Mobile Device Management and Operation in Enterprise Neutral Host CBRS Networks

August 2021

celona

Contents

Overview of Neutral Host

In any type of wireless network there is a need for ubiquitous coverage and high throughput connectivity. Unfortunately, wireless networks often lack seamless mobile coverage, and poor user experience is common in many indoor venues. New CBRS systems can help with this problem, but coverage problems can still remain. A wide variation of indoor venue environments (for campuses in general) require flexible installation and customization to provide full coverage. However customization of traditional indoor cellular systems is typically too costly and complex for enterprise deployment at smaller venues. Consequently, there is large gap between the top end of the indoor cellular market directly served by Service Providers (SPs) and hundreds of thousands of smaller, low-traffic ("mid-market") venues. This creates an opportunity for wireless networks that 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. This dilemma has opened the door for low-cost solutions that remove complex business models associated with the multi-operator cellular support.

Despite the significant enhancements with LTE, good and reliably indoor coverage has has illuded many enterprises. This is primarily due to RF signal penetration indoor using macro cell. And the variability of signals based on the material used for the building construction.

Distributed Antenna Systems (DAS) solutions are a popular and potential solution but are often cost prohibitive for the enterprise. DAS solutions require dedicated cabling and are restricted to addressing coverage for a specific MNO. In contract CBRS LTE, and soon 5G, networks can provide for a seamless way to not only support enterprise managed devices, but also a myriad of BYOD and vistor/customer devices.

CBRS networks that can accommodate users with subscriptions from different operators treating, these networks to be same as their home network, are considered to be a neutral host network (NHN). The subscriptions can belong to a macro network operator (MNO), a Multiple System Operator (MSO), Mobile Virtual Network Operator (MVNO) or, a private enterprise Network operator. CBRS LTE Enterprise Networks can be enabled to act as a NHN. The home network operators that allow for connectivity into the neutral host networks are called Participating Service Providers (PsPs).

The fundamental concept of a neutral host is sharing of deployed network components. Network sharing is enabled through passive methods such as sharing the campus, tower, rooftop, power, cabinets, lighting, and air conditioning. Active sharing of the network involves dynamic realtime sharing of antennas, access networks, transmission, spectrum, RF design, planning, and core network functions.

One of the key aspects that allows for network sharing to occur is the use of unlicensced spectrum. The FCC recently opened the CBRS band (Band 48) to the public defining specific procedures for how to acquire part of the spectrum for localized use. Given this spectrum can be used by any of the network operators, both public and private, this creates a unique ecosystem of end user devices and networks that can support offload. Offloading traffic to the NHN based on the business agreement can help accommodate immediate transitions or as a means to extend coverage when the footprint for the home network operator is poor or non-existent. The NHNs can be used for offload for load balancing under congested scenarios.

Current Indoor Solutions

A Dual-SIM NHN is based on an approach having two independent credentials: one with the home operator network and other with the enterprise network. The typical behavior is to support data and voice traffic on the enterprise network independently at different transition points. Data offload is supported with the enterprise credential while voice traffic is retained with the home operator network. When the user equipment (UE) is in the home operator network-only coverage, both data and voice is supported on the MNO's network. When the UE is in the coverage area of both the home operator network and the enterprise network, data is offloaded to the enterprise network while retaining the voice service over the MNO. When the UE is only in the enterprise network coverage (i.e. no MNO footprint), data is offloaded with the enterprise credential and the voice connectivity is supported by tunneling connections to the home operator network over the internet. This last option allows for treating the CBRS network as a trusted Non-3GPP access with the VoIP service supported as 'LTE calling'.

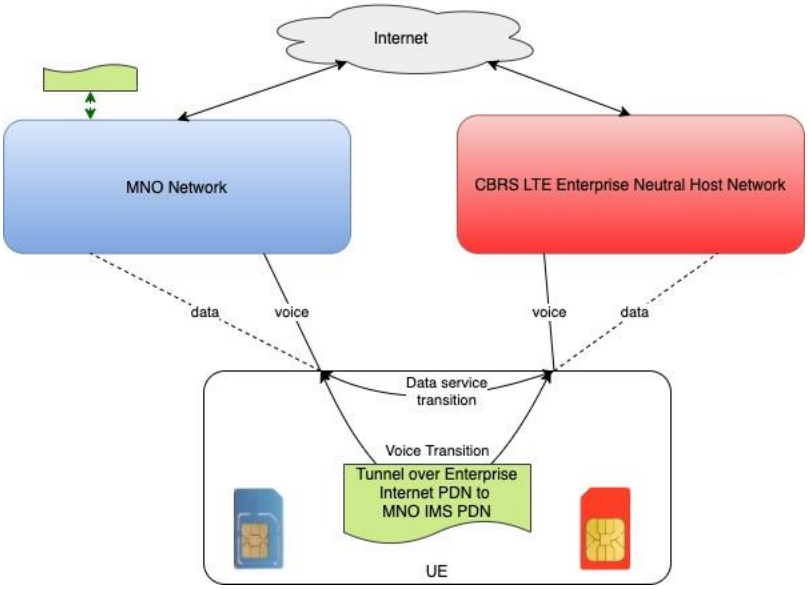

Figure 1 : Dual-SIM NHN

Distributed Antenna System (DAS) – This deployment of NHN is enabled by splitting the transmitted power among several antenna elements, separated in space so as to provide coverage over the same area as a single antenna but with reduced total power and improved reliability. DAS systems can be used for both indoor and outdoor deployments, although they are typically employed for indoor coverage extension. This requires dedicated radio heads and dedicated connectivity to the E node B (eNB) channels card for connectivity, making it a very high priced solution. Functionally, this can be envisioned as a specific variant of MORAN NHN.

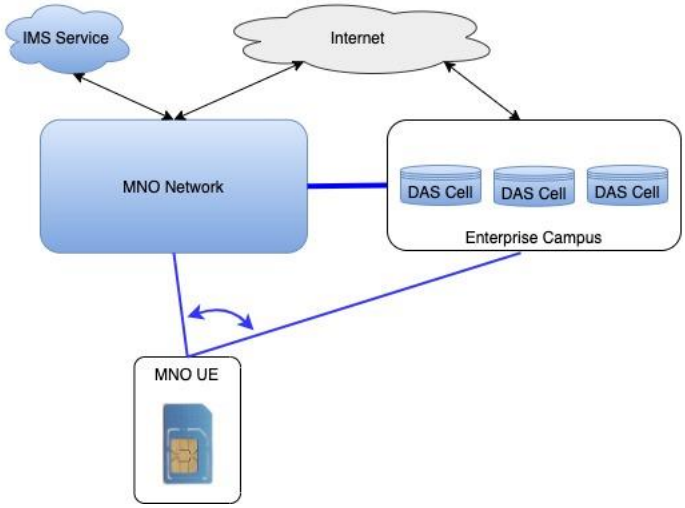

Figure 2 : Distributed Antenna System (DAS) based NHN

Multiple-Operator Radio Access Network (MORAN) – This deployment of NHN shares some elements of the radio access network (RAN), but with each home network operator running on a different channel. The nodes behind the RAN are independently managed by the individual home operators. Given that each MNO requires an independent channel, this is not an effective use of the available capacity with rigid channel partitions. This model is typically not widely employed in the market.

