OnGo Neutral Host Network Deployment Guide

September 2021, v1.0.1

Contents

Contents

Overview

With the opening up of the CBRS band to the public, the FCC removed several key barriers to deploying LTE networks. The new requirements enable you to significantly increase the speed and reduce the cost of deploying an LTE network. Neutral Host Networks (NHNs) that provide services to users of multiple networks are also much more practical to deploy. This paper is a guide for deploying an NHN using OnGo's LTE technology in the CBRS band. It is intended to familiarize you with key aspects of designing and deploying an NHN, so you're prepared for discussions with equipment makers, service providers, and network operators. In addition, this guide provides a walk-through of the deployment process and examines many of the major design decisions involved in deploying an NHN.

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.

What is a Neutral Host Network?

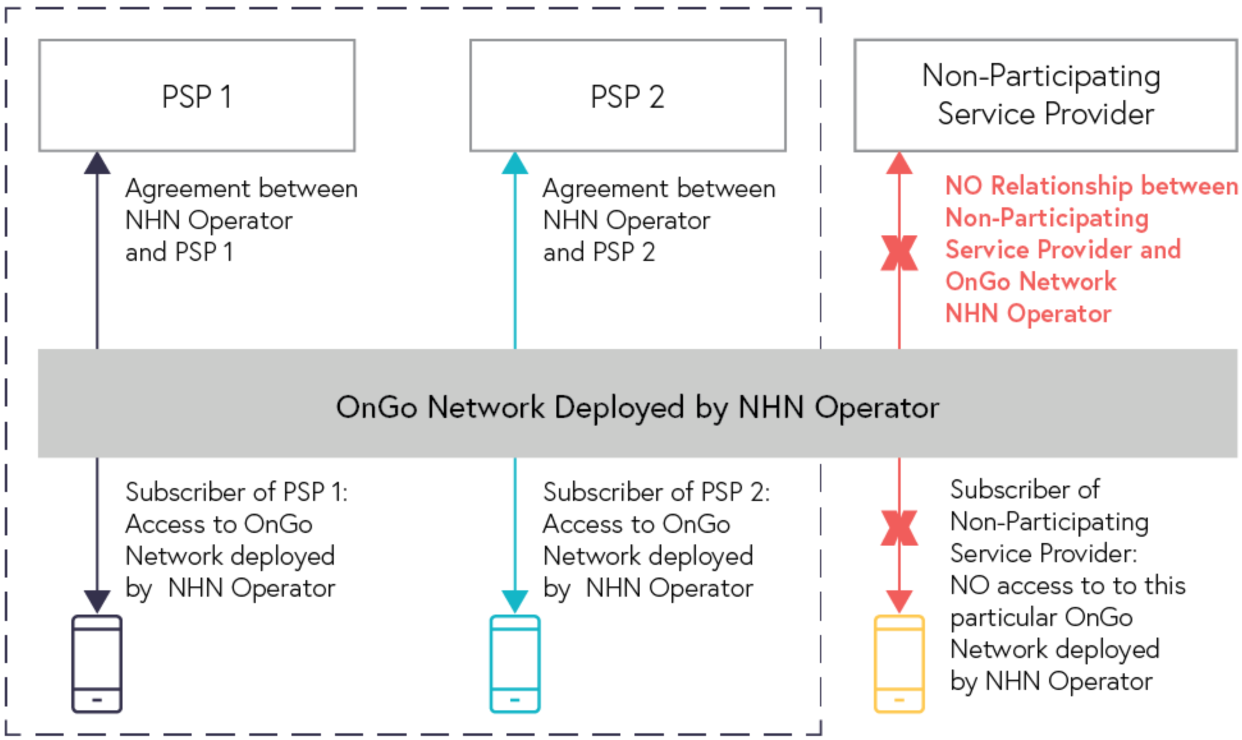
A Neutral Host Network (NHN) is defined as a network that allows multiple Participating Service Providers (PSPs) to share the network's services. The network is deployed and operated by an NHN operator, an independent entity, or an existing network operator. For users of the network, the NHN operates 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. PSPs can also offload capacity in areas where networks are congested due to a large number of users or high data traffic loads.

NHNs can be deployed in multiple ways, with different capabilities, architectures, and limitations. This guide examines several different types of networks:

- Roaming-Based NHN – This is an NHN deployed using the standard roaming systems of LTE to roam from up to six PSP networks.

- MORAN NHN – This is an NHN sharing some radio network elements of multiple operators, but with each PSP operating on a different channel.
- MOCN NHN – This is an NHN that shares the radio network itself, and routes the network traffic to the different PSP networks.



Who Are the Participating Service Providers?

The PSPs provide the subscribers using a given NHN. The PSPs can be any network operator that offers LTE-based services such as a Mobile Network Operator (MNO) (e.g., AT&T, T-Mobile, Verizon), Multiple System Operator (MSO) (e.g., Comcast, Charter, etc.), Mobile Virtual Network Operator (MVNO) or other network operators. For a network operator to become a PSP, they must agree to participate and provide connections to the NHN.

Who Should Read this Guide?

We have written this guide for organizations interested in deploying and operating OnGo-based LTE NHNs in their facilities to improve coverage or provide increased capacity. 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 NHN.

Much of the design, deployment and operational tasks 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 service needs and select an appropriate service provider.

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, the wireless spectrum, or 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 the 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 so private organizations can share this spectrum with incumbent users. The OnGo Alliance created OnGo to promote the use of LTE in the 3.5 GHz band, although

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.

other technologies can also use 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).

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 auctions 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 interference protection from each other.

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 emit less than one watt of power per 10 MHz channel. Category B devices, typically used outdoors, emit up to 50 watts per 10 MHz channel. In an OnGo network, the LTE eNodeBs (base stations) are physically connected to CBSDs and are often in the same device.

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.

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	45 (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 the power can't exceed < 23 dBm/10 MHz (<200 mW). EUDs may operate with permission by a CBSD. In an OnGo network, the EUDs are generally LTE 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 SAS maintains 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 the SAS can prevent CBRS interference with the naval operation. The SAS uses propagation models to predict potential interference with incumbent systems and transmits operating parameters to CBSDs so potential interference can be avoided.

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. 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.

Process Summary

Deploying and operating an NHN involves multiple steps. They consist of the following stages:

1. Gather Requirements. Information should include how many people will use the network, which network operators are the best PSP choices, and determine the requirements the PSPs need to participate in your NHN.
2. Survey and Planning. In this stage, you survey the physical space the NHN 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 and satisfies the requirements from the PSPs.
4. Installation. It's time to begin installing your network – CBSDs, radio hardware, backhaul connections, etc.
5. Maintain. Once the NHN is deployed and operating, you'll need to stay on top of monitoring to ensure that the network is operating correctly and is in compliance with the key requirements from the PSPs.

