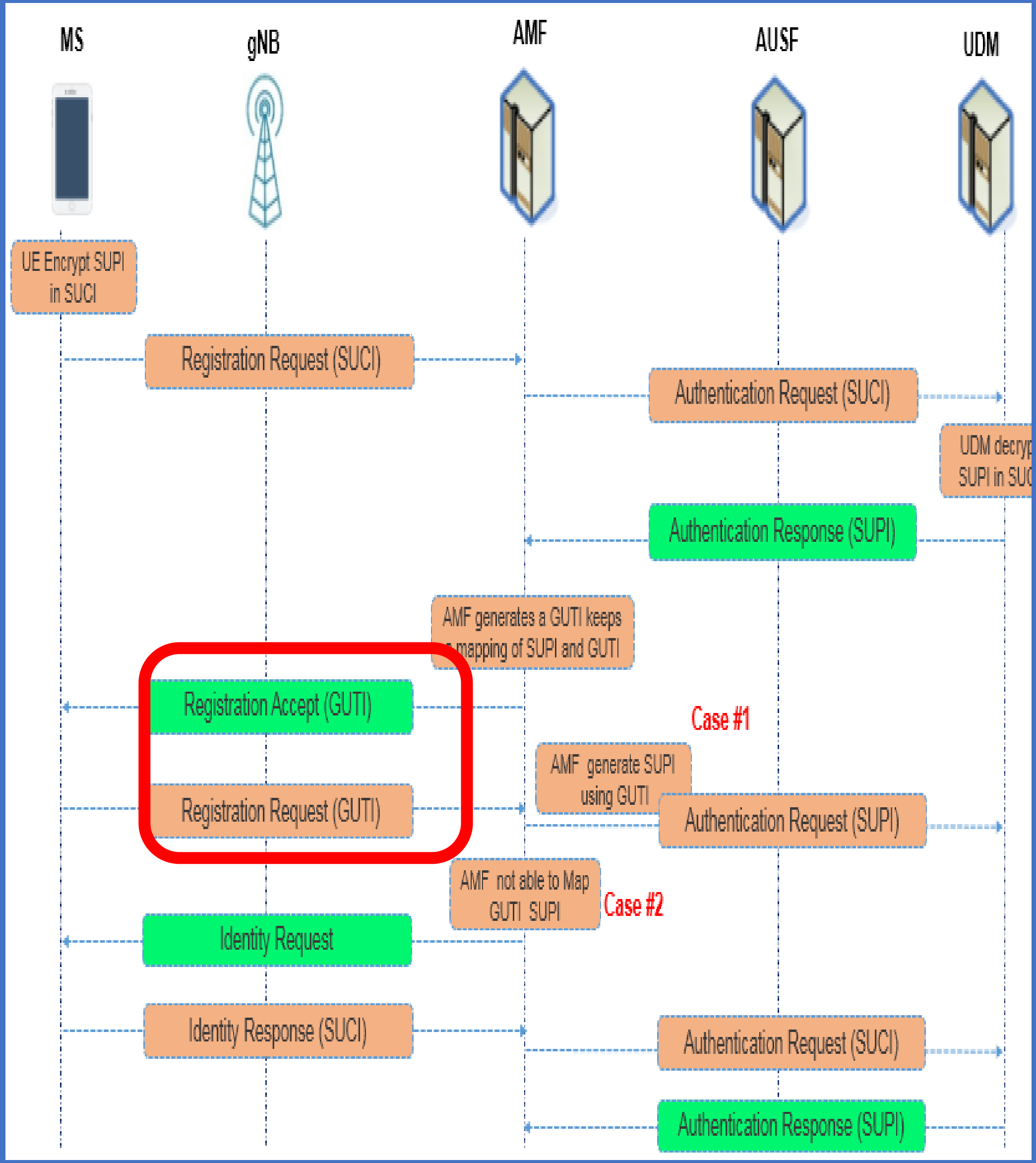


2) non-seamless non-3GPP offload indication; or

3) 5G ProSe Layer-3 UE-to-network relay offload indication.

5G Authentication Security Enhancements SUPI, SUCI, GUTI types





5G Security Architecture & Authentication Procedure - 1

The 5G System Architecture introduces the following Security Entities in the 5G CN

AUSF: AUthentication Server Function;

ARPF: Authentication credential Repository & Processing Function;

SIDF: Subscription Identifier De-concealing Function;

SEAF: SEcurity Anchor Function.

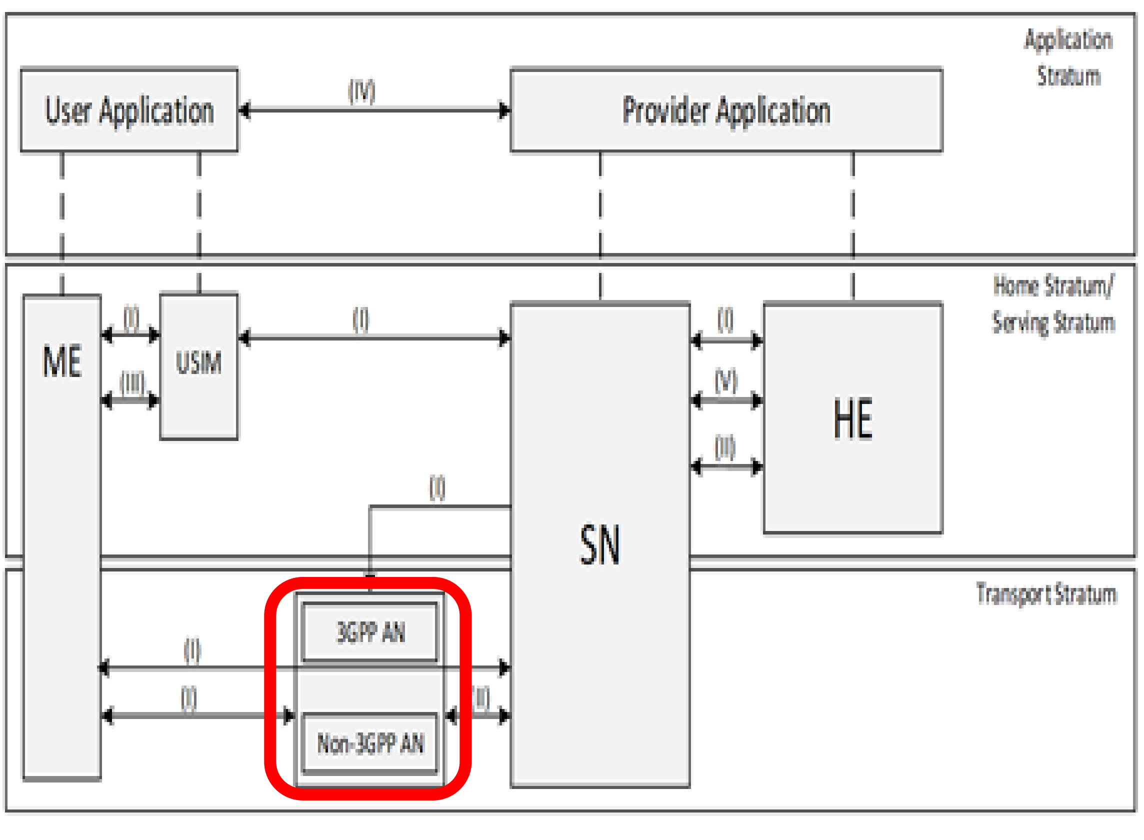


Figure 4-1: Overview of the security architecture

The figure below illustrates the following Security Domains:

- Network Access Security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN to AN for the access security.
- Network Domain Security (II): the set of security features that enable network nodes to securely exchange signalling data and user plane data.
- User Domain Security (III): the set of security features that secure the user access to mobile equipment.
- Application Domain Security (IV): the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely. Application domain security is out of scope of the present document.
- SBA Domain Security (V): the set of security features that enables network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains . Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to TS 33.401 [10].
- Visibility and Configurability of Security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.

NOTE: The visibility and configurability of security is not shown in the figure.

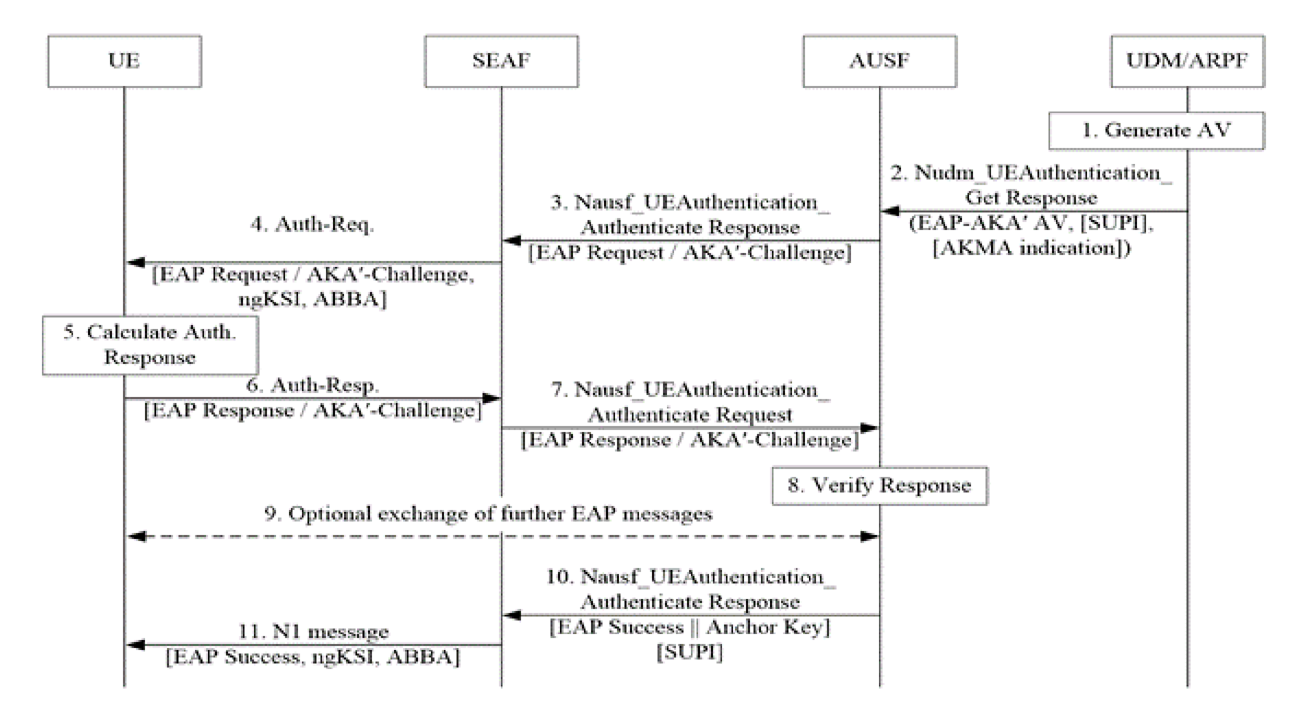


Figure 6.1.3.1-1: Authentication procedure for EAP-AKA'

5G Security Architecure and Authentication Procedure - 2

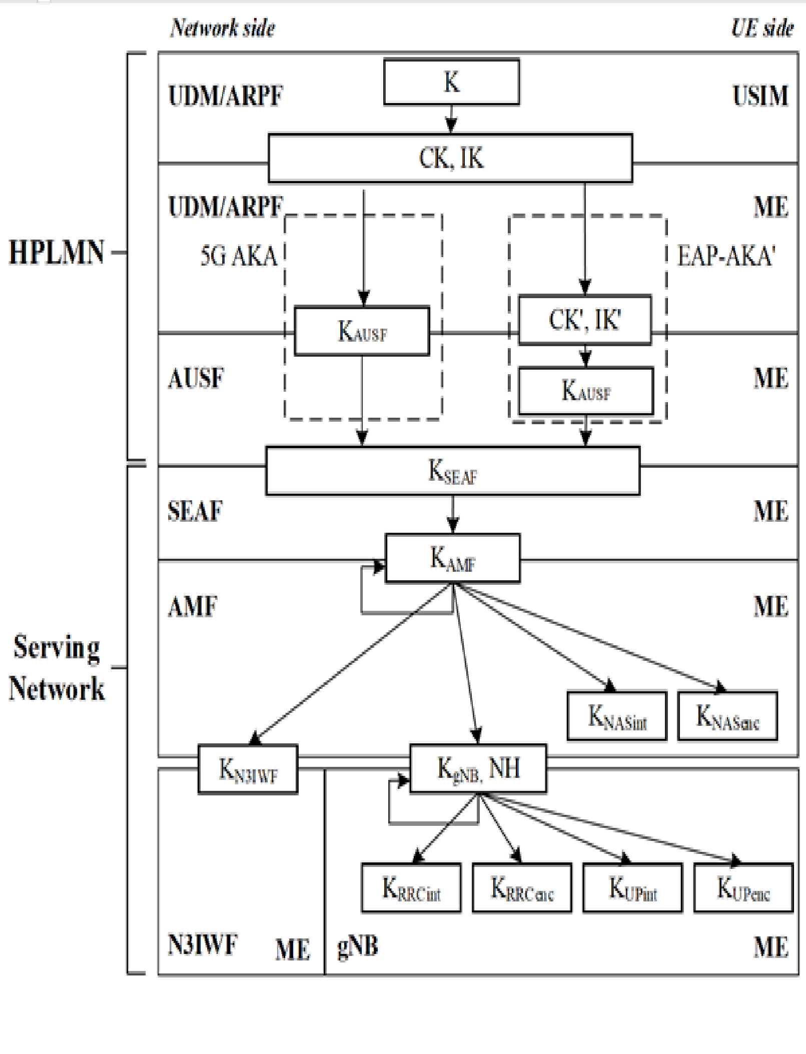


Figure 6.2.1-1: Key hierarchy generation in 5GS

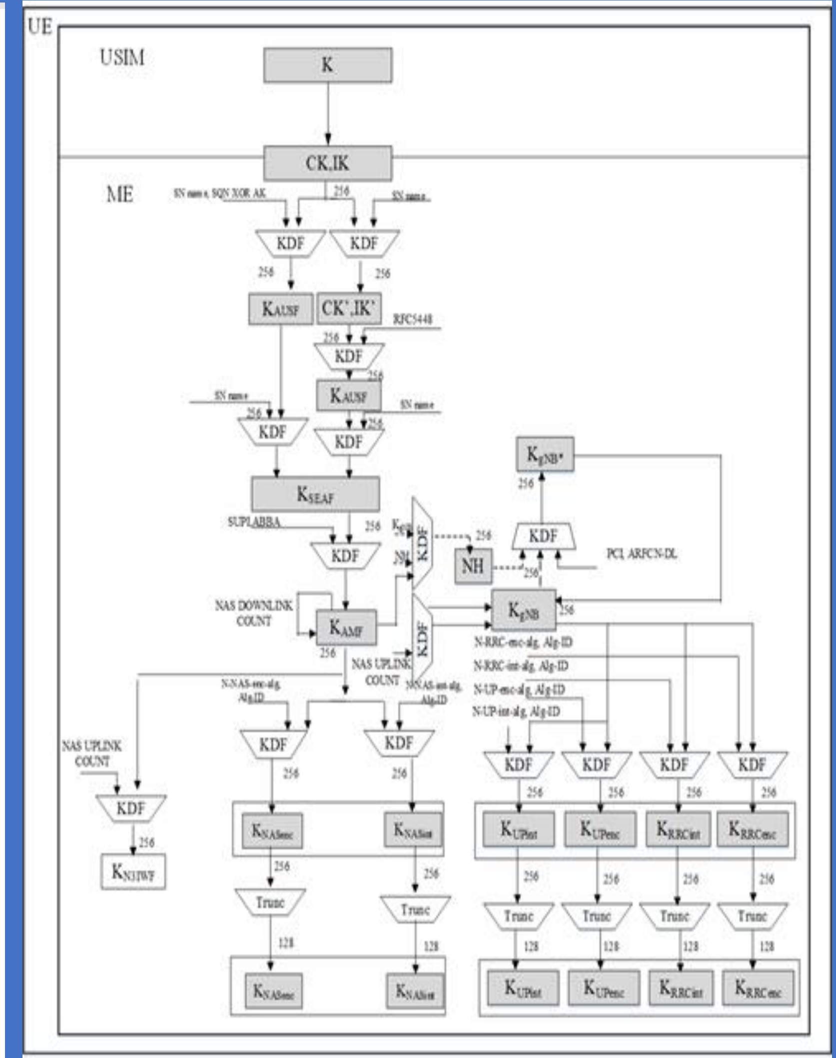


Figure 6.2.2-2: Key distribution and key derivation scheme for 5G for the UE

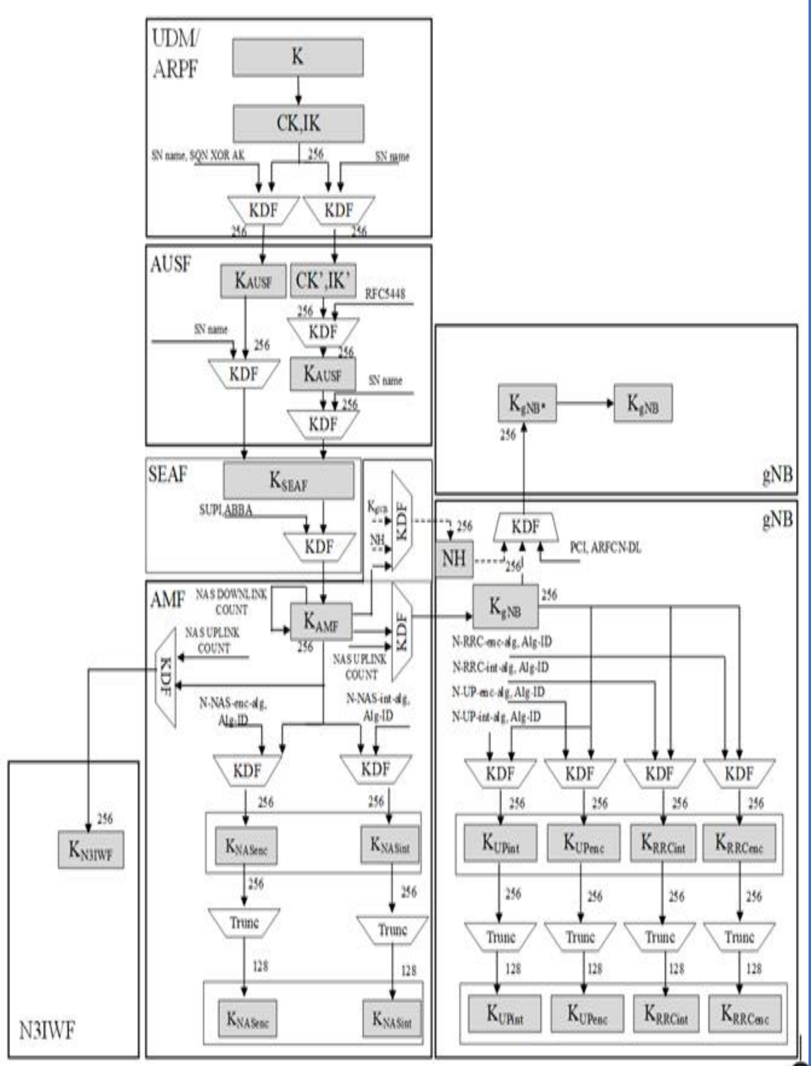
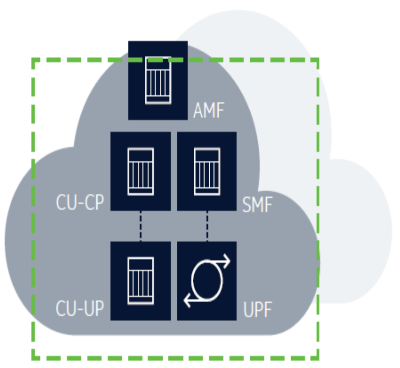


Figure 6.2.2-1: Key distribution and key derivation scheme for 5G for network nodes

2. RAN Core Convergence via CUPS implementation



RAN-Core convergence

4.2.3 Non-roaming reference architecture

Figure 4.2.3-1 depicts the non-roaming reference architecture. Service-based interfaces are used within the Control Plane.

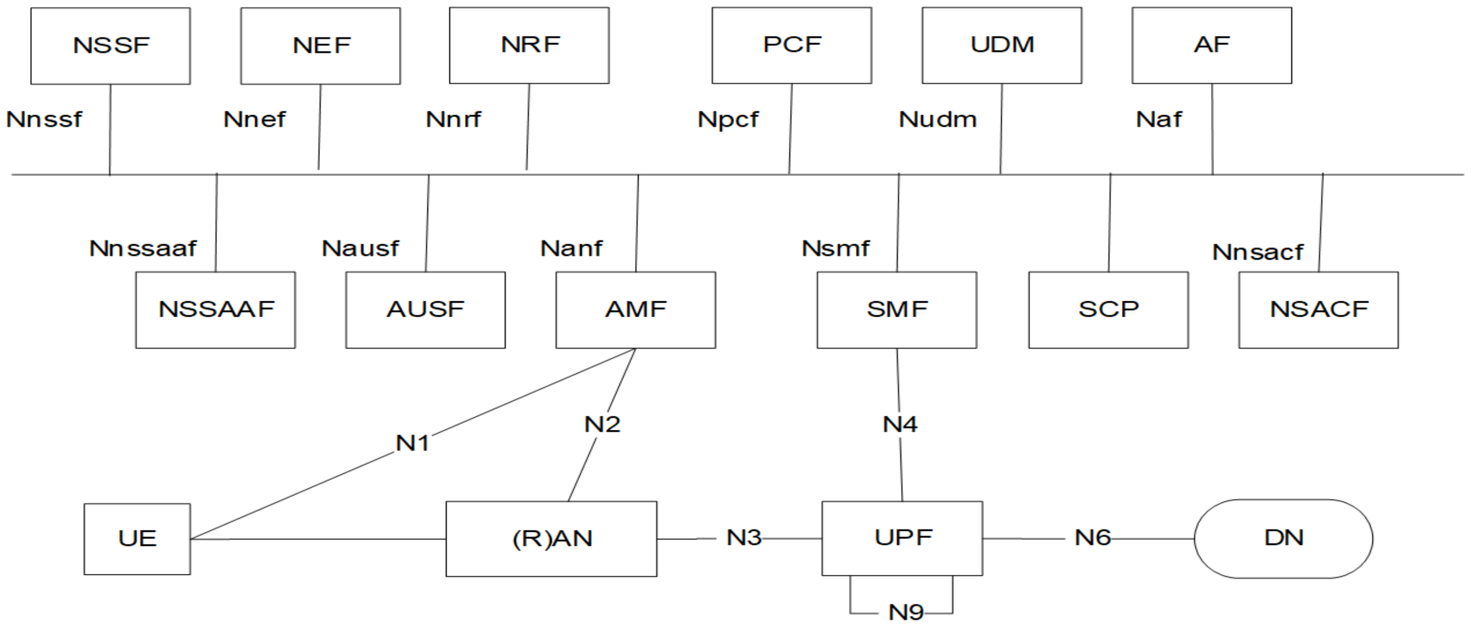


Figure 4.2.3-1: 5G System architecture

NOTE: If an SCP is deployed it can be used for indirect communication between NFs and NF services as described in Annex E. SCP does not expose services itself.

2. 5G UP GW SEPP and SeCoP - 2

Solution Key Issue #27: Policy based Authorization for Indirect Communication between Network Functions (NFs)

This solution addresses KI #22 - Authorization of NF Service Access in Indirect Communication.

The solution proposes Policy-based Authorization of NF Consumer requests in the **SeCoP (*Service Communication Proxy)*** associated with the NF Producer.

A Set of Policies are provisioned in the SeCoP which allow the SeCoP to recognise an incoming Service Request from a NF Consumer and determine whether to allow the request and set of services that can be allowed for the requesting NF.

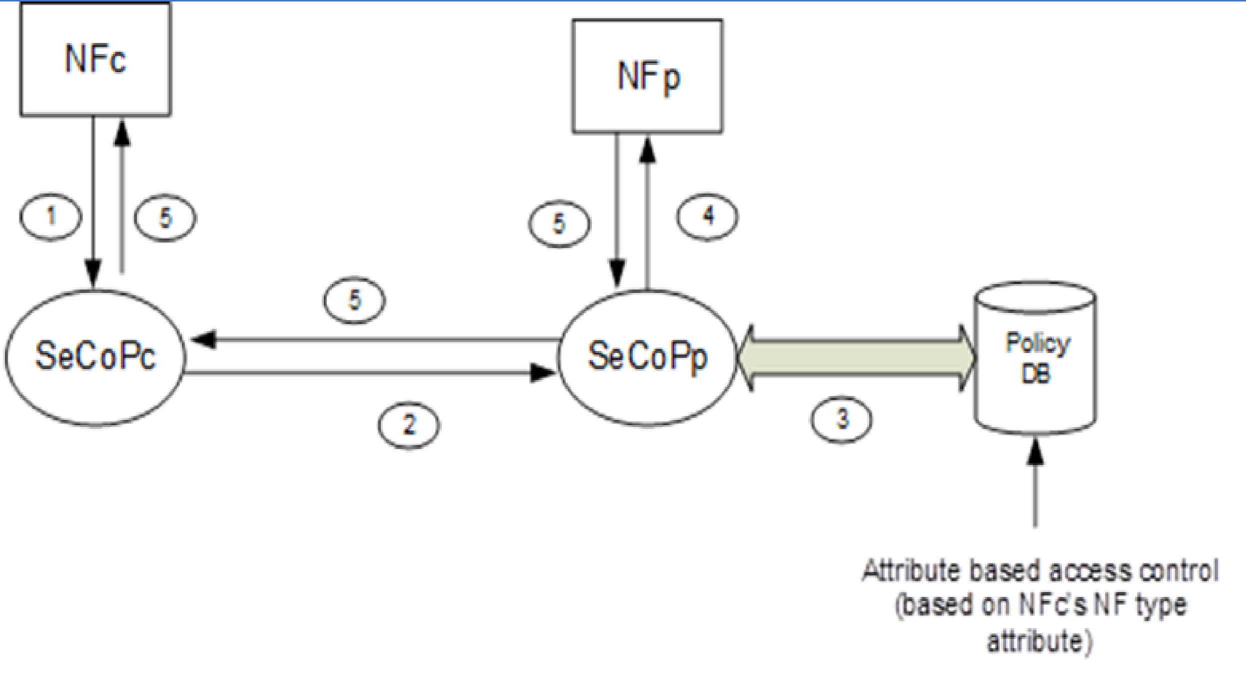


Fig.: Policy based Service Access authorization of NF consumer

5G NDL - Network Data Layer

separation of the 5G "Compute" from "Storage" via 5G UDM in NFs implementation into VNFs & PNFs related

(NF) Application Context (Unstructured Data in UDSF)

from

(NF) Application Business Logic (Structured Data in UDR)

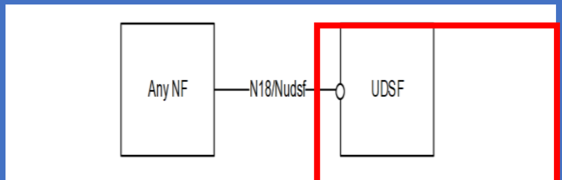


Figure 4.2.5-1: Data storage architecture for unstructured data from any NF

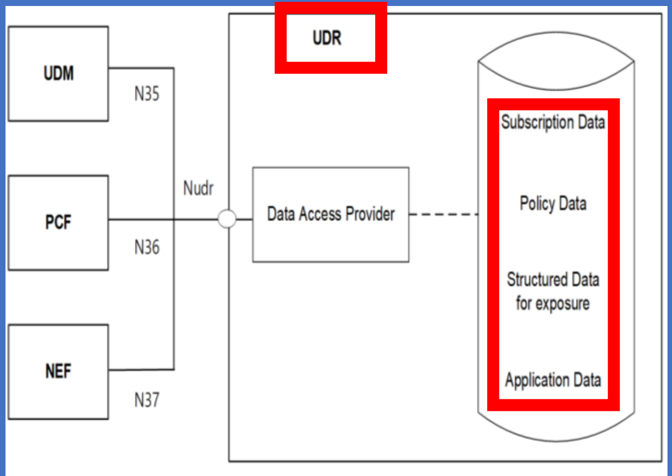


Figure 4.2.5-2: Data storage architecture

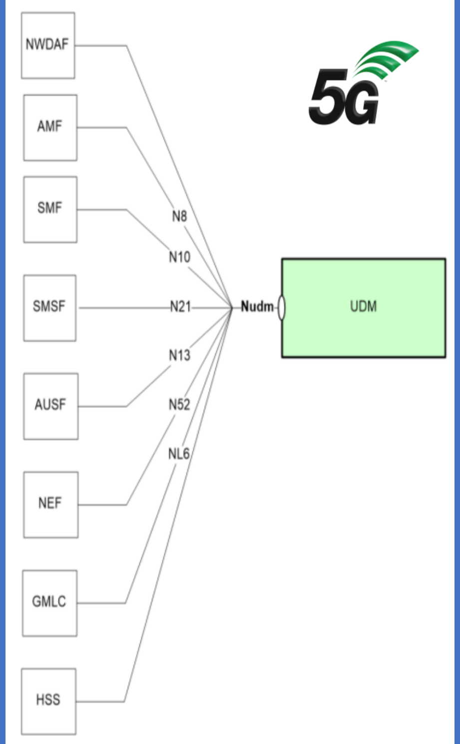


Figure 4.1-1: Reference model – UDM

5G NF as a Service "Producer" and "Consumer" (+ Intent)

Communication between consumer and producer	Service discovery and request routing	Communication model
Direct communication	No NRF or SCP; direct routing	A
	Discovery using NRF services; no SCP; direct routing	B
Indirect communication	Discovery using NRF services; selection for specific instance from the Set can be delegated to SCP. Routing via SCP	C
	Discovery and associated selection delegated to an SCP using discovery and selection parameters in service request; routing via SCP	D

Table E.1-1: Communication models for NF/NF Services interaction

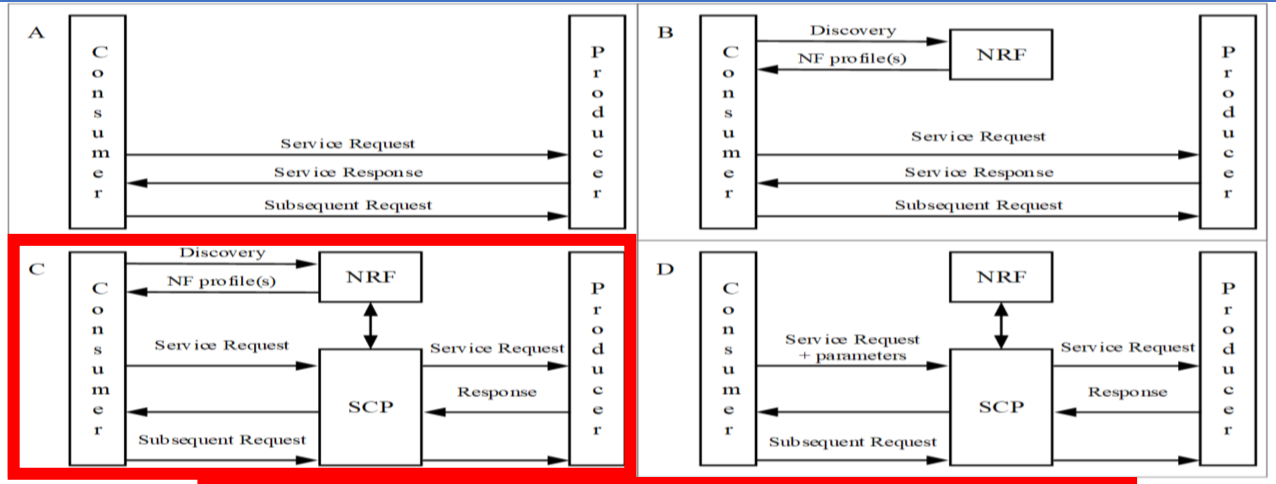


Figure E.1-1: Communication models for NF/NF services interaction

Stateless NFs (for any 5GC NF type)

An NF may become Stateless by Storing its Contexts as Unstructured Data in the UDSF.