Neutral Host Opportunity

There are several compelling aspects driving the use of a neutral host, and much of it stems from the need for ubiquitous coverage and high throughput connectivity:

- Lack of seamless mobile coverage and poor user experience is common in many indoor venues,

- Costly and comple indoor cellular systems that are too cumbersome for 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,
- A growing need for a Neutral Host Network (NHN) operator, which is a Managed Service Provider (MSP), 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, and
- The need for a low-cost solution that removes complex business models associated with the multi-operator support

Figure 3 : Enterprise NHN Opportunity

The goal of neutral host service is to enable seamless roaming between cellular 4G LTE and 5G NR mobile devices (UEs) to enterprise CBRS networks for data and voice services. For this purpose, one set of devices of interest are those provided by enterprise network managers to employees and users. Another set of devices are personal cellular devices which are typically serviced by MNOs such as devices used by visitors or guests that come into enterprise or BYOD for enterprise employees) (referred as MNO UEs). There are two scenarios of interest for roaming between Enterprise Network and MNO network:

- Enterprise UE → access to MNO WAN
- MNO UE → access to Enterprise Network

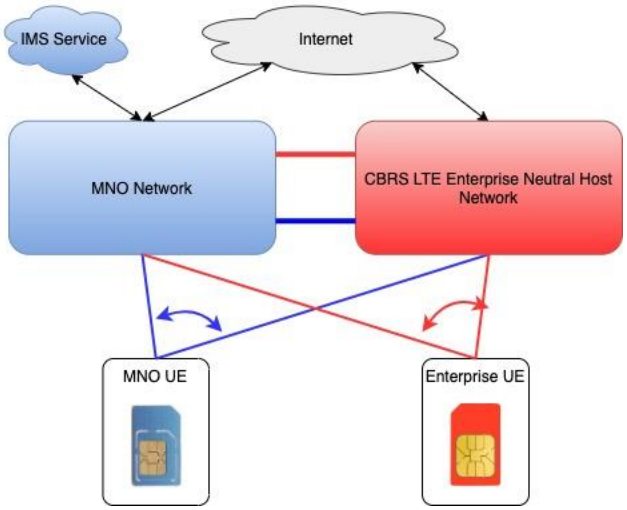

Figure 4 : MNO and Enterprise UE transitioning across Enterprise and MNO networks

Enterprise Network Deployment Variants

Enterprise LTE networks are typically deployed and managed by enterprise IT. The installation and administration of these networks need to be mimic the ease of a Wi-Fi while retaining the functionality and operations of a macro network. The deployed networks can be used for enterprise connectivity (private networks), for MNO connectivity (neutral hosts), or can be used for both enterprise and MNO connectivity.

Private Enterprise Networks

Private enterprise networks are deployed, operated, and managed by the enterprise-IT. The subscriptions and access to the network is regulated by the enterprise-IT. The UEs operating on the private enterprise network are typically identified, configured, and issued to users and referred to as CYOD (choose your own device). The enterprise-IT, defined campus policies may also allow for individual users to BYOD (bring your own device) and supply the required credentials to associate to the network.

As with any cellular 3GPP networks, specific identifiers are needed for the UE to find and associate with the enterprise network. MNOs typically have specific geographic footprints along with their unique identifiers for their service. Given enterprise deployments are typically within small areas (as compared to MNOs), common identifiers are used and the address spaces for the identifiers are shared amongst the entities deploying these campus networks.

Neutral Host Enterprise Networks

A private cellular network can be enhanced to enable neutral host functionality. Of the network sharing methods outlined, the approaches of traditional roaming, MOCN, and Dual-SIM NHNs are the most likely solutions that will be adopted by the market.

As mentioned earlier, the Dual-SIM NHN a supports data offload using enterprise credentials and retains the voice service on the MNO through either direct MNO radio connectivity or through a VPN tunnel routed as ‘LTE calling’.

Based on the established business partnerships with the MNO, the enterprise system will broadcast the home operator system information, or the operator(s) that have roaming agreements with the home operator. The LTE access points allow for the enterprise subscribers and the MNO subscribers to camp on the system, broadcasting the system identifiers of both enterprise network PLMN ID and MNO network PLMN ID. Up to six PLMN IDs can be transmitted from the access points, allowing for the system to act as neutral host

for the broadcasted PLMN IDs. As a result, the enterprise network functions as a NHN, typically behaving as both a private network and as a neutral host.

Network sharing and NHN realizations

At a minimum, the sharing of the neutral host network requires connectivity to the home operator network to authenticate the credentials of the user and/or device. There are different architectures of network sharing that are defined by the standards bodies.

Traditional Roaming based NHN – A standard 3GPP roaming mechanism build in the UE functions is used to transition to the NHN and will typically occur when the home network operator (MNO) has poor or no coverage in the region where the NHN is deployed. The NHN network will broadcast the system identifiers of the home network on its network so that the UE see this NHN as the home system to which it can initiate access. When the NHN does not transmit the home network system identifiers, but the UE has this system information included in its PLMN list, the UE will treat this as a roaming network and not see it as a typical home network system. For both of the above scenarios, the NHN network is utilized only when the home operator network does not have coverage and may not be a good user experience.

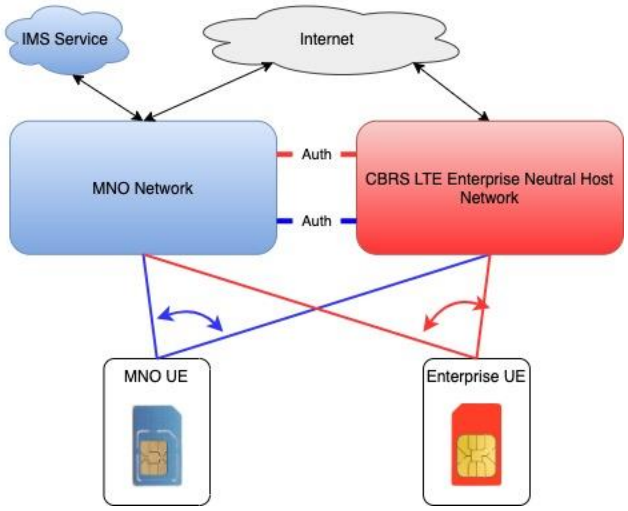

Figure 5 : Traditional Roaming based NHN

Multiple-Operator Core Network (MOCN) NHN – This deployment of NHN is supported using a single eNB that broadcast the system information of all the MNOs that allow for their UEs to camp o this system.

