WHITE PAPER

Celona Neutral Host Network

Primer for Network Admins

OCTOBER 2024

celona

Contents

Introduction

Solving the challenge of fast and reliable in-building connectivity to public mobile network operators (MNO's) has remained elusive for decades. While solutions do exist, each suffers from one or more shortcomings such as high implementation costs, lack of scalability, limited control or a loss of important end-user features. Because of this, building/campus owners and operators have been left with less than desirable options to distribute wireless public carrier services indoors to users that demand them.

However, now that the private spectrum options, such as the Citizens Broadband Radio Service (CBRS) in the United States, have been made available to enterprises with no licensing fees attached, organizations now can deploy their own cellular wireless network from Celona throughout their buildings using a wireless LAN (WLAN) approach that leverages the existing corporate IT infrastructure.

This approach radically reduces this cost and complexity of other indoor cellular propagation options such as distributed antenna systems (DAS) by allowing Celona access points operating in the private cellular spectrum to be deployed and connected over an existing enterprise local area network (LAN) environment. Voice and data traffic from mobile devices that have active mobile network operator (MNO) subscription is then automatically offloaded to the Celona network and securely tunnelled to the respective MNO. In this model, software defined rules and configuration changes within the private cellular network will allow for multiple MNOs to be supported – and simply moves, adds and changes to improve coverage and enable new services.

This document provides an overview of what a Neutral Host Network (NHN) is, how it can help solve indoor wireless challenges and an overview of Celona's unique architecture for neutral host. It is intended for IT architects interested in learning more about NHN design and deployment options from an enterprise network viewpoint.

What is a Neutral Host Network?

Neutral host networking is the use of a private LTE/5G wireless infrastructure within the enterprise premises to transmit certified third-party wholesale carrier service(s) to users that have access to the public carrier's network. This extends the MNO service(es) across the private LTE/5G network deployment that private cellular capable devices can access.

The role of an NHN is to leverage existing private LAN, WAN and cellular radio access network (RAN) network infrastructure to propagate MNO carrier signals. This architecture can create enhanced signal strength or increased capacity in locations where signal strength is poor – or at certain venues where it doesn't make sense for each MNO to deploy and manage a separately owned RAN. MNO's can also offload capacity leveraging a private NHN in areas where networks are prone to user/bandwidth congestion issues, providing added scalability.

Neutral host networking is a relatively new concept that, unlike traditional models, allows multiple parties - both private and public - to securely share the same network infrastructure within an organization. Doing so provides wireless connectivity to a wide range of MNO subscribers with the goals of increasing public cellular network coverage and capacity while dramatically reducing capital and operating expenses using a shared network infrastructure approach.

For users of the network, an NHN operates seamlessly with their MNO's regular cellular network and will be entirely transparent to them. Accessing the NHN requires no user input and is independent of enterprise network authentication. It does not require any action on user's part to roam into and out of the network.

Solving the challenge for indoor cellular in the enterprise

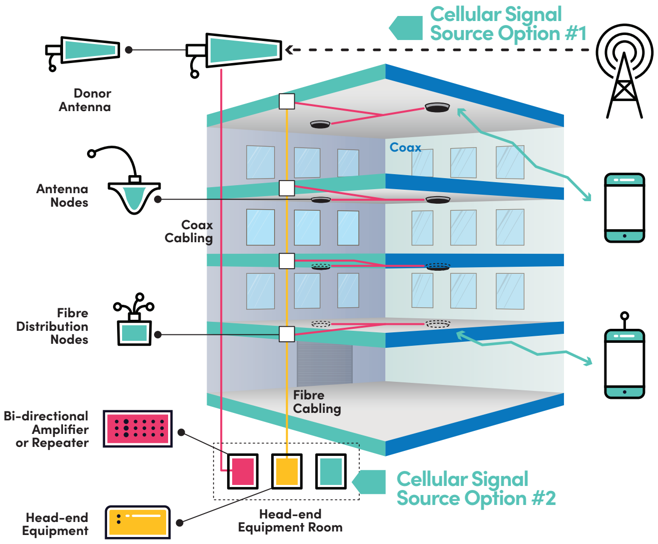
Indoor wireless is a challenge that has long been an issue for IT departments that manage buildings, campuses, warehouses, and manufacturing plants. In some cases, public MNO signal is non-existent. In others, wireless signal propagation from MNO macro cells that are located too far away or cannot penetrate well inside buildings due to modern building materials such as the use of low-emissivity (Low-E) glass.

