OnGo Private 5G Deployment Guide

April 2022, v1.0.0

Contents

Contents

Introduction

Overview

With the opening up of the CBRS band to the public, the FCC removed several key barriers to deploying small-scale 5G networks. It is now possible to deploy Private 5G networks much more quickly and at a much lower cost than ever. This paper is an updated guide for deploying Private 5G networks using OnGo's 5G in the CBRS band. The 5G NR updates follow the Technical Specifications workgroup updates to documents: CBRSA-TS-1001-V3.0.0 to Rev4.0.0 and CBRSA-TS-1002-V2.0.0 to Rev3.0.1. It provides an updated walk-through of the changes in deployment process and examines the major choices involved.

Note: 5G is a new technology, and devices that support its various capabilities are only recently coming on the market. Some of the features discussed in this guide may not be available just yet, but are coming soon.

At the end of this document, you'll find a glossary defining terms and acronyms used throughout the document and a "checklist" to help drive the planning process.

Who Should Read this Guide?

We have written this guide for enterprises and other organizations interested in building a private OnGo-based 5G network to meet their business needs. We want company leaders to learn the current "art of the possible," while also helping network engineers ask the right questions when planning to deploy an OnGo Private 5G network. We expect the reader to have some familiarity with LTE and wireless networking.

Much of the design, deployment, and operational tasks described in this paper can be addressed in detail by an OnGo system service provider – many of whom belong to the OnGo Alliance. Understanding the scope of services, and the nature of the various tasks involved, will help you define their service needs and select an appropriate service provider.

Why Deploy an OnGo Private 5G Network?

This guide is focused on *how* to deploy an OnGo Private 5G Network. Before deploying a network, though, we need to consider what a private network is, and why you might want to deploy one. The OnGo Alliance is developing additional resources to address the business cases for deploying an OnGo Private 5G Network in more detail – this section gives a high level overview.

What is a Private Network?

A private network is a dedicated network that provides communication connections to people or things belonging to a specific enterprise and provides the services necessary for the business of the enterprise. The traditional private network was built with wired Ethernet or Wi-Fi, with PCs and smartphones being the main devices connected. Private networks allow the enterprise to provide the services you need, where you need them. Since you control the network, you control the data, ensuring privacy, and allowing you to analyze the data to optimize your system. You also have control of adding new services and capabilities when you need them, giving you the ability to scale your network on your own terms.

Why Cellular for Private Networks?

Private networks using cellular technologies like the 3GPP's 4th generation LTE technology bring a number of advantages over other systems:

- High reliability – LTE provides carrier-grade reliability and availability
- Low Latency – LTE provides consistent, low-latency communications
- Mobility – Devices moving around the network are provided seamless connectivity
- Internet of Thing (IOT) – LTE supports connecting massive numbers of devices, with low latency and optimized bandwidth
- Security – Carrier-grade network and data security
- Quality of Service – Network optimization based on device, user, and application
- Network Slicing – Network segmenting and virtualization

Introduction

Why Private 5G?

This ongoing digital transformation of industry in every sector is driving the need for high performance wireless communications. Applications such as industrial robotics, drones, sensors, AR/VR devices, autonomous vehicles, and more, demand high performance wireless communications to be deployed succesfully. The 3GPP's 5G technology is designed to address the needs of these use cases, by improving on LTE with new and upgraded capabilities:

- More bandwidth with increased spectral efficiency.
- Reduced latency to support latency sensitive applications.
- Improved network slicing and virtualization support to allow greater deployment flexibility.
- And more!

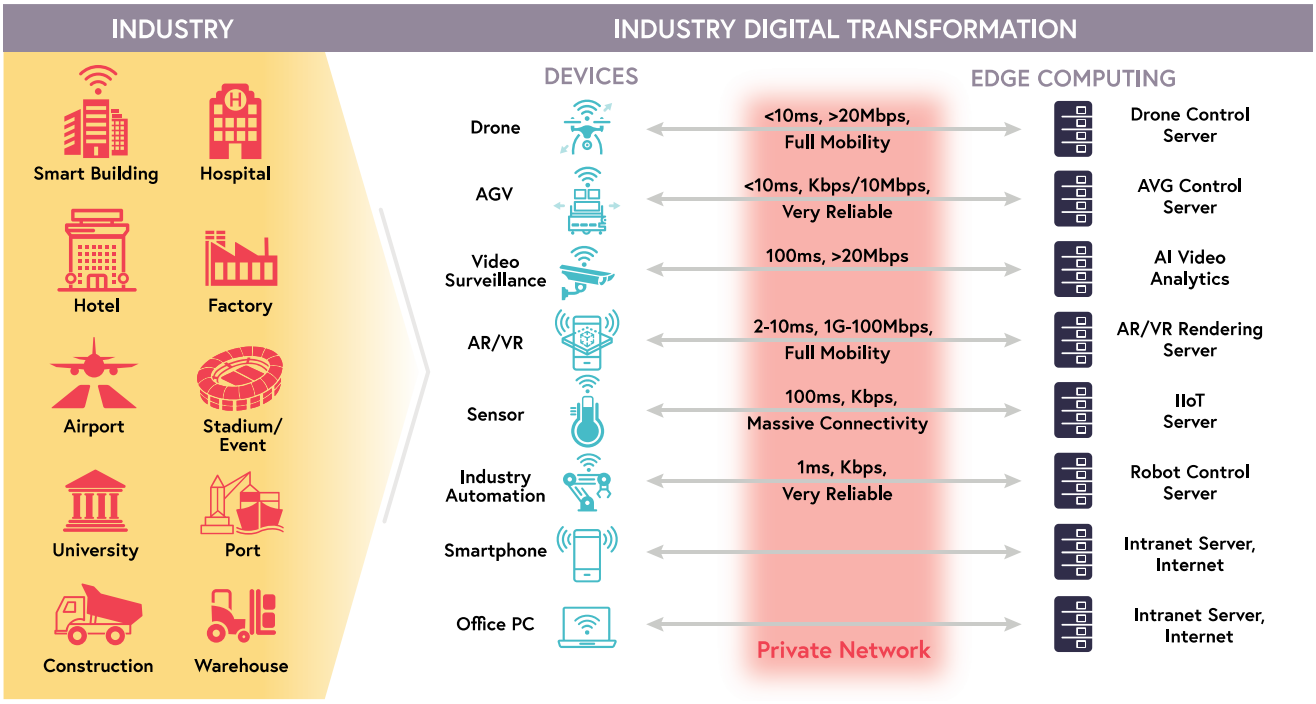

Figure 1: Industry Digital Transformation and requirements for communication connection.

The benefit being that enterprises can now address more use cases with a private cellular network than ever before.

Introduction

Why OnGo Private 5G?

One of the main barriers to deploying private cellular networks has been access to the needed wireless spectrum. Private cellular networks have typically operated in licensed bands, which are both expensive and time consuming to acquire, and not something many enterprises are capable of obtaining. OnGo eliminates this step, by taking advantage of the dynamically shared spectrum of the CBRS band. This makes it possible to deploy private cellular networks at a cost and speed more in-line with unlicensed wireless networks like WiFi.

CBRS Overview

Wireless communication has become the “fourth utility.” It has become as essential as power, water, and internet connectivity for most organizations. Yet, while demand for mobile communication appears limitless, unfortunately the wireless spectrum – the medium for carrying wireless information – is finite, and increasingly scarce and valuable.

In April 2015 the Federal Communications Commission (FCC) formally established the Citizen Broadband Radio Service (CBRS) to address current and future needs for wireless spectrum. Previously reserved solely for military and other government-approved uses, the CBRS band opens up 150 MHz of spectrum at 3.5 GHz band so that private organizations can share this spectrum with incumbent users. The OnGo Alliance created OnGo to promote the use of LTE and 5G in the 3.5 GHz band, although other technologies can also make use of the band. The FCC partitioned 150 MHz of the 3.5 GHz band into 15 x 10 MHz channels. Access to the channels is dynamic and controlled by dedicated spectrum-management services known as Spectrum Access Systems (SAS).

Band 48 Properties

For wireless communications, different frequency bands have different properties. In general, lower frequencies are better for long-range communications, while higher frequencies have larger bandwidths, which allow for higher data rates. At 3.5 GHz, the CBRS Band (Band 48) provides a balanced "mid-band” mix of capabilities – good propagation characteristics, with good data capacity.

PAL vs. GAA

Users who operate in the CBRS band have different priority levels. Top priority lies with the Tier 1 incumbent users such as the federal government, fixed satellite users, and grandfathered wireless users. Next in priority are Tier 2, or Priority Access License (PAL), users. These are licensed users who acquire spectrum licenses through an FCC auction. PAL users must not cause harmful interference to Tier 1 users. Third priority is given to Tier 3 General Authorized Access (GAA) users who deploy "lightly-licensed" devices. GAA users must not cause harmful interference to the higher-tier users.

The FCC auctioned PALs on a per-county basis, with sublicensing permitted. Of the 15 channels in the CBRS band, the FCC allocates seven for PAL licensees. Any spectrum not used by PAL holders or the protected incumbents can be used by GAA users. Currently, GAA users are not afforded any interference protection from each other.

Who's Who in OnGo

OnGo is the result of work by many organizations:

- The FCC – The Federal Communications Commission defined the part 96 regulations that opened access to the CBRS band.
- WInnForum – The Wireless Innovation Forum defined the requirements for CBRS- compliant physical devices.
- OnGo Alliance (OnGoA) – The OnGo Alliance defines the requirements for OnGo technologies in the 3.5 GHz band and certifies OnGo-compliant equipment. (The OnGo Alliance was previously known as the CBRS Alliance.)
- 3GPP – The 3rd Generation Partnership Project standards body represents the community of 3GPP equipment manufacturers and service providers, and defines the LTE and 5G NR standards.

CBSDs

Access Points are termed Citizens Broadband Radio Service Devices (CBSDs) in CBRS. CBSDs come in many types – fully integrated small-cells, distributed radio heads, or antenna clusters. CBRS defines a CBSD as a logical entity that radiates RF power, has antenna characteristics and is geolocated. CBSDs come in two classes, defined by their output power, and range. Category A devices must emit less than one watt of power per 10 MHz channel. Category B devices, typically used outdoors, may emit up to 50

watts per 10 MHz channel. In an OnGo network, the 5G gNodeBs (gNBs – base stations) are connected to CBSDs, and are often in the same device.

Table 1: CBSD category summary.

Device Type	Maximum EIRP (dBm/10 MHz)	Limitations
Category A CBSD	30 (1W)	• Outdoor antenna height limited to six meters Height Above Average Terrain (HAAT). • If operation exceeds antenna height or max Category A power limits, the device is subject to Category B limitations.
Category B CBSD	47 (50W)	• Limited to outdoor operation. Must be professionally installed.

EUDs

In CBRS, End User Devices (EUDs) are the user-facing element. These devices can be either mobile or fixed and their power can't exceed 23 dBm/10 MHz (200 mW). EUDs may operate with permission from a CBSD. In an OnGo 5G network, the EUDs are generally 5G User Equipment (UE) devices.

SAS

All CBSDs must register with an FCC-certified Spectrum Access System (SAS) and obtain a channel grant from the SAS before transmitting in the CBRS band. To prevent interference with incumbent systems, the SAS allocates the spectrum to individual CBSDs and PAL license holders. To coordinate the CBRS band's usage, the SASes maintain a database of CBSDs and incumbent devices to calculate the aggregate interference.

For a SAS to grant access to channels in the lower 100 MHz of the CBRS band, the SAS must have access to an Environmental Sensing Capability (ESC). The ESC is a network of sensors used to detect federal frequency use in the 3550–3650 MHz band where U.S. Navy radar systems can operate, primarily along the Pacific, Atlantic and Gulf coasts. The ESC informs the SAS of radar operations so that the SAS can prevent any CBRS interference with the naval operations by suspending/terminating existing grants

and/or rejecting any new grants in that location for those channels. The SASes use a combination of tools to create realistic propagation model to predict potential interference with incumbent systems, and can provide guidance to CBSDs via operating parameters to CBSDs so as to avoid potential interference.

A new CBSD requests access to a range of frequencies from the SAS, and, based on the location of the CBSD, its category, and its antenna characteristics, the SAS grants access to one or more CBRS channels. When higher-priority users need channel access, the SAS can direct the CBSDs to reduce their output power, stop using currently allocated channels, or shut down entirely to avoid interference with PAL users or incumbent systems.

Several FCC-certified SAS systems are deployed across the country. These systems are operated by various companies that share information among each other. Before a CBRS user deploys a CBSD, they need to subscribe to a SAS service from an FCC-certified SAS administrator. Under Part 96 rules, a SAS does not guarantee interference protection among GAA users. However, WInnForum, the OnGo Alliance, and other standards bodies have developed a coexistence framework for GAA users, to help manage GAA operations.

CPIs

Most CBSDs must be registered by a Certified Professional Installer (CPI), who collects and registers information about the CBSD and provides detailed location information to the SASs. The FCC doesn't require a CPI to install CBSDs, but a CPI needs to register each new CBSD with the SAS. CPIs are certified by one of the Training Program Administrators (TPAs) approved by WInnForum. A list of the TPAs is maintained by the WInnForum, and can be found here: https://cbrs.wirelessinnovation.org/cpi-program-administrator.

Process Summary

Deploying and operating a OnGo Private 5G network involves multiple steps. They consist of the following stages:

Introduction

1. Gather Requirements. Information should include how many people will use the network, what their data service needs are, and what are the key use cases for your network.
2. Survey and Planning. In this stage, you survey the physical space the network needs to cover, identify vendors of the system elements and services, and estimate bandwidth needs and capabilities.
3. Design. Now you begin selecting vendors and refining your network design. During this phase you'll conduct signal measurements and modeling to make sure your network provides the needed level of coverage.
4. Installation. It's time to begin installing your network – CBSDs, radio hardware, backhaul connections, etc.
5. Maintain. Once the network is deployed and operating, you'll need to stay on top of monitoring to ensure that the network is operating correctly.

The rest of this guide walks you through the process, providing further details on each of these steps.

This section describes the different ways an OnGo 5G network can be deployed.

Service Provider Use Case

This is the "traditional" use case for 3GPP-based networks with a service provider (SP) such as a Mobile Network Operator (MNO), Multiple-System Operator (MSO), or Mobile Virtual Network Operator (MVNO), providing services to their subscribers. Subscribers to the SP are able to access the OnGo network, just like the rest of the SP's network. Subscribers to other SPs can only use the SP's OnGo network if they have set up conventional 3GPP roaming agreements and procedures.

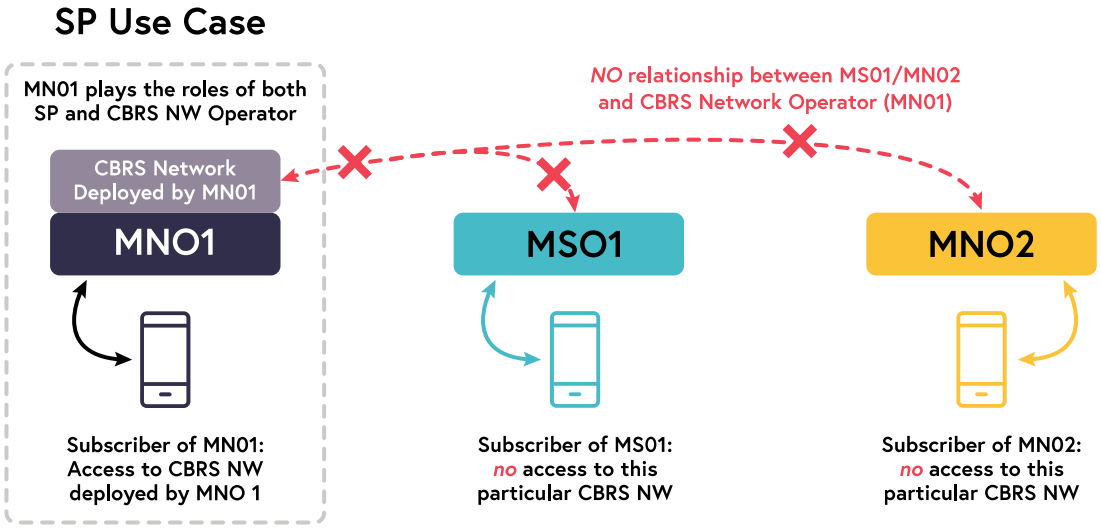

Figure 2: Service Provider (SP) Use case

Private Network Use Case

A private network is a system that provides services specifically for a group or an enterprise(s); e.g., a mall or a school campus. Private networks are typically not accessed by the general public, and are set up to provide services to a limited number of users.

The end users and devices in a private network have a business relationship with the operator of the private network, and are authorized by the operator to access the network. Users can be customers of the operator, employees, or guests otherwise granted access to the network.

In the 5G specifications, private networks are also referred to as non-public networks (NPNs). A 5G network that operates in the CBRS band is an OnGo Private 5G network.

Devices that access a private network can operate come in two types – single-subscription, or multi-subscription capable devices.

Single Subscription Devices

Devices that can only be attached to one network at a time are single subscription devices. Employees or customers of the organization deploying the network (Enterprise 1 in the below figure) are granted a subscription to access the OnGo Network. Enterprise 1 does not have any business relationship with MNO1 or MSO1; hence the Subscribers of MNO1 or MSO1 do not have access to the OnGo Network deployed by Enterprise 1.

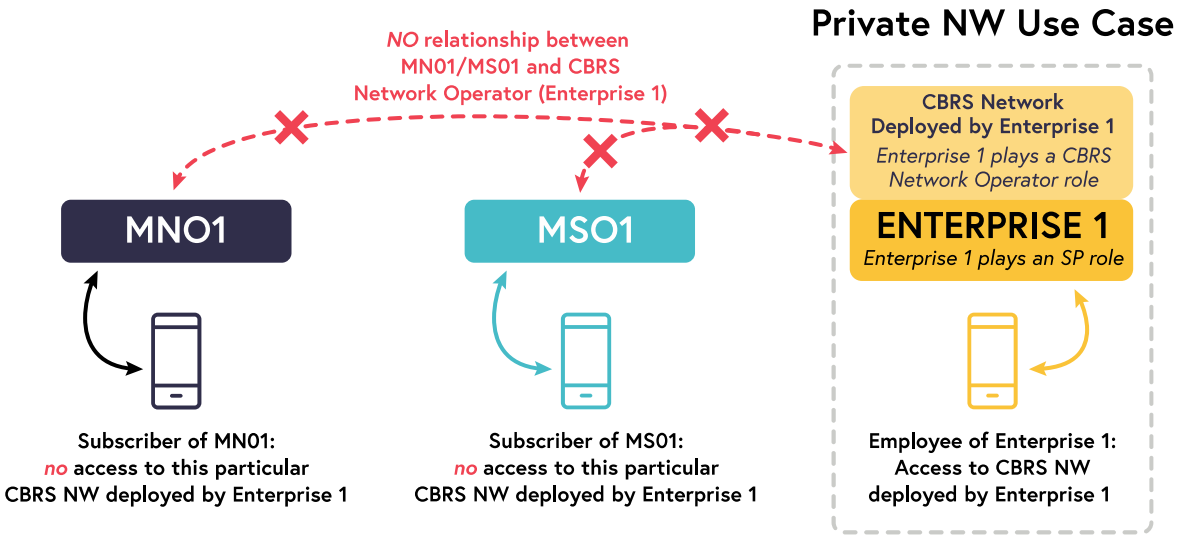

Figure 3: Private Network Use Case – Single-Subscription Devices

Multi-Subscription Devices

This is a variation of the Private Network – Single-Subscription Device use case, where the UE used in a Private Network has, in addition to a subscription with the Private Network, a subscription with another SP. This other SP may be an MNO, MSO, or MVNO, or even another Private Network. The device uses separate credentials for access to each network, such as a dual-SIM capability.