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

Gathering Requirements

The first step in any successful deployment requires a detailed understanding of your organization’s needs and the problems you want to solve by deploying an OnGo NHN. 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

When identifying critical use cases for your NHN, here's a list of questions to help define your network requirements:

- What is the primary purpose of the NHN? NHNs usually address one (or more) of the following challenges:
  - Provide coverage in an area with low coverage.
  - Provide offload capacity in an area with congested networks.
  - Provide coverage to occupants of a building.
  - Provide coverage at venues with limited equipment space.
  - Provide coverage with lower infrastructure costs.
- How many PSP networks should the deployment support?
  - The number of PSP networks can determine what NHN architecture you can use.
- What networks will be participating in the NHN? Each network can support multiple PSPs, and you need to make arrangements with each provider. In addition, each PSP may have specific requirements of the NHN to participate. PSPs can be any service provider, including:
  - Mobile Network Operator (MNO) (e.g., AT&T, T-Mobile, Verizon)
  - Multiple System Operator (MSO)
  - Mobile Virtual Network Operator (MVNO)
  - Any other network operator
- Do the PSPs have any specific requirements that affect the configuration and capabilities of each NHN? Determining those requirements early in the process is critical for success. For example, some of their requirements may include holding

a PAL, providing carrier aggregation support, or prohibiting access restrictions. Or they could require you to deploy network visibility and monitoring systems.

- Will the network also serve as a Private LTE network?
  - An NHN can also provide services to users and devices that are not part of a PSP's network. This is called a Hybrid Network and is primarily a matter of configuring the backend elements of the NHN. See the Private LTE Deployment Guide for details on deploying Private LTE services. (https://www.ongoalliance.org/wp-content/uploads/2020/12/OnGo-Private-LTE-Deployment-Guide-2.0.pdf)
- 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 information.
- In what environment will the system be deployed?
  - Given that OnGo networks function both indoors and outdoors, your specific environment will determine many aspects of your system.
- Is latency a significant concern?
  - Some applications require low-latency operations, which will impact your network design.
- What wireless data infrastructure do you already have?
  - If you already have LTE systems deployed, such as a Distributed Antenna System (DAS) or a small-cell system, you will need to consider them as you design your NHN deployment. The NHN system can coexist with existing systems to provide additional coverage and capacity. You can also use the existing systems for private LTE traffic offload, or the existing systems can be replaced entirely by adding a private LTE slice to the NHN system.
- 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.
- Do you need a local breakout of data traffic?
  - An NHN can route data traffic to the PSP's network or to the local services or the Internet directly from the NHN. Routing traffic can impact backhaul requirements and may be a requirement for a PSP to participate.
- 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-premises hosting options, local hosting 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 for a sports venue where the NHN is providing additional capacity during an event. Scenario B is an NHN deployment in a shopping mall focused on extending coverage inside the building. By going through the detailed deployment process of each scenario, we hope to give you clear examples to help guide the planning of your network.

Scenario A: Sports Venue NHN for Capacity Expansion

In this scenario, we'll consider the deployment of an NHN at a stadium or sports complex. When there can be up to 45,500 people in the stadium, network congestion prevents many attendees from accessing the network. Lack of access prevents the stadium from offering services to attendees, such as ordering concessions via a smartphone app. (Note: The Private LTE Deployment guide examines a purely private network deployment at a sports venue. Here, we will focus on the NHN aspect, with the private aspect addressed in that guide in detail. A private LTE network slice could be provided in this deployment as well, as in the second scenario here, but is not considered for this scenario for the sake of simplicity.)

Scenario B: Shopping Mall

This scenario is for retail shopping mall. The mall operators want to deploy an NHN to extend coverage to areas where the coverage is insufficient. For tenants, service deficiencies irritate customers and make it difficult for the operator and the mall's tenants to deploy smartphone-based applications for their customers. The mall has about 1.5 million square feet of space, on two floors, with approximately 150 stores. Up to 30,000 customers and 1,500 workers and staff can be onsite at any given time. While up to 10% of the customers may be making voice calls, the primary objective of the NHN is to allow data access for a store's app.

Survey & Planning

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" LTE signals and operates at a lower power level (<50 watts) than a macro LTE 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 coverage 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 onsite infrastructure elements as required (data center, networking elements, network management systems, controllers, etc.).
- Location and interfaces, including wired and wireless, and any existing devices that will connect to your network.
- Location of equipment closets, fiber point 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 12 to 20 Wi-Fi Access Points depending on terrain and other factors.

Adjacent LTE Networks

It is often helpful to know what other LTE networks are in your area and some basic configuration information about those networks. Although a SAS can provide basic information about other LTE networks in the CBRS band, other LTE 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, including any PAL operators and other incumbent users with 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, though the PSPs will often have specific capacity requirements to participate. 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.

OnGo networks use Time Division Duplexing (TDD), with the CBSDs/eNBs and EUDs/UEs on the same frequency channel transmitting and receiving at specific times. The throughputs can be calculated depending on several parameters such as the TDD configuration, channel bandwidth, downlink, and uplink modulation supported, and the MIMO capability of the CBSD. See examples in the table below. The table lists peak rates shared across all connected users. You can use an online calculator (https://www.cellmapper.net/4G-speed) to determine the available bandwidth. The further you are away from the CBSD you can expect total throughput to drop. To compensate, we recommend designing your RF footprint to maintain a cell edge that sustains 15/5Mbps DL/UL throughput. The OnGo signal will typically reach longer ranges and perform more reliably at the cell edge than a Wi-Fi signal.

TDD Config (with: Normal Cyclic Prefix + Special Config0)	Channel Bandwidth	Modulation	MIMO	Peak DL	Peak UL
1	10	DL - 64 QAM UL – 16 QAM	2x2 4x4	33.48Mbps 66.96Mbps	10.44Mbps 10.44Mbps
1	20	DL - 64 QAM UL – 16 QAM	2x2 4x4	66.96Mbps 133.92Mbps	20.88Mbps 20.88Mbps
2	20	DL - 64 QAM UL – 16 QAM	2x2 4x4	97.2Mbps 194.4Mpbs	10.8Mbps 10.8Mbps
6	20	DL - 64 QAM UL – 16 QAM	2x2 4x4	51.84Mbps 25.92Mbps	103.69Mbps 25.92Mbps
6	20	DL - 256 QAM UL – 64 QAM	2x2 4x4	69.12Mbps 138.24Mbps	38.88Mbps 38.88Mbps
1	20+20 DL-CA 20+20 UL-CA*	DL - 256 QAM UL – 64 QAM	2x2 2x2	178.56Mbps 178.56Mbps	31.32Mbps 62.64Mbps

* In development now.

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 go up. If this is the case, we recommend adding 10% to your calculated bandwidth requirements.

Based on your total bandwidth needs, you can estimate the number of channels you'll need. Suppose your scenario needs more data than can be provided in a single channel. In that case, 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 more (or less) uplink capacity.

Note: OnGo CBSDs are only allowed to support TDD Uplink/Downlink Configuration 1 (balanced) and 2 (downlink-heavy). Other configurations may be supported but are not required. EUDs (UEs) support of the configuration is also required. Your PSPs can tell you what devices on their networks support which TDD configurations.