An UDM, PCF and NEF may also Store own Structured Data in the UDR.

An UDR and UDSF cannot become stateless.

An NF may also be deployed such that several stateless network function instances are present within a set of NF instances. Additionally, within an NF, an NF service may have multiple instances grouped into a NF Service Set if they are interchangeable with each other because they share the same context data. See clause 5.21 of 3GPP TS 23.501 [3].

.

6.5.3 Stateless NFs (for any 5GC NF type)

6.5.3.1 General

An NF may become stateless by storing its contexts as unstructured data in the UDSF.An UDM, PCF and NEF may also store own structured data in the UDR. An UDR and UDSF cannot become stateless.

An NF may also be deployed such that several stateless network function instances are present within a set of NF instances. Additionally, within an NF, an NF service may have multiple instances grouped into a NF Service Set if they are interchangeable with each other because they share the same context data. See clause 5.21 of 3GPP TS 23.501 [3].

A UDM / AUSF / UDR / PCF group may consist of one or multiple UDM / AUSF / UDR / PCF sets.

6.5.3.2 Stateless NF as service consumer

1. When the NF service consumer subscribes (explicitly or implicitly) to notifications from another NF service producer, the NF service consumer may provide a binding indication to the NF service producer as specified in clause 6.3.1.0 of 3GPP TS 23.501 [3] and clause 4.17.12.4 of 3GPP TS 23.502 [4], to enable the related notifications to be sent to an alternative NF service consumer within the NF (service) set, in addition to providing the Callback URI in the subscription resource.

2. A NF service producer or SCP may use the Nnrf_NFDiscovery service to discover NF service consumers within an NF (service) set.

3. An NF service producer may become aware of a NF service consumer change, via receiving an updated binding information (i.e. when the binding entity corresponding to the binding level is changed), or via an Error response to a notification, via link level failures (e.g. no response from the NF), or via a notification from the NRF that the NF service consumer has deregistered. The HTTP error response may be a 3xx redirect response pointing to a new NF service consumer.

NOTE: When the binding entity other than the one corresponding to the binding level is changed, it indicates the

Management Services (MnS)

An Management Service (MnS) offers Capabilities for Management and Orchestration of Network and Service.

The entity producing an MnS is called **MnS Producer.**

The entity consuming an MnS is called **MnS Consumer.**

An MnS provided by an MnS Producer can be consumed by any entity with appropriate Authorisation and Authentication.

An MnS Producer offers its services via a Standardized Service Interface composed of individually specified MnS Components.

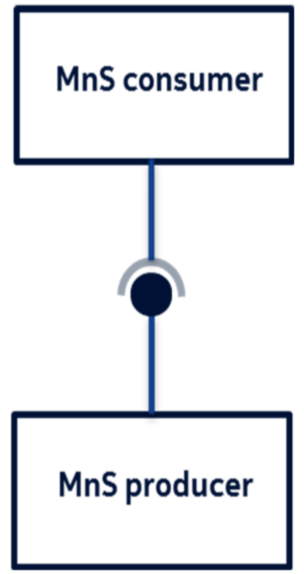


Figure 4.1.1: MnS producer and MnS consumer

5G NFs Services as Producer and Consumer

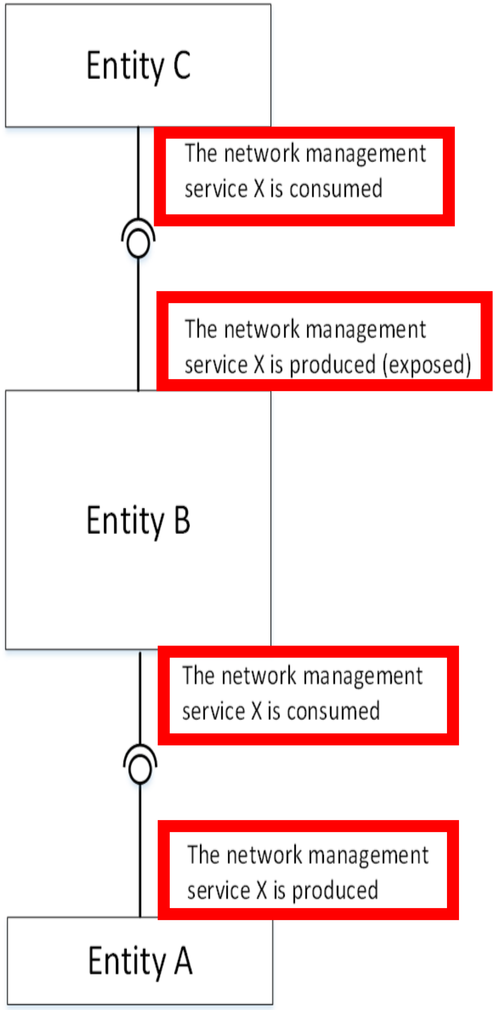


Figure 5.1.1-1. Example of producers and consumers of the management service

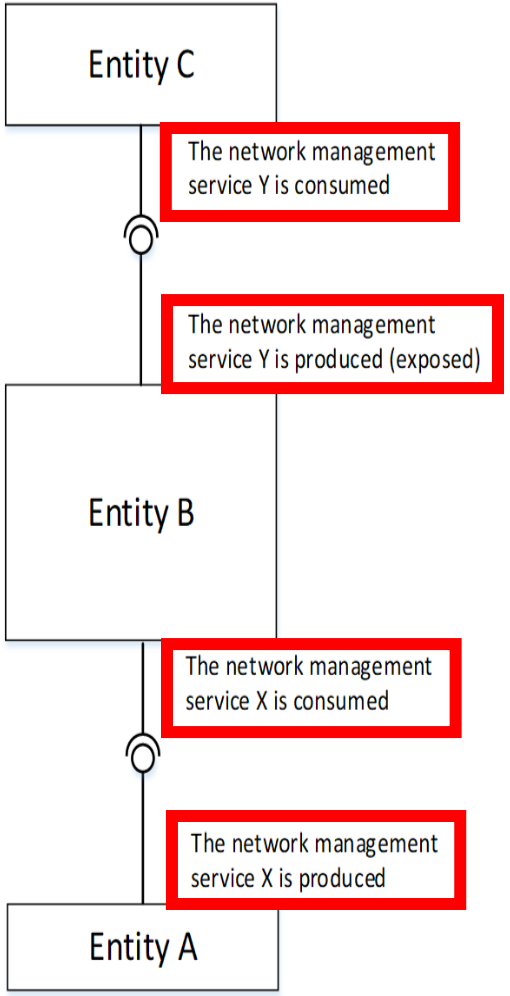


Figure 5.1.1-2. Example of producers and consumers of management services

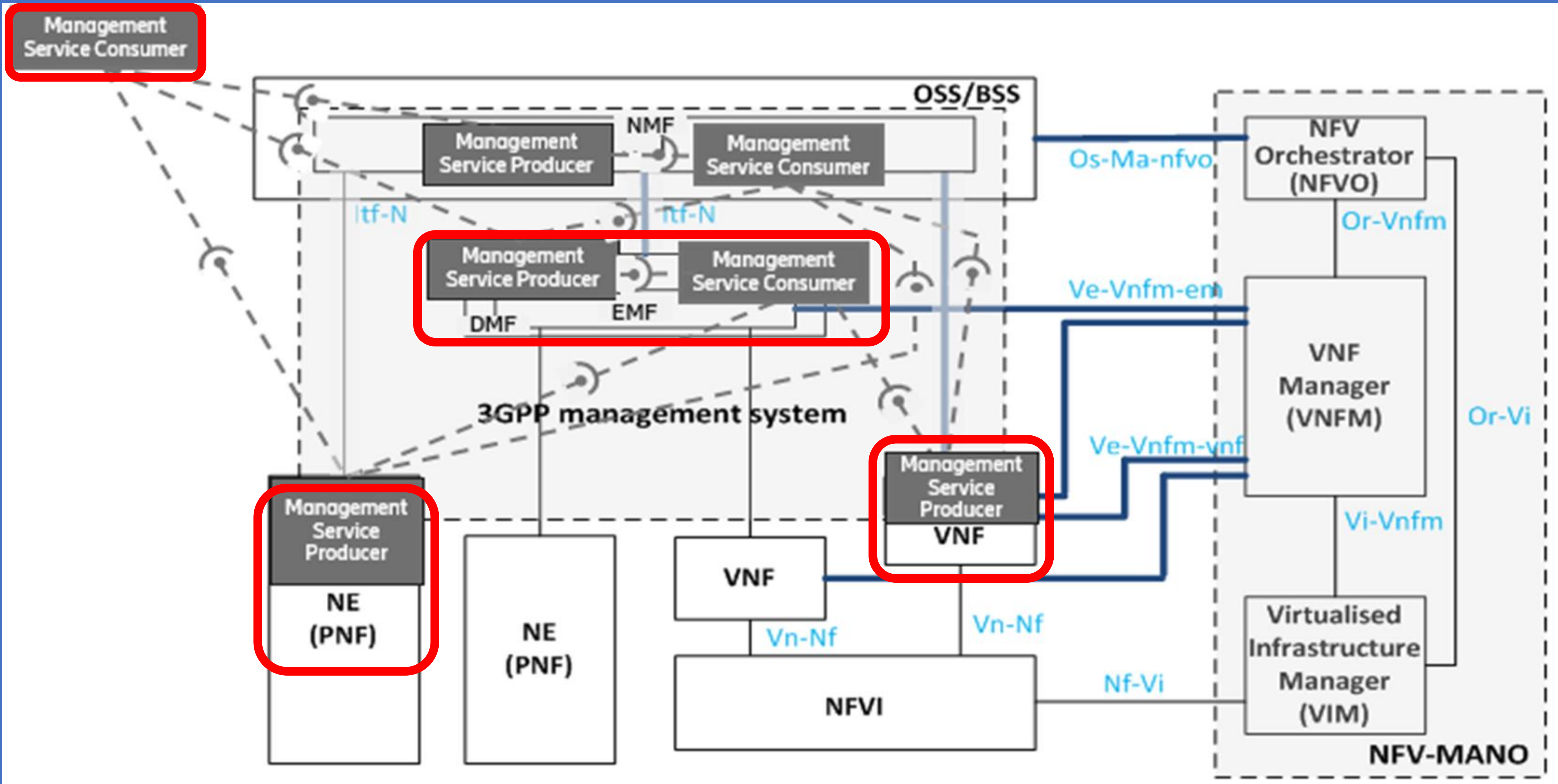


Figure C.1: Example of Management service producer and consumer interaction mapped into the pre-Rel-15 management reference model [10]

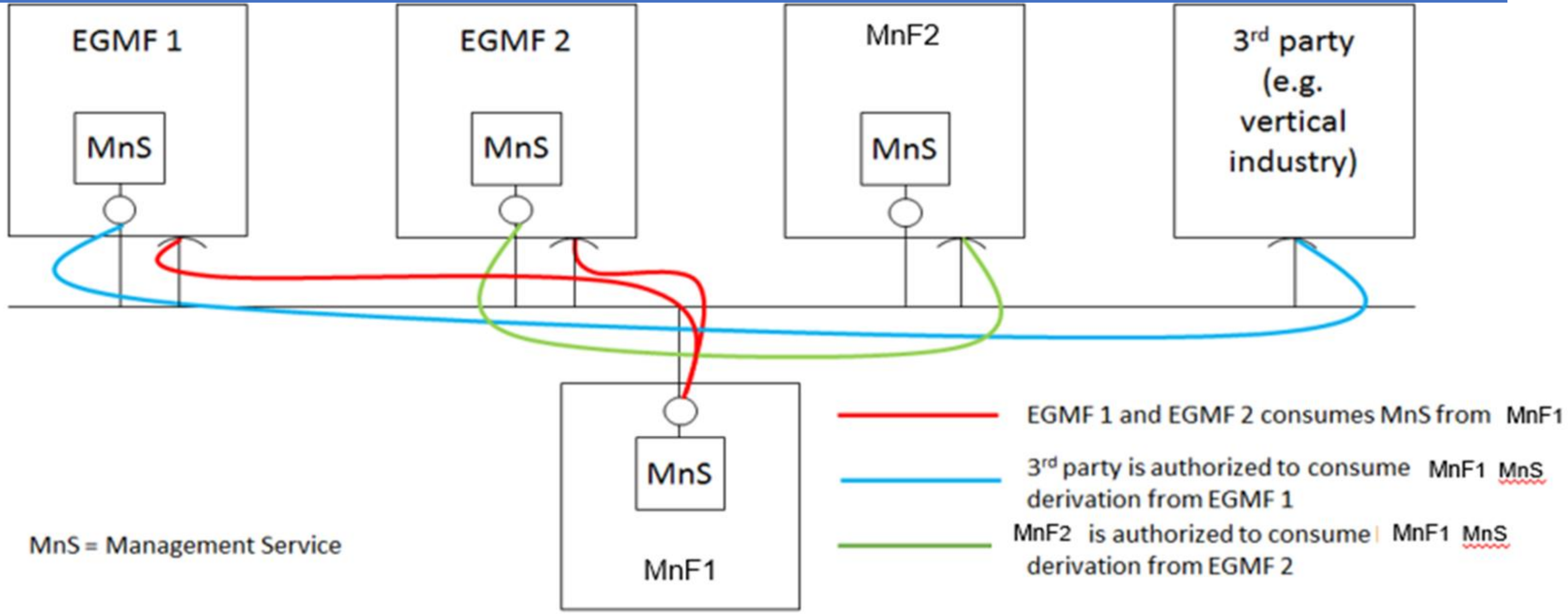


Figure A.3.1: MnF-1 Management Service (MnS) exposed through Exposure Governance Management Function 1 (EGMF 1) and through Exposure Governance Management Function 2 (EGMF 2)

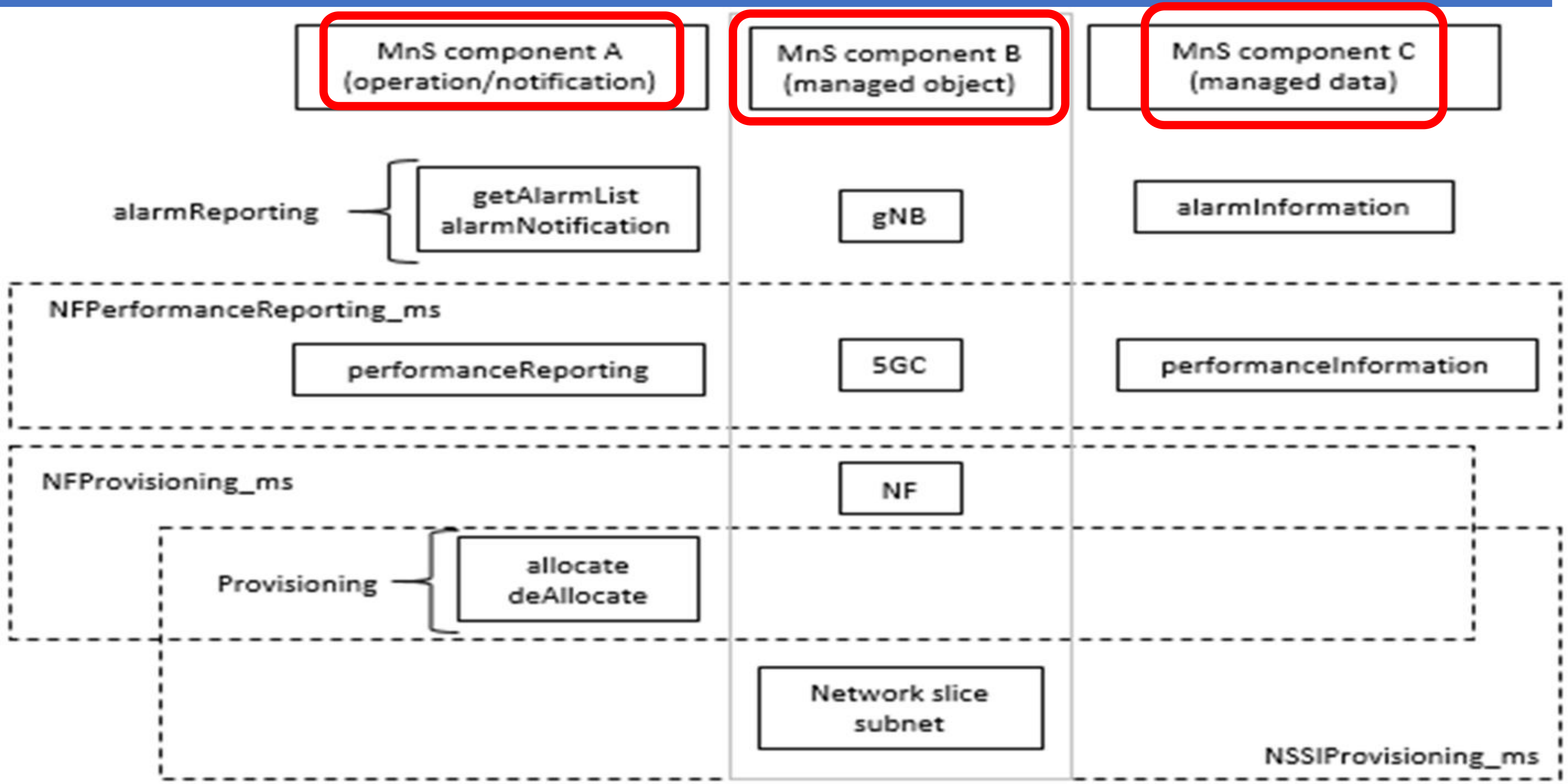


Figure 4.3.1: Example of Management Service and component type A, B and C

Intent driven Management Service (Intent driven MnS) concept

Perform Network Management Tasks

Identifying, Formulating and Activating Network Management Policies

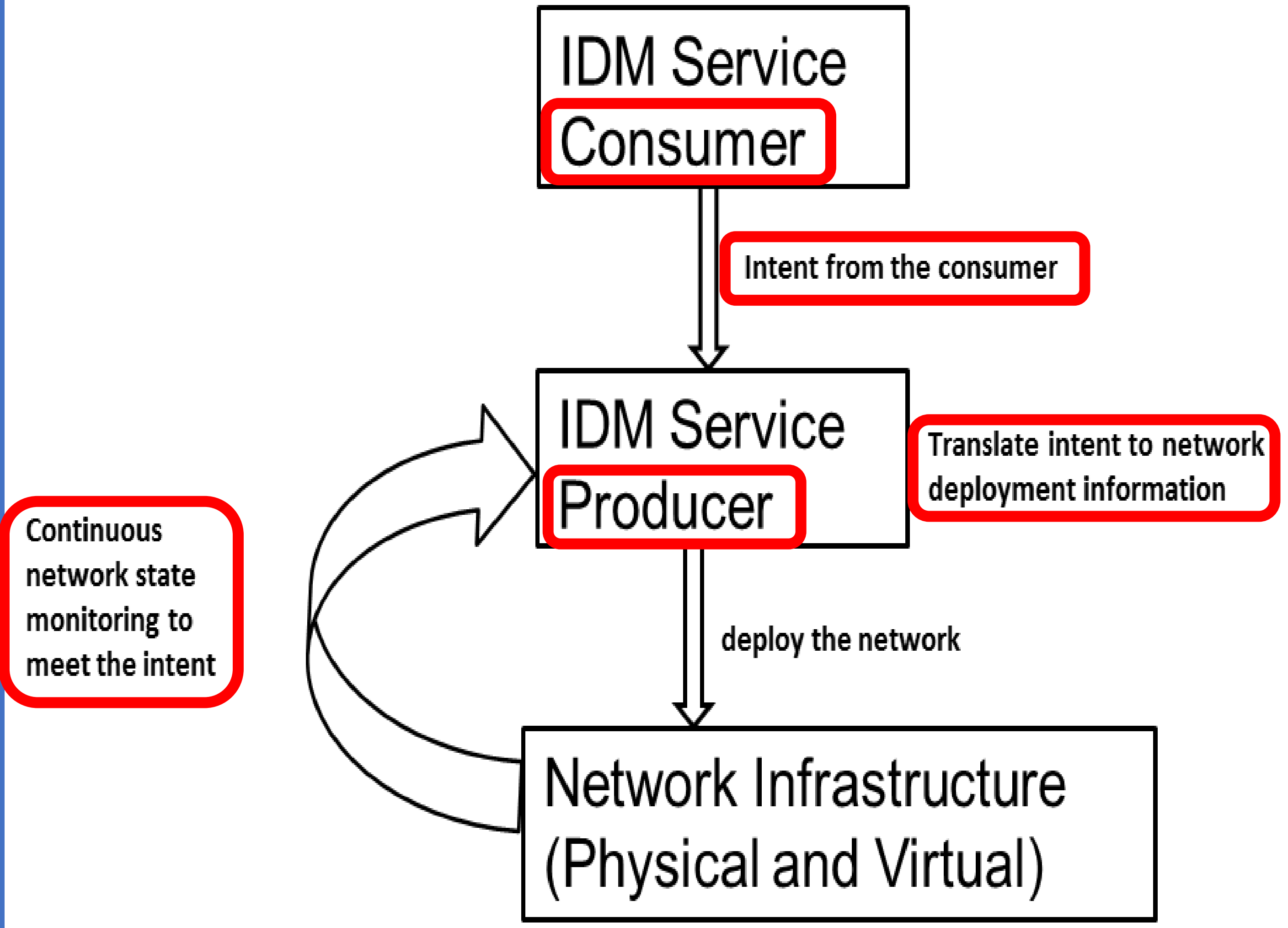


Figure 4.1.2.1-2: An example of using Intent driven management service for network provisioning

- Intent from Communication Service Provider (Intent-CSP)
- Intent from Network Operator (Intent-NOP)

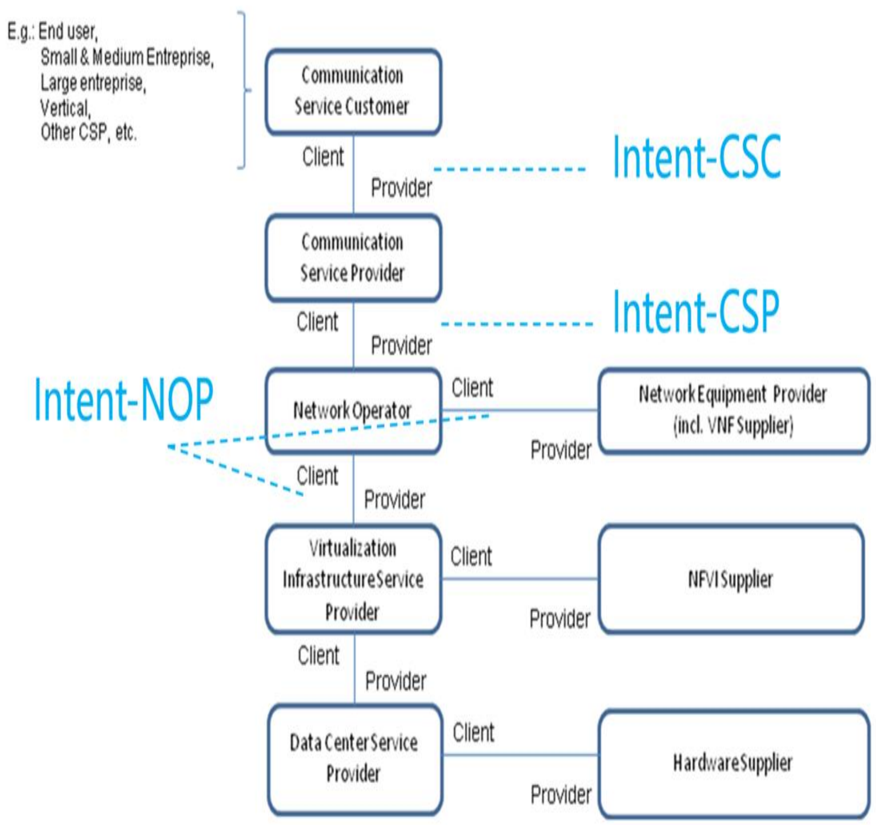


Figure 4.1.2.4-1: Concept for utilization of intent

4.1.2.5 Intent driven Management Service (MnS) interactions with 3GPP management functions

The following figure shows the interaction of intent driven management service (MnS) with management functions.

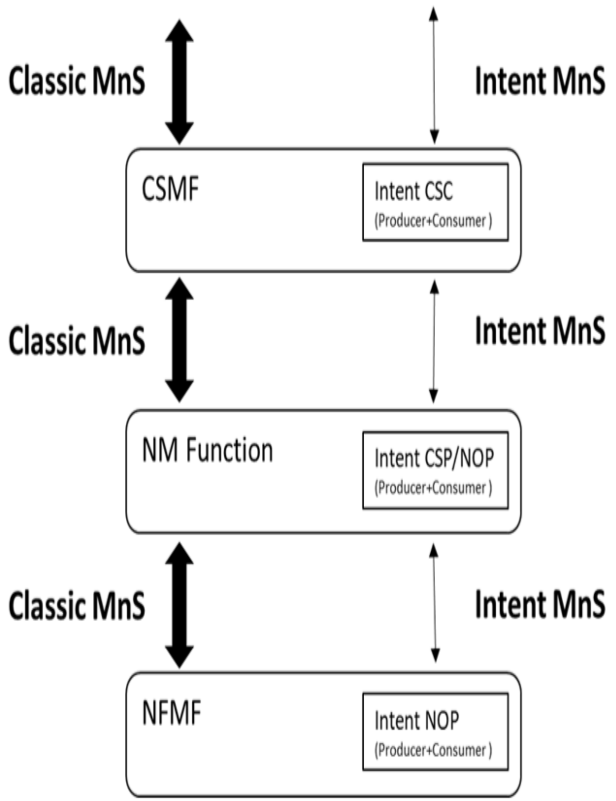


Figure 4.1.2.5.1: The intent driven management service (MnS) vs classic MnS

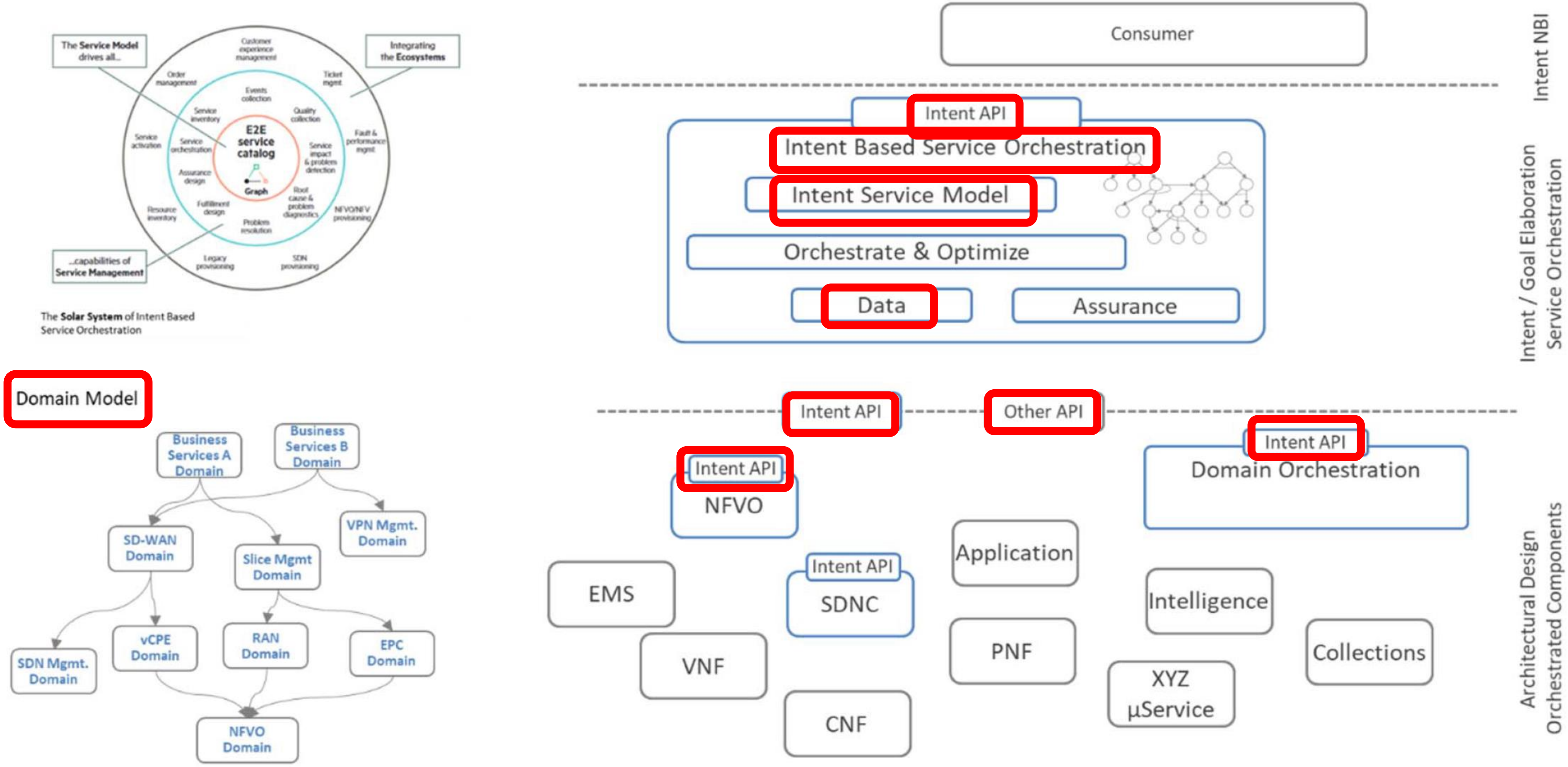


Figure 10: Intent-based Service Orchestration across Domains, driven by Intent-based Service Models

Interface 1: NWDAF interacts with AF (via NEF) using NW layer SBI.

