Hype Cycle for the Future of CSP Networks Infrastructure, 2020

Published: 7 August 2020 **ID:** G00450437

Analyst(s): Sylvain Fabre

This Hype Cycle can assist in selecting appropriate technology portfolios for network-based CSP infrastructure and matching service strategies that support ubiquitous broadband, digital services and the Internet of Things.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

This document was republished on 26 August 2020. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

This Hype Cycle highlights several of the technologies that are key to communication service providers' (CSPs) transformation as well as enabling a whole new set of competitors.

Communication service providers (CSPs) continue to try defending — with limited success — against digital giants and dragons looking to disrupt what were previously proprietary services (voice, messaging, private mobile networks, 5G infrastructure, etc.).

CSPs also have been outpaced in the pursuit of adjacent network opportunities, such as cloud (infrastructure as a service [IaaS]), Internet of Things (IoT) and financial payments, and are hoping to secure increased relevance in verticals with 5G.

While the multilayered architecture of 5G (network plus software and services) can create opportunities for CSPs to expand beyond connectivity-centric solutions, the disaggregation also allows new entrants, including digital dragons, to influence and derive value. This includes recent moves by large hyperscalers into both infrastructure as well as connectivity as a service.

Digital ecosystems are increasingly impacting the way industries function and how new value propositions based on technology solutions are defined. A key characteristic is that the value exchanged is not proprietary and often the value is common and derived indirectly. CSPs need to transform their networks for openness to facilitate, and participate fully in those ecosystems, as well as their IT systems (CSPs should also consult "Hype Cycle for Communications Service Provider Operations, 2020" for back-end and operations capabilities).

The Hype Cycle

This year's Hype Cycle has some key changes over last year (see "Hype Cycle for the Future of CSP Wireless Networks Infrastructure, 2019") to reflect the need to align investments and efforts in capabilities evolution. Key changes are within the following categories:

New wireless connectivity options: this includes 6G, private 5G, NR-light, open-source radio access, standard private LTE, mmWave, shared spectrum access.

New connected endpoints and distributed Intelligence: such as bidirectional brain machine interface, edge AI, CSP AI, eSIM.

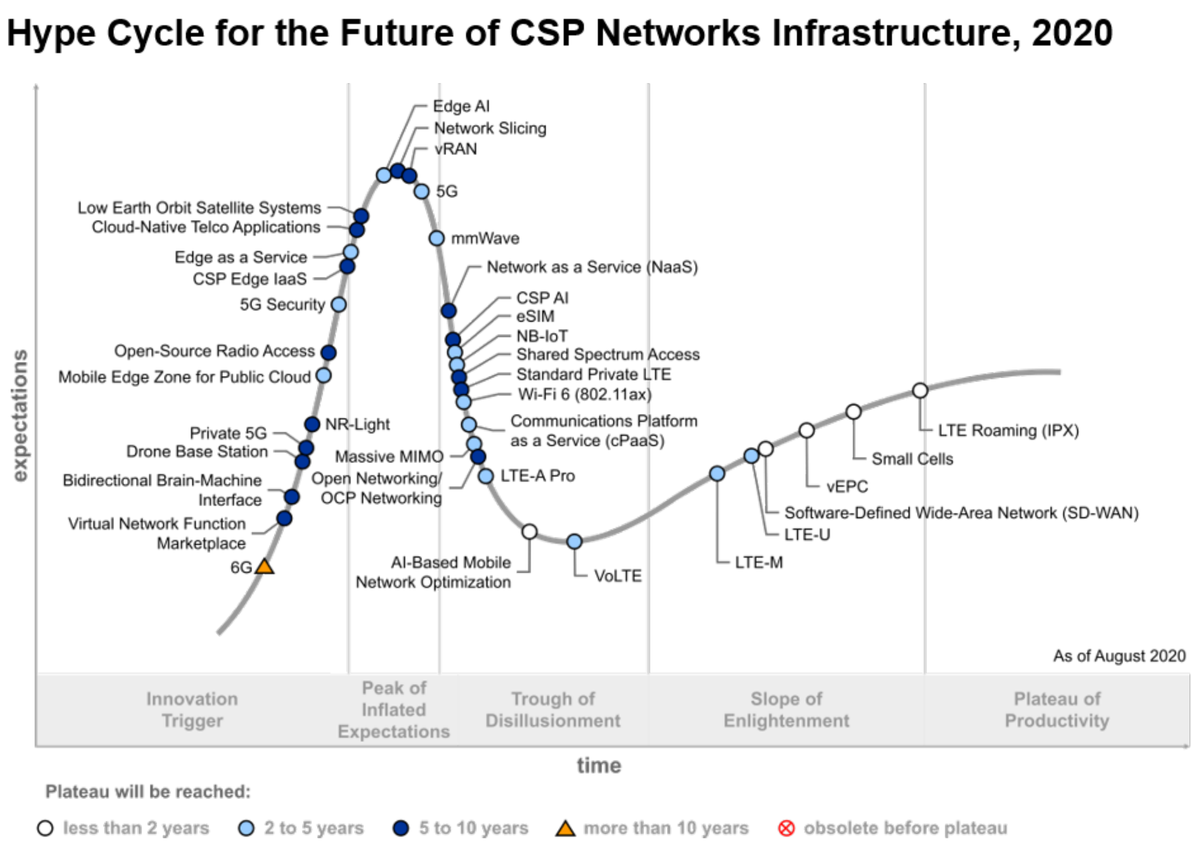
Network capabilities and deployment options: mobile edge zone for public cloud, 5G security, edge as a service, network slicing, network as a service.

