Neutral Host

RWA Webinar

celona

RWA
RURAL WIRELESS ASSOCIATION

What is network sharing?

- Passive
  - Campus
  - Tower
  - Rooftop
  - Power
  - Cabinets
  - Lighting
  - Air Conditioning
- Active
  - Antennas
  - Access Network
  - Transmission
  - Spectrum
  - RF Design / Planning
  - Core Network
  - Air Conditioning

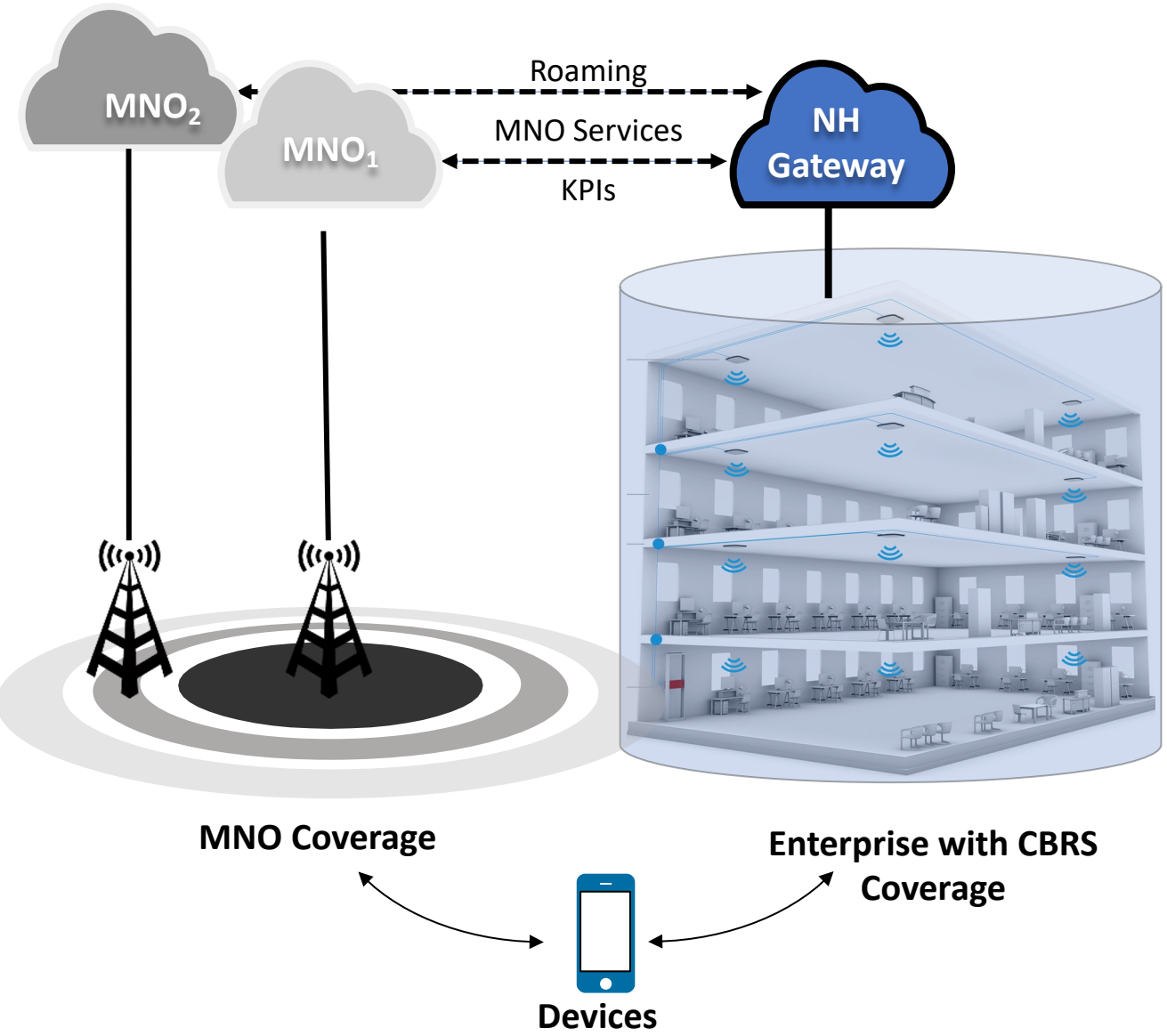
Focus is on the active aspects of network sharing

What is a neutral host?

- Motivation:
  - Lack of seamless mobile coverage and poor user experience is common in many indoor venues
  - Traditional indoor cellular systems are too costly and complex for enterprise deployment at smaller venues
  - The large gap between the top end of the indoor cellular market directly served by the Service Providers (SPs) and hundreds of thousands of smaller, low-traffic (“mid-market”) venues is stark
  - There is a growing need for a Neutral Host Network (NHN) operator to bridge the gap between very large projects with direct SP involvements and large numbers of smaller projects that are too small for SPs to consider, but too complex for enterprises to handle on their own
  - requires a low-cost solution that removes complex business models associated with the multi-operator support
- A network host is an enterprise network that allow for SP devices to camp on the system through established business arrangements
  - Primarily enabled through the use of shared spectrum
- Enable “five bar” mobile service indoor “mid-market” venues

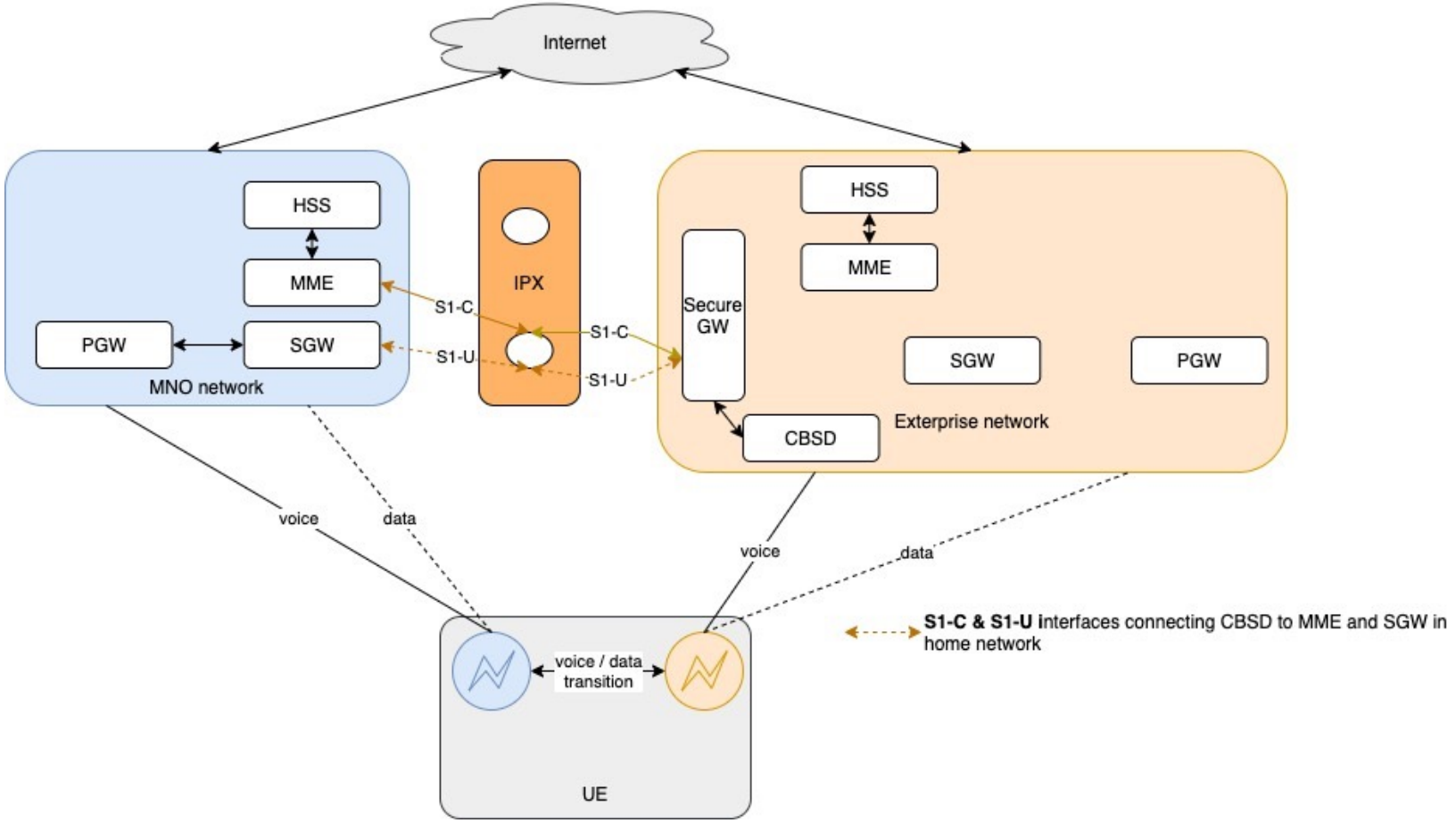
Neutral Host Opportunity

CBRS Neutral Host

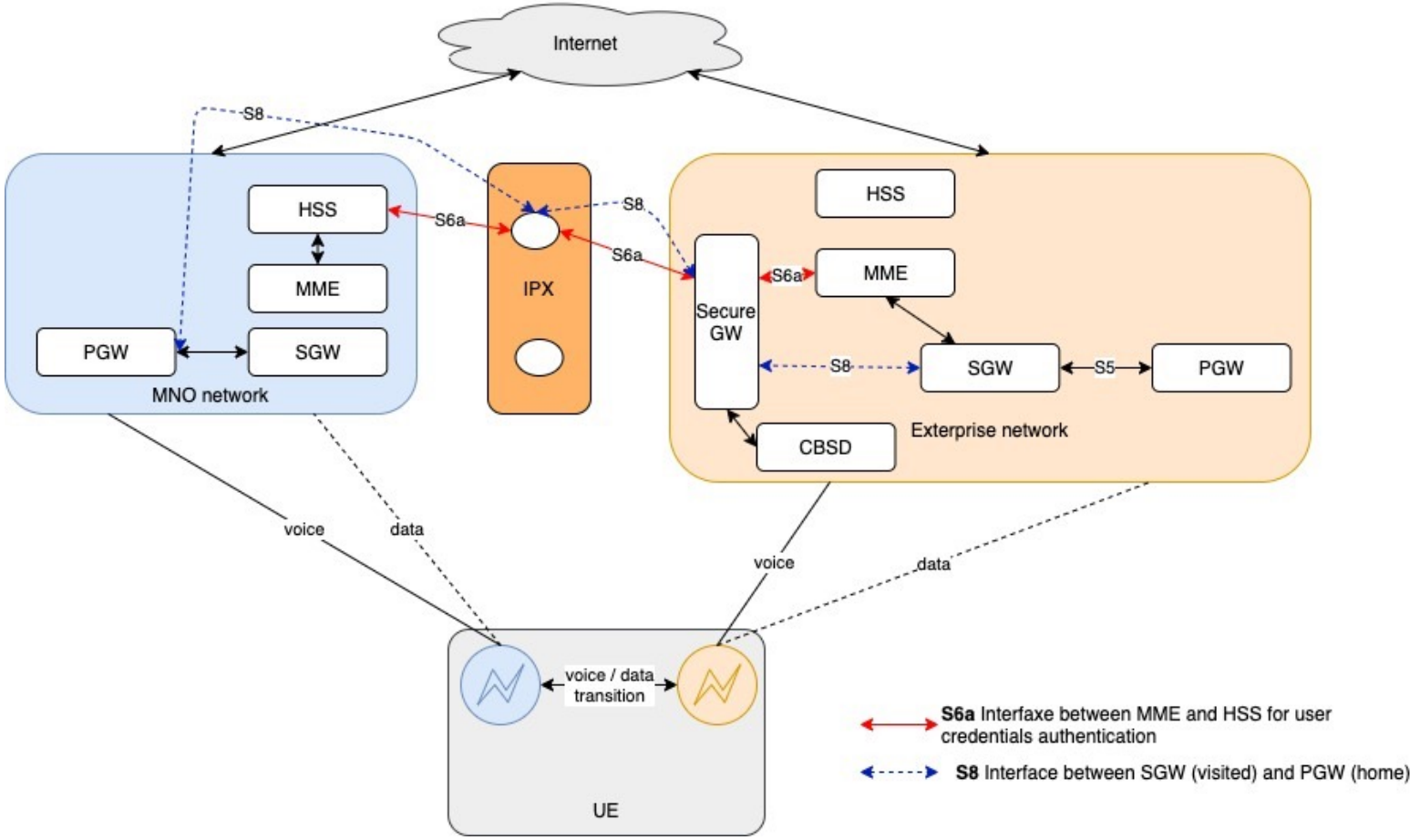


- Small cells in enterprise in shared spectrum (CBRS band)
  - Deployed independent of licensed band
- Enterprise connected to MNOs via MOCN Gateway
  - Well defined standards 3GPP interface
  - Connection to multiple MNO cores
- Devices are directed or self-discover and transition to Neutral Host
  1. CYOD devices provided by Enterprise IT
  2. BYOD devices by customer, visitor or employees