Devices that can support multiple-subscriptions can use any of the networks that they are subscribed to. Which network is used can be based on multiple factors, including which networks are available, what services the device or user is accessing, user selection, or other methods.

A Subscriber may use an SP subscription to access SP services using a Private Network as an untrusted network. In this case, the subscriber can use untrusted non-3GPP access procedures to access SP services. The tunnel is set up using IP connectivity provided by a Private Network after gaining the connectivity by authenticating with the Private Network using Private Network credentials. The Private Network in this use case can be LTE Private Network or NR Non-Public Network (i.e., SNPN or PNI-NPN).

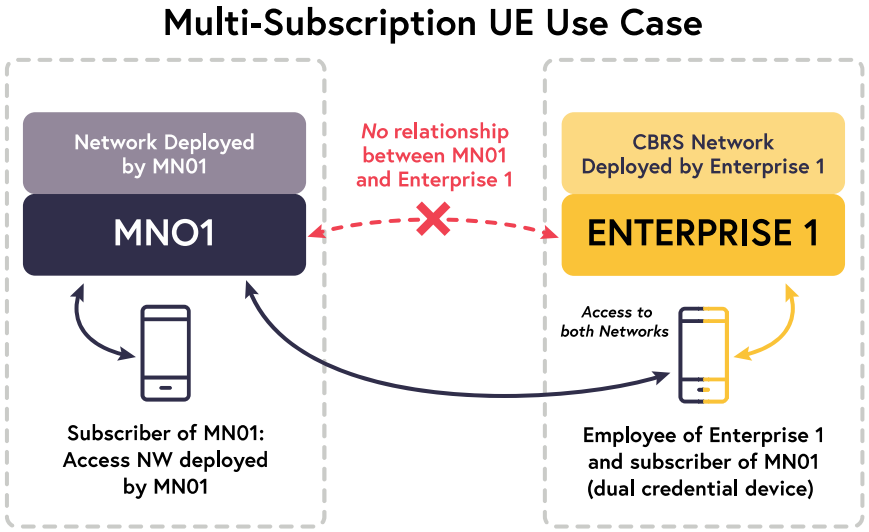

Figure 4: Private Network Use Case – Multi-Subscription Devices

Figure 4: gives an example of a Private Network use case with dual subscription. Enterprise 1 deploys an OnGo Private Network and provides private services to authorized users. Enterprise 1 does not have any business relationship with MNO1. An employee of Enterprise 1 also has a subscription to MNO1 with a separate MNO1 credential. This employee can access the private network services through the OnGo network deployed by Enterprise 1. If MNO1 is configured to allow it, the employee can also access MNO1's services with the OnGo network acting as an untrusted non-3GPP access.

Neutral Host Networks

A Neutral Host Network (NHN) is a network that allows a single network to provide services to the subscribers of multiple SPs. The network is deployed and operated by an NHN operator, an independent entity, or an existing network operator. For users of the network, the NHN operates seamlessly with their regular network and can be entirely transparent – it doesn't take any special activities to use and roam into and out of the network without any interruption of service. NHNs are an ideal choice for extending the coverage of existing mobile networks, especially where coverage is limited or non-existent, such as inside a building.

The OnGo Alliance has prepared an OnGo NHN Deployment Guide, which can be found here: https://ongoalliance.org/resource/ongo-nhn-deployment-guide/. That guide is focused on LTE-based NHNs. OnGo NHNs can be deployed using 5G, where the network slicing capabilities of the 5GS make implementing an NHN significantly easier than in LTE. The primary hurdle is putting in place the legal agreements and network connections with the SPs. The details for 5G will be addressed in a future deployment guide.

5GS Introduction

The 5G System (5GS) is the formal name for 3GPP's fifth-generation technology. It upgrades and replaces their fourth-generation LTE technology. The 5GS was defined in 2018 in release 15 of their specifications. Release 16 came in 2020, and added additional capabilities and features.

The additional features of the 5GS make an OnGo Private 5G network significantly more capable, but also more complex to design and deploy. This section provides an overview of the use cases addressed by 5GS, its major components, and what are the key capabilities of the updated system. This will help you better understand what the options are, and help ensure that your OnGo Private 5G network is configured to support your needs.

5GS Key Use Cases

The 5GS was designed to address three primary use cases:

1. Enhanced mobile broadband (eMBB): This covers the "typical" smartphone use case. The 5GS addresses this use case by increasing spectral efficiency for more available bandwidth, improved energy efficiency, and more devices per cell.
2. Massive machine type communications (mMTC): This is the "Internet of Things" use case, including sensors and wearable devices. 5GS supports this by enabling a much higher number of devices per cell, and increased energy efficiency.
3. Ultra-reliable and low latency communications (uRLLC): This use case is focused on advanced systems, such as telepresence, AR/VR, remote vehicle operation and remote surgery applications. These systems need low latency and high reliability. The 5GS introduces multiple features to achieve low latency (<1 millisecond) and increase connection reliability.

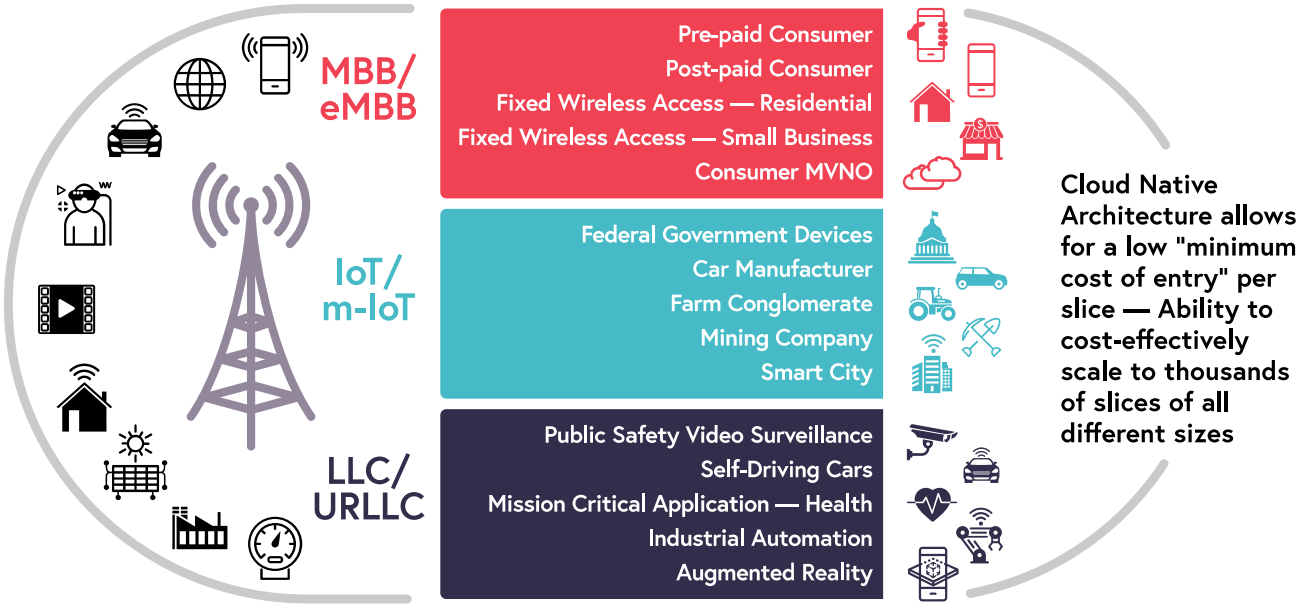

Figure 5: 5G Value Propositions and Use Cases

An OnGo Private 5G deployment can be configured to address one or more of these use cases, depending on your needs.

5GS Components

A 5GS network consists of the following components. This guide provides further information about these components below.

User Equipment (UE)

User Equipment (UE) is the 3GPP term for devices that connect to the network – smartphones, devices, sensors, etc. In CBRS terms, a UE is an EUD, and the terms can be used interchangeably.

5G NR RAN

The 5G New Radio (5G NR) radio access network (RAN) is the wireless link between the user devices and the 5G network. The base stations that the UEs connect to are called gNodeBs (gNBs) in 5G NR, replacing the eNBs of LTE. Base stations can have a variety of radio frequency band capabilities and power levels. In CBRS, a gNB contains a CBSD – or rather, the gNB's antennas are tied to a CBSD.

5G Core (5GC)

The 5G Core (5GC) or 5G Core Network (5G CN) is responsible for routing traffic to and from user devices. It replaces the Evolved Packet Core (EPC) of LTE.

5GS Major Features

The 5GS represents a significant update and change over LTE. Some of the key changes are summarized here, and are explained in further detail below.

Upgraded RAN – 5G NR

The 5G NR RAN bears much in common with its 4G LTE predecessor, using the same fundamental technology of Orthogonal Frequency Division Multiplexing (OFDM). However, 5G NR updates that basic architecture to be more efficient, more flexible, and to take further advantage of beam-forming and multiple-input multiple-output (MIMO) techniques. For an OnGo Private 5G deployment, this means that your network can be better optimized to support your needs, and better performance than a Private LTE network.

New Core Network Architecture – 5GC

In order to support the use cases targeted by the 5GS, the 5GC has been modified from the EPC that preceded it. Rather than focusing on individual component systems, the 5GC architecture is now focused on individual network functions (NFs) or services provided by the core network. Data traffic is also more clearly divided between the control plane and user planes, with the former being reserved for command and control, and the latter for user applications.

Upgraded Network Slicing

Network slicing enables Service Providers to offer logical virtual networks on shared 5G infrastructure. Each virtual network slice can be configured to have access to different services and capabilities. From the user and device perspective, these network slices appear to be entirely distinct networks, even while they are operating over the same physical hardware.

While LTE allowed for some network slicing, 5GS has greatly increased the capabilities of network slices, allowing for greater flexibility and control.

Improved Cloud and Virtualization Support

The support for network slicing is only one aspect of how the 5GS has added support for virtualization. The 5GC is designed to be deployed virtually – with some or all of the various network functions able to be deployed into the cloud as Virtual Network Functions (VNFs). Likewise, the base stations (gNBs) can take advantage of virtual RAN (VRAN) options. The key benefits of virtualization are the ability to scale rapidly, increased resiliency, faster deployment of services, and support for multi-cloud (public, private, hybrid) deployments.

New Bands – Frequency Range 2 (FR2)

The 5GS also supports a new band of frequencies at a much higher range. The "traditional" range of frequencies, known as Frequency Range 1, covers the frequencies used by LTE, from 410 MHz to 7125 MHz. The new band of frequencies, Frequency Range 2 (FR2) covers 24.25 GHz up to 52.6 GHz. Much attention has been paid to FR2 in the media, and many of the peak throughput capabilities of the 5GS are dependent on the larger channel sizes available in FR2. It is a common perception that 5G can only be deployed in FR2, or that the propagation characteristics of FR2 apply to all 5GS deployments. Fortunately, this is not true – 5G can be deployed in the CBRS band, which sits in FR1. In 5G, the CBRS band is labeled as band n48, and any UE (EUD) that supports band n48 is capable of operating in an OnGo network. Bands n77 and n78 also include the n48 band, so devices that support those bands can (generally) connect to an OnGo network.

5GS Deployment Modes

An OnGo Private 5G network can be deployed in several modes.

Non-Standalone (NSA) Mode

In this mode, the 5G network is deployed in parallel with a 4G LTE network. The LTE EPC is used as the network core, with LTE eNBs and 5G NR gNBs providing service to devices simultaneously. Control plane communication is handled over the LTE anchor link, with user plane data sent over the 5G NR link to devices that support it. UEs that can support connecting over the LTE and 5G NR links simultaneously are called Evolved-Universal Terrestrial Radio Access – New Radio Dual Connectivity (EN-DC). This mode can be used when upgrading an OnGo Private LTE network to 5G. See the section on Upgrading LTE to 5GS for additional information.

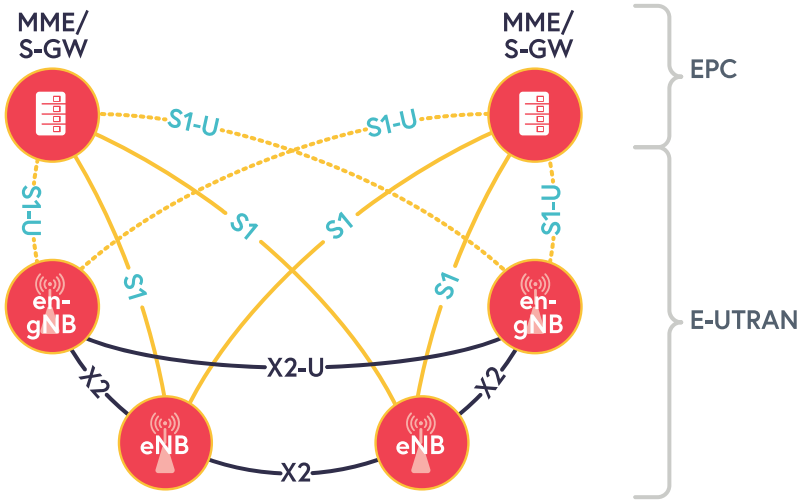

Figure 6: 5G NR Non-Stand-Alone (NSA) Network Architecture

Standalone (SA) Mode

In SA mode, the 5GS is deployed with no LTE anchor – the network operates independently of LTE, and uses a 5GC for its core network. This is a full 5GS network, able to take advantage of all the capabilities of the 5GS.

A SA network can operate as a standard public network, but it can also operate as a non-public (private) network, in one of two modes.

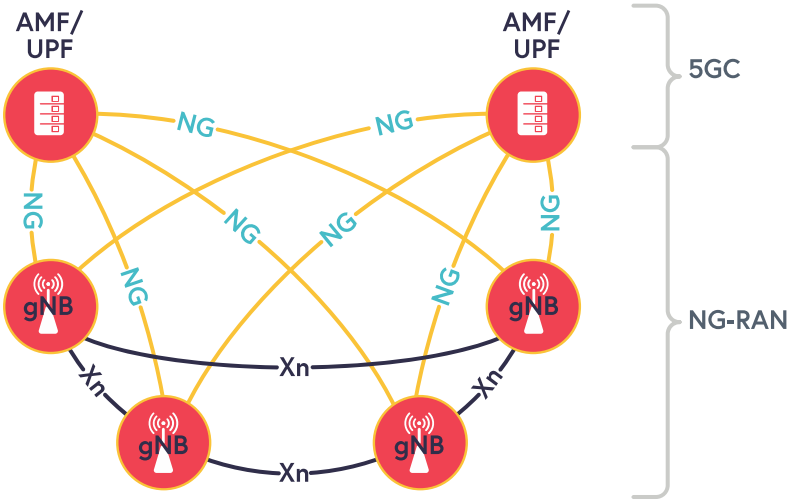

Figure 7: 5GS Stand-alone (SA) Architecture

SA Non-Public Network (SNPN)

This mode was added in release 16 of the 3GPP specifications, and is the most suitable mode for an OnGo Private 5G deployment. It allows for an isolated NR network deployed as a private network, and not depending on the network operator having their own PLMN-ID. The OnGo specifications support use of this mode when using the CBBRS Shared HNI (discussed later in this guide).

Public Network Integrated Non-Public Network (PNI-NPN)

This mode was also added in release 16, and allows a public network with a PLMN-ID to deploy private networks within that network, using a Closed Access Group (CAG). The current release of the OnGo specifications does not support this mode when using the CBRS Shared HNI. Support is being considered for future releases.

5G New Radio (5G NR) and Virtualization

The gNBs of the 5G NR RAN are similar in concept to the eNBs of LTE. They can be divided into multiple separate components:

1. The Base Band Unit (BBU), which performs the digital signal processing. 5G NR further divides the BBU into two sub-components, connected over the standardized F1 interface:
    - A Central Unit (CU) that handles higher-layer protocol processing.
    - One or more Distributed Units (DU), that handle lower-level processes.
2. The Remote Radio Head (RRH), which performs analogue/digital conversions.
3. The Antenna, which transmits and receives the wireless signals.

All of these components can be integrated into a single device, particularly for small cells. But for macro cells, the BBU's CU and DU, and the RRH are often separated. There has been an ongoing trend to consolidate the BBU component, in order to reduce the costs of deploying base stations:

- Distributed RAN (DRAN): DRAN solutions placed the BBU on-site, with each BBU able to support a small number of RRHs at the site. DRAN systems typically need dedicated fiber links between the BBUs and RRHs.

- Centralized RAN (CRAN): CRAN consolidated the BBUs into “BBU Hotels” that could be centrally located, and support more RRHs per BBU. As with DRAN, CRAN systems typically need dedicated fiber links between the BBUs and RRHs.
- Virtualized RAN (vRAN): VRAN takes the next step, and completely virtualizes the BBU as the virtual BBU (vBBU), allowing it to be deployed using COTS hardware, or “in the cloud”. vRAN systems can be deployed using high-performance Ethernet, rather than using optical fiber.

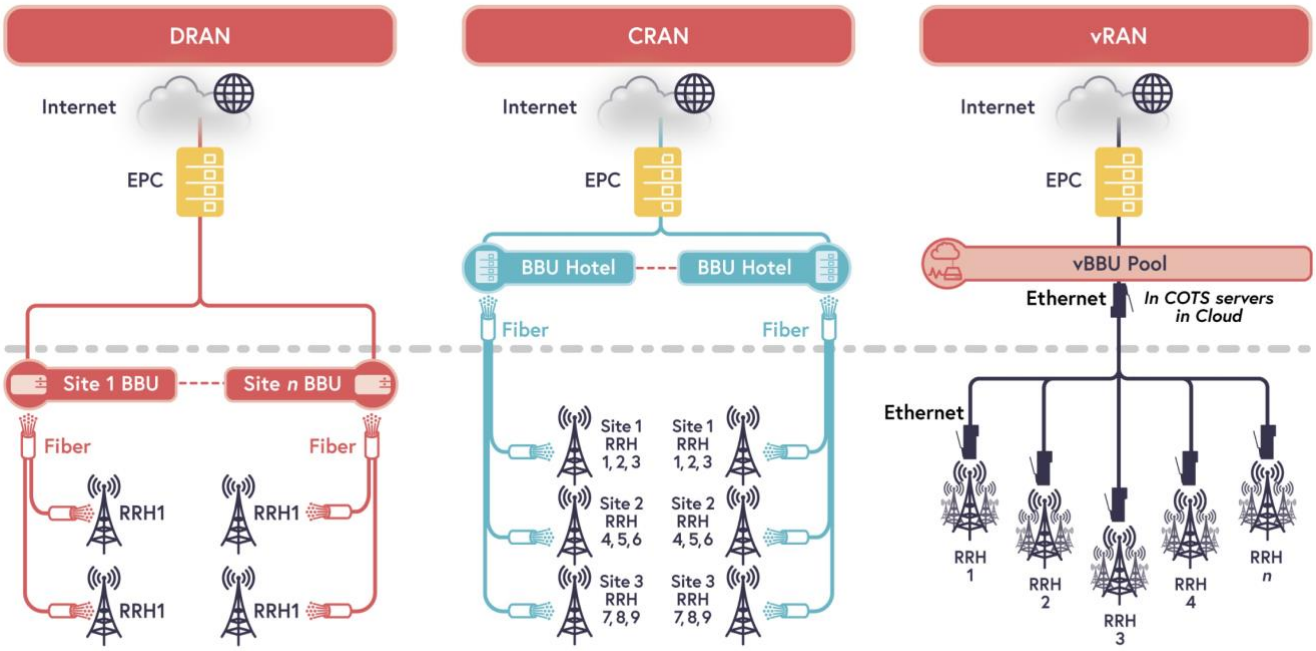

Figure 8: RAN architecture options.

The benefit of these systems is to reduce the cost of deploying base stations by sharing the BBU across multiple RRHs. When deploying lots of Category A (lower power) CBSDs, which is typical for indoor deployments, using a centralized BBU or CU can significantly reduce the overall cost of deployment.

