WHITE PAPER

Definitive Guide to 5G LANs

MAY 2022

celona

CONTENTS

Enterprise Wireless Challenges 3

Wi-Fi/Cellular Comparisons 6

Enterprise Cellular Options 9

Introduction to CBRS Spectrum in the United States 10

Private 5G LAN Advantages 12

The Celona 5G LAN Solution 13

Going Edgeless with 5G LANs 15

5G LAN QoS with MicroSlicing 17

5G LAN Routing 18

5G LAN Security 21

5G LAN Device Ecosystem 22

5G LAN Use-Cases 22

5G LANs for Neutral Host Networking 24

Enterprise Purchase Criteria for 5G LANs 26

Executive Summary

Businesses are increasingly aware that they must carefully choose their enterprise wireless technology wisely or risk of dealing with performance, reliability, and security issues. By combining the simplicity of conventional wireless LANs with advanced LTE/5G cellular wireless technology, Celona 5G LANs offer wireless coverage in the most challenging environments, interference free connectivity, deterministic performance, and uninterrupted mobility for a new generation of wireless networking use cases.

Developed as an IT-friendly overlay atop existing enterprise networks, Celona 5G LANs operate just like traditional wireless LANs – as a fully integrated end to end platform that includes indoor and outdoor small cell access points, mobile network services for 4G LTE and 5G cellular, and a comprehensive cloud-based orchestration platform. The result is a flexible and easy to use alternative to traditional private cellular solutions that are often cost prohibitive and succumb to inherent deficiencies in being able to seamlessly integrate with enterprise networks and policies.

This definitive guide to 5G LANs highlights common enterprise wireless challenges, reveals the benefits of 5G LAN architectures for private cellular networks and provides relevant details into the private spectrum options (such as CBRS in the United States) as well as an architecture overview of Celona's 5G LAN solution.

Enterprise Wireless Challenges

The use of wireless technologies allows for ease of deployment, mobility, and rapid scalability in a variety of use-case environments and scenarios.

For decades, companies have relied on wireless technologies including microwave, satellite – and specifically Wi-Fi, for wireless backhaul and access connectivity. While these technologies have helped us radically transform our networks, they do have limitations that business-critical applications will expose. Common examples include:

WIRELESS CHALLENGE	External Interference	Coverage Deficiencies	Device Capacity	Quality of Service	Data Security	Mobility	Device Onboarding
ENTEPRISE IMPACT	Unpredictable performance and reliability issues	Weak signal strength and dead spots prevent device connectivity	Co-channel interference between radios and client devices negatively impact performance	Inability to define latency and throughput service levels beyond QoS prioritization	Inability to define latency and throughput service levels beyond QoS prioritization	Performance dependent on client devices as they roam between wireless APs	IT admins and/or end users have to manually configure each device

External interference

Several popular wireless technologies such as Wi-Fi, Bluetooth, ZigBee and LoRa take advantage of unlicensed and unmanaged spectrum that is free to use and does not require any type of licensing to use. Of course, the downside of unlicensed spectrum is that it can succumb to reliability issues due to external interference. This is most commonly associated with competing wireless networks and/or devices in the same vicinity competing for the same frequencies.

Coverage deficiencies

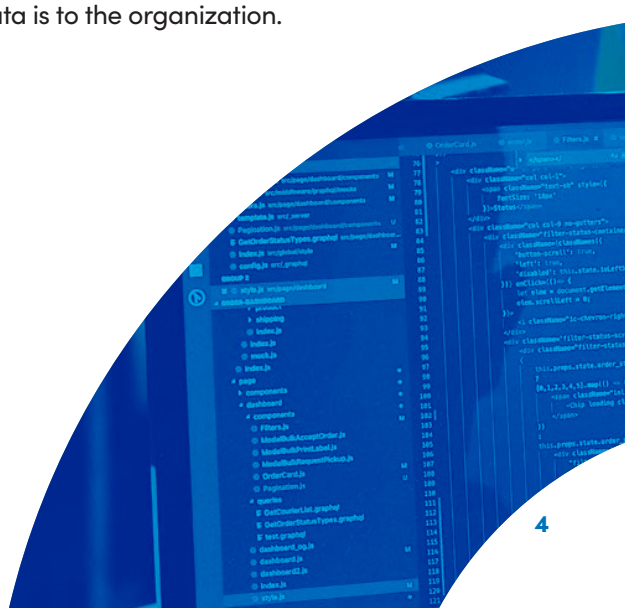
Areas where propagating wireless signal strength is a challenge can negatively impact business operations. Even with carefully prepared deployments including the use of wireless planning tools, site-surveys and spectrum analysis, wireless signals can fail to propagate where needed. Problems frequently relate to new, external interference that creates RF noise, preventing devices from properly joining a network. In other situations, physical obstructions introduced into the coverage environment prevent signals from penetrating critical areas of a building or campus.

Device capacity

In areas where large numbers of users and/or devices congregate, enterprise Wi-Fi networks experience increasing co-channel interference between the connected devices and the wireless access points in the area. This takes place because each device randomly tries to gain access to the wireless medium to transmit packets. This causes each device to "backoff" and wait their turn, and/or try to utilize a lower data rate during next round of transmission to improve the chances of gaining access. This operational model can quickly create performance and reliability issues in high density environments. A common workaround for this problem is to simply add more wireless access points with specialized configuration. Although this technique can work, it significantly increases both cost and wireless management complexity.

Quality of Service (QoS)

In a growing number of situations, the need for guaranteed throughput and latency levels for mission-critical business applications is essential. Like corporate LANs and WANs that have Quality of Service (QoS) parameters applied, many Wi-Fi networks rely on the same QoS principles when identifying and prioritizing wireless traffic. Unfortunately, these queuing and buffering mechanisms operate at a "best-effort" capacity with the inability to schedule dedicated bandwidth or latency to client devices no matter how important the data is to the organization.



Data security

Most wireless technologies configured with best-practice enterprise security settings are secure but can still be exploited. The ease at which a Wi-Fi access network or point-to-point link can be improperly secured leads to situations where sensitive data can easily be lost or stolen. Many Wi-Fi networks, if not all, still utilize pre-shared keys and open SSIDs to allow for IoT and/or guest device connectivity – opening doors to additional risk factors for critical enterprise infrastructure.

Mobility

In enterprise Wi-Fi networks, endpoints trigger roaming from one AP to another. This can become a serious challenge for large scale implementations if the differences between wide ranging set of Wi-Fi clients are not well understood in terms of their roaming capabilities. This makes it difficult for administrators to deploy Wi-Fi APs with uniform coverage patterns to guarantee smooth roams as the roaming trigger will be different from one device to the next. Thus, coverage dead spots may form for some endpoints while providing sufficient coverage for others.

Other issues, such as over saturated AP's or interference can also be detrimental to seamless mobility. Both can cause situations where a device should roam to an AP with a higher signal strength – but cannot make the switch due to too many devices being connected to the AP – or when an obstruction or external signal interference gets in the way of roaming from one AP to another.

Device onboarding

Given the number of wireless devices connecting to enterprise networks today, device onboarding procedures can become a tremendous time sink if not properly handled. Enterprise Wi-Fi solutions offer a few different device onboarding and connectivity options such as pre-shared keys and 802.1x authentication, but each come with their challenges.

