ATIS-I-0000073

Neutral Host Solutions for 5G Multi-Operator Deployments in Managed Spaces

Innovation to lower the cost of capacity and coverage for 5G and existing radio technologies.

Abstract

In a neutral host architecture, a shared wireless infrastructure is created which is used to provide services to end-users with subscriptions to several different hosted operators. Neutral host scenarios are particularly attractive in dense small cell deployments (as may be required for 5G mmWave service) which may require capital intensive buildouts and cumbersome backhaul and cell site infrastructure requirements. For example:

- Intercell distances for these deployments are in the order of 100's of feet. It may be impractically expensive for all mobile operators serving a specific area to fully deploy a dense small cell network in the same location or venue.
- In outdoor small cell deployments, local regulations may constrain how much infrastructure can be deployed. For example, there may only be physical space available for one antenna assembly at optimal small cell locations even though there may be many different operators interested in deploying in that location.
- Many indoor locations and venues are managed by a separate enterprise which may want to deploy their own small cell (e.g., Wi-Fi) network and may find it burdensome to work with and integrate access capabilities for the multiplicity of mobile/wireless operators that are serving the general area.

However, by utilizing a neutral host architecture, many different operators are able to share a common buildout provided by a neutral host provider.

Although neutral host architectures have been deployed with existing Wi-Fi and 4G technologies, the high performance promised by 5G mmWave access has sparked new interest in these architectures. With the introduction of 5G services and the system architecture evolution to Network Functions Virtualization/Software Defined Networking (NFV/SDN), the cost efficiencies of deploying 5G services may be leveraged by a neutral host service provider to provide tailored and differentiated services blended with services offered by Mobile Network Operators (MNOs) and to maintain continuity of these services within the coverage area of the neutral host.

A neutral host deployment can provide cost effective coverage and capacity for wireless environments such as dense metropolitan areas, enterprises, campuses, entertainment venues and shopping malls. This document assessment defines the neutral host concept and provides an overview of the technical solutions to support neutral host.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's business priorities. ATIS' 150 member companies are currently working to address 5G, cybersecurity, robocall mitigation, IoT, artificial intelligence-enabled networks, the all-IP transition, network functions virtualization, smart cities, emergency services, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle – from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user’s attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Copyright Information

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Table of Contents

Neutral Host Solutions for Multi-Operator Wireless Coverage in Managed Spaces

1 Scope, Purpose, & Application

Today, when deploying small cells within a managed space such as an enterprise office, a shopping mall, or a stadium, the landlord controls access to infrastructure. Visitors to the space will subscribe to many different wireless network providers. Thus, to get uniform cellular coverage for all employees, customers and guests, small cells from all major providers must be deployed in addition to Wi-Fi and other unlicensed access technologies.

Furthermore, 5G mmWave technologies will often be deployed in dense configurations to provide adequate coverage given the Radio Frequency (RF) propagation challenges in mmWave spectrum. Similar to managed space environments noted above, it is likely that all major providers will need to deploy in the same areas. Particularly in outdoor deployments, infrastructure and regulatory constraints may limit the number, and location of cell site placement.

These scenarios represent a high-cost and complex arrangement involving deployment of multiple infrastructures. A potentially more attractive arrangement is to have one common infrastructure system deployed that could be used by all service providers. Thus, a third-party provider (such as an independent access provider, a landlord, or delegate) becomes a neutral (not aligned with any specific provider) host for small cell coverage.

This paper examines and analyzes neutral host solutions assessing the technical and logistical implications.

2 Normative References

The following references contain provisions which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid.

[017 Market Drivers for Small Cells] Small Cell Forum SCF017.06.01, *Multi-operator market drivers*[1]

[22.261] 3GPP TS 22.261, *Service requirements for next generation new services and markets*[2]

[22.951] 3GPP TS 22.951, *Service aspects and requirements for network sharing*[3]

[23.251] 3GPP TS 23.251, *Network sharing; Architecture and functional description*[4]

[23.402] 3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses*[5]

[23.501] 3GPP TS 23.501, *System Architecture for the 5G System*[6]

[MulteFire] MulteFire Alliance[7]

---

[1] Available from the Small Cell Forum at: < http://scf.io/en/documents/017_-_R6_-_Multi-Operator_Market_Drivers.php >.

[2] Available from 3GPP at < http://www.3gpp.org/DynaReport/22261.htm >.

[3] Available from 3GPP at: < http://www.3gpp.org/DynaReport/22951.htm >.

[4] Available from 3GPP at: < http://www.3gpp.org/DynaReport/23251.htm >.

[5] Available from 3GPP at: < http://www.3gpp.org/DynaReport/23402.htm >.

[6] Available from 3GPP at < http://www.3gpp.org/DynaReport/23501.htm.>.

[7] See: < http://www.multefire.org/ >.

3 Acronyms & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3GPP	Third Generation Partnership Project
AP	Access Point
API	Application Programing Interface
ATIS	Alliance for Telecommunications Industry Solutions
CBRS	Citizens Broadcast Radio Service
CPRI	Common Public Radio Interface
CMSP	Commercial Mobile Service Provider
DAS	Distributed Antenna System
DDAS	Digital Distributed Antenna System
DL	Distributed Ledger
DLT	Distributed Ledger Technologies
eNB	eNode B (4G base station)
EPC	Enhanced Packet Core (4G)
ePDG	Evolved Packet Data Gateway (4G)
FAPI	Functional API
FCC	Federal Communications Commission
GAA	General Authorized Access
GERAN	GSM EDGE Radio Access Network
gNB	5G Node B (base station)
IMS	IP Multimedia Subsystem
ISM	Industrial, Scientific, and Medical
ISP	Internet Service Provider
KPI	Key Performance Indicators
LTE	Long Term Evolution
MAC	Media Access Control
MNO	Mobile Network Operator
MOCN	Multi Operator Core Network

M-SSID	Multi Service Set Identifier
MVNO	Mobile Virtual Network Operator
nFAPI	Network Functional Application Programing Interface
NFV	Network Functions Virtualization
NH	Neutral Host
O-DU	O-RAN Distributed Unit: a logical node hosting RLC/MAC/High-PHY layers based on a lower layer functional split.
O-RU	O-RAN Radio Unit: a logical node hosting Low-PHY layer and RF processing based on a lower layer functional split.
PAL	Priority Access License
PBX	Private Branch Exchange
PHY	Physical (protocol layer)
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RRH	Remote Radio Head
SAS	Spectrum Access System
SLA	Service Level Agreement
SON	Self-Optimized Network
SSID	Service Set Identifier
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
VoWi-Fi	Voice over Wi-Fi
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network

4 Introduction to Neutral Host

4.1 General Description of a Neutral Host

The term "neutral host" combines two concepts – the aspect of "hosting" and the aspect of "neutrality". The hosting aspect refers to an entity that provides a certain set of resources that are made available to clients such as mobile network operators in order to allow the hosted clients to provide continuous services. The resources that may be offered by a neutral host are addressed in the next section. The "neutrality" aspect refers to the host acting as a shared platform to multiple hosted clients. Neutrality in this context does not imply strict equality between hosted clients, as the resources offered to each hosted client are subject to commercial agreement between the neutral host and the hosted client, and policy-based management may be applied.

From a user's point of view, the system behavior and services using the resources of a neutral host should be available without user intervention and these should be seamless and identical to those provided by their hosted clients' dedicated resources. Because neutral hosting provides service equivalence to the user, it can be a viable alternative to conventional dedicated infrastructure.

4.2 Motivation and Market Need for Neutral Host Architectures

This document will specifically address neutral host architectures and scenarios where the neutral host entity provides access services to one or more client network operators. In these scenarios, a subscriber of a client network operator, upon entry into an area served by the neutral host, can receive access services from the neutral host as if the subscriber were directly connected to the client network. Service characteristics will be very similar to roaming and/or network sharing and indeed, many neutral host architectures leverage roaming or network sharing configurations. The primary difference is that the "visited network" is served by a business entity (the neutral host provider) that may not be a network operator. Neutral host business entities could include enterprises, venue owners or managers or other business entities/operators which may provide access infrastructure as a service.

Neutral host scenarios are well suited to small cell network deployments. Small Cell networks are currently deployed but present several challenges. For example:

- Dense small cell deployments (as may be required for 5G mmWave service) can be capital intensive to build out and maintain a backhaul and cell site infrastructure that may consist of 10's to 100's of nodes deployed in a relatively small area such as a downtown region, a venue or enterprise location. Quite often, intercell distances for these deployments are in the order of 100's of feet. It may be impractically expensive for all mobile operators serving a specific area to fully deploy a dense small cell network in the same location or venue.
- In outdoor small cell deployments, local regulations may constrain how much infrastructure can be deployed. For example, there may only be physical space available for one antenna assembly at optimal small cell locations even though there may be many different operators interested in deploying in that location.
- Many indoor locations and venues are managed by a separate enterprise which may want to deploy their own small cell (e.g., Wi-Fi) network and may find it burdensome to work with and integrate access capabilities for the multiplicity of mobile/wireless operators that are serving the general area.

These challenges can often be addressed through neutral host architectures where a single access entity builds and maintains the access infrastructure while allowing the subscribers of client networks to use this single access infrastructure transparently.

Although neutral host architectures have been deployed with existing Wi-Fi and 4G technologies, the high performance promised by 5G mmWave access has sparked new interest in these architectures. With the introduction of 5G services and the system architecture evolution to NFV/SDN, the cost efficiencies of deploying 5G services may be leveraged by a neutral host service provider to provide tailored and differentiated services blended with services offered by MNOs and to maintain continuity of these services within the coverage area of the neutral host. For example, a theme park may utilize a 5G architecture for tailored services, such as deep

AR/VR experiential services, and at the same time maintain continuity of broadband cellular services within the confines of the theme park.

In addition, new unlicensed and lightly licensed spectrum options are being developed that work effectively with Neutral host architectures.

In summary, neutral host architectures can provide coverage and capacity benefits with lower deployment and maintenance costs for client operators while enabling the neutral host entity to recover deployment costs by selling access to the client operators. Neutral host entities may also use their access infrastructure for their own business needs.

4.3 Definition of a Neutral Host

In the language of this report, neutral host is defined as the provider of a shared platform to hosted clients that require the following resources:

- Permanent Physical Equipment infrastructure: This refers to permanent (or quasi-permanent in the case of special events) structures and utility infrastructure needed to support the installation and operation of equipment. This could include:
    - Antenna towers, distribution systems, and/or other antenna mounting points.
    - AC/DC power and uninterruptable power equipment as needed.
    - Equipment racks or other locations to mount electronic equipment.
    - Signal cabling or optical fiber connectivity within the local environment (e.g., antenna feeders between antennas and equipment racks).
- Spectrum: This refers to mobile coverage as licensed (e.g., owned or leased/borrowed from hosted clients) or unlicensed.
- Antennas: This refers to physical antennas and associated equipment such as mast-head amplifiers as needed.
- Radio Access Network (RAN) edge nodes: This refers to the typical "base station" node such as 5G enabled Node B (gNB) base station, a 4G Long-Term Evolution (LTE) eNB (eNodeB), Wi-Fi access point or other radio technologies as appropriate.
- Optionally, all or parts of a mobile packet core providing common core support functions for the neutral host network.

The neutral host:

- Obtains use of the necessary resources in a specific geographic region (which could be within a building or a public space like a sports stadium or a distributed geographic area like a municipality’s streetlight poles);
- Manages these resources, subject to agreements with resource owners and clients; and
- Provides facilities and/or interconnection allowing hosted clients to make use of the platform(s) to provide continuous services to their end user customers.

The spectrum used by the neutral host may be licensed or unlicensed. In the case of licensed spectrum, it may be owned by the neutral host directly or may be obtained by the neutral host via an agreement with a licensed spectrum owner. The neutral host is active in managing the planning and utilization of the spectrum within its geographic area subject to agreement with the license holder, if any. Several hosted clients may share common spectrum, or individual hosted clients may use individual spectrum blocks.

Bearer and signaling interconnect are subject to agreement between the neutral host and the hosted clients.

4.4 Hosted Client

The hosted client (commonly a mobile service provider) is identified as the entity using all or a portion of the resources provided by the neutral host, possibly alongside other hosted clients, to bring services to their end users. The relationship between the neutral host and the hosted client will be governed by a commercial agreement including a technical Service Level Agreement (SLA).

The new 5G Core network provides new opportunities for both the hosted client and neutral host provider by enabling more flexible deployment of customized services. More detail regarding how the 5G core supports new capabilities in a neutral host environment will be covered in Section 5 of this document.

4.5 Requirements on Neutral Host from an End User Perspective

From an end user perspective, the provision of services by a neutral host should, ideally, appear identical to the provision of resources by the hosted client's dedicated resources. This implies that:

- The User Equipment (UEs) shall perform network selection and attachment according to the hosted client network's selection policy, and the policy of other stakeholders and user preferences. When the end user is in the area of the neutral host, according to the selection algorithm, the neutral host's coverage shall be selected seamlessly and without user intervention.
- Subject to business agreement and SLA, the services, including regulatory services, provided by the neutral host, should operate in a similar fashion to when in the hosted client's dedicated coverage.
- Mobility between dedicated and neutral host coverage should operate in a similar fashion to corresponding mobility events in dedicated networks.

Technical restrictions in neutral host solutions may prevent this ideal behavior from being realized. Limitations of particular solutions will be addressed in later sections.

On occasion, demand overload on the neutral host may mean it is not able to fulfill this ideal, and services have to be managed to maintain system operation. In this case, the neutral host shall apply a policy-based approach to manage the overload governed by the commercial agreement between the neutral host and the MNO.

4.6 Resource Management Within a Neutral Host

A neutral host offers resources that are shared by multiple end users that may belong to several hosted clients. As such, resources must be managed between users of one neutral host client, as well as between users belonging to different neutral host clients. This may be influenced by:

- The policy of one hosted client for its own end users.
- The SLAs agreed between the neutral host and the hosted clients, and how the neutral host implements that SLA in its policies.

The neutral host shall have the ability to:

- Obtain policy information from a hosted client in order to manage that client's end users.
- Define its own policies for management of resources, and particularly for how resources are partitioned between hosted clients.

4.7 Neutral Host Relationship to Hosted Clients

A number of points are important to consider in the context of the relationship between the neutral host and hosted client. These include:

- Confidentiality of sensitive information: The neutral host should provide role-based access controls to ensure different hosted clients are only able to access and control the resources assigned to them.
- Security: The solution should ensure that the hosted client's network security is comparable to that offered by individual hosted clients dedicated resources.
- Charging: The neutral host shall provide wholesale charging to the hosted client for usage of neutral host resources by that client's subscribers.
- Service level: The neutral host must form an SLA with hosted clients to set agreed performance standards.
- SLA verification: The processes are required to ensure that the terms of SLAs are being met.
- Network management: The processes are required to ensure that hosted clients can continue to provide the expected levels of customer support and network management, including fault resolution, when users are within the coverage of a neutral host.

4.7.1 Radio Network Planning Considerations

Since the goal of a neutral host is to act as a shared platform for several hosted clients, it is unlikely that the siting and specification of equipment will be individually optimized for each hosted client and their spectrum usage needs. Therefore, the neutral host should, guided by technical and business considerations, establish an approach that offers an attractive platform to a variety of hosted clients.

4.8 Neutral Host Example Scenarios

4.8.1 Company with a Real Estate Portfolio Acts as a Neutral Host

This scenario is based on the Small Cell Forum publication, Multi-operator market drivers, Section 5 "New approaches to kick-start the multi operator model".

An emerging model is for companies, who are not network operators, to build a portfolio of property, or property rights, that gives them access to sites that are suitable for deployment of small cells. Examples of ways in which this type of company may operate include:

- An organization has a large existing property portfolio (e.g., from broadcast infrastructure, transport infrastructure, or utility infrastructure). This organization sells rights to deploy cells on its property to a specialist company which establishes a neutral host, and then forms agreements with mobile operators or other hosted clients.
- A company purchases or leases from city government the right to use city facilities (e.g., lamp posts) as cell sites. The company then establishes a neutral host and forms agreements with mobile operators or other hosted clients.
- A company recognizes that property owners may prefer to outsource the activity of selling the rights to place small cells in their buildings, campus, or physical structures (e.g., lamp posts). The company makes agreements with several property owners and then establishes a neutral host and makes agreements with mobile operators or other hosted clients.
- The company owning the real estate rights typically does not have spectrum, or a license, to provide cellular coverage. However, it may have microwave spectrum to support back-haul from the cell sites and may either make use of unlicensed spectrum or hold non-cellular licenses.

4.8.2 Advantage of Neutral Host to Real Estate Owners

Historically, companies with sites suitable for deployment of small cells sold rights to individual network operators. This simple relationship allows sites to be utilized but means that the individual operator must bear all costs (capital and operating) associated with the use of the site. Users only gain benefit if they are subscribed to that operator.

Where space and other constraints permit, multiple operators may host small cells on the same site. Depending on the constraints, this may require one operator to act as the primary facilitator for the site with other operators' equipment being added with their consent. This kind of primary/secondary relationship can be difficult to establish and manage in practice.

By establishing a neutral host infrastructure, the company with the site portfolio gains several advantages:

- The ability to simultaneously sell to multiple operators increasing revenue opportunity.
- Increased participation in the value chain as a gate opener to operators and a service value add to real estate owners.
- Since the real estate may also require an independent Wi-Fi infrastructure for tenants, the cost of this infrastructure could be shared in a neutral host situation.

Mobile network operators and other hosted clients purchasing from such a neutral host also gain advantages:

- Effective sharing of infrastructure costs between multiple entities, thus reducing costs to individual hosted clients.
- Outsourcing of management of small cell infrastructure.
- Possibly increased flexibility of contract terms and reduction in length of commitments including short-term needs (e.g., for special events).
- Offers the possibility of social benefits and real estate added value due to coverage being provided from a wider variety of network operators.

4.8.3 Wireline Access Provider Acts as a Neutral Host

Wireline access providers and other local communications/access technology companies often have significant presence in areas suitable for dense high capacity small cell deployments. These companies may be in a position to build out a dense small cell architecture from which they may launch Neutral Host services. These companies may include:

- Traditional wireline network access providers that may today provide cable and/or fixed wireless services.
- DAS (Distributed Antenna System) providers interested in expanding their portfolio.
- Enterprise communication technology management companies who may manage the communications infrastructure for Enterprises as a service.
- Wi-Fi local access companies who today may provide hotels, airports and venues with public Wi-Fi access.

4.9 Neutral Host Sharing Options

Many different sharing options exist depending upon spectrum and technology choices. Neutral host providers could:

- Use unlicensed spectrum with Wi-Fi along with technologies such as Hotspot 2.0 and Wi-Fi calling to provide client network operators seamless access to client services.
- Use lightly licensed spectrum (e.g., Citizens Broadcast Radio Service [CBRS] in the 3.5GHz spectrum with private LTE) to enable more formalized roaming-based interconnections with client operators.
- Use licensed spectrum with Multi Operator Core Network (MOCN) or roaming architectures to share access to specific spectrum blocks managed by the neutral host.
- Use the 5G NR architecture to share access to specific spectrum blocks managed by the neutral host.