Enterprise interworking with MNO using S1 interface



Enterprise interworking with MNO using S6a / S8 interfaces

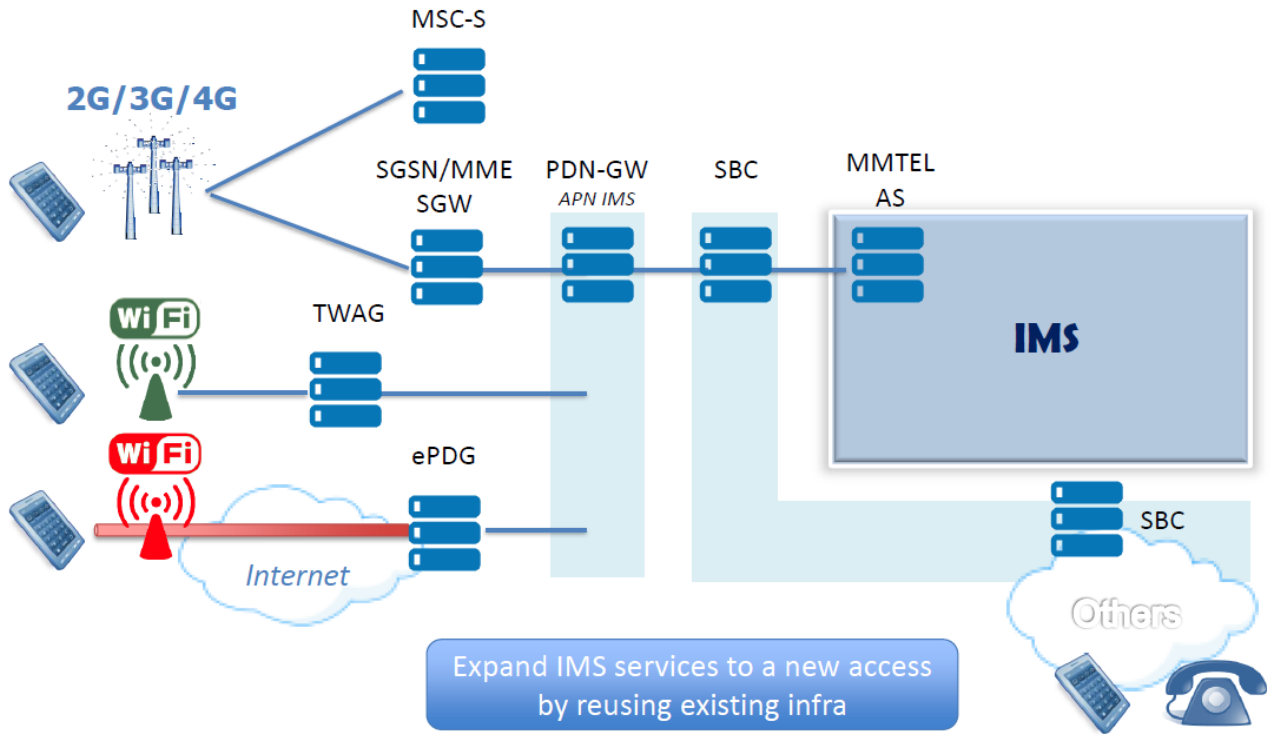


CBRS Enterprise network implementation details: Internet Connectivity (for data)

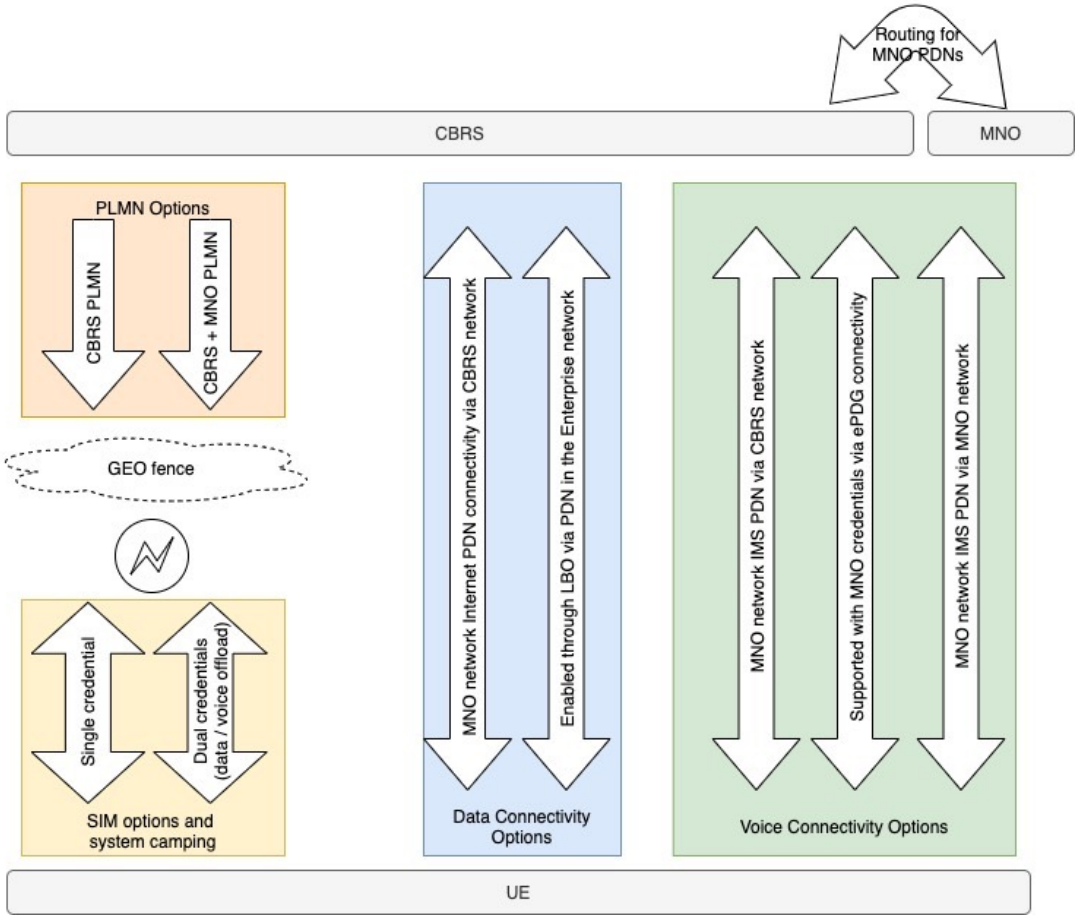
- With S1 interface with MNO credentials
  - All traffic is routed to the home network except for specific LTO support based on the filters configured in the router
- With S6a/S8 interface with MNO credentials
  - Internet traffic is supported with a CBRS Enterprise Internet APN with the below options:
  - With single-SIM credentials require the CBRS Enterprise MME to recognize Internet APN and establish the appropriate PDN connection
    - This choice is typically done together with IMS traffic offload into the CBRS Enterprise network
- With dual-SIM credentials, data offload is done using the CBRS Enterprise credentials as LBO (local breakout)

MNO connectivity from untrusted enterprise networks

- With dual-SIM and Internet offloaded to enterprise network
- No S1 or S6a/S8 connectivity with the MNO core
- VOPS not enabled in the network
- Support of “Wi-Fi calling” over the Internet PDN
- UE procedure to establish connectivity to IMS PDN over the Internet PDN using the IPSec tunnel to the ePDG node
- A fallback option when explicit connectivity cannot be established with the MNO core



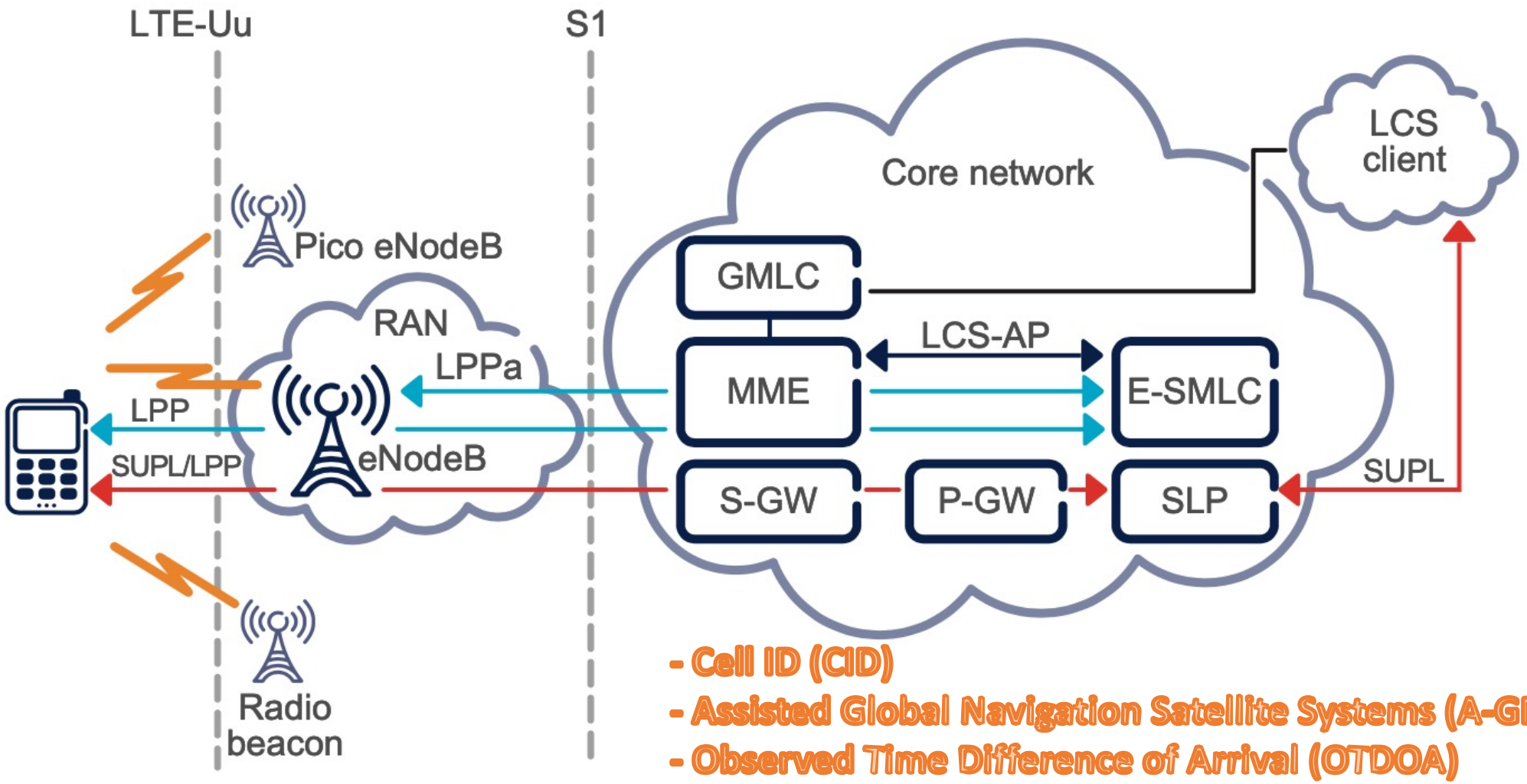
CBRS roaming UE & network configuration options