TDD Synchronization

In the CBRS band, LTE systems must operate in TDD mode. In that mode, CBSDs (eNBs) need to coordinate with nearby LTE CBSDs to prevent interference. Without coordination, the higher power transmissions of the CBSD can effectively drown out the lower power transmissions of UEs in nearby cells, even when they are on adjacent frequency channels. This interference can occur when the CBSDs use different TDD frame configurations or if the timing is not synchronized between the CBSDs to transmit at the same time.

Being in the same TDD configuration and aligning the timing between cells significantly reduces interference. LTE has existing mechanisms for synchronizing timing between eNBs, using GPS or similar signals for a common timing reference, which is critical for proper functioning. However, the SAS doesn't currently have provisions for coordinating the TDD configurations.

The OnGoA defines an optional coexistence manager system element to help coordinate between OnGo networks and to minimize TDD-related interference within the CBRS band. This system will coordinate between OnGo networks to select an appropriate TDD configuration. That may constrain what TDD configurations your network can use, but you'll experience significantly reduced interference. Until these systems are online, you'll need to coordinate directly with other OnGo networks in your area to determine which TDD configuration won't interfere with those networks or with your network. An integrated solution provider will be able to help with these issues if needed.

PAL vs. GAA

For most NHN deployments, you shouldn't need a PAL. However, consider sublicensing a PAL if your implementation meets one or more of the following criteria:

- Large area or outdoor deployment – If your implementation uses Category B (outdoor) CBSDs, or covers a large geographic area.
- Mission-critical – A PAL gives your network higher priority, 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 protected from GAA users.

The FCC auctions PALs on a per-county basis. Light-touch leasing rules allow 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.

If any of the PSPs in your NHN have a PAL in the area, they may be willing to sublicense access to the PAL. Likewise, any PAL holders in your area might want to participate in your NHN as a PSP.

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.
- Are there many other CBRS networks in your area? If other private GAA CBRS users exist in the same area, a PAL will help ensure that you receive preferential access.
- Does your network cover a large area? The more extensive your network, the more likely you will overlap with another CBRS network. A PAL will reduce the chances of interference.

If you did not secure a PAL in the auction, you may be able to sublicense from an existing PAL holder. However, given that PAL holders are not required to lease, it may not be possible to get a PAL in your area.

SAS administrators can provide guidance on the availability of spectrum in your area.

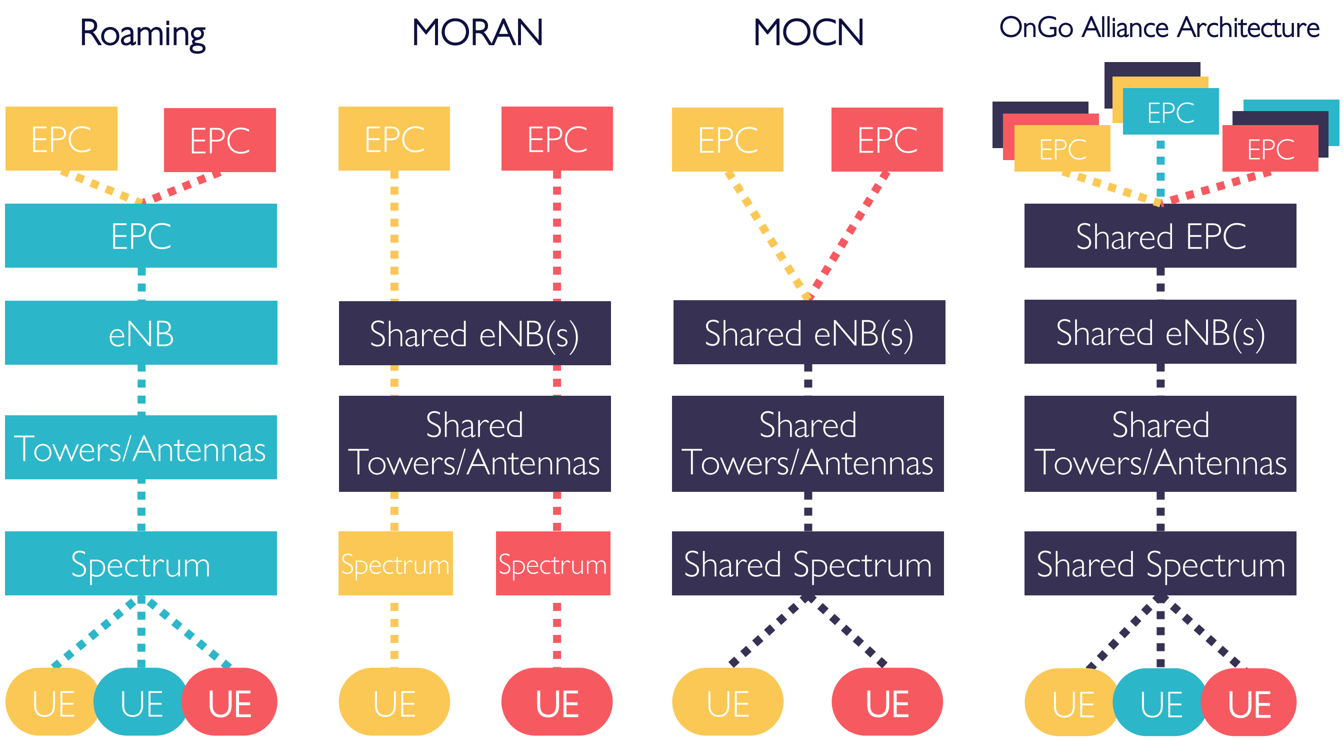
Carrier Aggregation

LTE supports the bundling of channels to provide additional bandwidth via a mechanism known as Carrier Aggregation (CA). CA 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.

In addition, CA can be used across bands. For NHNs, this means that a PSP could use CA to combine channels from their licensed spectrum bands with channels provided via the NHN. Combining channels requires all system elements to support such CA and close coordination with the PSP.

NHN Architecture Selection

As mentioned previously, there are multiple architecture options when deploying an NHN. The following describes the options available, including the advantages and disadvantages.



Roaming-Based NHN

Standard LTE, as defined by the 3GPP, has built-in mechanisms to handle roaming when coverage isn't available from the user's home network provider. Roaming agreements need to be in place with each PSP and special interfaces are required between the hosting and PSP network systems. Users can see that they are operating on a different network and are usually notified when roaming. Different charging and billing plans usually apply to roaming users who are traveling internationally. While not strictly speaking a Neutral Host Network, this is the form of network sharing that is in common use.

MORAN NHN

A Multiple-Operator Radio Access Network (MORAN) NHN is a system that shares some elements of the radio interface between multiple operators, but they use separate radio channels. In other words, they use the same radio hardware, but end devices and users see entirely separate networks. Usually, each PSP provides its EPC network hardware for the MORAN system to connect with the radio control hardware. Each PSP can configure the radio network as needed, with minimal restrictions.

A MORAN system is the best choice when traffic loads are relatively low, or few PSPs need support since each PSP uses their own separate 10 MHz channel.

A Distributed Antenna System (DAS) NHN is, functionally, a type of MORAN NHN.

MOCN NHN

In a Multiple-Operator Core Network (MOCN) NHN, the eNodeB is shared between PSPs, with the shared eNB routing traffic of a given UE to the appropriate PSP. From the user's perspective, the connection appears to come from their home network, transitioning seamlessly to and from the network. The NHN can only support up to six PSPs per channel, but the PSPs don’t have to provide dedicated equipment to support the system.