The eNB is connected to the individual home operator's core network through a Multi-Operator Core Network Gateway (MOCN GW). The control signaling interface is aggregated at the MOCN GW while user plane traffic is routed directly to the individual eNBs deployed on campus. The MOCN GW acts as the Mobility Management Entity (MME) to the eNBs, while the MOCN GW itself acts as an eNB to the home operator network MME. This architecture allows f maximum flexibility for the load balancing of radio resources to accommodate multiple MNOs while retaining the control for access and operation of a given UE with the home operator core network. This approach also suffers from the same issue of UE transitioning to the NHN only when there is no coverage of the home operator network.

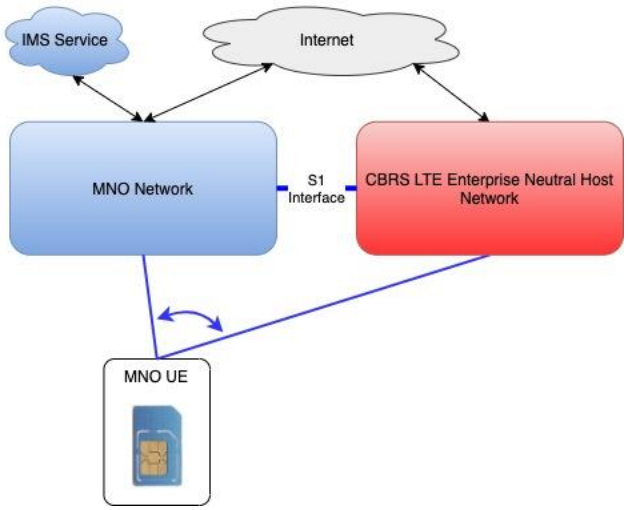

Figure 6 : Multiple-Operator Core Network (MOCN) NHN

Connectivity options between enterprise NHNs and MNO core networks

S1-C / S1-U Interfaces based connectivity. With this option, traffic is separated at the CBSD and routed to the MNO network. Enterprise deployed eNBs are connected via secure tunnels to the participating MNOs.

The S1 interface has two parts : An S1-C interface is used for control signaling and an S1-U is used for exchanging user plane / data traffic. S1 aggregator support may be required via IPX between the CBRS enterprise networks and MNO. Only the RAN aspects are supported from the enterprise network and all the core network functions are supported directly from the MNO network.

The routing of the traffic between enterprise-deployed eNBs and the MNO core network is supported through a MOCN GW (Multi-Operator Core Network). The MOCN GW appears to the MNO LTE packet core to the enterprise eNB. The MOCN GW appears to the eNB as the MNO LTE packet core. The MOCN GW serves as a concentrator for the control plane and accommodates connectivity to multiple MNO core networks. The S1-U interface from the eNB may be terminated at the MOCN GW, or a direct logical user plane connection between eNB and the MNO LTE packet core. The latter is the preferred option to enable direct packet routing to the enterprise-deployed eNB from the MNO LTE packet core.

This approach is emerging as the preffered approach to interconnect enterprise NHNs with the MNO networks.

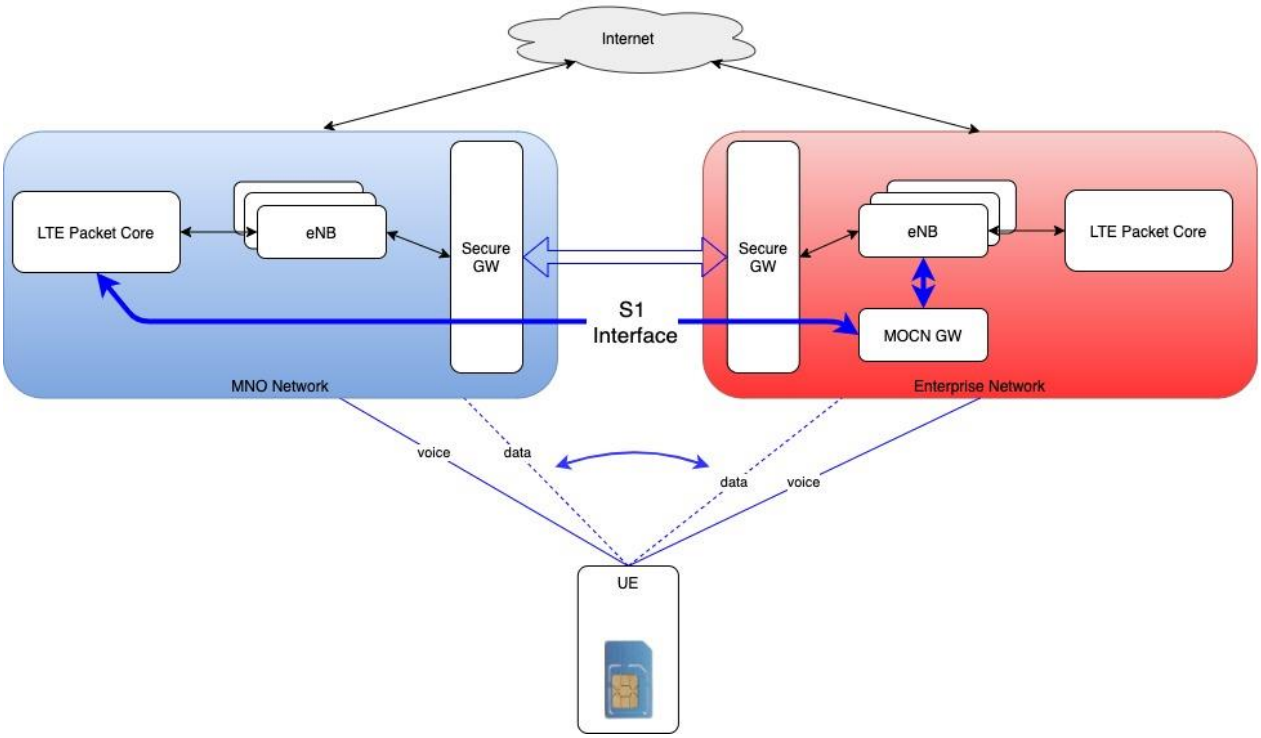

Figure 7 : S1-C / S1-U Interfaces based connectivity

S6a / S8 Interfaces based connectivity: MME (Mobility Management Entity) and SGW (Serving Gateway) functions are hosted within the enterprise LTE packet core network. The UE exchanges control traffic with the MME to be authenticated and obtains an IP address. User plane data traffic is routed through the SGW. S6a interfacing to the MNO-HSS (Home Subscriber Server) supports user authentication; S8 interfacing to the MNO-PGW (Packet Gateway) to assigns the IP address to the user and supports the routing of user plane traffic.