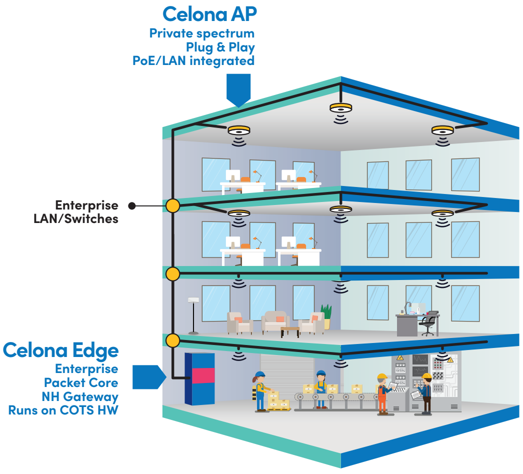
While several public carrier signal extension methods exist including signal boosters and Wi-Fi calling, the most popular option is to deploy a distributed antenna system (DAS). The architectural philosophy behind DAS is that it amplifies cellular carrier signals over passive cabling that is run throughout a given site. This disparate and discrete system requires the costly design and deployment of specialized cabling, RF antennas and carrier infrastructure equipment to process signals, terminate and route connections.

Let's now contrast the shortcomings of DAS with a neutral host alternative that's built and deployed using a Celona 5G LAN. Unlike DAS that requires a wholly separate network in addition to space/power for MNO network equipment deployed within a building, the Celona 5G LAN leverages the existing enterprise IT infrastructure with its local area and wide area network to consolidate public MNO coverage within a unified private cellular network. This concept is much like the consolidation of analog/digital phone systems onto IP networks using voice over IP (VoIP) technologies.

The following diagram shows how a Celona 5G LAN can significantly simplify integration processes while simultaneously reducing infrastructure cost.

DAS vs Celona 5G LAN





Wireless networks utilizing the private cellular spectrum, such as CBRS in the US, will grow significantly now that a majority of cellular wireless capable devices fully support the spectrum. Full list of such devices can be found at celona.io/devices.

In fact, most smartphones/tablets and enterprise-grade IoT devices manufactured in the last three years include wireless chipsets and associated firmware that is natively compatible with networks that operate in the frequency range for private spectrum (e.g., 3550 to 3700 MHz CBRS in the US).

Not only can this frequency spectrum be used for private mobile network purposes, but a defined portion of the available bandwidth can also be used to advertise public MNO networks. This means that any private cellular capable device with a public carrier SIM that's being advertised on the private spectrum via the private cellular network can connect and use the MNO network services natively as if it were connected to a public MNO cell tower. No other free-to-use spectrum can accomplish this feat.

It should also be pointed out that the owner of a Celona 5G LAN, which includes private spectrum access, becomes the mobile network operator within such facility via neutral host networking. This is appealing to private enterprises as they are no longer at the mercy of the MNO when public cellular connectivity and coverage problems occur for their employees or their guests within their facilities. NHNs may be managed by a third-party managed services provider (MSP) or the enterprise organizations themselves. Either way, an NHN enables private mobile network devices and public mobile network operator (MNO) subscribers to share secure cellular wireless connectivity within the enterprise footprint.