Virtualized gNBs and CBSDs

When using a virtualization option like DRAN, CRAN, or vRAN, the relationship between the CBSD and gNB gets a little more complicated. The CBSD is tied to the transmission point of the gNB – the antenna and the RRH, rather than the BBU. This means each RRH or antenna is treated as its own CBSD.

Fronthaul

For all of DRAN, CRAN, and VRAN, the critical constraint is the fronthaul connection – the connection between the BBU and the RRH. The performance needed is quite high, especially for DRAN and CRAN systems:

- Latency: <800uSec round trip (from RRH to BBU and back to RRH), with 150 to 200 µsec for the transmission path.
- Bandwidth: >1 Gbps per RRH – more if using multiple MIMO layers.
- Synchronization: <16 ppb frequency and <3 µsec phase synchronization.

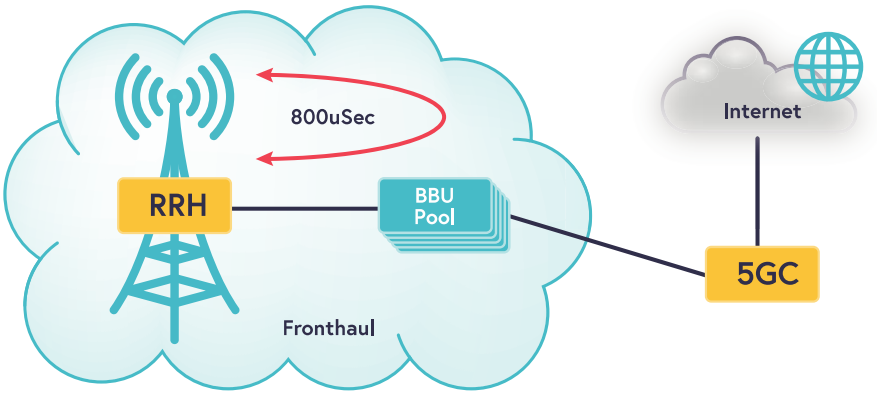

Figure 9: RAN Fronthaul diagram.

These high-performance requirements typically require fiber using the Common Public Radio Interface (CPRI) standard. Other fiber-based options can be used as well, such as Optical Transport Network (OTN), or Passive Optical Network (PON). Both OTN and PON use statistical multiplexing techniques that help in aggregating the signals coming from multiple RRHs into one signal towards the vBBU.

For a vRAN solution, CPRI over Ethernet can be used for the fronthaul connection. CPRI over Ethernet uses existing Ethernet infrastructure available at the site and helps reduce the cost of laying fiber to some extent. However, Ethernet overheads on top of CPRI payload increases the bandwidth requirements further and has higher latency than fiber.

Recent introduction of millimeter wave (E band and V band) that supports larger bandwidth and higher throughputs has made wireless a viable option for fronthaul.

However, it can be used only in case of short distances (<200m) and provided there is a clear Line-of-sight between two points of connectivity.

Which fronthaul solution you use is largely a function of what is currently available at your location and the latency needed by your applications. If fiber is already installed at your facility and not being fully utilized, the potential savings of using vRAN are significant. Even if you need to install dedicated fiber links, it may still be cost effective. Likewise, if extremely low-latency is not needed, a cloud-based vRAN using Ethernet can be used.

Midhaul

The connection between the BBU's CU and the DU(s) is termed midhaul. This typically has much lower bandwidth requirements than the fronthaul, and can be deployed over Ethernet.

Open RAN

The interface between the CU and DU is defined by the 3GPP as the F1 interface, so it is (in theory) possible to mix CUs and DUs devices from different vendors. The other interfaces in a virtualized gNB, such as between the BBU and RRH, are not defined and are often proprietary. Open RAN is an ongoing effort by various network equipment makers to define those interfaces, both hardware and software. The ultimate goal being to allow for increased customization and flexibility, allowing network designers to use the components that are best suited to their needs.

5G Core (5GC)

The 5G Core (5GC) is responsible for controlling the gNBs, managing the devices within the network, and routing data traffic to and from devices. The overall architecture of the 5GC has shifted to a network functions (NFs) model, using a REST services-based model to better support virtualization of the 5GC. The NFs are software, and can be deployed on commercial off-the-shelf (COTS) hardware, in a data center on premises or off, or in the cloud. The 5GC is highly customizable, incorporating only the NFs needed by your network. It is also extensible and expandable, allowing you to flexibly add additional services over time.

Data going to and from user applications, including things like voice and web traffic, is referred to as user plane data. In the 5GC, user plane data is kept separate from the control plane data that handles the network connection management.

5GC Network Functions

The main 5GC network functions (NFs) and functionalities are given below. Depending on your deployment, certain functions may not be needed.

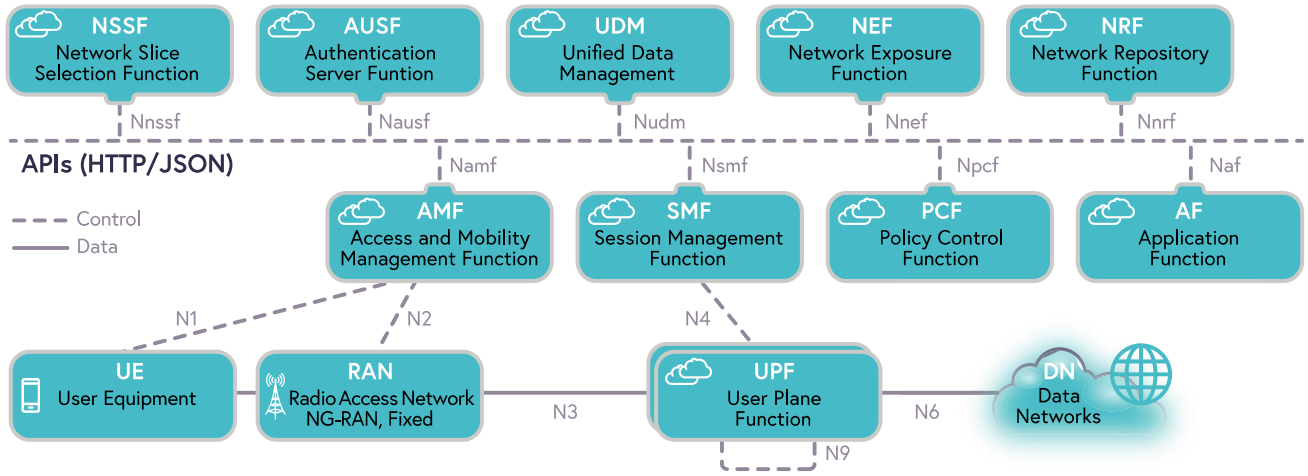

Figure 10: 5GC Network Function system architecture.

- Access and Mobility Management function (AMF) is a control plane function, and handles registration management, connection management, mobility management, access authentication and authorization, and security context management. It acts as a single-entry point for the UE's connection to the network – when a device wants to attach to the network, it interacts with the AMF. In LTE terms, the AMF has part of the EPC's MME and PGW functionality.
- Session Management function (SMF) is responsible for setting up and managing the IP connections to UEs. It is a control plane function that supports PDU session management, IP addressing, and the like.
- User Plane function (UPF) is responsible for routing user plane data to and from external data networks, using PDU sessions managed by the SMF. It supports packet routing & forwarding, packet inspection, and QoS handling. The UPF is also

the anchor point for intra- & inter-RAT mobility, allowing the 5GC to use other radio access technologies (RATs) in conjunction with 5G NR. The UPF has part of the SGW & PGW functionality of the LTE EPC.

- Policy Control function (PCF) is a control plane function that provides policy and user subscription information to the other NFs, including the AMF and SMF. It is to implement business rules based on the user's subscription type. It is used to configure the QoS of the connections available to a given UE, prioritize their data traffic, configure reselection and how to offload data to other RATs like WiFi. PCF has part of the old PCRF functionality.
- Authentication Server Function (AUSF) acts as an authentication server. It allows the AMF to authenticate the UE, and generates keys for use by other security procedures within the 5GS. When compared with the 4G EPC, the AUSF is similar to the HSS/AAA Server.
- Unified Data Management (UDM) supports generation of Authentication and Key Agreement (AKA) credentials, user identification handling, access authorization, subscription management, storing the data used by the AUSF as part of authnentication. It maintains the list of available Network Functions instances and their profiles. It also performs Service registration & discovery so that different Network functions can find each other via APIs. When compared with 4G EPC, it's functionalities resemble the HSS/AAA Server of a 4G Network.
- Application Function (AF) acts as an application server for specific services provided over the network. Multi-Access Edge Computing (MEC) services are deployed using the AF.
- Network Exposure function (NEF) supports exposure of the capabilities of the 5GC to external networks and applications. It can also be used to send events to external applications. It exposes services and resources over APIs within and outside the 5G Core. The NEF uses RESTful APIs.
- NF Repository function (NRF) supports service discovery by maintaining a list of services available in the 5GC. The various NFs register with the NRF when they start up, providing information on their capabilities and how they can be reached.

- Network Slice Selection Function (NSSF) is a control plane function that supports network slicing. It maintains a list of the Operator defined network slice instances, and redirects traffic to the intended network slice. The AMF authorizes the use of a network slice based on the subscription info stored in the UDM, or it can query the NSSF to authorize access to a slice based on the service requirements.

LTE EPC Mapping

If you are familiar with the functions of the 4G EPC, those components can be mapped to the NFs of the 5GC, per the below diagram.

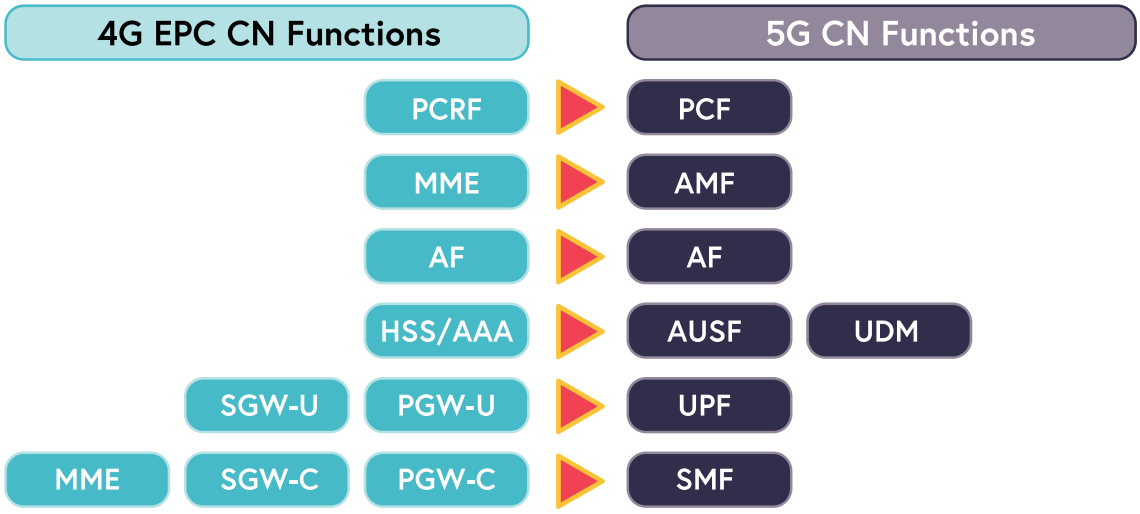

Figure 11: LTE EPC to 5GC element mapping.

5GC Deployment Options

The different elements of the 5GC can be run on separate devices or integrated into a single device. 5GC network elements can be deployed entirely in the cloud, on-premises together with CBSDs, or in a hybrid mode. The architecture you select depends on the needs of your deployment, and should include available backhaul, desired latency, and cost considerations. Likewise, your deployment needs (such as seamless roaming to/from the public networks, network slicing, etc.) dictate the features your 5GC will need to support. 5GC and NF providers can provide a range of solutions based on your needs. They often offer different management system capabilities, which we discuss in more detail later in this guide.

Network Slicing

5G networks now support providing multiple independent virtual networks on a single physical network, a technique named Network Slicing. Each of these virtual network slices can be finely tuned to specific applications, each configured with their own independent configurations, controls, and features. This gives network operators much greater capability to tune the services and capabilities offered by the network. For example, one slice can be optimized to support remote vehicle operation, while another slice is tuned to support IoT sensors.

The services offered by a network slice are also customizable. A “public” slice could provide open access to the Internet to all devices and users, while a “private” slice could be configured to give staff access to your internal network. A “devices” slice can be optimized to support a large number of devices, and give them access to central data storage systems.

Multi-Access Edge Computing (MEC)

Moving services to the edge of cloud, multi-access edge computing (MEC), is often necessary to support specific applications. For example, for applications where low latency is critical, services can be deployed close to the edge of the network. With the network slicing capabilities of the 5GC, MEC services can be attached to specific slices, and deployed at the optimum location. Specific network functions provided by the 5GC combine to create an end-to-end service. Slices can be created using only the functional components needed to support the specific requirements of the service or customer.

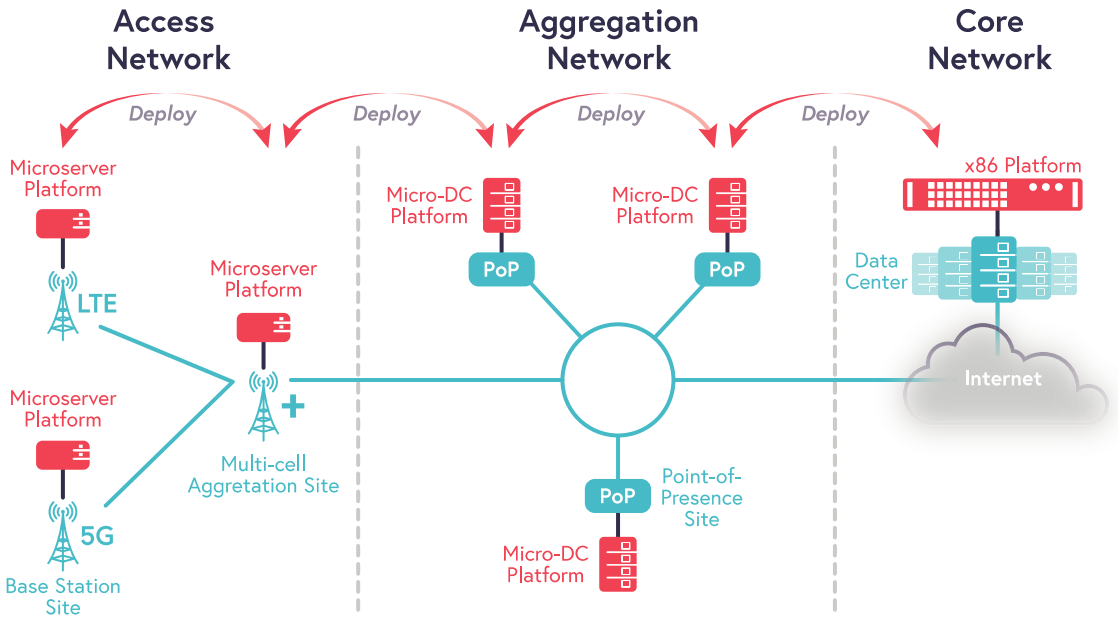

Figure 12: MEC allocation options.

Table 2: Network split overview.

MEC Location	Description
Access Network	Essential for low latency and local content, as it is the closest deployment to the user
Aggregation Network	Provides regional cloud presence that scales the virtual and container functions that support the distribution of the connectivity to the end sites
Data Center Clouds	House the core network operational manager of the user access and content distribution
Data Center	House scalable compute and storage capability

5G Security

Security is of ever-increasing concern for operators of all networks and services. The changing threat landscape, and the changes in the 5GS have created new challenges to security, and new requirements.

Table 3: Security Requirements for 5G Networks[1]

[1] Table courtesy of the Next Generation Mobile Networks Alliance.

Requirements respect to 4G	Improve resilience and availability of the network against signaling based threats including overload caused maliciously and unexpectedly.
	Specific security design for use cases which require extremely low latency
	Comply with security requirements defined in 4G 3GPP standards. Need to apply especially to a virtualized implementation of the network
	Provide public safety and mission critical communications (resilience and high availability)
Requirements from Radio Access perspective	Improve system robustness against smart jamming attacks
	Improve security for 5G small cell nodes

This section assesses the threats, the changes in the 5GS that impact security, and how the 5GS addresses them. Our forthcoming LTE and 5G Security Whitepaper will provide additional details on the security features of 3GPP systems, and what actions you can take to further increase the security of your networks.

Security Threats

Attacks against a network can be classified into two basic types: passive attacks and active attacks.

Passive Threats

For a passive attack, attackers attempt to learn or make use of the information from the legitimate users but do not intend to attack the communication itself. Common passive attacks in a cellular network are two kinds, i.e., eavesdropping and traffic analysis. Passive attacks typically aim to violate data confidentiality and user privacy.

Active Threats

Active attacks can involve modification of the data or interruption of legitimate communications. Typical active attacks include man-in-the-middle attacks (MITM), replay attacks, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks.

Table 4: Attacks on Wireless Networks

Attack	Type	Description
Eavesdropping	Passive	Sniff signals to reconstruct data streams.
Traffic Analysis	Passive	Monitor aggregate signals to monitor users.
Jamming	Active	Prevent communication with radio noise.
Denial of Service	Active	Prevent communications with hostile signals.
Man-in-the-middle	Active	Intercept and modify data transmitted across network.
Spoofing	Active	Impersonate a valid device with fake credentials.

Security Considerations in 5G

From a security perspective, there are three significant changes in in the 5GS that impact security:

- The Virtual Network Functions (VNFs) and service-oriented capabilities of the 5GC mean that trust needs to be established between the various NFs and services of the 5GC, and their connections to the UEs.
- The uRLLC and mMTC use cases need security mechanisms that don't interfere with the latency and power consumption requirements of those use cases.
- The general need to improve the security, reliability, and accessibility of 5G wireless networks.

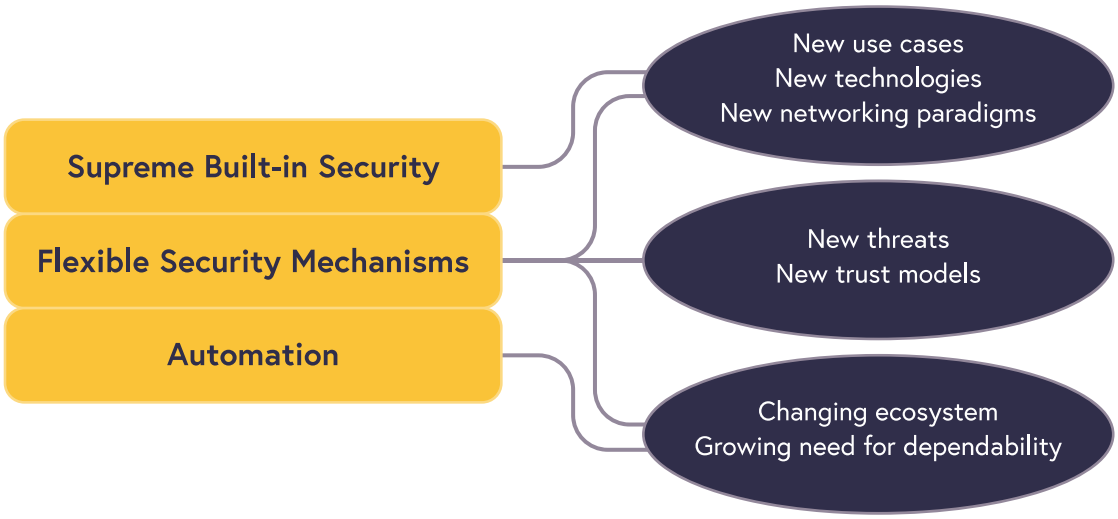

Figure 13: Major drives for 5G wireless security.