This option is not the prevailing approach to connect the enterprise NHN with the MNO networks.

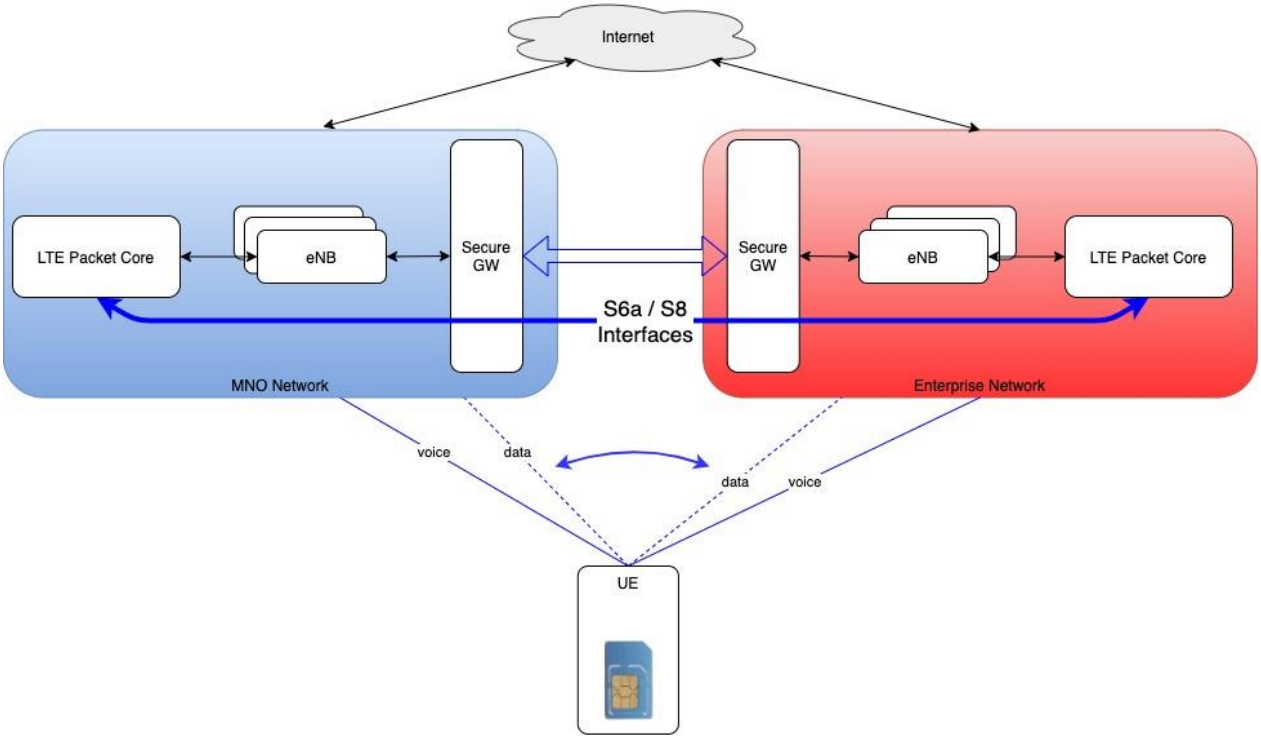

Figure 8 : S6a / S8 Interfaces based connectivity

Based on market requirements, a NHN may need to allow for supporting both S1-C / S1-U and S6a / S8 Interfaces. However, current market trends indicate that the interwork of the enterprise NHN and MNO core is satisfied with the S1 interface implementation.

MOCN GW deployment

To enable a CBRS private LTE network to a NHN, the MOCN GW function is added to the network. Indoor eNBs deployed in the enterprise campus are typically two sector eNBs (see Figure 9). This equally extends to an outdoor eNB. The MOCN GW functions as an aggregator for an enterprise campus acting as the LTE core for enterprise deployed eNBs and as a single eNB to the MNO core representing the entire campus deployment.

MOCN GW functions

The MOCN GW supports the following functions to enable the abstraction of the enterprise campus to the MNO core:

- Secure tunnels from eNB (Enterprise, MNOs)
- Control S1-C aggregation
- Optional user plane S1-U aggregation (this is not the preferred configuration to avoid unnecessary packet processing)
- Enterprise eNB IP address mapping for packet routing from MNO core
- MNO selection based on the UE's association with the enterprise network
- Relaying of the WEA messages received from an MNO MME for broadcast (messaging carried on S1-AP)
- In campus mobility of the UE across enterprise deployed eNBs

The two sector eNB will be visible as a single eNB to the MOCN GW and MNO MME. A single S1 will be established between two sector eNB and MOCN GW. CSO will configure the sectors with independent eNB IDs. E node B devices receive all configuration as part of Bootstrap resolving the IP address assignment for the eNB. THe eNB itself is agnostic to MOCN GW and simply treats it as another LTE packet core network. The sectors within the eNB are seen as a single eNB by the MOCN GW and the MNO core network with the UE mobility between the sectors managed directly by a given eNB. The over-the-air broadcasts will use independent eNB IDs and will be seen as independent cells by the UE. Supporting the UE for downlink and uplink channel assignment across the two sectors is handled within the eNB.

MOCN GW is a run as a Kubernetes service and inherits the high availability characteristics of a container-based solution. Upon eNB power up, the required PLMNs

support is identified. When the eNB associates with the MOCN GW, the MOCN GW initiates connectivity to the required set of PLMNs.