Inevitably, pre-shared keys will become completely insecure as the shared password is leaked out and used by unauthorized users and devices. And while 802.1x mechanisms allow for individual usernames and passwords to be used it is common for these credentials to be mishandled, finding their way into the hands of unauthorized users. Finally, the complexity required to setup 802.1x using external user databases, network policy servers and device certificate servers can be tedious and quickly grow in complexity.

Wi-Fi/Cellular Comparisons

Most network administrators are familiar with the interworking of enterprise-grade Wi-Fi network architectures, deployment strategies and management processes. Comparing Wi-Fi to private cellular connectivity in the enterprise has proven to be an effective way to help potential Celona customers familiarize themselves with similarities and differences between the two technologies.

If administrators understand and have first-hand knowledge with potential shortcomings of their existing Wi-Fi infrastructure, they will better be able to understand how private 4G and 5G cellular wireless connectivity can better operate in certain use-case scenarios.

As Wi-Fi standards evolve to deliver more deterministic operation, challenges noted above will remain. For instance, Wi-Fi 6 makes use of cellular's OFDMA methodology for providing access to the wireless medium. However, to gain access to a specific channel, Wi-Fi 6 still requires the use of CSMA-CD, a network protocol requiring devices to sense and listen to hear if a given channel for transmission is busy or not. In other words, devices still must contend for access to a wireless channel. Only after a device determines that a channel is "clear to send" can it use OFDMA to transmit on that channel.

In contrast, LTE/5G cellular technology doesn't have this limitation as access to the medium and the channel is centrally scheduled by the network for all devices. This effectively eliminates media contention, giving each devices dedicated access to the wireless spectrum – and removes unpredictable performance in how different devices behave in different network configurations and physical environments.

Useful comparisons of Wi-Fi to 5G LANs include:

	Enterprise Wi-Fi	5G LAN
Spectrum	Unlicensed Spectrum used by Multiple Technologies	Coordinated Spectrum Allocation between networks by SAS
Layer 1	20-36dBm EIRP indoors/outdoors Limited data rate selection	30dBM EIRP indoors and 47dBm outdoors Better receiver sensitivity & H-ARQ More granular data rates
Layer 2/3	Distributed contention (CSMA even with OFDMA Statistical prioritization via WMM queues (performance dependent on load Co-Channel Interference is Blocking (limiting frequency reuse and network capacity	Central coordination by infrastructure and scheduled transmissions Guaranteed SLAs with QoS traffic scheduler (strict priority independent of load) Full frequency reuse across network (higher user density and network capacity)
Auth	User and cert based credentials Seperation of services via "SSIDs"	SIM (pSIM or eSIM) based credentials Seperation of services via "slices"
Mobility	Channel scanning and mobility decisions initiated by devices	Mobility controlled by infrastructure with precise timing
Voice	Wi-Fi calling with limited roaming and QoS	Neutral host service 3GPP VoLTE and roaming

Data transport scheduling

A major differentiator that sets a private cellular apart from Wi-Fi technology is how the network schedules when a device can or cannot transmit data. Unlike Wi-Fi that requires user equipment to listen and wait for an opportunity to transmit data, cellular is fundamentally different as access is centrally scheduled by the network itself. The difference here is significant as network administrators are now given full control to prioritize and configure dedicated throughput and latency controls with strict service level agreements for device and application traffic.

For newer Wi-Fi 6 and 6E deployments, orthogonal frequency division multiple access (OFDMA) does help by allowing for concurrent devices to transmit data simultaneously across the same wireless channel, it still lacks the level of application performance guarantees that only cellular-based wireless networks can offer.

Wireless spectrum

Wi-Fi operates on unlicensed spectrum in the 2.4, 5 and now 6GHz frequency ranges for Wi-Fi 6E. For many enterprise IT departments, the spectrum becomes a mixed blessing. While a large chunk of Wi-Fi spectrum can be freely used by anyone, this freedom makes it prone to performance and reliability issues when external interference is introduced. Alternatively, private LTE and 5G networks are designed to operate within private spectrum options that deliver interference-free operation, such as the Citizens Broadband Radio Service (CBRS) in the United States. While this band offers unlicensed spectrum that is free to use like Wi-Fi, additional operational precautions have been put into place to effectively eliminate the risk of interference. Note that many other countries, such as UK, Germany, France, have allocated spectrum in a similar manner to the United States, with specific frequency ranges differing from one country to the next.

Access point coverage and capacity

Because Wi-Fi operates in fully open and unlicensed spectrum, one way the Wi-Fi standard attempts to eliminate external interference is by restricting the power and antenna gain capabilities of an access point (AP). In ideal deployment settings, this limits the coverage area of a single Wi-Fi AP with an omni-directional antenna to a maximum of 150 feet for indoor deployments and 300 feet for outdoor or line-of-site (LoS) deployments.

A private 5G LAN, on the other hand, is allowed to legally operate at higher power and gain levels compared to Wi-Fi. This is largely since private cellular spectrum options such as CBRS help manage external interference and thus works in the background to ensure that competing private LTE / 5G networks do not interfere with each other. This level of centralized management and interference protection allows for coverage areas that eclipse Wi-Fi by 4-10 times. Currently, in the United States, the FCC has approved two classes of wireless access points for private CBRS spectrum access: Category A with a maximum equivalent isotopically radiated power (EIRP) of 30 dBm/10 MHz and Category B with a maximum EIRP of 47 dBm/10 MHz.

Device onboarding

Wi-Fi networks use the concept of a Service Set Identifiers (SSIDs) to let Wi-Fi endpoints find and or join the wireless LAN. SSID's that are broadcasted across the operating wireless channel are detected by the Wi-Fi endpoints seeking a network to join. Depending on the type of access-control security policies used, the connecting user or device may need to enter authentication credentials prior to being granted access to the network.

A private cellular network, on the other hand, uses a similar network identification approach known as a cellular System Identifier (SID). An SID can be broadcasted across the private spectrum and can be picked up by compatible cellular endpoints that are seeking to join. In a private cellular network, the device identification and authentication information is tied to a physical Subscriber Mobility Module (SIM) or an embedded SIM (eSIM) in digital form. The information required by a cellular device to be onboarded and join the private cellular network is more granular and thus administrators have more control over which users/devices can communicate across the wireless infrastructure.

Data security

Wi-Fi networks can be deployed with varying levels of cyber security from an authentication and data encryption perspective. In some cases, an SSID is configured to be "open" – meaning that no authentication is required, and anyone can join. Stepping up one level, a pre-shared key can be used as a simple access-control authentication method. The problem, however, is that multiple devices can use and reuse the same key across an unlimited number of devices. This lack of control over which users and devices can connect creates a situation where the business is prone to unauthorized network access – risking privacy and security of the rest of the critical application infrastructure.

Finally, enterprises commonly deploy their secure corporate networks using the IEEE 802.1x standard that leverages the Extensible Authentication Protocol (EAP) for authentication. EAP uses a backend authentication server (typically tied to Microsoft Active Directory) that requires each user/device to authenticate using individual username and password credentials.

Once a device has successfully authenticated, encryption can be used across the wireless medium to protect data from being intercepted and read. It is important to note, however that some Wi-Fi encryption methods available are secure than others. Thus, enterprise Wi-Fi administrators must understand and configure encryption appropriately on a per-device basis.