Federated Network enablers: CSP edge IaaS, LTE roaming (IPX).

CSPs, and in particular those with network assets, are undergoing significant changes. There are disruptive forces from new types of CSPs as well as players from other industries. New cloud-native CSPs are ambitious with their market, technology, services scope and operating model. In such a scenario, incumbent CSPs in particular need a structured approach to continue modernizing their network platform.

No single technology will help CSPs make the transition to being digital service providers, and they must explore technologies from outside of CSP operational technology (CSP-OT). Many technologies/capabilities on this Hype Cycle are not specific to CSPs but have different benefits and velocity as compared to other industries and are reflected here within the CSP context, bearing in mind telecommunications-industry-specific trends.

Figure 1. Hype Cycle for the Future of CSP Networks Infrastructure, 2020



Source: Gartner
ID: 450437

The Priority Matrix

Transformational technologies, interestingly, are both required to truly become a digital CSP with wide relevance to industry and enable new competitors easier access to the telecom space and reduce lock-in to a given CSP.

Starting with the most immediate impact, vEPC supports virtualization of the CSP core, enabling a more scalable, cost-effective production platform. On the other hand, this capability is also now within the remit of a public cloud provider (Microsoft acquired Affirmed Networks and Metaswitch).

Edge artificial intelligence (AI) improves operational efficiency, such as enhanced visual inspection systems in a manufacturing setting, and enhances customer experience. It also enables cloud providers to add value and execute their AI at the CSP edge. eSIM allows choice across multiple CSPs and may also enable easier entry for nontraditional CSPs and mobile virtual network operators (MVNOs).

MVNOs are also further enabled by network slicing, an opportunity for CSPs to support business-to-business-to-x (B2B2X) models and fuel growth of a large number of specialist IoT MVNOs. Cloud-native telco applications can provide a cheaper way to run network workloads, but conversely allow network infrastructure to be provisioned by hyperscalers.

CSP AI allows communications service providers to leverage AI and machine learning technology to improve customer experience, reduce costs, generate new revenue opportunities and optimize their IT and infrastructure operations. Conversely, other providers could step in to provide the telco AI as a service, gradually building up their expertise of the telecom domain.

On the wireless access side, low-earth-orbit satellite systems may allow connectivity for currently underserved areas, wider private mobile networks, and are provided by satellite providers rather than CSPs.

Figure 2. Priority Matrix for the Future of CSP Networks Infrastructure, 2020

Priority Matrix for the Future of CSP Networks Infrastructure, 2020

benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational	vEPC	Edge AI eSIM	Cloud-Native Telco Applications CSP AI Low Earth Orbit Satellite Systems Network Slicing	6G
high	AI-Based Mobile Network Optimization Small Cells Software-Defined Wide-Area Network (SD-WAN)	5G Communications Platform as a Service (cPaaS) Edge as a Service LTE-A Pro Massive MIMO NB-IoT Wi-Fi 6 (802.11ax)	Bidirectional Brain-Machine Interface CSP Edge IaaS Network as a Service (NaaS) NR-Light Private 5G Shared Spectrum Access Standard Private LTE vRAN	
moderate	LTE Roaming (IPX)	5G Security LTE-M LTE-U mmWave Mobile Edge Zone for Public Cloud VoLTE	Drone Base Station Open Networking/OCP Networking Open-Source Radio Access Virtual Network Function Marketplace	
low				

As of August 2020

Source: Gartner
ID: 450437

Off the Hype Cycle

We had many changes, additions and removals of profiles this year to take into account the drastic shifts currently affecting the CSP space, in particular the aggressive moves of hyperscalers.

Some profiles were removed; others renamed this year. We provide a brief justification for these changes below.