IMS and RCS service

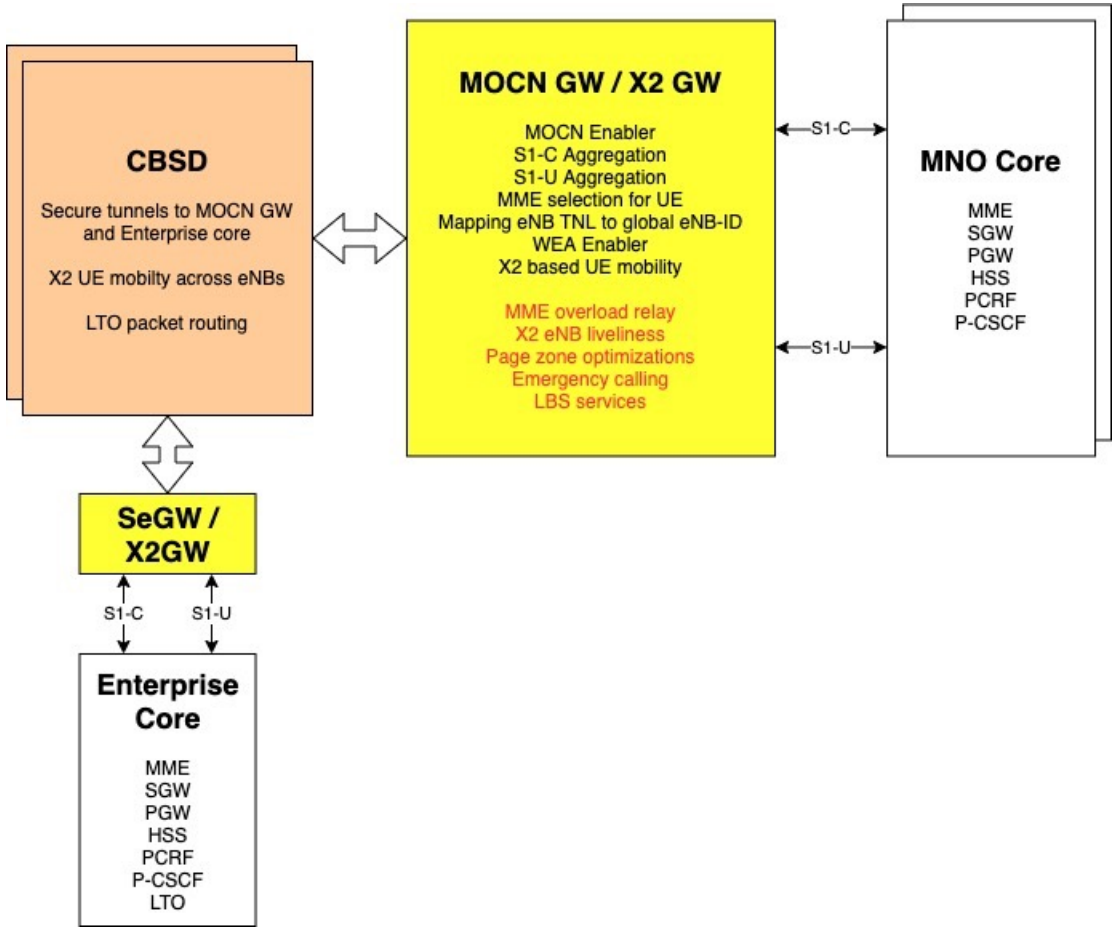
- Connectivity based on IMS PDN support from the MNO
- eNBs scheduler manages the QoS treatment based on the Priority and ARP settings associated with the QCI for the individual flows
  - SIP signaling, VoLTE, VT, IM, FT, …
  - Scheduler will be optimized for VoLTE / VT
  - Supporting RAN features are enabled to accommodate VoLTE while maintaining system capacity
- Flows are admitted based on the resource availability
  - The rates supported within the flows will be based on the current congestion levels in the network
- E911 Options:
  - Fallback to MNO network for emergency calling
  - Enable enterprise network to support emergency calling

Positioning architecture in LTE



- Cell ID (CID)
- Assisted Global Navigation Satellite Systems (A-GNSS)
- Observed Time Difference of Arrival (OTDOA)

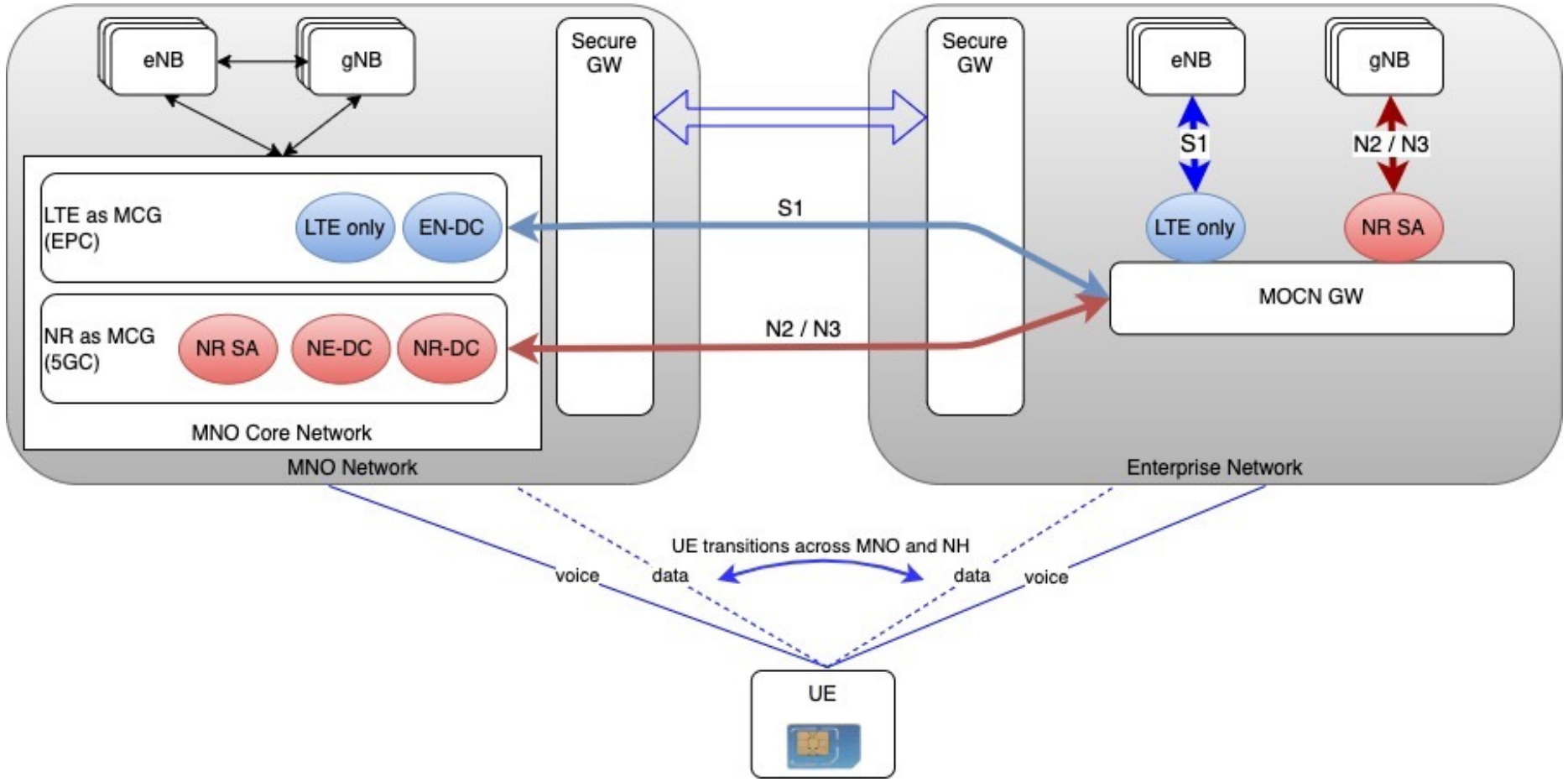
MOCN GW and eNB functions



Mobility between MNO network to Enterprise network

- Idle transitions:
  - MNO → Enterprise : The typical behavior is idle transitions from macro MNO to enterprise network. Essentially, the UE will wait until it transitions to idle and use Cell-Selection procedures to transition from the MNO to the Enterprise network.
  - Enterprise → MNO :
- Active transitions: This requires active connection to be moved from macro MNO to enterprise network
  - The S1AP message exchange steps involved are
    - HANDOVER REQUIRED (Source to Target requesting resource allocation) → HANDOVER COMMAND (Target to Source providing eNB resource allocation) → HANDOVER REQUEST (Source to Target initiating the Handover)
  - With MOCN GW, the specific eNB where the resources need to be allocated cannot be reached by the MNO MME given that the communication is only with the MOCN GW.
  - Specific customizations are required to the S1AP messaging protocol to mobility from MNO network to specific eNBs within Enterprise campus