Alternatively, a private cellular network requires that all devices authenticate and provide encryption using the highest levels of device identification, authentication, and data encryption available on enterprise wireless networks today. Because there is no way to incorrectly modify or alter these security functions, it eliminates any risk of misconfiguration that is possible with Wi-Fi. Additionally, because of the use of SIM-based authentication and strict access control after a user/device is authenticated, private cellular networks align perfectly with zero trust security architecture frameworks.

Enterprise Cellular Options

There are three primary cellular delivery options for enterprise users. Each one has different price-points, privacy considerations and planning/deployment/management requirements. Here is a brief breakdown of each option:

Private network slice on a public carrier network

Some public 5G carriers offer a logically segmented network slice that can be used to transport enterprise customer data. This logically segmented slice of the public cellular service specifies bandwidth and latency service level agreements (SLAs) to which the network must adhere. All customer traffic is placed into this secure slice created for the entire enterprise client device mix, protected from all other traffic flows on the public network. Although this option may be suitable for use-cases that require far-reaching cellular access across large geographic areas, concerns over data ownership and privacy, high operational costs, and a lack of granular controls for individual app QoS or device performance are common.

MSP operating a private 5G LAN (Local Area Network)

If available where a business requires wireless connectivity, an enterprise may opt to become a customer of a managed service provider (MSP) that operates their own private 5G LAN. Depending on the service offering(s) available, this option may provide increased levels of control over throughput and latency for application-specific traffic. In most cases, the operational expenditures of using a MSP-delivered 5G LAN will be lower than that of public 5G alternatives.

Privately deployed and managed 5G LAN

For businesses wanting full control, visibility, and complete data privacy in their RAN (Radio Access Network) – like how they currently manage their Wi-Fi LAN (WLAN), a privately deployed 5G LAN would be the optimal choice. This gives enterprises the deployment flexibility, on-demand configuration options and per-application QoS control on-demand. The trade-off for this architectural model is an increase in capital expenditure and the need for IT resources that can properly design, deploy and maintain 5G LAN network operations.

Introduction to CBRS Spectrum in the United States

In the United States, privately deployed LTE and 5G networks can operate using the 3550-3700 MHz Citizens Broadband Radio Service (CBRS) frequency band. This is also commonly referred to as "band 48".

While similar spectrum management services are available in other countries (see figure below) that attempt to replicate what CBRS offers, understand that frequencies, spectrum width, channel availability and licensing may differ drastically. For the purposes of this document, our focus will be on CBRS within the US.

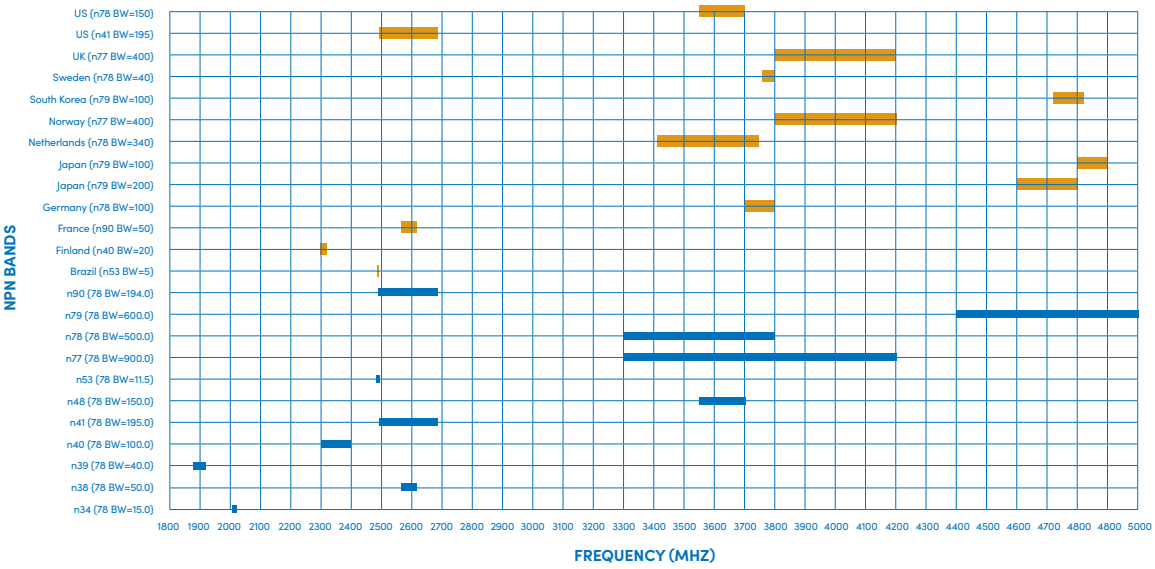


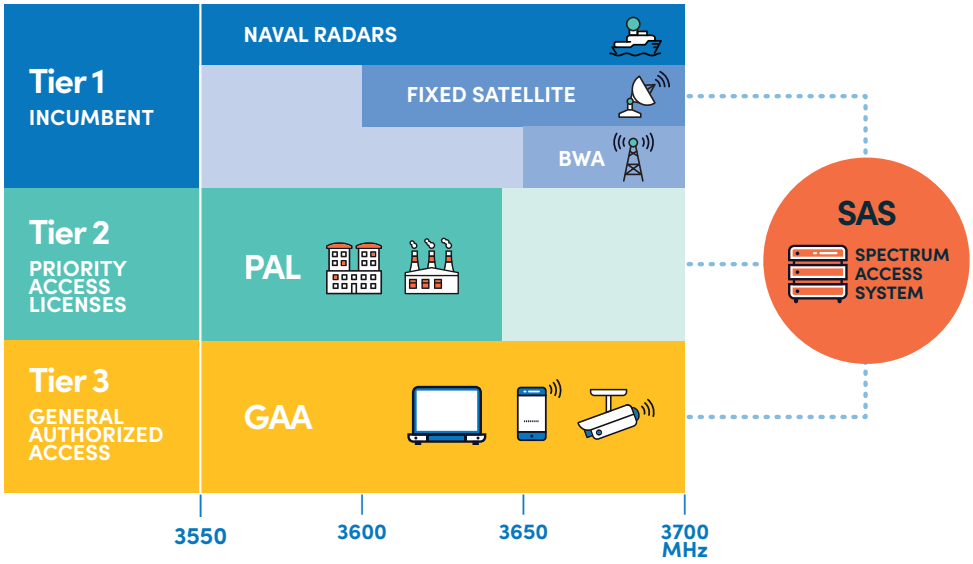
FIGURE: Regulated unlicensed nonpublic network spectrum allocation globally

The history of CBRS dates to 2015 when the FCC adopted new rules that allowed for a three-tiered access and authorization system that was designed to allow for private and free access to the band when not in use by higher-priority, federal uses or licensed priority access.

Tier-1, or incumbent access is reserved for federal purposes. Tier-2 access is referred to as a Priority Access License (PAL). This tier requires a license issued and managed on a county-by-county basis. Each license lasts 10 years before renewal is required. Finally, the General Authorized Access (GAA) tier is the free-to-use tier in which most private 5G LANs operate. If the higher tiers do not consume all available channels, any business can opt to reserve access to those channels for their own private use.

The Spectrum Access System (SAS) is the central platform that manages CBRS channel use by prioritizing channel access for higher tiers while also working to limit channel interference between CBRS GAA users in the same geographic location.