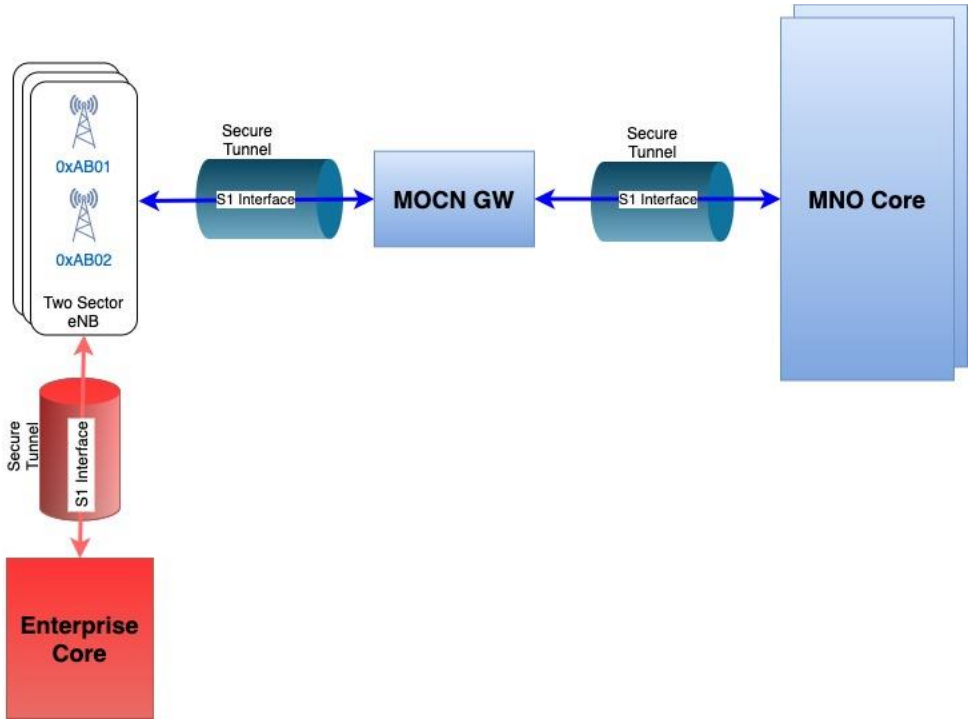

Figure 9 : Extending a CBRS LTE private network as NHN with MOCN GW

S1 connectivity establishment with MOCN GW / MNO core

The S1 interface between the MOCN GW and the MNO core is established on an MNO basis. Individual MNO core connectivity failures are treated independently.

Hearbeat keep-alive messages between the eNB and MOCN GW and from the MNOC GW and MNO core are done perodically to detect connectivity failures. MNO core connectivity failures are propagated to the enterprise eNBs and the failed PLMNs will not be broadcast from the eNB. From a connectivity perspective, the S1 interface between the enterprise deployed eNB and MOCN GW remains independent from the failure of the S1 interface connectivity between the MOCN GW and MNO MME.

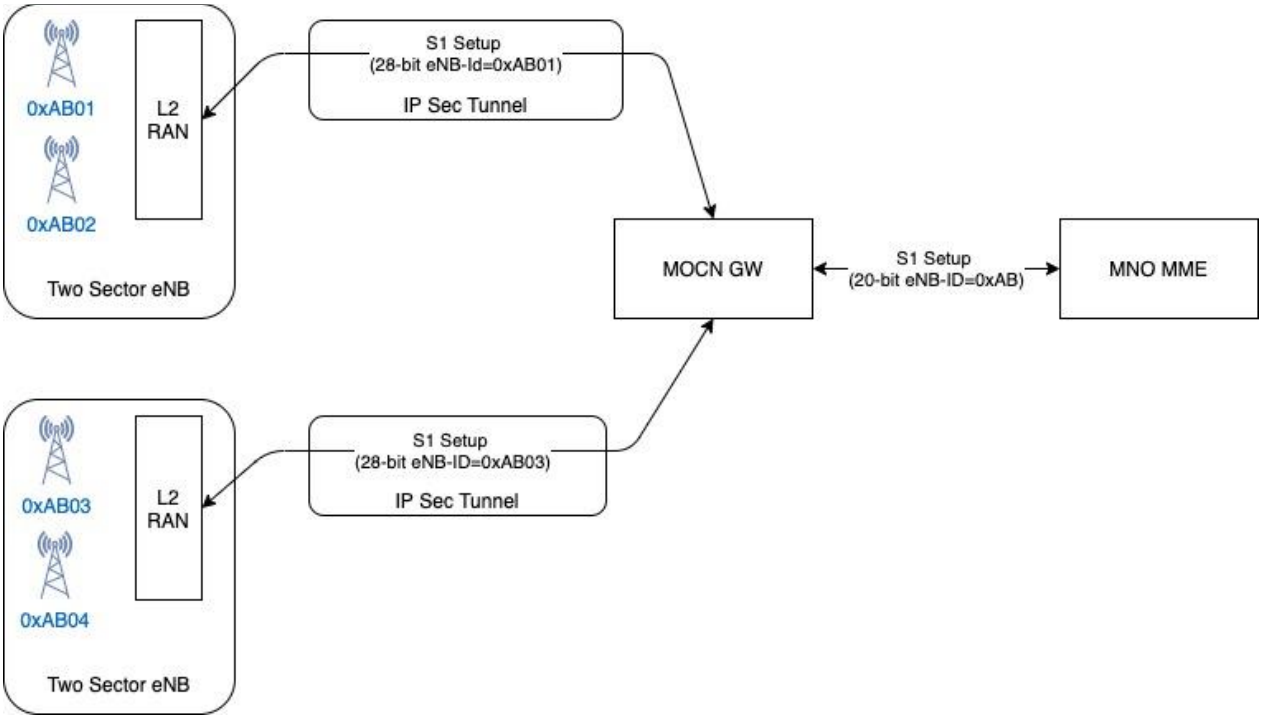

Figure 10 : S1 Connectivity Establishment with MOCN GW

UE Attach procedure upon entering enterprise campus

Independent from which sector of the two-sector-eNB to which the UE associates, a single eNB ID (one of the two eNB IDs) is used to establish the UE context with the MOCN GW and the hence the MNO core. From MOCN GW and MNO core UE will be assumed to be camped on one of the single selected eNB IDs. Paging the UE and UE Access procedures are always managed from one of the two sectors. In connected mode, the eNB supports carrier-aggregation across the two sectors for DL traffic and selects one of the two sectors for UL traffic.

It is expected that the footprint of coverage of the two sectors will overlap. For LBS services, the UE reports measurements from both sectors independently to the MNO core (E-SMLC in particular) for location determination. Trilateration procedures adapt according to the measurement information received from the UE on the individual sectors.