Interface 2: N1/N2 interface.

Interface 3: O&M layer configures the NF profile in the NRF, and NWDAF collect the NF capacity information from the NRF.

Interface 4: MDAF interacts with Application/Tenant using Northbound Interfaces (NBI).

Interface 5: MDAF interacts with RAN DAF using O&M layer SBI.

Interface 6: NWDAF consumes the services provided by MDAF using cross layer SBI.

Interface 7: MDAF consumes the services provided by MWDAF using cross layer SBI.

Interface 8: MDAF collects data from NW layer via trace file/monitoring services.

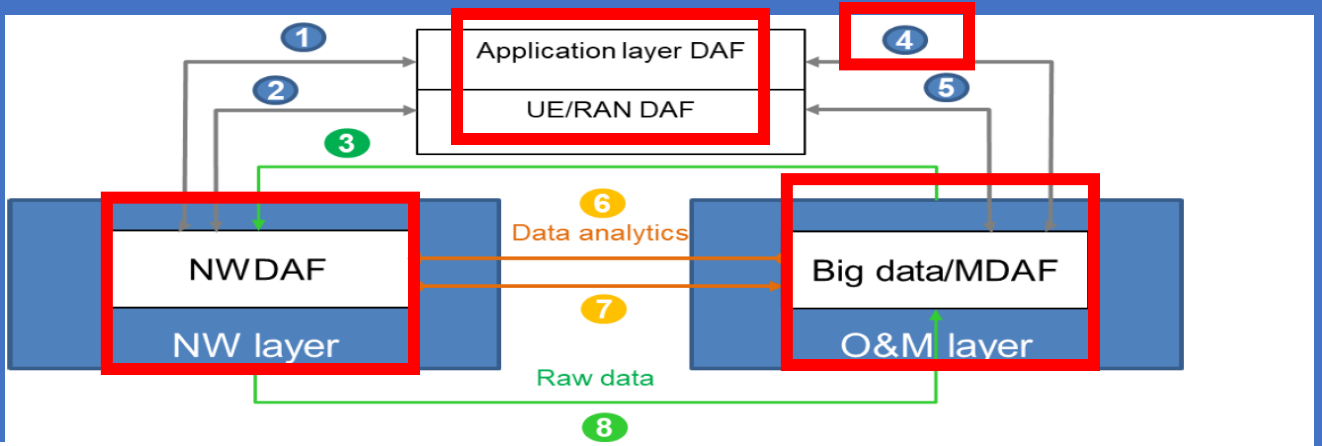


Figure 4-3: Data Analytics framework in 5G Mobile Network Architecture

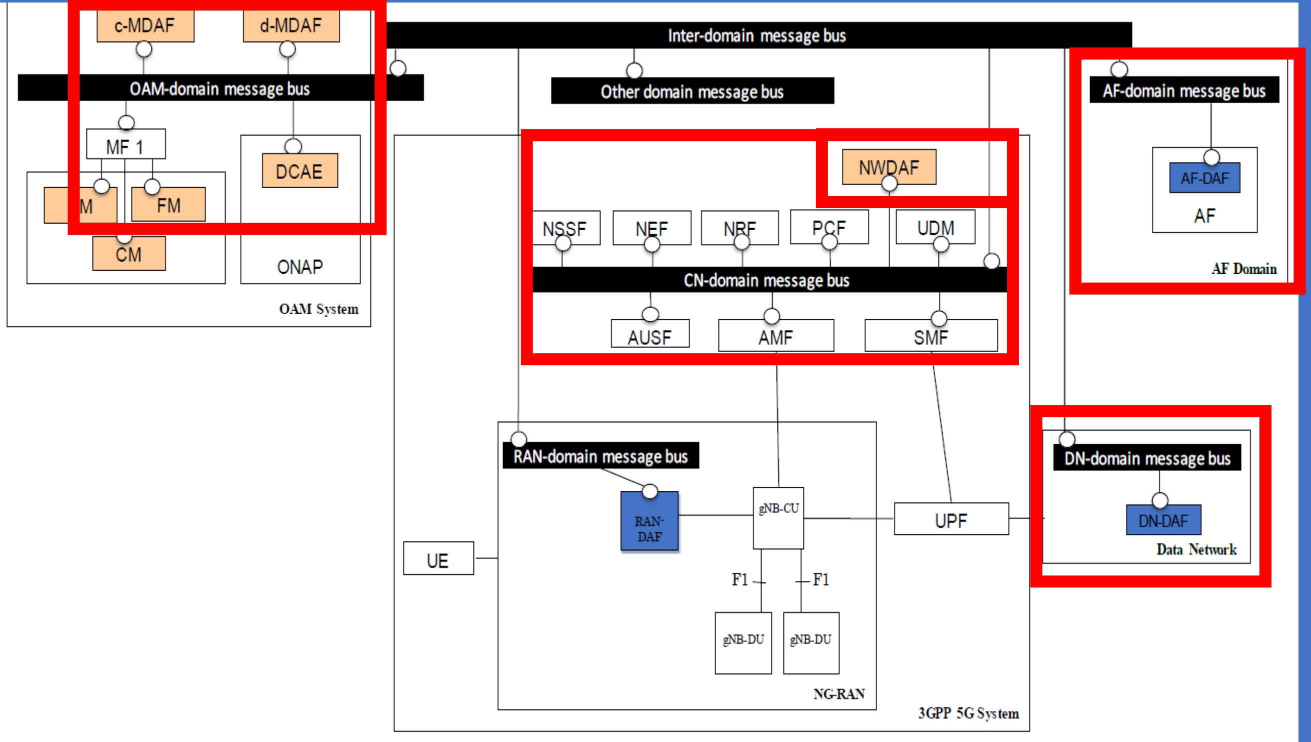


Figure 4-4 5G Mobile Network Architecture Integrated Analytics Architecture

Service Subscriptions related to Latency in Standardized and Private Slice Types

Network Slice Providers can build their Network Slice Product offering based on S-NESTs (Standardized Network Slice Type) and/or their P-NESTs (**Private NESTs).**

Standardized Network Slice Type (S-NEST) NST-A, for which the attribute Packet Delay Budget Value Range is between **1 ms and 100 ms is specified by 3GPP.**

Network Slice Provider **(NSP)** may offer 3 products based on **NST-A**:

- **Platinum NST-A** based Network Slice Product, where the attribute ' **Packet Delay Budget' Value Range is between 1 ms and 10 ms**

- **Gold NST-A** based Network Slice Product, where the attribute **Packet Delay Budget' Value Range is between 11 ms and 50 ms**

- **Silver NST-A** based Network Slice Product, where the attribute **Packet Delay Budget' Value Range is between 51 ms and 100 ms.**

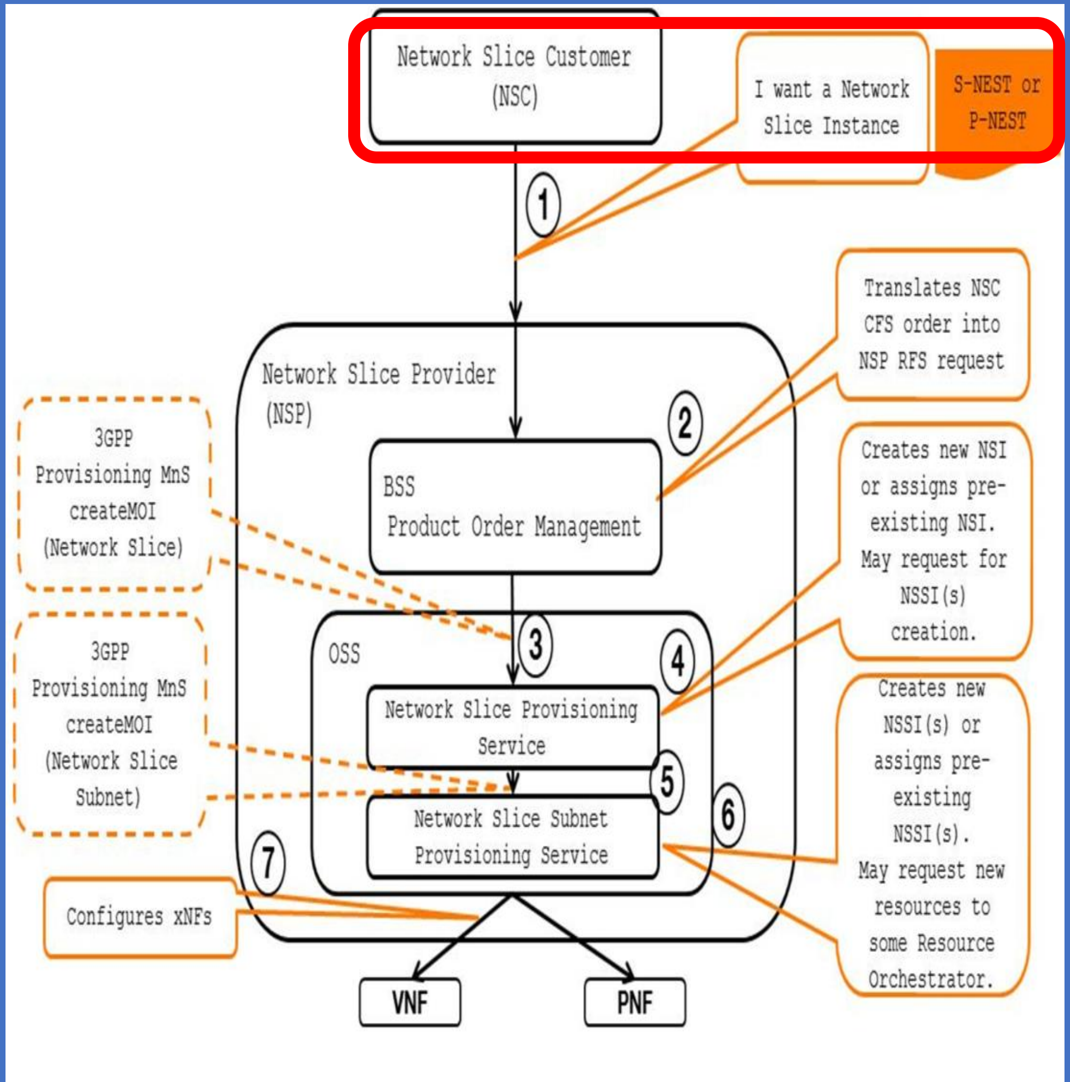


Figure A.2: Network Slice journey (NSaaS model) – high-level call flow

Use of 5G CN LADN (Local Area Data Network) support

- LADN in a certain Service Area (SA) where the Applications are deployed.
- Access to a LADN is only available in a specific LADN SA (Service Area), defined as a Set of Tracking Areas (TAs) in the serving PLMN

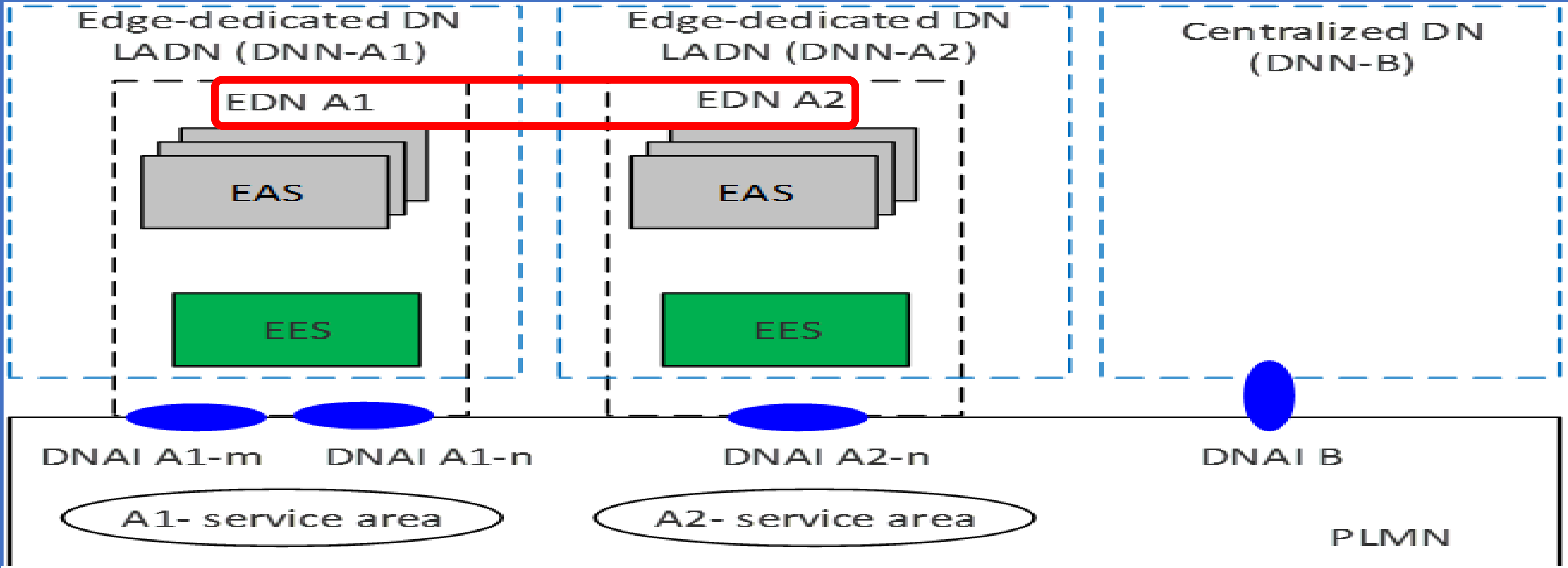


Figure A.2.4-1: Option 3: Use of LADN(s)

1. 3GPP 5G System Architecture (PDU) SSC Modes 1 - 3 General

Each PDU Session supports a single PDU Session type

The following PDU Session types are defined:

- IPv4,
- IPv6,
- IPv4v6,
- Ethernet,
- Unstructured

- PDU Sessions are established (upon UE request),
- Modified (upon UE and 5GC request) and
- Released (upon UE and 5GC request)

using NAS SM signalling exchanged over N1 between the UE and the SMF.

Upon request from an Application Server (AS), the 5GC is able to trigger a specific Application in the UE.

Table 5.6.1-1: Attributes of a PDU Session

PDU Session attribute	May be modified later during the lifetime of the PDU Session	Notes
S-NSSAI of the HPLMN	No	(Note 1) (Note 2)
S-NSSAI of the Serving PLMN	Yes	(Note 1) (Note 2) (Note 4)
DNN (Data Network Name)	No	(Note 1) (Note 2)
PDU Session Type	No	(Note 1)
SSC mode	No	(Note 2) The semantics of Service and Session Continuity mode is defined in clause 5.6.9.2
PDU Session Id	No	
User Plane Security Enforcement information	No	(Note 3)
Multi-access PDU Connectivity Service	No	Indicates if the PDU Session provides multi-access PDU Connectivity Service or not.

NOTE 1: If it is not provided by the UE, the network determines the parameter based on default information received in user subscription. Subscription to different DNN(s) and S-NSSAI(s) may correspond to different default SSC modes and different default PDU Session Types

NOTE 2: S-NSSAI(s) and DNN are used by AMF to select the SMF(s) to handle a new session. Refer to clause 6.3.2.

NOTE 3: User Plane Security Enforcement information is defined in clause 5.10.3.

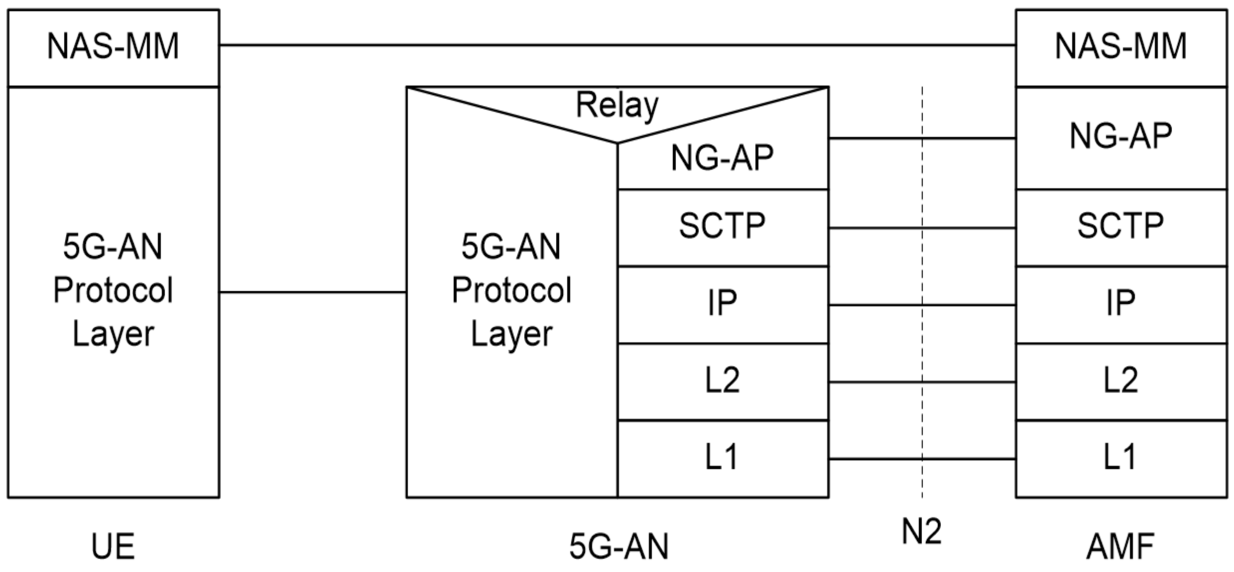
NOTE 4: The S-NSSAI value of the Serving PLMN associated to a PDU Session can change whenever the UE moves to a different PLMN, while keeping that PDU Session.

Control Plane (CP) Protocol Stacks between the UE and the 5GC

A single N1 NAS signalling connection is used for each access to which the UE is connected. The single N1 termination point is located in AMF. The single N1 NAS signalling connection is used for both Registration Management and Connection Management (RM/CM) and for SM-related messages and procedures for a UE.

The NAS protocol on N1 comprises a NAS-MM and a NAS-SM components.

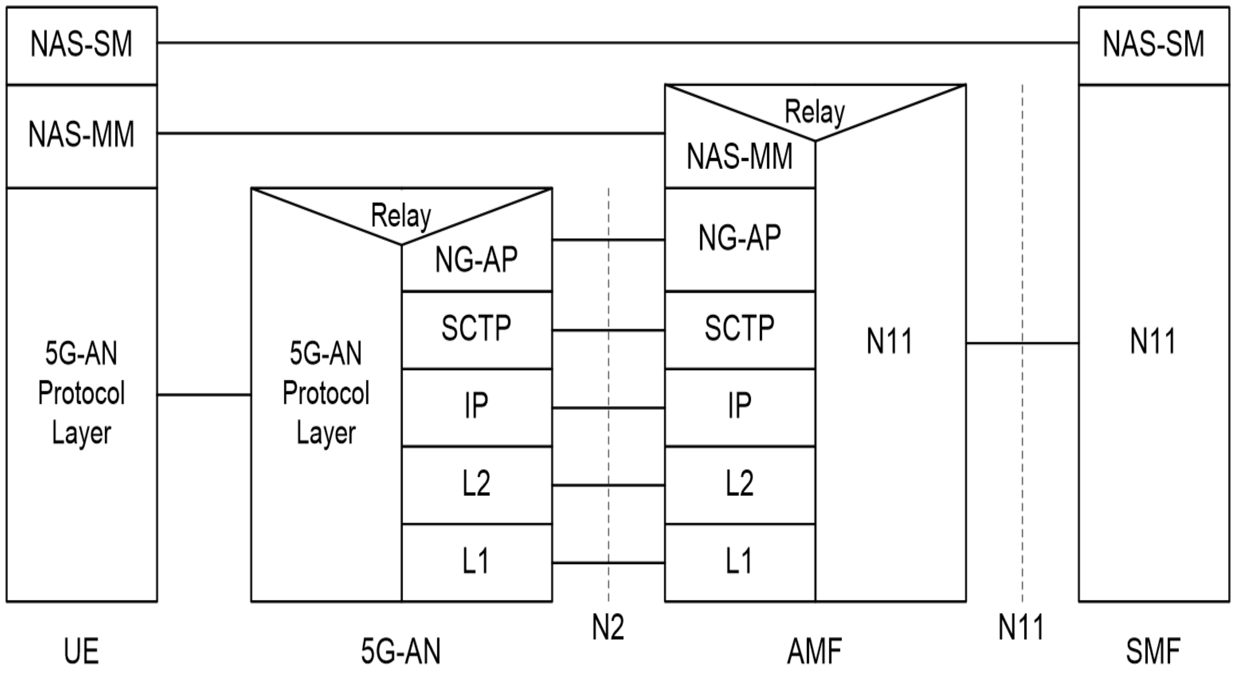
UE - AMF



Legend:
- **NAS-MM:** The NAS protocol for MM functionality supports Registration Management Functionality, Connection Management Functionality and User Plane (UP) Connection Activation and De-activation. It is also responsible of Ciphering and Integrity Protection of NAS signalling.
- **5G-AN Protocol Layer:** This set of protocols/layers depends on the 5G-AN. In the case of NG-RAN, the Radio Protocol between the UE and the NG-RAN Node (eNodeB or gNodeB) is specified in 3GPP NR TS. In the case of non-3GPP access, see clause 8.2.4.

Figure 8.2.2.2-1: Control Plane (CP) between the UE and the AMF

UE – SMF



Legend:
- **NAS-SM:** The NAS protocol for SM Functionality supports User Plane (UP) PDU Session Establishment, Modification and Release. It is transferred via the AMF, and transparent to the AMF. 5G NAS protocol is defined in 3GPP TS.

Figure 8.2.2.3-1: Control Plane protocol stack between the UE and the SMF

Table 1: 5G User Equipment (UE) Service Access Identities & Service Access Gategories Configuration

Table 1: 5G User Equipment (UE) Service Access Identities Configuration

Access Identity number	UE configuration
0	UE is not configured with any parameters from this table
1 (NOTE 1)	UE is configured for Multimedia Priority Service (MPS).
2 (NOTE 2)	UE is configured for Mission Critical Service (MCS).
3	UE for which Disaster Condition applies (note 4)
4-10	Reserved for future use
11 (NOTE 3)	Access Class 11 is configured in the UE.
12 (NOTE 3)	Access Class 12 is configured in the UE.
13 (NOTE 3)	Access Class 13 is configured in the UE.
14 (NOTE 3)	Access Class 14 is configured in the UE.
15 (NOTE 3)	Access Class 15 is configured in the UE.

NOTE 1: Access Identity 1 is used by UEs configured for MPS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN, PLMNs equivalent to HPLMN, and visited PLMNs of the home country.
Access Identity 1 is also valid when the UE is explicitly authorized by the network based on specific configured PLMNs inside and outside the home country.

NOTE 2: Access Identity 2 is used by UEs configured for MCS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN or PLMNs equivalent to HPLMN and visited PLMNs of the home country. Access Identity 2 is also valid when the UE is explicitly authorized by the network based on specific configured PLMNs inside and outside the home country.

NOTE 3: Access Identities 11 and 15 are valid in Home PLMN only if the EHPLMN list is not present or in any EHPLMN. Access Identities 12, 13 and 14 are valid in Home PLMN and visited PLMNs of home country only. For this purpose, the home country is defined as the country of the MCC part of the IMSI.

NOTE 4: The configuration is valid for PLMNs that indicate to potential Disaster Inbound Roamers that the UEs can access the PLMN. See clause 6.31.

Table 2: 5G User Equipment (UE) Service Access Categories Configuration

Access Category number	Conditions related to UE	Type of access attempt
0	All	MO signalling resulting from paging
1 (NOTE 1)	UE is configured for delay tolerant service and subject to access control for Access Category 1, which is judged based on relation of UE's HPLMN and the selected PLMN.	All except for Emergency, or MO exception data
2	All	Emergency
3	All except for the conditions in Access Category 1.	MO signalling on NAS level resulting from other than paging
4	All except for the conditions in Access Category 1.	MMTEL voice (NOTE 3)
5	All except for the conditions in Access Category 1.	MMTEL video
6	All except for the conditions in Access Category 1.	SMS
7	All except for the conditions in Access Category 1.	MO data that do not belong to any other Access Categories (NOTE 4)
8	All except for the conditions in Access Category 1	MO signalling on RRC level resulting from other than paging
9	All except for the conditions in Access Category 1	MO IMS registration related signalling (NOTE 5)
10 (NOTE 6)	All	MO exception data
11-31		Reserved standardized Access Categories
32-63 (NOTE 2)	All	Based on operator classification

NOTE 1: The barring parameter for Access Category 1 is accompanied with information that define whether Access Category applies to UEs within one of the following categories:
a) UEs that are configured for delay tolerant service;
b) UEs that are configured for delay tolerant service and are neither in their HPLMN nor in a PLMN that is equivalent to it;
c) UEs that are configured for delay tolerant service and are neither in the PLMN listed as most preferred PLMN of the country where the UE is roaming in the operator-defined PLMN selector list on the SIM/USIM, nor in their HPLMN nor in a PLMN that is equivalent to their HPLMN.
When a UE is configured for EAB, the UE is also configured for delay tolerant service. In case a UE is configured both for EAB and for EAB override, when upper layer indicates to override Access Category 1, then Access Category 1 is not applicable.

NOTE 2: When there are an Access Category based on operator classification and a standardized Access Category to both of which an access attempt can be categorized, and the standardized Access Category is neither 0 nor 2, the UE applies the Access Category based on operator classification. When there are an Access Category based on operator classification and a standardized Access Category to both of which an access attempt can be categorized, and the standardized Access Category is 0 or 2, the UE applies the standardized Access Category.

NOTE 3: Includes Real-Time Text (RTT).

NOTE 4: Includes IMS Messaging.

NOTE 5: Includes IMS registration related signalling, e.g. IMS initial registration, re-registration, and subscription refresh.

NOTE 6: Applies to access of a NB-IoT-capable UEto a NB-IOT cell connected to 5GC when the UE is authorized to send exception data.

UE Route Selection Policy (URSP)

The URSP is defined and is a set of one or more URSP rules, where a URSP rule is composed of:

a) A precedence value of the URSP rule identifying the precedence of the URSP rule among all the existing URSP rules;

b) A traffic descriptor, including either:

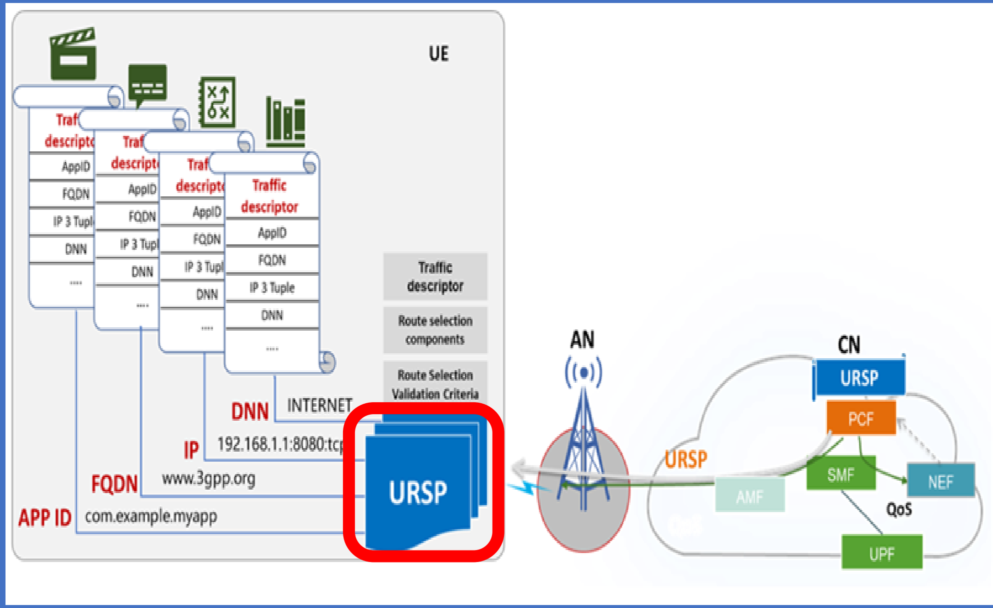
1) match-all traffic descriptor; or
2) at least one of the following components:
   - A) one or more application identifiers;
   - B) one or more IP 3 tuples i.e. the destination IP address, the destination port number, and the protocol in use above the IP;
   - C) one or more non-IP descriptors, i.e. destination information of non-IP traffic;
   - D) one or more DNNs;
   - E) one or more connection capabilities; and
   - F) one or more domain descriptors, i.e. destination FQDN(s) or a regular expression as a domain name matching criteria; and

c) one or more route selection descriptors each consisting of a precedence value of the route selection descriptor and either

1) one PDU session type and, optionally, one or more of the followings:
   - A) SSC mode;
   - B) 1 or more S-NSSAIs;
   - C) 1 or more DNNs;
   - D) Void;
   - E) preferred Access Type;
   - F) Multi-Access Preference;
   - G) a Time Window; and
   - H) Location Criteria;

2) non-seamless non-3GPP offload indication; or

3) 5G ProSe Layer-3 UE-to-network relay offload indication.