Security in 5G

The 5GS has enhanced security from its LTE predecessor in several ways, both at the physical layer, and cryptographically.

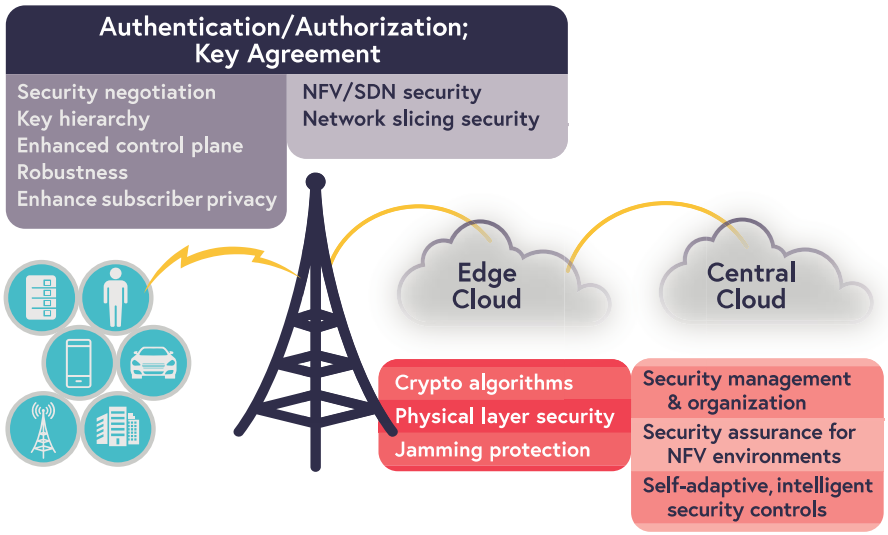

Figure 14: Elements in a 5G Security Architecture

Improved Physical Layer Security

The 5G NR RAN includes multiple features to protect against attacks, both passive and active. Most notably, the increased use of MIMO and beamforming techniques in 5G NR makes eavesdropping attacks significantly more difficult, as each beam must be intercepted in order to reconstruct the signal. These technologies also make jamming attacks more difficult.

New Trust Relationships

Trust relationships can now be established between the network and the services provided over them. Authentications are required not only between subscribers and the two operators (the home and serving networks) but also among service parties in 5G wireless networks. This even applies to individual network slices, with a given slice being given trusted access to only those services that are needed within that slice. Additional trust mechanisms have been added to prevent spoofing of the home network.

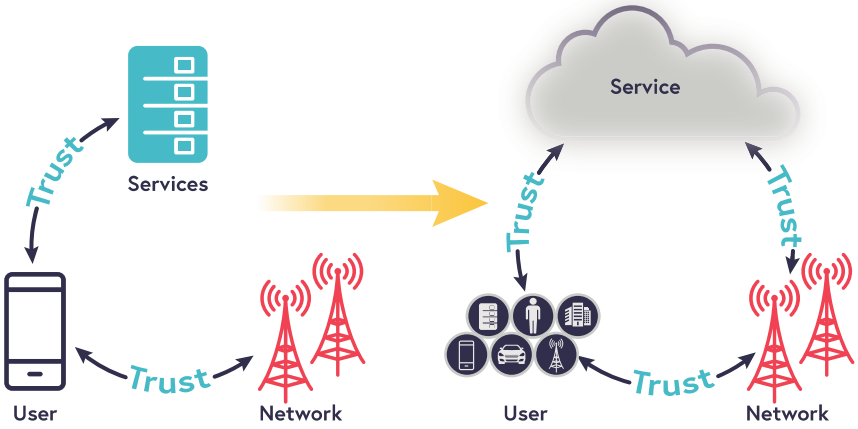

Figure 15: Trust Model of 4G and 5G Wireless Networks

Upgraded Cryptographic Security

Cryptographic security has been built into 3GPP networks since their inception, and the use of USIM-based security mechanisms to authenticate UEs is well established. These systems have been enhanced to make decryption of data significantly more difficult. The 5GS also adds additional encryption of the identifiers used by the UEs, preventing spoofing and man-in-the-middle attacks.

Flexible Security Mechanisms

New security mechanisms have been added as well, to support the needs of uRLLC and mMTC use cases, where the latency and power consumption of the techniques used in LTE are not acceptable. The ability to encrypt communications across different connections (when using WiFi offload, for example), has been increased, ensuring security even when in a heterogeneous network (HetNet) environment. The flexibility of the 5G security means you can also add additional security mechanisms to the services provided by your network when needed.

The 3GPP designed the ability to upgrade a 4G LTE network to 5G in a phased approach. This allows for 5G to be deployed smoothly, and without interrupting operation of LTE devices. This process can be used for OnGo networks as well, allowing you to upgrade an OnGo Private LTE network to an OnGo Private 5G network.

The upgrade process takes place in three stages:

1. Add a Non-Standalone (NSA) 5G network to the existing LTE network.
2. Migrate to a Standalone (SA) 5G network,
3. Retire the LTE network.

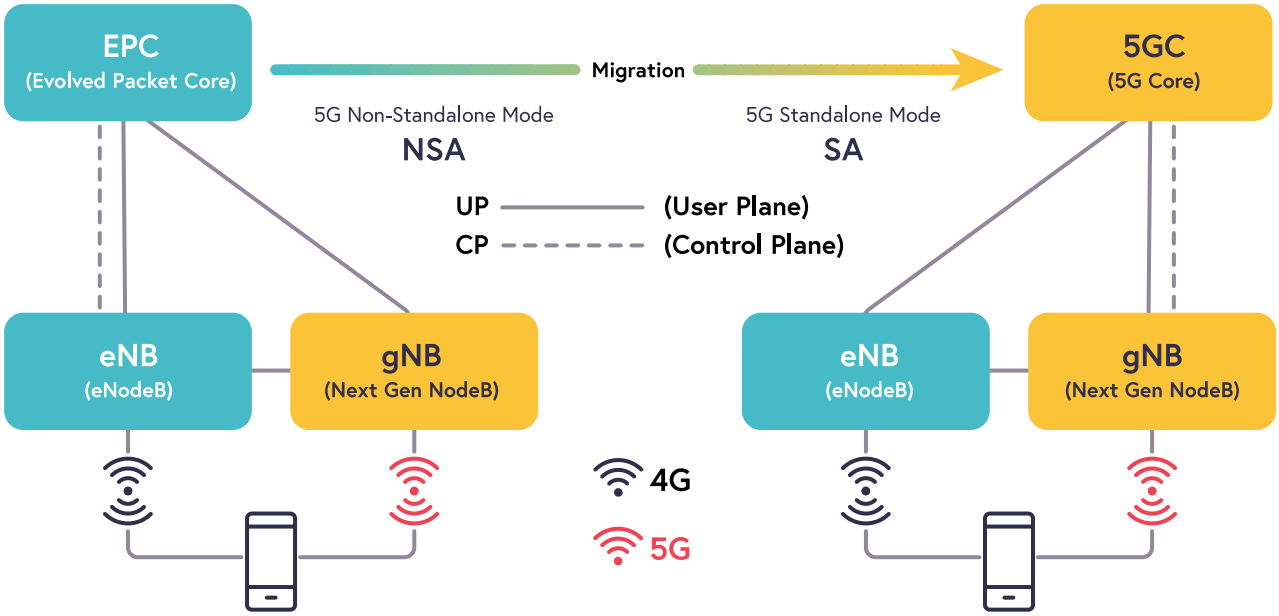

Figure 16: Migrating from LTE to 5G.

Further detail on each stage is provided below.

Adding 5G NSA

The first step in the migration involves deploying a 5G NR RAN in parallel to the existing LTE network. 5G gNBs are deployed, and use the existing EPC core network to operate. The 5G gNBs operate on a separate channel from the LTE network. Control signaling is done over the LTE link, and with user data sent over the 5G NR link. Thus,

devices that support connecting to LTE and 5G NR simultaneously (EN-DC) are able to take advantage of the bandwidth offered by the 5G channel. Control plane information is provided over the LTE connection, while user plane data is sent over the 5G NR connection. This can even improve the performance of LTE-only devices, as the offloading of traffic to the 5G channel makes more bandwidth available over LTE data.

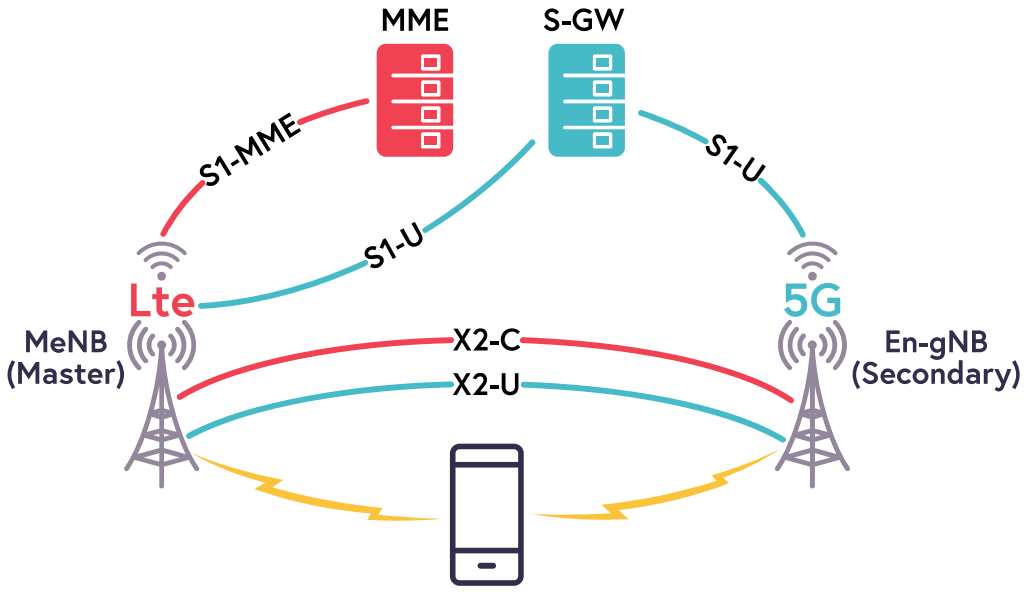

Figure 17: 5G NR NSA EN-DC Network Architecture, with user plane connection from EPC to eNB and gNB.

There are multiple options for deploying the 5G NSA channel in an OnGo network:

- As an additional 10 MHz channel in the CBRS band, if one is available. This can be done even if the LTE component isn't using the CBRS band.
- On half of the 10 MHz channel that the base OnGo LTE network operates, with each getting 5MHz. This is less efficient than operating on a separate channel.
- Using traditionally licensed spectrum, or even in unlicensed spectrum, as supported by 5G. This obviously requires working with the owner of the licensed spectrum, or accepting the limitations of unlicensed spectrum.

Migrating to 5G SA

The next stage is to transition the LTE EPC to a 5GC core network. Once deployed, control plane information can be sent over the 5G NR link. The benefit of the shift is to be able to access more of the features available in the 5GS, taking more advantage of the improved efficiency and performance in 5G. Devices that only support 5G communications will be now able to use the network.

Support for LTE-only devices can be maintained in this mode, by upgrading the LTE eNBs to support interfacing with the 5GC. These are known as Next Generation eNBs (ng-eNB), and the upgrade is typically just a software update.

Retiring the LTE Network

As the number of devices supporting and needing LTE for connectivity decreases, the LTE component of your network can be retired. This can be done gradually, by decreasing the channel size of the LTE component (going from a 10Mhz/10Mhz split between LTE and 5G NR, to a 5 MHz/15 MHz split), or done all at once.

Migration Options

The 3GPP has provided a number of options for migrating from LTE to 5G. The primary differences lie in how the core network (EPC or 5GC) are connected to the base stations (eNBs and gNBs), and how the base stations are able to communicate with directly with each other. Options 3 and 7x are the most common options, and are what we describe above.

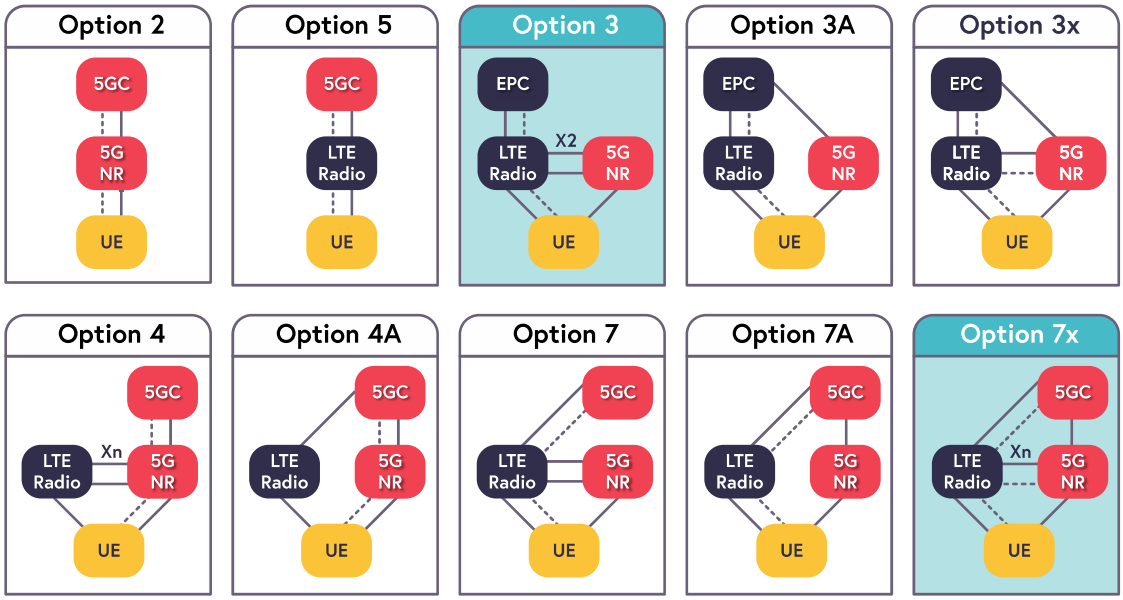

Figure 18: Migration options for moving from LTE to 5G.

Gathering Requirements

The first step in any successful deployment requires a detailed understanding of your organization's needs and the problems you wish to solve by deploying an OnGo Private 5G network. Start by identifying your critical use cases, so your networking team, or an OnGo service provider, can design a system to meet your needs.

Understanding Needs, Use Cases, & Problems to be Solved

The first step in gathering requirements is to identify the critical use-cases for your OnGo Private 5G network. Here we provide a list of questions you should consider when defining your network requirements:

- What is the primary purpose of your Private 5G network?
  - For example, will the network need to provide data connectivity for IoT devices, or will it be used exclusively for mobile phones? If for mobile phones, will your mobile devices also require support for data? The answers to these initial questions will drive many decisions and provide the answers to the more detailed questions below.
- Who will be connecting to your Private 5G network?
  - Should access to the network be limited to a static list of users? Employees of your organization only? Or will visitors, external partners, or guests also require access to the network?
  - Will users require privileged access to critical business assets? Will users be members of particular groups requiring constant wireless connectivity, such as executive leadership, IT, security, or development? Understanding roles and access privileges will ensure proper authentication and security, as well as your device and user-provisioning needs.
- What will be connecting to your network?
  - This can include gateways, internal communication channels, and applications, as well as IoT devices, cameras, and various mobile user devices.
  - If you have existing devices that you want to connect via your Private 5G network, what interfaces do they have?

- Can you group your user/devices into distinct “classes” with different needs?
  - If a couple of different classes of users and devices can be identified, it may make sense to divide your private network into multiple slices, and consider the answers to the questions given here for each slice.
- What services will be provided over your network? Where are they hosted? Do any of them need low-latency connections?
  - Applications needing low-latency may require the service to be located on-premises, or within your existing network infrastructure. It can also influence the choice of your RAN architecture, as options like vRAN can add additional latency.
  - Services located on-premises (or in your own cloud) can be incorporated into your network as MEC services.
- What level of security do you need?
  - To supply enterprise-grade 5G security (e.g., device authentication, traffic encryption), an OnGo network requires little to no extra work. If you need additional protection, you should define your security requirements as early as possible. Access to specific services can be restricted to specific slices, as an additional security measure.
- Are the devices connecting to your network going to be mobile or fixed-in-place?
  - Fixed and mobile devices have different network architectures and device-management requirements.
- How many users, devices, or IoT nodes will access the network?
  - Whether you need to support hundreds or thousands of connections, correctly scoping the network is crucial to achieving the required performance.
- What type of traffic will those users and devices be generating?
  - For example, the data requirements of a voice call are very different from a device periodically providing status updates.
- What will the devices be connecting to?

  - If devices and users need to connect to other company networks or the Internet at large, you need to make provisions for backhaul communications. However, backhaul support may be unnecessary if the devices will be sending data only among each other.

- Will mobility into and out of the network be needed?
  - If needed, you can configure your Private 5G network to allow devices to roam seamlessly into and out of the network. Arrangements must be made with existing network operators to support roaming to and from their systems.
- In what type of environment will the system be deployed?
  - Given that OnGo Private 5G networks function both indoors and outdoors, your specific environment will determine many aspects of your system.
- What wireless data infrastructure do you already have?
  - If you have an existing WiFi network, you can allocate devices and data traffic to the system that best supports your needs. This can improve the performance of both networks.
  - If you already have an LTE system deployed, you will need to consider it as you design your deployment, and how you will migrate from LTE to 5G.
- How mission-critical is your network?
  - The CBRS band provides multiple levels of licensing, with licensed users having priority when allocating channels. If your deployment requires high availability, you may need to engage the services of a provider with a PAL license.
- What growth do you anticipate over the next one-to-three years?
  - If you expect to add more users, nodes, functionality, or sites, you should plan your deployment accordingly.
- What kind of infrastructure deployment approach do you prefer for the network and management elements – on-premises, cloud, hybrid cloud?

  - If you already have on-premise hosting options, hosting locally may make sense. However, if preferred, some or all of the network elements may live in the cloud.

- How do you want to install, operate, and own the network?
  - For example, does your organization want to capitalize some, or all, of the equipment? Or would you prefer subscription services? Will your internal team manage the core network, or do you want a managed services option? OnGo deployments provide the flexibility to match your service deployment needs with your business model.

This guide will take you through the different deployment processes for two separate sites, each with very distinct requirements. Scenario A is a typical new building deployment. Scenario B is for a larger and more complex sports venue. By going through the detailed deployment process of each, we hope to give you clear examples to help guide the planning of your network.

Once you've determined your primary use cases and requirements, the next step is to begin planning your deployment.

Nominal Design

For in-building or venue applications, collect floorplans and do an initial coverage design. Working this out during the initial design will create a proposed blueprint for antenna/CBSD placement. The site survey, described below, offers you the opportunity to verify the design and make changes based on constructability.

Site Survey

To begin, you'll also need to survey the area you intend your network to cover and how many CBSDs will be required, along with their location. The frequency band where CBSDs operate (3.5 GHz) does not propagate in the same way as "regular" 5G signals and operates at a lower power level (<50 watts) than a macro 5G cell. While the actual list of information required to plan a full deployment may be longer, here are some examples of the type of information you'll need to cover the overall dimensions of the area, such as the length, width, height, area usage type, etc.:

- Dimensions of the outdoor coverage areas.
- Dimensions of the indoor coverage areas.
- Wall dimensions and construction materials, such as concrete, wood, metal studs, etc.
- Location and dimensions of structures in the area, including large pieces of furniture, large objects, obstructions, construction materials, etc.
- Locations of power and data sources, as well as inaccessible areas. Note: If the Wi-Fi infrastructure already exists, you can use the Wi-Fi Access Points as a simple way to map out convenient locations for CBSDs.
- The location of Wi-Fi Access Points and other wireless communications infrastructure, such as DAS or small-cells.
- Areas of potential interference (incumbents, radars, cell towers, etc.).