SAS is a cloud-based management platform that is operated by several private technology corporations including Google, Federated Wireless, Sony and CommScope. The SAS handles all private-use registrations/de-registrations, spectrum inquiries and spectrum channel grants on the FCC's behalf. It also enforces the need to allow higher-priority users gain access to the spectrum first. The following diagram shows the CBRS tiering structure and how all tiers are centrally managed and monitored by way of the SAS:



The relative ease at which CBRS channels can be accessed and used by any organization at nearly any location in the US is a key reason why private 5G LANs are expected to have a significant impact in the enterprise.

Private 5G LAN Advantages

Owning and operating a private 5G LAN comes with several advantages across a host of use-case scenarios. These advantages include:

Speed of deployment – Celona 5G LANs can be installed and deployed in a manner of hours as opposed to days or weeks using incumbent cellular equipment providers. Because 5G LANs are designed as a turnkey system with all the requisite components optimized as a single system, the 5G LAN deployment process effectively mirrors traditional enterprise Wi-Fi LANs, using a framework very familiar to IT staff.

Wider coverage area – Because 5G LAN access points can transmit signal and antenna gains at higher levels compared to alternative technologies such as Wi-Fi, for critical use cases we will discuss later in this paper, far fewer APs are required to cover the same area next to the existing enterprise Wi-Fi network.

Deterministic connectivity – Apps that require real-time response from the network infrastructure and associated data flows that require low packet loss / delay and predictable bandwidth need a transport medium that can identify these flows and prioritize them using strict service level objectives. Deterministic network capabilities that offer this type of functionality are built-in to 5G LANs.

Data security – MSP-managed or in-house management of a private 5G LAN gives enterprises complete control and visibility over the network that transports sensitive business data. Given certain data privacy and compliance requirements within an enterprise organization, this is a must-have. For others, it lessens the risk of data loss or theft due to third-party ownership and control over the wireless transport medium.

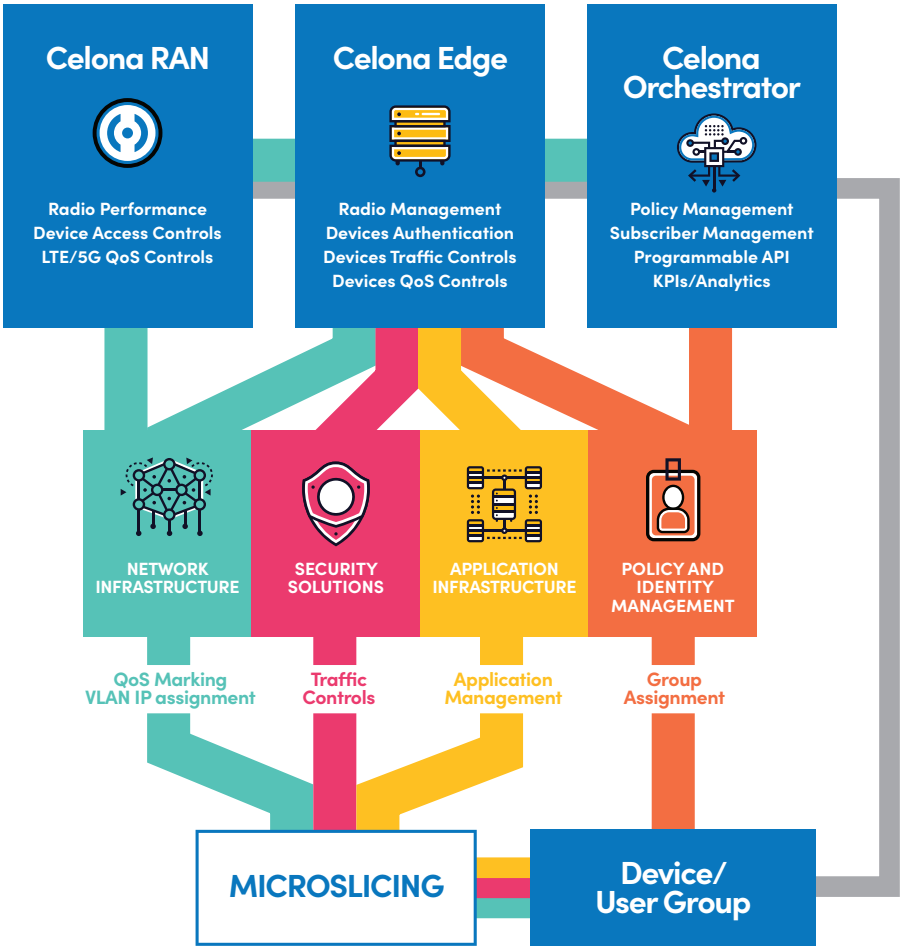
Granular quality of service (QoS) for critical apps – To get the utmost in granular performance controls all the way down to the application and workload level, a private 5G LAN is the best choice. Celona's patented MicroSlicing™ technology allows network administrators and managed service providers create per-application slices that adhere to strict service level objectives for latency, packet loss and throughput.

Simplified administration – The device onboarding process is far easier with a 5G LAN since access control and authorization is built directly into cellular SIM cards, deployed as physical SIMs and eSIMs. Thus, administrators can reduce the time it takes to provision devices and onboard users. End users do not have to select any specific SSIDs or worry about the network settings on the device they are using device group and role based network access are managed centrally by the network administrators and/or managed service providers.

Cost savings – Celona 5G LANs have been designed to be delivered at a cost that rivals conventional private cellular networks, promising up to 6x cost savings. If a private 5G LAN is part of an organization's long-term network connectivity strategy, building and operating one in-house will be the lower cost option. This is evident when alternative solutions continue to price their offers using a per-user or throughput-metered structure.

The Celona 5G LAN Solution

Celona's integrated 5G LAN platform includes all the essential elements including access points, LTE/5G core network edge hardware/software and cloud-based orchestration tools specifically designed and developed for enterprise network use-cases. As opposed to traditional solutions, a private 5G LAN allows for enterprises to have full control over company data with a predictable long-term cost structure. The following diagram highlights each element within Celona's 5G LAN platform:



The components that make up a Celona RAN include enterprise-optimized **Celona indoor/outdoor access points (APs)** that operate in private cellular spectrum, **Celona Edge** software as the extension of the Celona platform integrated to existing enterprise network infrastructures, the cloud-managed **Celona Orchestrator** and physical SIM or embedded SIM (eSIM) cards. Access points are designed for zero touch deployments, are application-aware across the wireless medium using Celona's MicroSlicing technology and offer a reliable and interference-free wireless experience.

The Celona Edge element of the overall Celona integrated platform is the private mobile core and control plane for the software-defined RAN. All data as directed through the edge platform – allowing for complete control and visibility of the data flows traversing the RAN and to allow for the application of various network services.

The Celona Edge acts as the gateway connecting the LTE/5G cellular wireless to corporate LAN resources. Support for NAT, static/dynamic routing and VLAN connectivity are possible in its ability to integrate with existing IP domains and enterprise network traffic forwarding requirements. Deployable either on-premises or within a public or private edge/cloud, the Celona Edge performs the following data-plane functions:

- Cellular radio spectrum management and data plane services for Celona APs
- Application performance and telemetry metric data collection
- User/device access control and data security

Finally, the Celona Orchestrator is responsible for the centralized control of:

- Celona AP and Celona Edge auto-provisioning, ongoing management
- User equipment (UE) onboarding, offboarding, device grouping via SIM provisioning
- Celona MicroSlicing policy creation and management for app QoS and service levels
- Cellular wireless visibility and monitoring of real-time performance against MicroSlicing policies

Going Edgeless with 5G LANs

One of the biggest questions on the minds of prospective Celona 5G LAN customers deals with how cellular wireless resources can be integrated within an existing network infrastructure from a physical and logical perspective.