In addition, use of virtualization/Cloud technologies as well as new 5G core capabilities such as network slicing can be used to optimize the deployment scenarios.

5 Enabling Technologies

5.1 5G Aspects Supporting Neutral Host Architectures

The 5G Core (5GC) network architecture is substantially different from the 4G Enhanced Packet Core (EPC). In constructing the 5GC, Third Generation Partnership Project (3GPP) has repartitioned many existing 4G functions while adding new functionality creating new architectural reference models with new functional entities and reference points. The new architecture and functionality provide several advantages and creates opportunities for new neutral host architectures enabling services and capabilities not possible in previous 3GPP architectures.

The 5GC makes a clear distinction between control plane functions (i.e., functions used for control purposes) and user plane functions (i.e., functions that carry user data between the client and the appropriate data network). The control plane elements connect to the user plane elements using the N1, N2 and N4 reference points. Advantageously, the 5GC can be expressed in two ways; one using service-based interfaces in the control plane and one using the more traditional reference point architectural view. In the Service Based Architecture (SBA) view, control plane functions are shown as connected via a “bus” where the service-based interface label is associated with each individual control function. The advantage of this architectural construct is that any authorized network function on the “bus” can access the services provided by any other control plane function on the “bus”. This enables the 5GC to implement new custom, value added features and capabilities while staying within the standardized architectural reference model.

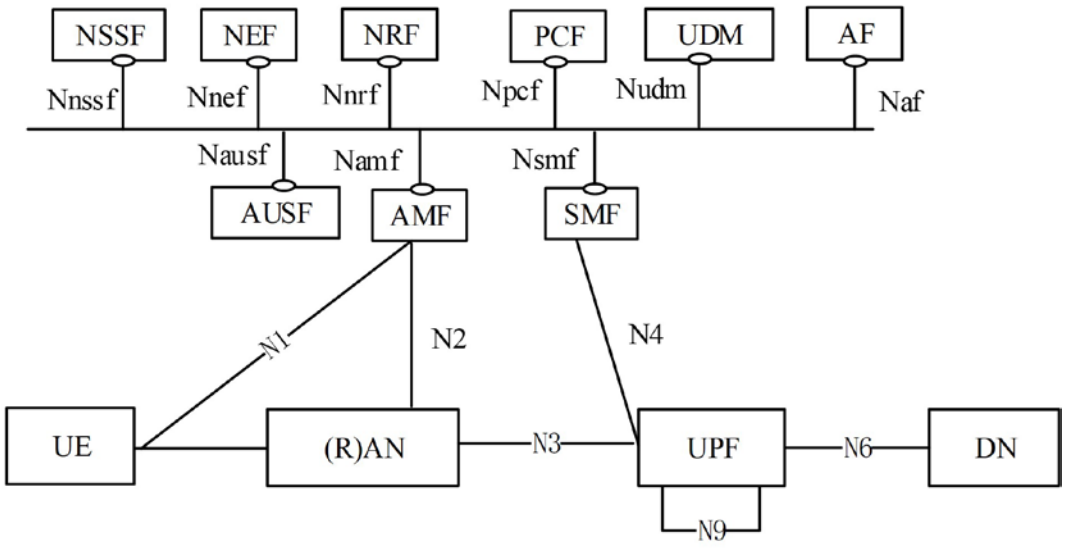

Figure 5.1-1 - Non-Roaming 5GC Reference Architecture with Service-Based Interfaces

The new functional entities shown in this architecture include:

- Access and Mobility Management Function (AMF) which provides access specific functions including access authentication and authorization along with registration, connection, reachability and mobility management functions.
- Authentication Server Function (AUSF) supports authentication for 3GPP access and untrusted non-3GPP access.

- Data Network (DN) refers to Internet or private network access along with any 3rd party services
- Network Exposure Function (NEF) supports the exposure of capabilities and events to other network functions enabling secure exposure to 3rd party application functions.
- NEF stores/retrieves information as structured data using a standardized interface (NUDR) to the Unified Data Repository (UDR).
- Network Repository Function (NRF) supports service discovery and provides the discovered network function instances to the calling network function instance.
- Network Slice Selection Function (NSSF) selects the set of Network Slice instances serving the UE.
- Policy Control Function (PCF) supports a unified policy framework to govern network behavior; providing policy rules to Control Plane function(s) while accessing subscription information relevant for policy decisions in a Unified Data Repository (UDR).
- Session Management Function (SMF) provides session management including session establishment, modify and release, IP address allocation and management, selection and control of the User Plane Function (UPF), and charging data collection.
- Unified Data Management (UDM) provides subscription management functions including generation of 3GPP AKA Authentication Credentials, user identification handling and access authorization based on subscription data.
- User Plane Function (UPF) provides user packet routing and forwarding as well as packet inspection, downlink buffering, gating, redirection, traffic steering, legal intercept and Quality of Service (QoS) marking.
- Application Function (AF) which may interact with the 5GC for application services that may include influences on traffic routing, accessing the Network Exposure Function and interacting with the Policy framework for policy control.
- User Equipment (UE).
- (Radio) Access Network ((R)AN).

A more complete description of the 5GC functional elements and interfaces can be found in 3GPP TS 23.501 - System Architecture for the 5G System.

For the purposes of this document, 5GC network architectures used to illustrate neutral host solutions will use the reference point perspective as shown in the figure 5.1-2.

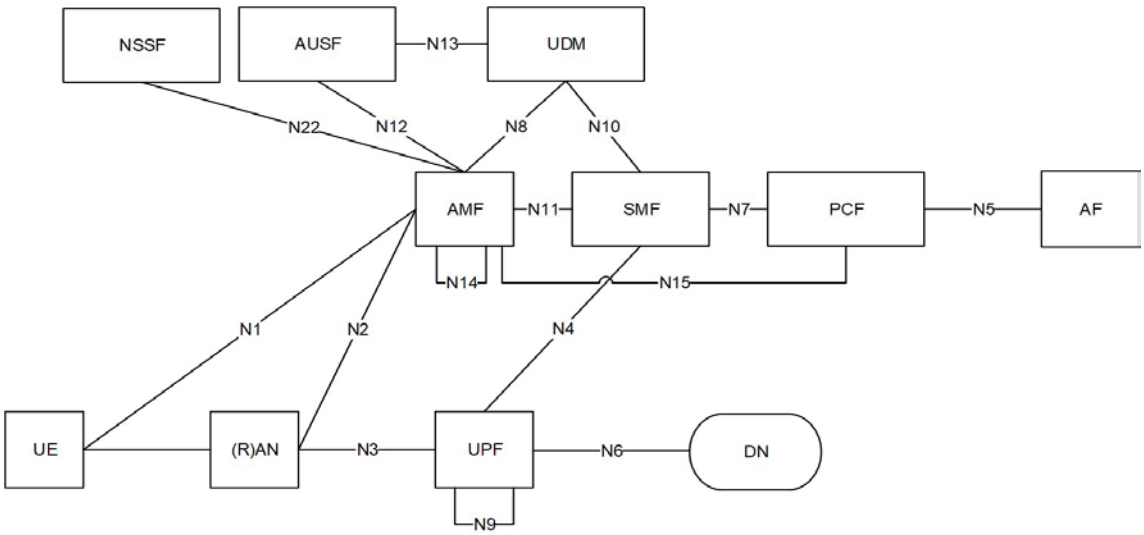

Figure 5.1-2 - Non-Roaming 5GC Reference Architecture with Reference Point Interfaces

The reference point-to-point diagrams do not show functions such as NEF and NRF (which are shown in the service-based architecture). However, all depicted network functions can interact with these functions as well as other functions not shown such as the NetWork Data Analytics Function (NWDAF).

As noted earlier, the 5GC explicitly supports the separation of the control plane from the user plane. This enables deployment scenarios where multiple UPFs (User Plane Functions) can serve the same UE. For example, UEs concurrently accessing two (e.g., local and central) data networks using multiple PDU Sessions is illustrated in the figure 5.1-3. This figure shows the architecture for multiple PDU Sessions where two SMFs are selected for the two different PDU Sessions. However, a single SMF may also have the capability to control both a local and a central UPF within a PDU Session.

This use of multiple UPFs can be advantageous for some Neutral Host architectures since both the Neutral Host as well as the hosted client network are now able to terminate traffic from a single UE simultaneously.

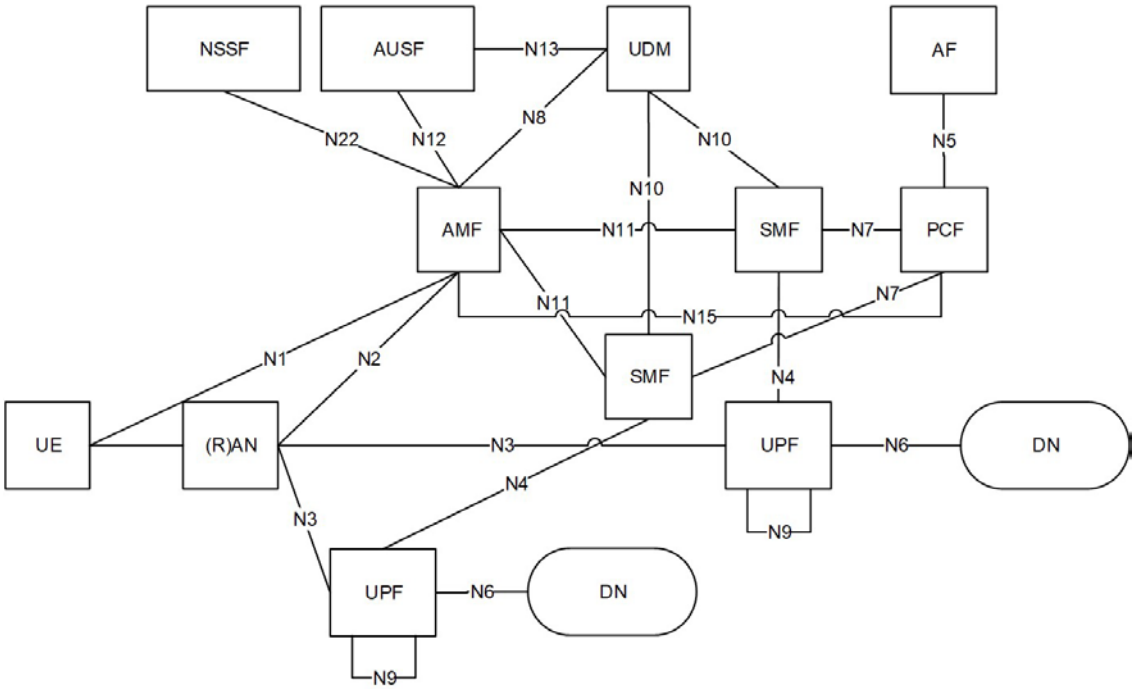

Figure 5.1-3 - Non-Roaming 5GC Reference Architecture with Multiple User Plane Functions

In addition, the 5GC architecture also supports concurrent access to two (e.g., local and central) data within a single PDU Session through the use of two UPFs in series. This architecture is shown in the figure 5.1-4. As in the previous case, this architecture may also be of interest in 5G Neutral Host deployments where both the Neutral Host as well as the hosted client network.

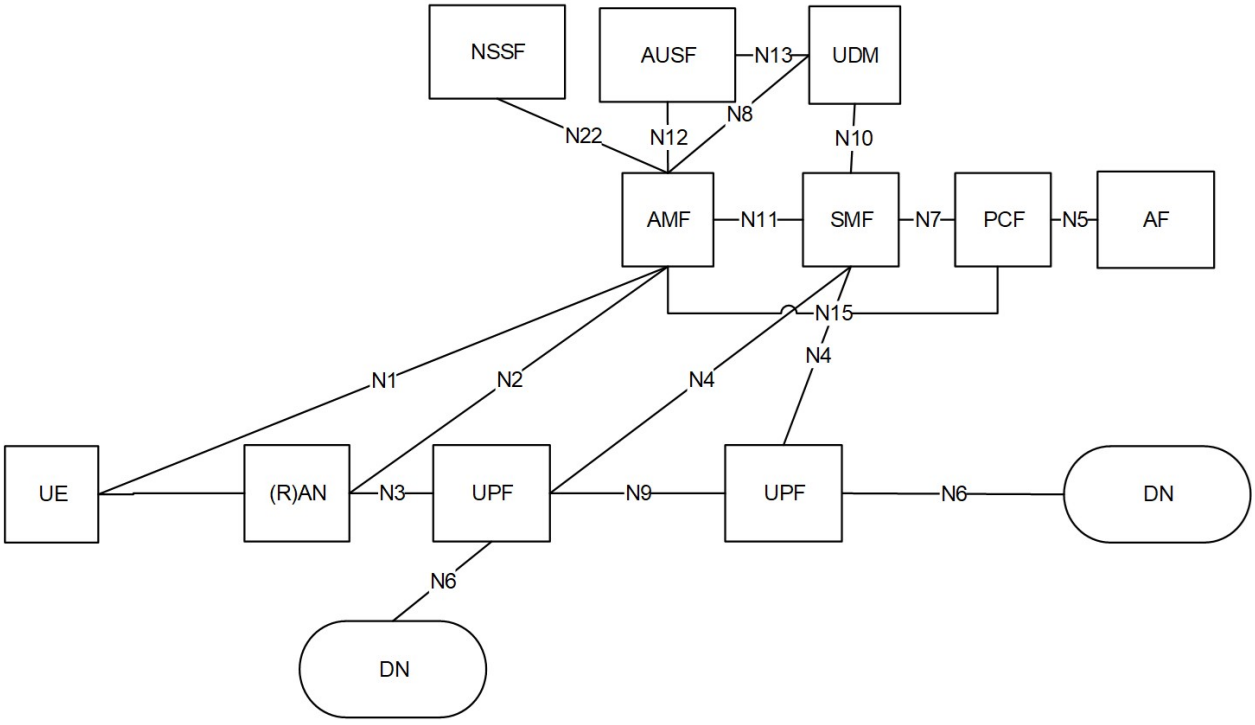

Figure 5.1-4 - Non-Roaming 5GC Reference Architecture with Multiple User Plane Functions

5.1.1 Roaming Architecture

3GPP Release 15 supports both local breakout and home routed roaming architectures. For the purposes of neutral host deployments, the home routed architecture, shown 5.1.1 in reference point representation, is most relevant. In a neutral host deployment, the neutral host is the “visited network”, and the client operator’s network is the “home network”. Multiple roaming clients can be supported.

In this view, the visited (neutral host) network would provide dedicated instances of an NSSF, PCF, AMF, SMF, and a UPF. The visited network must expose the following reference points (interfaces):

- N31 for network slicing control
- N24 for policy
- N8 for subscriber data
- N12 for authentication
- N16 for session management
- N9 for data plane

The AMF in the visited network may be shared with that network’s other traffic or may be a dedicated instance to support the roaming carrier.

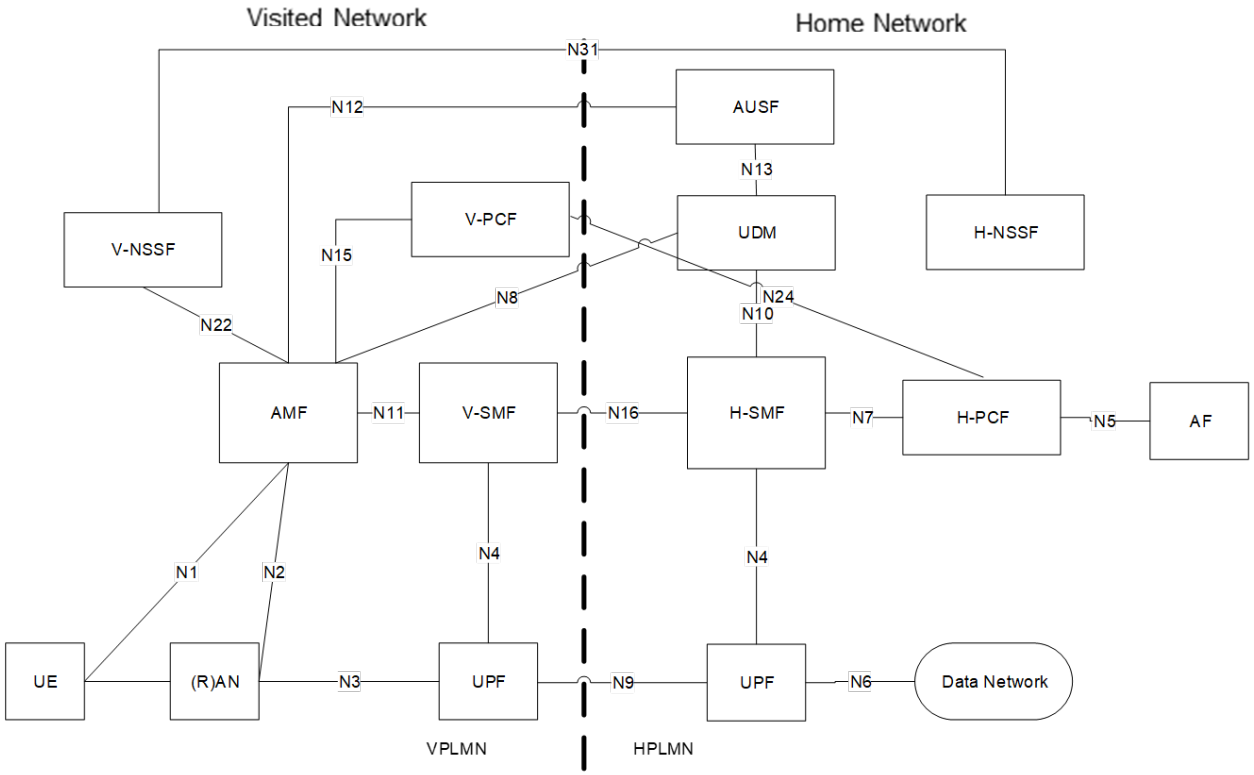

Figure 5.1.1 - Roaming 5G System Architecture-Home routed scenario

5.1.2 Support for Non-3GPP Access

3GPP Release-15 provides for general, uniform support for untrusted non-3GPP access mechanisms, all making use of common 3GPP control plane elements. Figure 5.1.2-1 shows the elements required for non-3GPP access support in the context of a Next Generation Network in a non-roaming scenario.