From a public carrier perspective, each MNO permits the broadcasting of their public network identifier. The MNO also is fully in control of their own wireless services as core network functions and services such as IP multimedia subsystem (IMS) are derived and managed from the MNO's existing network. Connectivity between a Celona 5G LAN and multiple MNO networks is accomplished through the establishment of individual secure IPsec connections across the internet to the respective MNO cores. This eliminates the need for MNOs to deploy their hardware on-premises and instead leverage the available Celona 5G LAN.

End-user experience on a Neutral Host Network

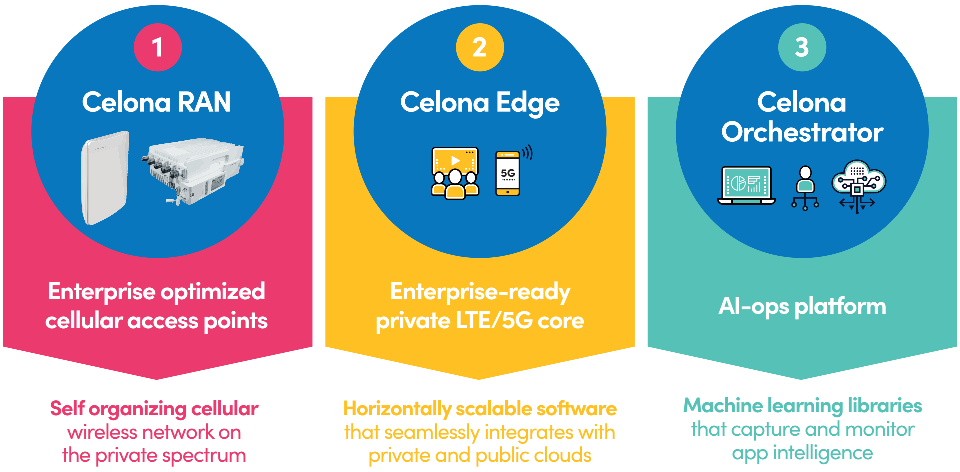
Connecting a device to a private cellular network enabled with neutral host operates in the same way a mobile device would roam to any public MNO network. The mobile device with private cellular spectrum support will automatically discover the NHN by scanning the private spectrum frequency band for a network broadcasting the MNO PLMN-ID apart from the private network identified (e.g. CBRS Identifier (CBRS-I) in the United States).

This lets the end device know that neutral host services are enabled on this band. The end device looking to join a public network then reads the list of MNO identifiers to determine if the MNO they use is on this list. If it is, the end device will join the private cellular network within its MNO credentials.

The devices then will gain access to MNO location/emergency services (emergency calling, Wireless Emergency Alerts (WEA), and Wireless Priority Services (WPS)) that do not function when using Wi-Fi calling.

Celona's Neutral Host architecture

Celona's 5G LAN has been devised with cost-savings, deployment simplicity and ease-of-management in mind. This includes a fully-integrated, cloud-first approach with few on-premises network services required. As depicted in the following graphic, Celona RAN equipment and Celona Edge platform services are deployed on-site leveraging the existing enterprise IP network while the Celona Orchestrator, operating as the management and operations plane, resides in the cloud.


1
Celona RAN
Enterprise optimized cellular access points
Self organizing cellular wireless network on the private spectrum
2
Celona Edge
5G
Enterprise-ready private LTE/5G core
Horizontally scalable software that seamlessly integrates with private and public clouds
3
Celona Orchestrator
AI-ops platform
Machine learning libraries that capture and monitor app intelligence