Celona's Edgeless Enterprise architecture provides flexible deployment options for enterprises to easily deploy and operated 5G LAN control functions within a common mobile edge compute environment. This allows for 5G LAN network services to be centralized and placed closer to vital enterprise applications within the same compute environment already in place. You can see Celona's Edgeless architecture white paper for more details.

Below is an overview the Celona 5G LAN operation and how the integration process works:

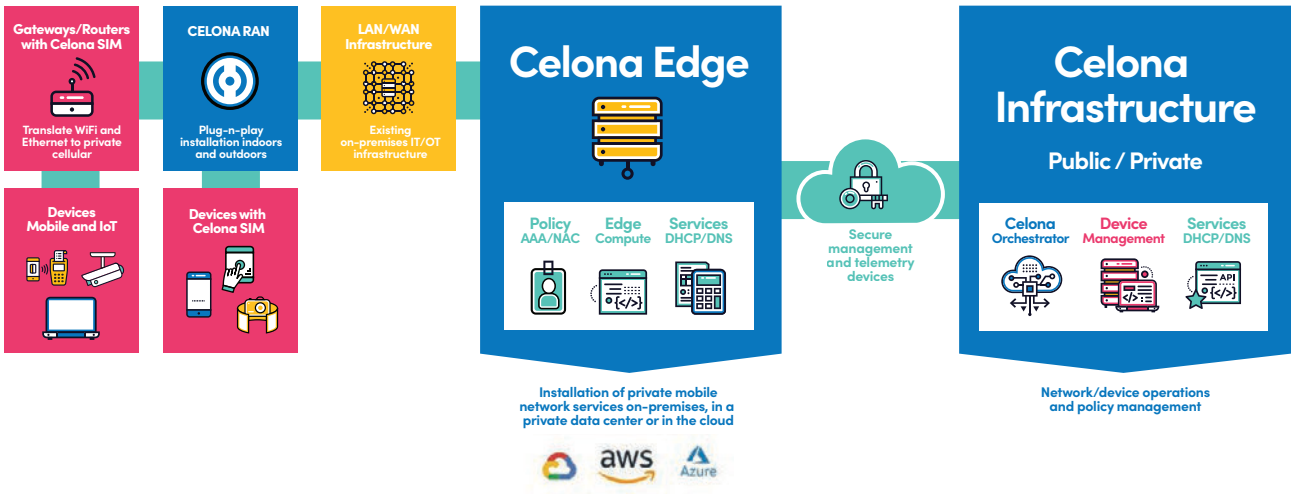


FIGURE ABOVE: Celona 5G LAN Overlay Deployment Model

Celona APs attach directly to any Layer 2/3 wired enterprise network using standard PoE from a midspan or PoE switch. Standard AC adapters are also an option. Once activated for operation on the desired network through Celona Orchestrator, Celona APs automatically "phone home" for their configuration over encrypted tunnels to the Celona Edge, a full, cloud-native 4G/5G software stack developed specifically for enterprise use.

The Celona Edge then assigns each Celona AP with the optimal spectrum allocation, channel assignments and power levels required for ideal operation (e.g., as specified by the authorized CBRS SAS in the United States).

All AP traffic then runs through the Celona Edge where vital enterprise network services such as encryption, network address translation, static or dynamic routing and advanced, service level and QoS enforcement are applied.

Once up and running, compatible cellular devices with the enterprise sanctioned physical SIM or eSIM automatically connect to the Celona 5G LAN just like any cellular device. Information contained within the SIM/eSIM is used for secure authentication. SIM provisioning across a 5G LAN can be done through the Celona Orchestrator. This eliminates the need for configuring user passwords or certificates on client devices. For non-SIM supported devices, CBRS gateways are used to translate cellular signals to Wi-Fi or Ethernet.

For traffic optimization, Celona MicroSlicing technology is used to uniquely automate end to end QoS enforcement of wireless traffic on a per application or device group basis. Within the Celona Orchestrator, administrators simply specify the applications or devices requiring strict QoS handling. Up to nine MicroSlicing policies can be configured to automatically control latency, packet loss and throughput metrics on the cellular wireless medium – for any application mix or device group. These MicroSlicing policies can then be converted to IP DSCP QoS assignments to enable enforcement once the data leaves the Celona 5G LAN and traverses the corporate network.

The following diagram shows the Celona 5G LAN components from an integration perspective:

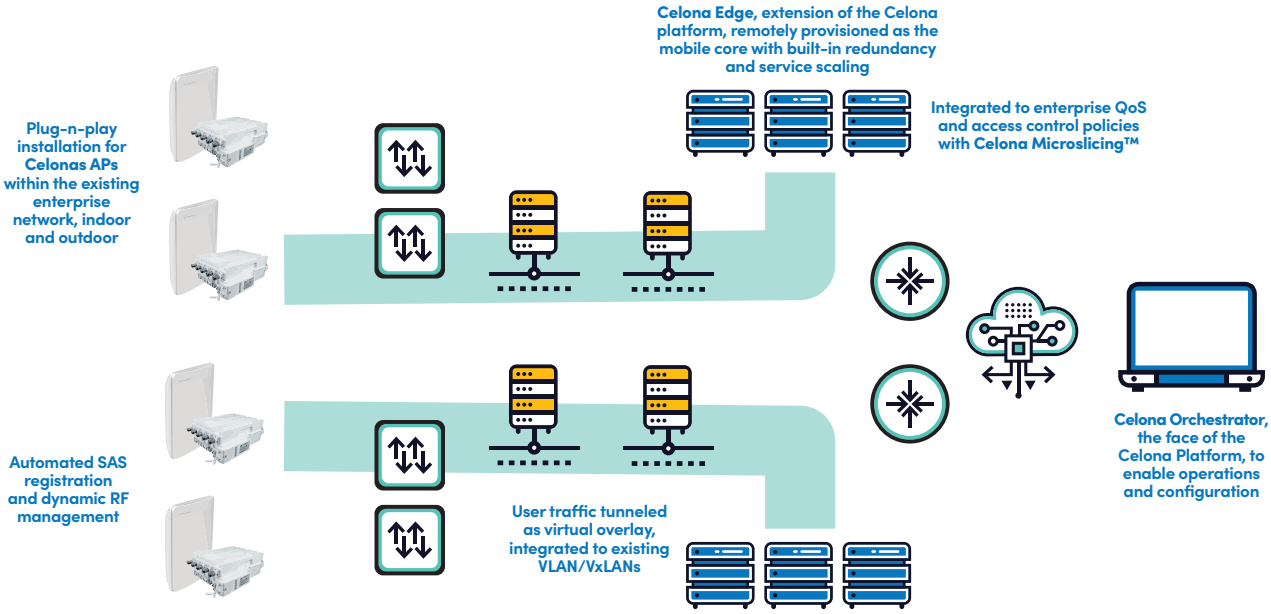


FIGURE ABOVE: Celona 4G/5G integration with existing enterprise infrastructure

5G LAN QoS with MicroSlicing

Quality of Service (QoS) is a generic term used to describe how networks can identify, categorize, and apply priorities to data flows. Within a Celona 5G LAN, QoS policies can be created for a mix of applications across different device groups using Celona's patented MicroSlicing technology.