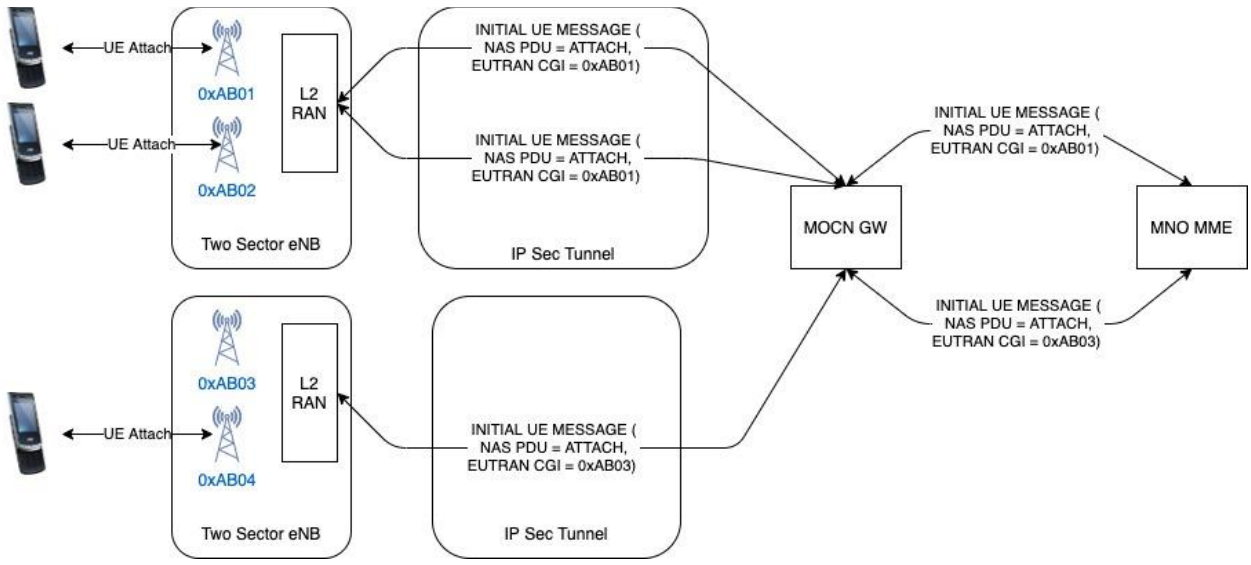

Figure 11 : UE Attach with MOCN GW

In campus mobility

Both idle and connected mobility follows the same procedures are with any macro networks. Idle mode is supported through the cell-reselection procedure using the neighbor information and the transitioning parameters broadcastfrom the eNB. For connected mode, the handover procedure is either handled as S1 interface-based transitions or employ X2GW based transitions across the eNBs. X2 is the inter-eNB interface across access points supported on enterprise campus. The X2GW allows for routing control and user plane traffic between eNBs so UE context can be transitioned from the source eNB to the target eNB for mobility with loss-less transitions. Similar functions can be performed using the S1 interface and using the MOCN GW to execute the transitions. Figure 12 shows a high-level view of the in-campus mobility with the MOCN-GW and X2GW and the support of the secure tunnels involved. Based on the specific deployment, it is possible for the MOCN-GW and X2GW to be located on independent nodes with the traffic routing and the secure tunnels establishment altered accordingly.

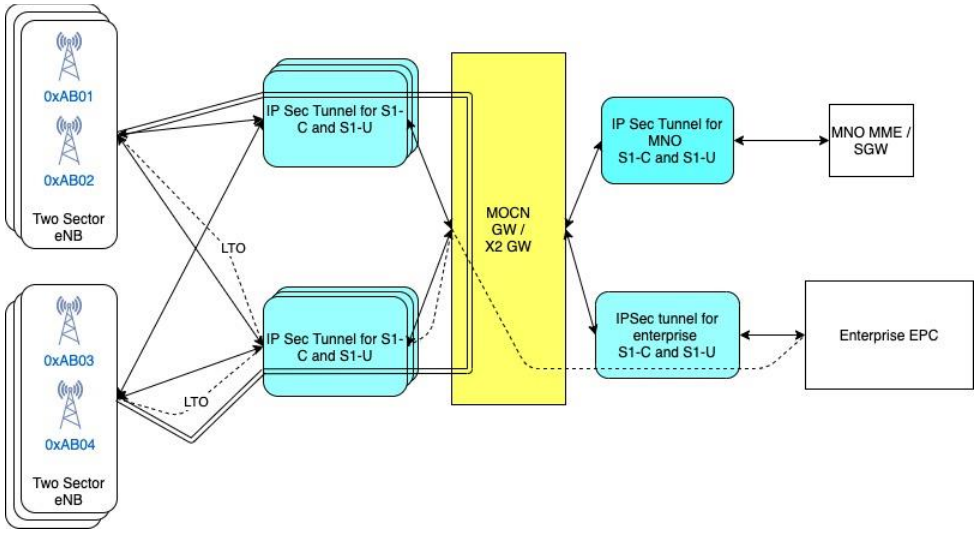

Figure 12: In campus mobility with MOCN-GW & X2GW

UE connectivity to NHN with BYOD, CYOD, COPE

Enabling enterprise campus connectivity requires the IT to plan the devices to support and the manage their access and security postures. The choice(s) will dictate the extent of control the enterprise IT has on the devices as well as the costs incurred for supporting the device population. Some form of device protection is needed. Integration with enterprise mobility management (EMM) and mobile device management (MDM) is also required. Apart from CYOD and COPE devices, BYOD with NHN roaming and dual-SIM support needs to be supported. Even with CYOD & COPE, MNO credentials apart from enterprise credentials must be supported. The involved tradeoffs with the device types are discussed below.

TOPIC	**BYOD**	**CYOD**	**COPE**
Expansion	Bring your own device	Choose your own device	Corporate-owned, personally-enabled
Devices provided by	Employee	Enterprise provides a set of pre-approved mobile devices; Some flexibility for user to choose amongst approved devices	Enterprise
Device management	Optional based on enterprise. Regulated by the user installing an agent / application on the device	Configured with security protocols and business applications before assigning device to employee	Enterprises have the most control on these devices, they can be regulated for specific types of access and even lock down the devices as needed

Device maintenance	Employee	Enterprise policy dependent – can be shared responsibility between enterprise and employee	Owned, maintained, and managed by the enterprise
Security policy	Managed by employee	Managed by enterprise. With restricted set of devices, the security feature are installed prior to assigning to user	Devices are pre-configure to maintain device and data security
Costs	Device and data connectivity managed by the employee	Partly managed by the enterprise and the employee	Wholly managed by the enterprise
Comfort of device use	Employee choice and hence most compatible to user preferences	Can be restrictive based on the device choices made available by the enterprise	Most restrictive given that the enterprise assigns device of their choice to each employee; Employees still provided the option to customize their device and potentially use it for non-work related functions

Table 1: BYOD, CYOD, COPE tradeoffs

UE UE roaming behaviors

Figure 13 below shows a high level steps for UE and network sequence of steps involved in UE entering and leaving a Enterprise Network.