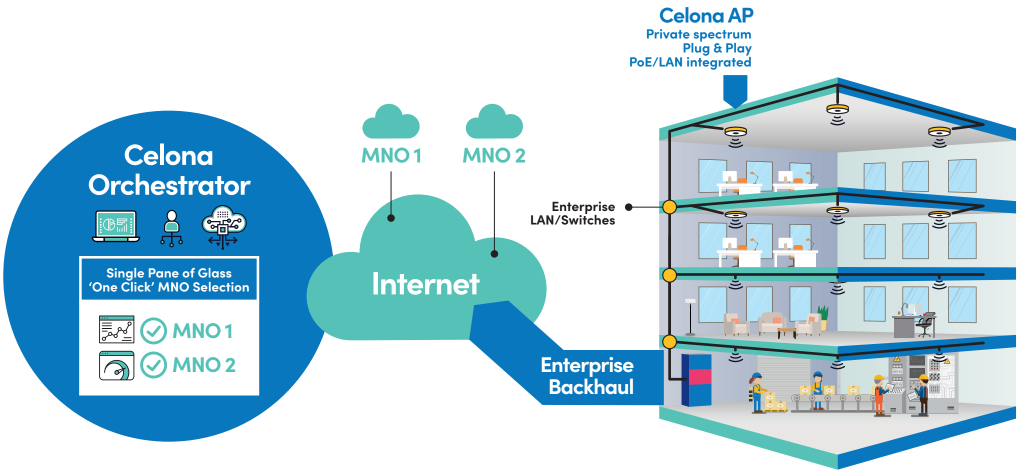
The fundamental concept of NHN is the sharing of deployed network infrastructure components. Network sharing is enabled through methods such as sharing the campus, tower, rooftop, power, cabinets, lighting, and air conditioning. Active sharing of the corporate network involves dynamic real time sharing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

When a private Celona 5G LAN is first designed, architects should calculate the total throughput capacity of the new radio network and ensure that this additional bandwidth can be supported by the existing LAN infrastructure. If not, upgrades will need to be made to support the added throughput capacity.

Additionally, bandwidth calculations for all traffic sent between the Celona network and MNO(s) across the established IPsec tunnel(s) will need to be calculated and internet WAN resources need to be adjusted to handle the additional traffic load.

NHNs add the ability to easily utilize private cellular access points to broadcast multiple signatures of different MNO networks, securely tunneling traffic directly to each requisite MNO's mobile core. The following diagram illustrates how Celona brings multiple MNO services to a 5G LAN:

Celona's Vision for Neutral Host



The one unique component to a Celona private mobile network that also supports neutral host capability is the inclusion of a mobile operator core network (MOCN) gateway that establishes an IPsec tunnel between the Celona 5G LAN and the MNO core. The MOCN gateway provides critical services for NHN to operate efficiently and with data security in mind.

Neutral Host design and deployment considerations

A certain level of trust along with defined management/troubleshooting roles are required between the MNO and private cellular network operator. Once a Celona 5G LAN is deployed with neutral host services, enterprises simply need to work with one or more certified MNO's to establish a secure IPsec tunnel between the MNO network and the Celona MOCN gateway.

The MNO will also require that the Celona 5G LAN exposes API access to key performance indicators (KPIs). This will be used by the MNO for monitoring and troubleshooting purposes. Celona offers a rich API structure that allows any MNO to easily integrate this data into their existing systems to monitor the user experience. Example KPI's that an MNO would want visibility into include:

- Total Radio Resource Control (RRC) attempts
- RAN resource success/failure rate
- Total VoLTE calls
- Call retainability
- Average and peak utilized bandwidth usage

In the context of ongoing management and troubleshooting, when problems occur on the NHN, monitoring and alerting tools on the customer side as well as separate MNO operated tools analyzing KPI information on the carrier side will notify both parties of any network performance issue.

If the problem detected is on the private cellular infrastructure across the enterprise LAN and out to the MOCN gateway, the local administrator will be responsible for resolving any issues. All other issues that occur within the MNO's core network on the opposite of the IPsec tunnel will be the responsibility of the MNO to resolve.