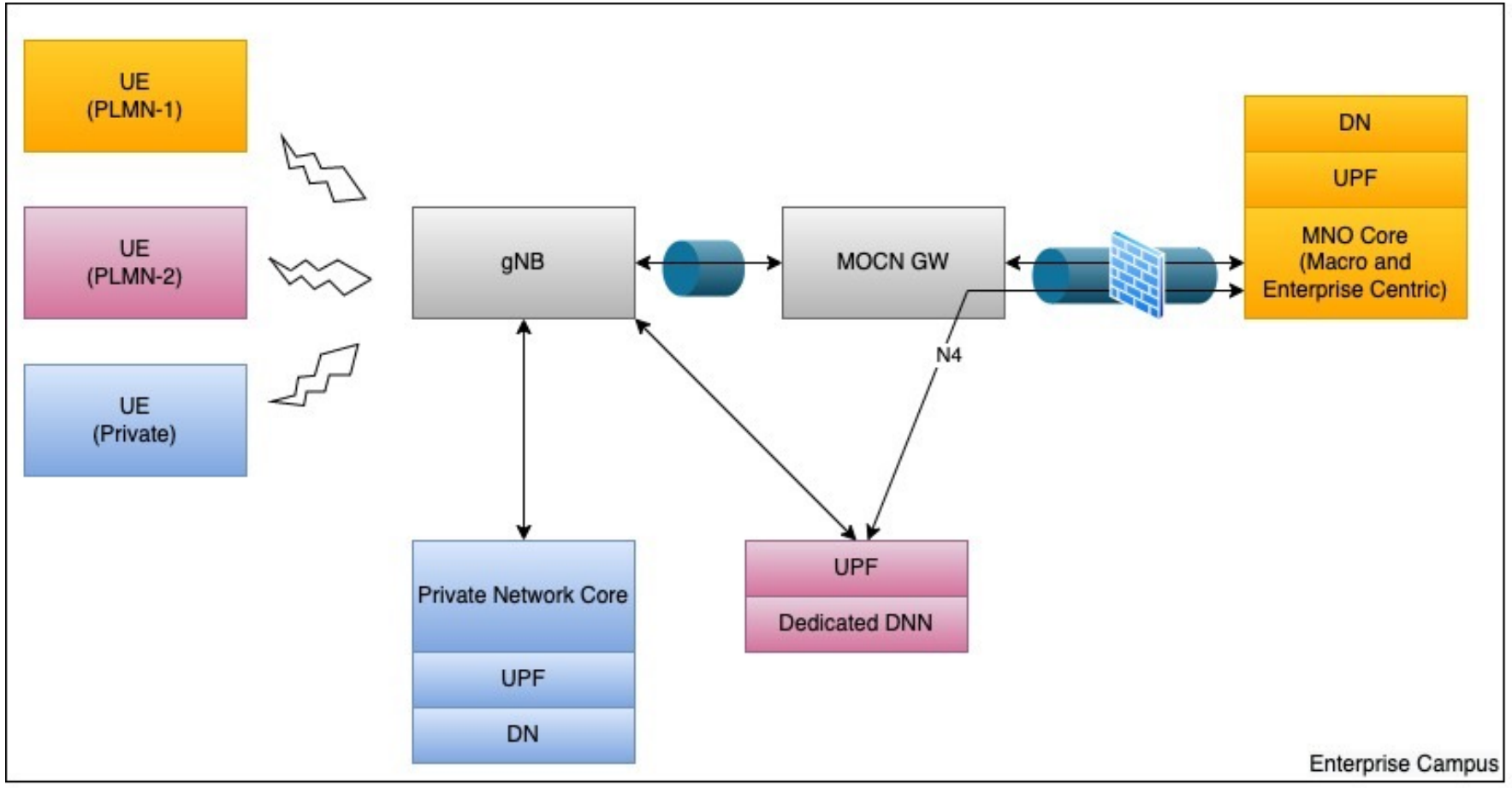
MNO to NH transitions



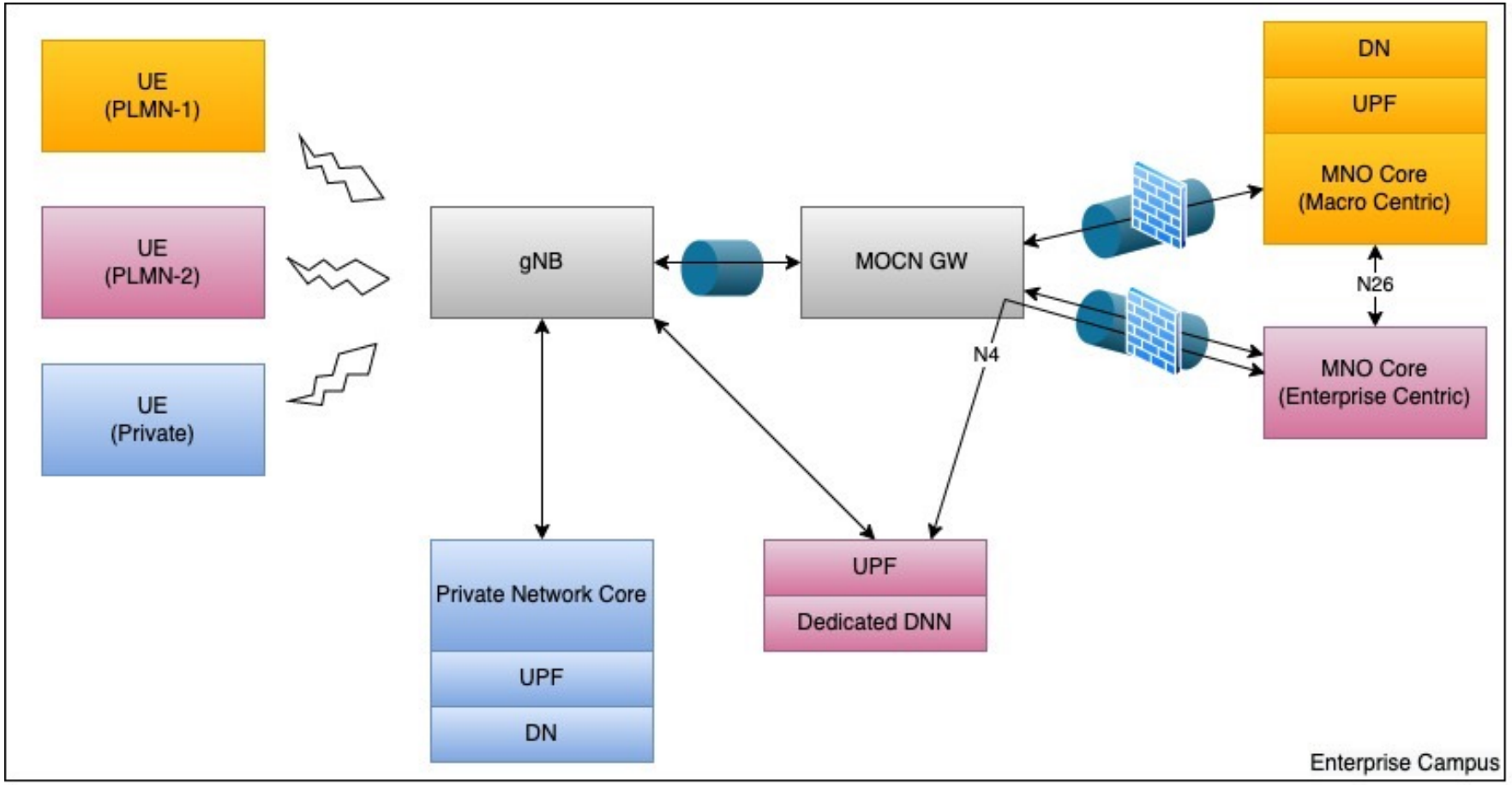
3GPP Rel-16: SNPN and PNI-NPN based operation

- This slide addresses the evolution to 3GPP Rel-16 based enterprise networks
- UEs are provisioned with both MNO-PLMN and NID; UEs use one of both of the identifiers to find the enterprise network;
- The enterprise network includes the MNO-PLMN apart from the other PLMNs in its broadcasts. It also includes the 3GPP-NID identifying the SNPN operation of the enterprise network
- CAG support to further protect the UE access to specific enterprise networks can be envisioned
- Connectivity to the MNO core from the enterprise network is per the prior established procedures via the MOCN GW

PNI-NPN Evolution-NR Integrated Core



PNI-NPN Evolution-NR Independent Cores



Appendix

Detailed reference material for offline reading

System Camping

Information used by UE for system selection

EHPLMN

- Equivalent HPLMN (Home PLMN). It contains the list of PLMNs which can be regarded as a Home PLMN.

HPLMNwAcT

- 'HPLMN with Access Technology'. It stores the HPLMN and list of available Access Technologies. This parameter contains the list of (PLMN, Access Technology) pairs

PLMNwACT

- 'User Controlled PLMN with Access Technology'. This parameter contains the list of (PLMN, Access Technology) pairs. This information is determined by the user and defines the preferred PLMNs of the user in priority order.

OPLMN

- Operator controlled PLMN selector with Access Technology. This parameter is set by Network Operator. This is where Network operator put another networks which has roaming agreement with. This parameter contains the list of (PLMN, Access Technology) pairs.

Forbidden PLMN

- PLMNs where the UE encountered failures and marks them as forbidden in volatile memory

Tracking Area Code Reject

- TAU rejects from the network with back-off based on error codes. Retained in volatile memory

EF_HPPLMN

- Higher Priority PLMN search period

Available system selection mechanisms

System Selection

- Single PLMN : This is the typical configuration used by most MNOs. The LTE SIB will transmit a single PLMN that the UEs can use to identify the system to camp.
- MOCN : Multi-Operator Core Network. This mechanism uses the LTE SIBs and allows for supporting multiple PLMNs from a single eNB. UEs use the preferred PLMN amongst the list broadcasted to enter the system. Enterprise LTE RAN is connected to multiple MNO core networks via the S1. MME is also shared between the MNOs

HPLPLMN Scan

- UE when camped on a lower preferred system, periodically looks for available higher priority systems restricting the scans to the MCC of the currently camped system.

EHPLMN

- When the UE looks for available networks, it will look for the most preferred system within the defined EHPLMN list before camping on a specific system. Once the UE is camped on a PLMN from the EHPLMN, it is in an equivalent home system and further prioritization within the EHPLMN list is not employed.