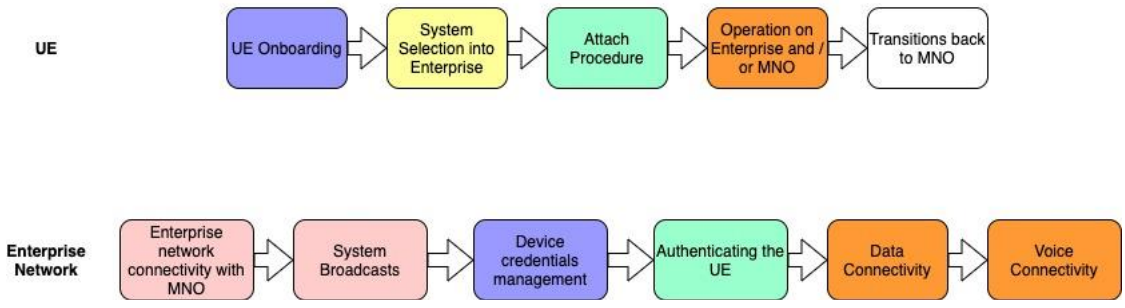

Figure 13 : UE and network sequence of activities for NH operation

UE entering the enterprise network

With single SIM credential

Idle mode transitions : The MNO PLMN is broadcast on the enterprise network for it to be treated as an NHN for the MNO. Multiple MNOs PLMNs may be broadcast on the enterprise network. UE finds the enterprise network when the UE is out of coverage on the MNO macro network footprint. Out-of-service based scanning with telescopic backoff is employed by the UE to detect available networks include macro and enterprise network deployment.

A manual scan of available systems when requested by the user enables the UE to look for all available networks and systems that the UE radio can support. The found PLMNs are presented to the user. This includes the MNO PLMN broadcasted by the NHN. The user selects PLMNs presented enabling the UE to associate with the NHN.

Connected mode transitions : Connected mode offload to enterprise networks can be useful. This likely to be employed only when the enterprise network is also deployed by the MNO. The connection to be wholly moved to the enterprise system with the core network and services supported from the MNO core network.

With dual SIM credential

Idle mode transitions : The UE has policies specified when to scan for the enterprise network typically driven from the HLOS. This can be based on periodic scans or per other radio and geographic signatures to initiate scans. UE offloads the data traffic on to the enterprise network while retaining the voice service on the MNO network.

When the MNO footprint is no longer available, the UE uses Wi-Fi calling (WFC) methods to connect to the MNO core network via an IPsec tunnel established over the data connectivity on the enterprise network. These are make-before-break transitions, however the session continutity is maintained with potentially some perceptible interruptions in service.

It is possible for the UE to be associated with the enterprise NHN with data connectivity supported with enterprise credentials and voice calling supported with MNO credentials. The UE is camped on the same eNB on the enterprise NHN supporting associations with both enterprise and MNO credentials for DSDS (dual-SIM dual-Standby) operation.

Connected mode transitions : Supporting DSDS operation with the same eNB on NHN with tight interworking with the MNO network, it is possible for the UE to be transitioned to the enterprise network in connected mode retaining continuity of service.

UE leaving the enterprise network

With single SIM credential

Idle mode transitions : UE transitioning out of the enterprise network is typically handled through idle mobility when the leaving campus coverage. When the UE is in connected mode on the enterprise network, it loses the RRC connection and transitions the connectivity on to the MNO network. Such transitions will be a break-before-make transitions.

Connected mode transitions : For a voice call, when entering the enterprise campus, it is sufficient to continue the service on the MNO network as there typically MNO coverage available even if it may be in weak coverage. Given the smaller size of the enterprise footprint, when leaving the campus network, it is important to support call continuity from enterprise to the macro network. This transition can be done with tight integration between the enterprise and MNO networks supporting measurement procedure of the MNO pilots and performing transitioning of the data traffic context from the enterprise network to the MNO network. This requires PDN connectivity and potentially L2 level context to be transitioned from enterprise the MNO network while ensuring minimal loss of packets during the transition. This feature is typically not enabled in the field.

With dual SIM credential

Idle mode transitions : UE transitioning out of the enterprise network is typically handled through idle mobility when the leaving campus coverage. When the UE is in connected mode on the enterprise network, the UE loses the RRC connection and transitions the connectivity on to the MNO network. Such transitions will be a break-before-make transitions and will apply for both data and voice traffic independent of the credential that is used for individual services.

Connected mode transitions : With data connectivity supported with enterprise credentials, the UE will always be a break-before-make. The UE transitions the data services to the MNO credentials when transitioning to the MNO network.

With DSDS camping on the NHN with both enterprise and MNO credentials on the enterprise eNB, transitioning active voice calls from enterprise network to the MNO network may be required. Roaming is possible when there is tight integration between the NHN and MNO networks. However, this feature is typically not employed and likely idle transitions with some perceptible breaks in service is employed.

Services support on enterprise campus networks

As the UE transitions across the MNO and enterprise networks, it offloads specific services on the enterprise network while still being associated with the MNO networks for other services. The transition points for the different services may occur at independent points based on the relative prioritization and the RF footprint of the two networks.

Figure 14 below provides a high-level view of the different transitions across MNO and enterprise networks and the available options for data and voice traffic offload. The specific options are available based on the subscriptions supported in the UE : MNO only or MNO and enterprise subscriptions.

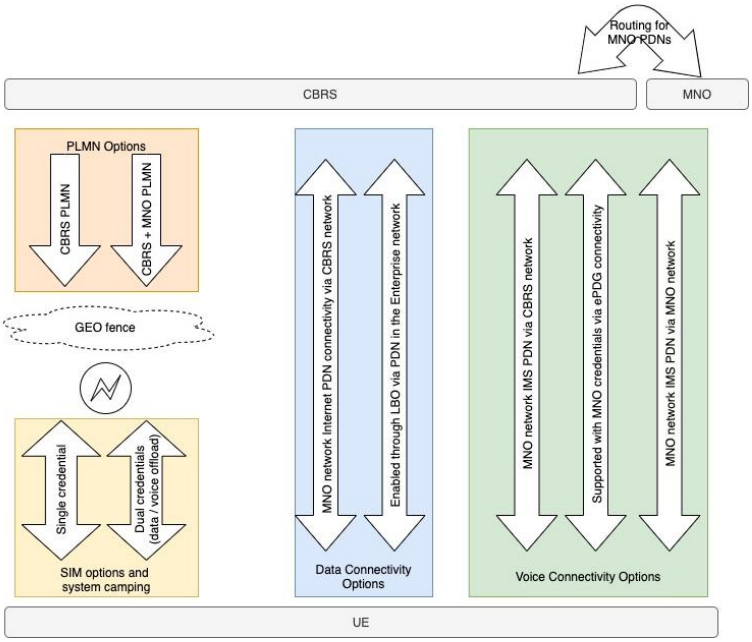

Figure 14: UE transitions into CBRS Enterprise Network

With single-SIM MNO credentials : The NHN network transmits the MNO PLMN. The UE based on moving out of macro MNO network coverage, geofenced scans, or through manual scans, the UEfinds the enterprise NHN network. The data and voice connectivity are offloaded to the enterprise NHN network with the IP termination points in the MNO core network and with the radio access point connectivity provided from the enterprise network.