- The current and expected device and subscriber density. You need to understand the expected end use cases, such as IoT device types, mobile users, etc.
- Location and availability for on-site infrastructure elements as required (data center, networking elements, network management systems, controllers, etc.).
- Location and interfaces, including wired and wireless, of any existing devices that will connect to your network.
- Location of equipment closets, fiber points of presence, power and grounding, cable trays, and the conduit between floors, etc.
- Any future planned remodeling or construction.

These questions are here to help you scope out the overall scale of the deployment. During deployment, installers will require special tools for measuring signal strength and propagation to ensure complete network coverage. It's also good to conduct a baseline walk test with a scanner to understand what other signals are present and their relative strength in the planned coverage area so you can determine what design margins are required for co-channel penetration.

If your site already has Wi-Fi infrastructure, you can use a high-level rule-of-thumb to determine your CBSD requirements. For indoor deployments one CBSD will typically supply the equivalent coverage of two to three Wi-Fi Access Points. For outdoor deployments, one CBSD can replace from 12 to 20 Wi-Fi Access Points depending on terrain and other factors.

Adjacent LTE and 5G Networks

It is often helpful to know what other LTE or 5G networks are in your area and some basic configuration information about those networks. Although a SAS can provide basic information about other LTE and 5G networks in the CBRS band, other LTE/5G networks are also of concern. Information you want to know includes:

- The band/channel those networks are using.
- Signal level penetration of adjacent networks into the proposed coverage area.

- The Tracking Area Codes, Mobility Management Entity Codes and Group IDs (MMEC and MMEGI), and the Physical Cell Identities used by those networks (see the Identifiers section for more information).

You can get some of this information using the Field Test Mode on devices connected to that network. The details on how to activate and use this mode depend on the device. Typically, activation involves dialing a unique code on the phone, which you can find with a basic internet search. Several websites (such as http://www.cellmapper.net/ or http://www.antennasearch.com/) provide tower and network information and can help identify other networks in your area. The PSPs can also provide this information for their networks.

CBRS Band Availability

The SASs can provide information about channel availability in the area, and potential interference sources. This includes any deployed PAL operators, and other incumbent users that may have higher access priority.

Planning – Indoor/Outdoor, Use Cases, Spectrum Usage

You can now begin planning where to place your CBSDs. CBSDs have different power limits depending on their class: One watt for Category A devices (indoor or outdoor) and 50 watts for Category B devices (typically outdoor). In general, a one-watt CBSD can effectively cover about 10,000 square feet in a typical office environment. For outdoor applications, a 50-watt CBSD has an average effective range of 1.5 – 2 miles using an isotropic antenna 160-feet above the ground. To avoid interference with any others in the area using the same band, CBSDs may have to lower their power levels. As a result, the range of the CBSDs, particularly outdoors, may be reduced on occasion.

In addition to range considerations, you'll need to estimate the number and types of devices connecting to each CBSD, so you can determine your data bandwidth requirements. This analysis allows you to estimate the capacity needed on a given CBSD. Finally, you'll need detailed modeling of the signal propagation to estimate the worst-case available bandwidth and confirm if there will be sufficient capacity on a given CBSD for different channel configurations.

Throughput Calculation

Determining the throughput capacity of a 5G network is non-trivial. It depends on multiple factors of how the network is configured, the capabilities of the devices, and the level of interference. As a first order estimate, we provide some tables of expected maximum downlink and uplink capacities. We also provide links to some online tools, and the full equation from the 3GPP. Before we get to the tables, we need to define some terms.

Channel Size

5G can use a variety of channel sizes. In the CBRS band (n48) it can operate in a channel as small as 5 MHz, and as large as 100 MHz. Channels are requested in 10 MHz intervals from the SAS, with a single PAL holder able to get 40 MHz of spectrum. Through use of carrier aggregation (CA), multiple channels, both within the CBRS band and outside of it, can be combined to further increase bandwidth capacity. Devices (gNBs/CBSDs and UEs/EUDs) are typically limited in how much bandwidth they can use.

Carrier Aggregation

5G supports the bundling of channels to provide additional bandwidth via a mechanism known as Carrier Aggregation (CA). A CA capable device can operate within the CBRS band, allowing multiple 10 MHz channels to be combined. These channels can be contiguous or non-contiguous for maximum flexibility. While there is some additional overhead, for estimation purposes you can just add the bandwidth of each CA channel together.

Sub-Carrier Spacing

The 5G NR RAN, as an OFDM system, transmitters use multiple sub-carriers operating on a single channel. In band n48, these sub-carriers can operate with a sub-carrier spacing of 15 or 30 kHz. In general, 15 kHz sub-carrier spacing has slightly higher capacity, but is a bit more susceptible to interference.

Modulation

In 5G, different modulation rates can be used to encode data. Higher modulation rates allow multiple bits to be sent simultaneously, but are more susceptible to interference.

5G automatically adjusts the modulation rate in response to interference. Can be QPSK, 16QAM, 64QAM, or 256QAM – with 256 QAM only available on the downlink.

Layers

This represents the number of different beams being used to transmit data using MIMO techniques. More beams mean more data, but are more prone to interference. The maximum is 8 in the downlink, and 4 in the uplink. 2 is a typical value, with 4 or 8 possible in ideal beam-forming conditions, if the devices support it.

Time Division Duplexing (TDD)

OnGo networks use Time Division Duplexing (TDD), with the CBSDs/gNBs and EUDs/UEs using the same frequency channel, but transmitting and receiving at specific times. In 5G, the network can dynamically shift between an uplink or downlink heavy configuration, as needed, switching between a number of different formats for allocating time slots to the uplink and downlink. There are some limitations, but broadly speaking, the channel can be almost completely allocated to downlink or uplink. Different gNBs can support different TDD configurations, but are required to at a minimum support allocating ~55% and ~75% to downlink (10 of 18 and 14 of 18 slots with 30 kHz sub-carrier spacing, and 4 of 9 and 7 of 9 with 15 kHz subcarrier spacing).

Pre-Calculated Tables

The below tables provide maximum capacities for various conditions and channel sizes, assuming the channel is fully allocated to downlink or uplink. To get the value in the default configurations, multiply the final value by 55% or 75% on the downlink, or 45% and 25% for the uplink.

Table 5: Typical Peak Downlink Bandwidths [Mbps] by Channel Size

Channel Size [MHz]	Conditions	Modulation	Layers	30 kHz Sub-Carrier Spacing DL Bandwidth [Mbps]			15 kHz Sub-Carrier Spacing DL Bandwidth [Mpbs]		
				Max	75%	55%	Max	75%	55%
10	Ideal	256 QAM	4	206	155	113	222	167	122
10	Moderate	256 QAM	2	102	77	56	112	84	62
10	Poor	64 QAM	1	38	29	21	42	32	23

20	Ideal	256 QAM	4	436	327	240	454	341	250
20	Moderate	256 QAM	2	218	164	120	226	170	124
20	Poor	64 QAM	1	82	62	45	86	65	47
40	Ideal	256 QAM	4	924	693	508	908	681	499
40	Moderate	256 QAM	2	462	347	254	454	341	250
40	Poor	64 QAM	1	174	131	96	170	128	94

Table 6: Typical Peak Uplink Bandwidths By Channel Size

Channel Size [MHz]	Conditions	Modulation	Layers	30 kHz Sub-Carrier Spacing UL Bandwidth [Mbps]			15 kHz Sub-Carrier Spacing UL Bandwidth [MBps		
				Max	25%	45%	Max	75%	45%
10	Ideal	64 QAM	4	164	41	74	178	45	80
10	Moderate	16 QAM	2	54	14	24	60	15	27
10	Poor	2 QPSK	1	14	4	6	14	4	6
20	Ideal	64 QAM	4	364	91	164	350	88	158
20	Moderate	16 QAM	2	122	31	55	116	29	52
20	Poor	2 QPSK	1	30	8	14	30	8	14
40	Ideal	64 QAM	4	728	182	328	742	186	334
40	Moderate	16 QAM	2	242	61	109	248	62	112
40	Poor	2 QPSK	1	60	15	27	62	16	28

Online Calculation Tools

There are several online tools that implement the formula (https://tools.pedroc.co.uk/5g-speed/ or https://5g-tools.com/5g-nr-throughput-calculator/). These take care of the calculations for you.

Manual Calculation

The throughputs can be calculated depending on several parameters such as NR-Band, Sub Carrier Spacing, channel Bandwidth, Scaling Factor, downlink and uplink Layers, TDD Pattern configuration, Downlink and Uplink Modulation supported. The formula used to calculate the bandwidth is rather complicated:

$$10^{-6} \cdot \sum_{j=1}^{J} \left(v_{Layers}^{(j)} \cdot Q_m^{(j)} \cdot f^{(j)} \cdot R_{\max} \cdot \frac{N_{PRB}^{BW(j),\mu} \cdot 12}{T_s^{\mu}} \cdot \left(1 - OH^{(j)}\right) \right)$$

- J – The number of aggregated component carriers in a band or band combination. For most OnGo Private 5G deployments, this will be 1. If you are aggregating with channels outside the CBRS band, then this number will be higher. The bandwidth calculation is effectively a sum of the bandwidths for each component carrier.
- R_{max} – This is a constant (948/1024).
- v_{layers} – Number of multiple-input multiple output (MIMO) layers – maximum of 8 in the downlink, 4 in the uplink. 2 is a typical value, with 4 or 8 possible in ideal beam-forming conditions.
- Q_m – The modulation order, with higher modulations possible in good conditions. Can be 2 for QPSK, 4 for 16QAM, 6 for 64QAM, 8 for 256QAM. 8 (256 QAM) on the downlink and 6 (64 QAM) on the uplink are typical.
- $f^{(j)}$ – Scaling factor, which reflects the ability of the device to handle high modulation orders on multiple carriers, and can take any value from 1/0.8/0.75/0.4. A scaling factor of 1 can be used with most devices.
  - Note: Devices much be able to support a values of v_{layers}, Q_m, and $f^{(j)}$ such that $v_{layers} \bullet Q_m \bullet f^{(j)}$ is at least 4.
- μ – The 5G NR Numerology, which can take any value from 0 to 4, and defines the sub-carrier spacing. For an OnGo Private 5G deployment, this value can range from 0 to 2, and is either 1 (for 30 kHz SCS) or 2 (for 15 kHz SCS). The μ value is used to calculate two different values:
  - $T_s^{\mu} = 10^{-3}/(14*2^{\mu})$ – Average OFDM symbol duration in a subframe for a given μ value.
  - $N_{PRB}^{BW(j),\mu}$: Maximum resource block (RB) allocation in bandwidth, BW(j)with numerology (μ). The value can be found by referencing the below table. For a

typical OnGo Private 5G deployment in a 10 MHz channel, the μ value is 0, so the value should be 52.

Table 7: $N_{PRB}^{BW(j),\mu}$ lookup table.

μ	Sub-Carrier Spacing [kHz]	Channel Bandwidth [MHz]								
		10	20	30	40	50	60	80	90	100
0	15	52	106	160	216	270	NA	NA	NA	NA
1	30	24	51	78	106	133	162	217	245	273
2	60	11	24	38	51	65	79	107	121	135

- OH(j) – The overhead, which depends on the frequency range and the link direction. For an OnGo Private 5G deployment, which uses the frequency range of the CBRS band (FR1), the value is 0.14 for calculating the Downlink, and and 0.08 for the Uplink.

This gives the available bandwidth for the channel – since OnGo Private 5G networks typically operating in a time-dividsion duplex (TDD) configuration, with the uplink and downlink sharing the channel.

Table 8: Calculation Example – Downlink

Element	Value
Frequency Range Designation	FR1 (Sub6) 450-6000 MHz
Frequency Band	n48: 3550-3700 MHz
μ (Numerology)	1
Sub-Carrier Spacing (from μ)	30 kHz
Bandwidth	10
Scaling Factor	1
Layers	2
Modulation	8 (256QAM)
$N_{PRB}^{BW(j),\mu}$ (Max Resource Blocks)	24
OH (Overhead)	14%
Downlink Maximum Bandwidth [Mbps]	102

Table 9: Calculation Example – Uplink

Element	Value
Frequency Range Designation	FR1 (Sub6) 450-6000 MHz
Frequency Band	n48: 3550-3700 MHz
μ (Numerology)	0
Sub-Carrier Spacing (from μ)	15 kHz
Bandwidth	10
Scaling Factor	1
Layers	2
Modulation	6 (64QAM)
$N_{PRB}^{BW(j),\mu}$ (Max Resource Blocks)	24
OH (Overhead)	8%
Uplink Maximum Bandwidth [Mbps]	82

Simulation

An accurate estimate of available capacity requires simulation of signal strength and quality in the target location using a combination of direct measurement and software simulation. This is often done at design-time as part of determining the optimum placement of CBSDs. System integrators and service providers can provide this as a service.

Needed Capacity Calculation

Next up is to estimate how much bandwidth the targeted use cases will need. You should also note where the data streams are going. If your traffic is staying entirely within your private network, any connection to external networks will be unaffected. However, if you are going to send multiple video streams to the Internet, your backhaul infrastructure will need sufficient capacity to handle the load.

Throughput needs of some various applications:

- 480p video (640x480) – 2.5 Mbps
- 720p video call (1280x720) – 3 Mbps (each way)
- 1080p HD video (1920x1080) – 8 Mbps
- 4k HD video – 20–25 Mbps

- Normal voice call – 12 kbps
- HD voice call – 50 kbps

Note: When a device is moving, its effective bandwidth demands increase. If this is the case, we recommend you add an additional 10% to your calculated bandwidth requirements for planning purposes.

Based on your total bandwidth needs, you can estimate the number of channels you will need. If your scenario needs more data than can be provided in a single channel, you can deploy multiple channels – either operating as a single 20 MHz channel, or using carrier aggregation to provide more throughput. The network can also allocate downlink and uplink data in different ratios, allocating for more (or less) uplink capacity.

TDD Synchronization

In the CBRS band, 5GS (and LTE) systems must operate in TDD mode. In congested environments, where coverage areas from different OnGo networks are close by or overlap, they are susceptible to crosslink interference. Crosslink interference occurs when a CBSD higher-power downlink transmissions drown out the lower power UEs uplink transmissions in nearby cells. Crosslink interference can even occur when CBSDs are operating on adjacent frequency channels. This interference can be of particular concern when the OnGo network is outdoors, using higher-power Category B CBSDs, or is deployed near another OnGo network using Category B CBSDs. More details on crosslink interference can be found here: https://www.ericsson.com/en/blog/2020/6/cross-link-interference-tdd-networks.

Crosslink interference can be reduced by having the CBSDs use the same TDD uplink/downlink patterns, and synchronizing the timing between the CBSDs. 5GC already has existing mechanisms for synchronizing timing between gNBs, using GPS or similar signals for a common timing reference, which is critical for proper functioning.

However, a mechanism is still needed to ensure that the CBSDs are using the same TDD uplink/downlink patterns. The OnGoA is defining an optional coexistence manager (CxM) system element of the SAS to help coordinate between OnGo Networks to minimize TDD-related interference within the CBRS band. A SAS that supports the CxM

is referred to as a CSAS. This system will coordinate between OnGo networks to select an appropriate TDD configuration, based on their desired TDD configuration, if the CBSD is part of a related group of CBSDs, and measured interference between CBSDs. CBSDs are guaranteed to at least be able to use the default ~55% or ~75% downlink TDD configurations. This may constrain what TDD configurations your network can use, but you'll experience significantly reduced interference.

These systems are not yet deployed, as of this writing. Until these systems are online, you'll need to coordinate directly with other OnGo networks in your area to determine which TDD configurations won't interfere with those networks, or with your network. In addition, some of the existing SAS features, such as CxG groupings, as well as channel guidance and selection, can be used to help reduce crosslink interference, if your CBSDs support them. An integrated solution provider integrator will be able to help with these issues, if needed.

PAL vs. GAA

For most private indoor 5G deployments, you should not require a PAL. However, consider sublicensing a PAL if your implementation meets any of the following criteria:

- Large area or outdoor deployment – If your implementation uses Category B (outdoor) CBSDs, or otherwise covers a large geographic area.
- Mission-critical – A PAL gives you priority access to the licensed channels, and SAS assurance of interference free operation, increasing the chances of spectrum access.
- Crowded environment – For example, if your network is in a very dense urban environment. As noted earlier, PAL users are afforded protection from GAA users.

The FCC auctioned PALs on a per-county basis. Light-touch leasing rules allow for PALs to be sublicensed within a county, outside of areas where the PAL owner is broadcasting. PAL holders are not required to sublicense. Information on the PAL auction results and winners is here: https://www.fcc.gov/auction/105.

The FCC auctioned PALs on a per-county basis. Light-touch leasing rules allow for PALs to be sublicensed within a county, outside of areas where the PAL owner is

broadcasting. PAL holders are not required to sublicense, but can do so at their discretion. Information on the PAL auction results and winners is here: https://www.fcc.gov/auction/105.

What is a PAL, and Do I Need One?

There are three tiers of access to the CBRS band:

- Tier 1: Incumbent users such as the federal government and fixed satellite users.
- Tier 2: Priority Access License (PAL) users—licensed wireless users who acquire spectrum through an auction. The SAS will ensure PAL users don't cause harmful interference to Tier 1 users and will protect PAL users from interference by General Authorized Access (GAA) users.
- Tier 3: GAA users who deploy "lightly-licensed" devices. The SAS ensures GAA users don't cause harmful interference to Tier 1 incumbents or Tier 2 PAL users.

Of the 15 CBRS channels, PALs are available for up to seven in the lower 100 MHz. Unused channels (and channels not being used by the incumbents) are available for GAA users. PAL users do not receive guaranteed access to a channel but are much less likely to be denied access by the SAS.

If a PAL holder fails to use their allocated channel(s) for more than seven days, the SAS frees up those channels for GAA users.

Whether or not you need a PAL depends on several factors:

- How critical your network is to your operations? PAL holders are much less likely to be impacted by other users and can only be denied access when an incumbent user needs access to the channel.

Vendor Identification

As part of deploying your Private 5G network you will need to select your vendors. In the planning stage, you should begin to identify potential vendors. Once you reach the design stage, you will need to select your vendors.

As an alternative to contracting with individual vendors, many companies provide integrated Private 5G solutions and services. They provide turn-key solutiuons that

include everything you need to deploy a Private 5G network, including CBSDs, 5GC applications, SIM and subscriber management, CPI services, and SAS subscriptions. These vendors can take care of the details of planning, design, installation, and operations support for your Private 5G network. In 2021, many telecommunications and cloud service companies announced Private 5G solution offerings, in addition to startups that offer innovative solutions. Many of these providers are members of the OnGo Alliance. A list of our members can be found here: https://ongoalliance.org/members/.

SAS Administrators

The FCC has already approved several SAS administrators. While the FCC defines the essential functions of the SAS, each SAS vendor offers a variety of additional services and a range of commercial terms. You can view a list of current SAS administrators here: https://cbrs.wirelessinnovation.org/sas-administrators.

CBSD Vendors

Multiple CBSD vendors offer OnGo-certified devices. Differences between vendors include power levels, antennas, number of devices, throughput, support for virtualization options like CRAN or vRAN, Open RAN support, and other configuration options. A complete list can be found here: https://www.ongoalliance.org/certification/.

5G Core (5GC) Vendors

To function, OnGo CBSDs must connect to a 5G Core. The 5GC provides mobile device management functions in the control plane and enables data packet exchanges between the mobile device and applications in the packet network on the data plane. You may deploy an 5GC on-site, co-locate with the CBSDs, or use a cloud- based 5GC service. CBSDs interoperate with the 5GC; therefore, it is essential that you select a compatible 5GC.

Element and Device Management System (EMS/DM) Vendors

The EMS and DM systems are tightly integrated with the CBSD and the 5GC. The EMS typically provides control, configuration, management, and data collection services for

the 5GC. At the same time, the DM handles lifecycle management for the CBSDs, including activation, configurations, and fault and performance management. The EMS/DM may be provided by the CBSD or 5GC vendor, or by independent network management vendors that support the necessary management standards.

