Pipeline | Volume 17 | Issue 10
Pipeline
UNLOCKING AGILITY WITH ETSI
POWERING AGILITY WITH CLOUD
ENTERPRISE COLLABORATION & TRANSFORMATION
CROWDSOURCING+ AIOPS
COMBINING BPA AND UCC
3D AI WITH AR & VR
REGIONAL CLOUDS
O-RAN AND STANDALONE PRIVATE 5G
NEXT-GEN B/OSS & NEXT-GEN NETWORKS
AGILITY

www.pipelinepub.com
Volume 17, Issue 10

Standalone and the 5G Private Network Opportunity

By: Ankur Sharma

There has been a lot written on the coming Industry 4.0 transformation and how 5G will spur new opportunities and innovation. Much of the focus has been on a variety of use cases such as increasing enterprises' quality of service requirements, enhancing mobile-broadband experiences or delivering superior resource utilization and sufficient bandwidth to handle massive machine-type communications. 5G networks with enabled slicing, new models of private networks and the use of licensed and unlicensed spectrum options are exciting, yet they also have challenging issues that need to be addressed.

The most important 5G use case today is enhanced mobile broadband (eMBB) and it is drawing major interest from mobile network operators (MNOs). Extending LTE-Advanced's use cases of consumer-to-consumer (C2C) or business-to-business (B2B), the 5G era is focused on revenue-generating use cases in B2B2B, B2B2C and many more.

To get there, 5G must be software-controlled, simplify processes and be capable of being deployed quickly. It must be provisioned with Industry 4.0-grade security but still meet service level agreements (SLAs) and performance requirements. The challenge is to define and provide a network architecture that can be adapted to support many different types of consumer, business and industry use cases that have large ecosystems of heterogeneous devices, while also effectively increasing the return on investment (ROI) and reducing the total cost of ownership (TCO).

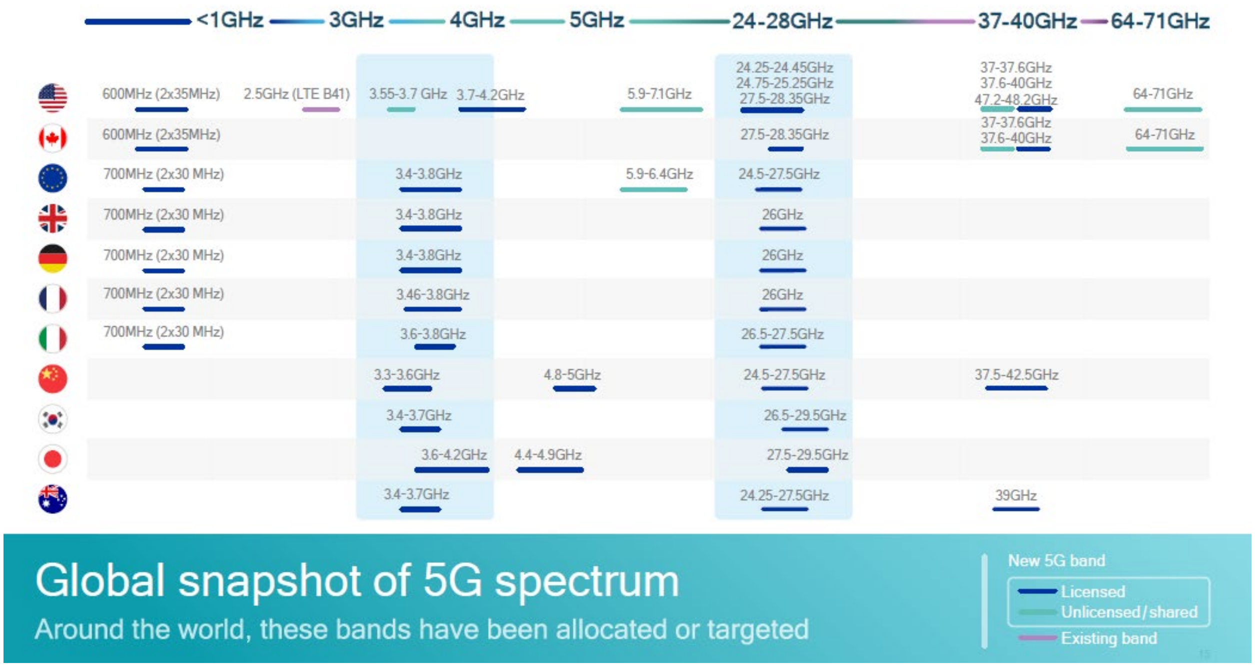
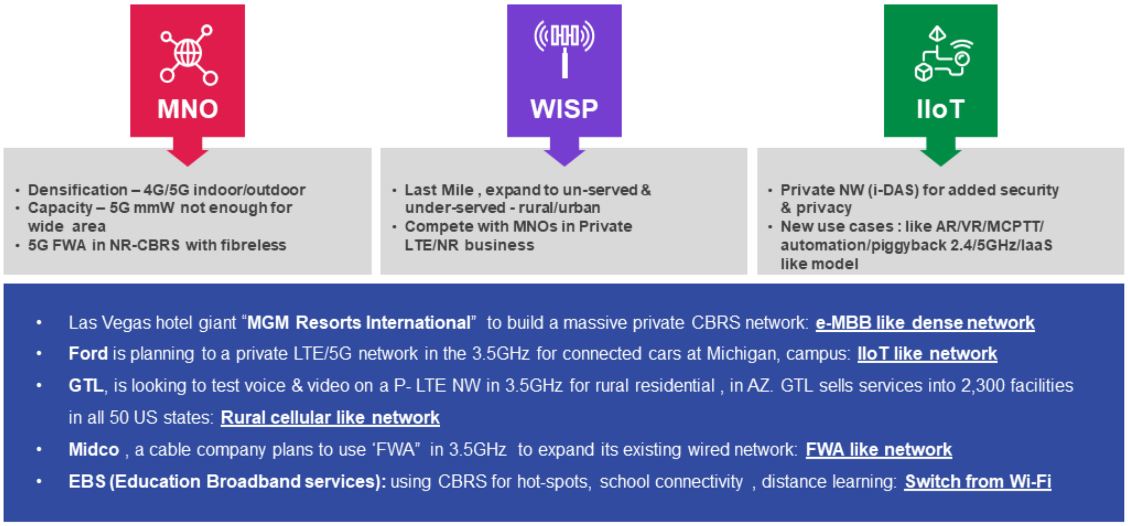