With dual-SIM MNO and enterprise credentials : The UE transitions the data connectivity to the enterprise network while retaining the voice services over the MNO network.

When the UE loses macro MNO network connectivity, it also transitions voice services to the enterprise network. With enterprise NHN support, the UE transitions to using DSDS support on the enterprise eNB. When enterprise does not have NHN support, the voice service is supported as a tunneled connection to the MNO core over the enterprise LTE data connectivity – 'LTE calling'. This is similar to 'Wi-Fi calling' feature with QoS support for voice service over the enterprise LTE network.

Emergency calling

Emergency calls are supported as VoLTE calls. The key added requirement is location support of the UE. Enterprise deployed eNBs location information is populated into the MNO networks E-SMLC (Evolved Serving Mobile Location Center) database. The SUPL (Secure User Plane Location) protocol between the E-SMLC and the UE, executed in-band treating the enterprise network as a passthrough, is executed with measurements reports from the UE to determine UE location. Moving forward vertical positioning is also required within a three meter accuracy–becoming very important for enterprise deployments with indoor coverage. With enterprise deployments, it is sufficient to locate the UE on a cell for both horizontal and vertical position with indoor eNB. With outdoor eNB, trilateration can be performed with the UE measurement of the surrounding cells. Alternative methods of positioning with WLAN technologies of Wi-Fi and Bluetooth® and potentially the UE reporting altitude information can be used for vertical positioning. For instance, Android supports advanced positioning algorithms with ELS service support that is leveraged for emergency positioning as well.

Other MNO services

There are specific services that currently are supported over the MNO that do not transition directly to the enterprise network. The MNO networks have service level agreements (SLAs) with content providers and specific services enabled through them with third parties. One possible approach is to obtain similar agreements for the enterprise network and support the service over the RAN or/and the core of the enterprise network. The more immediate approach will be to have the UE transition to the MNO macro network to support these services. This is a UE based function to transition when such services are enabled by the user.

A good example of such a service is eMBMS or broadcast and multicast service. The information carried on this channel is based on operator agreements with the content providers and will be carried on the MNO frequencies. When the user enables the application to monitor the service, the UE transitions to the MNO frequency to receive this service. Given that the enterprise network does not broadcast information associated with the eMBMS on the MNO frequencies, when the user activates the application, the UE needs to transition to the MNO frequencies to even check if the MNO coverage is available

and if the service is active on the channel. When there is no MNO coverage or the service is not active, the UE transition back to the enterprise network as part of the regular procedures of finding the campus network.

Enterprise local services for NHN UEs

When the UEs with MNO subscription are camped on the enterprise NHN network, all traffic is routed to the MNO core. To enable access to enterprise local services, traffic separation handled by an explicit LTO function (Local Traffic Offload). This entity can be supported as an independent function or integrated into exiting deployed components.

With S1 interface style NHN interworking, all traffic is routed to the home network. The exception for this is specific LTO support based on the filters configured in the router with the LTO either integrated into the eNB or in the path between the eNB and MOCN GW. With S6a/S8 style of NHN interworking, the LTO function is integrated with the LTE enterprise core network.

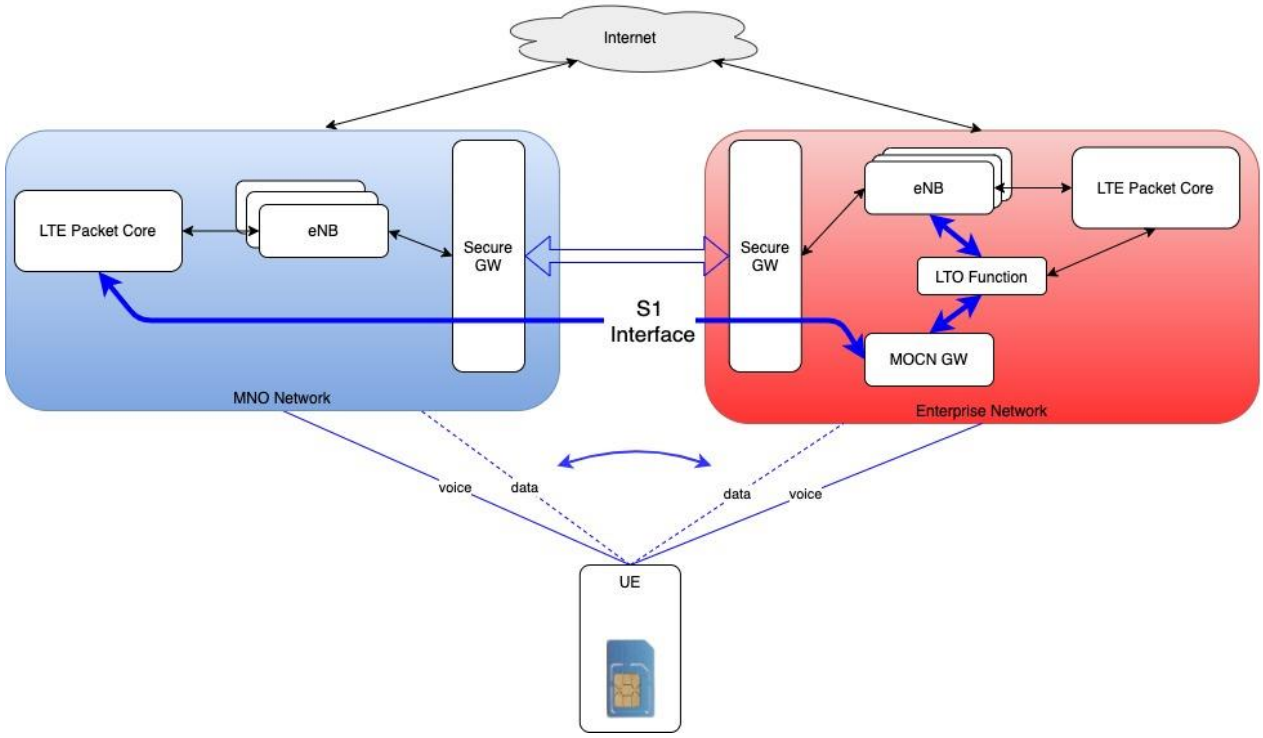

Figure 15: Enterprise local services for NHN UEs with S1 Interface