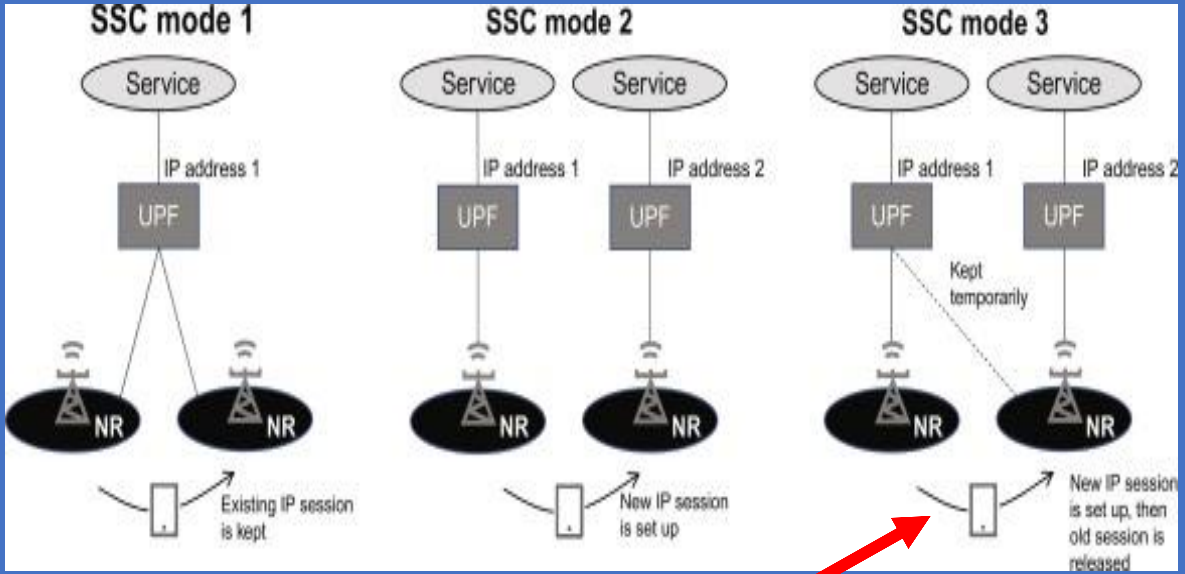
The following three (3) modes are specified with further details provided in the next clause:

- With **SSC mode 1**, the Network preserves the Connectivity service provided to the UE. For the case of *PDU Session of IPv4 or IPv6 or IPv4v6 type, the IP address is preserved*.

- With **SSC mode 2,** the Network may release the connectivity service delivered to the UE and release the corresponding PDU Session(s). For the case of *IPv4 or IPv6 or IPv4v6 type*, the release of the PDU Session induces the release of IP address(es) that had been allocated to the UE.

- With **SSC mode 3**, changes to the User Plane can be visible to the UE, while the network ensures that the **UE suffers no loss of connectivity**. A connection through new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. For the case of **IPv4 or IPv6 or IPv4v6 type**, the IP address is not preserved in this mode when the PDU Session Anchor changes.

NOTE: The addition/removal procedure of additional PDU Session Anchor in a PDU Session for local access to a DN is independent from the SSC mode of the PDU Session.



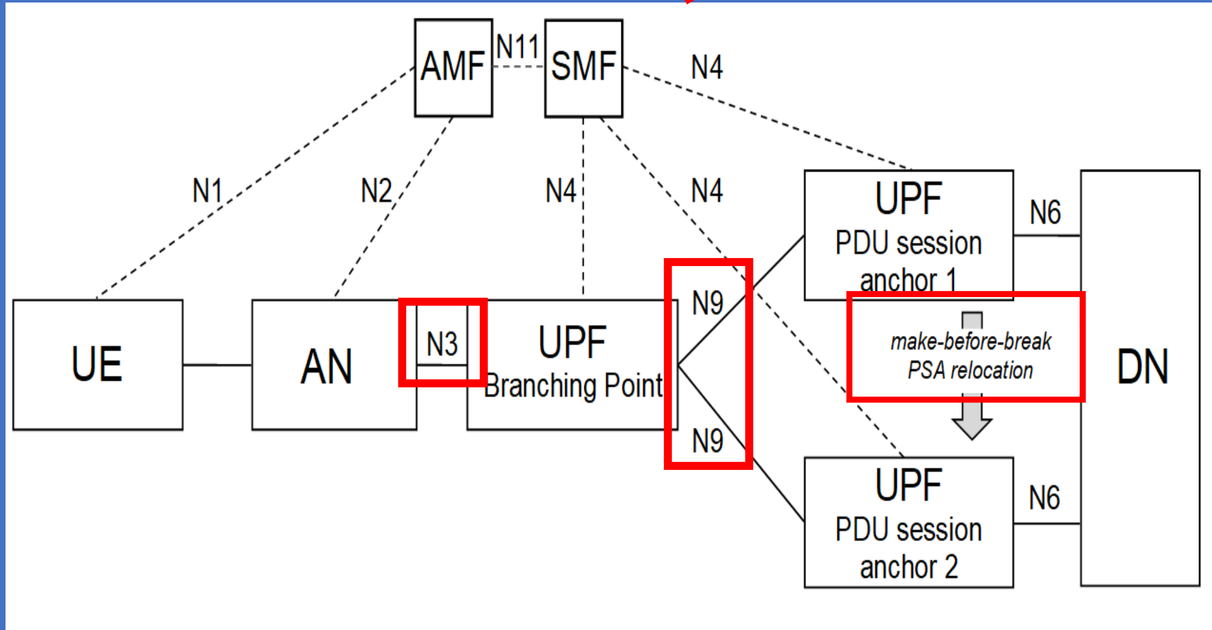


Figure 5.6.4.3-1: Multi-homed PDU Session: service continuity case

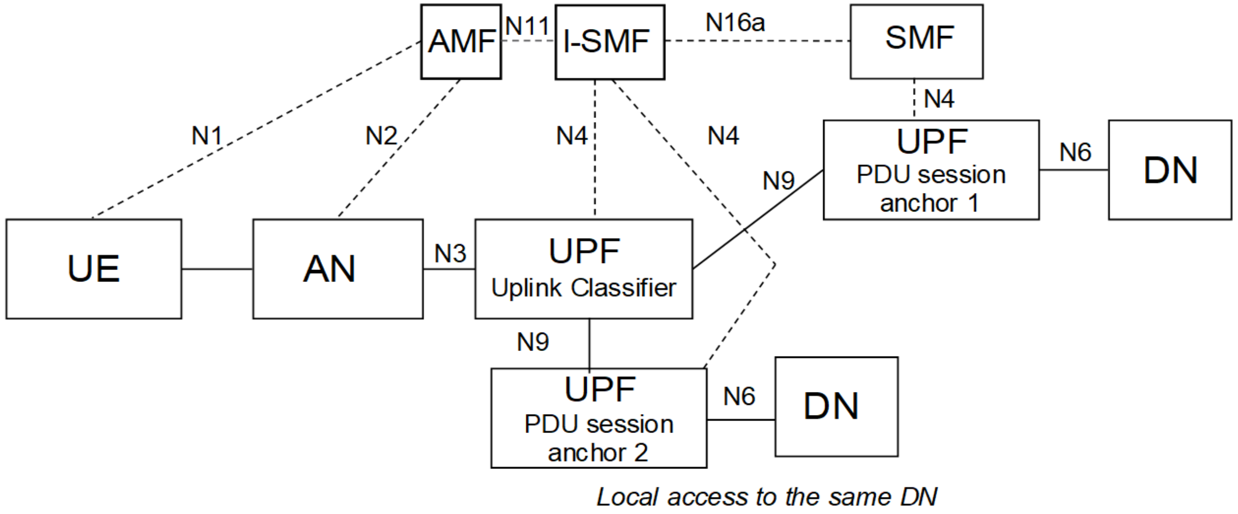
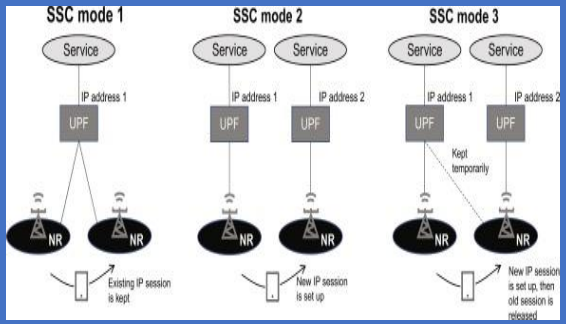


Figure 5.34.4-1: User plane Architecture for the Uplink Classifier controlled by I-SMF



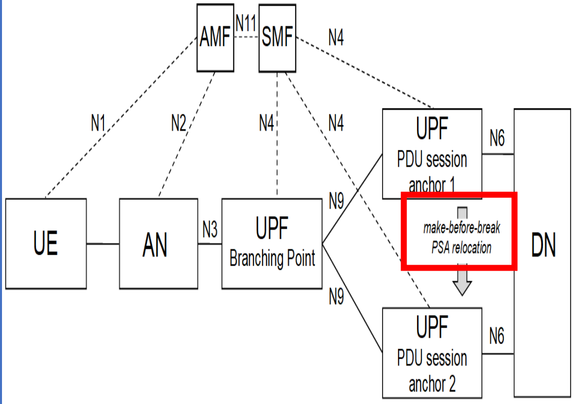


Figure 5.6.4.3-1: Multi-homed PDU Session: service continuity case

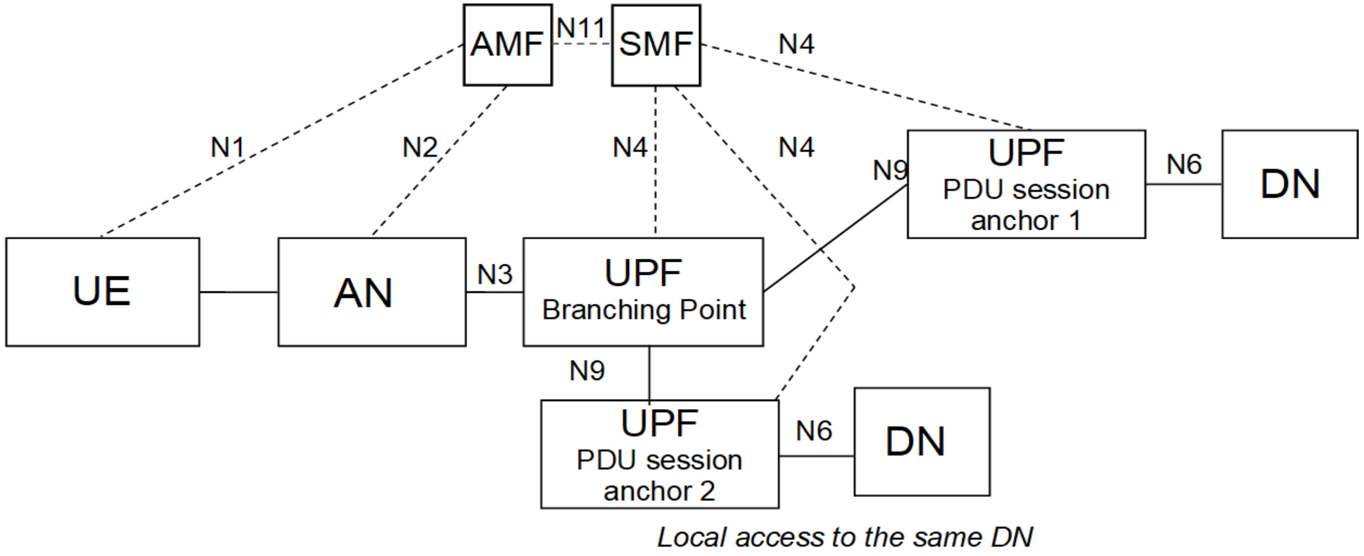


Figure 5.6.4.3-2: Multi-homed PDU Session: local access to same DN

5GS Support for Ultra Reliable Low Latency Communication (URLLC)

Redundant Transmission for High Reliability Communication

Dual Connectivity based End to End (E2E) Redundant User Plane (UP) Paths

The redundant User Plane (UP) set up applies to both IP and Ethernet PDU Sessions.

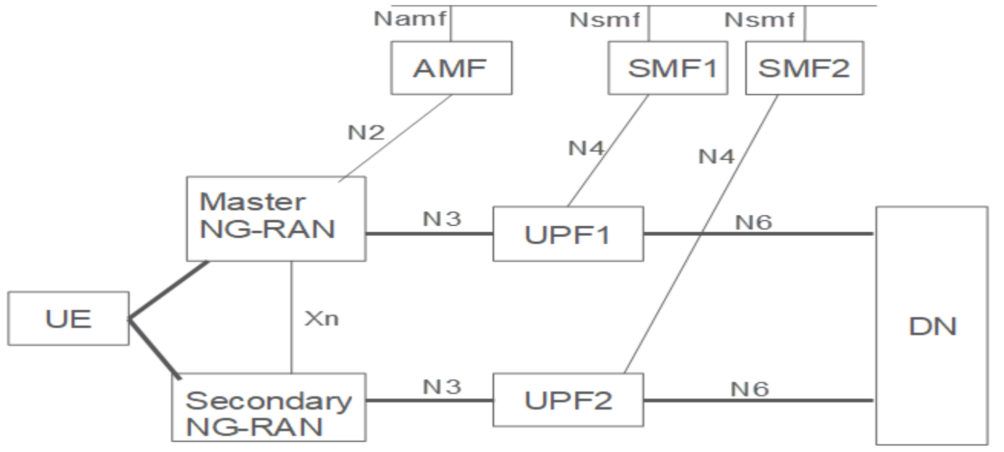


Fig. Example for E2E Redundant User Plane paths using Dual Connectivity

Support of Redundant Transmission on N3/N9 Interfaces

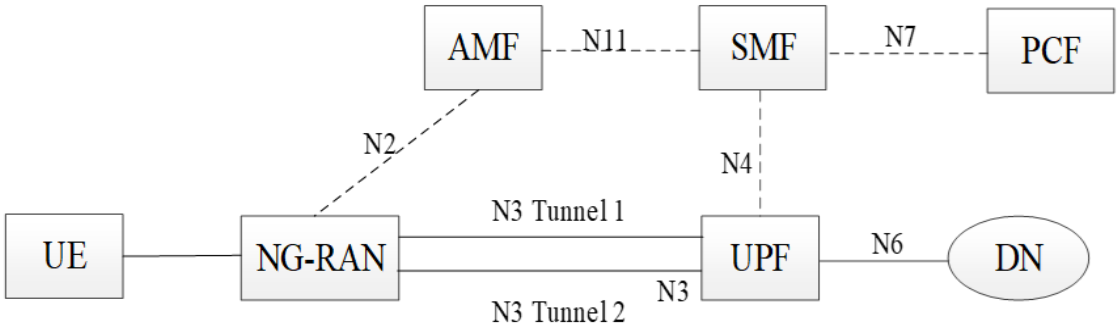


Fig.: Redundant Transmission with two N3 tunnels between the PSA UPF and a single NG-RAN Node

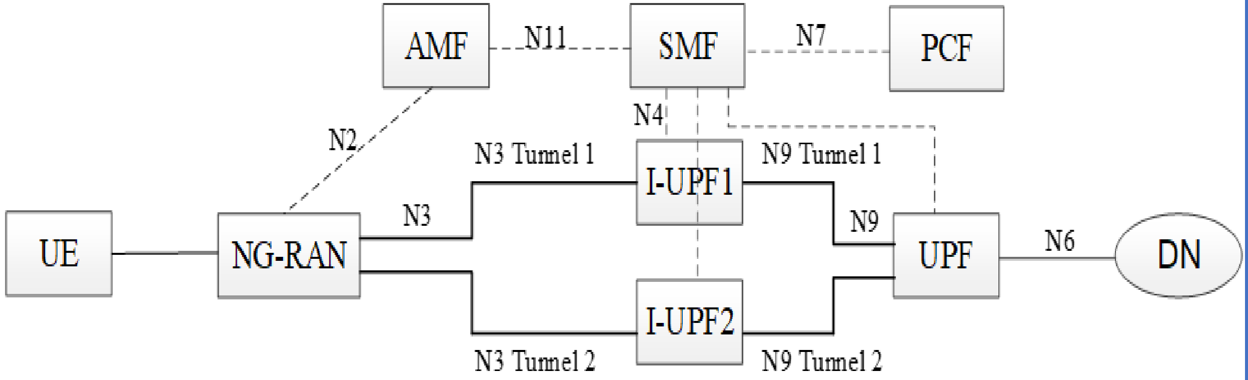


Fig: Two N3 and N9 tunnels between NG-RAN and PSA UPF for redundant transmission

5G System Architecture Rel. 16 Access Traffic Steering, Switch and Splitting (ATSSS)

The ATSSS feature enables a Multi-Access (MA) PDU Connectivity Service, which can exchange PDUs between the UE and a Data Network (DN) by simultaneously using one (1) 3GPP Access Network and one (1) non-3GPP Access Network and two (2) independent N3/N9 tunnels between the PSA and RAN/AN.

The Multi-Access PDU Connectivity Service is realized by establishing a Multi-Access PDU (MA PDU) Session, i. e. **a PDU Session that may have User-Plane (UP) Rsource on two(2) Access Networks (ANs).**

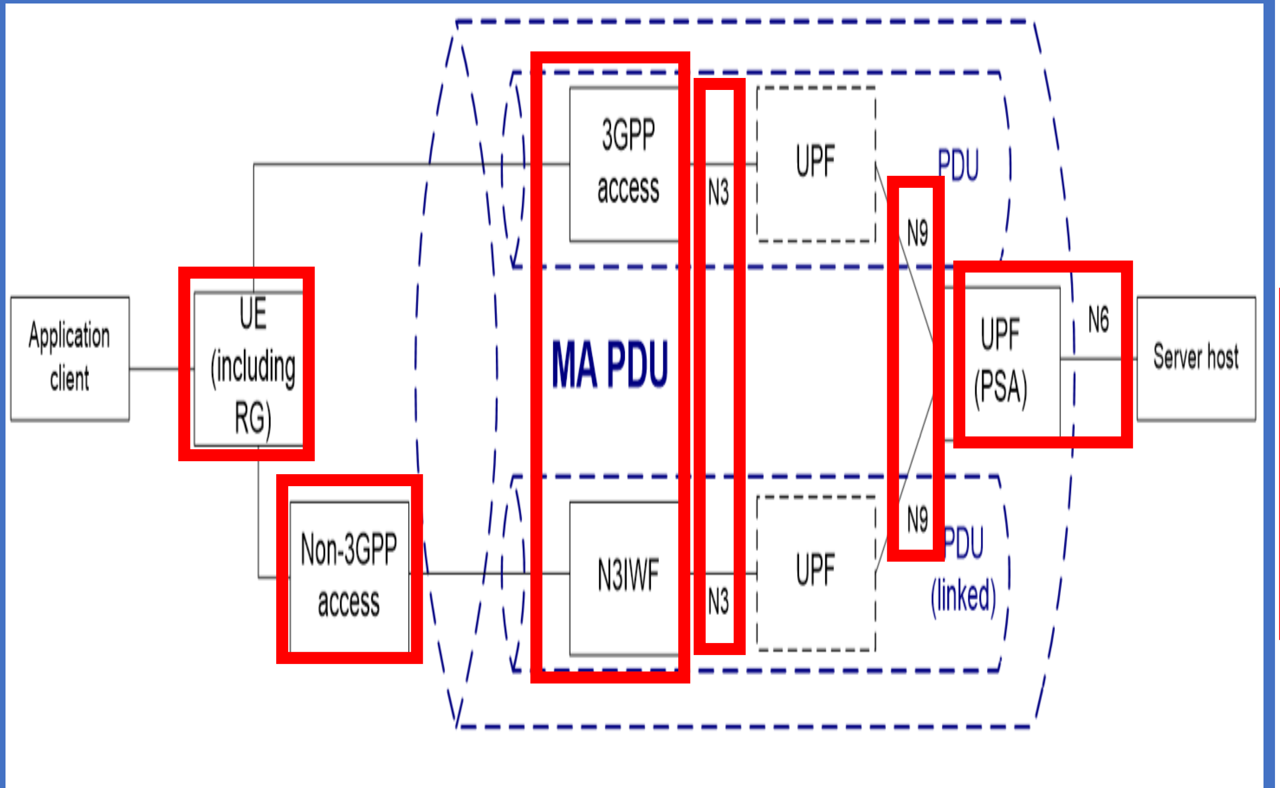


Figure 1: MA PDU session

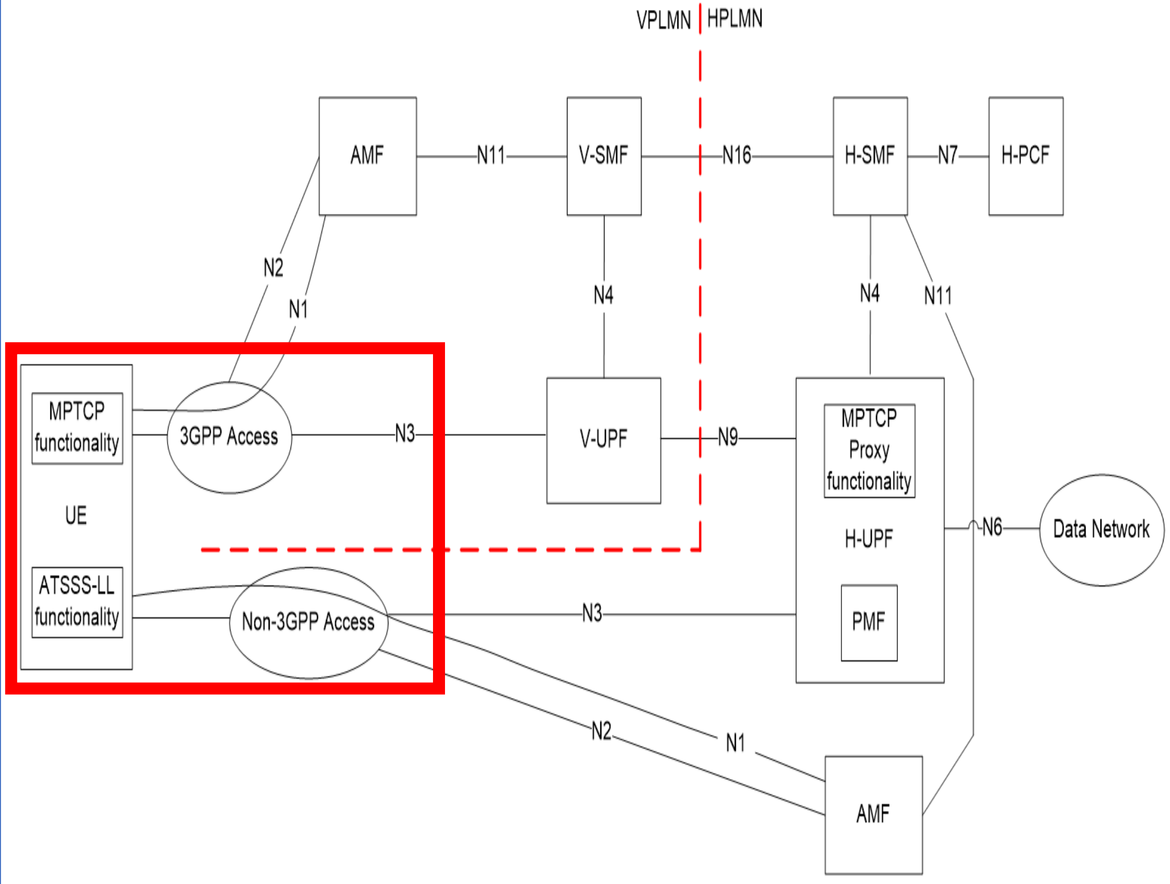


Figure 4.2.10-3: Roaming with Home-routed architecture for ATSSS support (UE registered to different PLMNs)

5.5 Use case: UE accessing Services provided by PIN Devices behind 5G enabled gateway(s)

5.5.1 Description

There are more and more PIN Devices, e.g. media server, printer, smart thermostat/sprinkler/blinds NAS server, etc., that can provide services for users at home or out of home. These PIN devices are usually behind a wireless gateway. In recent years, there are some security risks found in such settings due to port forwarding and unsecure connectivity provided by the wireless gateway for in home devices.

When considering the gateway with 5G capability for accessing 5G services, e.g. UE or evolved Residential Gateway (eRG), it is important to enable the support of the secure connectivity for allowing authorized users from anywhere in the world to access authorized services provided by these PIN Devices in terms of user authentication and authorization.

Figure 5.5.1-1 shows the scenarios of the 5G network enabling connectivity service support for the UE using 3GPP indirect (case a) or direct (case b) communication or non-3GPP access (case c) to access services provided by PIN Devices. Each PIN Device may provide one or more services. For example, the PIN Device is a media server, smart TV, smart video doorbell, etc., which provide one media service. For another example, the PIN Device is a NAS server which can provide multiple services, e.g. media service, web server service, live security cams services, etc.

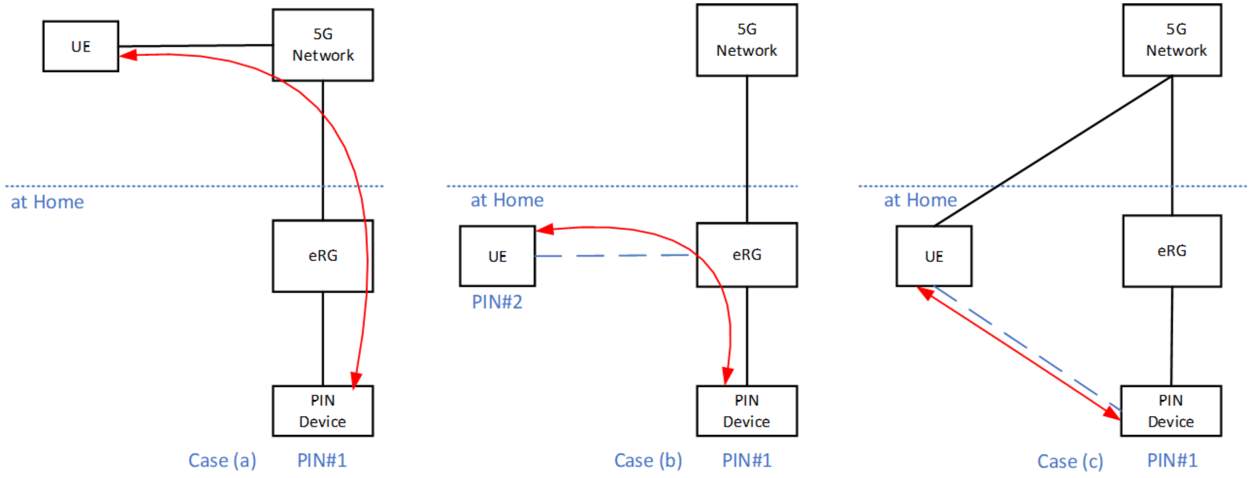


Figure 5.5.1-1: 5G network support for a User/UE accessing services provided by in Home Devices

Residential Gateway (RG):

The Residential Gateway (RG) is a Device providing, e.g.

- Voice,
- Data,
- Broadcast Video,
- Video on Demand,

to other Devices in Customer Premises.

In 5G Architecture, 3GPP, in collaboration with the BroadBand Forum (**BBF**), has specified UC solutions where a single 5G Core Network is used to also control Fixed Broadband Access. Solutions like 5G LAN & UE relaying have been specified for **Residential UCs & Traffic Scenarios (e.g. Homes & Small Offices**) & identifies related New Potential Functional Requirements & Potential Key Performance Requirements in the following three (3) Areas: 1. Enhancements for Wireline Wireless Convergence, 2. Enhancements for Fixed LAN - 5GLAN integration, & 3. Enhancements for indoor Small Base Stations. **For 5G Services that require specific QoS (e.g. Guaranteed flow Bit Rate (GBR), Latency) or e.g. that rely on Edge Applications**, it is important that the 5G Network can differentiate the related Service Data Flows in order to treat them accordingly. This also applies in case **a PRAS is connected via an evolved Residential Gateway (eRG)** & an indoor infrastructure. The 5G Capabilities (e.g., High Performance, Long-Distance Access, Mobility & Security) can be used to build a Secure Connection between the 5G LAN & the fixed IP VPN. E.g. when People are working from Home, they probably need to access the Enterprise's intranet by using the Devices connecting to the Home 5G LAN. The Connection of 5G LAN with fixed IP VPN aims to enable the Devices within the 5G LAN to access the Intranet through the Fixed IP VPN. This use case intends to make use of the 5G capabilities (e.g., high performance, long-distance access, mobility and security) to build a secure connection between the 5G LAN and the fixed IP VPN. The **evolved Residential Gateway** (**eRG**) is a Device providing **Services as e.g. Voice, Data, Broadcast Video, Video on Demand, AR/VR** etc. to other Devices in Customer Premises (e.g. Homes, Work Offices). 5G UE including eRG can enable a Multi-access (MA) PDU Connectivity Service, in which case the PDU Session is simultaneously associated **with both 3GPP Access & Non-3GPP Access & simultaneously associated with two (2) independent N3/N9 tunnels** between the PSA & RAN/AN (as shown in Figures below).