Figure 1: Global 5G spectrum snapshot. Source: everythingRF
click to enlarge

The private network challenge

Recently, ABI Research issued a report noting that private network deployments are expected to generate revenue of over $64 billion by 2030. Much work has been done to establish the standards and lay the groundwork for how private networks can be operated. However, at this stage, the reality is that the ability to deploy a private network remains cost-prohibitive for the majority of enterprises today. Specifically, enterprises face two significant challenges: the overall cost of radio access network (RAN) equipment and maintenance and the cost of spectrum licensing.

Thankfully, these challenges are being addressed. The first by a growing ecosystem of open telecom vendors developing a number of interoperable solutions, including Open RAN, that provide best-of-breed selection and greater flexibility for network design and deployment. The second is being addressed by governments with regard to spectrum. This includes spectrum in the US's Citizens Broadband Radio Service (CBRS) spectrum (150 MHz: 3550 MHz-3700 MHz) and recent government decisions to make additional spectrum available (3450-3550 MHz). It also includes unlicensed spectrum options like 5 GHz and 6 GHz and dedicated locally licensed spectrum options being made available by governments in the UK and Germany. This attracts more business players (see Figure 2 on page three), each with their individual interests and capabilities.



MNO

- Densification – 4G/5G indoor/outdoor
- Capacity – 5G mmW not enough for wide area
- 5G FWA in NR-CBRS with fibreless

WISP

- Last Mile , expand to un-served & under-served - rural/urban
- Compete with MNOs in Private LTE/NR business

IIoT

- Private NW (i-DAS) for added security & privacy
- New use cases : like AR/VR/MCPTT/ automation/piggyback 2.4/5GHz/IaaS like model