There is no need to manually touch client devices for MicroSlicing policies to be applied, and the policies can be changed in real-time as application and device mixes within a Celona 5G LAN evolve over time.

A MicroSlicing policy is defined as a set of network functions within the Celona 5G LAN that form an end-to-end logical policy fabric. A single policy can be configured to meet an application's network performance requirements with service level objectives on flow priority, packet delay budget (aka. latency), packet error rate (PER) and bandwidth.

The control plane of a Celona 5G LAN continuously monitors and adjusts traffic transmissions to meet such service level objectives. These processes and functions guarantee deterministic performance of critical enterprise applications when on private cellular – in addition to ensuring that QoS rules for higher-priority traffic over lower-priority flows are enforced in real-time.

Accordingly, within the Celona 5G LAN, in addition to simply prioritizing one traffic flow over the other, each traffic flow is monitored for latency, error rate and throughput within the Celona Orchestrator – on device group and application basis. Here is a quick summary of each:

Device groups – Administrators can group cellular wireless endpoints via their SIM identities into specific groups and logically segment them by device type or use case. In many scenarios, the type of device often dictates what apps/services are being operated on a regular basis. This helps to coordinate which devices are assigned which MicroSlicing policy.

Applications – Applications can be configured based on server IP / subnet mask and start/end ports. Once defined, the application flows are identified by the Celona platform in real-time as client devices connect. Once a combination of device groups and application types are married to specific MicroSlicing policy, service level objectives are enforced.

QoS policies can also be maintained when transporting data between the Celona network and the corporate LAN. Each MicroSlicing policy within the Celona 5G LAN can be assigned with dedicated DSCP markings to translate cellular wireless service level requirements to traditional QoS enforcement on the enterprise network. QoS policy can then be created around these DSCP tags on the wired network to provide preferential treatment to mission-critical application flows using queuing, forwarding and discarding mechanisms such as traffic shaping or traffic policing.

Celona's platform has been designed with enterprise administrators in mind. From an IT operations standpoint, Celona has taken great care to help enterprise network operations, cybersecurity and service delivery teams feel comfortable configuring and monitoring a private cellular wireless infrastructure. Taking cues from popular cloud-managed enterprise wired, SD-WAN and Wi-Fi solutions, concepts found in Celona's operational model will prove to be similar and accessible by administrators from different parts of the IT organization.

For more detailed information on Celona MicroSlicing, please see our whitepaper on the topic: https://www.celona.io/resources/celona-microslicing-whitepaper.

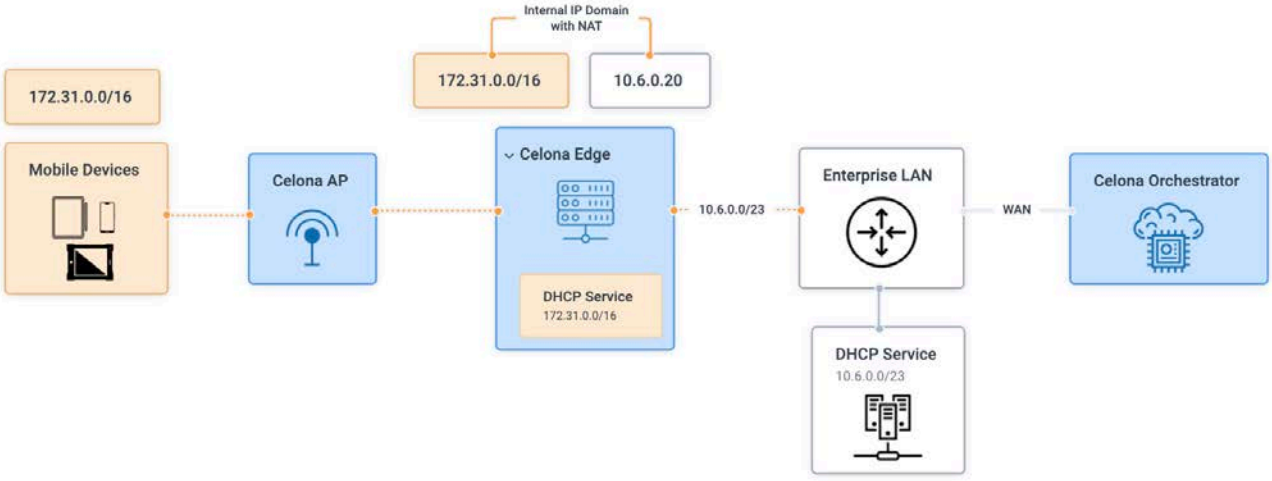
5G LAN Routing

A Celona network can be integrated with the existing corporate LAN using one of two IP Domain configuration modes:

Internal IP Domain (NAT)

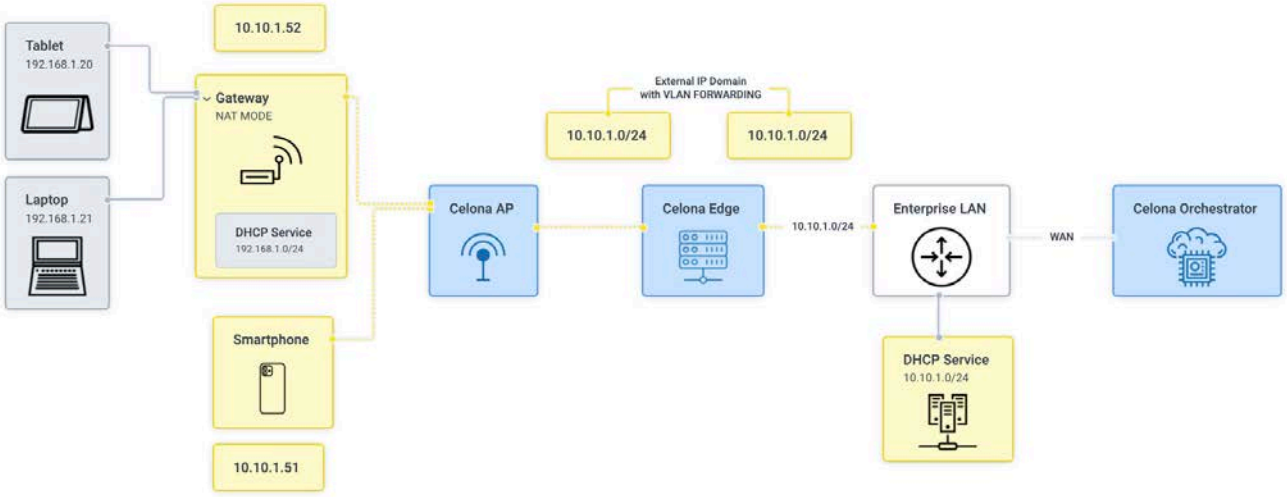
The default IP domain option is set to Internal mode. This means that the Celona Edge platform acts as a network address translation (NAT) gateway in a similar fashion that a traditional router or layer 3 switch translates internal IP addresses to one or more external IP addresses. All devices connected to the Celona 5G LAN receive their IP addresses through an internal DHCP service and shares the same DNS settings as the Celona Edge.