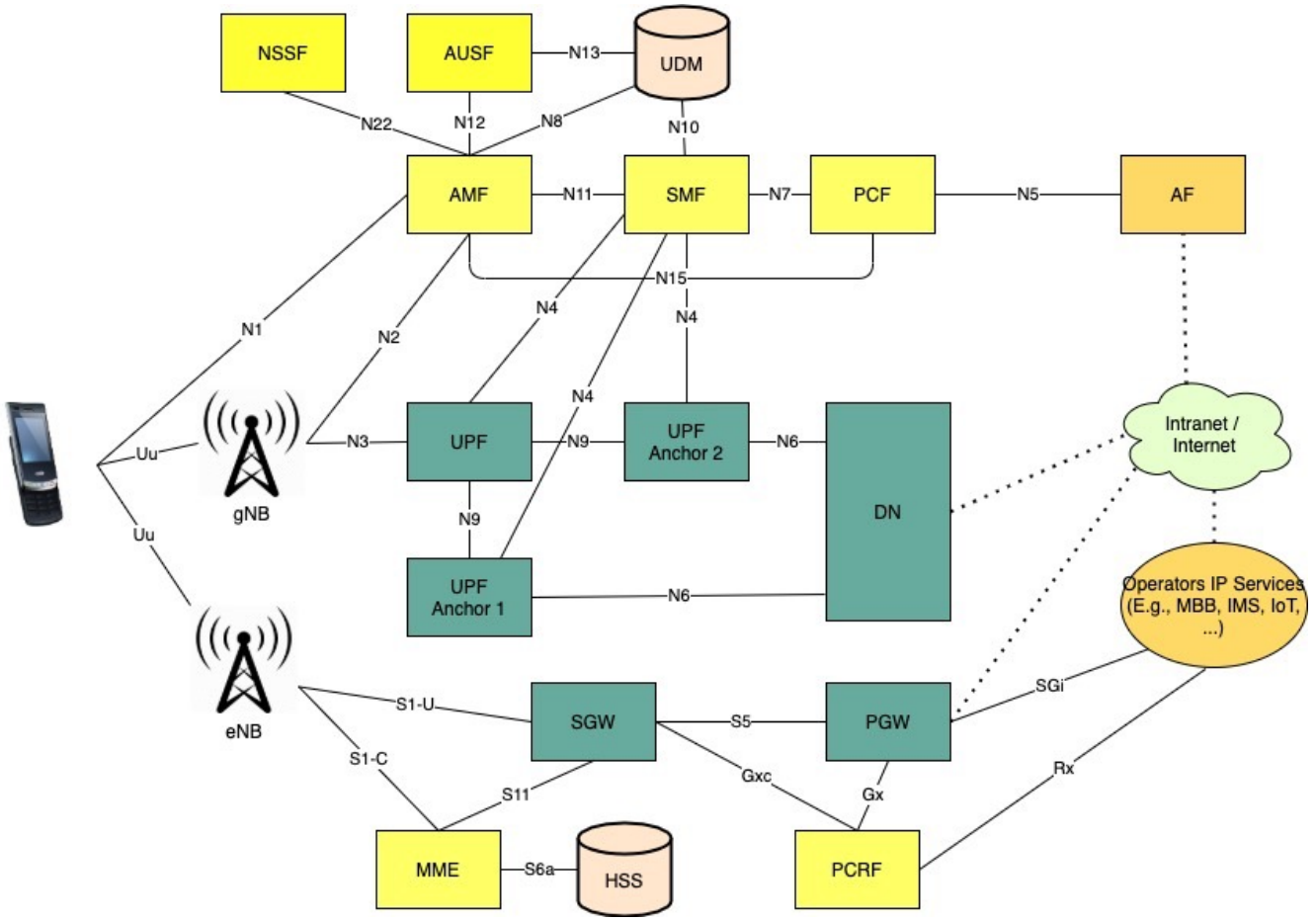
Identifiers for CBRS Systems

Identifier	Identifies	Comments
Shared HNI (SHNI)	315-010 indicates a CBRS system	Further Shared HNIs could be assigned
NID	CBRS Network	NOT based on SHNI NID (Network ID) based on LTE CSG-ID needs to be unique so that devices can recognize their system(s).
IMSI	Subscription	Based on SHNI
GUMMEI	MME (Mobility Management Entity)	Important for roaming. Based on SHNI
Cell ID/ECGI	Cell or sector (eNodeB)	Based on SHNI
TAI/TAC	Network (locally)	Based on SHNI

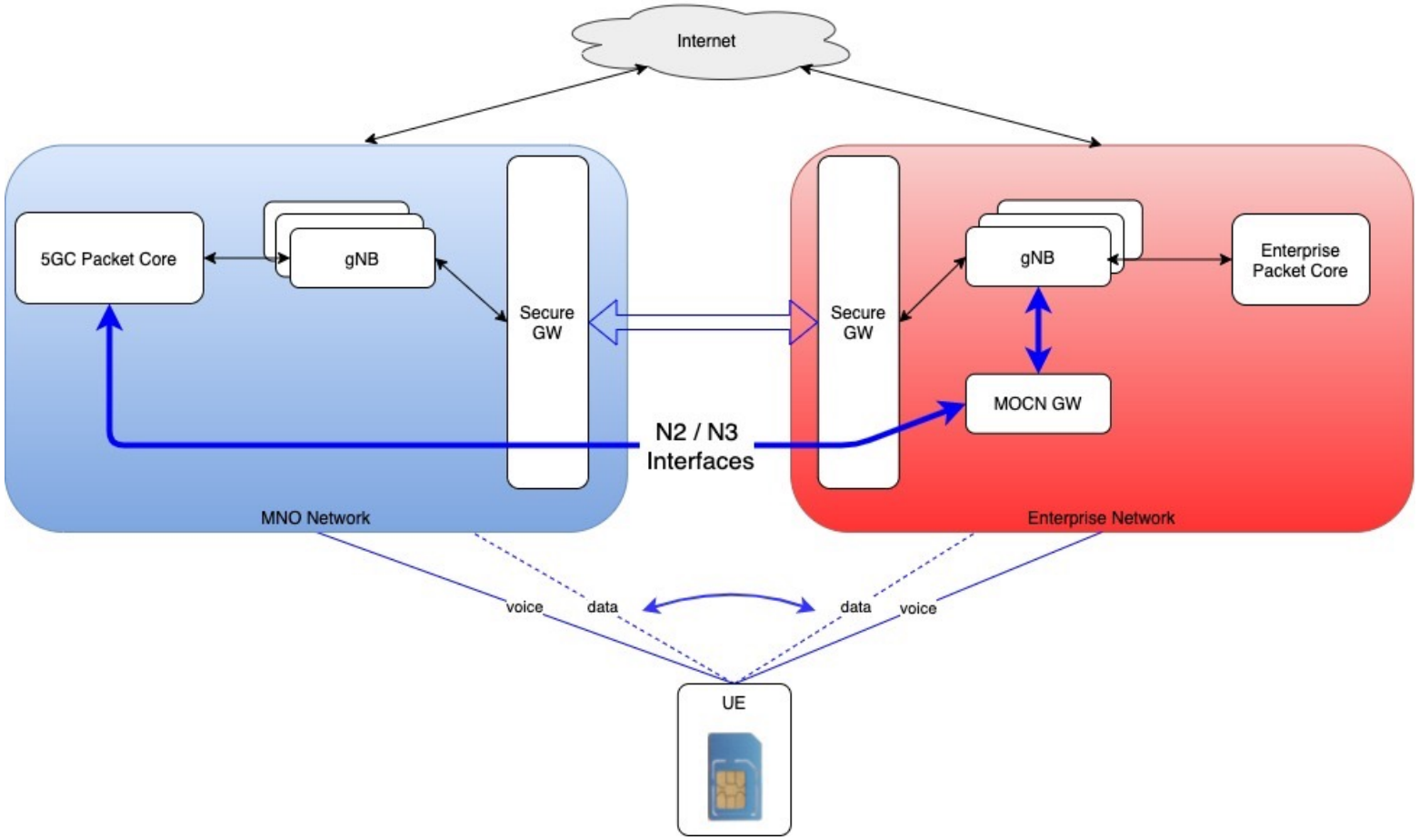
Discussions in OnGo to support TAC-ID/Cell-ID to make it unique for both MNO Core and Enterprise networks.