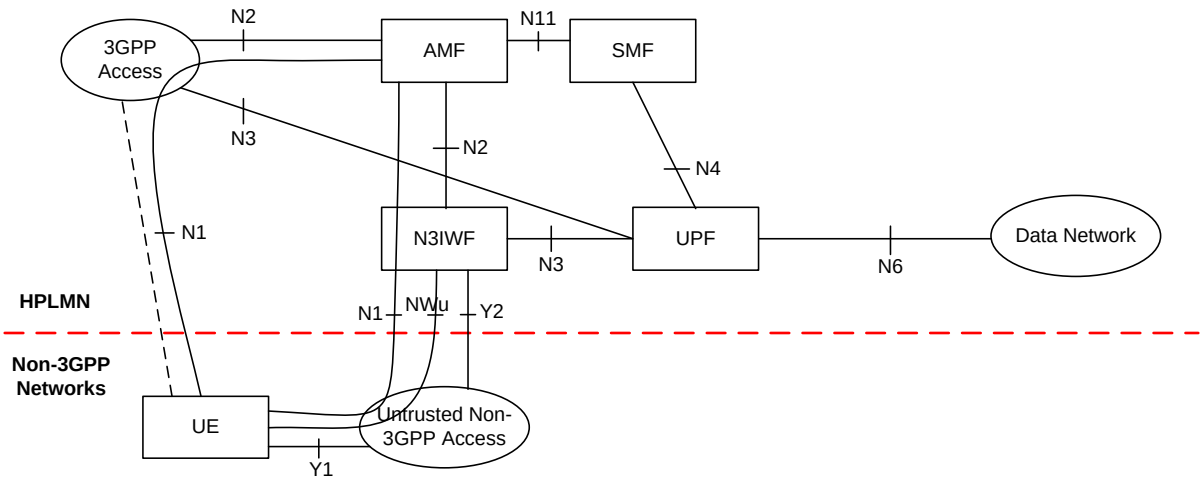

Figure 5.1.2-1 - Non-roaming architecture for 5G Core Network with non-3GPP access

Both control and user plane interactions between the Next Generation Core (NGC) and the Non-3GPP access network are mediated by a newly defined network function, the Non-3GPP Interworking Function (N3IWF). Once the UE establishes a connection to the NGC, an N1 reference point is established between the UE, and the AMF. The UE then supports NAS signalling with the 5GC via the N1. User plane traffic travels between the N3IWF and

the untrusted non-3GPP access network via the NWu reference point. In turn, the N3IWF supports an N3 reference point to a UPF for the non-3GPP access network's user plane traffic.

A UE may be connected to the non-3GPP and a NG-RAN simultaneously, in which case it will maintain separate N1 reference point instances to the AMF, one for each access network. All of the N1s from a single UE are anchored to the same AMF.

There are a number of roaming scenarios supported for non-3GPP access networks. For the purposes of neutral host, the most relevant is shown in the figure 5.1.2-2:

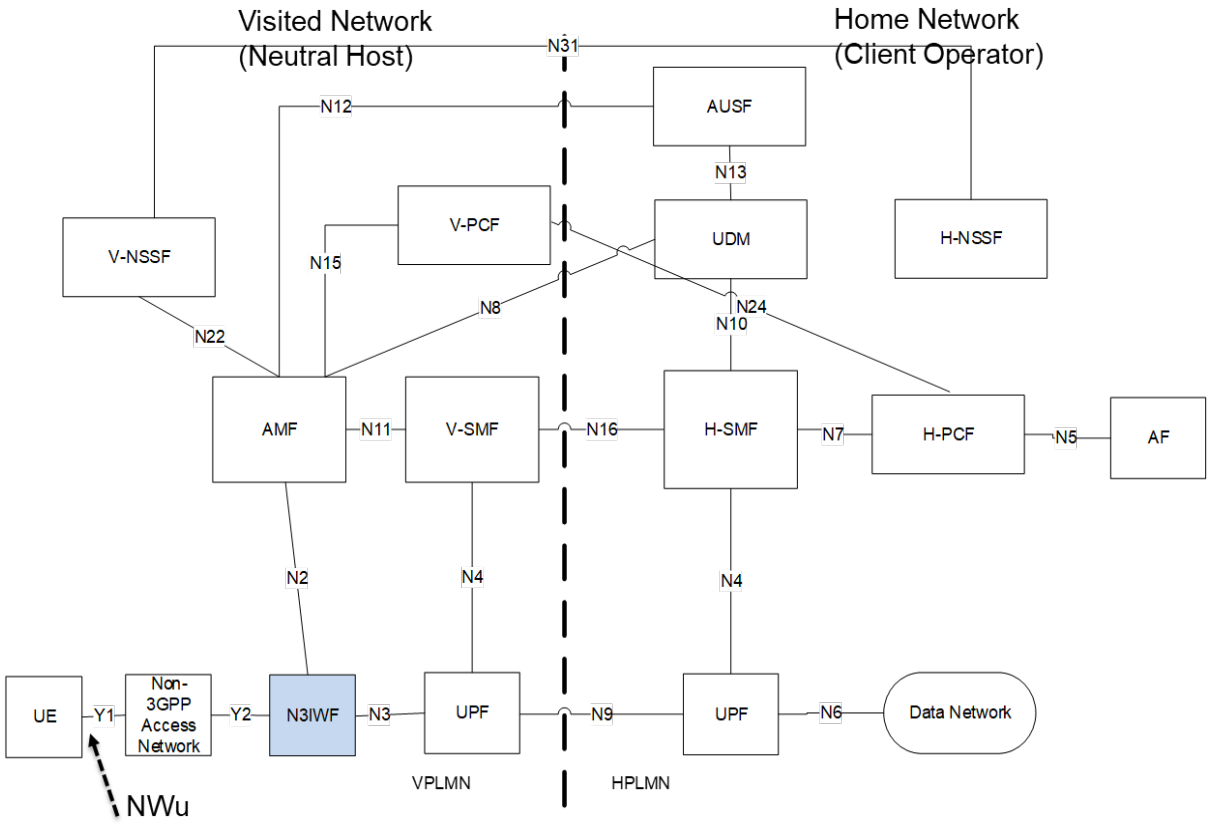

Figure 5.1.2-2- Home-routed Roaming Architecture for Non-3GPP Accesses, N3IWF in same PLMN as 3GPP access

In Figure 5.1.2-2 the N3IWF is provided by the visited network (neutral host), completely abstracting the access mechanism from the home network (client operator). This enables the neutral host to provide 3GPP compliant roaming without restricting the type of access network used.

5.1.3 Access Traffic Steering, Switching and Splitting

In 2017, 3GPP SA2 approved a study item documented in 23.793 and targeted for 3GPP Release 16, that looks at supporting Access Traffic Steering, Switching and Splitting (ATSSS) between 3GPP and non-3GPP (N3GPP) access networks. This work promises to offer a much more seamless and richer experience for users, than has been possible to date, as they roam between 3GPP and N3GPP access networks, much more akin to the seamless handover experience within 3GPP access networks. Within the scope of the Neutral Host scenario, the work paves the way for a seamless user experience when moving between a 3GPP access network and the Neutral Host.

The scope of the 3GPP work is to define mechanisms to support Multi-Access (MA PDU) sessions over 3GPP and N3GPP access networks. A MA PDU session is a type of PDU session that allows an application to send/receive traffic either over a 3GPP access, a non-3GPP access, or both accesses simultaneously. A MA PDU session comprises of a PDU session over a 3GPP access and a "linked" PDU session over a N3GPP access, or vice versa. Each of the PDU sessions may have its own set of UPFs, but both PDU sessions share a common PDU session anchor (PSA). For a MA PDU session, applications in the UE and the host server are not aware of the ATSSS and traffic splitting function across multiple access networks.

Figure 5.1.3 illustrates the ATSSS functionality split between a 3GPP and N3GPP access network.

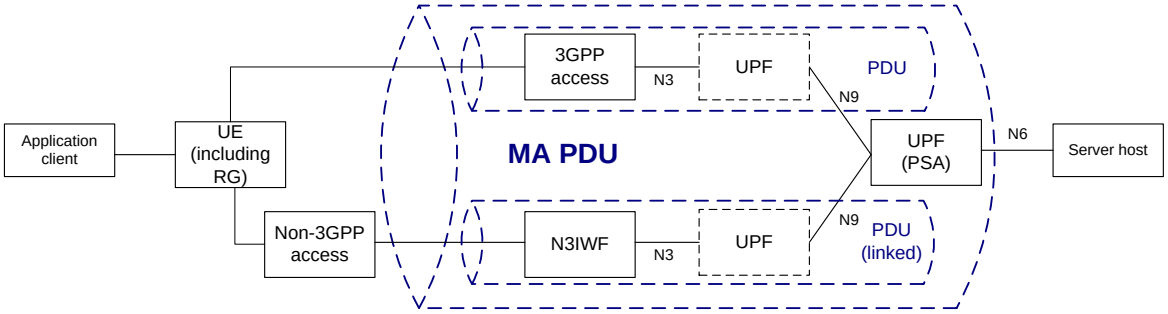

Figure 5.1.3 - MA PDU session

The 3GPP PDU session and linked N3GPP PDU session of a MA PDU session share the following attributes:

1. DNN: Data Network Name is the name of the data network and end point for an application PDU session
2. SSC mode: SSC stands for Session and Service Continuity. It is related to how an application PDU Session is established to support session and service continuity in general (pre-dates ATSSS) as follows:
   a. SSC mode 1: the network preserves connectivity and IP address but the same UPF is maintained regardless of mobility (could lead to inefficient routing)
   b. SSC mode 2: “break before make”, the network release PDU Session and instructs UE to establish a new one.
   c. SSC mode 3: “make before break”, the network allows new PDU session establishment before old one is released
3. S-NSSAI: Single Network Slice Selection Assistance Information. It is the network slice serving an application PDU session.
4. PDU session type (IPv4, IPv6 or Ethernet)
5. IP address (for IPv4 and IPv6 PDU session type)

In particular, the study item considers solutions that specify the following:

- How the 5GC and the 5G UE can support multi-access traffic steering between 3GPP and non-3GPP accesses.
- How the 5G Core network and the 5G UE can support multi-access traffic switching between 3GPP and non-3GPP accesses. This includes the conditions that can trigger the switching of data traffic to a new access type.
- How the 5G Core network and the 5G UE can support multi-access traffic splitting between 3GPP and non-3GPP accesses. This includes the conditions that can trigger the splitting of data traffic across multiple accesses.
- How the multi-access traffic steering, switching and splitting can be taken into account by the charging framework. For example, in order to enable the network operator to differentiate charging for data traffic that is switched and/or split between 3GPP and N3GPP access networks.

- How the policy framework can be extended in order to support the requirements for ATSSS.

The study is restricted only to ATSSS procedures applied in the 5G core network. Initially, the study considers ATSSS functionality between the NG-RAN and untrusted non-3GPP access networks. Subsequently, after the 5GS architecture is enhanced to support trusted non-3GPP access networks, the study will also consider ATSSS functionality between the NG-RAN and trusted non-3GPP access networks. ATSSS procedures that may be applied in the NG-RAN are not considered.

If this work is incorporated into normative 3GPP standards, ATSSS procedures could be used to create a layer 2 multipath (L2MP) solution. This in turn can enable session-based link aggregation between 3GPP and non-3GPP access and could prove to be very useful with 5G mmWave where signal conditions may change dramatically within very short time intervals. Linking mmWave sessions to alternate access could provide a more seamless experience since traffic could seamlessly share the aggregate bandwidth as individual Radio Frequency (RF channel bandwidth varies. This becomes interesting from a neutral host perspective since both 3GPP and non-3GPP access needs to terminate on the same anchor, favoring neutral host architectures that fully support and integrate local unlicensed access as well as 3GPP access capabilities.

5.1.4 Network Slicing

Mechanisms that permit partitioning of a single network into a number of distinct logical networks have existed for some time. GPRS networks defined the concept of the Access Point Name (APN) to pair a UE's Packet Data Network (PDN) with a particular SGSN. In 4G, this concept was extended in Release 13 to permit pairing of a PDU session from the UE with a particular MME via the Dedicated Core Network (DECOR) in Release 13, and the Enhanced Dedicated Core Network (eDECOR) in Release 15.

The 3G and 4G mechanisms for partitioning a network had limitations and lacked flexibility. Release 15 introduces a more robust and flexible mechanism, 5G Network Slicing.

While the initial conception of network slicing was based on partitioning traffic based on services (e.g., enhanced Mobile Broadband, IoT, Ultra-reliable Low Latency), the concept has since broadened. A network slice can be established to support a logical network dedicated to a customer (e.g., an enterprise, or a neutral host client network), to a Mobile Virtual Network Operator (MVNO), to partitions based on individual applications (or groups of applications). A 5G UE may support up to eight simultaneous distinct active slices.

A 5G network slice is (minimally) defined as a distinct SMF/UPF pair, though it will likely contain other network functions as well. All the active slices from a particular UE share the same AMF but will likely be mapped to a different SMF and UPF instance. The access and mobility characteristics for a particular UE will be the same for all application, but each application may have its own unique session management, policies, user plane characteristics, etc.

Figure 5.1.4 shows an example of the Release 15 network slicing architecture applied to the Neutral Host use case. It shows two UEs, each native to a different client operator, each connected via the Neutral Host (NH) network to its respective home network. For illustrative purposes, the diagram also shows a car that is generating traffic for a manufacturer's IoT network, and simultaneously generating browser traffic. In this example, the car is a customer of the neutral host.

In the figure, there is a network wide UDM, and a global NSSF and NRF, all of which serve the entire NH network. Slices 1 and 2 are assigned to two different NH client operators. In addition to the dedicated SMF and UPF that define the slice, each contains its own NRF, AMF, and PCF. The slice-dedicated NRF in each of these slices is used to enable discovery of the NFs assigned to that slice, and that discovery is only available within that slice (so, for example, the set of NFs assigned to NH-Client #1, for example, can only be discovered within slice 1.) Similarly, slice 1 has its own set of policies that apply, and are visible, only within that slice.

The car's traffic is mapped to two different slices, one for the manufacturer's IoT applications (e.g., telemetry, etc.), and the other for more generic browser traffic generated by the car's passengers. In the example, all the car's slices share a common AMF, and a global NRF and PCF that apply to all of the car's slices. In addition to the common policies, each of the two slices may have its own set of distinct policies, contained in its own, dedicated PCF.

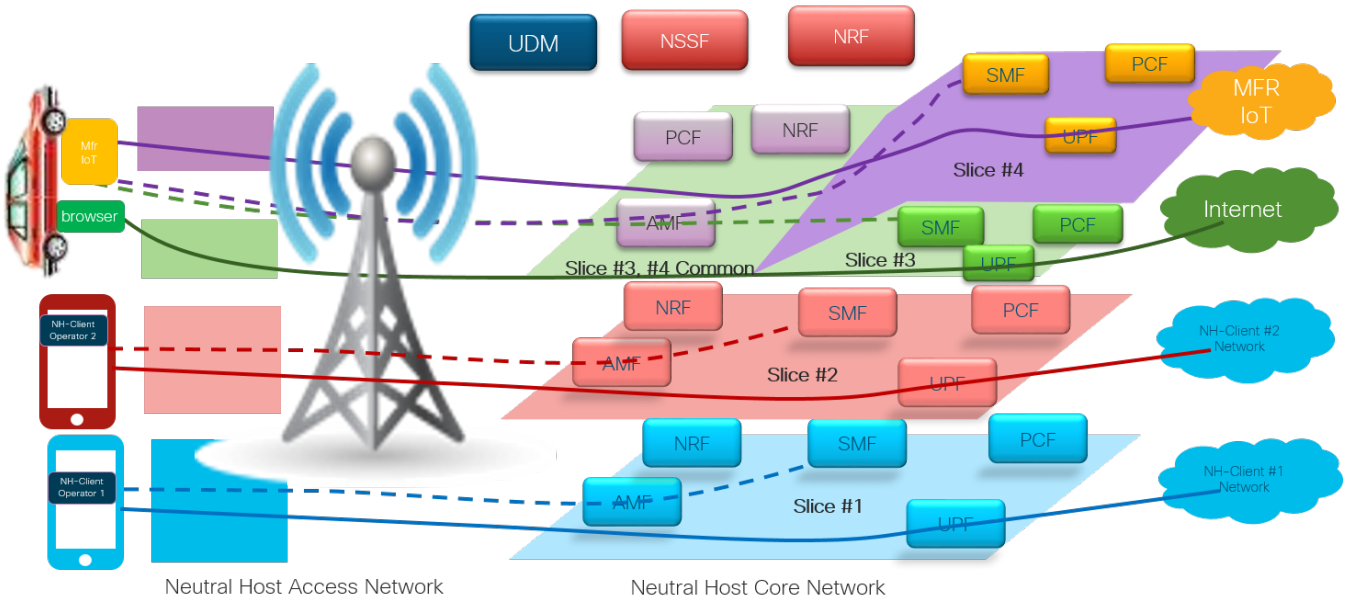

Figure 5.1.4 - Release 15 Network Slicing Architecture

Some Release 15 network slicing characteristics are:

- Policy for binding applications to network slices is flexible, and may be provided to the UE during registration, or may be configured directly on the UE. These policies may be changed after registration.
- Policies for slice selection may be centralized in the NSSF or may be configured in each AMF.
- The concept of network slicing can be extended through the access network and RAN. Slice IDs of each PDU session are provided to the RAN to enable it to assign resources, per slice, according to policy.

In a roaming scenario, only the basic slice types are supported. However, multiple instances of these slices can exist to support multiple roaming partners.

5.2 Identity Management in Neutral Host Architectures

5.2.1 Authentication Methods

Flexible authentication methods for various types devices will be required for 5G Neutral Host applications. The Neutral Host environment may need to support a variety of non-3GPP use cases including IoT, private factory networks, and different access technologies. To enable this flexibility, 3GPP SA3 has defined primary authentication (mandatory) and a secondary authentication (optional) methods. Primary authentication provides access to the 5G core. The secondary authentication is only enabled after a successful primary authentication and allows the user to provide credentials to access other (e.g., private) networks. For example, secondary authentication can be used between an enterprise and the UE to authenticate access to a corporate APN. Both authentications support EAP, the Extensible Authentication Protocol. In this way, authentication in 5G can meet different requirements from the various use cases.

EAP is an authentication framework defined in RFC 3748 and is updated by RFC 5247. It is not a specific authentication mechanism. Rather, EAP provides common functions and negotiation capabilities to support a wide variety of standardized and proprietary authentication methods. There are many different EAP methods defined, including:

- EAP Transport Layer Security (EAP-TLS),
- EAP Protected One-Time Password (EAP-POTP)
- EAP Pre-Shared Key (EAP-PSK)
- EAP Internet Key Exchange v2 (EAP-IKEv2)
- EAP Subscriber Identity Module (EAP-SIM)
- EAP Authentication and Key Agreement (EAP-AKA) and
- EAP Authentication and Key Agreement prime (EAP-AKA')

Note also that the primary authentication is radio access technology independent. Thus, it can run over non-3GPP technology such as IEEE 802.11 Wireless Local Area Networks (WLANs).