- Named data networking is removed as it is not showing visible traction beyond academia and test beds at the moment.
- AR cloud is removed as it is not yet a distinct part of CSP infrastructure.
- Uplink-downlink decoupling is removed as it is more of a vendor roadmap item.
- Intercarrier service automation is removed as it has not materialized as a distinct inquiry topic.
- Remote expert guidance solutions is removed as it is more of an application rather than CSP infrastructure.
- 5G services is removed as not directly infrastructure.
- The following two profiles were merged: private LTE and LTE for mission-critical and public safety networks, and replaced by standard private LTE.
- Universal CPE is removed as it is not a core component of the CSP infrastructure.
- LoRa is removed as it is more specifically used for IoT and not as a core part of the overall network.
- Vehicle-to-vehicle communications is removed as it is not clearly under the CSP remit.
- Open-source base station is renamed open-source radio access.
- Edge computing for CSPs is taken off the Hype Cycle as the market seems to be moving away from siloed solutions toward cloud approaches. The topic of edge in a telco context is now covered in other profiles that align more closely with the growing trend of hyperscalers entering the telco domain: mobile edge zone for public cloud and CSP Edge IaaS.
- Wi-SUN is removed as it has not turned out to be a core CSP technology.
- Mobile self-organizing networks is renamed AI-based mobile network optimization to reflect changes in the priorities of CSPs as well as vendors' movements.
- Augmented reality is removed as it is more of an application rather than CSP infrastructure.

On the Rise

6G

Analysis By: Kosei Takiishi

Definition: 6G is the generic name for the next generation of cellular wireless that is expected to be the successor to 5G. In 2020, the features and timetable for 6G are not clearly defined although it's expected to emerge around 2030. 6G is really in the incubation period and it is focusing on "big picture" discussions such as 6G concept, vision and transition from mere technology to platform/ solution or current technology research continuation such as Terahertz usage.

Position and Adoption Speed Justification: Major 6G related announcements in the past 12 months include:

- In June 2019, SK Telecom signed agreements with Ericsson, Nokia and Samsung Electronics for joint research and development (R&D) in advanced 5G and 6G.
- In August 2019, Huawei at its Ottawa Research and Development Center has begun early stages of researching on 6G technology.
- In October 2019, NTT, Intel and Sony established Innovative Optical and Wireless Network (IOWN) Global Forum dedicated to realizing the communications of the future.
- In January 2020, NTT DOCOMO released a white paper promoting 6G communication system.
- In March 2020, the second 6G wireless summit 2020 has been organized as a virtual event in 17 March 2020 onwards.

Gartner assumes that these “too early” 6G announcements aim to support companies and any stakeholders to emphasize their 6G leadership in the middle of 2020s. This is mainly for their technical marketing message and what they did for 5G in 2013/2014 time span. Just the timing of next next-generation engagement announcement might have been ahead of schedule several years.

Technically speaking, 6G will enhance recent 5G capabilities and will be able to provide higher peak data rate (e.g., 100 Gbps to 1 Tbps), lower latency (e.g., 0.1 msec latency), much more connection density, better radio spectrum efficiency and energy efficiency (e.g., 10 times more efficient).

User Advice: We advise:

- Observe the current emerging 6G discussion carefully.
- Do not consider deploying 6G commercially till late 2020s. However, there could be deliverables of the 6G research projects that emerge in other wireless areas before 6G. E.g., THz wireless systems could well emerge before 2030.
- Support your regulators and government to create their new national policy by 5G evolution and 6G.

Business Impact: As of today, there is no clear 6G definition and the telecom industry is just trying to add one generation every 10 years (same as before). 6G will not impact any businesses till late 2020s but its social impact and accountability will be unfathomable.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Ericsson; Huawei; LG; Nokia; NTT DOCOMO; SK Telecom

Recommended Reading: “3 Technologies Critical to 6G Network Product Roadmaps”

Virtual Network Function Marketplace

Analysis By: Amresh Nandan

Definition: Virtual network function (VNF) marketplace refers to a platform-enabling commerce of VNFs, which allows developers/companies to offer VNFs for enterprises or SMBs to purchase/consume them. The marketplace is to request, procure, onboard, deploy VNFs, manage and provide support services in one or more commercial models. A communications service provider (CSP) VNF marketplace can enable CSPs to extend their enterprise network services to include offering VNFs, as well as service packages for multiple market segments.

Position and Adoption Speed Justification: VNF marketplace adoption is becoming one of the mainstream ways to commercialize and distribute VNFs. The idea has been implemented by certain leading CSPs like AT&T, Telstra and Verizon as well as by cloud service providers such as Amazon Web Services (AWS) and Microsoft Azure. Enterprise digital transformation and new business requirements present several opportunities for CSPs to commercialize VNFs through marketplaces. Network-based CSPs can target further revenue growth by augmenting their network as a service (NaaS) offerings with VNF marketplace. Among many opportunities in the form of IT, security, infrastructure and connectivity, is the opportunity to offer VNFs with flexible commercial and operational models. VNF marketplace enables enterprises to procure VNFs such as a router, switch and firewall to use with network function virtualization (NFV) points of presence (POPs) in a CSP's network or with universal customer premises equipment (uCPE).