End-User Devices (EUDs)

Of course, critical to an OnGo Private 5G deployment are the EUDs, also referred to as user equipment (UE), that will connect to your network. Any 5G UE device that supports band n48 can connect to an OnGo network. Fortunately, many handsets on the market today already support band n48.

If you have existing devices that you want to connect to your Private 5G network that do not support band n48, you will need a bridging device. This can be a USB dongle or similar device that connects to an existing physical interface. If the device supports another wireless technology, the use of an OnGo EUD bridge in this manner can extend your OnGo Private 5G network to include multiple devices, effectively using OnGo as a backhaul connection.

The complete list of FCC-authorized EUDs that support band n48 can be found on the OnGo website: https://ongoalliance.org/certification/fcc-authorized-end-user/.

SIM Provisioning

You will also need a system for provisioning SIMs. You can purchase either a dedicated UICC writer, or a software package for eSIMs. The type of SIM provisioning system you need is based on the EUDs that will connect to your network. SIM provisioning is typically part of an EMS/DM solution, but you may need to acquire this capability separately.

Certified Professional Installer (CPI)

The FCC Part 96 rules that define CBRS generally require that CBSDs be registered with the SAS by a Certified Professional Installer (CPI). All Category B CBSDs, and any Category A CBSDs that cannot self-geolocate, must be registered by a CPI. While CPIs are not required to install the CBSDs themselves, they are responsible for the accuracy of the registration data.

There are currently several training options for CPIs. You can find a list of WInnForum-accredited Training Program Administrators (TPAs) here: https://cbrs.wirelessinnovation.org/cpi-program-administrator.

Networking Plan

The primary consideration for IP networking is what type of physical network infrastructure your CBSDs will use to connect to each other and your internal network. Different CBSDs support different interfaces for their backhaul connections – Ethernet, optical fiber, or even wireless links. If your CBSDs use Ethernet for their backhaul, your existing Ethernet infrastructure for your Wi-Fi network may work just fine for your OnGo deployment. However, if your deployment will use a lot of channels to support very high bandwidths, or your network infrastructure already carries significant traffic, make sure your backhaul connection has enough available bandwidth to support your needs. If not, you may need to add additional backhaul capacity.

If using CBSDs (gNBs) that support virtualization options like DRAN, CRAN or vRAN, you also need to consider the fronthaul connections between the BBU and RRHs. For DRAN and CRAN, these are usually optical fiber, while you can use ethernet for vRAN. In either case, these systems are very bandwidth hungry, so if you intend to use existing infrastructure, make sure there is sufficient bandwidth available.

You also need a backhaul connection if your system interfaces with other networks (such as the public Internet). As with the internal network, ensure that your total backhaul capacity can support the amount of data you will be carrying. The contract often sets the bandwidth, so check to see if you have sufficient bandwidth to meet your needs. Even if your network doesn't provide access to the Internet, the CBSDs and Domain Proxies must be able to connect to the SAS. That's why we recommend installing high-availability or redundant connections wherever possible. Otherwise, your CBSDs will shut down if they can't check in with a SAS periodically.

As a general rule, bandwidth demand rises 30% per year. So, rather than aiming for "just enough," we recommend building in additional bandwidth, particularly in your on-site infrastructure. You can increase backhaul bandwidth relatively quickly, but

installing more cables is a lot more difficult. Most plan for twice your current bandwidth needs to provide reasonable headroom for growth.

Customer Premises Equipment and CPE-CBSDs

In the telecommunications world, the term "Customer Premises Equipment" (CPE) is widely used. Unfortunately, the term's exact definition can often vary depending on the segment of the industry and the technology in use. In the OnGo context, the term CPE officially means an LTE UE operating in the CBRS band. However, the term is often applied to any non-mobile device that is part of an OnGo network, especially if the device does not face an end-user, including CBSDs. Therefore, if you see the term CPE, clarify what it means.

There is also another type of CBSD called a CPE-CBSD. A CPE-CBSD can transmit at a higher total power level (>23dBm EIRP) than other end-user devices (EUDs) but only after it's registered with the SAS. These devices are typically used in Fixed-Wireless Access (FWA) applications, as a CPE-CBSD must be non-mobile. In addition, since they have a higher transmit power level, CPE-CBSDs can connect to a base station at a more extended range than normal EUDs.

In an OnGo deployment, a CPE-CBSD can be an LTE UE (EUD) that can connect to another CBSD over longer distances than other UEs. It may also include an eNB, allowing the CPE-CBSD to extend your coverage area when wired backhaul is impractical.

Security

Any network system must address security. Fortunately, OnGo has 5G security "baked-in" to the system, so achieving enterprise-level protection of the wireless link is relatively easy. All elements of your deployment will need to consider both physical and cyber security in the design to ensure that the overall system is secure. Security needs should be considered in your selection of CBSDs and management systems.

CBRS uses digital certificates for security purposes, authenticating and securing communications between elements of the system, including the SASs, CBSDs, and Domain Proxies. If you have an existing Public Key Infrastructure (PKI), leverage it to generate the certificates used by your system, or rely on the certificates provided by the manufacturers.

See the 5G Security section for a discussion of the security features of 5G.

Existing Data Infrastructure

When planning your OnGo deployment, consider any existing data infrastructure, particularly other wireless systems such as Wi-Fi. OnGo excels at providing mobility and coverage in complex RF environments; and reliable, consistent connectivity for a large number of connected devices. In a multi-network architecture, assigning devices (and their traffic) to the most appropriate network can improve the entire network's performance. As a simple example, fixed devices can be placed on a Wi-Fi (or wired ethernet) network, while mobile devices and devices in locations with poor Wi-Fi connectivity can be assigned to the OnGo network.

Business Case

When deploying any new system, it is essential to assess both costs and benefits. While the details differ with each system, keep in mind that once you have deployed an OnGo Private 5G network to address a particular use case, the incremental cost to support additional use cases is much lower. Adding incremental use case cases (such as a Neutral Host Network) the deployed private 5G network can significantly improve the network's ROI. And with the network slicing capabilities of the 5GC, these new use cases can be deployed without impacting the security and performance of your initial use cases.

After defining the network capabilities needed for your Private 5G deployment, site surveying your location, and selecting vendors, the next step is identifying the network elements best suited for your deployment, including endpoint devices, a radio system, access points, and core network services. The easiest path for many enterprises is to contract with a managed service provider or system integrator. Both can provide design and implementation services, as well as select the appropriate vendors for your deployment.

Vendor Selection

SAS Selection

In this stage, you'll need to contract with a SAS administrator to provide service for your deployment. Different SAS administrators will offer a variety of commercial and contract terms (per CBSD, flat fee, etc.). Select the one that best supports your deployment. Your choice of a SAS administatror will depend on many factors, including:

- Commercial terms for interfacing with the SAS.
- Additional services provided by the SAS administrator, such as spectrum planning and area information.
- Support for the Coexistence Manager element (CxM).
- Does the SAS administrator have ESC sensors deployed for your area?
- Need for a Domain Proxy (see below).

CBSD Selection

Now you are ready to select the CBSDs. The general requirements that you should consider when choosing a vendor include:

- Indoor and outdoor CBSD options.
- Supported power levels.
  - Category A devices can transmit up to one watt of power, but many vendors offer options with lower power levels.

- The number of devices each CBSD can support.
- Uplink/downlink configuration support.
- Need for a CPI (see below).
- Carrier aggregation support (uplink and downlink) if bandwidth needs require more than one channel.
- Lifecycle management capabilities (activation, provisioning, operating, monitoring).
- Backhaul options.
- Ability to support multiple-location deployments in a single platform.
- Flexibility of adding new CBSD devices from different vendors.
- Integration capability with existing Fault/Performance Management and other systems.
- Integrated Domain Proxy capabilities.
- Support for DRAN, CRAN, or vRAN (if desired).
- Ability to use certificates from existing PKI (if any).
- Price.

5GC Selection

Selecting 5GC vendor(s) is based on multiple factors:

- Support for needed NFs.
- Number of connected UE devices supported.
- 5GS release support (release 16 supports use of OnGo SHNI).
- Cloud/virtualization support.
- Hardware requirements.
- Network slicing configuration options.
- MEC configuration options support.

- Security services provided, such as use of hardware-based security, etc.
- Price and pricing model.

In theory, NFs can be provided by different vendors, as the interfaces between them, and with the gNBs, are standardized. In practice, we recommend that you check that the different components are compatible.

Element Management System (EMS)/Device Management (DM) Selection

An EMS/DM can be located on the premises or in the cloud. It can also reside side-by-side with the 5GC and perform 5GC and Device (CBSD) management functions. Key considerations include:

- Standards support (SNMP, TR-069, NetConf, etc.).
- Simplified dashboards of overall status, and key performance indicators, and alarms.
- CBSD Device Management capabilities to enable ease of device deployment and ongoing management.
- Data analytics and reporting of Key Performance Indicators (KPIs) and other performance metrics.
- Fault management and alarming.
- Troubleshooting and diagnostic support.
- Redundancy and resiliency.
- Ability to support multiple-location deployments in a single platform.
- Flexibility of adding new CBSD devices from different vendors.
- Integration capability with existing Fault/Performance Management and other systems.

CPI Selection

It's also time to select a CPI. Key considerations include understanding the payment terms and additional services the CPI can provide. The CPI can be an internal resource, as long as the person is trained using one of the authorized Training Program Administrators (TPAs), described above.

Note: Some Category A CBSDs have an auto-sensing function that can detect their location using GPS/GNSS and don't require a CPI to register their configuration with the SAS.

Do I Need a CPI?

For some OnGo deployments, you may not need a CPI. For example, you should be able to skip having a CPI involved if all of the following are true:

- Your NHN is not a MORAN (or DAS) deployment.
- All of your CBSDs are Class A (< one watt).
- All of your CBSD antennas are less than six meters in height above average terrain.
- All of your CBSDs include the capability to determine their location automatically.
- You aren't using a PAL.

CBRS Channel Selection

There are 15 channels of 10 MHz size available in the CBRS band. While each channel has similar propagation characteristics, which channel(s) your network operates can greatly impact the performance of your network, as they can have different levels of interference from other networks operating in the CBRS band. Crosslink interference (described above) can vary based on which channels you use.

Some channels may be allocated to a PAL – even if they aren't in active use. While you may be able to use those channels, if the PAL holder starts using them in your area, you will be directed by the SAS to relocate to other channels.

Multiple channels can be used as well, allowing for additional bandwidth via carrier aggregation (CA). Or you may want adjacent CBSDs to operate on different channels to reduce interference between the CBSDs. Which option provides better performance requires detailed modelling, as discussed in the Design Optimization section, below.

Your SAS administrator will be able to provide you with information about the PAL channels allocated and in use in your area, and may be able to provide guidance on which channels have the least interference.

CBSD Configuration

The primary element of an OnGo deployment is the CBSDs – the devices that connect with your end-users. Depending on your implementation, you may need one CBSD or many. Exactly how many, where they need to be placed, and how they will be sectored, are functions of the detailed geometry of your site. An RF engineer or solutions provider can ensure that the CBSDs are placed and configured to provide coverage where needed.

Key aspects to consider at this stage include:

CBSD Placement and Sectorization

CBSDs and their antennas need to be placed to provide optimum coverage of the devices using your system with the minimum number of CBSDs. If the area to be covered is large or contains lots of obstructions (walls, trees, and other obstacles), detailed signal measurements and pattern maps may be needed to determine the required coverage.

CBSDs need power and a data connection to the local network (backhaul). The costs of plumbing in power and data feeds can be high and should be considered when planning your CBSD placements. Placing CBSDs where such infrastructure exists (like where there are Wi-Fi Access Points) may reduce the overall cost of deploying an OnGo network.

Channel Configuration

In addition to determining the placement, your CBSDs also need to be configured to support your deployment. For example, you can configure your CBSDs to provide more uplink or downlink capacity by adjusting the number of 10 MHz channels used, and the frame structure of those channels, depending on the kind of data traffic the system needs. Which channels they request access to from the SAS must also be configured,

based on the CBRS Channel Selection analysis given above. CBSDs can be sectorized as well by segmenting the coverage area into different sectors operating in parallel.

Existing CBRS Networks/Incumbents

The presence or absence of other CBRS networks in the area can affect your deployment and should be checked early in the design process. Your selected SAS may be able to provide this information, or use a spectrum analyzer (or similar equipment) to determine potential interference in the area.

Virtualized gNB Configuration

Depending on your deployment, the use of a virtualization option like vRAN may be a good option. The benefit is reducing the cost of each gNB, as the BBU (and the CU) is shared. This benefit can be especially notable when deploying lots of smaller (Category A) CBSDs. The cost is the price of the fronthaul connection between the shared BBU and the RRH, and the potential increase in system latency. If there is optical fiber (DRAN, CRAN) or Ethernet (vRAN) already in place, with sufficient available capacity, you can take advantage of the cost savings with minimal additional overhead.

Domain Proxies

You can group CBSDs behind a Domain Proxy service that communicates with the SAS. The Domain Proxy aggregates all communications from the CBSDs. It provides a single interface point from the SAS to the CBSDs, reducing your configuration and registration complexity, particularly if you have many CBSDs. Whether or not a Domain Proxy is needed depends on the capabilities of the selected CBSDs, as well as the terms offered by your selected SAS administrator. The Domain Proxies are generally CBSD-vendor-specific and are part of the EMS, and are often integrated within the CBSD device.

Design Optimization

Proper placement and configuration of the CBSDs are a critical system component and may go through several revisions during the design process. For example, installing a CBSD in your desired location may be prohibitively costly or impractical, requiring the CBSD to be placed elsewhere. Likewise, signals from adjacent systems and networks

may interfere with your network. That's why measuring signal strengths, and benchmark testing, should be performed to ensure that the CBSDs can provide the needed coverage, and should be repeated as the design is updated and modified during installation.

The SASs, as noted above, can also provide guidance on the location of any nearby incumbents, availability of channels, and any likely power restrictions in your area.

5GC Network Design

The 5GC has many more design options than the EPC is replaces. This section addresses some of the design choices that you will need to consider when designing your 5GC layout.

Hosting Options

You have multiple options for where the 5GC resides physically:

- On premises. This option makes sense for smaller deployments, or when low-latency is needed for some applications or services offered by the network. This option can take advantage of your local IT infrastructure.
- Remote data center. If you have multiple physical locations covered by your network, the 5GC for all of those networks can be located in a central data center. This can be a data center you operate, or one hosted by a third party.
- Cloud based. The 5GC can be fully virtualized, placing it in the cloud. This allows you to rapidly scale your network, and take advantage of reliability and redundancy of cloud-based systems at reduced cost.
- Hybrid. NFs do not all have to be hosted in the same fashion, allowing you to deploy individual NFs as needed. For example, you could host the AUSF (the Authentication Server Function) locally, to maintain control of physical security.

Network Slicing

The capabilities of the 5GS to support multiple virtual networks adds another set of design choices. Individual slices can be tuned to support different users and use cases in a number of ways:

- User Access. Slices can be restricted so that only designated users or devices can access a particular slice.
- Available Services. Slices can have different services exposed to them. For example, a sensor-oriented slice could restrict devices to only access certain data stores attached to your internal network, and not have access to the internet. A guest-user slice could allow visitors to your facility to access the internet, but have no visibility to your internal services.
- Quality of Service. Different slices can have different quality-of-service rules, prioritizing different types of traffic depending on what slice the user or device is using. For example, a guest-user slice could have lower priority and reduced data speeds than a slice for employee users.

How you configure the slices in your OnGo Private 5G network is a function of the use cases your network is supporting. As an initial guide, we recommend categorizing the types of users and devices that your network will be supporting. From there, you can determine if they have different service and performance needs, which will give you a good set of initial candidate slices.

Adding Public Network Slices

You can also add slices to your private network so that the public networks can use your network. This is treated much like any other slices, with the users of the public network able to use the services of their MNO, MSO, or MVNO, but not being able to access the services of your private network. This is the primary way to implement a Neutral Host Network within 5G.

Using Public Network Slices

You can also deploy your private network as a slice of the public network. This is a service that can be offered by the carriers in your area, and the capabilities of such a

slice are subject to commercial terms as set by the carrier. See the next chapter for more information on the different ways this can be done.

Network Services

Closely associated with network slicing is how you will be deploying the services offered by your network. Services can be deployed over the internet in the "traditional" fashion, but they can be integrated into the network directly via the Application Function in the 5GC as a MEC service. They can be pushed all the way to the edge, with the services connected to the gNBs, hosted with your 5GC, in-the-cloud, or in between.

The benefits of pushing your services out to the edge include:

- Reduced latency. For applications that require low latency (<5 ms), pushing to the edge can remove much of the transport latency.
- Reduced backhaul bandwidth. For applications that can create a lot of data traffic, pushing the service to the edge reduces the bandwidth consumed on your network's backhaul links.

On the other hand, deploying services within your own data centers or private cloud can leverage your existing IT infrastructure, maintain physical control of the services and data, and allow you to scale up the services more flexibly.

5G Identifiers

3GPP networks (LTE and 5G) use several identifiers in order to uniquely identify networks. Most significant is the Public Land-Mobile Network Identifier (PLMN-ID) or Home Network Identifier (HNI), which identifies the network to devices.

The number of available PLMN-IDs is limited, and the process to obtain one is complex. In order to facilitate deploying lots of small 5G (and LTE) networks, a PLMN-ID has been reserved for use by networks operating in the CBRS Band – the CBRS Shared HNI (SHNI), which has the assigned value of 315-010.

As of Release 16 of the 5GC specifications, support for the use of an SHNI or shared PLMN=ID has been added. Individual networks using the SHNI are distinguished using a

5GC Network Identifier (5GC-NID). To make things easier for organizations deploying OnGo Private 5G networks, the OnGo Alliance offers a managed identifier service. This service can be used to get a unique CBRS Network Identifier (CBRS-NID) to use as the 5GC-NID. If you use the SHNI, and an assigned CBRS-NID, the 5GC-NID is used in Assignment Mode 2.

Identifiers can be obtained from the OnGo Alliance online: https://ongoalliance.org/ongo-identifiers/. Contact SHNI@ongoalliance.org for additional information on identifiers.

Do I Need a CBRS-NID?

Probably. 5GC allows three different assignment mods for the 5GC-NID. We recommend using assignment mode 2, using the CBRS-NID. In assignment mode 0, you can use a Private Enterprise Number (PEN) as assigned by the Internet Assigned Numbers Authority (IANA), and does not require the PLMN-ID to be unique. If your company already has a PEN, and hasn't deployed an LTE-based OnGo network, this mode can work for you.

Note: Use of the CBRS SHNI is not currently supported for Release 15 Private 5G networks. We are considering adding management of the identifiers needed to support Release 15 with the SHNI. When that service becomes available, we will update this document, and offer them on our web portal (https://ongoalliance.org/ongo-identifiers/).

IMSI Block Numbers

If your network is using devices that connect only to your system, you will need to obtain an IMSI Block Number (IBN), which can be assigned by the US IMSI Administrator (https://imsiadmin.com/imsi-home). Each IBN allows you to create 100,000 unique IMSIs. If you are going to have more than 100,000 devices, you will need an additional IBN. This IBN can be used to generate IMSI numbers to be assigned to a device's SIM card or an equivalent system such as an eSIM.

Backhaul

Now is an excellent time to make sure any additional network infrastructure you will need is in place. You'll need to consider providing power and IP connectivity to the CBSD sites and ensure that the CBSDs have the bandwidth needed to connect to other networks, including the Internet.

End-User Devices (EUDs)

End-User Devices (EUDs) are what connect to your Private 5G network. Devices can include mobile phones, tablets, laptops, IoT devices, internal communication systems or applications, modems, cameras, gateways, or routers to other networks and systems. Because OnGo uses 5G as its foundational technology, industry standards exist for security, interoperability, and service provision.