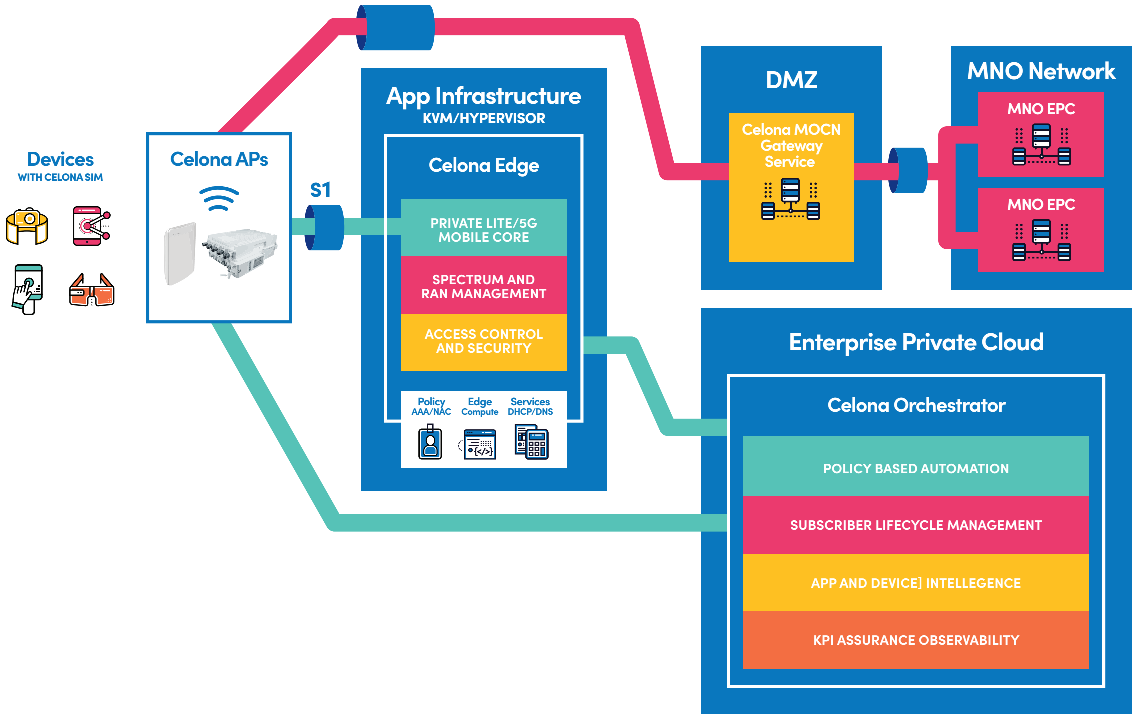
Neutral Host data security and segmentation Celona understands the sensitive nature of data traversing a corporate LAN. That is why steps have been taken to logically segregate private network traffic from public MNO traffic enabled via neutral host.

The following diagram shows how separate IPsec tunnels are established at each Celona access point (AP). One tunnel is for private network traffic while the second tunnel transports data destined to one or more remote MNO networks.

Once the MNO traffic reaches the MOCN gateway, traffic from the single MNO tunnel is segmented onto individual IPsec tunnels and transmitted to the carrier's core network services.

The MOCN gateway provides a host of IPsec tunnel security services. These are:

- Standards compliant, IKEv2 and IPsec tunnel configuration,
- Internal IPsec tunnel termination from the private cellular access points,
- External MNO IPsec tunnel termination from the MNO gateway, and
- Internal and External IPsec certificate handling to provide the best level of security for IPsec tunnel establishment.



RAN Sharing with MOCN

The MOCN architecture approach that Celona uses is unique from a RAN sharing perspective. Unlike other models that requires each MNO to advertise their network using licensed frequencies or separate unlicensed channels, MOCN allows for multiple carrier and private networks to be advertised using a single private spectrum channel. This allows for much greater deployment flexibility for multi-MNO carrier in-building propagation in addition to private LTE/5G who can all share a single access point and antenna infrastructure.

SEE THE CELONA TECHNOLOGY IN ACTION

Request a proof of concept and custom product demonstrations by visiting us at **celona.io/journey**.

hello@celona.io | celona.io

celona