End-to-end network architectures

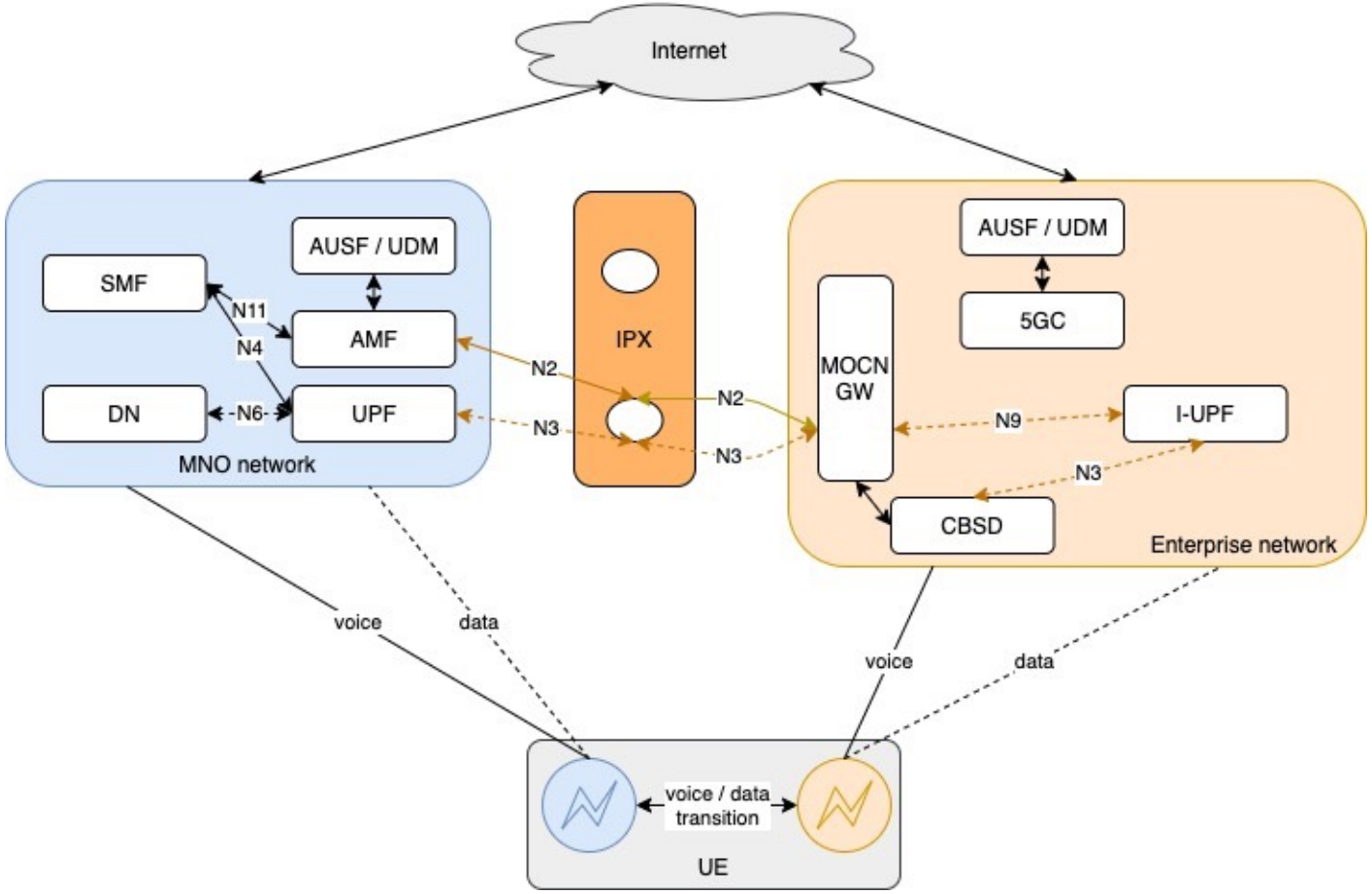
4G and 5G E2E Architecture



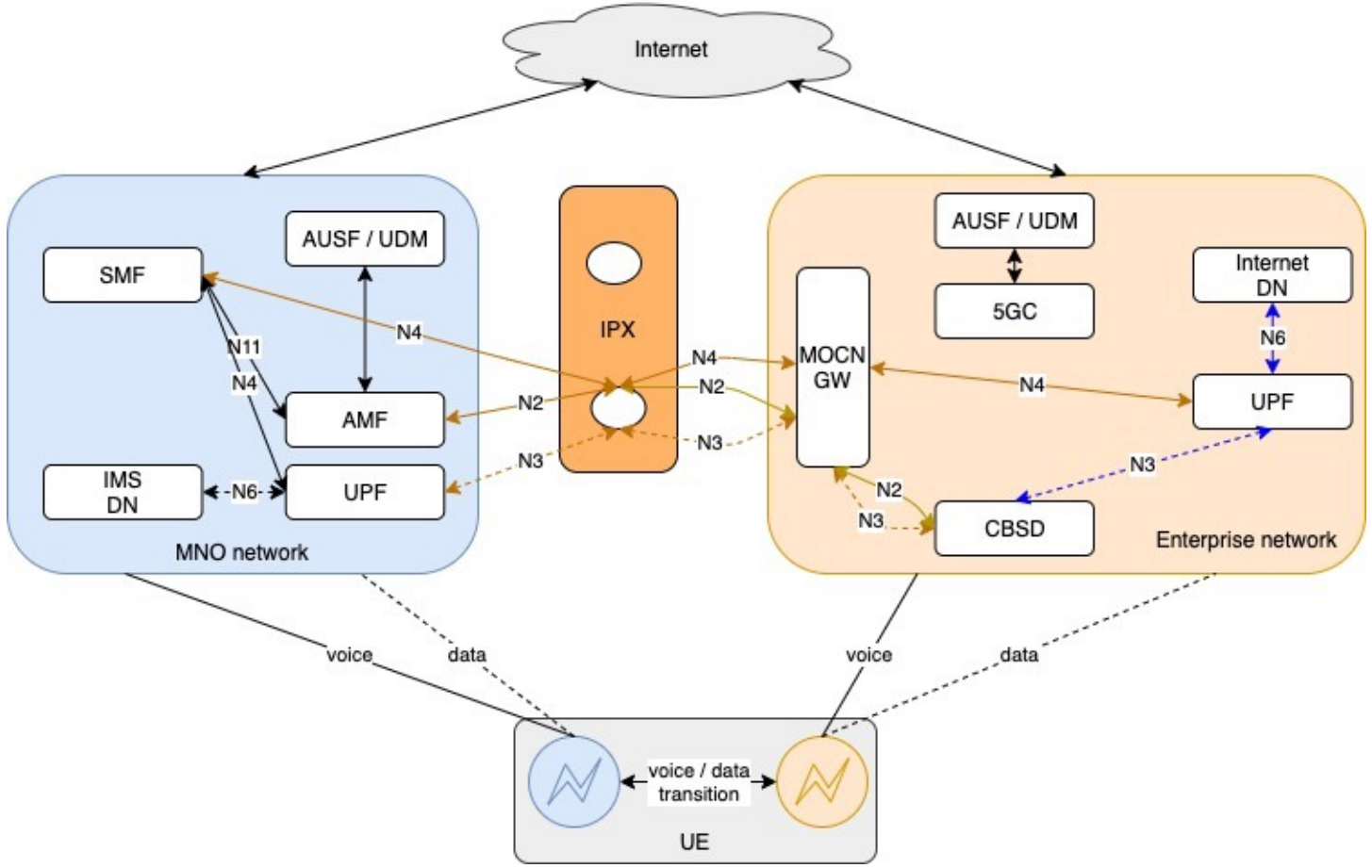
NR Neutral Host Architecture : N2/N3 OVER MOCN GW



Enterprise Roaming Network Architecture - MOCN



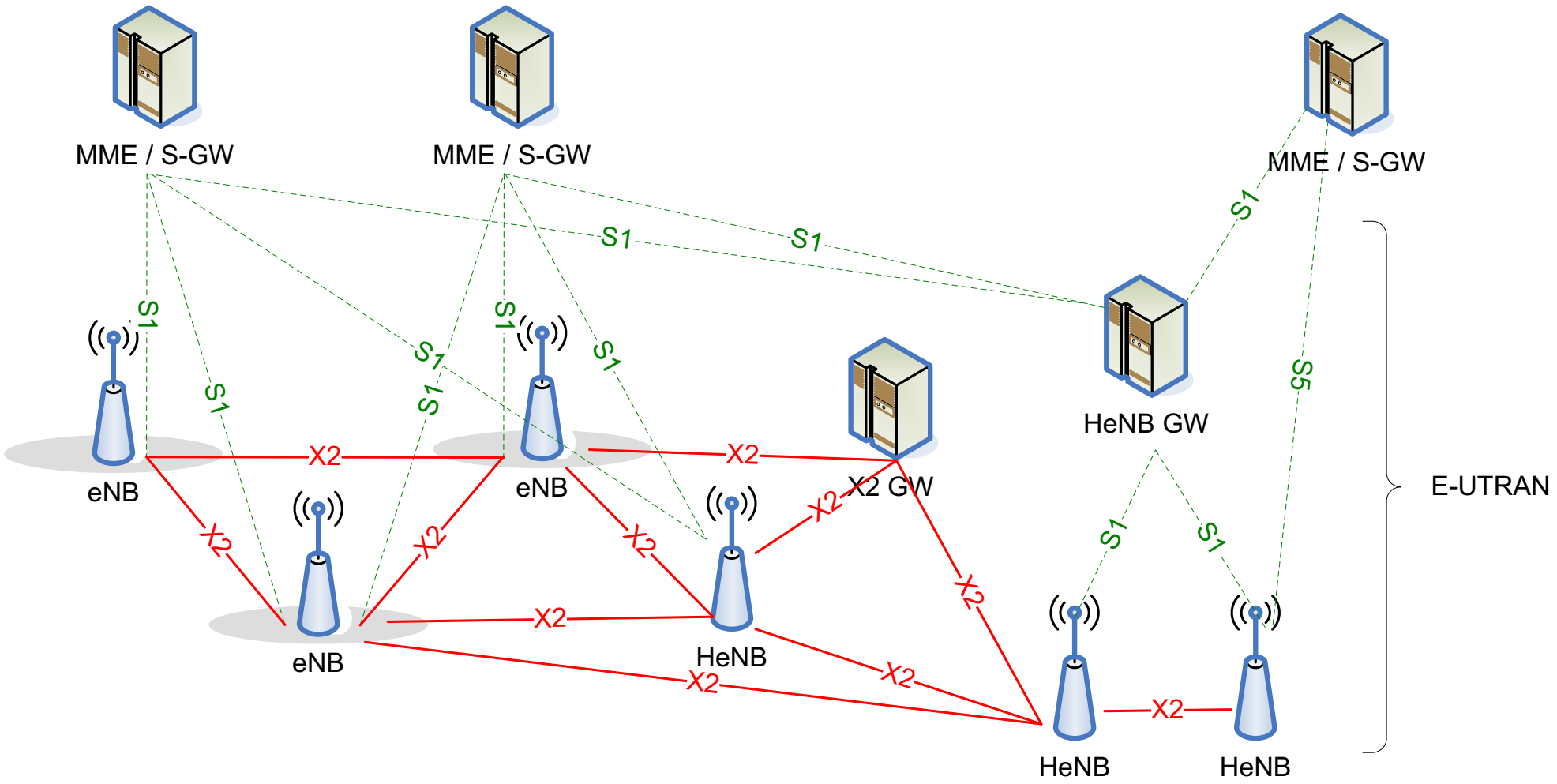
Enterprise Roaming Network Architecture - MOCN with DNN / NETWORK SLICING



HeNB GW functions

- Terminating non-UE associated S1 application part procedures towards the eNB and towards the MME.
  - In case of S1 SETUP REQUEST message, verifying, as defined in TS 33.320, that the identity used by the eNB is valid.
  - In case of S1 PWS RESTART INDICATION message and PWS FAILURE INDICATION message, verifying, as defined in TS 33.320, that the indicated cell identity is valid and replacing the eNB ID by the MOCN GW ID before sending the PWS RESTART INDICATION message (respectively the PWS FAILURE INDICATION message) to the MME.
- Upon receiving an OVERLOAD START/STOP message, the MOCN GW should send the OVERLOAD START/STOP message towards the eNB(s) including in the message the identities of the affected MME node.
  - The eNB uses this information received from the OVERLOAD START message to identify to which traffic the above defined rejections shall be applied.
  - The eNB shall apply the defined rejections until reception of an OVERLOAD STOP message applicable to this traffic, or until the eNB receives a further OVERLOAD START message applicable to the same traffic, in which case it shall replace the ongoing overload action with the newly requested one.

Overall E-UTRAN Architecture with deployed HeNB GW and X2 GW.



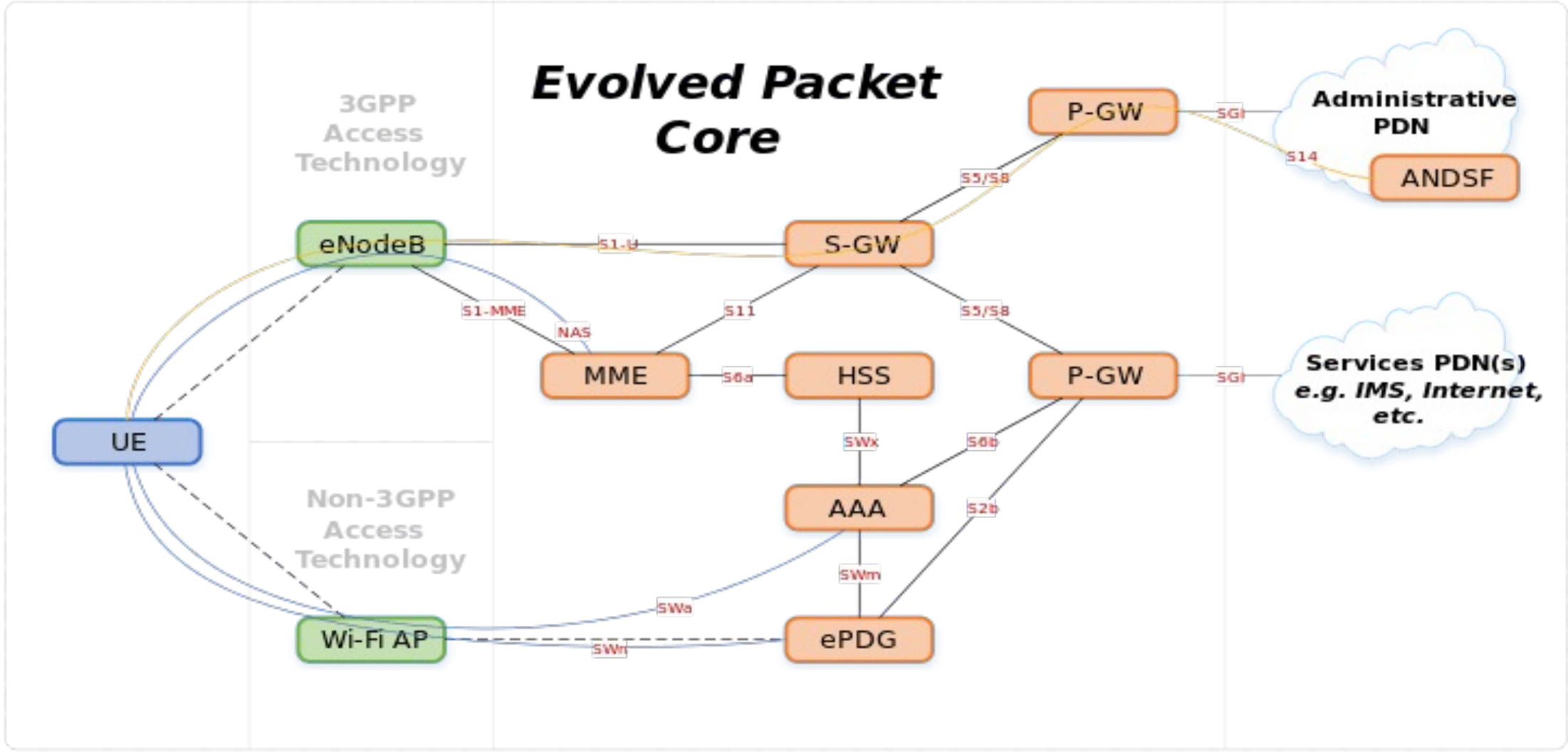
X2 mobility across HeNB / eNB

- Routing the X2AP X2 MESSAGE TRANSFER message to target eNB or HeNB based on the routing information received in the X2AP X2 MESSAGE TRANSFER message.
- Informing the relevant (H)eNBs upon detecting that the signaling (i.e. SCTP) connection to a (H)eNB is unavailable. The relevant (H)eNBs are the ones which had an "X2AP association" with this (H)eNB via the X2 GW when the signaling connection became unavailable.
- Mapping the TNL address(es) of a (H)eNB to its corresponding Global (H)eNB ID and maintaining the association.