Keep in mind, however, that in NAT mode, 5G LAN endpoints sitting behind the NAT gateway will not be accessible from devices on the outside of the NAT gateway. If traffic must be initiated from the corporate LAN into the RAN, you must use the External IP Domain mode. The following diagram shows an example Celona RAN connecting to an Enterprise LAN while in Internal IP Domain mode:



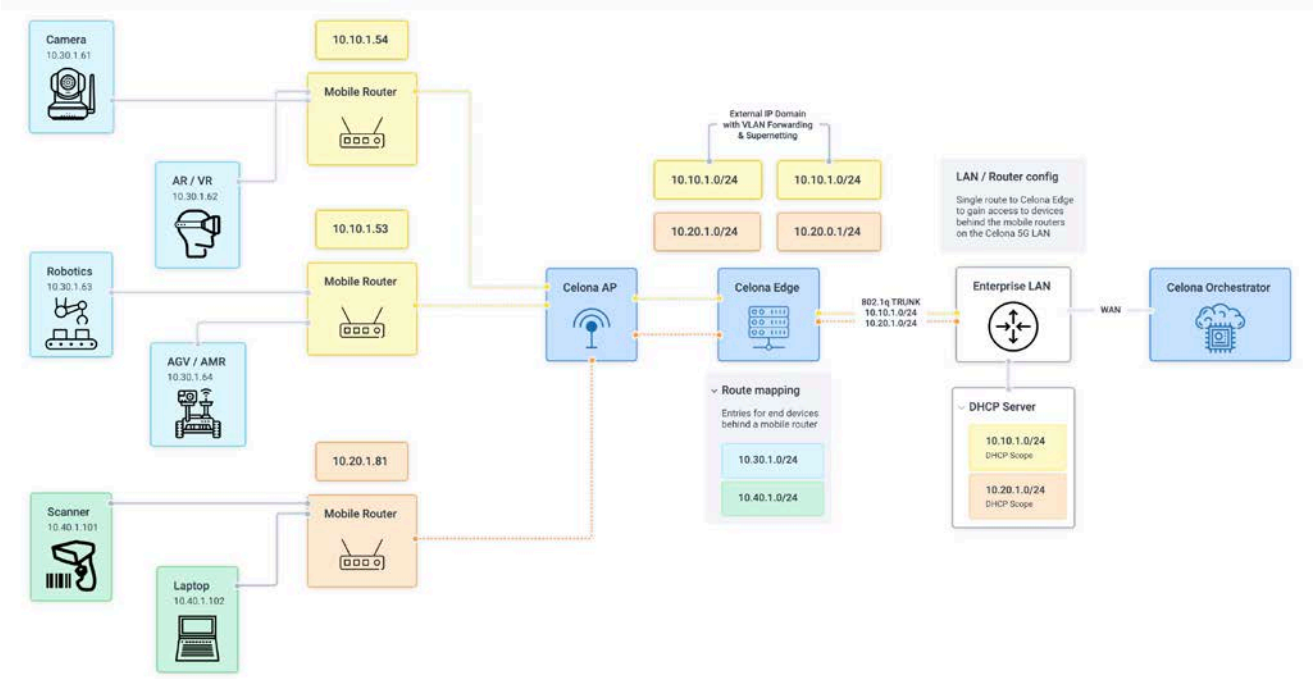
External IP Domain

With the External IP Domain, the network interface on the Celona Edge attaches itself to multiple IP subnets that are already configured on the corporate LAN. In this configuration, DHCP and DNS servers within the enterprise network are utilized to enable IP connectivity for the client devices connected to a Celona network. Celona Edge simply acts as a translator between cellular wireless and existing VLANs assigned to different device groups. This diagram shows how Celona 5G LAN can forward existing IP domains to private cellular wireless:



Finally, for devices that do not natively support private cellular connectivity, mobile routers need to be used to enable end to end connectivity. For these configurations, a Celona 5G LAN external IP domain can be configured with supernetting to provide visibility to such endpoints from the enterprise LAN.

To enable this unique capability, the Celona Edge maintains a list of IP subnets that map to the ones used by the endpoints behind the mobile routers. In the following diagram, we highlight how such endpoints can be made fully visible from devices residing on the Enterprise LAN. This unique capability is instrumental in enabling remote control of video camera, mobile robotics and other mission critical IoT infrastructure. In addition, endpoint management tools can then be used to identify and track devices and apply device policies just like any other parts of the network.



For more detailed information on Celona 5G LAN Routing, please see our whitepaper on the topic: [https://www.celona.io/resources/celona-5g-lan-routing-whitepaper.](https://www.celona.io/resources/celona-5g-lan-routing-whitepaper)

5G LAN Security

5G LANs offer clear benefits over alternative wireless solutions. Data security is one area where clear advantages can be seen. Unlike Wi-Fi security which has evolved over time, which introduces the chance of insecure misconfigurations, only the latest and best security mechanisms are built directly into the cellular wireless 4G LTE and 5G connectivity. Thus, network administrators do not have to concern themselves with the thought of accidently deploying a wireless network using inferior authentication and encryption mechanisms.

Reaching the level of authentication, authorization, and encryption that a private 5G LAN provides highest levels of enterprise wireless security. The use and management of X.509 public key certificates are not required as proof of endpoint identity as this process within the Celona 5G LAN is handled with the identification information contained within the SIM card assigned to a specific device. There is no SSID or network name or network password for the end user or the network administrator needs to provision – and the policies of when, where, how that specific SIM card could be provided network access can be defined via software, in real-time, based on logical policies.

User/device authentication and access control within a 5G LAN are designed to adhere to zero trust philosophies and frameworks. Of course, device identification and authentication are two key tenants of zero trust principles. With the use of physical or digital SIM cards that secure store subscriber identities, devices without the proper SIM identification information will never be able to join the 5G LAN.

Additionally, zero trust philosophies can be applied to administrative tasks. For example, the latest secure privileged access technologies can be used for administrative authentication purposes. This includes Security Assertion Markup Language (SAML) which can be seamlessly integrated across private 5G LANs for the purpose of centralizing and securing privileged management access.

Celona also allows for Application Programming Interface (API) access for external control/monitoring using third-party tools. Relevant security telemetry data can be collected for security analysis purposes.

Finally, application flows can be placed into secure Celona MicroSlicing policies where each device group and application mix per policy can be safely isolated from all other traffic traversing the 5G LAN.

For additional details on how 5G LANs can help improve enterprise wireless security for a new generation of critical applications and how it can positively contribute to the zero trust strategies implemented within enterprises, please see our whitepaper on the topic: https://www.celona.io/resources/celona-5g-lan-security-whitepaper.

5G LAN Device Ecosystem

Wireless networks utilizing the private cellular spectrum, like CBRS in the US, is growing significantly now that most cellular wireless capable smartphones, laptops, tablets, handhelds (and even robotics) natively support the spectrum. Additionally, according to a recent SNS Telecom and IT report, by 2023, 90% of all smartphones shipped in the US will have native CBRS band compatibility. For additional details, please see our detailed list of private LTE/5G capable devices in the market.

For devices that do not support native CBRS bands – only Ethernet or Wi-Fi – there are several options available including cellular-capable USB adapters, portable cellular gateways and hotspots that connect one or more devices via Ethernet or Wi-Fi while using private 5G for backhaul transport.