MOCN functionality is typically integrated into the eNB as a feature. If the eNBs do not support MOCN directly, a MOCN gateway system can be used to provide the needed MOCN interfaces. A MOCN gateway can also

DAS, NHNs, and CBRS

A Distributed Antenna System (DAS) is a type of MORAN system. Multiple service providers share an antenna system, with each PSP transmitting on a separate carrier on the same antennas. In addition, each PSP has onsite hardware responsible that is for the system.

For example, you may already have a DAS system deployed but need additional capacity/coverage. In that case, it may make sense to simply add a CBRS-based NHN in parallel to the DAS system, as modifications to the DAS system may require re-certification.

As of this writing, passive DAS systems will be able to operate in the CBRS band soon, with some additional complexity for handling the interface with the SAS. Such a system would allow adding a Private LTE capability and additional PSPs without needing additional channels. The specific details are being resolved within the WInnForum. Active DAS systems cannot currently be deployed in the CBRS band but are being considered by the FCC and may be allowed in the future.

be used to aggregate the interfaces of multiple eNBs, providing a single connection point to the PSPs' networks. Individual gateways for each PSP can be used, which allows the gateways to be configured and maintained individually, increasing overall reliability.

A MOCN system is preferred to a MORAN system when traffic loads are higher, as up to six PSPs can be supported per channel, regardless of the size of the channel.

A Gateway Core network (GWCN) NHN is very similar to a MOCN, but the PSPs also use a shared EPC element.

OnGoA NHN Architecture

The OnGo Alliance has defined a variant of NHNs, similar to a MOCN system, but with additional capabilities. Like with a MOCN system, all radio network elements are shared, but there is a shared EPC managed by the NHN operator, which routes traffic of a given device to the appropriate PSP's network. In addition, an OnGoA NHN can support many more PSPs than the other options – up to 54 PSPs per carrier. However, few user devices currently support OnGoA NHNs; only those that support OnGo Alliance Profiles II, III, or IV.

Category	Roaming	MORAN	MOCN	OnGoA
PSPs per Channel	6	1	6	54
Channels	Shared	Separate	Shared	Shared
eNodeB	Shared	Partial Shared	Common	Common
Radio Network	Separate	Separate	Partial Shared	Fully Shared
EPC Needed	Yes	No	No	Yes
Standard	3GPP	3GPP	3GPP	Custom

Participating Service Provider Outreach

At this stage, it's time to start approaching the service providers you want as PSPs for your NHN. Potential PSPs may have no interest in participating or have specific requirements to participate. Requirements from PSPs for an NHN in the CBRS band may include things like:

- Only support a specific NHN type
- Specific signal-to-interference-plus-noise ratio (SINR) limits
- Target quality of service (QoS) and QoS Class identifier, and throughput
- Coverage analysis accuracy resolution
- Key Performance Indicator (KPI) measurement and reporting
- Network visibility and monitoring
- Equipment ownership demarcation
- Design criteria (% of the area covered at an agreed KPI)

PSPs may also want data about the site (estimated number of users, etc.) in order to decide whether to participate in an NHN.

PSPs may also have licensed spectrum operating in the area of your NHN deployment, either in other bands or in the CBRS band via a PAL. The PSP may even want to use carrier aggregation (see sidebar) to increase system capacity, which will factor into any requirements the PSP may have regarding the capacity of the NHN.

NHNs have limitations on how many PSPs they can support. For example, in a MORAN system, each PSP has its own channel, which means that an NHN deployment will need more channels. A MOCN system, on the other hand, can support up to six PSPs per channel.

Carrier Aggregation and NHNs

LTE supports the increasing the bandwidth available through the use of Carrier Aggregation (CA). In CA, the EUD (UE) connects to multiple carriers within the same band or in different bands, with one of the carriers serving as the primary and the rest as secondary. For example, PSPs may wish to use an NHN as a secondary cell to provide additional bandwidth for devices, with their licensed-spectrum network serving as the primary cell. However, this requires that the CBSDs (eNBs) support CA. For indoor implementations, this often requires that the eNBs are co-located to function correctly.

Vendor Identification

As part of deploying an NHN, you will need many vendors. In the planning stage you should begin to identify potential vendors based on your NHN architecture. 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 solutions services. These vendors can take care of the details of planning, design, installation, and operations support. Many are members of the OnGo Alliance. A list of our members can be found here: https://www.ongoalliance.org/about-the-cbrs-alliance.

SAS Administrators

The FCC has approved several SAS administrators. While the FCC defines the essential functions of the SAS, each SAS administrator 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, and other configuration options. Also, pay particular attention to the types of NHN the CBSD supports – not all CBSDs support every type of NHN operation, and in a MOCN NHN, the CBSDs need to have support for MOCN functionality. A complete list can be found here: https://www.ongoalliance.org/certification/.

MOCN Gateways

As discussed above, when deploying a MOCN NHN, a gateway can be used to provide the needed interface (if the CBSDs don't support them) or to consolidate the interfaces of multiple CBSDs. The gateway(s) must be compatible with the CBSDs.

Element and Device Management System (EMS/DM) Vendors

The EMS and DM systems tightly integrate with the CBSD and the EPC. The EMS typically provides control, configuration, management, and data collection services for the EPC. At the same time, the DM handles lifecycle management for the CBSD, including activation, configuration, and fault and performance management. As with the CBSD and EPC elements, not all available options will support any or all NHN architectures. Keep in mind that the EMS/DM may be provided by the CBSD or EPC vendor or by independent network management vendors that support the necessary management standards.

Evolved Packet Core (EPC) Vendors

To function, OnGo CBSDs must connect to an Evolved Packet Core (EPC). The EPC 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.

Different NHN architectures may need one or more elements of the EPC to be deployed as part of the NHN, or use the EPCs of the PSPs. For example, in MORAN and MOCN NHNs, no EPC needs to be deployed with the NHN, as the EPCs of PSPs are used instead.

If you want to deploy Private LTE services in addition to the NHN, your Private LTE service acts as one of the PSPs. In which case you will need to deploy your own EPC. It may be deployed onsite, co-located with the CBSDs, or use a cloud-based EPC service.

End-User Devices (EUDs)

Of course, critical to an NHN deployment are the EUDs, also referred to as user equipment (UE), that will connect to your network. Any LTE UE device that supports Band 48 can connect to an OnGo network. Fortunately, many handsets on the market today already support Band 48.

The complete list of certified devices can be found on the OnGo website: https://www.ongoalliance.org/certification/.

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.

You also need a backhaul connection if your system interfaces with other networks (such as the public Internet) and the PSPs. As with the internal network, ensure that your total backhaul capacity can support the amount of data you will be carrying, including providing sufficient bandwidth to each of your network's PSPs. Dedicated capacity for each PSP may be desired, or you can share a single "pipe" among them. 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 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 onsite infrastructure. You can increase backhaul bandwidth relatively quickly, but installing more cables is a lot more difficult. Most plan for twice their current bandwidth needs to provide 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 LTE 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. The PSPs will likely have specific security requirements to make sure their connections are secure. Consider these requirements 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.