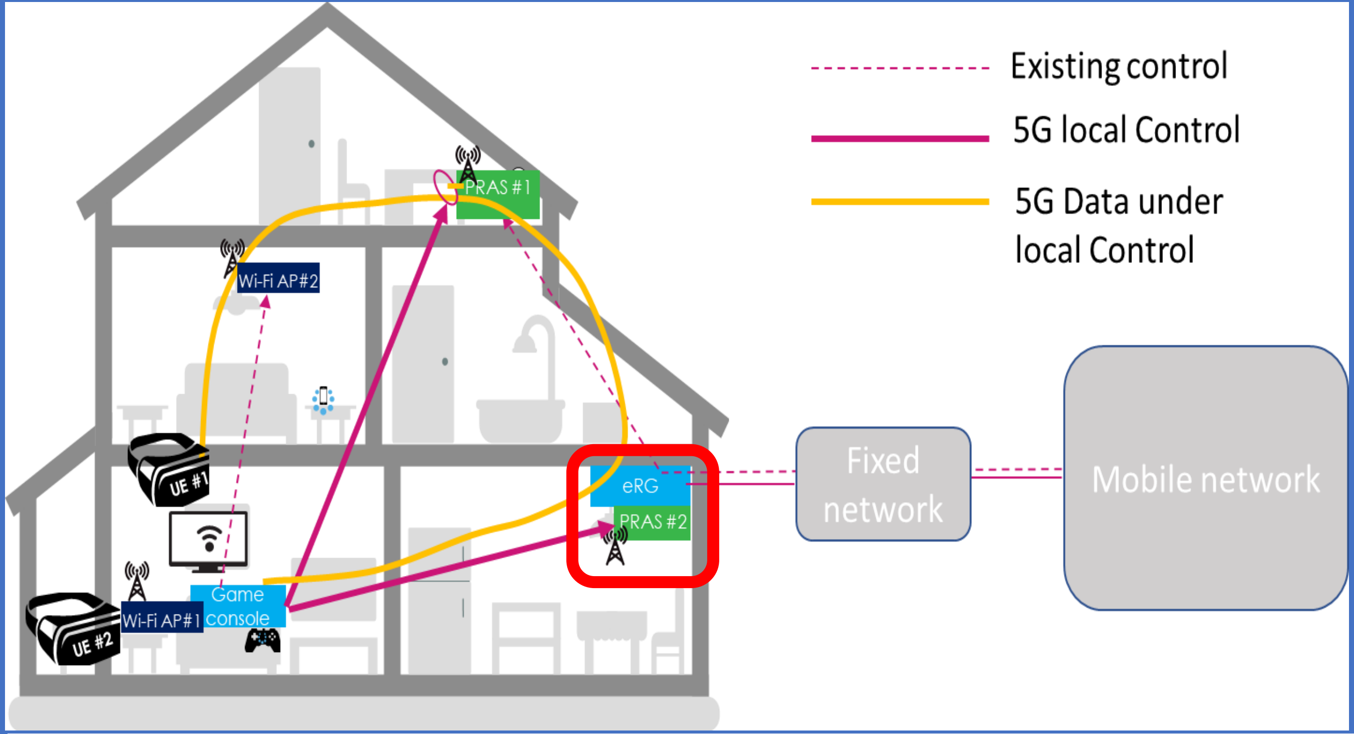


Fig. 5.12.1-1. 5G Local Control of Premise Radio Access Stations (PRASs) for UE to access CPN Device

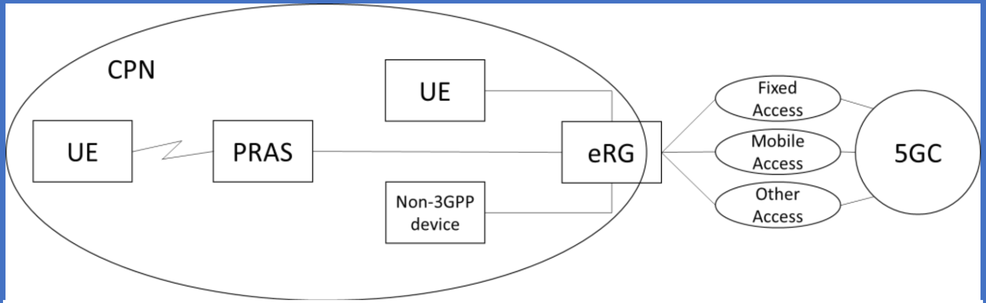


Fig. A.2-1: Customer Premises Network (CPN) connected to 5GC

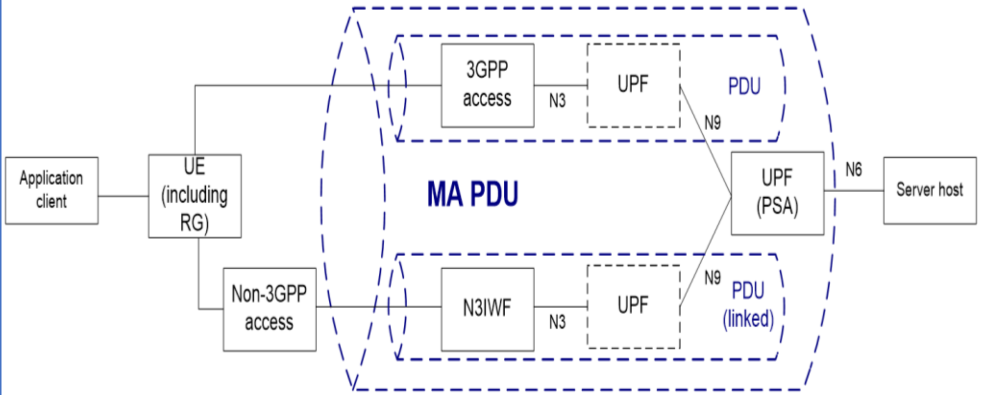


Fig. 1   5G enabled Multi Access (MA) PDU Session

Table 3: Performance Requirements for High Data Rate and Traffic Density Scenarios

	Scenario	Experienced data rate (DL)	Experienced data rate (UL)	Area traffic capacity (DL)	Area traffic capacity (UL)	Overall user density	Activity factor	UE speed	Coverage
1	Urban macro	50 Mbit/s	25 Mbit/s	100 Gbit/s/km^2 (note 4)	50 Gbit/s/km^2 (note 4)	10 000/km^2	20 %	Pedestrians and users in vehicles (up to 120 km/h	Full network (note 1)
2	Rural macro	50 Mbit/s	25 Mbit/s	1 Gbit/s/km^2 (note 4)	500 Mbit/s/km^2 (note 4)	100/km^2	20 %	Pedestrians and users in vehicles (up to 120 km/h	Full network (note 1)
3	Indoor hotspot	1 Gbit/s	500 Mbit/s	15 Tbit/s/km^2	2 Tbit/s/km^2	250 000/km^2	note 2	Pedestrians	Office and residential (note 2) (note 3)
4	Broadband access in a crowd	25 Mbit/s	50 Mbit/s	[3,75] Tbit/s/km^2	[7,5] Tbit/s/km^2	[500 000]/km^2	30 %	Pedestrians	Confined area
5	Dense urban	300 Mbit/s	50 Mbit/s	750 Gbit/s/km^2 (note 4)	125 Gbit/s/km^2 (note 4)	25 000/km^2	10 %	Pedestrians and users in vehicles (up to 60 km/h)	Downtown (note 1)
6	Broadcast-like services	Maximum 200 Mbit/s (per TV channel)	N/A or modest (e.g. 500 kbit/s per user)	N/A	N/A	[15] TV channels of [20 Mbit/s] on one carrier	N/A	Stationary users, pedestrians and users in vehicles (up to 500 km/h)	Full network (note 1)
7	High-speed train	50 Mbit/s	25 Mbit/s	15 Gbit/s/train	7,5 Gbit/s/train	1 000/train	30 %	Users in trains (up to 500 km/h)	Along railways (note 1)
8	High-speed vehicle	50 Mbit/s	25 Mbit/s	[100] Gbit/s/km^2	[50] Gbit/s/km^2	4 000/km^2	50 %	Users in vehicles (up to 250 km/h)	Along roads (note 1)
9	Airplanes connectivity	15 Mbit/s	7,5 Mbit/s	1,2 Gbit/s/plane	600 Mbit/s/plane	400/plane	20 %	Users in airplanes (up to 1 000 km/h)	(note 1)

NOTE 1: For users in vehicles, the UE can be connected to the network directly, or via an on-board moving base station.
NOTE 2: A certain traffic mix is assumed; only some users use services that require the highest data rates [2].
NOTE 3: For interactive audio and video services, for example, virtual meetings, the required two-way end-to-end latency (UL and DL) is 2-4 ms while the corresponding experienced data rate needs to be up to 8K 3D video [300 Mbit/s] in uplink and downlink.
NOTE 4: These values are derived based on overall user density. Detailed information can be found in [10].
NOTE 5: All the values in this table are targeted values and not strict requirements.

Table 4: Performance Requirements for Horizontal and Vertical Positioning Service Levels

Positioning service level	Absolute(A) or Relative(R) positioning	Accuracy (95 % confidence level): Horizontal Accuracy	Accuracy (95 % confidence level): Vertical Accuracy (note 1)	Positioning service availability	Positioning service latency	Coverage, environment of use and UE velocity: 5G positioning service area	Coverage, environment of use and UE velocity: 5G enhanced positioning service area (note 2): Outdoor and tunnels	Coverage, environment of use and UE velocity: 5G enhanced positioning service area (note 2): Indoor
1	A	10 m	3 m	95 %	1 s	Indoor - up to 30 km/h Outdoor (rural and urban) up to 250 km/h	NA	Indoor - up to 30 km/h
2	A	3 m	3 m	99 %	1 s	Outdoor (rural and urban) up to 500 km/h for trains and up to 250 km/h for other vehicles	Outdoor (dense urban) up to 60 km/h Along roads up to 250 km/h and along railways up to 500 km/h	Indoor - up to 30 km/h
3	A	1 m	2 m	99 %	1 s	Outdoor (rural and urban) up to 500 km/h for trains and up to 250 km/h for other vehicles	Outdoor (dense urban) up to 60 km/h Along roads up to 250 km/h and along railways up to 500 km/h	Indoor - up to 30 km/h
4	A	1 m	2 m	99,9 %	15 ms	NA	NA	Indoor - up to 30 km/h
5	A	0,3 m	2 m	99 %	1 s	Outdoor (rural) up to 250 km/h	Outdoor (dense urban) up to 60 km/h Along roads and along railways up to 250 km/h	Indoor - up to 30 km/h
6	A	0,3 m	2 m	99,9 %	10 ms	NA	Outdoor (dense urban) up to 60 km/h	Indoor - up to 30 km/h
7	R	0,2 m	0,2 m	99 %	1 s	Indoor and outdoor (rural, urban, dense urban) up to 30 km/h Relative positioning is between two UEs within 10 m of each other or between one UE and 5G positioning nodes within 10 m of each other (note 3)		

NOTE 1: The objective for the vertical positioning requirement is to determine the floor for indoor use cases and to distinguish between superposed tracks for road and rail use cases (e.g. bridges).
NOTE 2: Indoor includes location inside buildings such as offices, hospital, industrial buildings.
NOTE 3: 5G positioning nodes are infrastructure equipment deployed in the service area to enhance positioning capabilities (e.g. beacons deployed on the perimeter of a rendezvous area or on the side of a warehouse).

Table: Standardized 5QI to QoS Characteristics Mapping

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget (NOTE 3)	Packet Error Rate	Default Maximum Data Burst Volume (NOTE 2)	Default Averaging Window	Example Services
1	GBR (NOTE 1)	20	100 ms (NOTE 11, NOTE 13)	10^{-2}	N/A	2000 ms	Conversational Voice
2		40	150 ms (NOTE 11, NOTE 13)	10^{-3}	N/A	2000 ms	Conversational Video (Live Streaming)
3		30	50 ms (NOTE 11, NOTE 13)	10^{-3}	N/A	2000 ms	Real Time Gaming, V2X messages (see TS 23.287 [121]). Electricity distribution – medium voltage, Process automation monitoring
4		50	300 ms (NOTE 11, NOTE 13)	10^{-6}	N/A	2000 ms	Non-Conversational Video (Buffered Streaming)
65 (NOTE 9, NOTE 12)		7	75 ms (NOTE 7, NOTE 8)	10^{-2}	N/A	2000 ms	Mission Critical user plane Push To Talk voice (e.g. MCPTT)
66 (NOTE 12)		20	100 ms (NOTE 10, NOTE 13)	10^{-2}	N/A	2000 ms	Non-Mission-Critical user plane Push To Talk voice
67 (NOTE 12)		15	100 ms (NOTE 10, NOTE 13)	10^{-3}	N/A	2000 ms	Mission Critical Video user plane
75 (NOTE 14)							
71		56	150 ms (NOTE 11, NOTE 13, NOTE 15)	10^{-6}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
72		56	300 ms (NOTE 11, NOTE 13, NOTE 15)	10^{-4}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
73		56	300 ms (NOTE 11, NOTE 13, NOTE 15)	10^{-8}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
74		56	500 ms (NOTE 11, NOTE 15)	10^{-8}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
76		56	500 ms (NOTE 11, NOTE 13, NOTE 15)	10^{-4}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
5	Non-GBR (NOTE 1)	10	100 ms NOTE 10, NOTE 13)	10^{-6}	N/A	N/A	IMS Signalling
6		60	300 ms (NOTE 10, NOTE 13)	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		70	100 ms (NOTE 10, NOTE 13)	10^{-3}	N/A	N/A	Voice, Video (Live Streaming) Interactive Gaming
8		80	300 ms (NOTE 13)	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		90					
69 (NOTE 9, NOTE 12)		5	60 ms (NOTE 7, NOTE 8)	10^{-6}	N/A	N/A	Mission Critical delay sensitive signalling (e.g. MC-PTT signalling)
70 (NOTE 12)		55	200 ms (NOTE 7, NOTE 10)	10^{-6}	N/A	N/A	Mission Critical Data (e.g. example services are the same as 5QI 6/8/9)
79		65	50 ms (NOTE 10, NOTE 13)	10^{-2}	N/A	N/A	V2X messages (see TS 23.287 [121])
80		68	10 ms (NOTE 5, NOTE 10)	10^{-6}	N/A	N/A	Low Latency eMBB applications Augmented Reality
10		90	832ms (NOTE 13) (NOTE 17)	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.) and any service that can be used over satellite access type with these characteristics
82	Delay-critical GBR	19	10 ms (NOTE 4)	10^{-4}	255 bytes	2000 ms	Discrete Automation (see TS 22.261 [2])
83		22	10 ms (NOTE 4)	10^{-4}	1354 bytes (NOTE 3)	2000 ms	Discrete Automation (see TS 22.261 [2]); V2X messages (UE - RSU Platooning, Advanced Driving: Cooperative Lane Change with low LoA. See TS 22.186 [111], TS 23.287 [121])
84		24	30 ms (NOTE 6)	10^{-5}	1354 bytes (NOTE 3)	2000 ms	Intelligent transport systems (see TS 22.261 [2])
85		21	5 ms (NOTE 5)	10^{-5}	255 bytes	2000 ms	Electricity Distribution- high voltage (see TS 22.261 [2]). V2X messages (Remote Driving. See TS 22.186 [111], NOTE 16, see TS 23.287 [121])
86		18	5 ms (NOTE 5)	10^{-4}	1354 bytes	2000 ms	V2X messages (Advanced Driving: Collision Avoidance, Platooning with high LoA. See TS 22.186 [111], TS 23.287 [121])
87		25	5 ms (NOTE 4)	10^{-3}	500 bytes	2000 ms	Interactive Service - Motion tracking data, (see TS 22.261 [2])
88		25	10 ms (NOTE 4)	10^{-3}	1125 bytes	2000 ms	Interactive Service - Motion tracking data, (see TS 22.261 [2])
89		25	15 ms (NOTE 4)	10^{-4}	17000 bytes	2000 ms	Visual content for cloud/edge/split rendering (see TS 22.261 [2])
90		25	20 ms (NOTE 4)	10^{-4}	63000 bytes	2000 ms	Visual content for cloud/edge/split rendering (see TS 22.261 [2])

NOTE 1: A packet which is delayed more than PDB is not counted as lost, thus not included in the PER.

NOTE 2: It is required that default MDBV is supported by a PLMN supporting the related 5QIs.

NOTE 3: The Maximum Transfer Unit (MTU) size considerations in clause 9.3 and Annex C of TS 23.060 [56] are also applicable. IP fragmentation may have impacts to CN PDB, and details are provided in clause 5.6.10.

NOTE 4: A static value for the CN PDB of 1 ms for the delay between a UPF terminating N6 and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. When a dynamic CN PDB is used, see clause 5.7.3.4.

NOTE 5: A static value for the CN PDB of 2 ms for the delay between a UPF terminating N6 and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. When a dynamic CN PDB is used, see clause 5.7.3.4.

NOTE 6: A static value for the CN PDB of 5 ms for the delay between a UPF terminating N6 and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. When a dynamic CN PDB is used, see clause 5.7.3.4.

NOTE 7: For Mission Critical services, it may be assumed that the UPF terminating N6 is located "close" to the 5G_AN (roughly 10 ms) and is not normally used in a long distance, home routed roaming situation. Hence a static value for the CN PDB of 10 ms for the delay between a UPF terminating N6 and a 5G_AN should be subtracted from this PDB to derive the packet delay budget that applies to the radio interface.

NOTE 8: In both RRC Idle and RRC Connected mode, the PDB requirement for these 5QIs can be relaxed (but not to a value greater than 320 ms) for the first packet(s) in a downlink data or signalling burst in order to permit reasonable battery saving (DRX) techniques.

NOTE 9: It is expected that 5QI-65 and 5QI-69 are used together to provide Mission Critical Push to Talk service (e.g. 5QI-5 is not used for signalling). It is expected that the amount of traffic per UE will be similar or less compared to the IMS signalling.

NOTE 10: In both RRC Idle and RRC Connected mode, the PDB requirement for these 5QIs can be relaxed for the first packet(s) in a downlink data or signalling burst in order to permit battery saving (DRX) techniques.

NOTE 11: In RRC Idle mode, the PDB requirement for these 5QIs can be relaxed for the first packet(s) in a downlink data or signalling burst in order to permit battery saving (DRX) techniques.

NOTE 12: This 5QI value can only be assigned upon request from the network side. The UE and any application running on the UE is not allowed to request this 5QI value.

NOTE 13: A static value for the CN PDB of 20 ms for the delay between a UPF terminating N6 and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface.

NOTE 14: This 5QI is not supported in this Release of the specification as it is only used for transmission of V2X messages over MBMS bearers as defined in TS 23.285 [72] but the value is reserved for future use.

NOTE 15: For "live" uplink streaming (see TS 26.238 [76]), guidelines for PDB values of the different 5QIs correspond to the latency configurations defined in TR 26.939 [77]. In order to support higher latency reliable streaming services (above 500ms PDB), if different PDB and PER combinations are needed these configurations will have to use non-standardised 5QIs.

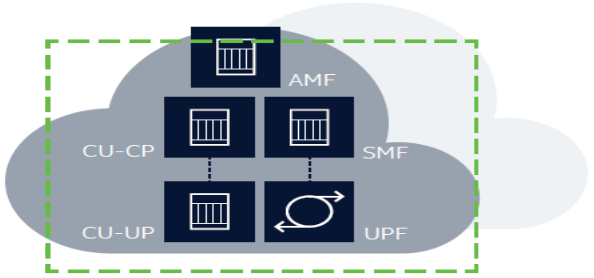
NOTE 16: These services are expected to need much larger MDBV values to be signalled to the RAN. Support for such larger MDBV values with low latency and high reliability is likely to require a suitable RAN configuration, for which, the simulation scenarios in TR 38.824 [112] may contain some guidance.

NOTE 17: The worst case one way propagation delay for GEO satellite is expected to be ~270ms, ~ 21 ms for LEO at 1200km, and 13 ms for LEO at 600km. The UL scheduling delay that needs to be added is also typically 1 RTD e.g. ~540ms for GEO, ~42ms for LEO at 1200km, and ~26 ms for LEO at 600km. Based on that, the 5G-AN Packet delay budget is not applicable for 5QIs that require 5G-AN PDB lower than the sum of these values when the specific types of satellite access are used (see TS 38.300 [27]). 5QI-<New Value> can accommodate the worst case PDB for GEO satellite type.

Editor's note: The worst case PDB of 832 ms for satellite access need to be verified with RAN and may need to be adjusted based on RAN feedback.

NOTE: It is preferred that a value less than 64 is allocated for any new standardised 5QI of Non-GBR resource type. This is to allow for option 1 to be used as described in clause 5.7.1.3 (as the QFI is limited to less than 64).

5G Cloud Native Adoption SCP



RAN-Core convergence

4.2.3 Non-roaming reference architecture

Figure 4.2.3-1 depicts the non-roaming reference architecture. Service-based interfaces are used within the Control Plane.

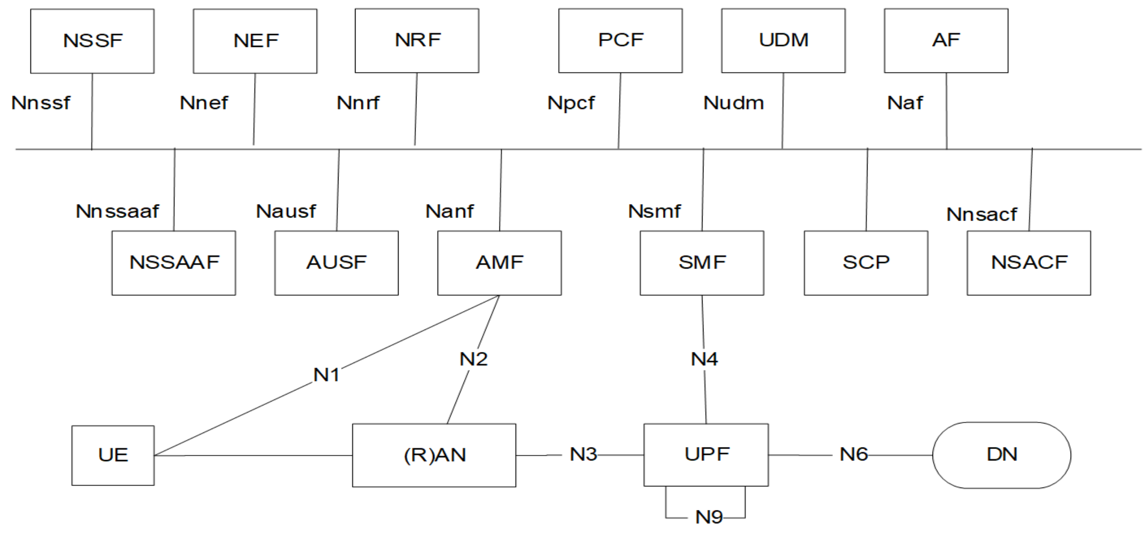


Figure 4.2.3-1: 5G System architecture

NOTE: If an SCP is deployed it can be used for indirect communication between NFs and NF services as described in Annex E. SCP does not expose services itself.

4.1.4 Cloud Native Network Functions

The term "Cloud Native" originates from the ability to realise an **Economy at Scale – HyperScale** – through

- Agile Code Development and
- Code Integration Design Patterns.

At the Core is the idea to de-compose a Function into Microservices that can exist as Multiple Instances to allow to scale with demand.

Cloud-native is commonly agreed to **define Applications that follow the 12-Factor Methodology** (https://12factor.net/) as outlined by various **Market Leaders (as Microsoft & VmWare** and summarised in Table 2.

Thus, if VNFs follow the aforementioned 12-Factor Code Development and Integration Methodology, they can operate as Cloud Native Network Functions (CNFs).

1. 3GPP 5G System Architecture Service Communication Proxy NF to NF Service Interaction

Model A - Direct communication without NRF interaction: Neither NRF nor SCP are used. Consumers are configured with producers' "NF profiles" and directly communicate with a producer of their choice.

Model B - Direct communication with NRF interaction: Consumers do discovery by querying the NRF. Based on the discovery result, the consumer does the selection. The consumer sends the request to the selected producer.

Model C - Indirect communication without delegated discovery: Consumers do discovery by querying the NRF. Based on discovery result, the consumer does the selection of an NF Set or a specific NF instance of NF set. The consumer sends the request to the SCP containing the address of the selected service producer pointing to a NF service instance or a set of NF service instances. In the latter case, the SCP selects an NF Service instance. If possible, the SCP interacts with NRF to get selection parameters such as location, capacity, etc. The SCP routes the request to the selected NF service producer instance.

Model D - Indirect communication with delegated discovery: Consumers do not do any discovery or selection. The consumer adds any necessary discovery and selection parameters required to find a suitable producer to the service request. The SCP uses the request address and the discovery and selection parameters in the request message to route the request to a suitable producer instance. The SCP can perform discovery with an NRF and obtain a discovery result.

Figure E.1-1 depicts the different communication models.

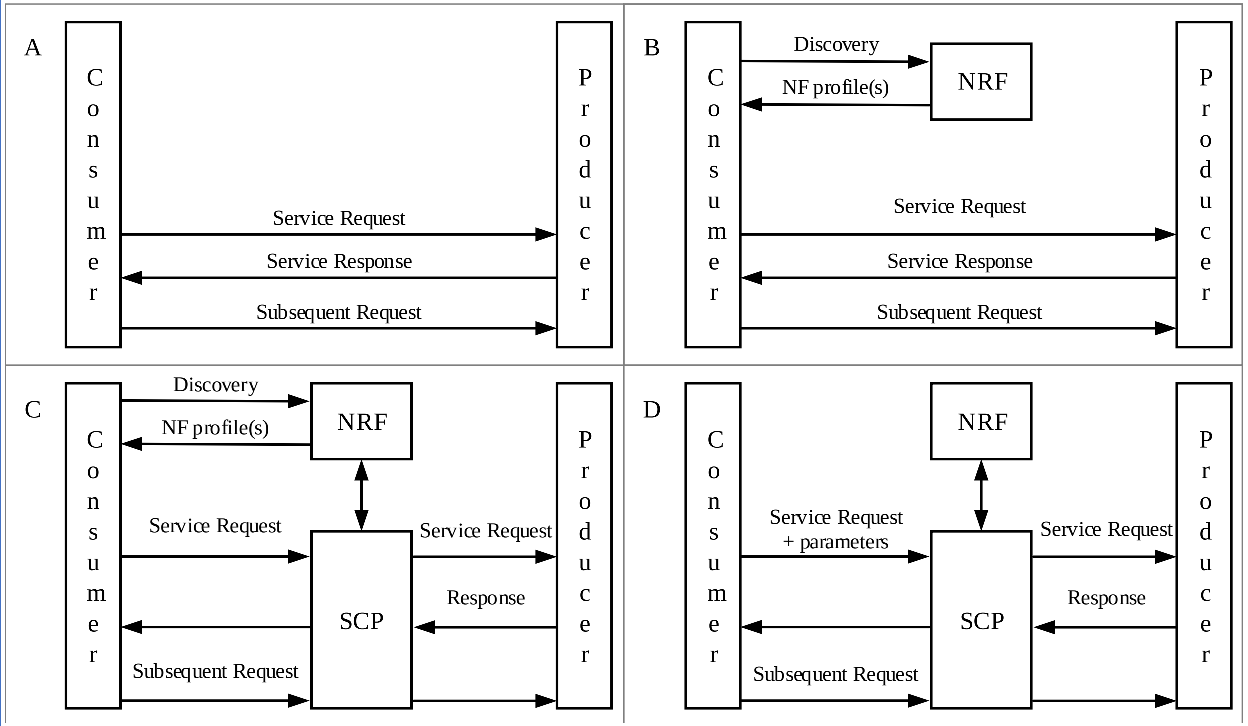


Figure E.1-1: Communication models for NF/NF services interaction

2. 5G UP GW SEPP and SeCoP - 2

Solution Key Issue #27: Policy based Authorization for Indirect Communication between Network Functions (NFs)

This solution addresses KI #22 - Authorization of NF Service Access in Indirect Communication.

The solution proposes Policy-based Authorization of NF Consumer requests in the **SeCoP (*Service Communication Proxy)*** associated with the NF Producer.

A Set of Policies are provisioned in the SeCoP which allow the SeCoP to recognise an incoming Service Request from a NF Consumer and determine whether to allow the request and set of services that can be allowed for the requesting NF.

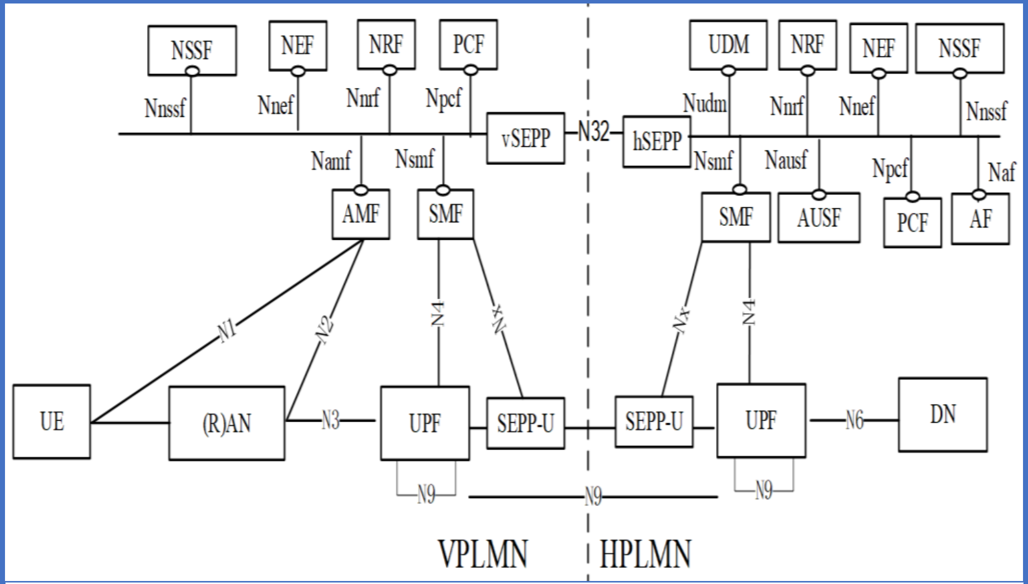


Fig.: UP GW Function SEPP (Secure Edge Protection Proxy) for the inter - PLMN N9 Interface

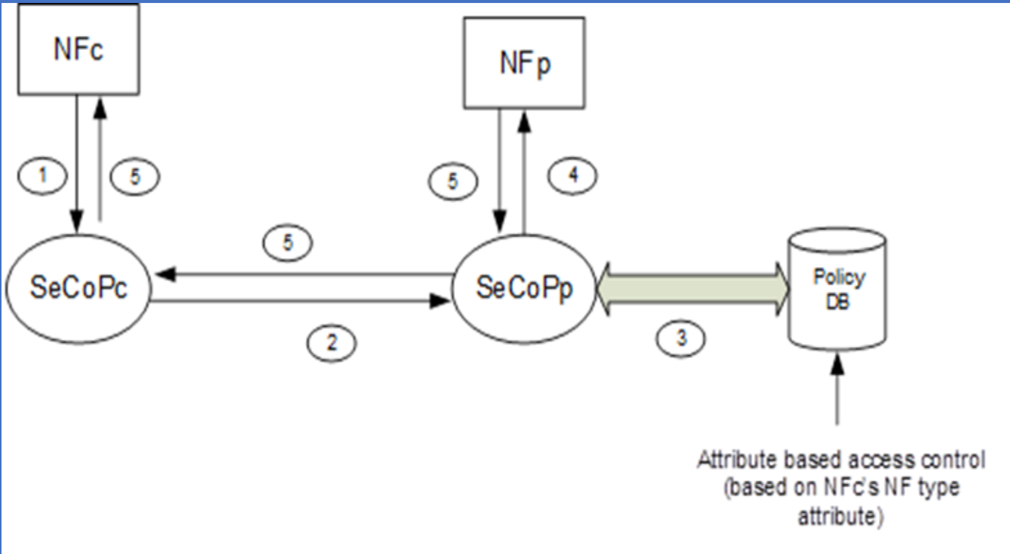


Fig.: Policy based Service Access authorization of NF consumer

Cloud Native

Thus, if VNFs follow the aforementioned 12-Factor Code Development and Integration Methodology, they can operate as Cloud Native Network Functions (CNFs).

Table 2: 12-factor app properties

Number	Property	Description
1	Codebase	One codebase tracked in revision control and being able to deploy it into different production stages (development, staging, production).
2	Dependencies	Explicitly declare and isolate software dependencies through packaging.
3	Configuration	Software configuration stored in environment and not “hard coded” inside binary allowing different deployment scenarios.
4	Backing Services	Any service an individual function relies on must be treated as an attached (remote) service that can be reached over a network. Examples are databases or external service such as Twitter or Google Maps.
5	Build, release, run	Separation of software development into separate stages disallowing changes to code after build phase to enforce proper code integration workflows.
6	Processes	The application is decomposed into individual stateless processes that can be packaged as individual microservices.
7	Port binding	Mapping function from internal port to public port, e.g. public HTTP Port 80 is mapped inside instance to port 8080 where the function is listening.
8	Concurrency	Microservices of same type can be scaled out to meet demand.
9	Disposability	Maximise robustness of microservice with fast start-up and graceful shutdown.
10	Dev/prod parity	Keep development, staging, and production as similar as possible.
11	Logs	Treat logs generated by a microservice as event streams that can be analysed outside of the application.
12	Admin Processes	Run admin/management tasks as one-off processes such as database migration.