The integration of EAP methods into the 3GPP 5G security framework allows a 5G neutral host more flexibility in supporting a variety of devices and authentication methods and business models. Figure 5.2.1, for example, the neutral host provider could now host clients that are simply enterprises wishing to support their devices in the neutral host environment. An example scenario could operate as follows:

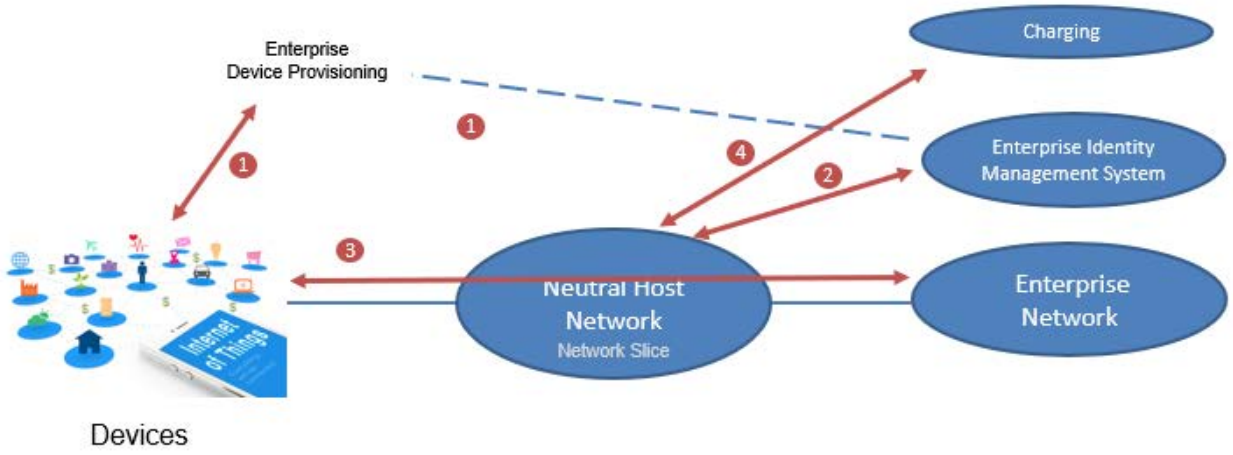

Figure 5.2.1- Neutral Host with Enterprise Client

1. The enterprise assigns a unique global identity to its devices, which incorporates a reference to the enterprise's identity to aid in discovery. For example, an NAI (Network Access Identifier) of the form user@realm could be used. This identity along with credentials can then be provisioned onto the device as well as the enterprise identity management system.
2. When in the neutral host environment, the device can initiate attachment procedures to attach (connect) to the neutral host network using a specific unlicensed technology:

   - The neutral host receives the global identifier from the device in an attachment request.
   - The neutral host validates the identity of the enterprise presented in the global identifier and the existence of a business and service relationship between the neutral host and the enterprise.
   - After validating the enterprise, the neutral host facilitates the use of the appropriate EAP method to authenticate the device with the enterprise (using the enterprise authentication database).
   - The enterprise completes authentication of the device.

3. The neutral host may then complete attachment of the device and may associate the device to a network slice specifically provisioned for the appropriate level of security and trust. Once attached, the neutral host can provide packet/object transport services.
4. The neutral host creates charging records for all network services provided to the device for the purpose of upstream billing of the enterprise.

5.2.2 Authentication Framework

3GPP Release 15 expanded and unified the set of supported authentication mechanisms, applying to both 3GPP and non-3GPP access, with control centralized in a single network function. Also, Release 15 increases Home Network control of the authentication process.

Several NGC network functions are engaged in authentication, but control of authentication is centralized in the Authentication Function (AUSF) in the Home Network, (Neutral Host Client Network) for all access types. 3GPP has adopted the Extensible Authentication Protocol (EAP) framework to integrate the IMSI/AKA methods that were used prior to Release 15, with methods used for non-3GPP access networks

Control of authentication is located in the Authentication Server Function (AUSF) in the Home Network. The Visited Network (Neutral Host Network) performs EAP Authentication via the Security Anchor Function (SEAF), which is located in the Visited Network's Access and Mobility Function (AMF). The network functions involved in authentication are shown in the Figure 5.2.2.

The EAP framework supports authentication for devices that use the pre-5G SIM/AKA identification/authentication mechanisms, as well as 5G-AKA. This is an evolution of the EPS-AKA mechanism, giving the Home Network more control over authentication. The AMF/SEAF in the Visited Network performs partial verification of the device's identity, while full validation is performed by the AUSF in the Home Network.

The User Data Module (UDM) in the Home Network provides policy information to the AUSF, to support deciding the authentication method that applies to a particular identity. The UDM also acts as the Authentication Credential Repository and Processing Function (ARPF) for SIM/AKA authentication.

For untrusted non-3GPP access, the N3IWF in the Visited Network acts as a proxy for the UE. The UE first establishes an IPsec tunnel with the N3IWF using the EAP-5G method (which may be vendor specific). The actual authentication of the UE is performed by the AUSF in the Home Network using either an EAP based method or 5G-AKA, with messages encapsulated in the tunnel.

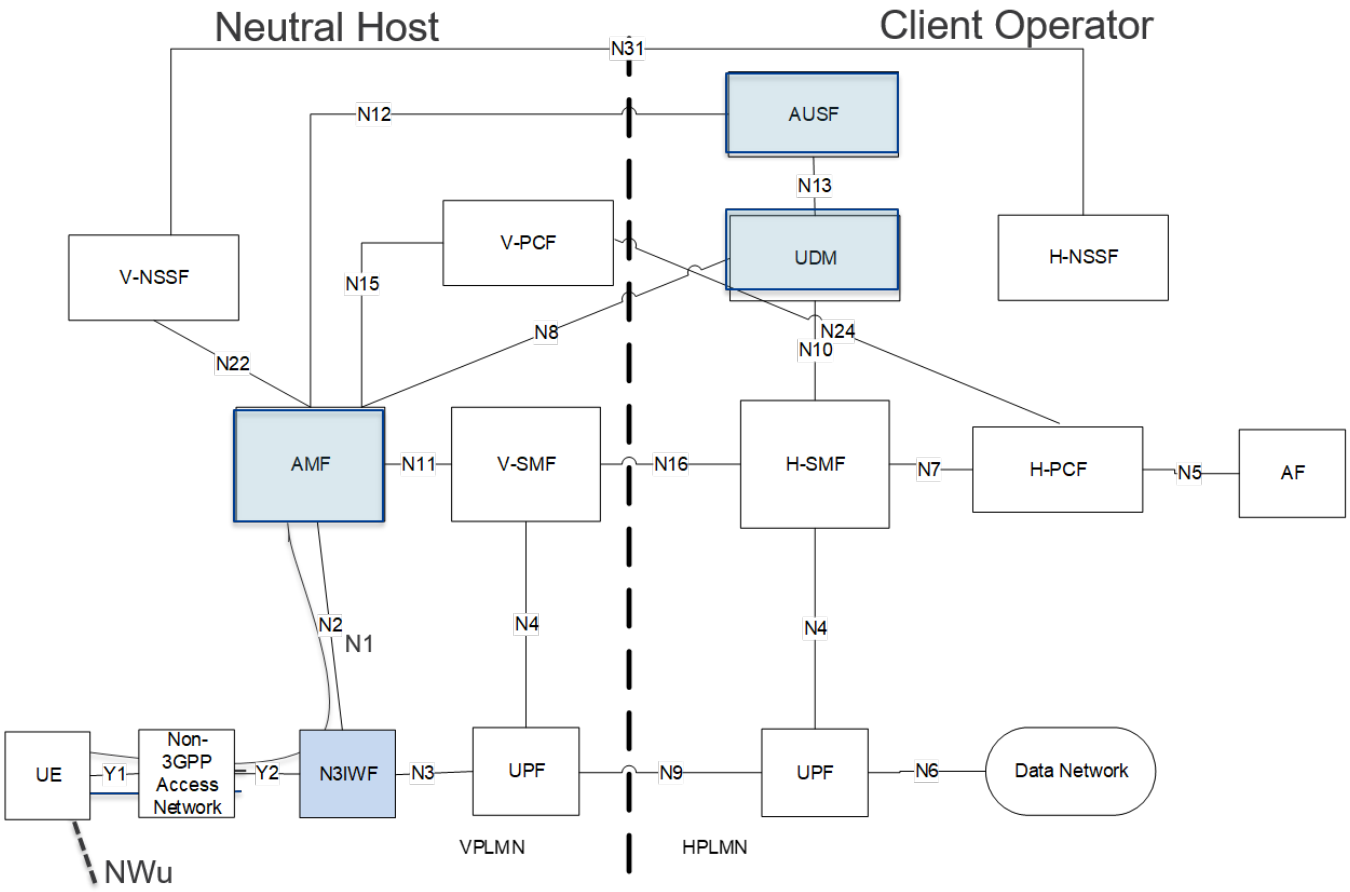

Figure 5.2.2 - Neutral Host with Enterprise Client

5.2.3 Subscriptionless Services

Given the large number and variety of unlicensed communication options, the neutral host could also offer subscriptionless connection services. For example, when an unlicensed device attempts to connect to a supported radio interface protocol, the neutral host could attach the device to a portal that presents a payment screen. This allows the neutral host provider to offer limited connection services (limiting time or bandwidth) in exchange for viewing advertisements or a given sum of money.

5.3 Charging for Neutral Host Scenarios

Generally, the neutral host will charge their client (operator) for providing access services to each client's subscribers. Charging is often proportional to the network resources used in the neutral host network. As such, 3GPP standard charging models, as might be applied for roaming purposes, may also be applied to neutral host arrangements.

The current 3GPP architecture for network service charging and billing relies on data collection at the Visited Public Mobile Network (VPMN) and relaying Charging Data Records (CDRs) information to billing systems operated by an intermediary Data Clearing House (DCH) as illustrated in the figure 5.3.1. These billing systems process the CDRs in accordance with a Home Public Mobile Network (HPMN) roaming and tariffs agreement with the VPMN. For the purpose of the following discussion, the neutral host may be considered synonymous to the VPMN.

The DCH generates consolidated subscriber reports for the HPMN who then settles costs incurred with the VPMN based on the information provided. The settlement and billing to the HPMN is based on reconciliation relative to

specific Service Level Agreements between the HPMN and VPMN. The VPMN sends CDR information to the DCH as a Transfer Account Procedure (TAP) file. The DCH is responsible for conversion of the CDR files and the generation of billing cost information for resources consumed in the VPMN in accordance with the corresponding roaming agreement and agreed tariffs. The DCH then transmits the TAP files and billing information to the HPMN. The HPMN may generate Returned Account Procedure (RAP) files in order to reconcile accounts by the DCH.

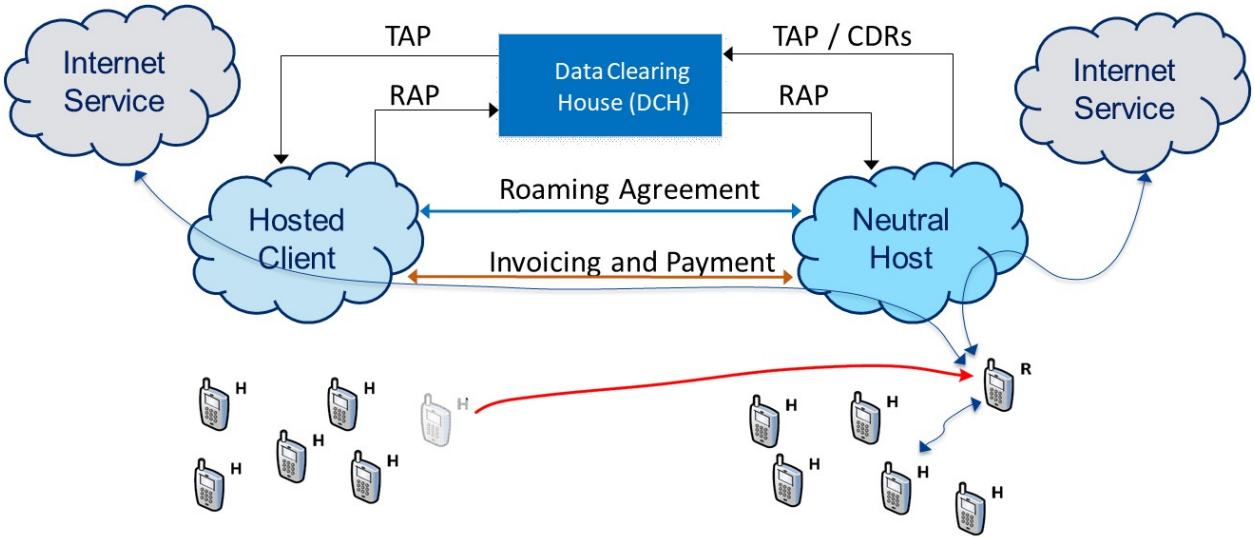

Figure 5.3-1 Roaming Charging Architecture

This process of reconciling the CDRs and generating the billing information is typically an offline process and there is a time delay associated with the generation of the user's resource consumption data for the HPMN. The HPMN settles charges with the VPMN based on information provided by the DCH. For subscriber data that experiences Local Breakout (LBO) in the VPMN network, there is no direct and verifiable accounting trail to the actual resources consumed by a user since user data does not pass to the HPMN.

Similar charging arrangements could be configured for neutral host architectures where the neutral host plays the role of the VPMN and the client operator plays the role of the HPMN. However, 5G based neutral host deployments may require additional service functions to handle accurate, high bandwidth, real-time charging with verifiable accounting trails. Some examples of the envisioned services are:

- Enable the client operators to reduce and manage costs by gaining access to fine grained, real-time resource consumption information specific to charging/policy functions in the neutral host network.
- Use of NFV/Virtual Network Function (VNF) constructs in the neutral host network to perform fine grained management of traffic by enabling the client operator to instantiate specific charging/policy functions in the neutral host network as needed on a per subscriber basis.

Digital Ledger Technologies (DLT) may offer the potential for providing service flexibility and scaling the current 3GPP systems in addition to simplifying neutral host charging while enabling real-time accountability for charging events. This latter capability becomes much more attractive with 5G systems offering a rich and diverse set of services to a HPMN host without the need to establish separate SLAs with each neutral host.

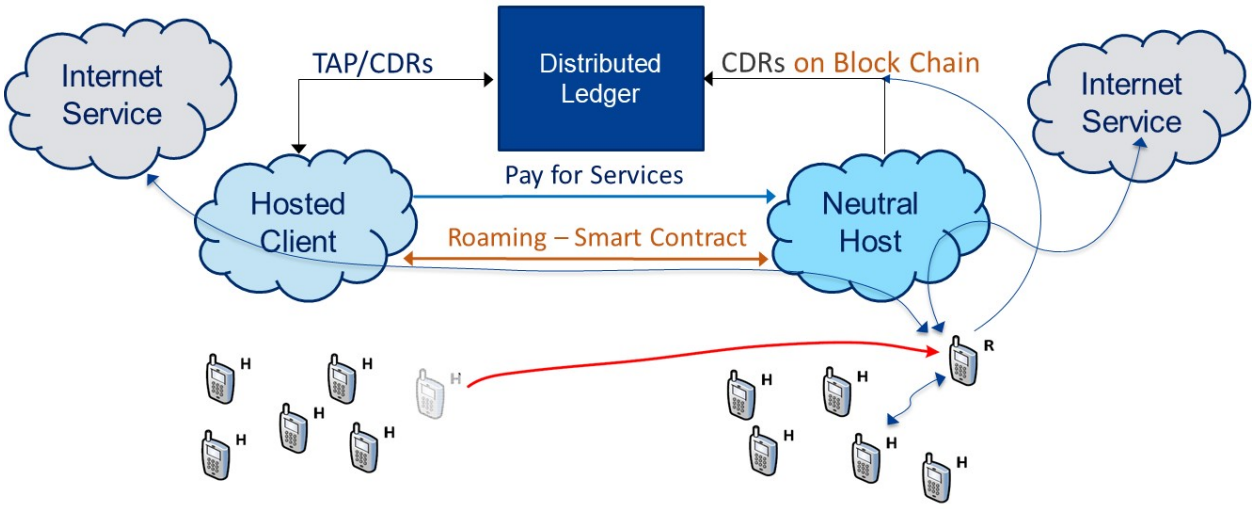

Figure 5.3-2 - Roaming Charging Architecture with Distributed Ledger

Figure 5.3-2 illustrates a DLT based charging arrangement for a generic neutral host architecture. The neutral host operator and associated client operators establish a smart contract for inter-operator services offered to their customers. When a subscriber of a client operator consumes services from a neutral host, CDRs are generated and registered into a block chain-based Distributed Ledger (DL). As services are consumed the neutral host and client operator register CDR information into the DL. A mobile device may optionally log CDR information into the distributed ledger, in order to provide traceability, accuracy of information, and prevent fraud.

The DL is processed by a billing system, in accordance with the smart contract between the neutral host and client operator. The billing system automatically reconciles the CDR records, produces TAP files and generates billing cost information for resources consumed in the neutral host network, in accordance with the corresponding smart contract. The client operator can then settle payment with the neutral host provider. Consolidated subscriber reports are also automatically generated by the billing system for the client operator. Access to CDRs in a DL enables the client operator to gain access to real-time resource consumption information and lower costs while increasing the breadth of service offerings through automated reconciliation of accurate and reliable CDR information.

However, any charging solution needs to meet a minimum set of requirements relative to the charging records:

- Integrity (tamperproof)
- Authenticity of source
- Auditability of records collected
- Authorization (transparency control, access control based on real-time data)
- Traceability (reconciliation of CDR event logs)
- Verifiability (corroboration/verification across two parties)
- Non-repudiation
- Confidentiality
- Privacy (information available on a need to know basis)
- Accounting (smart contracts for records settlement transactions)

For DLT based solutions, these requirements may require the use of permissioned private ledgers. These digital ledgers offer separate control mechanisms to determine who is allowed to participate in the network, execute the consensus protocol and maintain the shared ledger. A private (permissioned) blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter. As such, the system places restrictions on who is allowed to participate in the network and determine which types of transactions are accessible.

To address privacy concerns, permissioned private ledgers often support the ability to segregate the network into channels. Each channel represents a subset of participants that are authorized to see data associated to that channel. Within the channel, participants may have create, read, and/or update access policy rules with separate roles enforced through encryption where the decryption keys are distributed only to authorized entities. In the context of a neutral host deployment, the neutral host to client operator relationship could be captured as a separate channel.

It is important to note that, as of the publication date of this document, the use of DLTs for charging applications is still under investigation and may or may not be suitable for neutral host architectures.