UE Attach with MOCN GW

- Independent of the sector of the two-sector-eNB the UE associates itself with, a single eNB ID (one of the two eNB IDs) is used to establish the UE context
- The Page / Access procedures always managed from a single sector
- The eNB selects the PCC assignment for the UE based on the UL loading given the UL CA is not supported
- It is expected that the footprint of coverage of the two sectors will overlap
  - For LBS services, the UE will report measurements from both sectors independently
  - E-SMLC will assume the single selected eNB ID as the camped sector.
    - However, the measurements can be requested across the two sectors from each eNB and the location determination will be based on any of the reported eNB sectors.
    - Note as well that the individual sectors can potentially have differing coverage and the GPS location / coverage information are independently managed / configured
    - The trilateration procedures will adapt based on the information associated with the individual sectors

Evolved Packet Core



MOCN GW Functions

MOCN GW functions

- The MOCN GW appears to the MME as an eNB. The MOCN GW appears to the HeNB as an MME.
- The S1 interface between the HeNB and the EPC is the same, regardless whether the eNB is connected to the EPC via a MOCN GW or not.
- The MOCN GW serves as a concentrator for the C-Plane, specifically the S1-MME interface.
- The S1-U interface from the eNB may be terminated at the MOCN GW, or a direct logical U-Plane connection between eNB and S-GW may be used
  - The MME may send two transport layer addresses of different versions only in case of MOCN GW which does not terminate user plane.
  - Selection of an IP version to be used for S1-U, if a requested ERAB configuration contains two transport layer addresses of different versions.
- The TAC and PLMN ID used by the eNB shall also be supported by the eNB GW;
  - If routing ambiguities are to be avoided, a TAI used in a HeNB GW should not be reused in another MOCN GW.

MOCN GW functions

- Selection of an MME at UE attachment is hosted by the MOCN GW instead of the eNB.
  - Upon reception of the GUMMEI from a UE, the eNB shall include it in the INITIAL UE MESSAGE message;
  - upon reception of the GUMMEI Type from the UE, the eNB shall also include it in the message if supported and supported by the MOCN GW.
- Relaying UE-associated S1 application part messages between the MME serving the UE and the eNB serving the UE
  - Except the UE CONTEXT RELEASE REQUEST message received from the eNB with an explicit GW Context Release Indication. In that case, the MOCN GW terminates the S1 UE Context Release Request procedure and releases the UE context if it determines that the UE identified by the received UE S1AP IDs is no longer served by an eNB attached to it. Otherwise it ignores the message.
  - In case of S1 INITIAL CONTEXT SETUP REQUEST message and S1 HANDOVER REQUEST message, informing the eNB about any GUMMEI corresponding to the serving MME, the MME UE S1AP ID assigned by the MME and the MME UE S1AP ID assigned by the MOCN GW for the UE.
  - In case of S1 PATH SWITCH REQUEST ACKNOWLEDGE message, informing the eNB about the MME UE S1AP ID assigned by the MME and the MME UE S1AP ID assigned by the MOCN GW for the UE.
    - Routing the S1 PATH SWITCH REQUEST message towards the MME based on the GUMMEI of the source MME received from the eNB.

Managing WEA

- Option 1:
  - Celona Edge to support receiving emergency broadcast information from the IPAWS (Integrated Public Alert & Warning System)
  - Note that IPAWS has been enhanced to:
    - Increasing the maximum character count from 90 to 360;
    - Adding support for Spanish-language WEA;
    - Adding two new alert categories in addition to Presidential, AMBER and Imminent Threat
      - Public Safety Message - Less severe in nature than Imminent Threat
      - WEA Test Message - Opt in message to support state and local WEA testing; and
    - Enhanced geo-targeting reaching 100 percent of the targeted area with no more than 1/10th of a mile overshoot.
- Option 2:
  - Preferred option : Select the MNO MME to receive the emergency broadcast messages. The choice of MME will need to be decided based on the GEO fencing of WEA messages handled by the MME
  - Alternative is to process the messages received from all MMEs and broadcast only non-duplicates; Requires duplicate message detection across MNOs.
- In both options, the MOCN GW needs to process the message to ensure relevance for transmission for the enterprise campus based on the indicated GEO targeting information provided

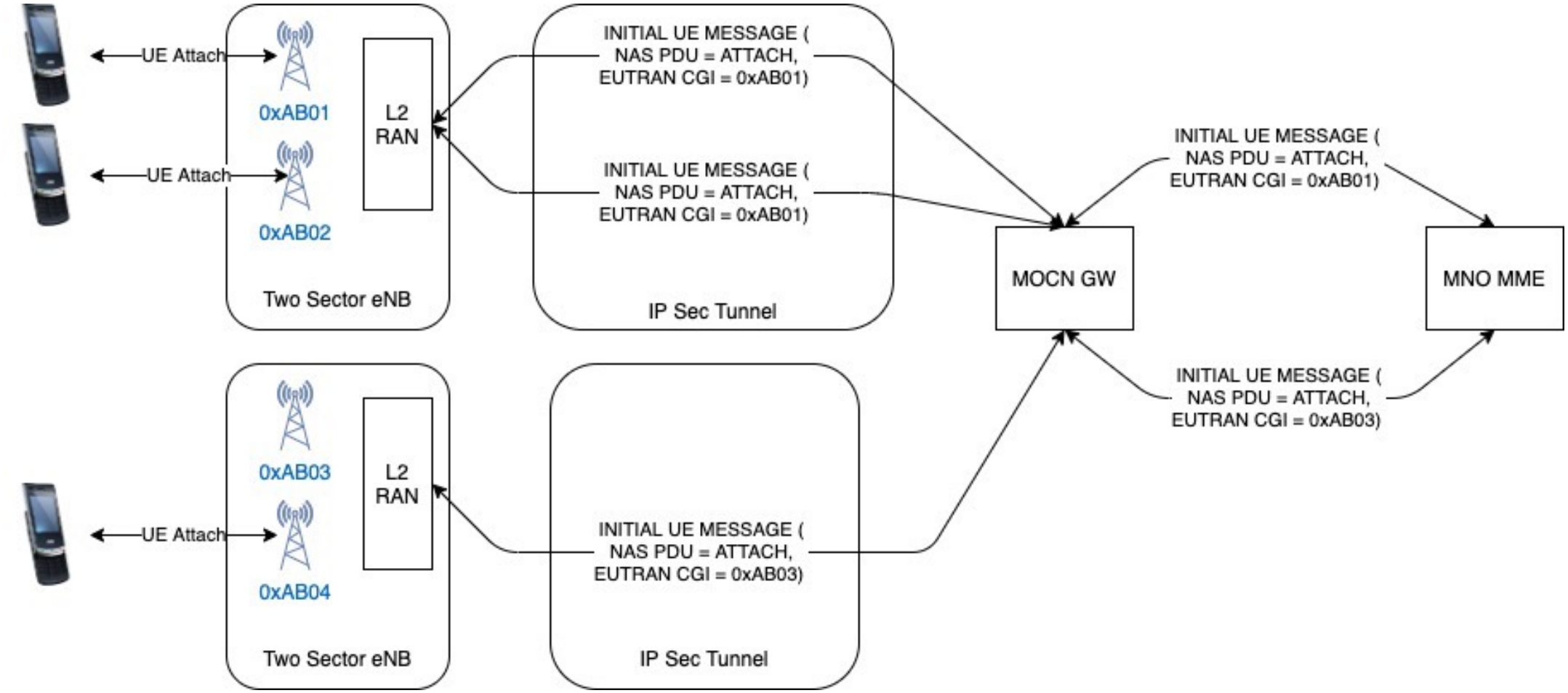
Secure tunnels from eNB (Enterprise, MNOs)

- From eNB
  - Two secure tunnels to be established
    - eNB to SeGW for Enterprise core traffic
    - eNB to MOCN GW for MNO core traffic
  - Both tunnels can be supported by the Enterprise IT including key management
- From MOCN GW
  - One secure tunnel with each eNB deployed in the Enterprise campus. Keys are managed by Enterprise IT
  - One secure tunnel with each MNO terminating both control and user plane traffic. Keys are managed by the MNO Core or by the IPX vendor
- From SeGW
  - One secure tunnel with ea ch eNB deployed in the Enterprise campus. Keys are managed by Enterprise IT
- Based on the mechanism of handling dual-sector eNBs, we may need to support two connections from the eNB to MOCN GW

Page optimizations

- An enterprise campus can be supported with one or more TAC. Typically a site, based on the size, will have only a single TAC.
- Option 1: Page the UE across all eNBs in the TAC
  - A simple approach
  - Based on the size of the campus, the paging channel capacity needs to be managed based on expected traffic
- Option 2: Page the UE based on previously known proximity
  - Select the group of eNBs relative to the previously known location of the UE based on prior accesses
  - Age the information and page across the full TAC after timer expiry
- Option 3: AI based
  - Learn the UE's patterns of mobility and page the UE first in the typical eNBs (sets of eNBs based on location) where the UE typically access the network
  - Subsequently page the UE across the full TAC

UE Attach with MOCN GW



NR Neutral Host

N2 / N3 over MOCN GW

- NG HO; Xn HO for a later phase
- The MOCN GW acts similar to the functional implementation for LTE based NH operation
  - The LTE S1-C / S1-U is replaced with N2 / N3 interfaces for NR
- The RAN network deployed in the enterprise is shared across enterprise operation and across one or more MNO PLMNs.
- The RAN functions of CU / DU / RU will be deployed in the enterprise network
- The user authentication, IP allocation, and QoS operations are managed from the MNO core
- MOCN GW support will keep it uniform across LTE and NR networks

3GPP Rel-15 based NR SA NH operation

- The enterprise network includes the MNO-PLMN along with the other PLMNs in its broadcasts
- UE is provisioned with the MNO-PLMN; Procedures used to find the LTE enterprise network for camping is used for 3GPP Rel-15 based NR SA enterprise network camping
  - Transitioning from LTE macro to enterprise NR
    - Macro network populates the SIB24 listing the enterprise NR cells as neighbors;
  - Transitioning from NR macro to enterprise NR
    - Macro network populates the SIB3 listing the enterprise NR cells as neighbors
- NH cell identifiers
  - TAC-ID : 24-bits
  - Cell-ID : 36-bits

3GPP Rel-16 features

- 3GPP Rel-16 SNPN and PNI-NPN
  - The enterprise network includes the MNO-PLMN apart from the other PLMNs in its broadcasts.
    - SNPN mode: It also includes the 3GPP-NID identifying the SNPN operation of the enterprise network
    - PNI-NPN mode: CAG support to further protect the UE access to specific enterprise networks where NH camping is allowed.
  - Connectivity to the MNO core from the enterprise network is per the prior established procedures via the MOCN GW
- It is possible that the UE introduces support per-PLMN based TAC-ID in the SIB in the future
- Dedicated-DNN for local breakout
- Network slices together with PNI-NPN
- LTE + 5G NR multimode campus deployments for NH

GSMA context

Based on “5G industry campus network deployment guideline”

GSMA ”5G industry campus network deployment guideline”

- NPN is a term defined by 3GPP [1] for a network that is intended for non-public use purpose. It could be exclusively used by a private entity such as an industry enterprise, and could utilize both virtual and physical elements and be deployed in different type of configurations. NPN could exist in two different formats [4] and their corresponding management aspects has been studied in [5]:
- Standalone NPN (SNPN)
  SNPN is operated by an NPN operator and not relying on the network functions provided by a Public Land Mobile Network (PLMN) owned by MNO. An NPN operator could be the enterprise itself or a 3rd party. An NPN operator has full control and management capability on the network functions provided by SNPN.
- Public network integrated NPN (PNI-NPN)
  PNI-NPN is an NPN deployed with the support from a public network. Based on the contract between the MNO and enterprise, the MNO could provide network resources extracted from the public network for the enterprise to use. PNI-NPN could be provided by means of dedicated Dynamic Neural Networks (DNNs) (assigned for industry customers) or network slicing from a public network (which is further explained in Section 3.1.2).