In addition to the 12 Factors, three (3) more have risen in the Cloud Community which are listed in Table 3.

Table 3: Additional three properties to the 12 factor app properties

Number	Property	Description
13	API First	Make everything a service. Assume your code will be consumed by a front-end client, gateway, or another service.
14	Telemetry	Ensuring that the microservice is designed to include the collection of monitoring, domain-specific, and health/system data as part of the logs.
15	Authentication/ Authorization	Implementation of identity across all microservices that form the application.

4.1.5 Cloud Native vs Cloudified Network Functions

Table 3: Additional three properties to the 12 factor app properties

Number	Property	Description
13	API First	Make everything a service. Assume your code will be consumed by a front-end client, gateway, or another service.
14	Telemetry	Ensuring that the microservice is designed to include the collection of monitoring, domain-specific, and health/system data as part of the logs.
15	Authentication/ Authorization	Implementation of identity across all microservices that form the application.

It becomes apparent that **VNFs implementing NFs such as:**

- **Firewalling,**
- **IP Address assignment or**
- **Switching & Routing**

might NOT be able to comply entirely with the 12-Factor Paradigm.

For instance, aiming at implementing a **3GPP SA2 Service Communication Proxy (SCP) as a CNF, a Component performing Proxy-like Routing tasks can be certainly de-composed into Micro Services based on their Workload type (e.g. Long-running Tasks versus Short Logical Operation to determine an outcome);**

However, by decomposing a NF into Microservices the newly created CNFs need to be addressable among each other based on Stateless protocols like HTTP.

The result is a typical "Chicken and the Egg" Problem!?!??!?!

4.1.5 Cloud Native vs Cloudified Network Functions

The result is a typical "Chicken and the Egg" Problem, as the CNFs were supposed to implement Service Routing, but relies on a Service Routing among them.

In addition to the 12 Factors, three (3) more have risen in the Cloud Community which are listed in Table 3.

Table 3: Additional three properties to the 12 factor app properties

Number	Property	Description
13	API First	Make everything a service. Assume your code will be consumed by a front-end client, gateway, or another service.
14	Telemetry	Ensuring that the microservice is designed to include the collection of monitoring, domain-specific, and health/system data as part of the logs.
15	Authentication/ Authorization	Implementation of identity across all microservices that form the application.

Other factors such as:

- Port Binding and
- Dev/Prod Parity

simply Do Not Apply to Functions that sit below the Transport Layer where Ports are exposed.

Furthermore, for Networking related Tasks (Routing, Firewalling, etc.) Packets from senders such as the UE that are supposed to be handled must be encapsulated in a Stateless Protocol to reach the next Microservice that forms the Networking Application.

Thus, not all VNFs can be ported to CNFs to enable an economy at scale.

Cloud Native vs Cloudified Network Functions

Furthermore, for Networking related Tasks (Routing, Firewalling, etc.) Packets from senders such as the UE that are supposed to be handled must be encapsulated in a Stateless Protocol to reach the next Microservice that forms the Networking Application.

Thus, not all VNFs can be ported to CNFs to enable an economy at scale.

However, even though not all 12 Factors can be fulfilled for some VNF types, VNFs can be Cloudified aiming at a high adoption of the Cloud Native factors without the notion of de-composing a VNF into Microservices (CNFs) that form the Application.

Thus, (it is argued) for the introduction of the term "Cloudified VNF (cVNF)" indicating the adoption of the Cloud Native factors 1-5, 10 & 11.

Table 2: 12-factor app properties

Number	Property	Description
1	Codebase	One codebase tracked in revision control and being able to deploy it into different production stages (development, staging, production).
2	Dependencies	Explicitly declare and isolate software dependencies through packaging.
3	Configuration	Software configuration stored in environment and not "hard coded" inside binary allowing different deployment scenarios.
4	Backing Services	Any service an individual function relies on must be treated as an attached (remote) service that can be reached over a network. Examples are databases or external service such as Twitter or Google Maps.
5	Build, release, run	Separation of software development into separate stages disallowing changes to code after build phase to enforce proper code integration workflows.
6	Processes	The application is decomposed into individual stateless processes that can be packaged as individual microservices.
7	Port binding	Mapping function from internal port to public port, e.g. public HTTP Port 80 is mapped inside instance to port 8080 where the function is listening.
8	Concurrency	Microservices of same type can be scaled out to meet demand.
9	Disposability	Maximise robustness of microservice with fast start-up and graceful shutdown.
10	Dev/prod parity	Keep development, staging, and production as similar as possible.
11	Logs	Treat logs generated by a microservice as event streams that can be analysed outside of the application.
12	Admin Processes	Run admin/management tasks as one-off processes such as database migration.

1. 3GPP 5G System Architecture Service Communication Proxy NF to NF Service Interaction

Annex E (informative):
Communication models for NF/NF services interaction

E.1 General

This annex provides a high level description of the different communication models that NF and NF Services can use to interact which each other.

Table E.1-1 summarizes the communication models, their usage and how they relate to the usage of an SCP.

Communication between Consumer and Producer	Service Discovery and Request Routing	Communication Model
Direct communication	No NRF or SCP; direct routing	A
	Discovery using NRF services; no SCP; direct routing	B
Indirect communication	Discovery using NRF services; selection for specific instance from the Set can be delegated to SCP. Routing via SCP	C
	Discovery and associated selection delegated to an SCP using discovery and selection parameters in service request; routing via SCP	D

Table E.1-1: Communication models for NF/NF services interaction summary

1. 3GPP 5G System Architecture Service Communication Proxy NF to NF Service Interaction

Model A - Direct communication without NRF interaction: Neither NRF nor SCP are used. Consumers are configured with producers' "NF profiles" and directly communicate with a producer of their choice.

Model B - Direct communication with NRF interaction: Consumers do discovery by querying the NRF. Based on the discovery result, the consumer does the selection. The consumer sends the request to the selected producer.

Model C - Indirect communication without delegated discovery: Consumers do discovery by querying the NRF. Based on discovery result, the consumer does the selection of an NF Set or a specific NF instance of NF set. The consumer sends the request to the SCP containing the address of the selected service producer pointing to a NF service instance or a set of NF service instances. In the latter case, the SCP selects an NF Service instance. If possible, the SCP interacts with NRF to get selection parameters such as location, capacity, etc. The SCP routes the request to the selected NF service producer instance.

Model D - Indirect communication with delegated discovery: Consumers do not do any discovery or selection. The consumer adds any necessary discovery and selection parameters required to find a suitable producer to the service request. The SCP uses the request address and the discovery and selection parameters in the request message to route the request to a suitable producer instance. The SCP can perform discovery with an NRF and obtain a discovery result.

Figure E.1-1 depicts the different communication models.

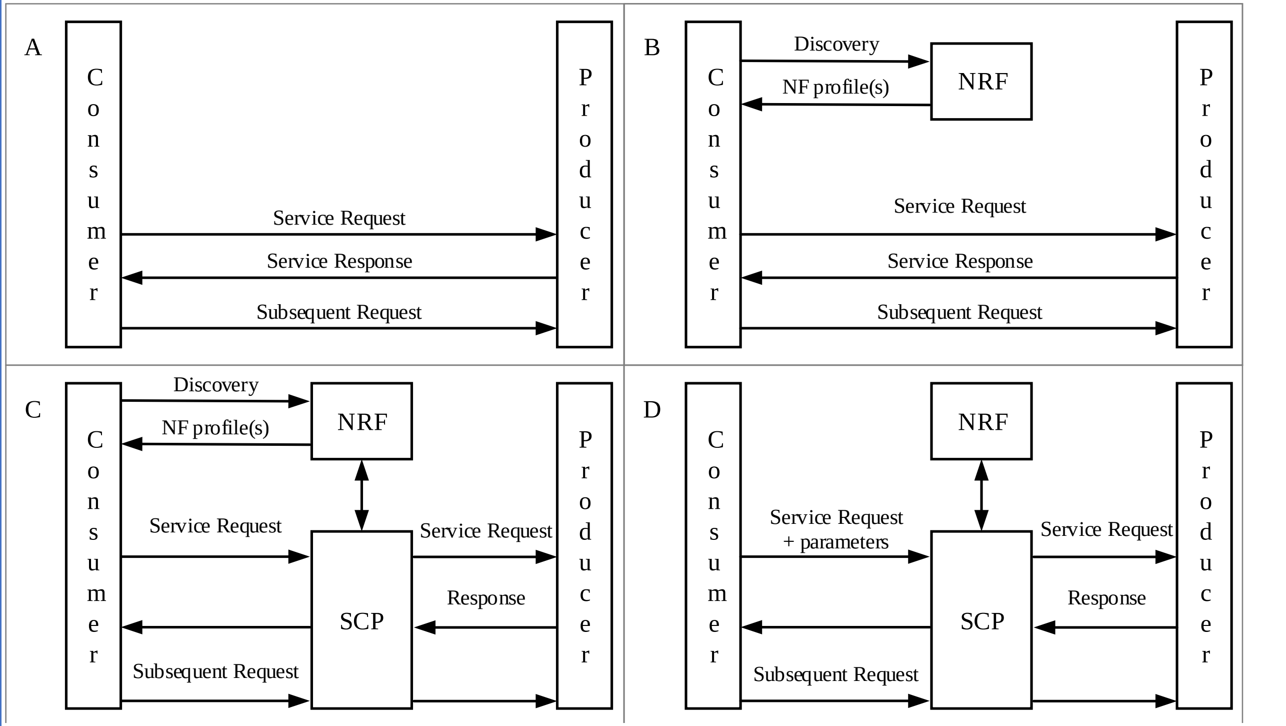


Figure E.1-1: Communication models for NF/NF services interaction

1. 3GPP 5G System Architecture Service Communication Proxy based on Service Mesh

G.2 **An SCP based on Service Mesh**

G.2.1 Introduction

This clause describes an SCP deployment based on a distributed model in which SCP endpoints are co-located with 5GC functionality (e.g. an NF, an NF Service, a subset thereof such as a microservice implementing part of an NF/NF service or a superset thereof such as a group of NFs, NF Services or microservices). This example makes no assumptions as to the internal composition of each 5GC functionality (e.g. whether they are internally composed of multiple elements or whether such internal elements communicate with means other than the service mesh depicted in this example).

In this deployment example, Service Agent(s) implementing necessary peripheral tasks (e.g. an SCP endpoint) are co-located with 5GC functionality, as depicted in Figure G.2.1-1.

In this example, **Service Agents and 5GC Functionality, although co-located, are separate components**.

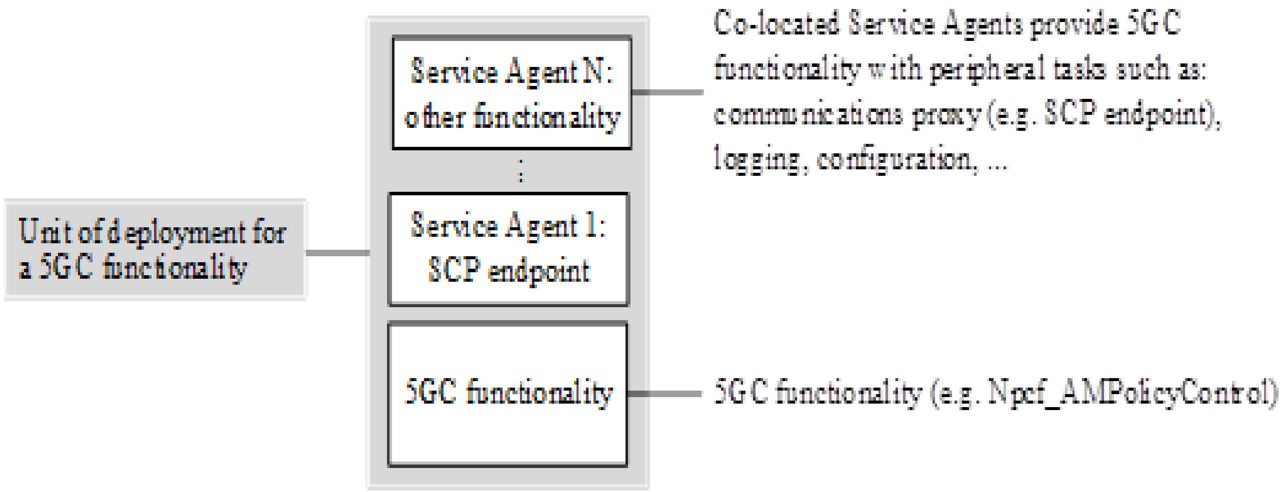


Fig. G.2.1-1: Deployment unit: 5GC Functionality & co-located Service Agent(s) implementing peripheral tasks

1. 3GPP 5G System Architecture Service Communication Proxy based on Service Mesh

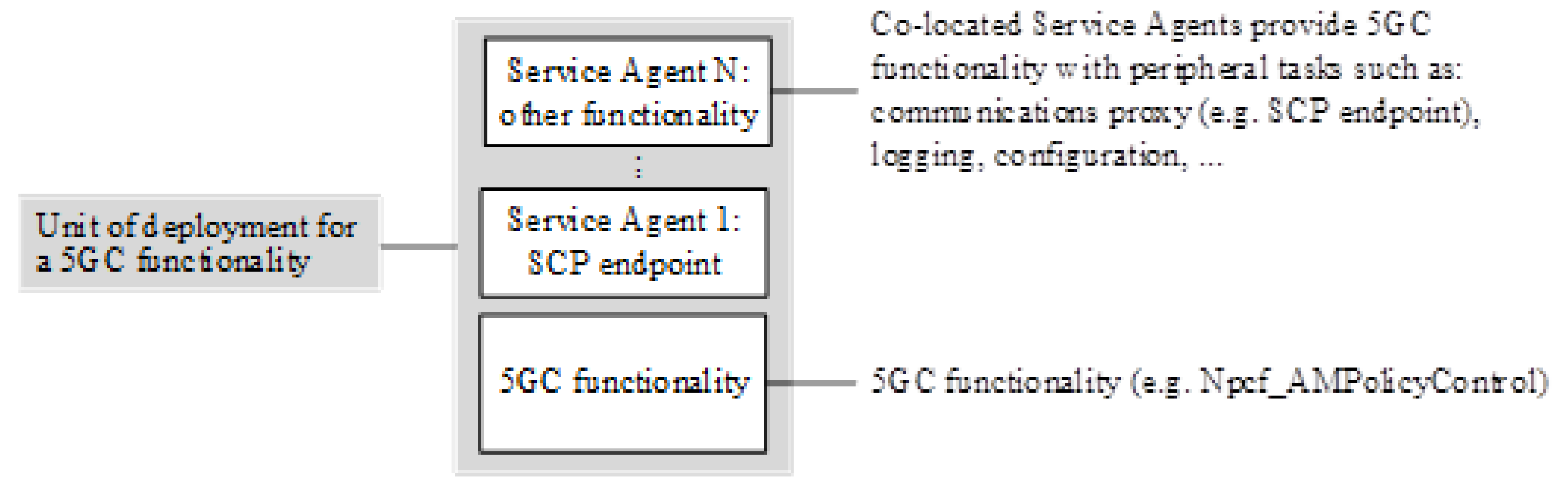


Fig. G.2.1-1: Deployment unit: 5GC Functionality & co-located Service Agent(s) implementing peripheral tasks

In this deployment example, an **SCP Service Agent, i.e. a Service Communication Proxy,** is co-located in the same deployment unit with 5GC Functionality and provides each deployed unit (e.g. a **Container-based VNFC**) with indirect communication and delegated discovery.

1. 3GPP 5G System Architecture SCP based on Service Mesh

Figure G.2.1-2 shows an overview of this deployment scenario. For SBI-based interactions with other 5GC functionalities, a consumer (5GC functionality A) communicates through its Service Agent via SBI. Its Service Agent selects a target producer based on the request and routes the request to the producer's (5GC functionality B) Service Agent. What routing and selection policies a Service Agent applies for a given request is determined by routing and selection policies pushed by the service mesh controller. Information required by the service mesh controller is pushed by the Service Agents to the service mesh controller.

In this deployment, the SCP manages registration and discovery for communication within the service mesh and it interacts with an external NRF for service exposure and communication across service mesh boundaries. Operator-defined policies are additionally employed to generate the routing and selection policies to be used by the Service Agents.

This example depicts only SBI-based communication via a service mesh, but it does not preclude the simultaneous use of the service mesh for protocols other than SBI supported by the service mesh or that the depicted 5GC functionality additionally communicates via other means.

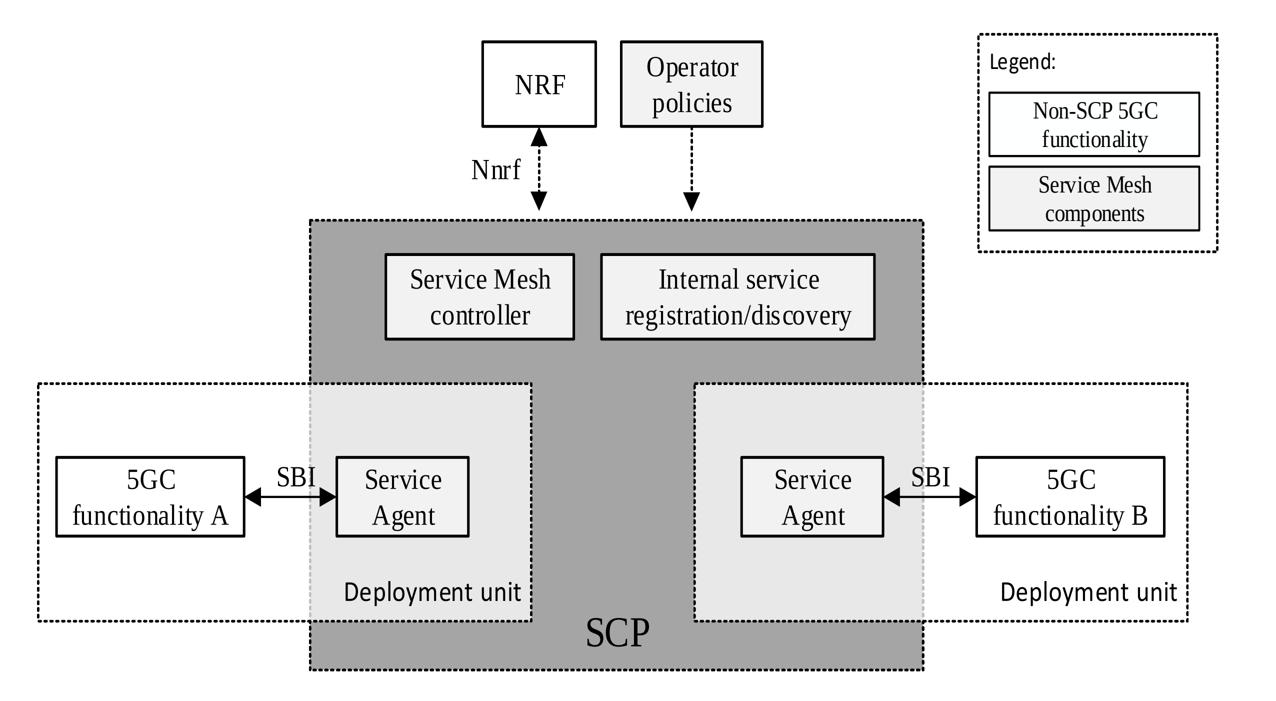


Figure G.2.1-2: SCP Service mesh co-location with 5GC functionality

1. 3GPP 5G System Architecture SCP based on Service Mesh

From a 3GPP perspective, in this deployment example a deployment unit thus contains NF Functionality and SCP Functionality.

Figure G.2.1-3 depicts the boundary between both 3GPP entities. In the depicted example, two (2) NF Services part of the same NF and each exposing an SBI Interface are deployed each in a Container-based VNFC.

A co-located Service Agent provides each NF Service with indirect communication and delegated discovery.

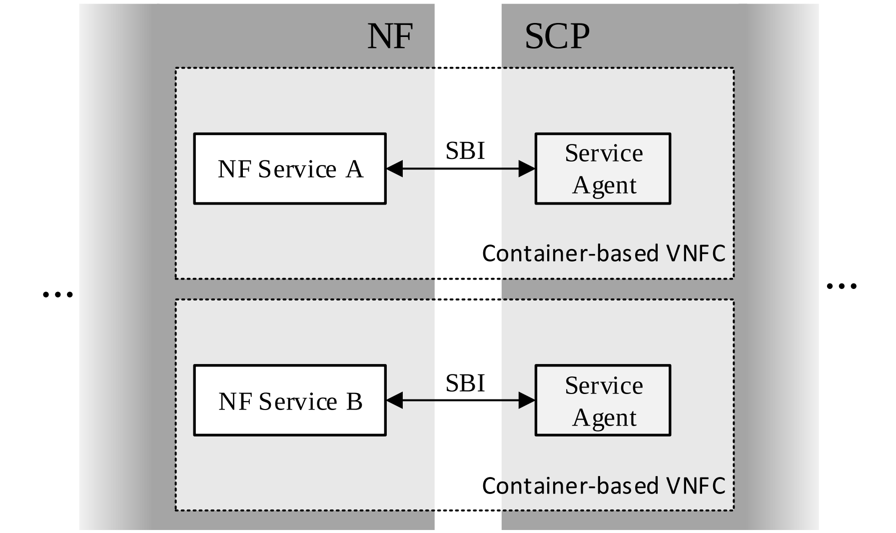


Figure G.2.1-3: Detail of the NF-SCP boundary

1. 3GPP 5G System Architecture SCP based on Service Mesh

G.2.2 Communication across service mesh boundaries

It is a deployment where a single service mesh covers all functionality within a given deployment or not. In cases of communication across the boundaries of a service mesh, the service mesh routing the outbound message knows neither whether the selected producer is in a service mesh nor the internal topology of the potential service mesh where the producer resides.

In such a deployment, as shown in Figure G.2.2.-1, after producer selection is performed, routing policies on the outgoing service mesh are only aware of the next hop.

Given a request sent by A, A's Service Agent will perform producer selection based on the received request. If the selected producer endpoint (e.g. D) is determined to be outside of Service Mesh 1, A's Service Agent routes the request to the Egress Proxy. For a successful routing, the Egress Proxy needs to be able to determine the next hop of the request. In this case, this is the Ingress Proxy of Service Mesh 2. The Ingress Proxy of Service Mesh 2 is, based on the information in the received request and its routing policies, able to determine the route for the request. Subsequently, D receives the request. No topology information needs to be exchanged between Service Mesh 1 and Service Mesh 2 besides a general routing rule towards Service Mesh 2 (e.g. a FQDN prefix) and an Ingress Proxy destination for requests targeting endpoints in Service Mesh 2.

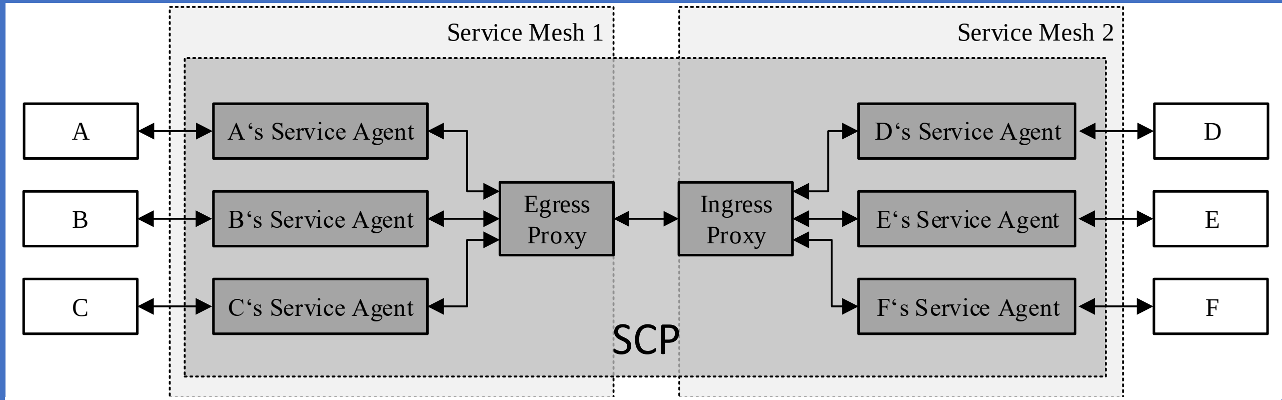


Figure G.2.2-1: Message routing across service mesh boundaries

1. 3GPP 5G System Architecture SCP based on Service Mesh

G.3 An SCP based on independent deployment units

This clause shows an overview of SCP deployment based on the 5GC functionality and SCP being deployed in independent deployment units.
The SCP deployment unit can internally make use of microservices, however these microservices are up to vendors implementation and can be for example SCP agents and SCP controller as used in this example. The SCP agents implement the http intermediaries between service consumers and service producers. The SCP agents are controlled by the SCP controller. Communication between SCP controller and SCP agents is via SCP internal interface (4) and up to vendors implementation.

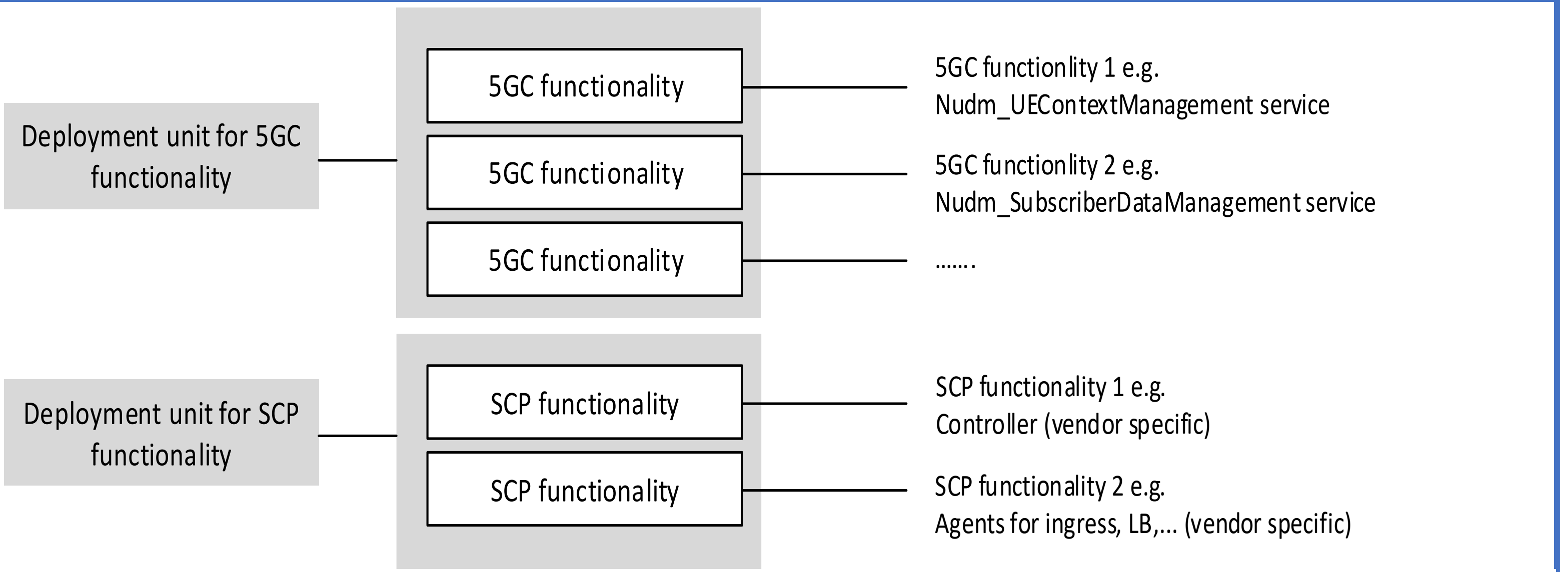


Figure G.3-1: Independent deployment units for SCP and 5GC functionality

1. 3GPP 5G System Architecture SCP based on Service Mesh

G.3 An SCP based on Independent Deployment Units

In this model it is a deployment choice to Co-locate SCP and other 5GC Functions or not.

The SCP Interfaces (1), (2) and (3) are Service - based Interfaces (SBIs).

SCP itself is not a Service Producer itself, however acting as http Proxy it registers Services on behave of the Producers in NRF.

Interface (2) represents same Services as (1) however using SCP Proxy addresses.

Interface (3) is interfacing NRF e.g. for Service registration on behalf of the 5GC Functions or Service Discovery.

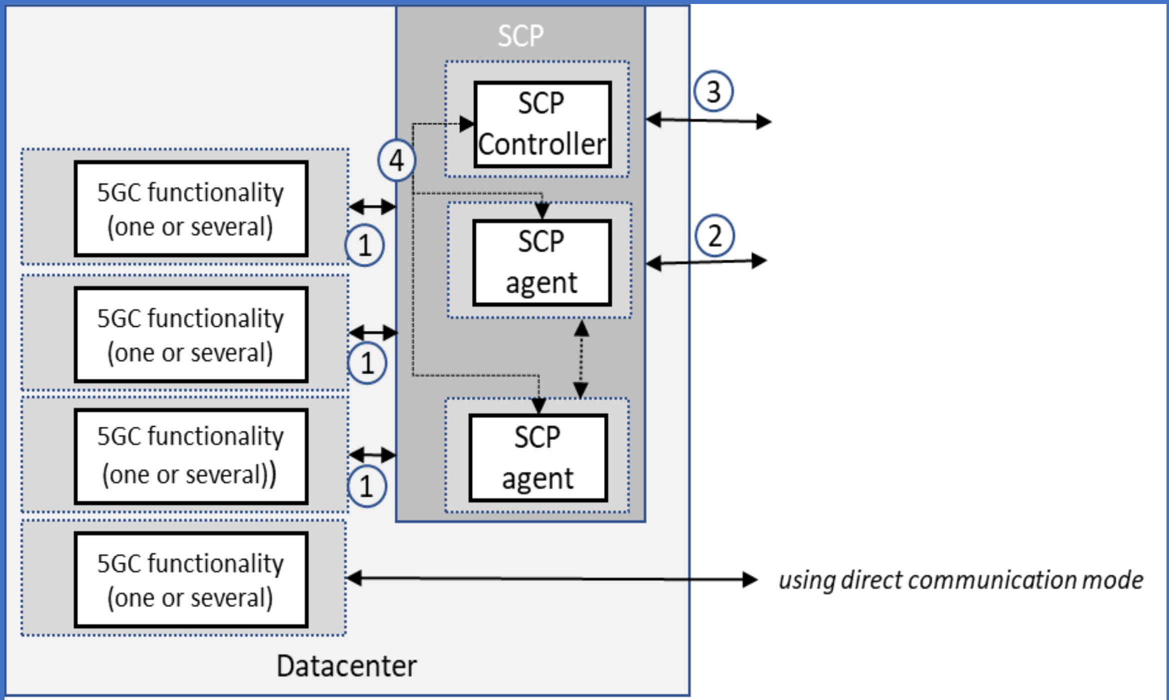


Fig. G.3-2: 5GC Functionality and SCP Co-location choices

2. 3GPP 5G System Architecture SCP based on Independant Deployment Units

SCP based on Independent Deployment Units

For SBI-based Interactions (SBI) with other 5GC Functions, a Consumer communicates through a SCP Agent via SBI (1).