5.4 Cloud/Virtualization Aspects

The increasing use of cloud services and NFV based virtualization can be leveraged to advantage in neutral host architectures. NFV structures enable a neutral host core network along with the virtualizable components of the radio access network to run on top of standard datacenter compute facilities in a data center. The Virtual Network Functions (VNFs) needed within the neutral host can either be:

- Provided by the neutral host entity as a menu of functions that can be selected by a client operator, or
- Instantiated and maintained by the client operator in the neutral host network in an NFV-as-a-Service (NVFaaS) arrangement. Each client operator could then choose VNFs from its preferred set of vendors while the neutral host entity provides a platform and connectivity.

Indeed, the neutral host datacenter components, core network components and the physical radio access components (e.g., radio heads, antennas, cabling and network connectivity) need not be provided by the same entity. For example, different Digital Distributed Antenna System (DDAS) providers could provide the radio access components in different venues/locations, while different core platform datacenters could be leased from a data center provider local to the venues, all managed by a single neutral host entity.

These possibilities are shown in figure 5.4.

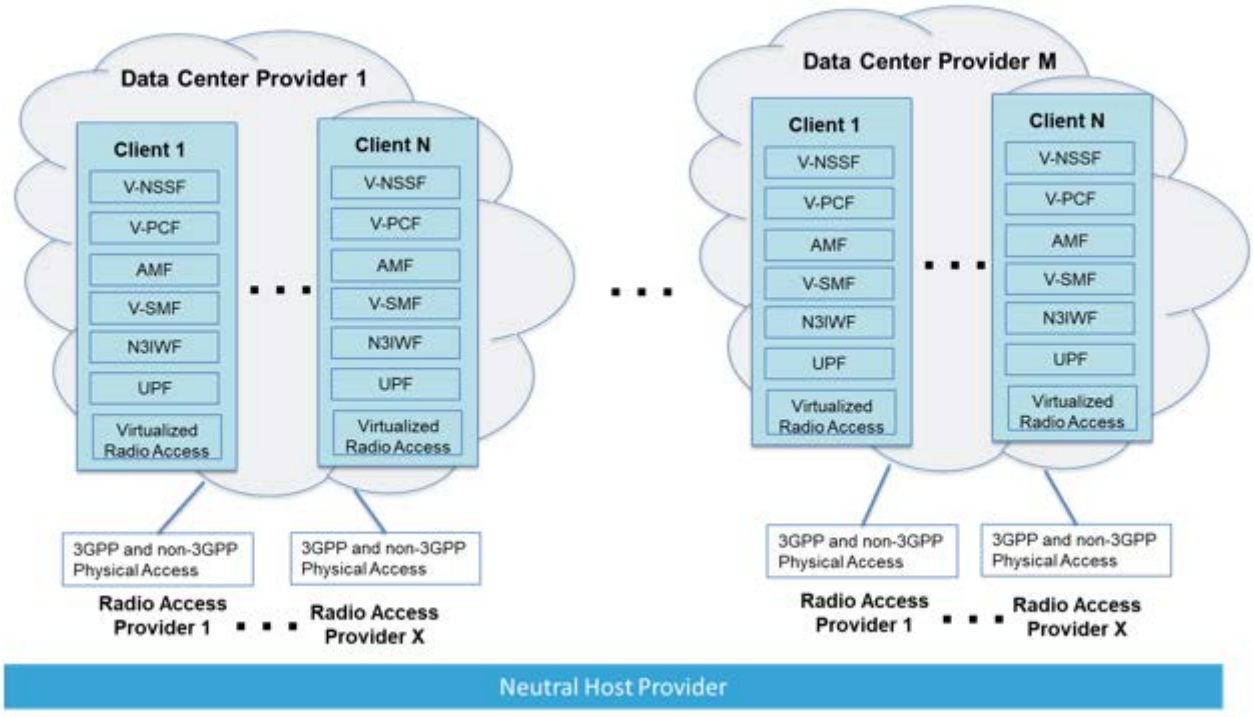

Figure 5.4 - Cloud Virtualization Neutral Host Architecture

Advantages of cloud/virtualization neutral host architectures include:

- More flexible and cost-effective deployment options since the neutral host entity can take advantage of existing nearby datacenter facilities as well as existing physical radio assets in the covered area.
- Client operators have more flexibility in utilizing their own VNFs even within the neutral host network.
- All of the advantages of NFV/Virtualization can be applied to the neutral host environment.

5.5 Hot Spot 2.0 (HS 2.0)

Hotspot 2.0 is a set of capabilities, specified by the Wi-Fi Alliance, that enables Wi-Fi devices to more seamlessly and securely connect to Wi-Fi services when a device enters a Hotspot 2.0 coverage area. Hotspot 2.0 is based on the IEEE 802.11u standard, which is a set of protocols published in 2011 to enable cellular-like roaming for Wi-Fi devices.

The Wi-Fi Alliance Passpoint® program provides certification for Hotspot 2.0 devices. Passpoint®-enabled networks eliminate public Wi-Fi log-in portals and browser redirects, providing automatic access to secure Wi-Fi networks using a Passpoint® profile stored on a device. Instead of the typical Wi-Fi portal splash screen, Passpoint®-enabled networks use 802.1x to authenticate users onto WPA2 encrypted connections, providing enhanced access security as compared to the portal-based Wi-Fi access.

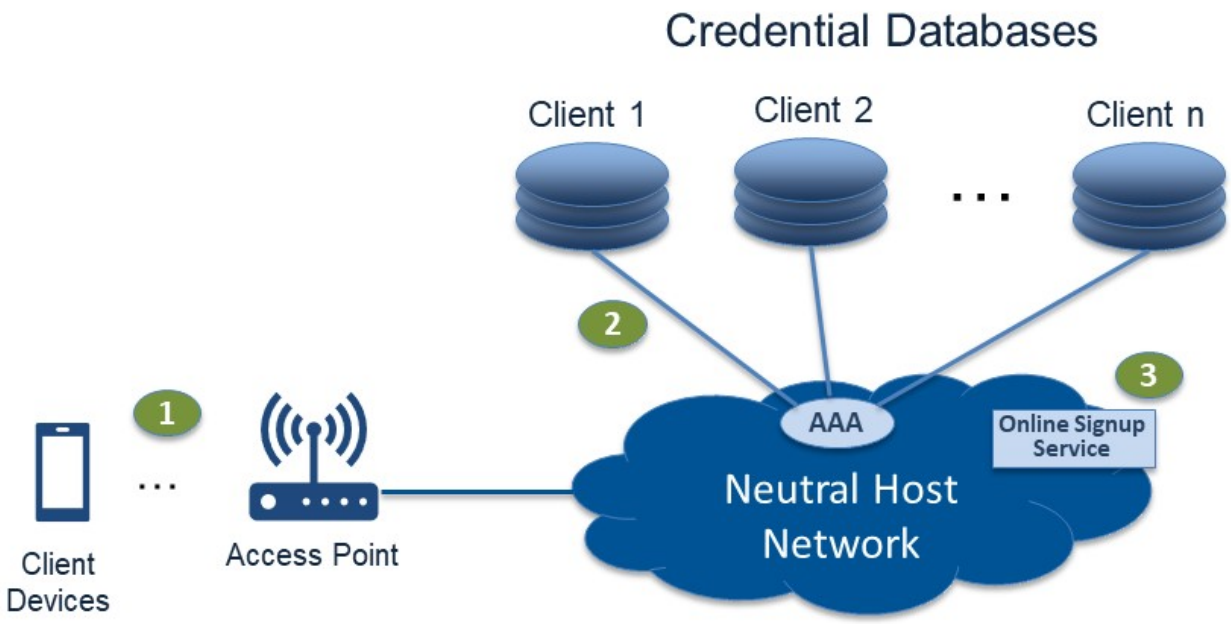

Figure 5.5 - Neutral Host Hotspot 2.0 Architecture

Hotspot 2.0 can be used with a neutral host provider as follows:

1. First, the client device and neutral host access point (AP) exchange information prior to association using Access Network Query Protocol (ANQP). (Specifically, a Hotspot 2.0 indication element in the APs beacons and probe responses will tell the client that Hotspot 2.0 is supported. The client then sends an ANQP query to the AP and the AP responds with the set of client service providers supported for authentication (e.g., the neutral host provider and supported client network operators) along with the Online Signup services available.
2. The client then checks to see if it possesses a credential for the neutral host provider or any of the supported client networks, and if so proceeds to associate and then authenticate using 802.1X and a provisioned credential. The neutral host network would utilize the appropriate client credential databases in the client network to support this authentication step. Hotspot 2.0 supports a wide variety of credentials including SIM/USIM cards, X.509 certificates and username/password pairs along with the appropriate EAP type.
3. If the client does not have credentials, it may utilize one of the listed Online Signup services to acquire credentials. No additional steps are required if the device already has SIM/USIM based credentials to access client networks associated with the neutral host as these credentials would also likely be supported for Hotspot 2.0 authentication.

Hotspot 2.0 release 2 provides mechanisms to provision credentials into the device when needed. In addition, Hotspot 2.0 supports a number of device management functions for credentials including:

- How they are provisioned,
- How they are stored on the device,
- How they are used in network selection, and
- How long they are valid.

The Open Mobile Alliance's Device Management (OMA-DM) framework is used to provide a standardized XML tree structure to support provisioning and management of credentials using a new PerProviderSubscription Management Object (PPS-MO). Use of Hotspot 2.0 with Passpoint®-enabled neutral host networks can greatly simplify Wi-Fi support and integration for many different Neutral Host solution architectures.

5.6 Voice Services in Neutral Host Environments

Most Neutral Host use cases considered in this document focus on data-oriented services and therefore assume that voice services are provided via a VoIP system such as IP Multimedia Subsystem (IMS). 3GPP architecture specifications define three different IMS roaming configurations that may be applicable to neutral host deployments. These configurations are provided in more detail in section 5.4 of 3GPP TS 23.221 and include:

1. A model where the UE has obtained IP connectivity from the Visited Service Provider's network (the neutral host) for IMS services and the Visited Service Provider's Proxy-Call Session Control Function (P-CSCF) is used to connect the UE to the home (hosted client) IMS. In this model, the P-CSCF function is provided by the visited (neutral host) provider which utilizes an IMS/SIP interface to the home (hosted client) network. The IP address for the IMS APN is anchored in the visited/neutral host network.
2. A model where the UE has obtained IP connectivity from the visited (neutral host) provider network and the home (hosted client) Service Provider provides the IMS functionality including the P-CSCF.
3. A model where the UE has obtained IP connectivity from the home (hosted client) Service Provider's network which then provides the IMS functionality.

The choice as to which model should be used in a neutral host environment will depend on the unique requirements associated with the neutral host deployment environment as well as the hosted client's processes and requirements. This choice will also affect hand-over requirements between the neutral host and client networks as UEs enter and exit the neutral host coverage area since the choice affects IP session continuity needs.

A variation of Model 2 above is commonly used for Wi-Fi calling in today's networks. In this configuration, the UE attaches to a non-3GPP (untrusted) network and acquires an IP address associated with this network. In neutral host scenarios, the non-3GPP network would be managed by the neutral host provider. The UE then creates an IPsec security association between the UE VoIP IMS client and an evolved packet data gateway (ePDG), essentially tunneling through the untrusted neutral host non-3GPP network. The ePDG then provides access to the IMS APN in the client network to enable IMS Voice and related services to the UE.

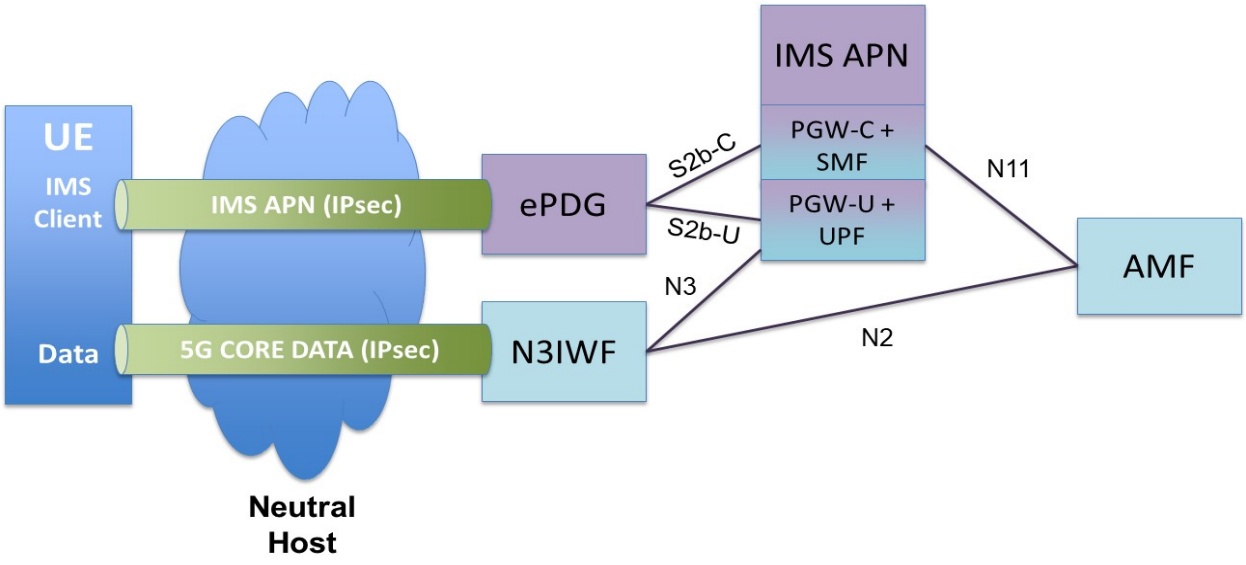

Figure 5.6 - Neutral Host Voice Architecture

The details of the interfaces between the UE and the Evolved Packet Data Gateway (4G) (ePDG), and between various EPC nodes is documented in 3GPP TS 23.402. Interworking between an ePDG connected to an EPC and the 5G Core network is described in 3GPP TR 23.501, Section 4.3.4.

The figure above also shows how the UE may similarly create an IPsec Security Association to an N3IWF for data services into a 5G core network.

An advantage of this configuration for neutral host scenarios is that Wi-Fi calling along with support for handover procedures are well understood.

More information relating to IMS roaming can be found in the GSMA document IR.65 titled “IMS Roaming and Interworking Guidelines”. This is a non-binding GSMA reference document that introduces guidelines for the usage of inter-Service Provider connections in the IMS environment, and requirements that IMS has for the Inter-Service Provider IP Backbone network.

6 Spectrum Considerations

6.1 Neutral Host in Licensed Spectrum

A neutral host may operate in licensed spectrum with agreement of the license holder. Scenarios involving use of shared and unlicensed spectrum are addressed in sections 6.2 and 6.3.

6.2 Neutral Host in Shared Spectrum (e.g., US 3.5 GHz CBRS)

6.2.1 Description

A neutral host small cell network in shared spectrum allows for cost-effective network sharing with Commercial Mobile Service Providers (CMSPs). An example of shared spectrum is the CBRS established by Federal Communications Commission (FCC) for shared wireless broadband use in 3550-3700 MHz band (3.5 GHz Band) in the U.S.

For the 3.5GHz bands there will be 3 tiers of users:

- Incumbent users: Highest priority, other users must vacate channel for incumbent users:
    - Federal users (e.g., Navy), Fixed Satellite Service, grandfathered terrestrial wireless ops for short time.
- Priority Access Licensees (PAL) users:
    - Each licensee can get up to 4 channels (40 MHz) in one licensing area which is a census tract.
        - License term is for 3 years, and can be renewed for 3 more years with no guaranteed renewal.
    - In one licensing area, up to 70 MHz can be licensed.
- General Authorized Access (GAA) users:
    - Can use any channel not used by incumbent or PAL users.
    - Potentially up to 80 MHz available for GAA users even if all 7 (70 MHz) PAL channels are awarded and deployed.

The Spectrum Access System (SAS) coordinates channel access, and needs channel usage information from incumbent, PAL and GAA users.

Various network architectures are possible to deploy neutral host in shared spectrum, including Roaming, Multi Operator Core Network, DDAS, Cloud RAN or Self-contained architecture (as described in detail in Section 7).

6.2.2 Advantage of Neutral Host in Shared Spectrum

Traditional small cells solutions need separate deployments for each wireless provider. The neutral host small cell solution offers a simple, low cost, venue/enterprise owners-led deployment option providing service to subscribers of multiple wireless service providers. Because these neutral host small cell networks operate in neutral spectrum, there is no need to coordinate Radio Frequency (RF) network planning with a mobile network operator’s macro

network. This solution also provides Wireless Wide Area Network (WWAN) grade of coverage, and service quality that is not provided by unlicensed technologies such as Wi-Fi. This also has the advantage of evolution paths comprising of LTE variants (e.g., MulteFire (see [MulteFire])).

6.2.3 Limitations of Neutral Host in Shared Spectrum

The wide scale adoption of a neutral host shared spectrum solution is dependent on availability of neutral spectrum (i.e., spectrum that is not used by one of the participating mobile network operators). However, recently there is a move in the industry towards tiered spectrum opportunities such as 3.5GHz in the U.S. The 3.5GHz (3550-3700 MHz) spectrum is well suited for deployments by third parties because of the lightly licensed regulatory approach adopted by the FCC.

6.3 Neutral Host in Unlicensed Spectrum

6.3.1 Description

Enterprise and even residential deployments of unlicensed technologies such as Wi-Fi are widespread, in-building, and increasingly outdoors. This use case leverages the ubiquity of this already extant technology to provide transparent or nearly transparent connectivity to customers of neutral host client operators, with minimal changes to existing radio resources. The neutral host may contract directly with client neutral host service providers to establish this capability via open Service Set Identifiers (SSIDs) or may leverage more general registry and authentication mechanisms (such as Hotspot 2.0).

Another technology option in the 5GHz unlicensed spectrum is MulteFire, which brings LTE-like performance with Wi-Fi-like simplicity. The MulteFire specifications are being developed by the MulteFire Alliance based on 3GPP standards. Wi-Fi and MulteFire will coexist in the 5GHz unlicensed band that offers global neutral spectrum.

6.3.2 Advantage of Neutral Host in Unlicensed Spectrum

The primary advantage of an unlicensed neutral host solution is that networks in unlicensed spectrum are already nearly ubiquitously deployed in-building, and there are minimal changes to existing networks and user devices required to provide service to customers of neutral host client service providers. Since these networks operate in unlicensed spectrum, there is no need to coordinate RF network planning with a client operator's macro network, and interference with an existing licensed macro network is non-existent.

MulteFire brings LTE-like performance (e.g., enhanced capacity and range, enhanced mobility and QoS) to 5GHz unlicensed spectrum deployments.