- Las Vegas hotel giant "**MGM Resorts International**" to build a massive private CBRS network: **e-MBB like dense network**
- **Ford** is planning to a private LTE/5G network in the 3.5GHz for connected cars at Michigan, campus: **IIoT like network**
- **GTL**, is looking to test voice & video on a P- LTE NW in 3.5GHz for rural residential , in AZ. GTL sells services into 2,300 facilities in all 50 US states: **Rural cellular like network**
- **Midco** , a cable company plans to use 'FWA" in 3.5GHz to expand its existing wired network: **FWA like network**
- **EBS (Education Broadband services):** using CBRS for hot-spots, school connectivity , distance learning: **Switch from Wi-Fi**

Figure 2: 5G business players
click to enlarge

As these examples indicate, cellular service with premium quality of service is now no longer dependent on the larger nationwide mobile operators. Instead, small players like local wireless Internet service providers (WISPs) and others could deploy their own CBRS network and then work to attract a larger known telecom partner to share spectrum costs through a roaming partnership. In this scenario, the business case for a private network would be feasible, but which private network model should they deploy? We will look at the options, including Open RAN, that are available to enterprises in the rest of this article.

Non-public networks

3GPP, the industry organization that oversees the development of cellular telecommunications technology specifications, issued Release 16, which introduced the first new architectural model to address such demand in private 5G: the non-public network (NPN). There are two NPN deployment types as defined in 3GPP TS 23.501 V16.3.0/TS 22.261:

- Public Network Integrated Non-Public Network (PNI-NPN)
- Stand-alone Non-Public Network (SNPN)

PNI-NPN is deployed in association with a public land mobile network (PLMN)/3GPP-based network. Nationwide mobile operators prefer this option so that their indoor solutions can have seamless and lossless session transfers to and from their macro-centric network. WISPs or local providers may adopt PNI-NPN (requires service level agreement with nationwide mobile operators) for dynamic services like telematics, asset tracking, and more.

On the other hand, SNPN is designed for a fully independent entity and does not rely on PLMN/3GPP-based networks. This option is most favorable for WISPs in Industrial IoT, local school districts, small to medium businesses and more. There is a limitation here, however; E911 services, roaming, mobility among SNPNs or between SNPN or PNI-NPN are not supported. Such networks can be identified by the combination of a PLMN ID and network identifier (NID – optional information in a human-readable network name). A 5G RAN can support broadcasting up to twelve NIDs.

SNPN Deployment Models

There are two SNPN deployment models that can be considered: a non-shared form of SNPN and a shared infrastructure model of SNPN.