5G LAN Use-Cases

Several key technical reasons set a private 5G LAN apart from alternative connectivity options, including:

- Improved coverage and signal range
- Predictable throughput and latency
- Reliable AP roaming/handoffs
- Less external wireless interference

Based on these technical advantages, use-cases can be found in the following business verticals:

- Higher education
- Public safety, utilities, transportation hubs, oil & gas and mining
- Warehouses and logistics centers
- Manufacturing plants
- Hospitals and healthcare facilities
- Retail chains
- Sports/entertainment venues
- Hotels/hospitality
- Agriculture/farming

VERTICAL	USE CASES	5G LAN BENEFIT
Manufacturing	Industrial IoT Mobile Robots Automated guided vehicles Computer vision Video surveillance	Uninterrupted mobility Improved up time for process digitization Capital cost reduction with fewer APs Lower latency device connectivity Deterministic wireless coverage
Logistics	Vehicle connectivity Inventory scanners Push-to-talk comms	Reliable in-vehicle connectivity Nonstop mobility Latency sensitive wireless remote control Very large area coverage per radio
Higher Education	Backhaul for remote Wi-Fi hotspots Community access Public safety	Reduce/eliminate additional cabling Simplified extension of campus network to community Outdoor wireless backhaul enables temporary locations
Healthcare	Clinical voice In-building cellular Wireless telemetry On demand clinics	Seamless mobility Lower latency, higher quality voice calls Improved cellular coverage Infrastructure-controlled mobility Outdoor wireless backhaul enables temporary locations
Stadiums	PoS systems Cellular coverage On field systems Video surveillance	Reliable in-vehicle connectivity Nonstop mobility Latency sensitive wireless remote control
Hospitality	Environmental controls Outdoor wireless extension PoS systems Video surveillance	Clean spectrum with CBRS Reliable connectivity for service staff Predictable performance for vital business apps Fewer APs cover entire property

5G LANs for Neutral Host Networking

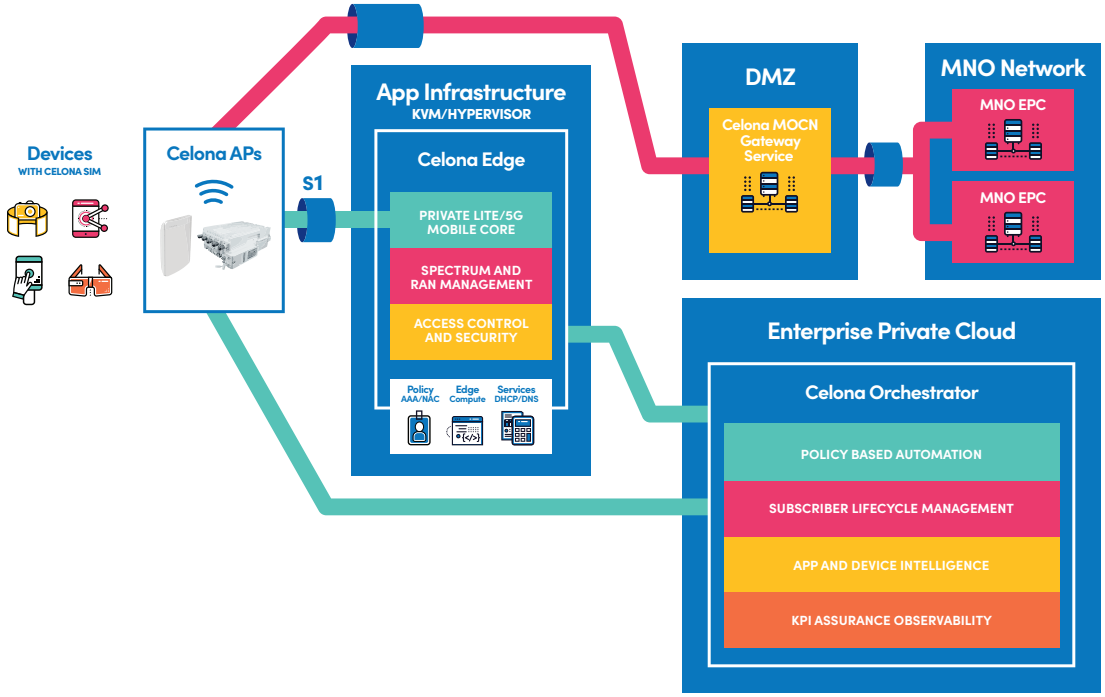
One of the most compelling and popular applications for a private cellular network is its future use to also onboard "guest users" and improve in-building cellular signal coverage for public MNO (Mobile Network Operator) subscribers.

Commonly referred to as neutral host networking (NHN), this modern approach distributes public cellular MNO voice and data services via the use of a private LTE/5G wireless infrastructure. The private cellular network can broadcast third-party carrier identity to users that have access to such carrier's network and deliver great value:

- Eliminate the use of expensive Distributed Antenna Systems (DAS) across the enterprise facility to improve indoor public cellular coverage,
- Prevent the need for expensive RF designs to extend public carrier licensed spectrum to indoor locations, and
- Eliminate the need for reserving bandwidth from nearby base stations of public carrier networks by simply offloading traffic flows to private cellular spectrum (such as CBRS in the US).

The role of an NHN is to leverage existing enterprise network resources, including the Celona 5G LAN infrastructure, to propagate public 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 radio network. Public cellular carriers 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 cellular wireless network. Doing so provides wireless connectivity to a wide range of public carrier 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.

For a more in-depth look at Neutral Host, take a look at our whitepaper on the topic: https://www.celona.io/resources/celona-neutral-host-network-primer-for-network-admins

Enterprise Purchase Criteria for 5G LANs

There are two phases that most enterprise IT decision makers will undertake within their 5G LAN decision making process. The first is to vet whether private cellular is the right technology for their use-cases and application performance requirements on enterprise wireless.

From this standpoint, following questions are common:

- Will 5G be more stable and reliable than alternative options?
- Can a 5G LAN solve my problems with highly mobile devices?
- Is a 5G LAN offer increased security for my needs?
- Do I have deterministic performance requirements for applications?
- Will I have full control over my data and traffic flows in the network?
- Will a private 5G LAN be cost-effective?

Once the decision has been made to invest in a 5G LAN platform, the next question will likely be, why Celona?

1. Celona is unique in its ability to offer an accessible, end-to-end solution that was built for enterprise environments and to be managed by administrators with enterprise IT operations skillset. Taking advantage of cloud networking principles that are now common across enterprise networks, it enables centralized automation and orchestration of complex infrastructure configuration – enabling deployment at scale and faster than any other solution in the market.
2. By taking advantage of Celona's 5G LAN operating system (OS), enterprise IT administrators can directly translate existing network configuration for IP domains, endpoint VLANs, DHCP/DNS service, firewall policies and QoS rules to cellular wireless infrastructure. By using well defined layer 2 and layer 3 network configuration options, cellular clients can be truly made part of the enterprise network instead of being treated as a separate island. As a result, enterprises can maintain flexible data privacy and security rules and translate them directly to new generation of mission critical applications that are supported by a Celona 5G LAN.
3. Last but not least, via the patented MicroSlicing technology, a Celona 5G LAN can enforce QoS priority and service level objectives (bandwidth, latency, packet error rate) on any application and device mix supported by cellular wireless connectivity. Instead of manually configuring each device on the network in order to enforce such granular performance requirements, administrators can update, create and enforce MicroSlicing policies as use cases evolve within the enterprise. This provides administrators the freedom to utilize the same network infrastructure for many applications, across different generation of connected devices, and across different sites within the same enterprise organization – significantly improving the return-on-investment (RoI) recognized and reducing the total cost of ownership (TCO).

SEE THE CELONA TECHNOLOGY IN ACTION

Request a free trial and custom product demonstrations by visiting us at celona.io/journey.

hello@celona.io | celona.io