SCP Agent selects a target based on the Request and routes the Request to the target SCP Agent (2).

What Routing and Selection Policies each SCP Agent applies for a given request is determined by Routing and Selection Policies determined by the SCP Controller using for example information provided via NRF (3) or locally configured in the SCP Controller.

The Routing and Selection Information is provided by the SCP Controller to the SCP Agents via SCP Internal Interface (4).

Direct communication can co-exist in the same deployment based on 3GPP specified mechanisms.

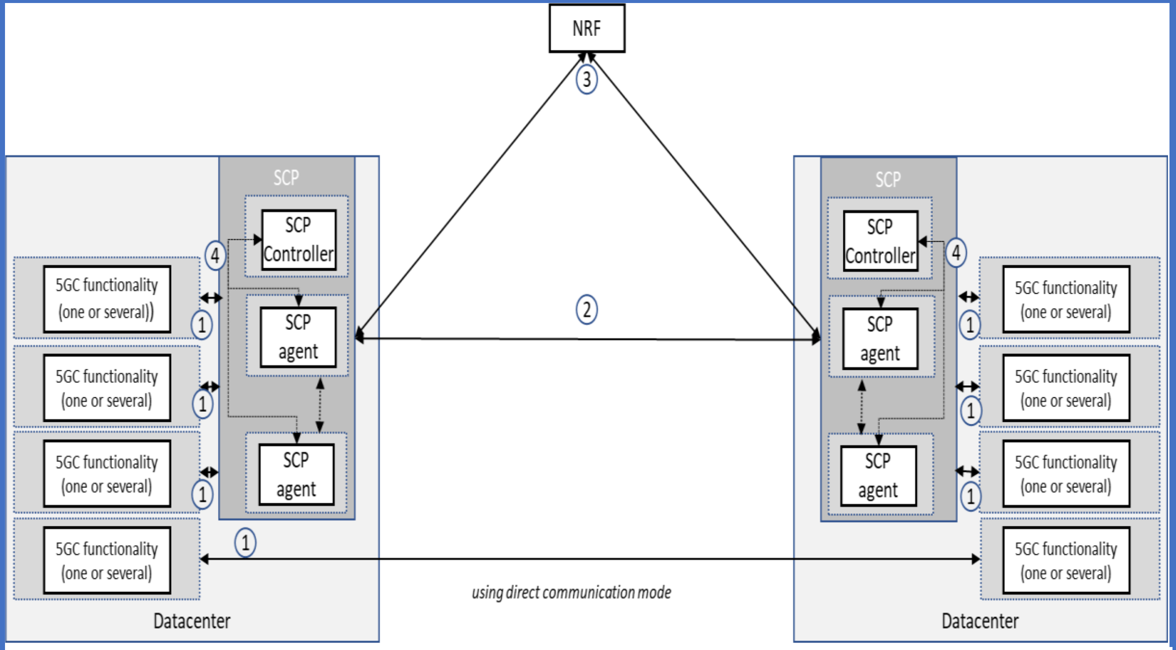


Figure G.3-3: Overview of SCP deployment

G.4 An SCP deployment example based on Name-based Routing

G.4.0 General Information

SCP based on a Name-based Routing Mechanism that provides
IP over ICN Capabilities such as those described in Xylomenos, George, et al.: "IP over ICN goes live", 2018 European Conference on Networks & Communications (EuCNC). IEEE, 2018.

SCP offering based on an SBA-platform to interconnect 5GC Services (or a subset of the respective services).

The Name-based Routing mechanism, described in this deployment example, is realized through a Path Computation Element which is the Core part of the SCP.

The 5GC Services are running as Microservices on Cloud/ deployment Units (Clusters).

A Service Router is the Communication Node (Access Node/GW) between the SCP and the 5GC Services and resides as a single unit within a Service Deployment Cluster.

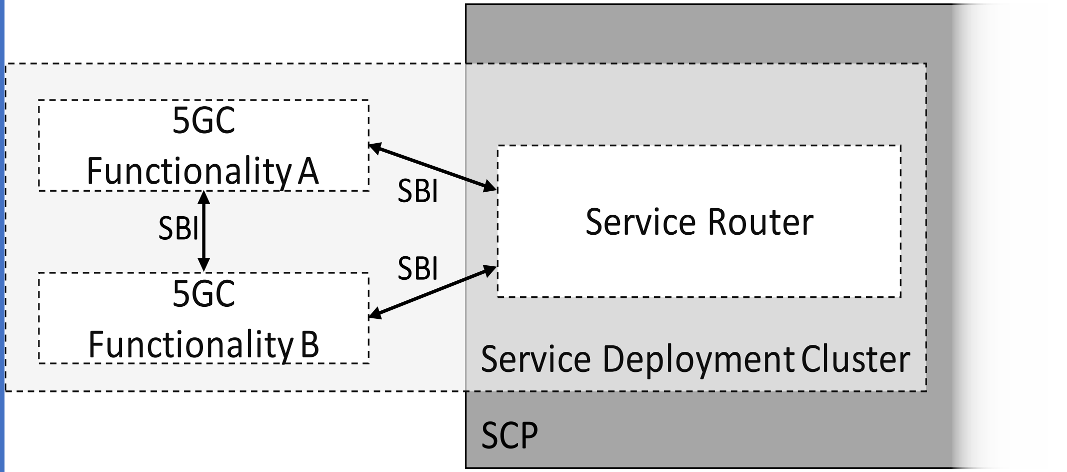


Fig. G.4-1: Deployment unit: 5GC Functionality and Co-located Service Agent(s) implementing peripheral tasks

G.4 An SCP based on Name-based Routing

G.4.0 General Information

The Service Router acts as Communication Proxy and it is responsible for mapping IP based messages onto ICN publication and subscriptions. The Service Router serves multiple 5GC Service Endpoints within that Cluster. For direct communication the Service Router is not used.

5GC Functionalities communicate with the Service Router using standardized 3GPP SBIs.

The Functionalities within the Service Deployment Cluster are Containerized Service Functions.
Depicted in Figure G.4-1, the Service Router act as SCP termination point and offer the SBI to the respective 5GC Service Functionalities.

Service Routers & 5GC Functionality, although co-located, are separate components within the Service Deployment Cluster.

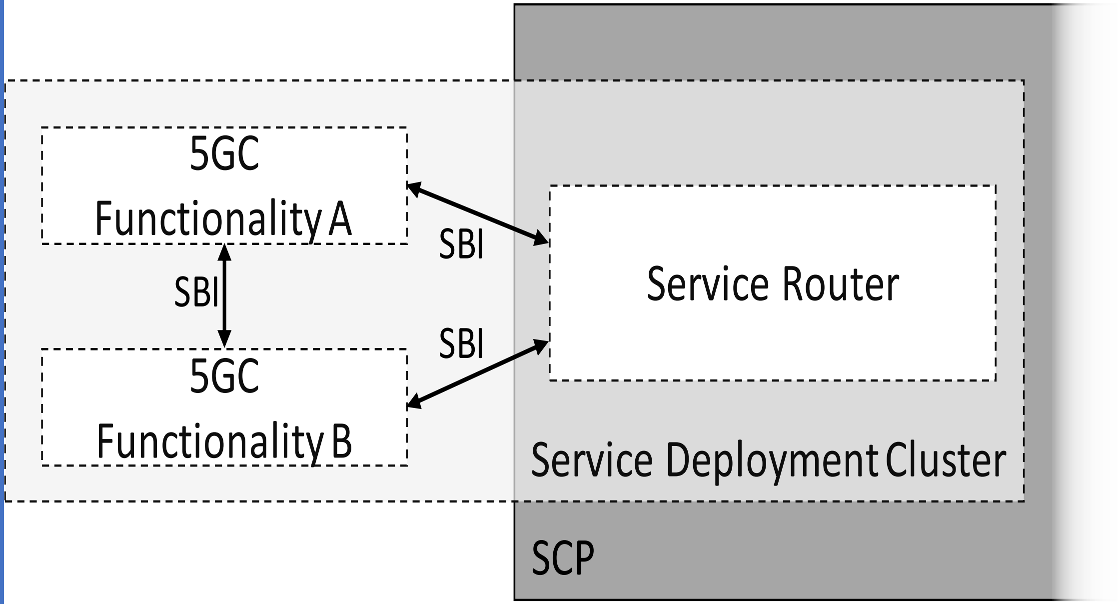


Fig. G.4-1: Deployment unit: 5GC Functionality and Co-located Service Agent(s) implementing peripheral tasks

Multiple Functionalities can exist within the Service Deployment Cluster, all served by the respective Service Router when needed to communicate to other Service Functionalities within different clusters.

1. 3GPP 5GS Architecture SCP implementations

G.4 An SCP based on Name-based Routing

G.4.0 General Information

In Figure G.4-1, the two (2) depicted 5GC Service Functionalities (A & B) (realized as Network Function Service Instances) may communicate in two (2) ways.

However, before the communication can be established between two 5GC Functionalities, Service Registration and Service Discovery need to take place, as described in Figure G.4.1-1.

Service Registration and Service Discovery are provided in a standardized manner using 3GPP Service Based Interfaces (SBIs).

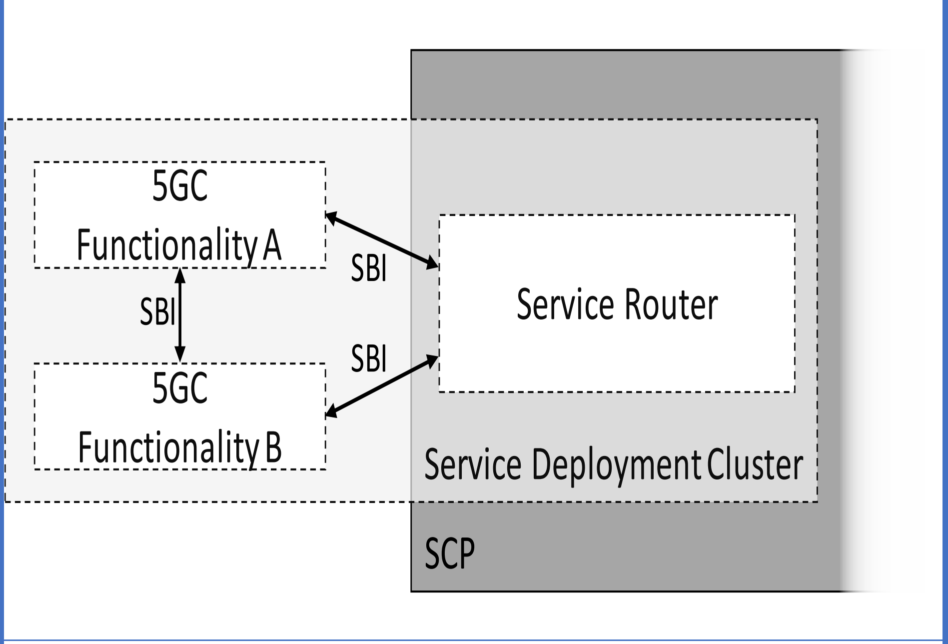


Fig. G.4-1: Deployment unit: 5GC Functionality and Co-located Service Agent(s) implementing peripheral tasks

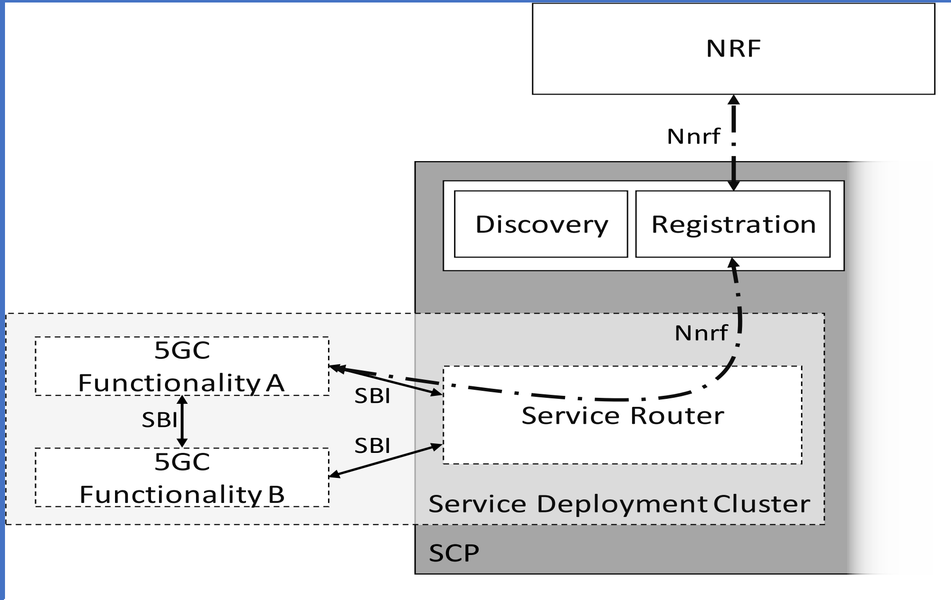


Fig. G.4.1-1: Registering 5GC Functionalities in the SCP

1. 3GPP 5GS Architecture SCP implementations

G.4 An SCP based on Name-based Routing

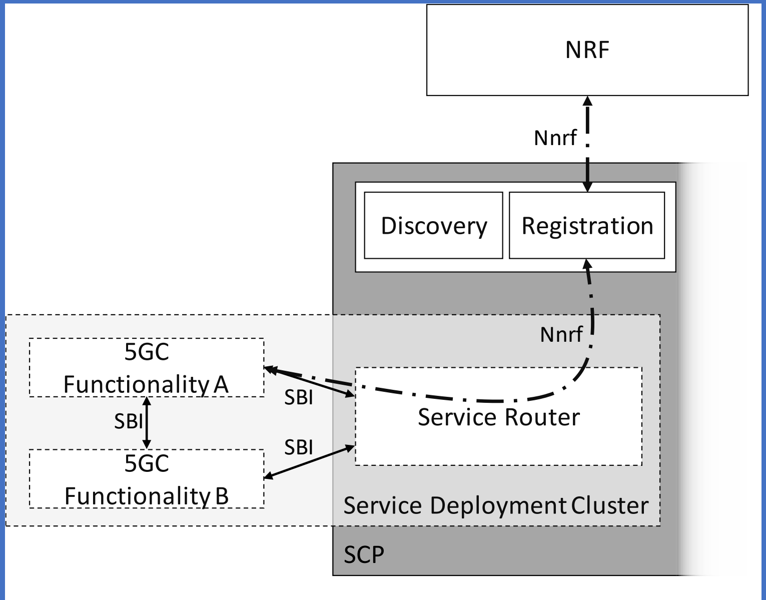


Fig. G.4.1-1: Registering 5GC Functionalities in the SCP

G.4.1 Service Registration and Service Discovery

Service Registration can be done in several ways.

One option is that ready 5GC Service Functions may register themselves with their Service profile via the Nnrf Interface.

The Registration request is forwarded to the Internal Registry as well as forwarded to the Operator's NRF.

The internal registration is used to store the address to identifier relationship and the Service Deployment Cluster location.

The external registration (NRF) is used to expose the Service Functionality to Services outside the depicted SCP.

Service discovery entails Function A requesting a resolvable identifier for Functionality B.

G.4 An SCP based on Name-based Routing

G.4.2 Overview of Deployment Scenario

Figure G.4.2-1 shows an overview of this deployment scenario. For SBI-based interactions with other 5GC Functionalities, a Consumer entity (e.g. 5GC Functionality B in the Cluster on the left side) communicates through the Cluster's Service Router with other entities in other Clusters (e.g. 5GC Functionality D in the Cluster on the right side).

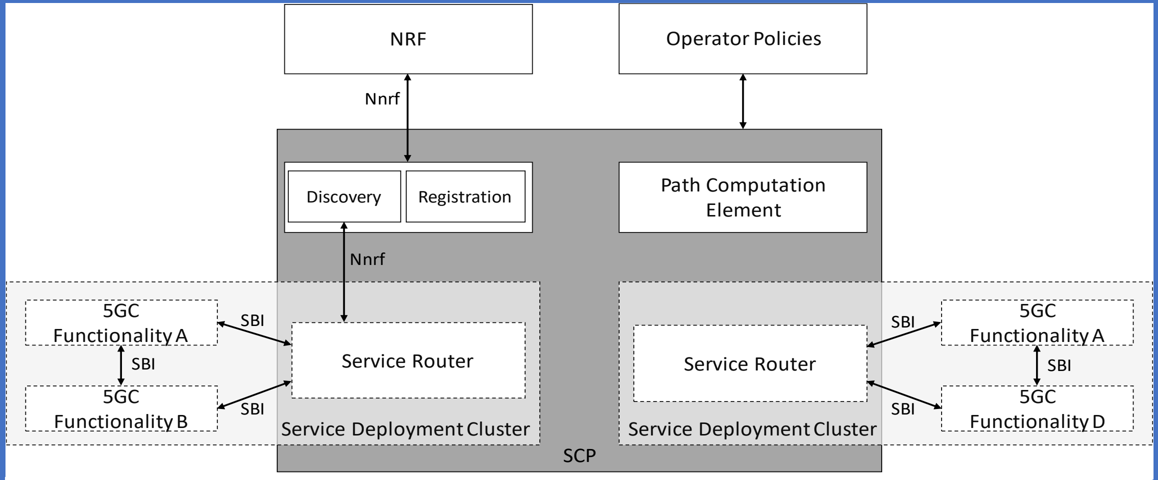


Figure G.4.2-1: (NbR-) SCP interconnects Multiple Deployment Clusters with external NRF

The target selection is performed through the platform's Discovery Service.

From the Client's perspective, the Service Router is the 1st and only contact point to the SCP.

The Platform resolves the requested Service identifier and aligns the results with the Platform's Policies.

The Path Computation Element calculates a path between the Consumer and the Producer (e.g. the shortest path between the nodes).

Thank you

Cell-Free Massive MIMO versus Small Cells

Hien Quoc Ngo, Alexei Ashikhmin, Hong Yang, Erik G. Larsson, and Thomas L. Marzetta

***Abstract*—A Cell-Free Massive MIMO (multiple-input multiple-output) system comprises a very large number of distributed access points (APs) which simultaneously serve a much smaller number of users over the same time/frequency resources based on directly measured channel characteristics. The APs and users have only one antenna each. The APs acquire channel state information through time-division duplex operation and the reception of uplink pilot signals transmitted by the users. The APs perform multiplexing/de-multiplexing through conjugate beamforming on the downlink and matched filtering on the uplink. Closed-form expressions for individual user uplink and downlink throughputs lead to max-min power control algorithms. Max-min power control ensures uniformly good service throughout the area of coverage. A pilot assignment algorithm helps to mitigate the effects of pilot contamination, but power control is far more important in that regard.**

Cell-Free Massive MIMO has considerably improved performance with respect to a conventional small-cell scheme, whereby each user is served by a dedicated AP, in terms of both 95%-likely per-user throughput and immunity to shadow fading spatial correlation. Under uncorrelated shadow fading conditions, the cell-free scheme provides nearly 5-fold improvement in 95%-likely per-user throughput over the small-cell scheme, and 10-fold improvement when shadow fading is correlated.

***Index Terms*—Cell-Free Massive MIMO system, conjugate beamforming, Massive MIMO, network MIMO, small cell.**

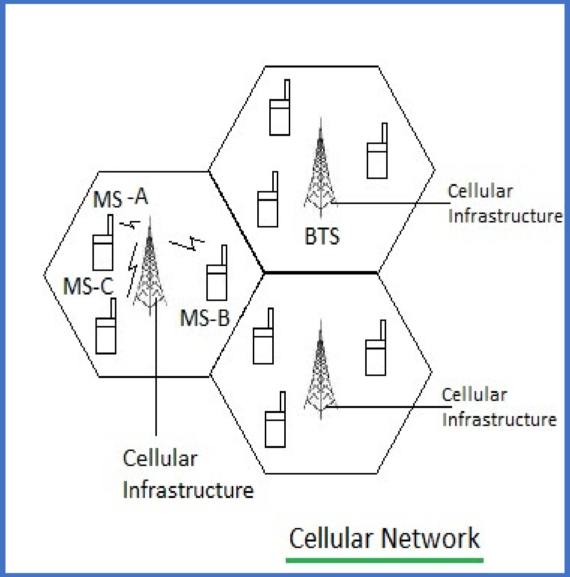
I. Introduction

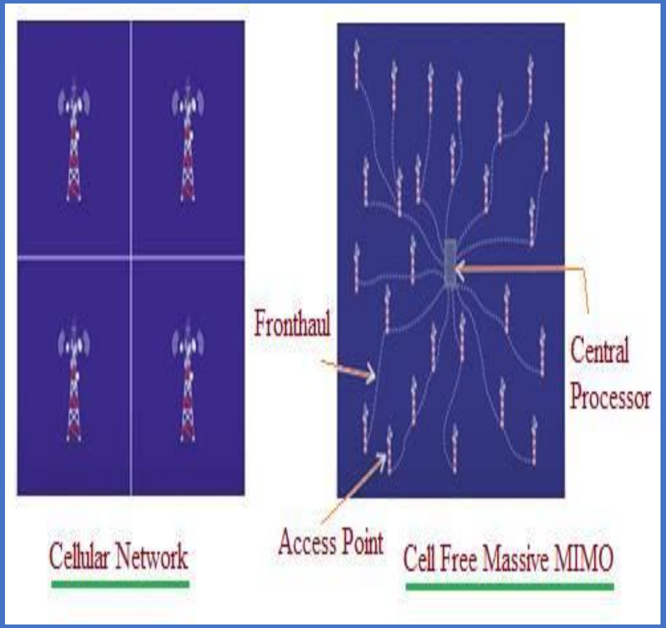
MASSIVE multiple-input multiple-output (MIMO)

to more efficiently exploit diversity against the shadow fading, distributed systems can potentially offer much higher probability of coverage than collocated Massive MIMO [4], at the cost of increased backhaul requirements.

In this work, we consider a distributed Massive MIMO system where a large number of service antennas, called access points (APs), serve a much smaller number of autonomous users distributed over a wide area [1]. All APs cooperate phase-coherently via a backhaul network, and serve all users in the same time-frequency resource via time-division duplex (TDD) operation. There are no cells or cell boundaries. Therefore, we call this system "Cell-Free Massive MIMO". Since Cell-Free Massive MIMO combines the distributed MIMO and Massive MIMO concepts, it is expected to reap all benefits from these two systems. In addition, since the users now are close to the APs, Cell-Free Massive MIMO can offer a high coverage probability. Conjugate beamforming/matched filtering techniques, also known as maximum-ratio processing, are used both on uplink and downlink. These techniques are computationally simple and can be implemented in a distributed manner, that is, with most processing done locally at the APs.[1]

In Cell-Free Massive MIMO, there is a central processing unit (CPU), but the information exchange between the APs and this CPU is limited to the payload data, and power control coefficients that change slowly. There is no sharing





(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2018 (14.06.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/103897 A1

(51) International Patent Classification:
H04B 7/0452 (2017.01) *H01Q 1/22* (2006.01)
H04B 7/04 (2017.01) *H01Q 1/46* (2006.01)
H04W 88/08 (2009.01) *H01Q 21/08* (2006.01)
H01Q 21/29 (2006.01) *H01Q 1/38* (2006.01)
H01Q 25/00 (2006.01)

(21) International Application Number:
PCT/EP2017/051669

(22) International Filing Date:
26 January 2017 (26.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16203149.6 09 December 2016 (09.12.2016) EP

(71) Applicant: TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) [SE/SE]; 164 83 STOCKHOLM (SE).

(72) Inventors: FRENGER, Pål; Enskiftesgatan 8, 583 34 Linköping (SE). HEDEREN, Jan; Nartomta Storgård, 585 62 Linghem (SE). HESSLER, Martin; Kompanigatan 16, 587 58 Linköping (SE). INTERDONATO, Giovanni; Rydsvägen 98C, 584 31 Linköping (SE).

(74) Agent: STRÖM & GULLIKSSON AB; P.O. Box 4188, SE-203 13 Malmö (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

(54) Title: IMPROVED ANTENNA ARRANGEMENT FOR DISTRIBUTED MASSIVE MIMO

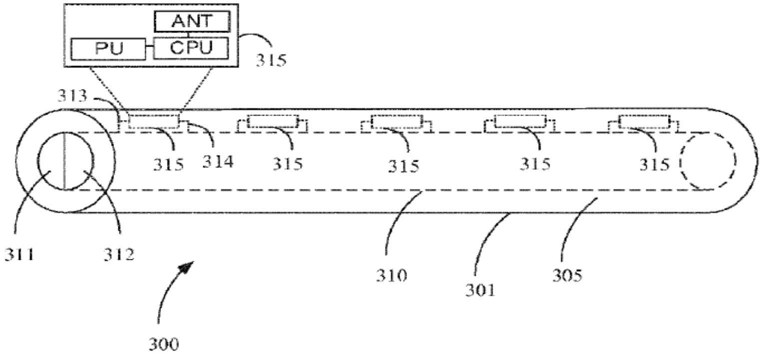
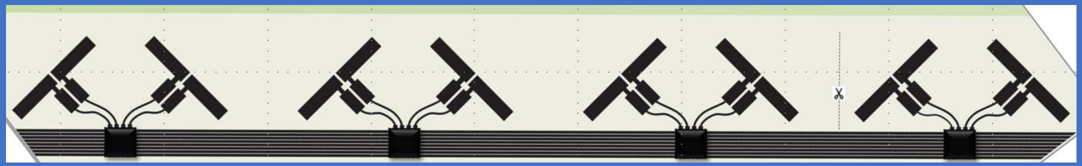


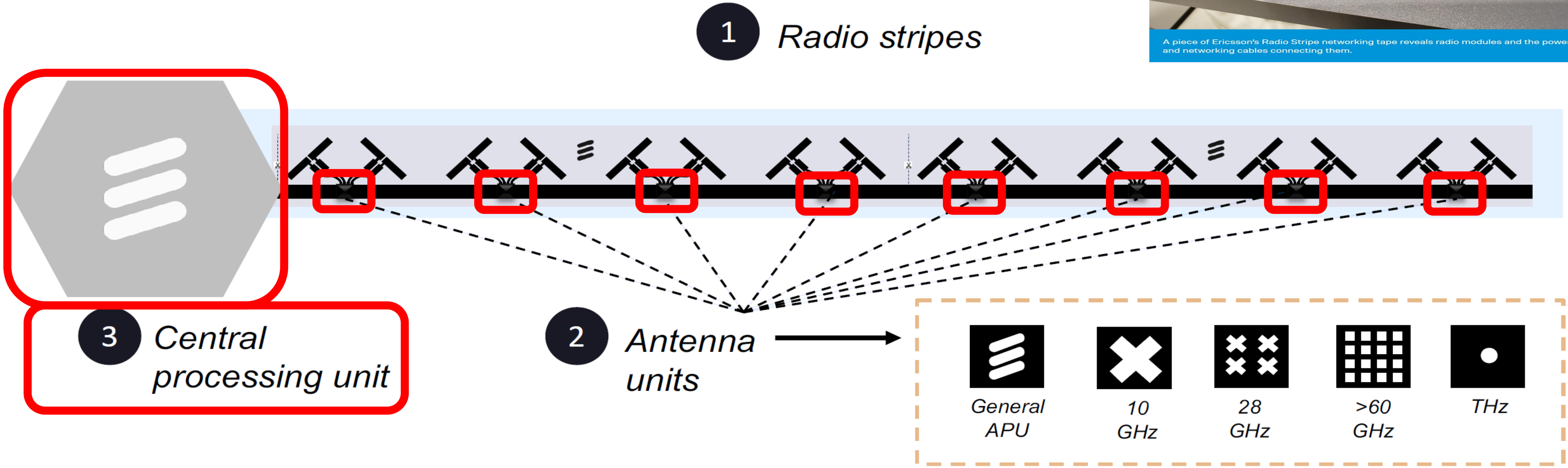
Fig. 3



A piece of Ericsson's Radio Stripe networking tape reveals radio modules and the power and networking cables connecting them.

Implementation Architecture: Radio Stripes

A piece of Ericsson's Radio Stripe networking tape reveals radio modules and the power and networking cables connecting them.



Can create as long stripes as we need

LINKÖPING UNIVERSITY

ERICSSON

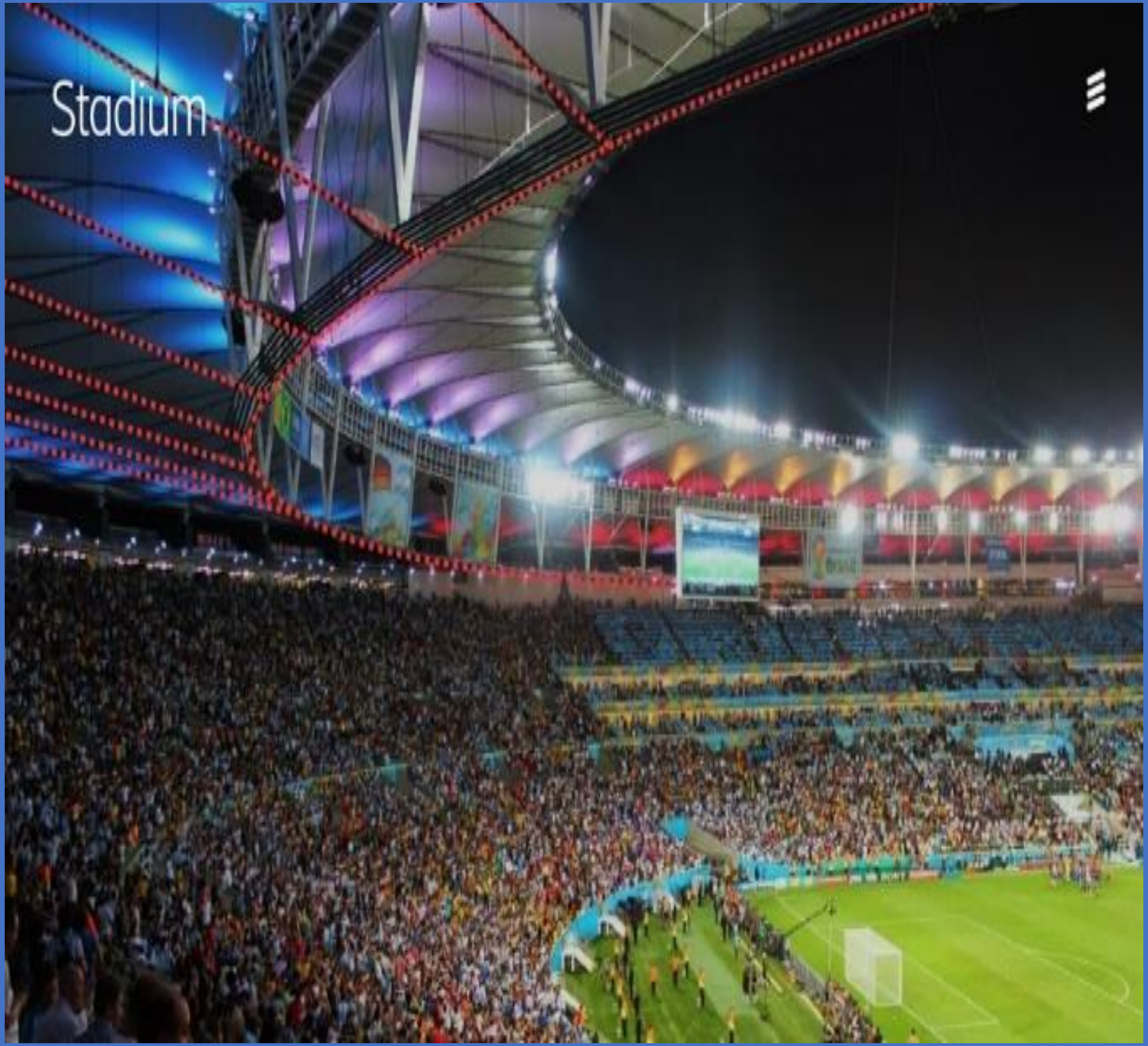
Ericsson Cell Free Radio Stripes

Pål Frenger, Radio Network Energy Performance Manager at Ericsson Research

A piece of Ericsson's Radio Stripe networking tape reveals radio modules and the power and networking cables connecting them.