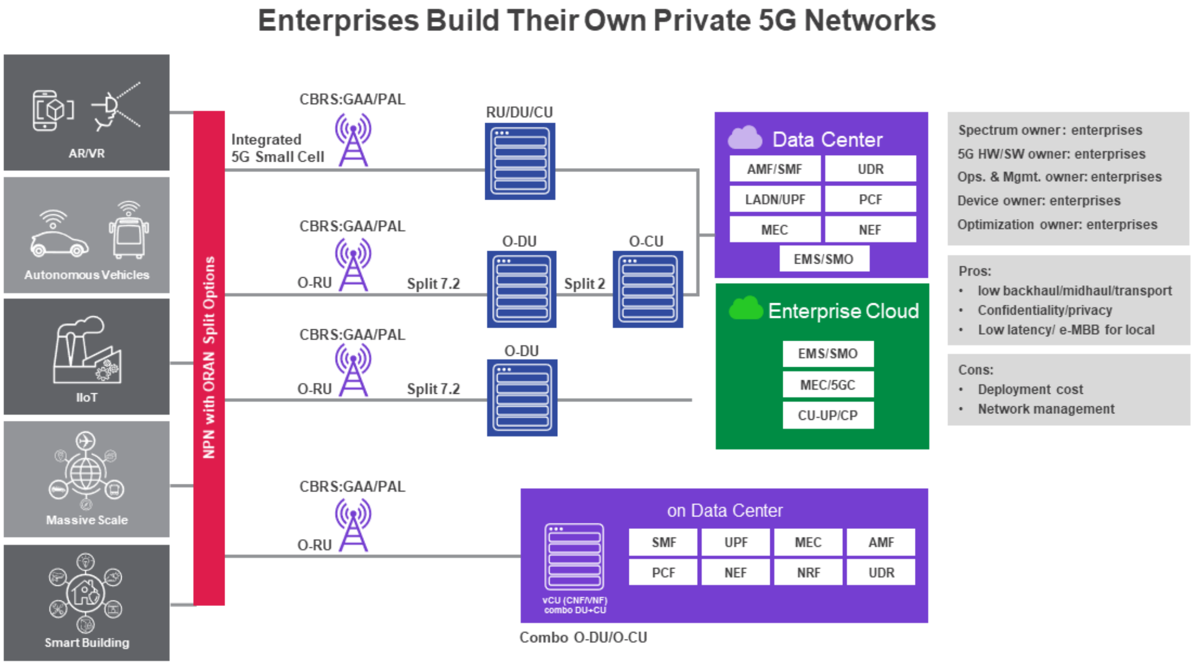


Figure 3: Enterprises building private 5G networks
click to enlarge

Non-shared form of SNPN: in this deployment model, enterprises use their own infrastructure-like CBRS unlicensed spectrum and their own hardware and software for all network functions (RAN, core, gateway, and edge processors) within their premises. Service providers' new radio (NR)-RAN/5GC will be configured with a combination of PLMN ID and NID to uniquely identify their device.

To maintain confidentiality and low latency, enterprises prefer to have analytics and processors at the far edge, and local user plane function (UPF) on-premises or local area data networking (LADN) topology. However, each network node's placement in anetwork needs some architectural changes on the device side as well as on the core side. A simplified non-shared SNPN design must have a configured user equipment (UE). The access mobility function (AMF) provides information of mobile edge, local UPF, and LADN servers during initial registration to the UE that explicitly requests a PDU session to a special access point network (APN).

The benefits of this design are security and privacy control for user data, such as security camera footage or videoconferencing sessions, which stays within a private enterprise network.

Shared infrastructure model of SNPN: in this deployment model (see Figure 4), the enterprises lack the most demanded and reliable licensed RF spectrum (FDD) for high penetration and propagation, though they may still want to use NR-U (TDD-CBRS) for user plane and capacity-centric applications. Hence a shared NR-RAN concept can be considered here. This concept assumes the enterprise and an MNO agree to various resource-sharing mechanisms (either RAN sharing [MORAN/MOCN], 5GC sharing, or both).

A RAN sharing model can be deployed in many ways: Unlicensed TDD with the MNO's FDD in carrier aggregation or dual connectivity mode such as CBRS + licensed FDD, licensed C-band + shared FDD, and mmWave + licensed FDD. There can be other combinations like unlicensed TDD, licensed TDD, carrier aggregation, and dual connectivity modes such as CBRS + C-band or mmWave + CBRS-band. 3GPP's Release 15/16 has advanced 5G features that enterprises can leverage as a complementary overlay of an MNO's FDD low band (<2GHz) to extend the downlink coverage and split off the uplink to FDD like in "supplement uplink" (SUL). On the other hand, MNOs benefit by extending their indoor coverage without additional cost. Mobility management, quality of service (QoS), and session transfer all depend on this mutual effort and interface connectivity.

Multiple topologies can be considered when SNPN is deployed in a shared infrastructure. This includes having a RAN/5GC (DU/CU-UP/LADN) user plane on-premises that belongs to the enterprise, while a control plane resides in an MNO's data center. This approach is useful for reducing user plane latency while improving user plane privacy. Conversely, enterprises can also let MNOs deploy everything on-premises for the MNO's users that are on the enterprise's property. This can be an expensive approach, but it suits certain providers such as hospitals or healthcare providers that prefer to keep user profiles— along with the control plane and the user plane—confidential.

But such shared deployments bring more challenges. Enterprises and MNOs need to consider the regulatory aspects and interference challenges associated with unlicensed spectrum (CBRS or NR-U), authorization of licensed spectrum operations from national regulators, and the interworking requirements with an MNO's network. Additionally, consideration must be given to the privacy, network security, net neutrality and isolation needs of the enterprise's SNPN assets and users.