Many existing 5G devices (UEs) already support OnGo. As long as the chipset used in the device supports the 3.5GHz CBRS band (referred to as band n48 in 5G), the device can use OnGo. Bands n77 and n78 also include the n48 band, so devices that support those bands can (generally) connect to an OnGo network. In many cases, existing equipment can be converted to the OnGo network without replacement, although some devices may need software updates from operators to enable the CBRS band. You can see the list of OnGo EUDs at: https://ongoalliance.org/certification/fcc-authorized-end-user/

Some important considerations when selecting EUDs:

- Does it need to be a consumer-grade or an industrial-grade device?
- Does it support other bands than CBRS?
- Does it support the bandwidth and power levels needed for your deployment?
- Does it support the carrier aggregation configuration of your network?
- Does it support the physical and wireless interfaces you need?
- What kind of SIM does it use? Does it support Dual-SIM operation?

CBRS SHNI and LTE

Using the CBRS SHNI in LTE networks creates some additional problems, with several identifiers that use the PLMN-ID to ensure global uniqueness becoming vulnerable to collisions when using the SHNI. To resolve this problem, the OnGo Alliance provides managed identifiers where needed to ensure global uniqueness. We recommend using one of those identifiers, the CBRS NID, as the 5GC-NID, to uniquely identify your Private 5G network. Since the bit length for the 5GC-NID is longer than the CBRS-NID, you'll need to pad with 13 leading 0 bits.

Our OnGo Private LTE Deployment Guide provides additional information on the managed identifiers used in LTE, and can be found here: https://ongoalliance.org/resource/ongo-private-lte-deployment-guide/

Your OnGo Private 5G network can also interoperate with public 5G networks. This can be as limited as allowing roaming of devices from the MNOs, MSOs, and MVNOs onto your network, or allocating slices on your network for use by the public networks. You can even work with a public 5G network to add a private slice for your own use. This section describes some of the options for interfacing with the public networks when deploying an OnGo Private 5G Network. We start with the roaming use case, which most people are familiar with, and then look at various levels of integration.

Roaming

The most basic level of interaction with the public networks is roaming. With roaming, subscribers to the public networks can use your network. They can make calls from within your network, and receive calls, just as with their own network. They'll see that they aren't on their home network when using your network, and service may be downgraded. To enable roaming, you will need to execute roaming agreements with each of the public network operators (MNOs, MSOs and MVNOs) that you wish to support. In addition to the commercial terms, the 5GC will need to be configured to support roaming. Agreements can be executed with multiple carriers as needed.

IP Exchange (IPX)

IP Exchange (IPX) service providers can also provide roaming capabilities to an OnGo Private 5G network. IPXs provide a business and technical framework for integrating data services across networks, both fixed and mobile. In the private LTE context, they can provide a single point of contact for working with the public carriers (MNOs, MVNOS, MSOs, etc.) so that instead of having to implement roaming agreements with each carrier directly, you just work with the IPX. On the technical side, they also have existing infrastructure for the interconnection between your network and the public carriers, enabling cross-network roaming.

Isolated OnGo Private 5G

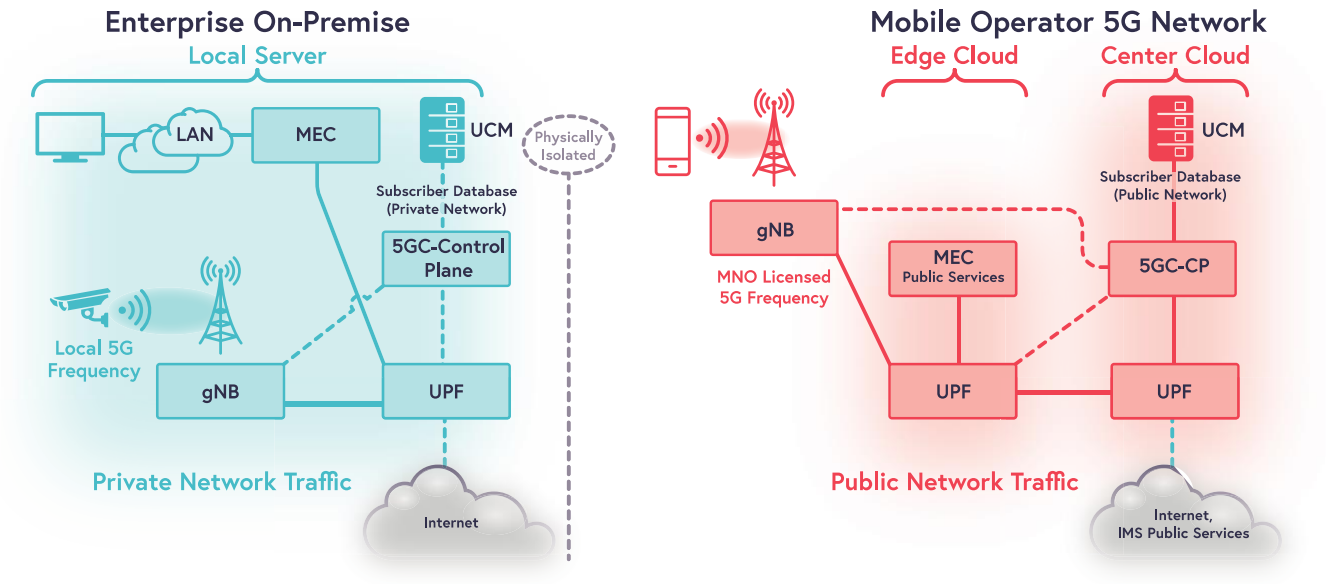

Figure 19: Isolated OnGo Private 5G network architecture diagram.

This is the default scenario for an OnGo Private 5G network: an enterprise deploys a complete standalone OnGo Private 5G Network on its premises (site/building). The network uses channels in the CBRS band (n48), not a MNO's licensed spectrum. The network is deployed by the enterprise, or by a third party (which could be one of the MNOs). The network can take advantage pf the ultra-low latency and ultra-connectivity capabilities of 5G technology to enable new services or optimize existing services.

Pros

- Privacy and Security: The private network is physically separated from the public network, keeping all data within the network for additional security.
- Ultra-Low-Latency: Since network services can be deployed close the device, the network delay between the device and the application servers can be within several ms, allowing URLLC application services to be deployed.
- No optical fiber to the building: There is no need for a working backhaul to keep the local service running. 5G service can be immediately provided to the

enterprises that do not have optical backhaul links, for example factories in rural area.

- Isolated from Public Network Failures: If the public networks fail, the private 5G private is unaffected.

Cons:

- Deployment cost: Deploying a standalone Private 5G network can be expensive.
- Operational personnel: Enterprises need to have the right engineers and IT support personnel with experience in 3GPP networks in order to deploy, maintain and operate an OnGo Private 5G network.

Variant: Private 5G Using Licensed Frequency

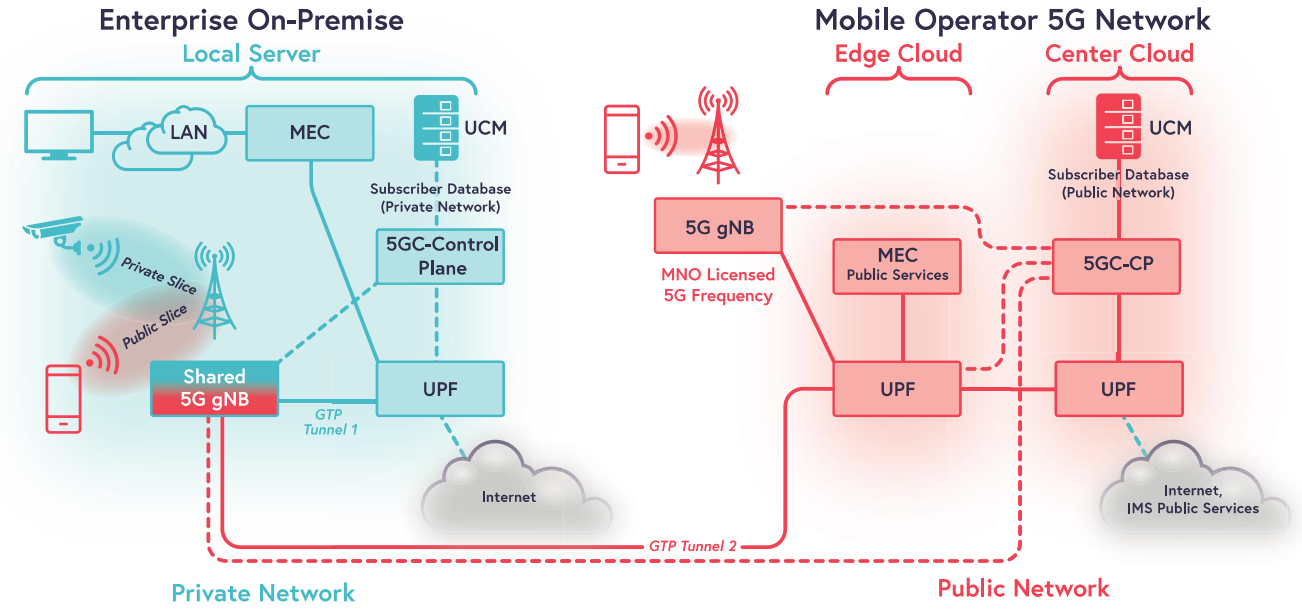

Figure 20: Private 5G Using License Frequency network architecture diagram.

As a variant, the Private 5G network can use channels that are owned by one of the public network operators, rather than CBRS-band spectrum. While not strictly an OnGo network, it is an option to be considered. The public network operator, as the owner of the license to use the spectrum, can set the commercial terms for sublicensing the

network. The public operators typically require that they are the ones that build and operate the private network.

Shared 5G NR RAN

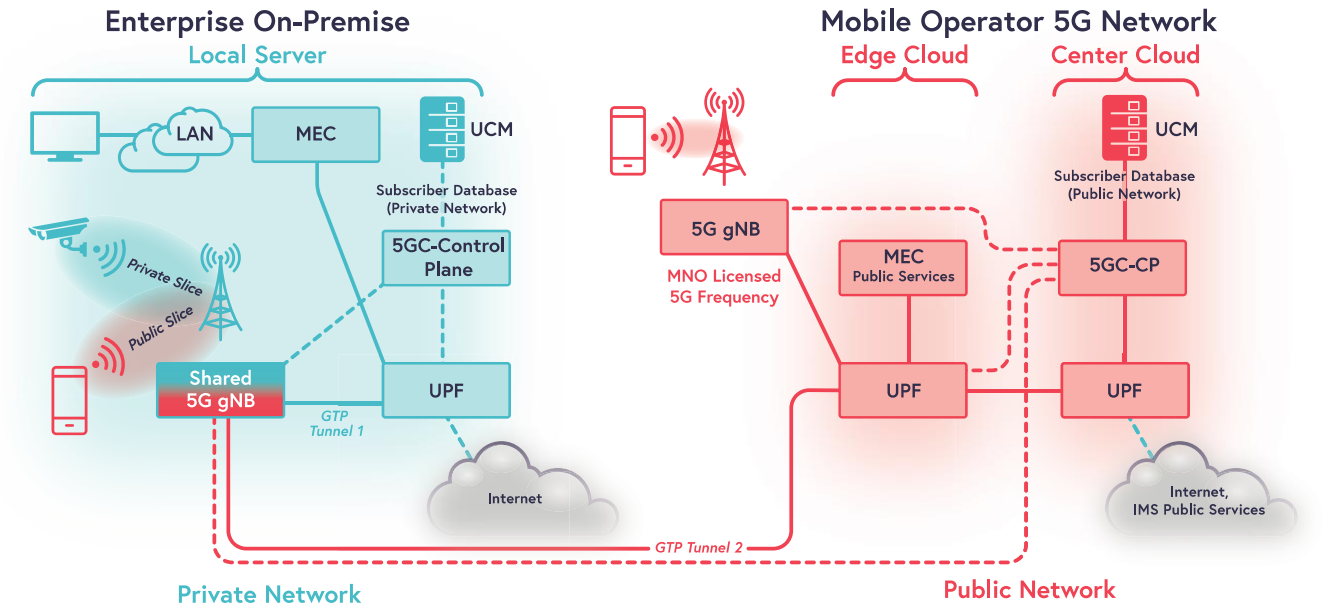

Figure 21: Shared 5G NR RAN network architecture diagram.

In this design, the on-site radio hardware of the 5G NR RAN is shared between the private network owner and the public network operator – the gNB base stations (BBU, RRH and antenna). The private and public networks operate on separate slices. The private network operator deploys a full 5GC system to support their slice. User plane traffic of the devices belonging to the private network is delivered to the User Plane Function (UPF) of the enterprise's 5GC, while data traffic of the devices belonging to the public slice (public network) is delivered to the UPF of the public network operator's edge cloud. Likewise, control plane data is routed separately. In other words, private network traffic such as in-house device control data, in-house video data, etc. stays in the private network, and public network service traffic such as voice and Internet are transferred to the mobile operator's network. The base stations (gNBs) are not physically isolated, but the logical separation within the 5GC architecture ensures the security of private network data traffic in the enterprise.

Likewise, the subscription and user information of the private network's users and devices are contained within the Unified Data Management (UDM) of the private network's 5GC, and are not visible to public network. MEC application services are located in the enterprise, providing enabling URLLC applications within the private network slice.

The frequencies used by the RAN can be the licensed channels of the public network operator, SAS-managed CBRS channels, or a mixture of the two.

Shared 5G NR RAN and Shared Control Plane

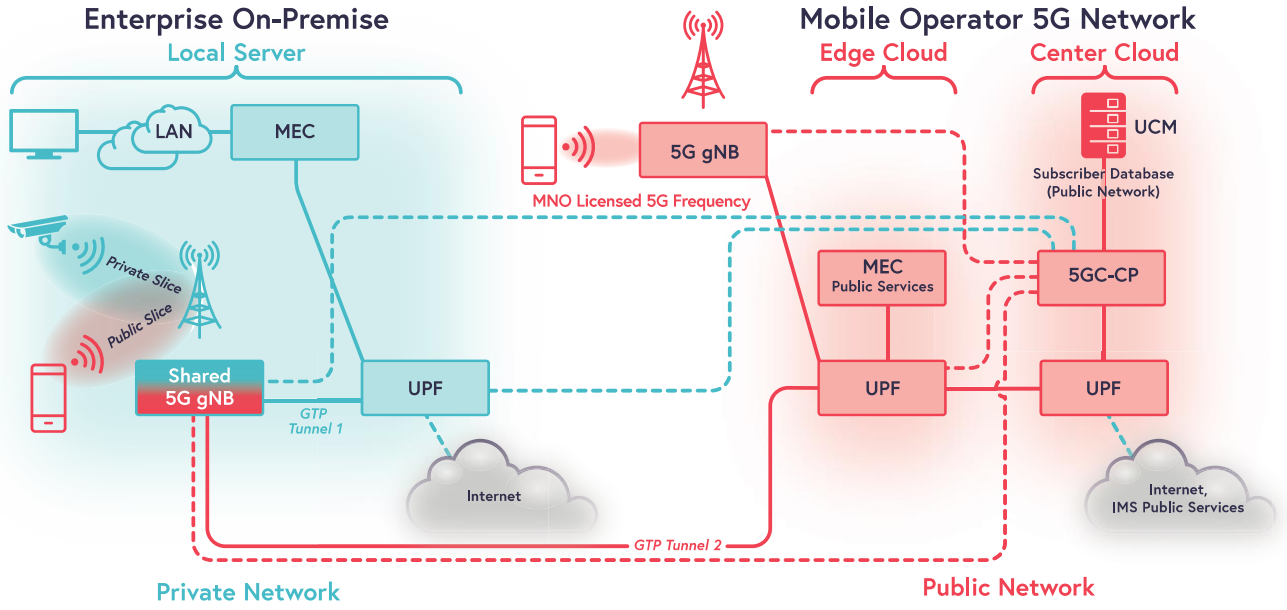

Figure 22: Shared 5G NR RAN and Shared Control Plane network architecture diagram.

Similar to the previous scenario, the radio hardware is shared, and user plane data is kept isolated. However, in this case, the control plane is handled by the public network operator. The benefit for the private network is that they do not have to deploy and maintain the control plane functions of the 5GC – they only need to deploy the UPF component. The downside is that the operation and subscription information of the private network's devices are stored in the mobile operator's server rather than in-house. They can still deploy MEC services as before, and URLLC applications.

End-to-End Network Slicing

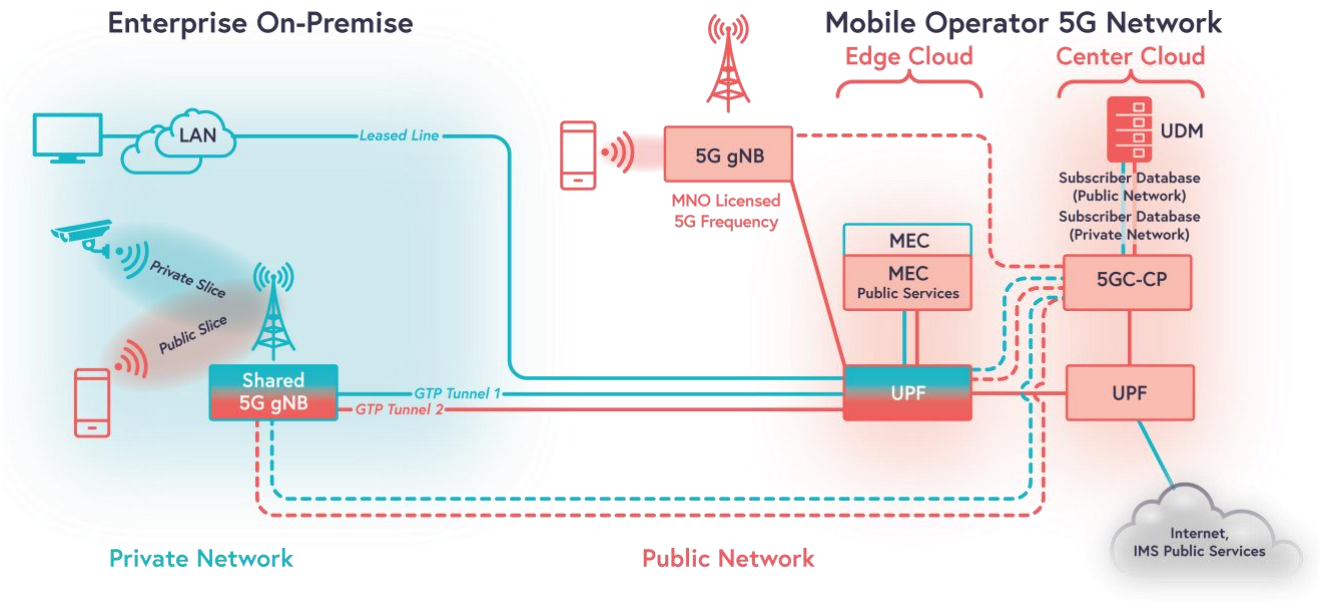

Figure 23: End-to-End Network Slicing network architecture diagram.

In this architecture, only the gNB is deployed on premises, with the 5GC, including UPF and MEC components are in the mobile operator's control. The private network is deployed as a slice of the public network. The benefit is that the private network operator doesn't have to deploy a 5GC to support their network. The cost is that services cannot be deployed as close to the edge of the network as there is no local traffic path between the private 5G devices and the private enterprises internal network. The public network operator may offer MEC services to private network slices, but as the MEC services are hosted by the public network, the overall latency may be too high for many URLLC applications. In addition, the private network's data – while isolated from the public network slices – is still being processed by the public network operator. User and subscription information is managed by the public network operator, who will have full visibility on it as well.