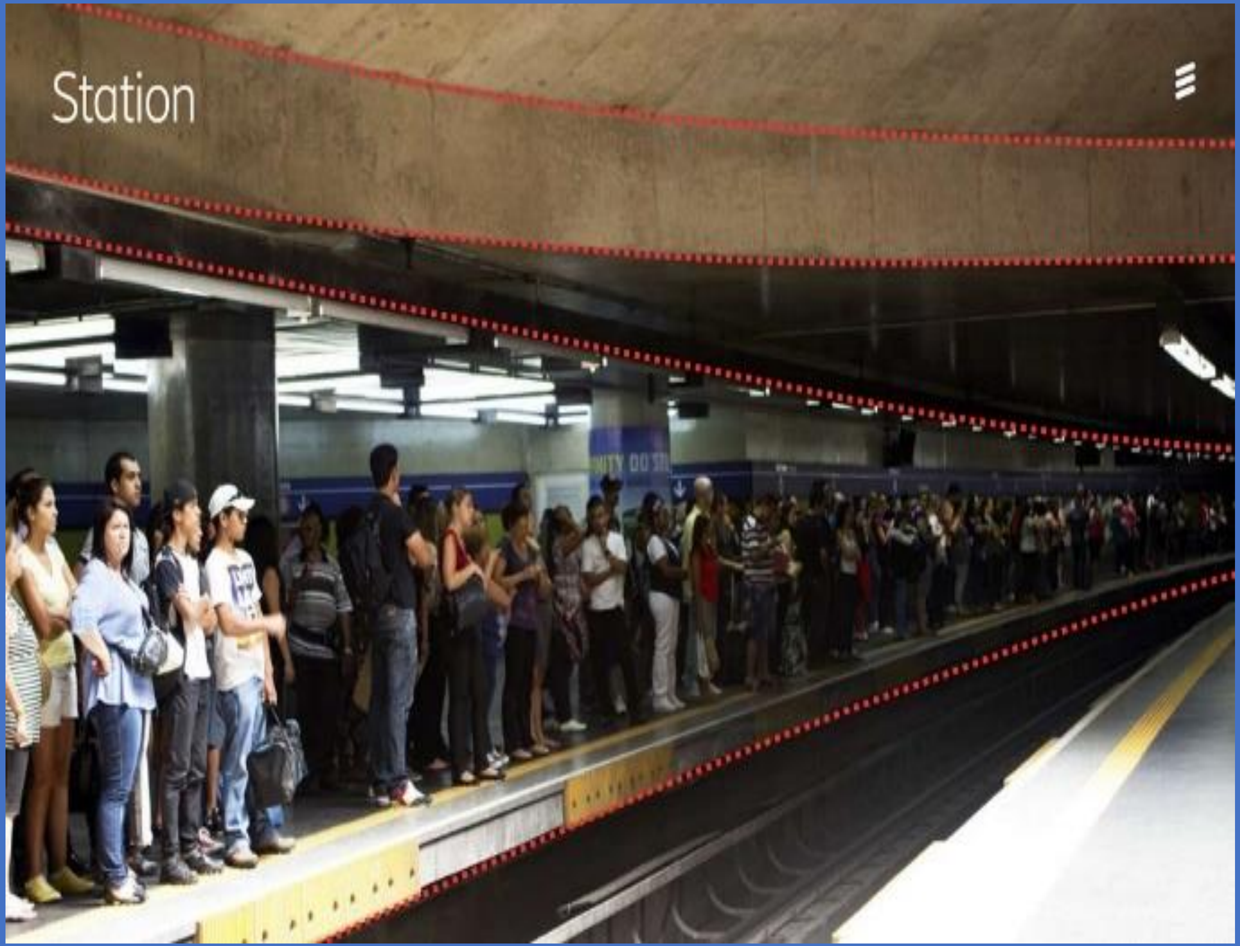
Ref. Digital Trends, Ericsson 5G Radio Stripe Network MWC 2019& Linköpings Universitet, Wireless communication by the metre, Dec. 2019

Ericsson Cell Free Radio Stripes Use Cases (UCs) - 1



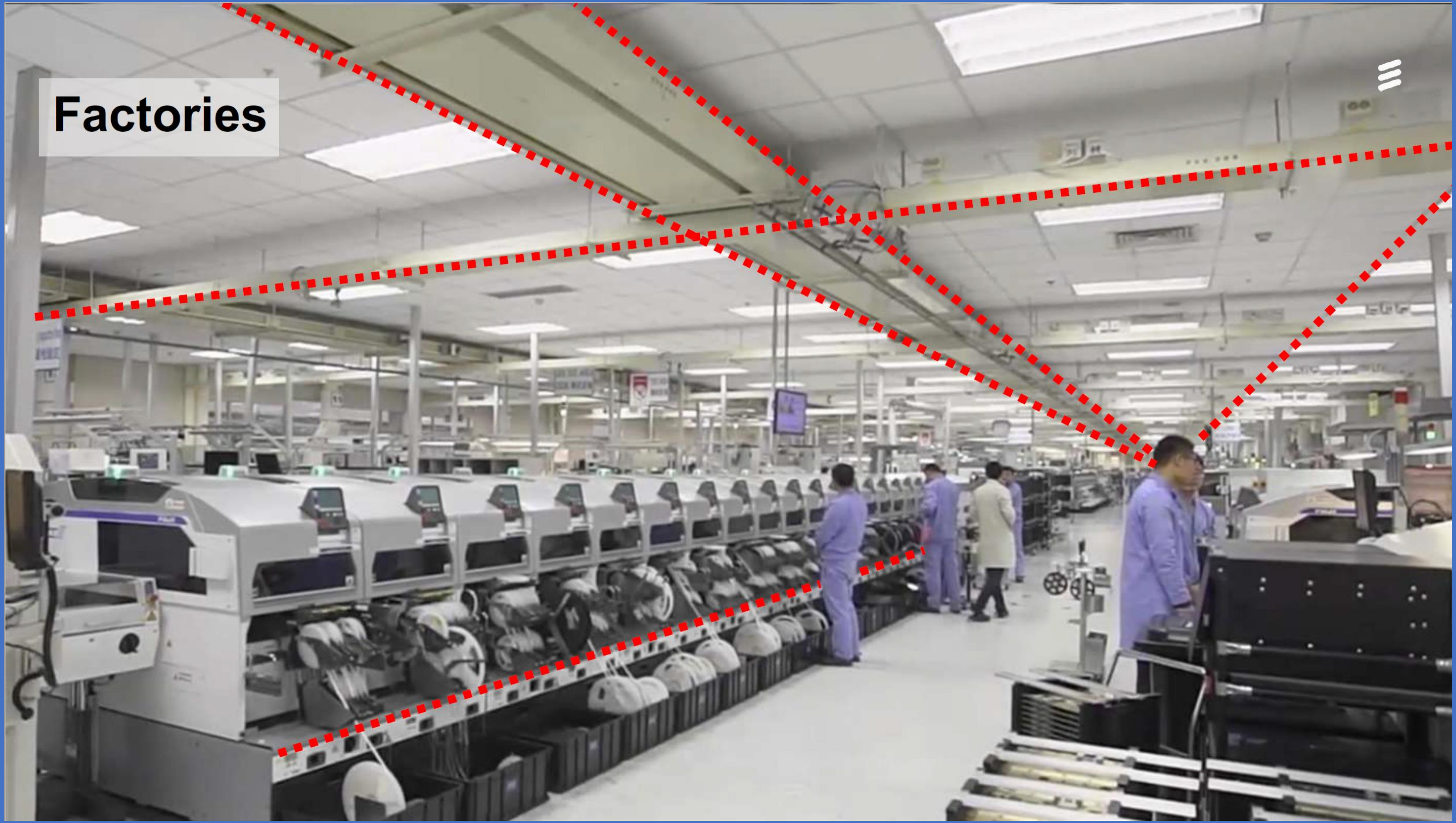
Ref. Ericsson, Radio Stripes: Re-Thinking Mobile Networks, Feb., 2019

Ericsson Cell Free Radio Stripes Use Cases (UCs) - 2



Ref. Ericsson, Radio Stripes: Re-Thinking Mobile Networks, Feb., 2019

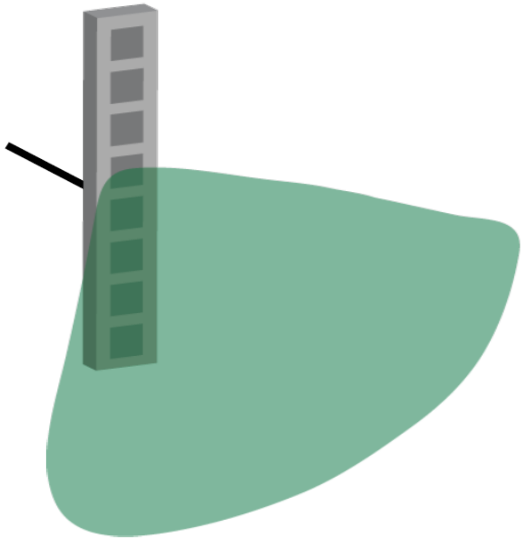
Ericsson Cell Free Radio Stripes Use Cases (UCs) - 2



Ref. Assoc. Prof. Emil Björnson, Pres, Beyond the Cellular Paradigm: Cell-free Architectures with Radio Stripes April, 2020: 22

Massive MIMO: 5G Attempt to Improve Spectral Efficiency

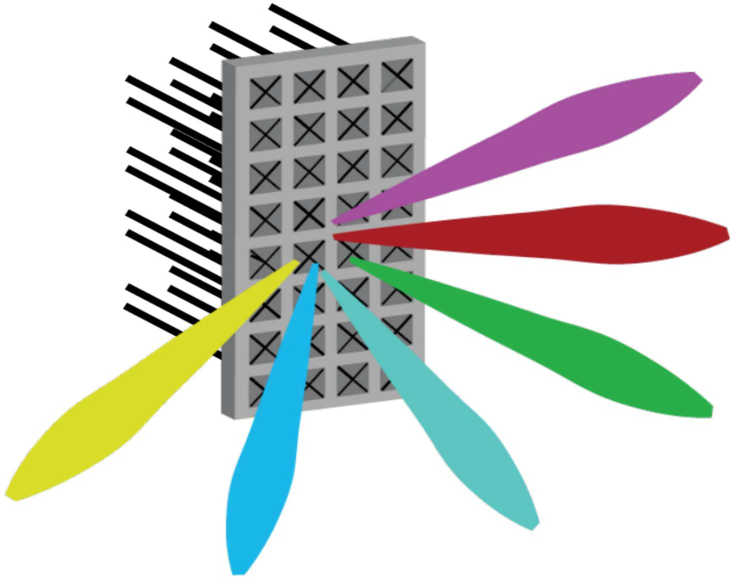
1 high-gain antenna



Classical antenna

Always the same directivity

64 low-gain antennas



"Massive MIMO"

Strong, adaptive directivity

Separate users in space

Reduce interference

Massive MIMO
(multiple-input multiple-output):

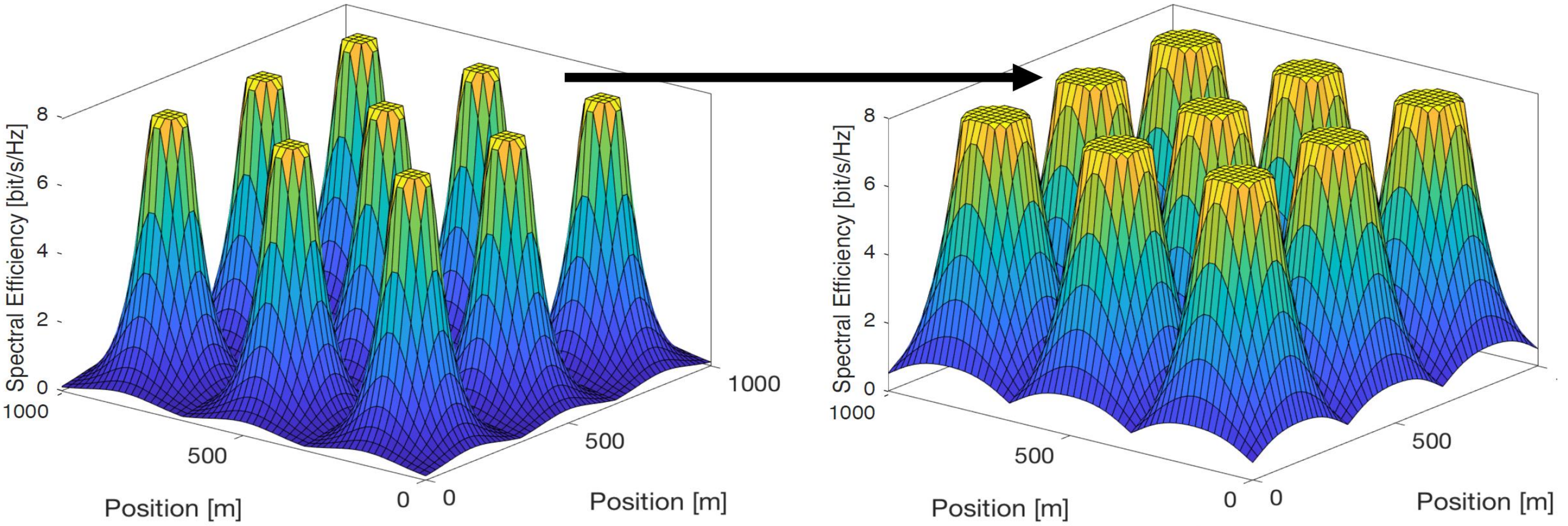
M antennas $\gg K$ users

8

Beyond the Cellular Paradigm: Cell - free Architecture with Radio Stripes

Can 5G Deliver Uniformly Good Service Everywhere?

Handles more users and give stronger signals, but problems remain!



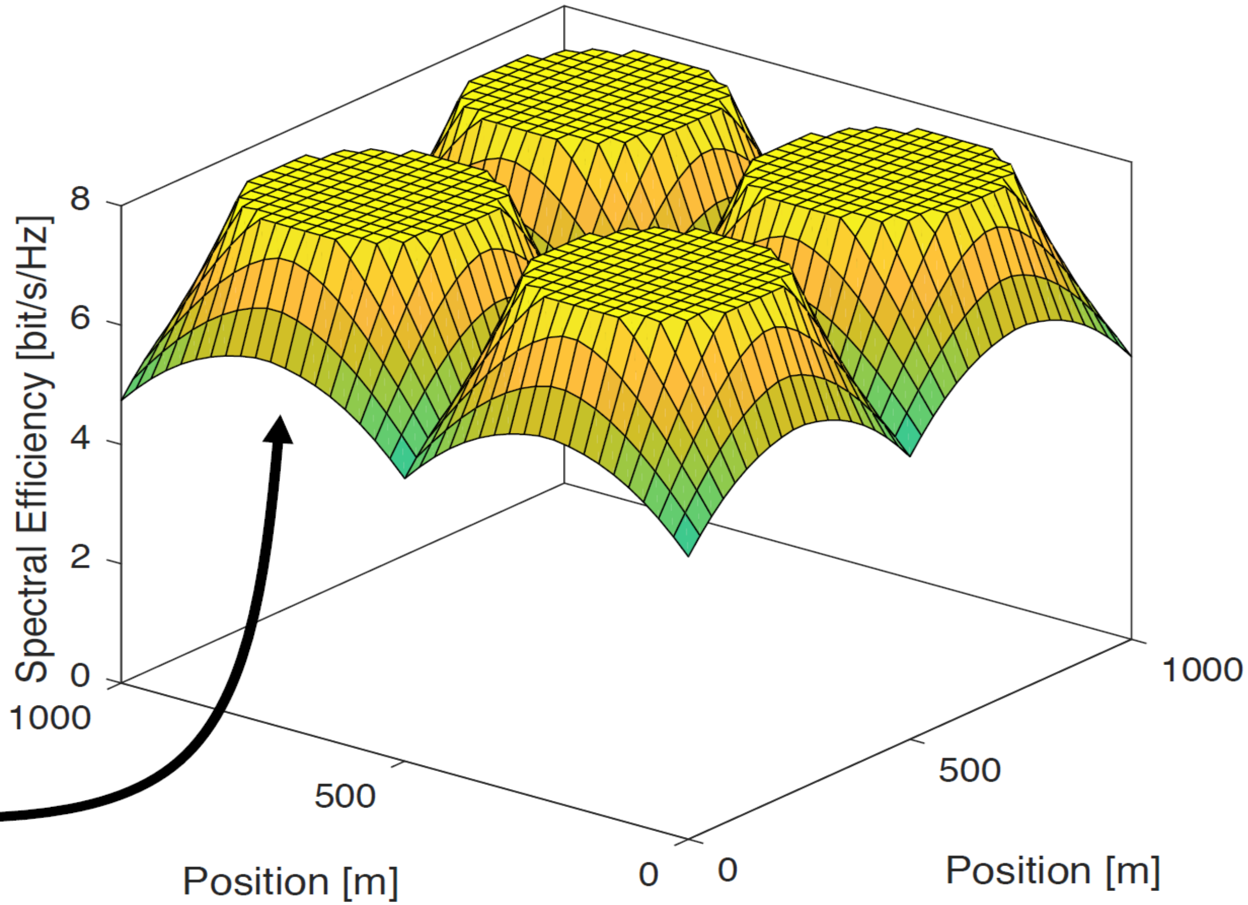
mmWave bands: Worse signal variations!

9

Wireless Dream: (Almost) Uniformly Good Service Quality

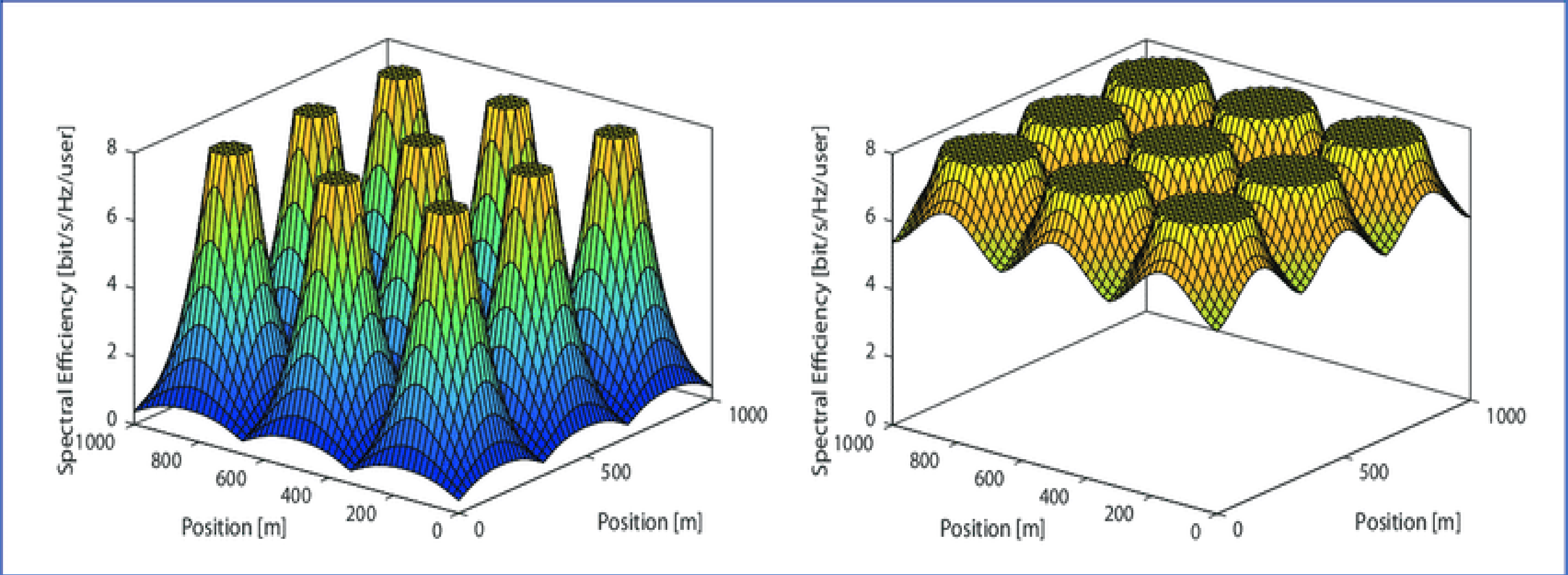
Users request same service everywhere

Easy to serve users in cell center
Most *active users* are at cell edge!



Can we deliver this somehow?

Ericsson Cell Free Radio Stripes

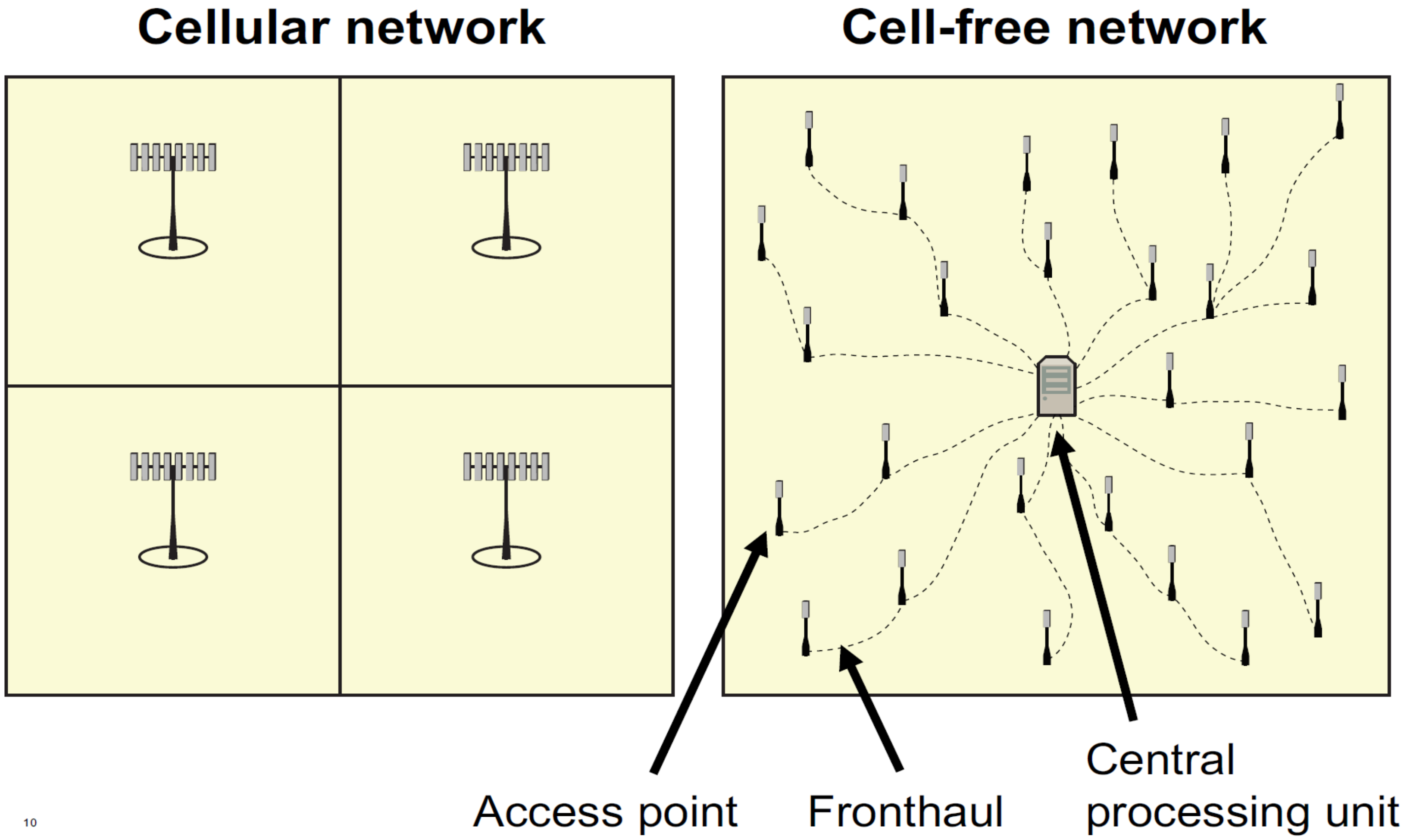


Data Coverage: Left: Cellular Network. **Right: Cell-Free Massive MIMO Network.**

SE achieved by UEs at different locations in an Area covered by nine (9) APs that are deployed on a regular grid. Note that 8 bit/s/Hz was selected as the maximal SE, which corresponds to uncoded 256-QAM.

Ref. Giovanni Interdonato

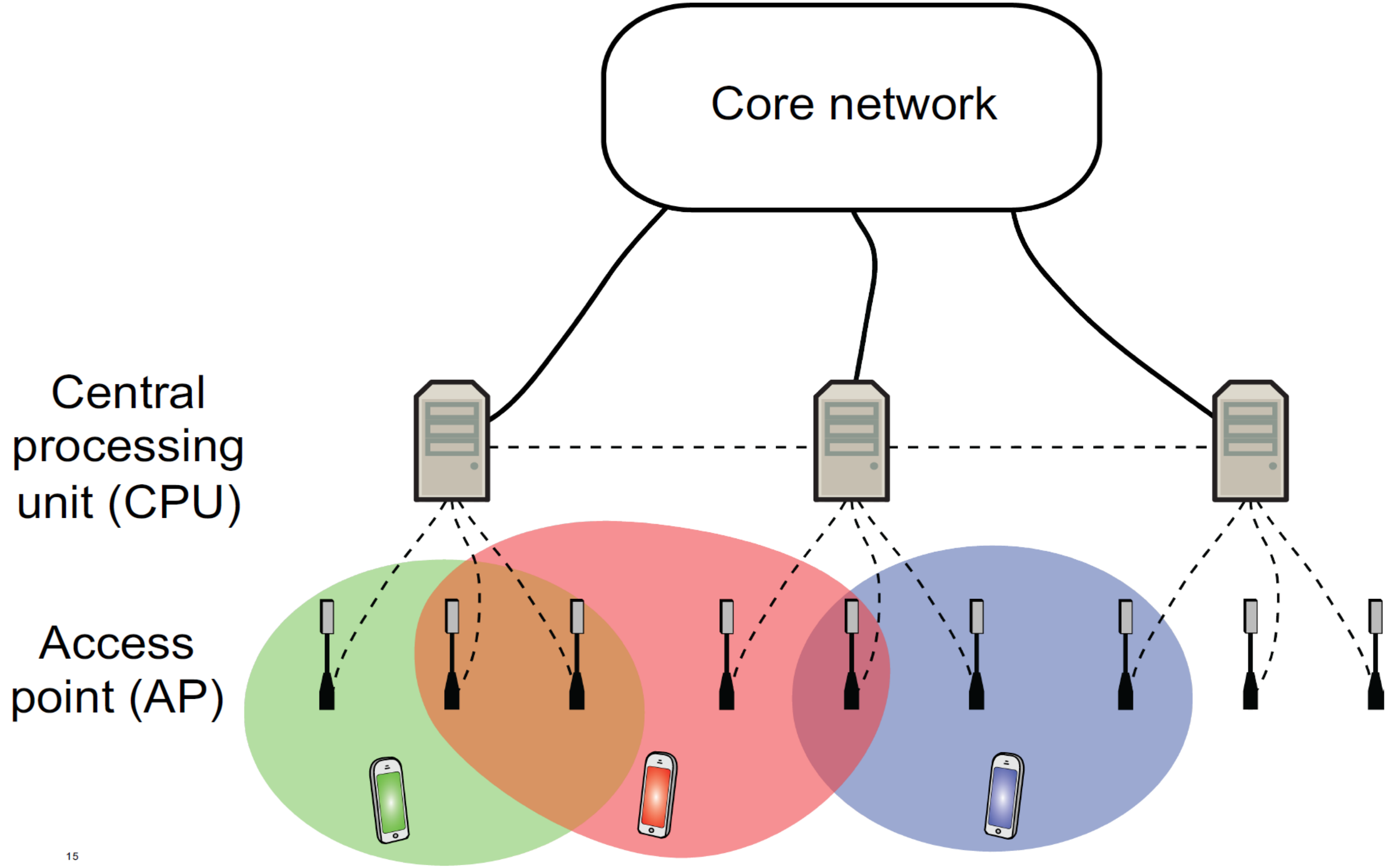
Moving Beyond the Cellular Paradigm



Massive number of distributed antennas:
Short distance from user to some antennas

Connection to Massive MIMO:
$M \gg K$
M antennas, K users

Signal Processing: Centralized versus Distributed



Processing tasks
Channel estimation
Precoding/combining
Data en-/de-coding

Centralized version
Every done at a CPU

Distributed version
Most processing at AP, fusing of signals at a CPU

Sparse Deployment of Access Points

Visible installation

Sensitive to blocking

Large variation in distance to users →
Large signal strength variations

4