Existing Data Infrastructure

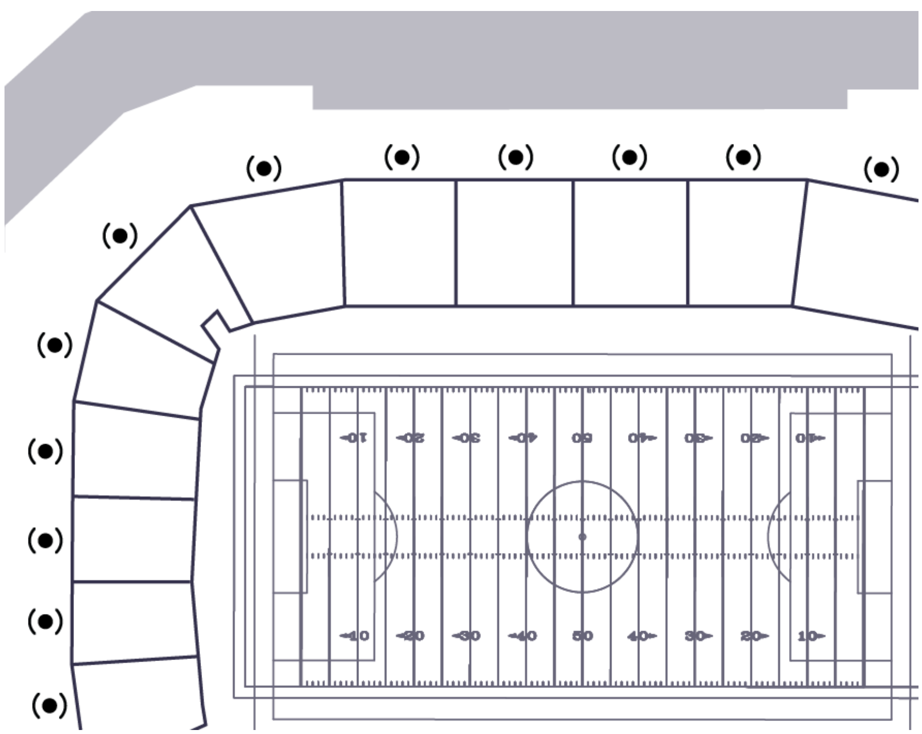
When planning your OnGo deployment, consider any existing data infrastructure, particularly other wireless systems such as Wi-Fi. OnGo excels at providing mobility, coverage in complex RF environments, and reliable, consistent connectivity for a large number of connected devices. In a multi-network architecture, 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. In contrast, 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 LTE network to address a particular use case, the incremental cost to support additional use cases is much lower. Adding incremental use cases (such as a Private LTE service) to the deployed LTE network can significantly improve the network's ROI.

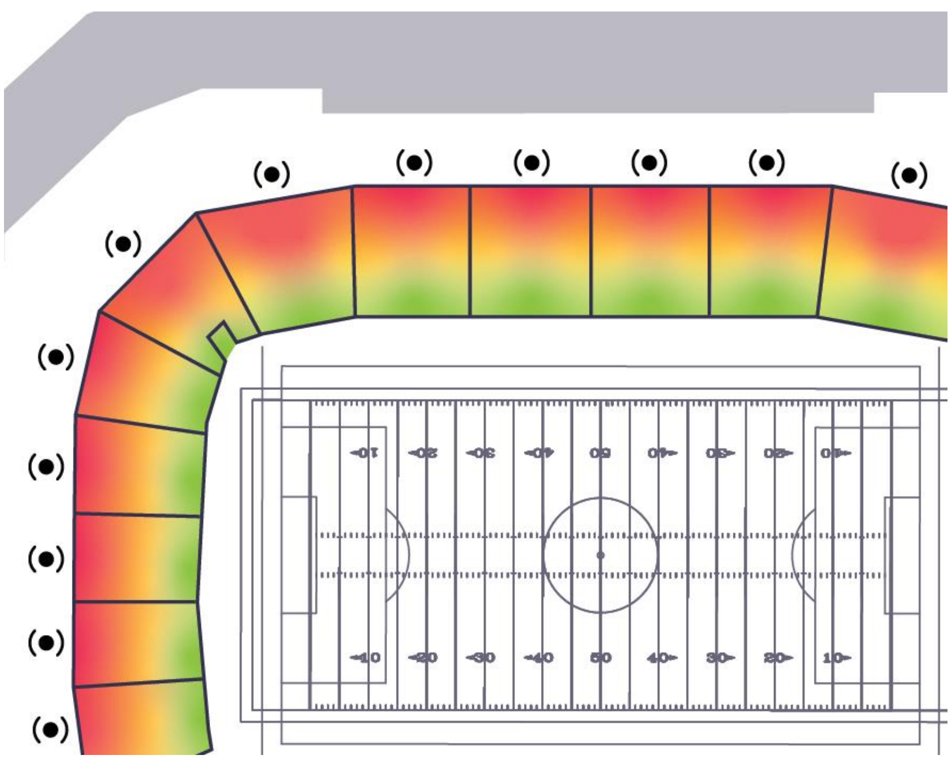
Scenario A: Sports Venue NHN Network Planning

To provide a more specific example of the planning required for your network, let's look at the sports venue scenario.



This NHN is focused more on increasing capacity rather than on expanding coverage. In this scenario, the main seating bowl area can seat up to 45,500 people, spread out over 12 acres. In the seating areas, attendees are dense with 1,625 users per 6,500 square feet. The structure is primarily reinforced concrete, with few obstructions within the stadium area. Power and data feeds can be routed to where CBSDs are needed.

Ideally, CBRS Access Points (APs) would be installed directly above the end-users to provide uniform coverage, good signal strength and minimal interference (SINR). However, in most deployments, the preferred CBRS AP placements are not practical given the physical layout of the stadium. That’s why CBRS capable, high-performance stadium antennas are better for optimizing coverage and minimizing radio count. One antenna per seating sector or 28 in total would be needed. The antennas would be mounted above and behind the seating section pointing down towards the field. Some other antenna mounting options such as handrail and Under the Seat (UTS) antennas were considered but are not feasible. They're also cost-prohibitive due to additional equipment and construction costs.



The biggest challenge is minimizing antenna pattern overlap, which results in degraded SINR performance and limits capacity throughput. Modeling of the signal propagation and performance allows you to calculate the worst-case user performance. Usually, 95% of a section will have an SINR performance of 3dB or better, so the minimum capacity available for 95% of the users will be at least 0.6 bits/second/hertz x 4 (for a 4X4 MIMO antenna) = 2.4 b/s/Hz. For a 10MHz channel, that will equal 21.6Mbps. For 80MHz of channel bandwidth, that will equate to 172.8Mbps (worst-case scenario) shared across 95% of all end users (1,625 seats) or 112kbps per user. There will be some variance in user experience depending on the seat location relative to the antenna.

Modeling determines that performance is equivalent with all CBSDs operating on the same channels or having CBSDs operating on alternating sets of channels with only half the available channels assigned to the CBSD.