6.3.3 Limitations of Neutral Host in Unlicensed Spectrum

The primary limitation of an unlicensed solution is that use of unlicensed spectrum is not controlled as tightly as licensed spectrum, resulting in the possibility of uncontrollable and/or unexpected interference. In many in-building venues, this has not proven to be a problem, since the unlicensed network operator has control of the physical premises in which the network is deployed and is able to control interference acceptably well. (If that were not the case, unlicensed networks would not enjoy the ubiquity they do today.) A second caveat, not really a limitation, is that—as is the case for the other neutral host use cases—a separate pairwise agreement may be required for each neutral host client and neutral host operator. However, mechanisms such as Open SSID (established by the Cable Consortium), and Hotspot 2.0 (marketed as Passpoint® by the Wi-Fi Alliance) overcome this limitation by establishing a network of participating Wi-Fi hotspots that can be accessed transparently by end-user devices, providing authentication and identity management.

7 Industry Solutions

7.1 Roaming

7.1.1 Description & References

From a technical point of view, the simplest means to provide a licensed spectrum neutral host solution is via inter-carrier roaming agreements. This can be implemented in several ways. One is that a spectrum license holder executes agreements with one or more prospective neutral hosts, providing the use of its spectrum and Enhanced Packet Core (EPC) network for use in those venues. Either the spectrum license holder or the neutral host then executes roaming agreements with other wireless service providers, allowing their customers' UEs to roam onto the license holder's network while in the neutral host venue. Either the neutral host or the spectrum license holder builds the necessary RAN infrastructure to provide service in the neutral host's venue. UEs entering the neutral host venue roam onto the spectrum license holder's network following the same rules applied for other roaming scenarios (i.e., the spectrum license holder's network is treated as a visited network).

Another way that roaming can be employed to realize a neutral host solution is for a prospective neutral host to execute an agreement with a spectrum license holder that does not operate its own EPC network. In this case, the neutral host may operate the RAN and the EPC and would act as the "visited network".

Neutral host solutions utilizing roaming standards have a number of unique aspects that affect the deployment of the solution. These differences can often result from the environment that neutral host solutions are often deployed where:

- Coverage areas are often very limited (e.g., a venue, campus or building).
- The number of roaming partners / hosted clients may be small (e.g., limited to providers offering services in that area).
- The hosted clients likely have local (home) facilities improving the performance of home routed services as compared to typical International roaming scenarios.
- Neutral Host solutions may be deployed in a potentially large number of independent sites (e.g., venue, campus or building locations) with many different neutral host providers.

These deployment attributes may affect capabilities such as handover, PLMN-ID assignments, voice support/emergency services and charging when designing a neutral host solution based on roaming standards.

7.1.2 Handover Considerations

Commonly, roaming is supported for both homes routed and local breakout network architectures. In home routed roaming:

- For 4G architectures, the RAN, MME and SGW are in the visited (neutral host) network while the PGW is in the home network.
- For 5G Core Network architectures, as shown in Section 5.1.1, the NG-RAN, AMF, SMF and UPF are in the visited (neutral host) network while the home network has its own SMF and associated UPF to provide IP anchor services.

For local breakout architectures, the IP address of user plane sessions is anchored in the visited (neutral host) network. However, in many neutral host use cases, the hosted client (typically a mobile network service provider) will want to utilize the home routed architecture for at least some of its services in order to support hosted client specific user plane services for their subscribers. In addition, since the mobility sessions are anchored in the neutral host (visited) network in local breakout scenarios, the call would drop as the UE moves out of Neutral Host coverage. This may not be a concern for many data applications since session continuity can often be provided at the application layer (e.g., using HTTP cookies). Nevertheless, we would fully expect to see the home routed architectures utilized in Neutral Host environments for many services, particularly where handover is an important service requirement.

Handovers from the Neutral Host network to the home network (e.g., as the UE moves out of the venue), will require support for network-based handover procedures which involve relocation of core control plane and user plane functions. For example:

- In 4G systems, the neutral host MME and SGW would need to be relocated to a home network based MME and SGW. The specific procedure can be found in 3GPP TS 23.401 section 5.5.1.2.2.
- In 5G systems, the neutral host AMF, SMF and UPF would need to be relocated to home network-based AMF and UPF (controlled by a home SMF). The specific procedure can be found in 3GPP TS 23.502 section 4.9.1.3.

These handover procedures cross entity boundaries and may require additional networking support, coordination and testing (e.g., the neutral host MME/AMF will need to communicate with the home network MME/AMF). In addition, core network relocation procedures tend to be slower and less efficient than direct base station to base station handover procedures.

7.1.3 PLMN-ID Assignments and Potential for Exhaust

Neutral host operators using a roaming model that do not own licensed spectrum and do not have their own radio access network may operate as a MVNO. In this case, the neutral host operator as an MNVO would be assigned a unique Public Land Mobile Network – Identifier (PLMN-ID). These identifiers consist of a 3-digit Mobile Country Code (MCC) and a 2- or 3- Mobile Network Code (MNC). As such, the number of possible PLMN-IDs within a country is quite limited.

Nevertheless, other options exist that mitigate the need for the neutral host operator to have a unique PLMN-ID. For example, the neutral host operator could operate in hosted client spectrum while using the client's PLMN-ID in that spectrum. This may be enabled by wideband, software-defined radios that permit the Neutral Host to deploy a single radio/antenna system that supports multiple hosted clients' spectrum, but may also be supported with multiple, hosted client-specific radios. Another possible scenario is when the neutral host operates in a single licensed operator's spectrum, using that operator's PLMN-ID. In that case, the spectrum owner would need to have roaming arrangements with other hosted clients. PLMN-ID exhaust is a key factor in considering roaming based neutral host architectures. In practice, a Neutral Host roaming architecture would more likely be used by nation-wide Neutral Host providers to avoid the need for PLMN-ID assignments on a per site or small region basis.

7.1.4 Charging

Charging interfaces will be required between the neutral host (visited) network and the hosted client (home) network entities. Section 5.3 describes the traditional charging model used in today's roaming scenarios. However, as noted above, neutral host solutions differ in many ways from traditional roaming. Relative to charging, neutral host solutions may not need to deal with international tariff issues, different tax requirements or monetary exchange rates. As such, new more efficient, real time charging methods should be explored for neutral host scenarios. For example, Section 5.3 discusses the potential to use Distributed Ledger Technologies (DLT) for charging.

7.2 Multi-Operator Core Network (MOCN)

7.2.1 Description & References

The MOCN solution is standardized by 3GPP. The requirements are documented in [22.951] and the 3G/4G solution is defined in [23.251]. In 3GPP Release 15, specification 23.501 describes the 5G multi-operator core network (5G MOCN) sharing architecture in Section 5.18.

The MOCN standard is a general approach to allow several operators with different core networks to share common RAN nodes. Though MOCN does not specifically target neutral host scenarios, MOCN could be used as a basis for a neutral host platform.

Each cell in the neutral host network will provide, in broadcast system information, the PLMN-IDs of the client network operators in the shared network. When a UE performs an Initial Registration to a network, one of available PLMNs can be selected by the UE for service and the UE then informs the (NG)RAN of the selected PLMN so that the neutral host network can route correctly.

The figure 7.2.1 shows an overview of the MOCN solution as applied to neutral host. Though MOCN can support GSM EDGE Radio Access Network (GERAN), Universal Mobile Telecommunications System (UMTS), LTE and 5G services, this discussion will focus on the case of MOCN applied to LTE and 5G. As shown in the diagram, the neutral host provides a shared LTE eNodeB or 5G gNodeB and associated radio equipment. The MOCN standard allows this (e/g)NodeB to be connected to more than one core network belonging to different hosted clients. The (e/g)NodeB broadcasts the identity of all core networks it is serving. Using standard procedures defined by 3GPP the UE will automatically select the MOCN (e/g)NodeB if it serves its home network. Using MOCN procedures, the (e/g)NodeB will route communications from the UE to the correct core network.

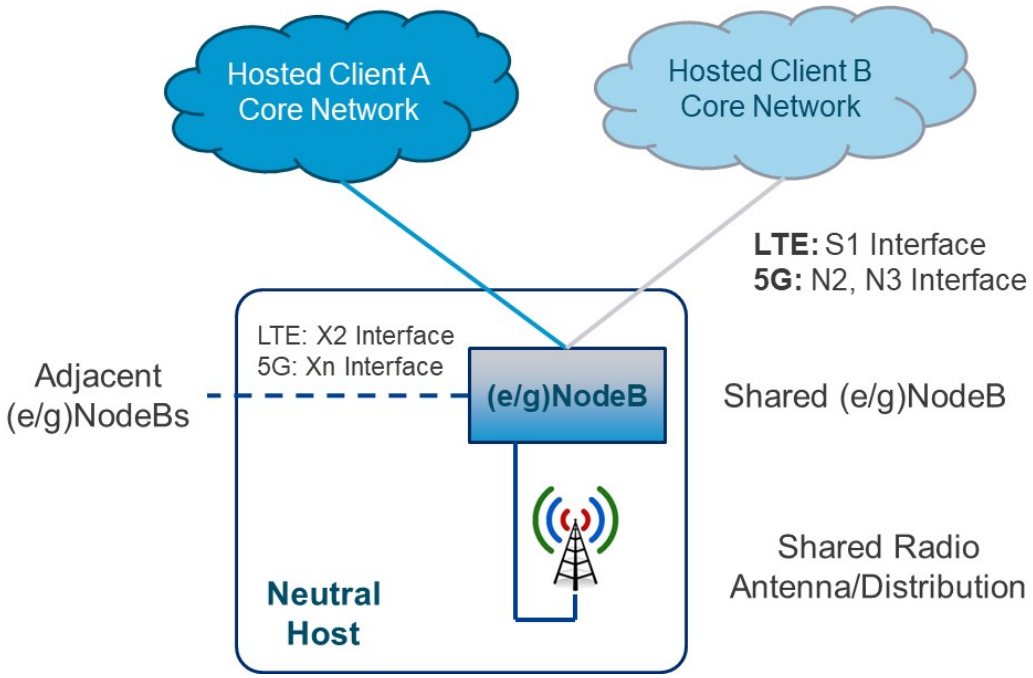

Figure 7.2.1 – Overview of MOCN for an 5G/LTE Neutral Host

7.2.2 Deployment Issues

MOCN is only standardized for 3GPP networks and radio technologies. Hosted clients must support a 3GPP core network and must have issued users with Universal Integrated Circuit Cards (UICCs) containing 3GPP subscription information and security credentials.

The use of MOCN requires a suitable SLA to be formed between the neutral host and the hosted clients. As well as addressing policy aspects, this SLA must make technical provisions for connection of the neutral host's eNodeB to the client core network via the S1 or N2/3 interfaces. Deployment of this interface will require both parties to work to ensure technical integration and interoperation.

In operation, the MOCN neutral host requires access to certain hosted client-specific information. For example, the neutral host must be able to communicate the appropriate list of adjacent cells for each hosted client.

7.2.3 Spectrum, Radio Coverage, & Radio Capacity Issues

The radio interface for a MOCN solution will typically operate in spectrum owned by one or more of the hosted client networks. The neutral host must form an agreement with its hosted clients to gain access to such spectrum. The MOCN standard does not specify how spectrum is divided between hosted clients. Therefore, it is up to the neutral host to agree upon a policy with their clients for the spectrum to be used. Possibilities include each client network operating in its own spectrum or all client networks sharing the same spectrum. Another possibility is to use neutral spectrum (e.g., 3.5GHz spectrum) in the U.S. which may be well suited for MOCN deployments.

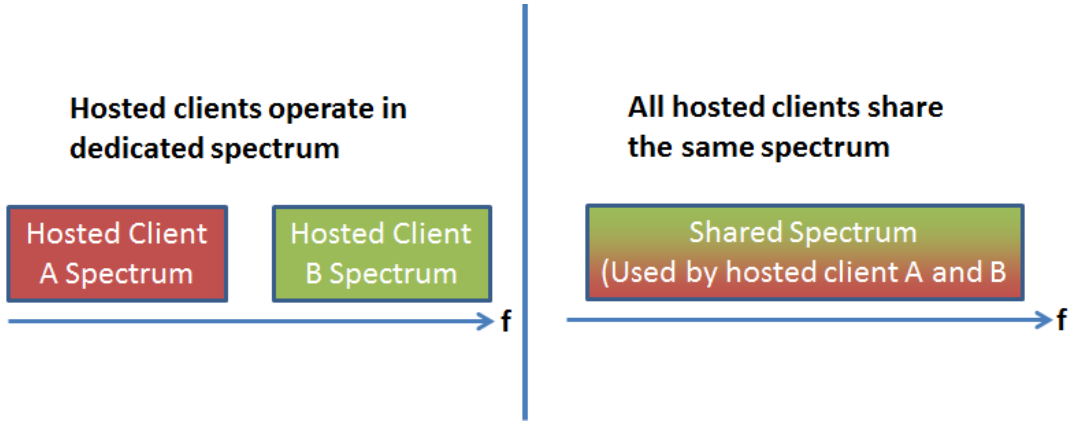

Figure 7.2.3-1 – Example Approaches to Spectrum Management in MOCN

Prioritization and management of traffic on the radio interface and for other limited resources is also not standardized in MOCN. The (e/g)NodeB is responsible for enforcement of policy which must be agreed between the neutral host and each hosted client. Possibilities include fixed resource reservations for each client, completely shared resources for all clients, or combined approaches that support a mixture of reserved and shared resources.

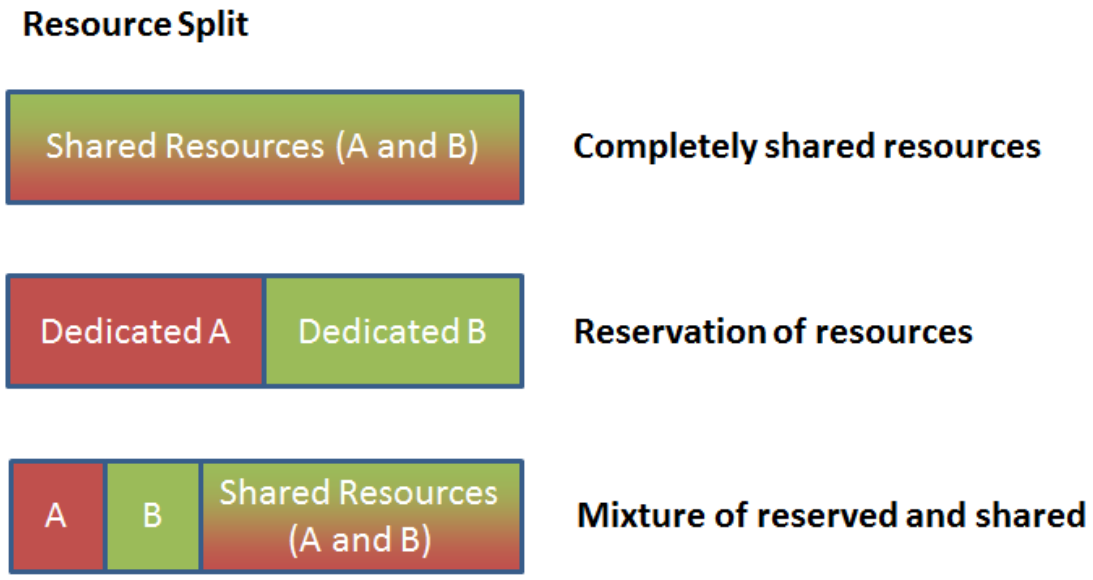

Figure 7.2.3-2– Example Strategies for Resource Management in MOCN

Arrangements will need to be made with each hosted client to support mobility in and out of the neutral host's coverage area. This will require specification of appropriate radio parameters and possibly connectivity between (e/g)NodeBs via the “X2/Xn” interface.

7.2.4 Network Issues

S1 and/or N2/3 connectivity is required between the Neutral Host and each client Core Network. This may require support of multiple IP Virtual Local Area Networks (VLANs) by the neutral host with flexibility to support different configurations and routing behavior for each client network. Security of the IP networks between the neutral host and the different hosted clients should be considered.

If the X2/Xn interface is supported to other base stations, then similar network flexibility is also required to support connection to adjacent dedicated (e/g)NodeBs belonging to different hosted clients.

7.2.5 Broadcast Services

For services that use information broadcast by the eNodeB, 3GPP specifications do not support separate broadcasts for each MOCN hosted core network. Therefore, special non-standard arrangements and coordination of broadcast information between hosted core networks may be required. This issue is of particular concern relative to the support of Commercial Mobile Alert System (CMAS)and Cell Broadcasting Service in 2G and 3G (CBS) systems that provide public warning services to users. As such neutral host solutions utilizing MOCN should consider any regulatory requirements associated with deployment of the solution.

7.2.6 Other Operational Issues

The neutral host must capture all information needed for charging of hosted clients and for SLA verification. MOCN standards have not defined the contents of this data or how it should be exchanged between the neutral host and the hosted clients.

3GPP specifications allow for up to six PLMN identifiers (operators) in an LTE MOCN arrangement. Neutral host solutions using MOCN would then be limited to 6 different client networks.

7.2.7 Evaluation

The MOCN solution is very compatible with hosted clients and devices that support 3GPP specified technology in licensed spectrum.

The basic functions needed to support neutral host are specified by 3GPP which should help with the design and integration of such systems. Standardization should also ensure a good user experience as normal 3GPP procedures are extensively reused. In concept, particularly for LTE and 5G, the MOCN neutral hosts are technically straightforward. However, the 3GPP standards do not specify how important operational requirements are to be realized; for example, how policies and SLAs can be defined and validated and how spectrum should be managed in MOCN neutral hosts. Therefore, neutral hosts will need to develop their own solutions for these aspects.

7.3 Distributed RAN Solutions for Neutral Host

The cost of deploying and operating a neutral host solution can be reduced by disaggregating the functions normally associated with a wireless base station (eNodeB, gNodeB), and by centralizing some of those functions. The centralized functions can be located remotely, serving multiple RF resources, and may be virtualized and operated in the cloud. There are several different ways that the base station functions may be split, each of which has certain advantages and disadvantages from a cost and performance perspective, and in terms of the extent to which the solution can be virtualized.

3GPP TR 38.801 presents the framework for naming and analyzing the options for splitting the processing between the radio edge and a resource pool.