MEC Local Breakout (LBO)

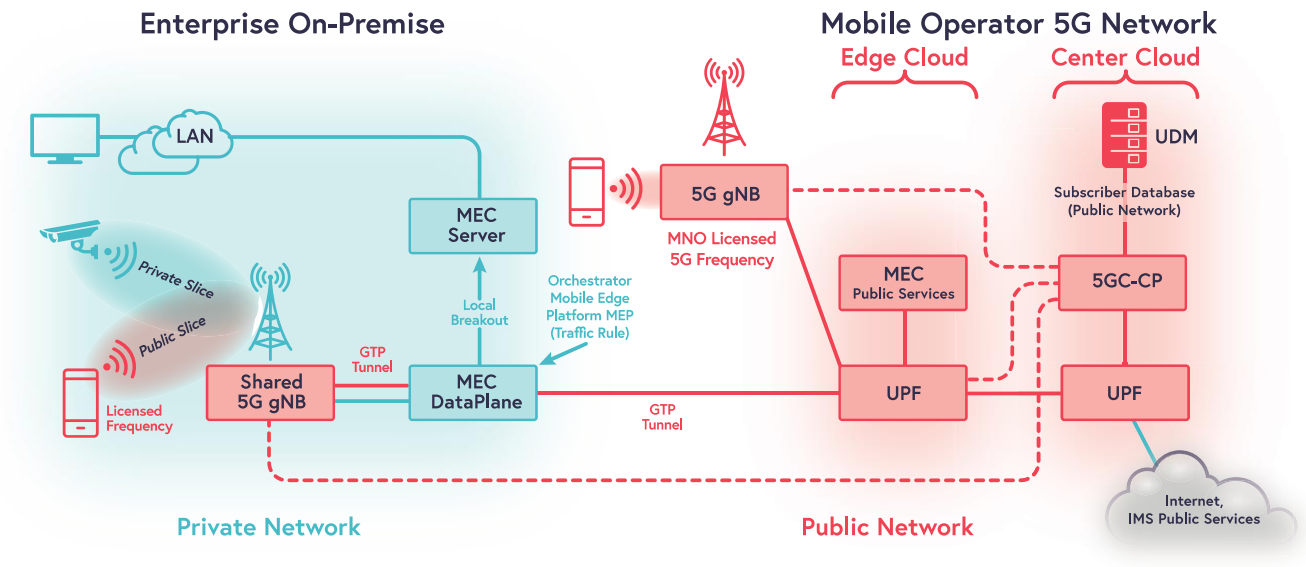

Figure 24: MEC Local Breakout (LBO) network architecture diagram.

Addressing some of the shortcomings of the End-to-End Network Slicing option, the MEC Local Breakout introduces a new system component – the MEC Data Plane (MEC DP). The MEC DP examines the data plane traffic, and routes it to local MEC services based on the IP address of the service being used. An Orchestrator from the public network operator configures the MEC DP's routing rules. The breakout can occur on the N3 GPRS Tunneling Protocol (GTP) connection between the shared gNB and the 5GC, or at the F1 interface connection within the gNB between the distributed unit (DU/RRH) and central unit (CU/BBU).

The upshot of this architecture being that the private network can deploy local MEC services without deploying 5GC functions, and keep the low latency required for URLLC applications. Control of user plane data is also maintained. Control plane data is not controlled, as the public network operator's 5GC is still relied upon for network management.

The MEC DP and MEC LBO are not standard methods of 3GPP, so there are some limitations associated with this – the mobility management and charging functions for private network devices is lost. This means you won't be able to charge for those

services, and mobile devices will experience service interruptions as they move about the network. This may be worth the tradeoff for the cost and performance benefits of this architecture.

Install

Now it is time to start installing your CBSDs, 5GC, and the other equipment in your deployment.

CBSD Installation

CBSDs typically need three connections to operate – power, a backhaul data connection, and one or more antennas.

CPI Requirements

All Category B CBSDs must be inspected and registered by a CPI. However, some Category A CBSDs can determine their location automatically via GPS/GNSS and don't always require a CPI. The most critical pieces of information that the CPI provides are the GPS coordinates of the CBSD, the power level, and the environment of the CBSDs (indoor or outdoor).

You can find more information on CPIs at the WInnForum website: https://cbrs.wirelessinnovation.org/cpi-program-administrator.

PAL Configuration & Spectrum License

If you have a PAL or are subleasing from a PAL holder, the SAS needs information about the CBSDs your network uses to add to the list of CBSDs associated with that PAL Protection Area (PPA). In addition, subleasing requires registration and certification with the FCC. If you don't have a PAL and are using GAA for access, no additional configuration information is required.

Each logical CBSD in your system can operate as either GAA or PAL. A physical CBSD device may contain multiple CBSDs, each with its own CBSD-ID, operating on different channels. These are treated as different CBSDs by the SAS, enabling the different logical CBSDs to use either PAL or GAA.

SIM Configuration and Provisioning

Devices that will connect exclusively to your network must be provisioned with SIM cards configured specifically for your network, with a custom IMSI (using your IBN). For physical SIM cards, you will need to acquire SIM cards in the appropriate form factor,

a SIM writer, and the necessary software. Devices with eSIMs can be provisioned using software, which is typically provided by the device manufacturer.

To properly configure your SIMs for connection to your network, you must set the Home Network Identifier (HNI) in the SIM to the Public Land Mobile Network Identity (PLMN- ID) of your network. For most Private 5G deployments using identifiers assigned by the OnGo Alliance, this is the OnGo Alliance's Shared HNI (315-010). Your specific network is identified by the CBRS-NID, which is provided in the SIM's Network Identifier (NID) field.

If you are building a standalone network and have not established agreements with any major network operators but want to support your users' personal devices on the system, you will need to provision those devices for dual-network support. This requires that your users have dual-SIM capable devices, and you configure the secondary SIM to connect to your network.

In either case, you will need to register the device with your network services to allow access for the device. The details of how to do this differ by system, but generally involve entering the IMSI or IMEI identification numbers into the management system.

5GC Configuration

At this time, your network's 5GC element needs to be deployed and configured correctly to support your deployment. Depending on the architecture you are using, the features of the 5GC functions you are using, this will involve some or all of the following steps:

- Allocating servers in your data center or cloud infrastructure.
- Installing and configuring the software for the network functions you need in your 5GC.

- Obtaining digital certificates and configuring security hardware such as TPMs, particularly for the Authentication Server Fuction (AUSF).
- Configuring MEC services and configuring Application Function (AF) services.
- Adding device a subscriber information to the Unified Data Management (UDM) network function.
- Configure the Quality of Service (QoS) policies within the User Plane Function (UPF).
- Configuring the network slices (if any) and the Network Slice Selection Function (NSSF).
- Enable any connections through your firewalls to external services.
- Set the identifiers for your network (SHNI, CBRS-NID, etc.)

Commissioning the CBSDs

Once installed, and with the configuration information (location, power level, etc.) recorded by the CPI, you can activate your CBSDs. The CBSDs will connect with the SAS and then request channel access. In most cases, mainly if there are no incumbents in the area, the SAS will grant access to your requested spectrum in near real-time. However, if you are close-by an incumbent, or in an area with possible incumbent activity (most commonly on the coasts), spectrum authorization can take up to 48 hours.

Commissioning of End Devices

Once the CBSDs are activated, and channel access granted by the SAS, it is time to start connecting your devices to the network. For many devices, it's merely a matter of using a properly configured SIM, turning on the device, and waiting for it to find your network. Others may require manual connection.

Key Performance Indicator (KPI) Verification

Once your network is commissioned and operating, confirm that your deployment provides the needed capabilities – coverage, available bandwidth, etc. CBSDs can be re-configured, moved, added, or removed where there is insufficient or excess coverage or capacity. Many of these changes require the CPI to update the SAS registration information. We recommend performing these checks as soon as you commission the CBSDs.

Specialist service providers can perform detailed coverage and capacity checks as part of their service offerings. They can also offer detailed analysis and recommendations of how to adjust your network to provide the needed capabilities.

Maintain

Like any system, a Private 5G deployment requires support. If there is a problem, it is essential to remember the system's elements that will most likely be the cause. Here are some recommendations for critical things to remember:

Network Operations Center (NOC) Support

A Private 5G deployment has an 5GC back-end system: the access network that includes CBSDs and end devices as well as the transport between 5GC, access, and end devices. All these components require operational support from a Network Operations Center (NOC). Faults in individual CBSDs or end devices may affect specific areas of the network. If there is a problem with the 5GC, the performance of the entire private network can be impacted. So it's crucial to have a NOC monitoring the system 24x7, particularly when mission-critical applications are running on the network.

HW/SW Alarms

Individual CBSDs, the 5GC, backhaul connections, or EUDs can develop hardware or software faults. These components generate an alarm when an error occurs to alert the NOC support team. Classification of problems, and time requirements for their resolution, are often included as part of the contracts with service providers.

SAS Connectivity

If connectivity to the SAS is lost, the CBSDs will shut down after just a few minutes, which is why we recommend high-availability or redundant communications. If connectivity is lost, the SAS retains the grant for your network for seven days. As long as the link is restored within that time frame, your network can resume operation immediately.

Channel Access

If an incumbent system becomes active, the SAS may direct your CBSDs to reduce power or even shut down entirely.

Interference from Other Networks

In general, the SAS prevents interference from other networks operating in the CBRS band, so don't worry about other networks. However, the SAS may instruct your CBSDs to reduce their power levels to prevent interference with other networks with higher priority (PAL holders and incumbents). If there is an interference problem that the SAS isn't automatically addressing, work with your SAS to help identify the problem source and resolve it.

Service Level Agreements (SLAs)

To ensure that your network operates at the needed level, you should establish Service Level Agreements (SLAs) with your vendors. The level of service guaranteed depends on how mission-critical your system is.

Key Performance Indicators (KPIs)

There are several predefined 5G-related KPIs that you can use to meet SLAs. Several broad categories of KPIs are typically used, given below, along with some example values.

- Availability – Used to measure the percentage of time the network is available for users to make full use of the offered services. Example KPIs include:
  - Call (data or voice) success rate >99.0%
  - Data bearer setup success rate >99.0%
  - Vo5G accessibility success rate >99.5%
- Retainability – This measures how often users lose connectivity to the network, typically due to inadequate coverage and quality.
  - Voice dropped call rate <1.5%
  - Data dropped call rate <0.5%
- Integrity – Used to measure the character of the network through metrics such as throughput and latency.
  - Average latency (uplink and downlink) <150 ms
  - Average jitter (uplink and downlink) <30 ms
  - Average downlink throughput >1 Mbps
- Mobility – Used to measure the network's performance while the users move through the system's coverage area.
  - Intra-network handoff success rate >98%

  - Inter-network handoff (hand in) success rate >99%
- Utilization – Used to measure network usage.
  - Downlink traffic volume (in Mbps)
  - Uplink traffic volume (in Mbps)

The source for the metrics for KPIs may come from the EMS of the CBSD vendor, or from the 5GC. KPIs can also be custom-designed for specific use cases.

Changes in the environment can impact the network's KPIs. Reporting can include coverage areas that are disturbed when adding or removing walls and partitions, installing large metal objects in the area, or even planting trees or other foliage. Check periodically to make sure your network is still providing capabilities that can detect any changes, which allows you to adjust network operations as needed.

Monitoring

A network monitoring system plays a vital role in any Private 5G deployment. This system should continually evaluate key performance metrics continually against your service level agreements (uptime, average throughput, etc.) and provide immediate notification of any problems that could impact critical services.

Priority Access License (PAL)

If system performance does not meet the desired level due to channel access limitations, you should consider acquiring or sublicensing a PAL.

Glossary

Term	Definition
AC	Alternating Current
AP	Access Point, the Wi-Fi equivalent of an eNB
Backhaul	Connection from a network node (CBSD) to other nodes and external networks.
BTS-CBSD	Base Transceiver Station CBSD: Fixed CBSD base station connecting to EUDs or CPE-CBSDs
BYOD	Bring Your Own Device
CA	Carrier Aggregation
CBRS	Citizens Broadband Radio Service
CBRS-NID	A CBRS Network ID, a CSG-ID that identifies the provider of a network
CBSD	Citizens Broadband Radio Service Device: Fixed Stations or networks of such stations that operate on a Priority Access or General Authorized Access basis in the Citizens Broadband Radio Service consistent with Title 47 CFR Part 96.
Category A	<30 dBm/10 MHz (<1 Watt/10 MHz) transmit power CBSD
Category B	<47 dBm/10 MHz (<50 Watt/10 MHz) transmit power CBSD
CPE	Customer Premises Equipment
CPE-CBSD	A fixed device that communicates with a SAS via a BTS-CBSD and can exceed the EUD transmit power limit. In an OnGo context, it functions as a non-mobile UE.
CPI	Certified Professional Installer, an individual authorized by the WInnForum to register information about a CBSD with the SAS.
CSG-ID	Closed Subscriber Group Identifier
DAS	Distributed Antenna System
DL	Downlink
DM	Device Management System (for CBSD)
eNB	Evolved Node-B, an LTE base station
EIRP	Effective Isotropic Radiated Power: the transmitted power level of a wireless device, including antenna gain
EMS	Element Management System
EPC	Evolved Packet Core provides network services to mobile devices in LTE
ESC	Environmental Sensing Capability
eSIM	Embedded SIM, a SIM system without a removable UICC/SIM card
EUD	End-User Device: an LTE UE in OnGo (e.g., a smartphone, sensor, etc.). It can be a fixed or mobile device. Transmit power level must be <23 dBm EIRP.

Glossary

Term	Definition
FCC	Federal Communications Commission
FWA	Fixed-Wireless Access: A wireless telecommunication system where the devices are non-mobile. Often used for providing backhaul for other services.
GAA	General Authorized Access
GHz	Gigahertz
GNSS	Global Navigation Satellite System (e.g., GPS)
GTP	GPRS Tunneling Protocol: a tunneling protocol for managing mobile bearer data between an SGW and a PGW in an EPC
GPS	Global Positioning System
GW	Gateway
HD	High Definition
HNI	Home Network Identifier, the PLMN-ID of a device's home network
HSS	Home Subscriber Server, the network element of an EPC, contains user-related and subscription-related information in a centralized database
IBN	IMSI Block Number, a block of numbers granted for use by a network operator
IMEI	Individual Mobile Equipment Identity
IMSI	Individual Mobile Subscriber Identity
IT	Information Technology
ITU	International Telecommunications Union
IoT	Internet of Things
IPX	IP Exchange
Kbps	Kilobits per second
KPI	Key Performance Indicator
LTE	Long Term Evolution, the 4th generation mobile technology; used in OnGo
LTE UE	LTE User Equipment: a device (mobile or fixed) used by an end-user to communicate (e.g., a smartphone).
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple-Input and Multiple-Output: a method for multiplying the capacity of a radio link using multiple transmission and receiving antennas to exploit multipath propagation

Glossary

Term	Definition
MME	Mobility Management Entity, the network element of an EPC that controls mobile device access to the EPC
MMEC	MME Code. An 8-bit number that identifiers an individual MME within an MME Group
MME Group	A collection of MMEs within a given network
MMEGI	MME Group ID identifies a specific MME Group within a network
MNO	Mobile Network Operator or a wireless carrier
MOCN	Multi-Operator Core Network—an NHN where a shared eNB system routes traffic to the EPCs of the PSPs.
MOCN Gateway	An optional system that provides a single MOCN interface from one or more CBSDs/eNBs to PSP networks. A MOCN gateway can also provide MOCN capability to a CBSD that doesn't natively support MOCN.
MORAN	Multi-Operator Radio Access Network—an NHN where the PSPs operate their eNBs, utilizing separate carriers, but sharing antennas and other RF elements
MSO	Multiple System Operator—an operator of multiple cable or broadcast satellite services.
MVNO	Mobile Virtual Network Operator— a wireless carrier that does not own the physical infrastructure that provides services.
NHN	Neutral Host Network, an LTE network that provides coverage to multiple MNOs.
NOC	Network Operations Center
OnGo	LTE in the CBRS band
OnGoA NHN	A specific NHN system architecture defined by the OnGoA for use in the CBRS band. **Note:** Other NHN architectures can be deployed in the CBRS band and supported by the OnGoA.
PAL	Priority Access License
PCI	Physical Cell Identity, an identifier broadcast by each cell in a network.
PGW	Packet Data Network Gateway, a network element of an EPC that provides connectivity from a UE to external packet data networks by being the exit and entry of traffic for UEs.
Physical Cell Identity	A number from 0 to 503 broadcast by each LTE cell. This number should be different from other cells in the area.
PLMN-ID	Public Land Mobile Network Identity
PPA	PAL Protection Area. the geographic area that the SAS protects from interference for a given PAL.

Glossary

Term	Definition
PSP	Participating Service Provider, a network that is using an NHN to provide services to their subscribers.
PTP	Precision Time Protocol
QoS	Quality of Service
QCI	QoS Class Identifier, how different data streams are prioritized within an LTE network.
RAN	Radio Access Network
RF	Radio Frequency
SAS	Spectrum Access System, manages and assigns CBRS spectrum use on a dynamic, as-needed basis across PAL and GAA users.
SGW	Serving Gateway, a network element of an EPC that routes and forwards user data packets to a PGW via GTP sessions while also acting as the mobility anchor for the user plane inter-eNodeB handovers.
SHNI	Shared Home Network Identifier, a common PLMN-ID for use by CBRS systems (315-010)
SIM	Subscriber Identifier Module
SINR	Signal-to-Interference Plus Noise Ratio
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SON	Self-Optimizing Network
TAC	Tracking Area Code, part of the TAI
TAI	Tracking Area Identifier
TPA	Training Program Administrator
UE	User Equipment, a device using the mobile network
UICC	Universal Integrated Circuit Card, a SIM card.
UL	Uplink
USB	Universal Serial Bus
VoLTE	Voice over LTE, a packet-based protocol for handling voice calls in LTE.
WInnForum	The organization that develops the standards for CBRS system elements that include the SAS, ESCs, CBSDs, and CPI certification.

Checklist

Requirements Gathering

What is the purpose of your Private 5G network?
Who will be connecting to your Private 5G network?
What devices will be connecting to your Private 5G network? How many of each? What SIM system do they use?
Which devices will be mobile within your network? Which devices will move into and out of your network?

Survey and Planning

Sketch of coverage area. Note locations of critical devices, existing Wi-Fi Access Points, power outlets, and data access.
How much data capacity do you need?
Is a PAL needed?
SAS Administrators, 5GC Vendors, CBSD Vendors, and EUD Vendors

Checklist

Design

Selected SAS Vendor:
Selected CBSDs:
Number of CBSDs:
Selected 5GC:
Selected EMS/DM:
Selected CPI:
Assigned CBRS NID: (SHNI@ongoalliance.org)
Assigned MME Group ID (MMEGI) (from lead PSP):
Assigned Macro eNB IDs (one per CBSD) (from lead PSP):
Assigned IMSI Block Numbers (1 per 100k devices): (https://imsiadmin.com/imsi-home)
Tracking Area Codes:
SIM Provisioning Option:
PAL License:

Install Checklist

Install and Configure CBSDs:
Install and Configure EPC:
CPI Registered With SAS:
SIMs Provisioned:
Commission CBSDs:
Commission End Devices:

Maintain & Service Assurance

KPIs:
Defined Alarms:
Internal Contacts (for alarms):
Operations Contact:
CBSD Support Contact:
EPC Support Contact:
PSP Contacts:

About the OnGo Alliance

The OnGo Alliance believes that 3GPP-based solutions in the 3.5 GHz band, utilizing shared spectrum, can enable both in-building and outdoor coverage and capacity expansion at massive scale. In order to maximize the full potential of spectrum sharing, the OnGo Alliance enables a robust ecosystem through the management of the OnGo brand, and the OnGo Certification Program. For more information, please visit www.ongoalliance.org and learn more about the expanded business opportunities OnGo is enabling.