The available capacity and performance should meet the needs of the PSPs, with some spare capacity to handle traffic growth. However, if additional capacity is needed or there are not eight 10Mhz channels available on GAA, the design will need to be adapted. Possible considerations:

- Smaller sectors.
- Alternate antenna placements.
- Subleasing PAL channels from PAL holders in the area, including PSPs.

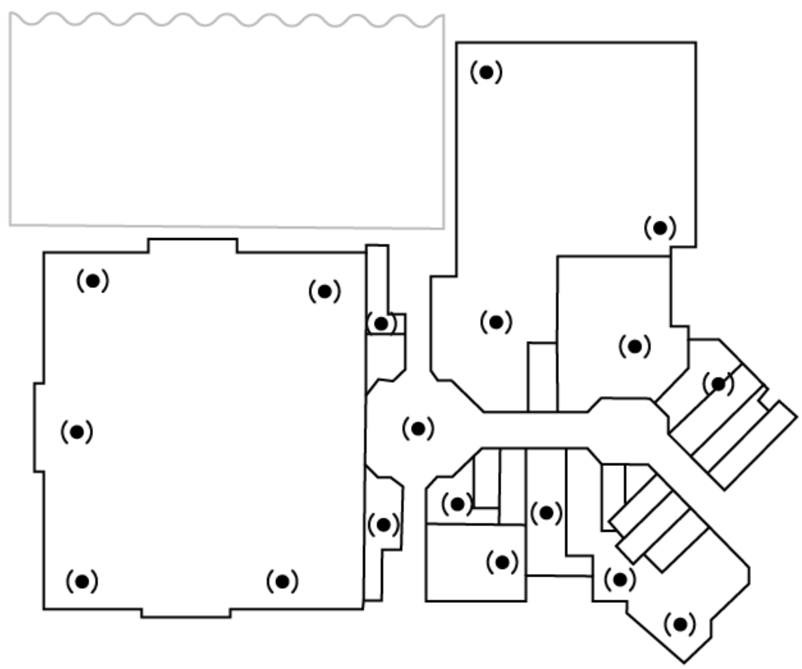
A MOCN architecture is preferred when there are a large number of CBSDs. Having different channels for each PSP (as required for MORAN) would result in too many channels. A MOCN gateway is included in the system design, to consolidate the connections to the CBSDs.

With an outdoor network you'll need many CBSDs, so it may be better to sublicense a PAL from a PAL owner in the county if one is available. A sublicense would help ensure a minimum service level.

Lastly, identify the top six service providers in the area and contact them about becoming PSPs in the NHN. They'll provide some initial guidance on the requirements needed to participate and their business terms.

Scenario B: Mall NHN Network Planning

Our second NHN scenario focuses on providing coverage. The building stands approximately 30-feet tall, with some areas rising as high as 50-feet, and the dimensions are 1600 x 940 feet. The building's structure is reinforced concrete, with a metal ceiling, and has many internal partitions, primarily drywall with metal studs. Floor displays, shelving units, and stands are distributed around the site. You can install power and data feeds in the ceiling relatively easily, and wired data infrastructure is ubiquitous. A wiring and computer room is in the office area.



Placement of the CBSDs is much less constrained than in the stadium scenario, resulting in much better signal propagation. Likewise, since this is an indoor deployment, interference is significantly lower.

With each Class A (<1 Watt) CBSD covering approximately 10,000 square feet, about 150 will be needed to provide full coverage. Several different placement scenarios are assessed based on measurements taken at the site and the modeling of signal strengths. Modeling shows good signal strength can be achieved for 95% of the area, resulting in worst-case performance on the order of 9.6 b/s/Hz, with 4x4 MIMO for an

86.4Mbps on a 10 MHz channel. The expected user density for a given CBSD is up to 400 users, which translates to 216 kbps per user.

Our modeling indicates that there is some benefit to having some of the adjacent CBSDs operate on separate channels, reducing interference between them. The available capacity and performance should be sufficient to meet the needs of PSPs. If additional capacity is needed, a CBSD can use two 10 MHz channels, raising the capacity to 432 kbps per user.

Since the deployment is indoors, the mall maybe relatively isolated from other facilities by parking lots. So, if there are few GAA users in the area, subleasing a PAL is not needed.

For the backhaul, at 30,000 customers, the total needed backhaul bandwidth is ~6.5 Gbps. Again, this should be within the site's service agreement's existing capabilities, so you’re not required to modify the backhaul.

A MOCN architecture is preferred, as there are many CBSDs, and having different channels for each PSP would result in too many channels. A Private LTE slice is included in the design to support staff and systems, so a complete set of identifiers is needed from the OnGo Alliance: a CBRS NID, an MMEGI, and 150 eNB IDs. In addition, an IBN is requested from the U.S. IMSI Admin for issuing SIMs for the Private LTE devices. The six Tracking Area Codes that come with an IBN will allow the private network slice to be split into six tracking areas to handle mobility control traffic.

The top five service providers in the area need to be identified, and initial contacts made about becoming PSPs in the NHN. In addition, they will provide some initial guidance on their requirements to participate and their business terms. One of the PSPs indicates that they would prefer that they have their own dedicated MOCN gateway, to consolidate the eNB connections, and to isolate their gateway from the other PSPs.

After defining the network capabilities needed for your NHN 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 the next stage, you'll need to contract with a SAS administrator to provide service for your deployment. Different SAS administrators 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 administrator 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.
- 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.
- Ability to use certificates from existing PKI (if any).
- Price.

EPC Selection

If you are deploying a hybrid network that includes a private LTE capability, or the NHN architecture requires it, you will need to select an EPC. For MORAN or MOCN systems, no local EPC is needed.

A basic EPC consists of four main network elements: MME, HSS, SGW, and PGW. The Mobility Management Entity (MME) and Home Subscriber Server (HSS) provide mobility and device access controls. The Serving Gateway (SGW) and Packet Gateway (PGW) are the network elements providing actual bearer data transport for mobile devices by routing data packets between CBSDs, your local network, and any connected networks such as the public Internet. The different elements of the EPC can be run on separate devices or integrated into a single device.

EPC 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 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 EPC will need to support. EPC providers can provide a range of solutions based on your needs. They often offer different management system capabilities, which we will discuss below.

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 EPC and perform EPC and Device (CBSD) management functions. Key considerations include:

- Ability to monitor and report PSP-required KPIs.
- 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.

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 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.

CBSD 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. 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 provide this information or use a spectrum analyzer (or similar equipment) to determine potential interference in the area.

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 repeated as the design is updated and modified during installation.

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

Network Design

At this stage, you need to decide on the design of the network infrastructure supporting your NHN network. Here are several important topics for you to consider:

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 CBSDs, and 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.

OnGo, LTE, and 5G

OnGo is currently LTE in the CBRS band. However, in the next release, we're adding 5G NR support. 5G will bring improved data rates, reduced latency, greater device density, and new network management features, including advanced network slicing options, to OnGo deployments.