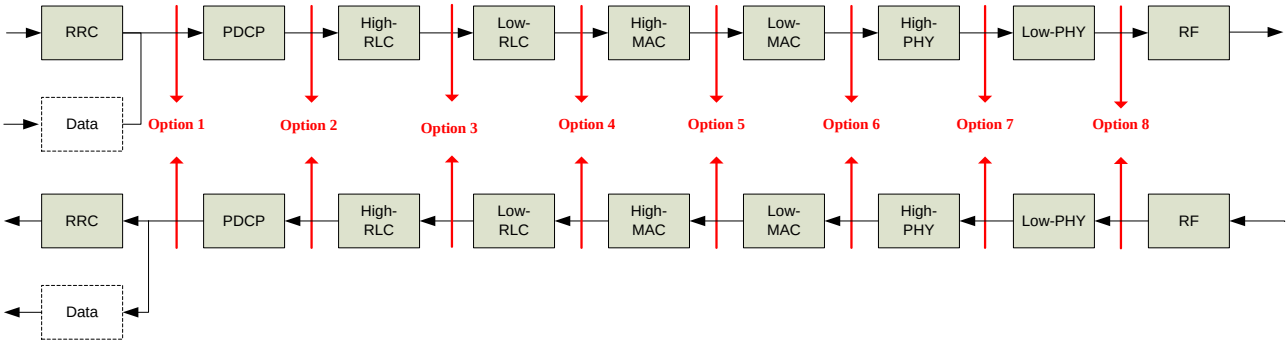

Figure 7.3: RAN Splitting Options Presented in 3GPP TR 38.801

The splits are characterized as Higher Layer Split (HLS) 1-5, and Lower Layer Split (6-8). In general, the lower numbered options (i.e., the higher layer splits) require the least transport bandwidth, are the least costly to deploy and operate, and are most easily virtualized, while the higher numbered options require the most transport bandwidth, are higher cost, and provide the best performance in terms of support for features such as multi-cell RF coordination. The HLS options can be supported over higher latency transport links (>1ms), while the LLS require low latency links (<1ms), in order to support hybrid ARQ (HARQ) and multi-cell RF coordination (COMP).

The options that have received the most attention and have been studied and elaborated to date are Options 2, 6, 7, and 8. Others, such as Split Media Access Control (MAC) solutions (Option 5) have been implemented in proprietary solutions, but have not been widely adopted and are still being studied with the aim of standardizing them. The following sub-sections discuss the more well-defined/studied options.

7.3.1 DDAS Neutral Host (Option 8)

A traditional Distributed Antenna System, or DAS, is a network of spatially separated antenna nodes connected to a common source using appropriate transport facilities. Typically, DAS systems are deployed in the same types of environments appropriate for Neutral Host solutions. A common DAS deployment architecture might be comprised of:

- Antennas spatially distributed across the venue, campus or building complex;
- Connected via network facilities to;
- A common point where the base stations of the various client operators are located and used to drive the antenna system.

In most conventional DAS deployments, passive RF components such as coaxial cable, splitters, taps and couplers are used to distribute signal from the base stations to the various antennas distributed across the coverage area.

However, new DDAS deployments are leveraging a Remote Radio Head (RRH) at the antennas to enable baseband signals from a base station to be distributed using Common Public Radio Interface (CPRI) or packet (e.g., Ethernet/IP) distribution technologies. The use of standard digital/packet-based transport technologies to connect an Antenna/RRH to a base station opens the way to more flexible base station deployment options.

In an Option 8 DDAS deployment, the CPRI transport link between the centralized Physical (protocol layer) (PHY) processing and the RRH can be costly, requiring <1ms latency and 50 GB/s bandwidth to support a 400MHz 5G radio.

The concept of DDAS can be extended to apply to other RAN splits For example, Cloud RAN techniques (described in more detail in a following section) can be deployed to enable a neutral host DDAS system to leverage virtualized RAN resources provided by the host client operators or by the DDAS operator themselves.

Indeed, DDAS technologies can be used with a number of different neutral host solutions in a hybrid fashion to take advantage of a distributed antenna architecture driving an (e/g)NodeB and mobile packet core-based roaming or MOCN neutral host solution.

7.3.2 Split-Phy Open RAN (Option 7)

3GPP has identified 3 variants of the Option 7 PHY-layer split, the details of which are described in TR 38.801 and are beyond the scope of this paper. The O-RAN Alliance has created an architecture which includes the use of Option 7-2x split between the O-RU (O-RAN Radio Unit) and the O-DU (O-RAN Distributed Unit), which is between the 3GPP-defined Option 7-2 and Option 8 interfaces and offers advantages over both. In particular, 7-2x requires less bandwidth and imposes less stringent latency constraints than the Option 8 (CPRI) split typically used by DDAS. This architecture allows virtualization of the higher layer functions while still providing good performance for many advanced RF features. It also has the advantage of permitting a multi-vendor solution. The O-RAN architecture is shown in Figure 7.3.2-1.

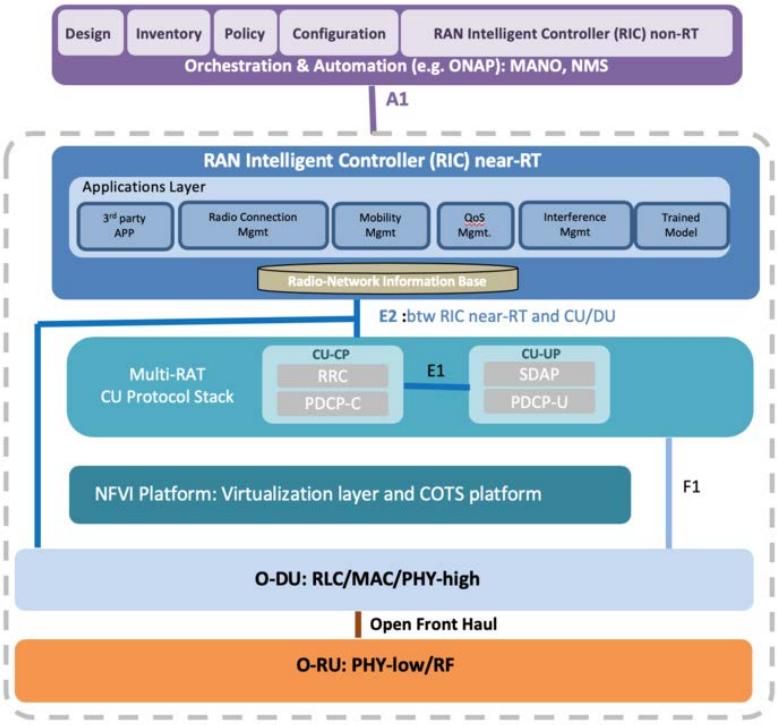

Figure 7.3.2 – O-RAN Reference Architecture[8]

7.3.3 MAC/PHY Split (Option 6) and the application to Cloud RAN

The Small Cell Forum (SCF) has focused on creating a virtualized, multi-vendor architecture to support het-net and neutral host deployments that use an Option 6 split between the MAC and PHY layers. This split permits less stringent latency constraints and requires less bandwidth than the higher numbered options. This architecture can be used to create a Cloud RAN.

The Small Cell Forum defines the Network Functional Application Programing Interface (nFAPI)[9] to support the MAC/PHY split. Figure 7.3.3-1 shows a Cloud RAN solution built on the SCF architecture. The key elements in the architecture include:

[8] Open RAN Alliance: https://www.o-ran.org/

- Broadband/multi-band intelligent radio heads are deployed in the venue of interest. These radio heads support multiple bands across the entire defined bandwidth of each band with an Ethernet friendly interface to a centralized baseband and control unit and can then be configured to segment the baseband content onto separate Ethernet streams for each specific band or sub-band of interest back to the central unit. The baseband unit deployment and operational management would be via the neutral host. Management would include such activities as radio head fault management, configuration management, accounting/charging management, security management, and necessary resource management of shared resources.
- The broadband/multi-band radio heads communicate with a more centralized baseband processing and control unit via nFAPI interface. The nFAPI extends the Functional API (FAPI) multi-vendor platform interface to support a virtualized small cell architecture. The nFAPI supports a virtualized MAC/PHY split enabling the use of standard Ethernet LAN technologies to connect baseband and control processing to a new "intelligent" radio head avoiding the need for direct fiber interfaces.
- A demarcation point separates the neutral host managed aspects from the hosted client aspects of the solution.
- The neutral host managed aspects include the radio heads along with the Ethernet LAN connection to a physical point of demarcation. Additionally, the neutral host provider may provide a centralized virtualized server infrastructure that terminates the Ethernet streams from the radio heads and provides basic routing and security functions as required.
    - This virtualization infrastructure could be centralized in an enterprise or in a network location that serves multiple venues and enterprises for a neutral host provider.
    - This virtualization infrastructure supports Network Function Virtualization (NFV) and as such, allows the neutral host to instantiate virtual baseband units to support all operators/vendors participating in the neutral host solution. Ideally, the neutral host provider supports inter-administrative domain NFV as being studied and defined in the ATIS NFV Forum to allow operators to dynamically order and have instantiated baseband and control VNFs in a venue as needed.
- Hosted Client aspects can include the hosted client's own baseband and control processing function, either as a physical function, a VNF in the hosted client's data center or a VNF specified and managed by the Hosted Client but instantiated in the neutral host's virtualization infrastructure.

The solution also supports native enterprise Wi-Fi for the enterprise use.

Effectively, this arrangement allows any hosted service provider that supports the deployment of a virtual baseband VNF to then instantiate that VNF in the target neutral host system and access its own spectrum deep within the enterprise facilities that may otherwise not be available.

---

[9] Small Cell Forum Press Release: http://www.smallcellforum.org/press-releases/small-cell-forums-nfapi-will-make-virtualized-hetnet-reality/ >.

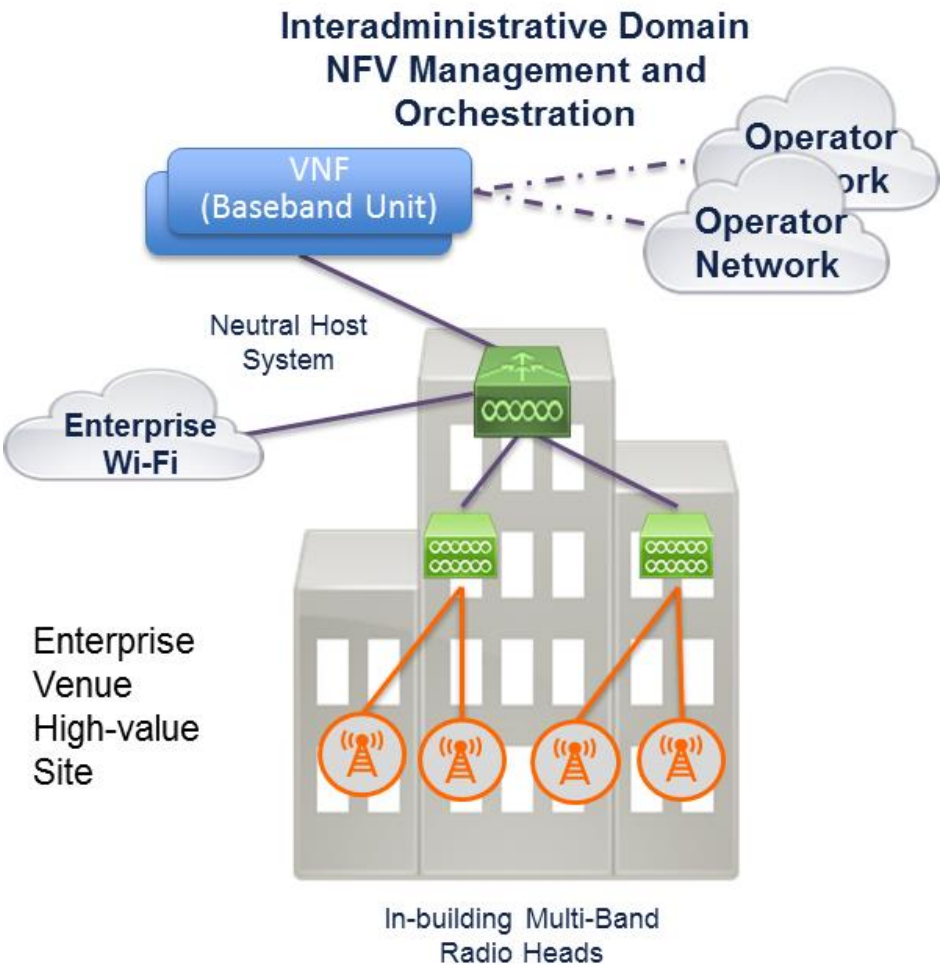

Figure 7.3.3 – Cloud RAN Neutral Host Solution based on Option 6 (MAC/PHY) split

7.3.4 PDCP/RLC Split (Option 2)

The high layer splits offer the lowest cost from a deployment and operational point of view, and require the lowest transport bandwidth relative to the lower layer splits. 3GPP selected the Option 2 split as the preferred High Layer Split (HLS) for study and standardization. This work is documented in 3GPP standard TR 38.806.[10]

In this split, the e/gNodeB functionality is divided into a Central Unit (CU) and a Distributed Unit (DU), where the CU contains the RRC, PDCP, and SDAP functions, and the DU contains the RLC, MAC, and PHY functions. While Option 2 requires much less bandwidth than the lower layer splits, the higher latency, particularly in the control plane, can make it impossible to perform some of the more advanced radio functions that require lower latency and more coordination. For this reason, 3GPP studied three different configurations for Option 2, involving splitting the control plane (CP) and user plane (UP). The three configurations discussed in TR 38.806 are:

- Scenario 1: Centralized CU-CP and CU-UP
- Scenario 2: Distributed CU-CP and Centralized CU-UP
- Scenario 3: Centralized CU-CP and Distributed CU-UP

Each of the scenarios has advantages and disadvantages in terms of cost and advanced RF and coordination feature support.

---

[10] 38.806 - Study of separation of NR Control Plane (CP) and User Plane (UP) for split option 2

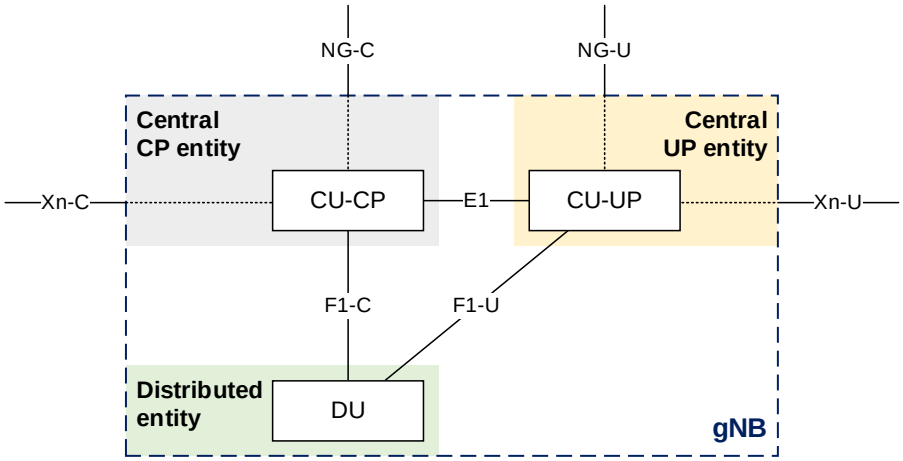

Figure 7.3.4-1: CU-CP and CU-UP centralized

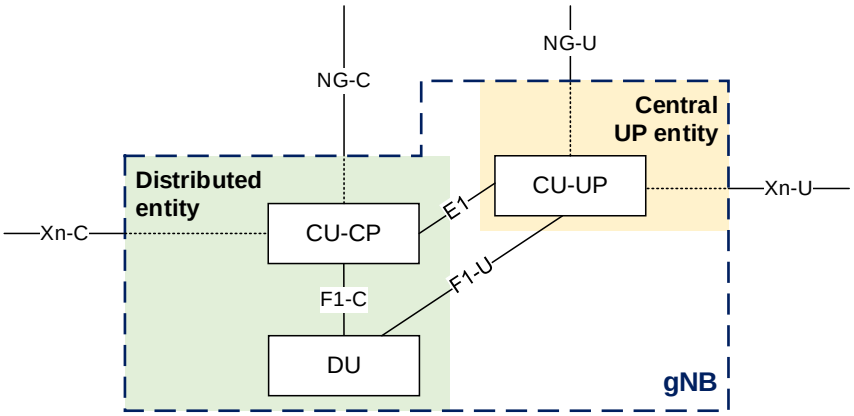

Figure 7.3.4-2: CU-CP distributed and CU-UP centralized

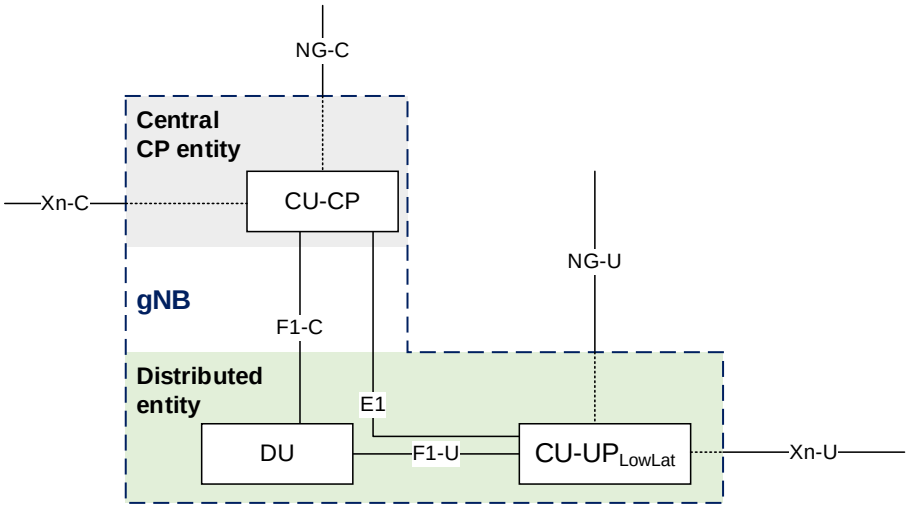

Figure 7.3.4-3: CU-CP centralize and CU-UP distributed

7.3.5 Spectrum, Radio Coverage & Radio Capacity Issues

In this case, the hosted operator is using its own (separate) licensed spectrum to provide service in the venue. As such, no new spectrum, radio coverage, or radio capacity issues exist other than the common issues associated with any licensed small cell radio system. It is of course highly desirable for the VNF baseband unit to support sufficient Self-Optimizing Network (SON) logic and algorithms to manage normal interference and hand-off issues that occur based on the physical deployment of the radio heads. Generally, the hosted operator has little control as to where the radio heads are deployed. Certainly, interference and handover performance will also depend on the specific band used. As such, this class of solutions may be challenged relative to interference and handover management in some situations. This may require close coordination between the hosted operators and the neutral host provider.

7.3.6 Other Operational Issues

In the stated solution, the hosted operator controls dedicated aspects of the radio heads but does not completely control the management or placement of the radio heads themselves. As such, operationally, the neutral host provider and the associated environment must somehow provide sufficient operational capabilities to enable the operator to properly manage its subscribers in the venue.

7.4 Neutral Host in Unlicensed Spectrum using Wi-Fi

7.4.1 Description and References

There are a number of neutral host solutions that can be deployed in unlicensed spectrum using Wi-Fi as the radio access technology. Some are already in widespread use; others are in various stages of development/deployment. The figure 7.4 illustrates an embodiment of Wi-Fi neutral host.