GSMA ”5G industry campus network deployment guideline”

- 3GPP defines that Radio Access Network (RAN) could be shared in different access scenarios, for instance, shared by one or multiple SNPNs, and one or multiple PLMNs, etc.
- NPN architecture aspects begins from 3GPP Release 16, and a number of enhanced features are further discussed in Release 17 [12], for instance:
  - enhancement to enable support for SNPN along with subscription / credentials owned by an entity separate from the SNPN
  - support device on boarding and provisioning for NPNs
  - enhancement to the 5GS for NPN to support service requirements for production of audio-visual content and services e.g. for service continuity
  - support voice/IMS emergency services for SNPN.

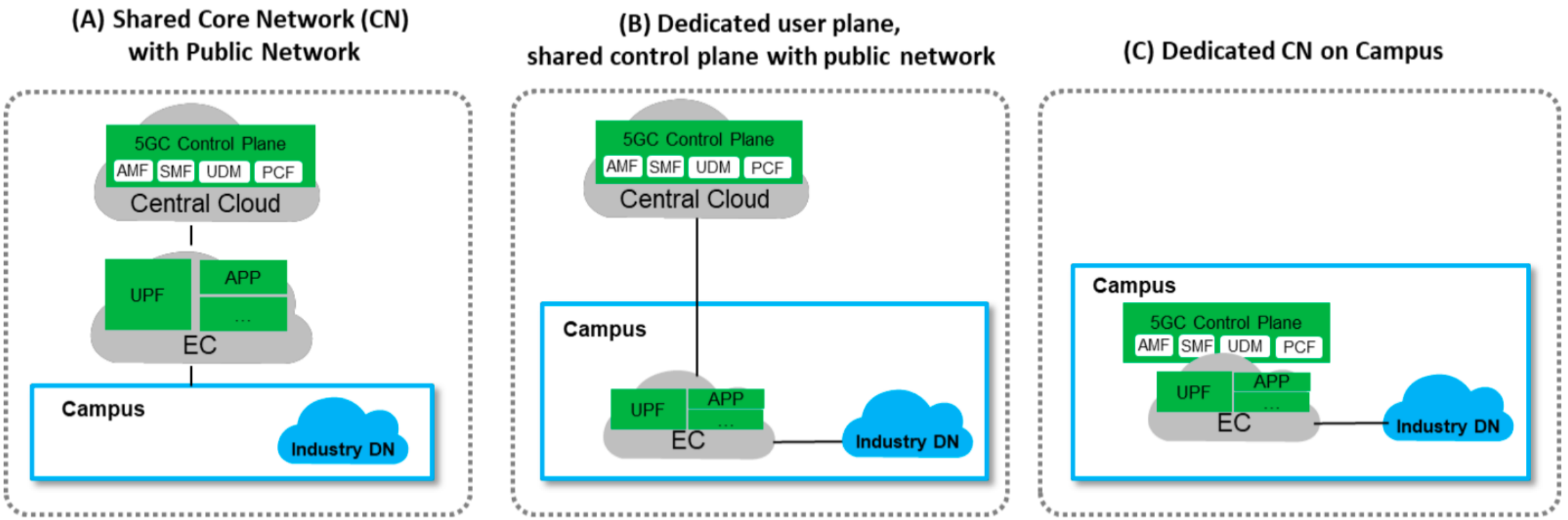
GSMA ”5G industry campus network deployment guideline” (Network Slicing)

- Network slicing could be used to provide public network services, or NPN services, especially PNI-NPN. Such network slice could contain specific network functions or features for industry customers like device on boarding, secondary authentication, TSN integration, etc. Moreover, certain network capability or Application Programming Interfaces (APIs) offered by the network slice could be exposed to the industry customers as well.
- The existing 3GPP network slicing functionalities for management could apply for managing such PNI-NPN following the Network Slice as a Service principle [6].
- What should be noticed is that, network slicing is a compulsory feature for 5G, so in theory, a SNPN could also contain one or multiple slices which are not related to PLMN.
- In order to have an end to end network slicing, it requires a cross standardization organization effort. For more information about the relevant network slicing industry, please refer to Annex B.

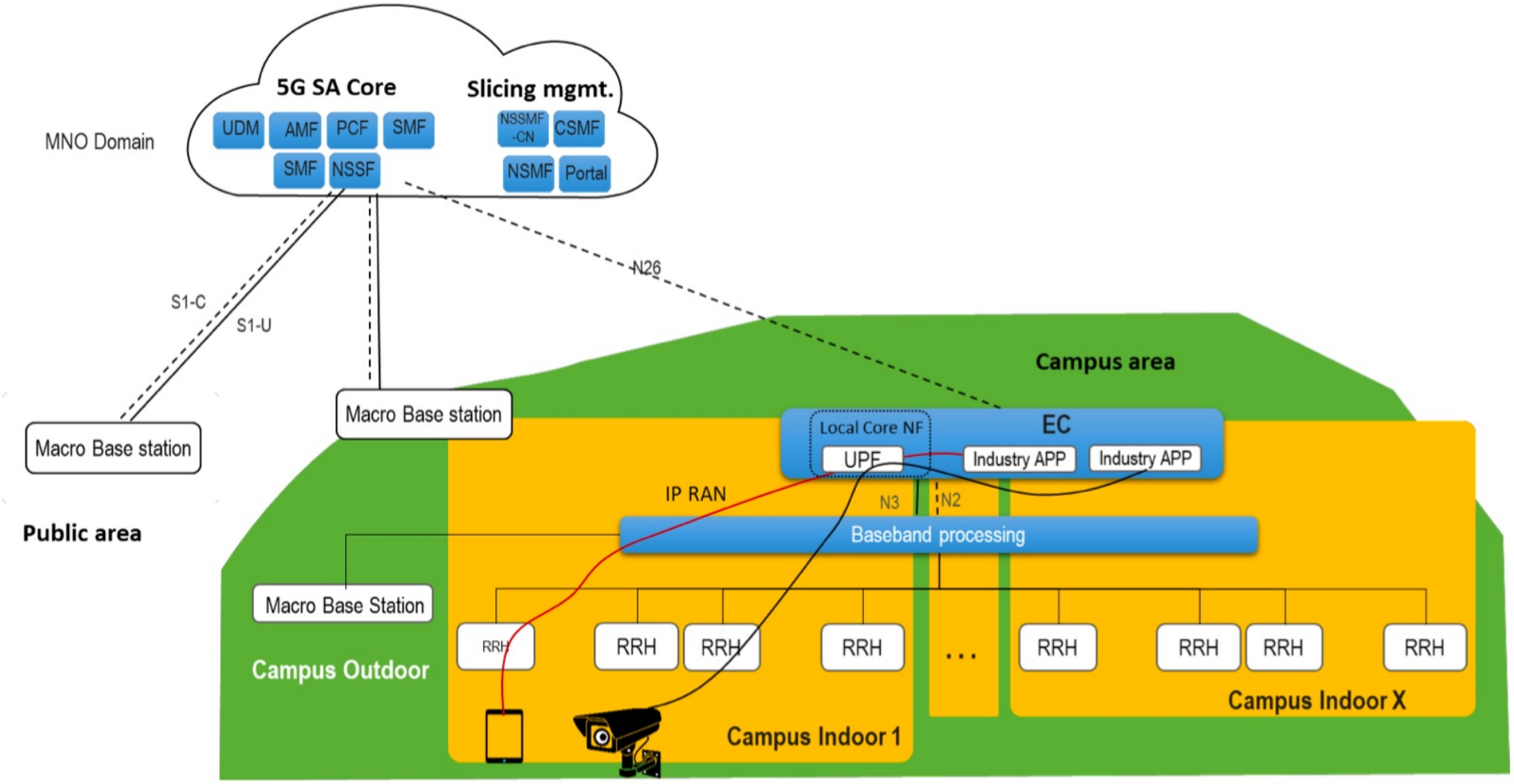
GSMA ”5G industry campus network deployment guideline” (NPN TERMINOLOGY)

- SNPN standalone: The combination of a PLMN ID and Network identifier (NID) identifies an SNPN. Hence, UE is configured with a PLMN ID and NID to access a SNPN. The NID could be self-assigned by individual SNPN or coordinated assigned [8]. The PLMN ID may be a private network ID (e.g. based on mobile country code (MCC) 999 as assigned by ITU1 for 3GPP), or the ID of a public PLMN that is operating that SNPN.
- SNPN with Shared RAN (see further down below for details): The UE is configured with both PLMN ID and NID. The UE can move from SNPN to PLMN connection and vice versa. In that case the UE needs to register with the new network. To connect to SNPN, the UE will listen to the IDs (PLMN ID + NIDs) broadcasted by the NG-RAN.
  - Note that emergency services are not supported in SNPN. The UE must be connected to the PLMN to use a emergency service.
- PNI-NPN: UE must have a subscription for a PLMN in order to access PNI-NPN. Hence, PLMN ID is used to access a specific PNI-NPN. Closed Access Group (CAG) could be optionally used to prevent the UE from trying to access some parts of the network. When PNI-NPN is delivered by the network slicing, a UE may be preconfigured with Single Network Slice Selection Assistance Information (S-NSSAI) to access certain slices.

NPN DEPLOYMENT – CORE NETWORK OPTIONS



NPN deployment example case



References

References

- Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 36.300
- Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification 36.331
- 3GPP TS 24.301; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
- 3GPP TS 38.300; NR; NR and NG-RAN Overall description; Stage-2
- 3GPP TS 38.331 NR; Radio Resource Control (RRC); Protocol specification
- 3GPP TS 38.304; NR; User Equipment (UE) procedures in idle mode and in RRC Inactive state
- 3GPP TS 24.501; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3

References

- Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP) 36.413
- 3GPP system - fixed broadband access network interworking; Stage 2 TS 23.139
- Evolved Universal Terrestrial Radio Access (E-UTRA); Mobility enhancements in heterogeneous networks 36.839
- Scenarios and requirements for small cell enhancements for E-UTRA and E-UTRAN 36.932
- Study on Small Cell enhancements for E-UTRA and E-UTRAN; Higher layer aspects 36.842
- Study on further enhancements of small cell high layer aspects for LTE 36.876
- Small cell enhancements for E-UTRA and E-UTRAN - Physical layer aspects 36.872

References

- Security of Home Node B (HNB) / Home evolved Node B (HeNB) 33.320
- Numbering, addressing and identification 23.003
- RP-142283: "New Study Item proposal: Study on further enhancement of small Cell high layer aspects for LTE", Contribution to 3GPP TSG-RAN meeting #66.
- R3-150538: "Consideration on UE associated signalling reduction", Contribution to RAN3 meeting #87bis.
- R3-151059: "S1 Signalling load for indoor scenarios", Contribution to RAN3 meeting #88.
- R3-151060: "S1 Signalling load for outdoor scenarios", Contribution to RAN3 meeting #88.
- R3-150345: "LS on Paging Optimization", Incoming LS from SA2 to RAN3 meeting #87.