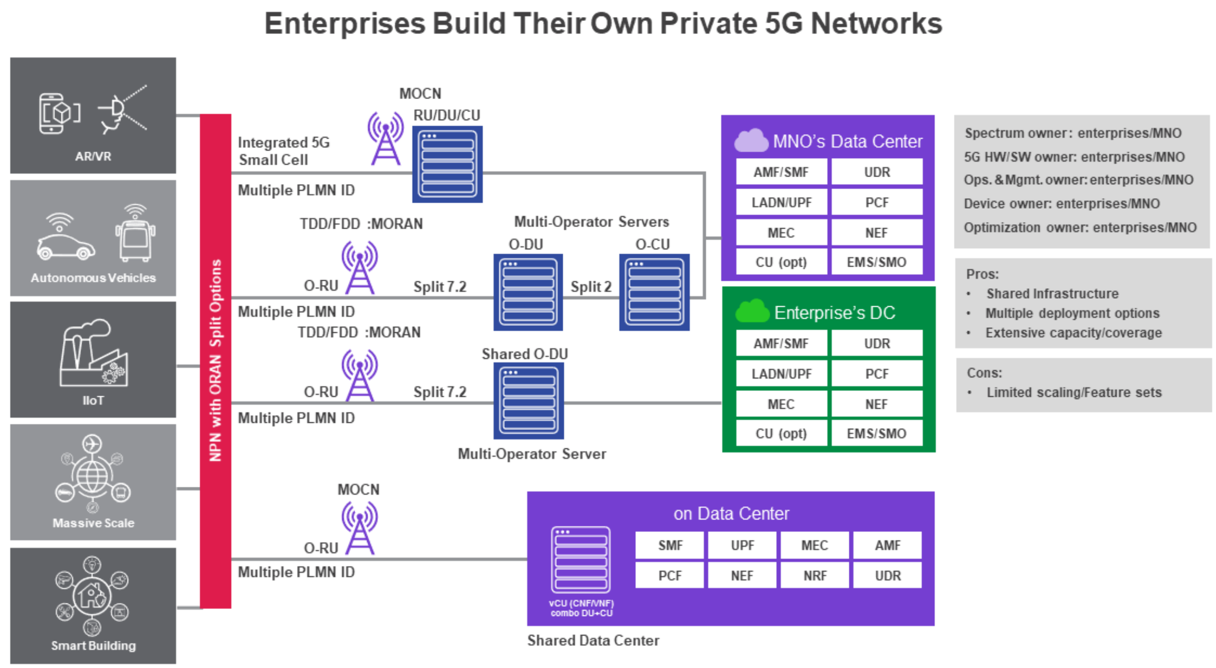


Figure 4: Shared infrastructure model of SNPN
click to enlarge

PNI-NPN Deployment Models

As explained earlier, an NPN model (private 5G), when associated with a nationwide MNO network through pre-defined network interfaces, is known as the PNI-NPN model. Compatible user equipment (UE) can accommodate all services not limited to mobility, session transfer or voice with multi-data connections from both networks, based on its location. UE credentials and subscriptions are available at common databases owned by the MNO. As a result, subscriber confidentiality is challenged. A key differentiation is that PNI-NPN models provide more advanced features like network slicing, larger coverage areas and multi-services scenarios as compared to an SNPN model where both domestic inbound and outbound roaming are assumed to be supported.A PNI-NPN model can follow the SNPN design to meet latency and user plane privacy when deployed, offering a simplified approach and lower maintenance costs for enterprises. Based on the service level agreement, multiple models can be considered:

Shared RAN/Shared core: CBRS or NR-U in association with an MNO's mmWave/FDD spectrum in premises with private user plane (UPF) for enterprises (like LADN design). This model provides the benefits of user traffic privacy, extended coverage, and a massive capacity-centric approach.

Private RAN with shared core: NR-U deployed and managed by enterprises but shares an MNO's 5G core for both control and user plane. The benefit of this model for enterprises is a low-cost RAN with NR-U only and extended mobility support. However, there is a trade-off in user data and traffic privacy. An MNO benefits from extended indoor coverage for its subscribers.

Private RAN/Private core with limited interface to an MNO's core: Enterprises own a local RAN in unlicensed spectrum, leased spectrum or CBRS spectrum with a private 5G core as the primary core, but they are connected to an MNO's core to support mobility. This model delivers added benefits for enterprises in terms of traffic privacy except when a user goes onto the MNO's network. It also reduces 5GC network components in premises, as the rest can be leveraged from the MNO.