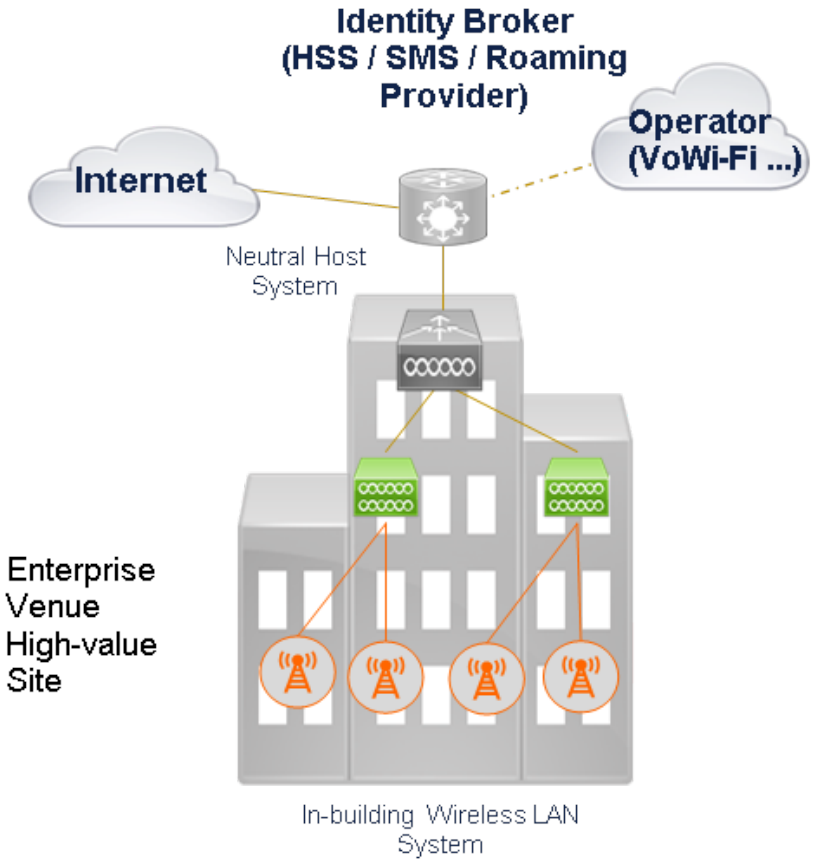

Figure 7.4.1 – Neutral Host Using Wi-Fi

A general description of the characteristics of a Wi-Fi neutral host solution is:

- The Wi-Fi neutral host system advertises the appropriate SSIDs for hosted clients. These may or may not be unique SSIDs for each hosted client.
- The neutral host system must broker and manage authentication with appropriate hosted operator's HSS. This may be accomplished using the mechanisms described in 3GPP 23.402 [23.402], section 4.2.2.
- Data services can be provided by the neutral host in two ways:
    - Via Wi-Fi and the neutral host's Internet Service Provider (ISP) in a data offload model, and may not necessarily incorporate the hosted client's policies, etc.); or
    - May be tunneled through an ePDG to route all data back to the hosted client's core network for the application of operator policies and charging rules.
- Voice services are provided via Voice over Wi-Fi (VoWi-Fi), tunneled to the hosted client's network.

Several embodiments are described below:

- Multi Service Set Identifier (M-SSID): In this embodiment, the Wi-Fi access point transmits multiple SSIDs, each potentially corresponding to a different neutral host client service provider network. The device attaches to the SSID corresponding to its home provider and authenticates transparently. This implementation requires the Wi-Fi Access Point (AP) to support multiple SSIDs.
- Cable Consortium Open Service Set Identifier (SSID): This case is similar to the previous one, except that an AP supporting multiple SSIDs is not required. Instead, a registry of participating neutral host clients is maintained, spanning many enterprise networks and APs. Identity management and authentication is provided by a central server. While this is conceptually simple, there are security concerns since traffic may be observed over the air. It will ultimately be replaced by the next example, HotSpot2.0.
- HotSpot2.0 (HS2): This mechanism, marketed as Wi-Fi Certified Passpoint® by the Wi-Fi Alliance, addresses many of the security issues of the Open SSID mechanism, but further security will be provided via WPA2 encryption of over-the-air traffic. An HS2-enabled device, upon entering an HS2 network, automatically joins the network without any user intervention. Support for billing based on tonnage, network loading, and user needs is supported.

7.4.2 Spectrum, Radio Coverage and Radio Capacity Issues

Neutral host WLAN solutions in unlicensed spectrum operate primarily in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band (802.11b, g/n, n), and in the 5 GHz band (802.11a/.h/j/n/ac). The ISM band is prone to interference, not only from nearby Wi-Fi networks, but also from other devices (e.g., microwave ovens, cordless phones) and can become very cluttered. While the 5GHz band is less cluttered with interferers, it does not propagate as well through obstructions. In practice, a well-designed Wi-Fi network for WLAN applications will also serve well as a neutral host network.

7.4.3 Network and Deployment Issues

From a deployment point of view, a neutral host solution can leverage an existing WLAN deployment, provided the WLAN was engineered to provide sufficient capacity for the traffic that client subscribers will bring. For the M-SSID solution, APs must be capable of transmitting multiple SSIDs.

7.4.4 Other Operational Issues

There are several challenges to an unlicensed neutral host solution:

- Emergency Location information: E-9-1-1 services via WLAN is being addressed by another ATIS effort.

- SMS Support: Non-IP based SS7 SMS is not supported, but SMS is supported via IMS SIP or other IP-based messaging services.
- Neutral host must support IPsec tunneling through Wi-Fi access network in order to support VoWi-Fi.
- Wi-Firesource allocation.

In addition to these, the same issues described for shared spectrum and Cloud RAN solutions apply (i.e., the client service provider does not control the management or placement of the APs). As such, operationally, the neutral host and the associated environment must somehow provide sufficient operational capabilities to enable the operator to properly manage its subscribers in the venue or must otherwise satisfy the operator that the user experience provided is sufficient.

7.4.5 Regulatory Issues

No new regulatory issues identified. E-9-1-1 services via WLAN is being addressed by another ATIS effort.

7.5 MulteFire Self-contained Neutral Host network

7.5.1 Description and References

A self-contained neutral host network architecture supporting multiple hosted client operators has been proposed by MulteFire Alliance [MulteFire]. At publication of this report, the details of the MulteFire solution were still being developed, and therefore this discussion is limited to a high-level description of the intended solution and its attributes.

The figure 6.6 shows the high-level self-contained neutral host network architecture. The neutral host can serve users from multiple hosted client operators. There is lightweight interworking between neutral host and the hosted client operators providing access to hosted client operator services (e.g., IMS voice) in neutral host coverage. The interworking framework leverages the WLAN interworking framework defined in 3GPP, and neutral host network connects to the hosted client operator's network using WLAN interworking interfaces. The UE can use ePDG (via SWu) to gain access to the hosted client operator's IP services.

There is also service continuity between the hosted client operator and neutral host for hosted client operator's services. Local IP services (e.g., enterprise Private Branch Exchange [PBX]) are provided by local breakout at neutral host. Neutral host networks complement the hosted client's networks, extend indoor coverage, and offload data. Offload of hosted client operator's UEs to the neutral host is controlled by hosted client operator's policies.

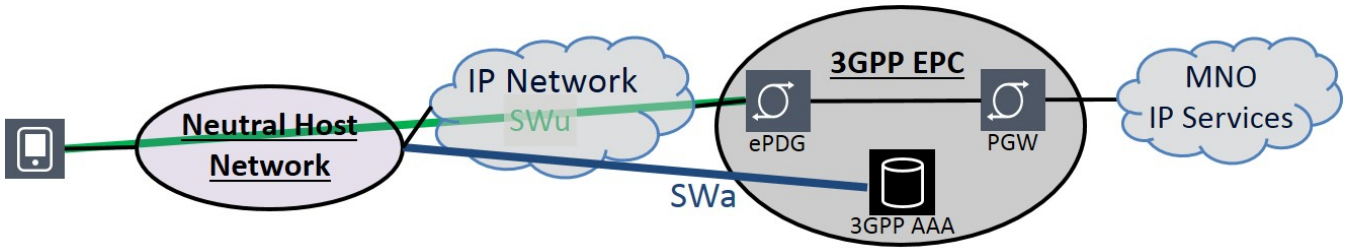

Figure 7.5.1 – Self-contained Neutral Host Architecture

7.5.2 Deployment Issues

Neutral hosts must support subscribers of multiple hosted client operators. These hosted client operators have SLAs with the neutral host for hosted client operator offload services using hosted client operator issued SIM cards. There is also a need to develop solutions for Key Performance Indicators (KPI) management and charging using existing industry standard interfaces.

7.5.3 Spectrum, Radio Coverage, and Radio Capacity Issues

For wide scale adoption of this neutral host solution, it is beneficial to have a neutral spectrum (i.e., spectrum that is not used by one of the Commercial Mobile Service Providers [CMSPs]).

The U.S. 3.5GHz spectrum is well suited for deployments by neutral host providers because of the lightly licensed regulatory approach adopted by the FCC and is generally less congested than the unlicensed spectrum.

7.6 Neutral Host in Shared Spectrum (CBRS)

The CBRS Alliance has defined the use of 3GPP LTE in a roaming based Neutral Host architecture, for use in the CBRS 3.5 GHz shared spectrum band. Since the LTE requires the use of 3GPP identifiers and since traditional 3GPP interworking is a valuable aspect of CBRS deployments, unique 3GPP identifiers (such as IMSI's and HNI/PLMN-IDs) are required to uniquely distinguish its service from other services. However, the existing identifier management structure may not support the large numbers of CBRS shared spectrum operators since potentially, each enterprise or venue with CBRS service could be an independent operator and thus requiring a unique set of identifiers.

The ATIS IMSI Oversight Council (IOC) oversees the U.S. Assignment of the 15-digit International Mobile Subscriber Identity (IMSI) and maintains the U.S. IMSI guidelines. The first six digits of the 15-digit IMSI is referred to as the Home Network Identity (HNI) or the "PLMN-ID". The HNI/PLMN-ID is comprised of a 3-digit MCC (Mobile Country Codes) along with a 2-3-digit MNC (Mobile Network Code). The ATIS IOC oversees allocation of all U.S. HNIs.

The ATIS IOC and the CBRS Alliance collaborated to develop a new "Shared HNI" assigned to CBRS spectrum operators versus a single "unique" HNI per CBRS operator. Advantageously, CBRS shared spectrum operators do not generally require the same volume of IMSIs. A new "IMSI Block Number (IBN) was created allowing for 10,000 assignments per shared HNI. Each IBN can the provide up to 100,000 unique IMSIs. Thus, each CBRS operator would be allocated a unique IBN to support a customer base of up to 100,000 unique IMSIs.

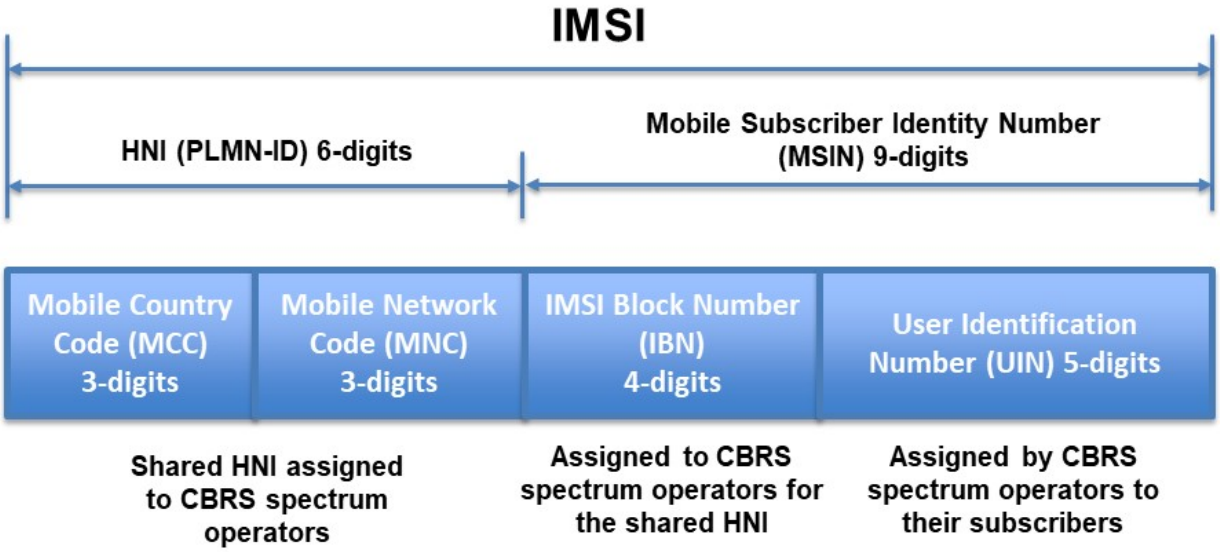

Figure 7.6 – IMSI Block Number Assignment

All IOC approved guidelines may be found at http://www.atis.org/ioc.

Note that mobile network operators with existing assigned HNIs are expected to use their existing HNIs for their CBRS services.

However, normal LTE operation uses the PLMN-ID/HNI separately in many different instances. For example, operators broadcast the PLMN-ID in the System Information Block 1 (SIB1) over the LTE channel to allow devices

to distinguish the network within their list of approved networks to know if they can attach to the network. To address this issue, the CBRS Alliance has decided to use the 3GPP Closed Subscriber Group (CSG-ID) to uniquely identify the network of a shared CBRS HNI. The CBRS Alliance will assign each CBRS operator a unique CSG-ID (CSG Identifier) called the CBRS-NID (CBRS Network Identifier). In addition, the CBRS alliance has identified cases where HNI is used with an LTE system and have provided guidance along with additional identifier assignments to make sure key functions are uniquely and consistently identified. Information is available on-line about how the IMSI code was created to advance use of the CBRS spectrum and how commercialization of it was set into action.

7.7 Neutral Host Using Private 3GPP Technologies

When a 3GPP technology is used in a private network context, a PLMN-ID is needed to uniquely identify the network as a private network. 3GPP, ATIS and other standards bodies which manage PLMN-ID/IMSI assignments are working to address this situation. More information on this issue can be found in 3GPP TR 23.734 - Study on enhancement of 5GS for Vertical and LAN Services in Section 6.1.

7.8 Neutral Host with 5G

Neutral Hosting is often needed in local areas and venues as described in Section 4.2. The new 5G RAN and core technology is a good fit for such deployments due to its applicability to a diverse set of bands (including mmWave bands) that are appropriate for local coverage.

The 5G design in 3GPP Rel-15 supports neutral hosting with solutions originally developed for LTE, including Roaming, MOCN, DDAS or Cloud RAN that are described in previous sections.

8 Regulatory Considerations

8.1 Emergency Services

Emergency services must be provided for UE's in the neutral host network. Given the typically small coverage area of many neutral host deployments, it is likely that emergency service centers for the neutral host coverage area will be in the hosted client network. Options for emergency services may include:

- The neutral host network may force the UE to perform a CS (Circuit Switched) Fallback for emergency calls so that IMS emergency calling is not required. This assumes that 2G/3G circuit switched access is available in the neutral host coverage area.
- Emergency Service support may be provided by the hosted client network (home network). In standard roaming arrangements, when the UE has roamed out of its home network, 3GPP standards indicate that emergency services shall not be provided by the home network and shall be provided in the roamed-to visited network. However, in the neutral host case, the home network likely has local presence along with emergency services capabilities to cover the neutral host coverage area. One approach to accomplish this is for the neutral host network to terminate the IMS emergency APN to a P-CSCF and an associated emergency CSCF (E-CSCF) that is in the hosted client network serving the neutral host coverage area. Alternatively, if the P-CSCF is in the neutral host network, it could have the ability to route directly to an E-CSCF in the hosted client's network that serves the coverage area.
- Emergency Service support may be provided by the neutral host network as would be typical for roaming situations. In this case, the neutral host network will terminate the IMS emergency APN to a P-CSCF and associated Emergency CSCF (E-CSCF) that is in the neutral host network. In this case, the neutral host is responsible for proper handling and routing of emergency calls.

In all cases, it is important that the neutral host network support the ability to:

- Provide emergency services call routing to emergency services facilities that cover the neutral host coverage area.

- Provide the necessary UE location information to the emergency services facilities. This may be particularly difficult when using unlicensed air interfaces and facilities.

More information regarding IMS emergency services can be found in the following 3GPP references:

- 3GPP TS 23.167, "IP Multimedia Subsystem (IMS) Emergency Sessions".
- 3GPP TR 23.771, "Study on system impacts of IMS emergency sessions over WLAN", evaluates solutions to support IMS emergency sessions in a carrier network that originate using a Wireless Local Area Network (WLAN).

In addition, ATIS has done significant work related to the application of Emergency Services in North America in environments typical to many neutral host scenarios. Specifically:

- ATIS-I-0000053, "Wi-Fi Emergency Calling Landscape Assessment", provides an excellent baseline for exploring Neutral Host Emergency Calling requirements. This document provides many references and addresses key use cases that illustrate a number of standards gaps.
- ATIS-0700015.v004, "ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination", identifies and adapts as necessary 3GPP common IMS emergency procedures for applicability in North America to support emergency communications originating from an IMS subscriber (wireline or wireless; fixed, mobile or nomadic) and terminating at an ESInet, or, for appropriate media, legacy emergency services network to support Multimedia Emergency Services (MMES).
- ATIS-0700028, "Location Accuracy Improvements for Emergency Calls" contains significant content on the subject of cellular emergency calling. It is important to note that operators supporting Wi-Fi emergency calls should be able to query the National Emergency Address Database (NEAD) from a location server using the "existing" Nq interface in ATIS-0700028 to obtain candidate dispatchable locations associated with the currently connected Wi-Fi access point as well as other nearby Wi-Fi access points and Bluetooth beacons seen by the originating device.
- ATIS-1000068, "Technical Report on Support of TTY Service over IP using Global Text Telephony" describes the means that the Teletypewriter (TTY) service can be provided over Internet Protocol (IP) between operators' networks through the use of the Global Text Telephony (GTT) capability which enables simultaneous audio and/or video with text media stream.

8.2 Charging and International Tariffs Issues

In some cases, the neutral host may need to support international roaming traffic. The specifics of how this may work will vary depending upon which neutral host option is chosen. Nevertheless, the chosen solution should be evaluated based on the need for support of international roaming and that any issues related to charging and international tariffs are met.

9 Summary & Recommendations

Several different technical approaches to supporting neutral hosts are possible. Each approach has different characteristics and range of applicability, and the approach used should be selected according to the specific objectives and requirements of the particular situation being considered. In addition to the technical implications, the practical deployment of neutral hosts introduces a range of commercial considerations that must be addressed by the neutral host and their hosted clients. Commercial use of neutral hosts should be supported by strong SLAs between the neutral host and the hosted clients and provide sufficient operational capabilities to enable the operator to properly manage its subscribers.