Network Slicing

You can configure your NHN to provide multiple independent virtual networks, each with different configurations, controls, and features. For example, you can slice your network to create a Private LTE network so staff can access your internal network and voice calls, while the NHN can only access the public Internet.

A Private LTE network slice in an NHN system functions much like an additional PSP, which means you need to allocate an extra channel for the Private LTE slice in a MORAN system. In a MOCN, the Private LTE slice uses one of the available PSP slots on the channel. See the Private LTE Deployment guide for additional details (https://ongoalliance.org/resource/ongo-private-lte-deployment-guide/).

Note: While LTE supports basic network slicing, more advanced capabilities are supported by 5G.

Quality of Service

LTE provides multiple features for prioritizing and shaping data traffic, and those features are also available in an NHN. The PSPs will have specific requirements for traffic prioritization, with the details likely set out in the participation agreement. A Private LTE slice of the network can also have separate prioritization rules, allowing for further service customization.

EPC

MOCN (and MORAN) NHN deployments do not need an EPC element. Private LTE, and some other NHN network architectures, require core network services to manage devices, enable mobility, and support voice, video, data, and application services. EPC solutions can be physically deployed on-premises, contracted as a service, accessed via the cloud, or delivered as a hybrid solution. Because OnGo LTE deployments are so flexible, organizations can either purchase or subscribe to core services to create a solution that best meets their technical and budget requirements. (See CBRSA-TS-1002 for details on possible core network configurations.)

EPCs can even interoperate with other bands and technologies to provide connectivity failover, expand capacity, and eventually accommodate 5G-based technologies. OnGo ecosystem service providers, system integrators, and vendors can help your organization select the optimal solution.

PSP Agreements

Now it's time to put PSP service agreements in place for service via your NHN. These agreements typically include the requirements from the PSPs you've identified. In addition to the technical requirements, these usually include several KPI and problem reporting requirements, as well as resolution requirements.

The commercial terms of such agreements are entirely up to the PSP and the NHN operator. Options can include fixed flat fees, per user fees, or per megabyte fees.

IP Exchange (IPX)

IP Exchange (IPX) service providers can also play a key element in setting up an NHN. IPXs provide a business and technical framework for integrating data services across networks, both fixed and mobile. In the NHN context, they can provide a single point of contact for working with PSPs so that instead of having to execute agreements with each PSP directly, you just work with the IPX. On the technical side, they also have existing infrastructure for the interconnection between your network and the PSPs and enabling cross-network roaming.

Identifiers

There are several identifiers used within LTE to uniquely identify elements of the system, either as a globally unique identifier or as a locally unique identifier that is different from other systems operating in the area of your NHN. Several of the identifiers are combined with the first PLMN-ID broadcast by your NHN to ensure global uniqueness. In those cases, the PSP for that first PLMN-ID will need to provide the value.

For MOCN and MORAN systems, you only need one identifier: a Public Land Mobile Network Identifier (PLMN-ID). Each PSP will have one (or more) PLMN-IDs that they use to identify their network. These are broadcast by the CBSDs, which are limited to six PLMN-IDs in a MOCN system.

If you are deploying a private LTE slice, or the NHN architecture requires an EPC, things get more complicated. While you can obtain your own PLMN-ID, a PLMN-ID has been created specifically for use by networks in the CBRS band – the CBRS Shared Home Network Identifier (SHNI). When using the CBRS SHNI (which is 315-010), you will need to obtain additional identifiers from the OnGo Alliance in order to ensure your network works correctly:

- The CBRS Network Identifier (CBRS-NID). This 27-bit number is used to uniquely identify networks that use the CBRS SHNI.
- A Mobility Management Entity Group Identity (MMEGI), which is used to identify the Mobility Management Entity (MME), a component of the EPC.
- A Mobility Management Entity Code (MMEC) is an 8-bit number used to identify the MME within the MME Group associated with a given MMEGI. For most deployments, you'll only need one, but if you have multiple MMEs, each one in a given MME Group needs a unique number. Any number between 0 and 255 will do, and does not have to be obtained from the OnGo Alliance.
- Tracking Area Codes (TACs). These codes distinguish tracking areas controlled by a single MME and must be globally unique when combined with the first PLMN-ID broadcast by your NHN. (See below for a discussion of how many tracking areas, and TACs, you will need.)

Do I Need to Reserve ID Numbers?

In order to prevent potential interference issues with other LTE networks in your area, we generally recommend you reserve ID numbers, especially if you are deploying a Private LTE slice in your NHN. Otherwise, the necessary identifiers will be provided by the "lead" PSP's (the first PSP advertised by the NHN).

- You will also need Macro eNB identifiers, one for each eNB in your deployment. These uniquely identify each eNB and are used in LTE's self-optimization systems, and need to be a globally unique value when combined with the first PLMN-ID broadcast by your NHN. The PSP for that first PLMN-ID will provide you with the Macro eNB Identifiers to use in your system. (This identifier is needed even for microcell deployments, despite the name.) If your system is using the CBRS SHNI, you can obtain unique identifiers from the OnGo Alliance.
- Physical Cell Identity (PCI) – This is a number between 0 and 503 and is broadcast by each cell in your network. (An eNB typically can operate multiple cells – Category A CBSDs generally have only one cell, while Category B CBSDs may have eNBs that support several cells.) CBSDs should use Physical Cell Identities different from other nearby LTE cells, including other LTE networks operating in different bands in your area. The PSPs should provide you a list of the identities used by cells in your area so that you can select locally unique values for the cells in your network. PCIs are often optimized by the RAN using LTE's built-in self-optimizing network (SON) functionality.

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

Tracking Areas

For deployments that do not need a local EPC (e.g., MOCN and MORAN NHNs), the PSPs are responsible for managing the tracking areas, and you will not need to worry about it

If your deployment includes an EPC element (e.g., for a private LTE slice), and covers a large area, the network needs to be divided into Tracking Areas,

Private LTE Networks

You can configure a CBRS deployment to function as a Private LTE network. A Private LTE network provides services to authorized users and devices independently of other service providers. Devices typically need to have a SIM configured to access the Private LTE network. Devices that support multiple SIMs can use one of the extra SIMs to access the Private LTE network.

A network can be configured to function as a hybrid network, providing NHN services and a Private LTE network.

A separate deployment guide provides additional details on OnGo Private LTE networks (https://ongoalliance.org/resource/ongo-private-lte-deployment-guide/).

each identified by a Tracking Area Code (TAC). These codes detect when devices have moved within your network. When the network wants to talk to a device (paging), it asks each CBSD/eNB in the tracking area where the device was last seen to connect to that device. With more tracking areas, your network can page devices more efficiently, at the cost of additional control traffic from the devices notifying the network when they have changed tracking areas. With fewer tracking areas, there's less overhead control traffic of devices notifying the network when they've changed traffic areas, at the cost of more control traffic when the network needs to page the device.

If your deployment consists of multiple coverage areas that don't overlap (for example, a network that provides coverage in multiple office buildings but not the outdoor areas between them), each coverage area should be a separate tracking area with its own TAC.

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 NHN. As these devices are associated with the user on the home network, you don't need to do anything to do to enable or deploy EUDs.