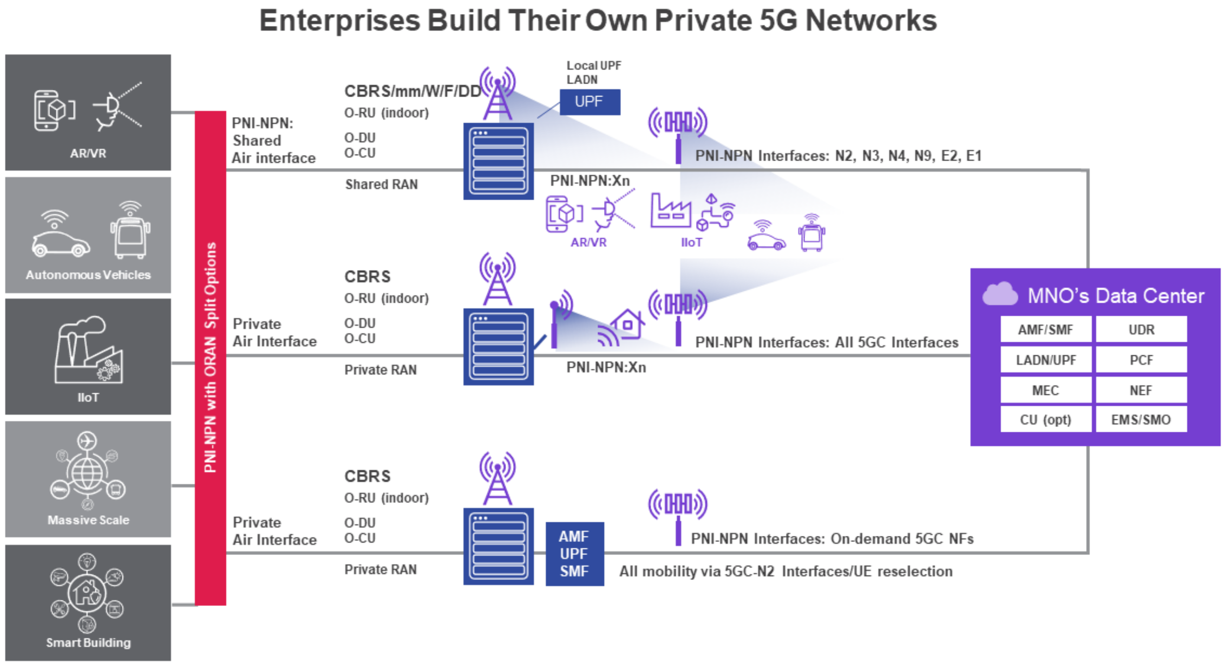


Figure 5: PNI-NPN deployment models
click to enlarge

The Private 5G Opportunity

Private 5G in both SNPN and PNI-NPN modes opens a number of opportunities, given the range of diverse 5G use cases. Enterprises prefer to have a competitive and "business-wise" scalable 5G service deployment with low TCO, new traffic models (UL/DL traffic ratio), a high degree of automation, self-healing and optimized network, which reduces their network maintenance costs. Open RAN solutions, along with 3GPP combinations, bring full openness and a path for enterprises to ease into multi-vendor IoT platforms. Open RAN with open API supports artificial intelligence and machine learning through the implementation of a RAN intelligent controller

(RIC). This further enables simplification of operation and low-cost maintenance, allowing MNOs the ability to increase their focus on the development and delivery of new connectivity services for new market segments. The inclusion of private or public cloud infrastructure adds more centralization gain but it has its own trade-offs and costs to bear.

With continuous effort and innovations from standards organizations including 3GPP, ETSI, GSMA, the NGMN Alliance, the Small Cell Forum (SCF), and the Open RAN community, 5G technologies are making 5G private networks more reliable and secure. Standards are also easing the interoperability challenges and increasing the availability of high-end quality of services even for high data capacity-centric applications like augmented and virtual reality and other latency-sensitive applications. By carefully considering which SNPN or PNI-NPN deployment model best fits their business needs, enterprises can begin to implement private networks that are not only more feasible, but ultimately more efficient and cost-effective.