Scenario A: Sports Venue NHN Design

At this point, your vendors have been selected. In this case, we will be using Class A CBSDs from a single vendor, which also provides the Domain Proxy and EMS elements. The SAS administrator has also been identified, with the commercial terms based on the Domain Proxy aggregating the CBSD communications.

The terms for becoming PSPs have been negotiated with the top six network operators in the area. They each have network configuration requirements in order to participate, which are configure in the EMS and the CBSDs (eNBs).

A specialist service provider has prepared a detailed map of the coverage area to determine the ideal placement of the CBSDs. Special antennas are used to reduce interference between CBSDs placed (relatively) close to each other.

To obtain a PAL, you have contacted the PAL owners in the area to discuss sublicensing terms. Also, given the need for a PAL and the fact that several of the CBSDs will be placed outdoors (Class B devices), you have hired a CPI to register the installations.

No EPC is needed for this deployment – as a MOCN NHN, the EPC component is provided by the PSPs.

A full set of identifiers is not required, as the PSPs will be providing their Network Identifiers – PLMN-IDs, MMEGIs, and TACs. However, you'll need Macro eNB IDs from the OnGo Alliance for each CBSD.

Scenario B: Mall NHN Design

At this point, your vendors have been selected. A single vendor will provide the CBSDs, Domain Proxies, and EMS, while the EPC is from an integrated solution vendor, making things easier to configure and maintain. Finally, the SAS administrator is selected, with the commercial terms based on the Domain Proxy aggregating the CBSD communications. Since all the CBSDs are Class A with an auto-sensing capability, a CPI is not required.

The terms for becoming PSPs are negotiated with the top five network operators in the area, with the Private LTE slice taking up the first PSP slot. Each PSP has network configuration requirements in order to participate, which are supported by the selected EPC.

A specialist has been contracted to check that the desired locations of the CBSDs will provide complete coverage. Based on the detailed measurements, the contractor can recommend where to place the CBSDs and how to best configure the antennas. In total, the 14 CBSDs required to handle data traffic can provide coverage throughout the mall.

The EPC managing the Private LTE slice will be physically located on the site, along with the MOCN gateways, in a network closet, and run on a single server along with the Domain Proxy and EMS elements.

Since a Private LTE network slice is part of this deployment, a set of identifiers is needed, including a CBRS NID for the Private LTE slice, along with an MMEGI and an eNB ID for each CBSD. To ensure that there are no interoperability problems with the PSPs, the Tracking Area Codes are set to values that are distinct from the PSP networks in the area.

Now it is time to start installing your CBSDs, EPC (if needed), 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

For NHNs, the SIMs are configured and provisioned by the PSPs. However, if you are operating a Private LTE network, in addition to the NHN (a hybrid network), you'll need to provision the Private LTE devices with SIM cards explicitly configured for your network, with a custom IMSI (using your IBN). SIM management is generally part of the EMS or EPC element of your deployment. See the Private LTE deployment guide for further information.

EPC Configuration

Your network EPC element needs to be deployed and configured if your network has an EPC. Specifically, the system needs to be configured with the appropriate identifiers – the PLMN-IDs of PSPs, MMEGI, Macro eNB IDs, etc. In addition, you'll need connections between your NHN and the EPC of the PSPs, which requires an exchange of IP addresses, as well as security credentials and certificates. Finally, your network configuration will also need to allow S1 and GTP tunnel connections to the PSPs.

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.

Key Performance Indicator (KPI) Verification

Once your network is commissioned and operating, confirm that your deployment provides the needed capabilities – coverage, available bandwidth, etc. In addition to your requirements, you'll need to confirm you've met the PSP's requirements. 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.

Scenario A: Sports Venue NHN Installation

In this situation, the CBSDs are installed, and the CPI registers its information and the information on the sublicensed PAL with the contracted SAS.

The Domain Proxy and EMS are installed and configured by their respective vendors. The vendor has also provided a set of SIMs to use in the devices connected to the network. The EMS is registering the information of the staff's devices so they can connect to the system.

Scenario B: Mall NHN Installation

The Category A CBSDs are installed and using their auto-sensing capabilities to register their location with the SAS. As a result, a CPI is not required.

The Domain Proxy, EPC, and EMS are installed and configured by the vendor. The vendor also provides SIMs for use in the devices, pre-configured for the devices to connect to the OnGo network.

Once everything is provisioned, the OnGo network is commissioned. After a few hours, the CBSDs will be activated by the SAS. Once the system is active, you can turn on the client devices and connect with the CBSDs.

Like any system, an NHN deployment requires support. The operator of the NHN is responsible for ensuring the integrity of the network it is providing to the PSPs. Here are some critical things to remember:

Network Operations Center (NOC) Support

All the components of the NHN 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 EPC, or the connections to the EPCs of the PSPs, the performance of the entire NHN can be impacted. So, it's crucial to have a NOC monitoring the system 24x7 when mission-critical applications are running on the network, and to ensure compliance with the PSP's requirements.

HW/SW Alarms

Individual CBSDs, backhaul connections, or end devices can develop hardware or software faults and 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 PSP agreements.

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 timeframe, 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.

Customer Support

PSPs requirements may include providing support to users if there are issues with a PSP subscriber's device within your NHN. These can include contact points and/or mechanisms for the PSP's NOC to coordinate a response to service issues if they arise.

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 necessary level of service depends on the requirements of the PSPs and how mission-critical the NHN system is for your operations.

Key Performance Indicators (KPIs)

There are several pre-defined LTE-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%
  - VoLTE 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-NHN handoff success rate >98%
  - PSP-to-NHN handoff (hand in) success rate >99%

  - NHN-to-PSP handoff 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 the EPCs of the PSPs. Specific KPIs for your system are typically defined in the PSP agreements and include how KPIs are measured, the measurement frequency, and how to report the KPIs to the PSP.

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. The PSPs may also require these checks.

Monitoring

A network monitoring system plays a vital role in an NHN 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.

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
CBRSA	CBRS Alliance, former name of the OnGo Alliance
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

Term	Definition
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.
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

Term	Definition
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
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	The OnGo Alliance, formerly the CBRS Alliance
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.

Term	Definition
PLMN-ID	Public Land Mobile Network Identity
PPA	PAL Protection Area. the geographic area that the SAS protects from interference for a given PAL.
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 Neutral Host Network?
Who will be connecting to your NHN?
What carriers/operators do you want your network to support as PSPs?
Do the PSPs have any requirements?
What devices will be connecting to your NHN? How many of each?
Which devices will be mobile within your network? Which devices will move into and out of your network?
Do you want your NHN also to have a Private LTE capability (slice)?

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, EPC Vendors (if needed), CBSD Vendors

Design

Selected SAS Administrator:
Selected CBSDs:
Number of CBSDs:
Selected NHN Architecture:
Selected EPC (if needed):
Selected EMS/DM:
Selected CPI:
PSPs:
PSP PLMN-IDS:
Assigned MME Group ID (MMEGI) (from lead PSP):
Assigned Macro eNB IDs (one per CBSD) (from lead PSP):
Tracking Area Codes (from lead PSP):
PAL License:
Network connections to PSPs:

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.