Key modules of VNF marketplace platform include VNF catalog, license management, revenue management and self-service and support. Further, a VNF marketplace requires modules, tools and processes for partners to test, certify and onboard VNFs. Operationally, a comprehensive toolchain and a uniform process of onboarding (and automating) as well as near-real-time support is essential. Commercially, the ability to offer standardized/pretested service chaining service packages priced according to the needs of various market segments, is crucial for developing a competitive offering. Some CSPs are also working on bring-your-own-VNF propositions.

User Advice: CSP's success with VNF marketplace depends on multiple factors, such as extent of ecosystem (partnerships for sourcing/developing/testing VNFs), agility and flexibility in VNF life cycle management and commercial contracts among VNF suppliers, CSPs and customers. Leading CSPs that have initiated efforts in developing a business via a VNF marketplace see the demand in a subscription model, which generates the requirement of sourcing VNFs in a pay-as-you-go model. Viability of VNF marketplace can be challenging unless the CSP targets a wide market segment, going beyond its national boundaries if the domestic market isn't large. CSPs should:

- Adopt a platform approach to enterprise services design, delivery and support — with a service factory model for operations.
- Craft a business strategy that allows leveraging the platform strategy for wider market segments, going beyond their national boundaries.
- Develop a blueprint of target services architecture and start developing/procuring specific modules as per the target architecture.

CSPs also need to pay attention to performance (connection quality and distance when the VNFs are hosted on CSP's network/uCPE suboptimized hardware or chipset for specific communication and security VNFs) and cost. Software license prices still pretty much as if they came with dedicated hardware. Cost of uCPE platforms should then be included. The approach is viable for end customers that have already decided to use three or more VNFs in the device. This limits ability to foster initial demand. For the other delivery model — network-based — there should be a dense-enough network of NFV POPs to satisfy performance requirements.

Business Impact: CSPs looking to expand their offerings for enterprises and SMBs can enhance their virtual customer premises equipment (vCPE) and WAN offerings through a VNF marketplace. Emergence of edge computing trends will further boost the demand for models like VNF marketplace, offering better exchange of values for both CSPs and customers. The platform can be integrated with a service (NaaS) management platform for easy bundling of VNFs and service packages. Such an approach can enable CSPs to target multiple market segments with VNFs sourced from multiple vendors — offering different price ranges and service packages. CSPs should develop and use a VNF marketplace platform offering for enterprises and SMBs when:

- They are open to developing a competitive positioning with VNF vendors, as this business model is disruptive for the traditional value chain.
- They have scaled their NFV implementation adequately with a robust VNF life cycle management process and tools.
- They have achieved a certain degree of automation in service design, service creation and service delivery across hybrid/virtual network.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Cisco Systems; F5; Fortinet; Juniper Networks; OpenVPN; Palo Alto Networks

Recommended Reading: "2018 Strategic Roadmap for CSP NaaS and VNF Marketplace Platform Operations"

"Toolkit: 2018 Strategic Roadmap for CSP NaaS and VNF Marketplace Platform Operations"

Bidirectional Brain-Machine Interface

Analysis By: Sylvain Fabre; Annette Jump

Definition: Bidirectional brain-machine interfaces (BMIs) are brain-altering neural interfaces that enable two-way communication between a human brain and computer or machine interface. Bidirectional BMIs allow not only monitoring of the user's EEG (electro encephalogram) and mental states, but also some action to be taken to modify that state based on analytics and insights. Brain state modification occurs via noninvasive electro stimulation through a head-mounted wearable, or an invasive implant. When connected, these enable the IoB (Internet of Brains).

Position and Adoption Speed Justification: It is still very early days for bidirectional BMI. There are already applications of one-way BMI wearables, where the focus is about monitoring the state of the user or using the user intent to operate some external device — but without trying to externally modifying the user's mood. Some of these solutions even measure the response and attitude of consumers to products and companies.

In September 2019, Facebook acquired the neural interface startup Ctrl-labs for over $500 million, and will work to include the technology as a computer interface and in AR/VR consumer products using Facebook Reality Labs.

In 2017, DARPA also awarded a $65 million contract to develop a bidirectional BMI.

In order to estimate the progress for bidirectional BMI, it is worth noting that a related earlier trend, smart wearables, experienced significant hype in 2016 through 2018, particularly fueled by interest in consumer smart wearables devices and software. However, venture capital investments in companies developing smart wearable products and solutions decreased from $2.8 billion in 2018 to $1.6 billion in January 2019 through October 2019. This return to 2017 investment levels highlights the shift in VC investors' evaluation of opportunities and potential markets for some smart wearables. The 2019 decline in VC smart wearable investment underscores the issues linked with smart wearable devices, to include high cost, slow consumer adoption, high drop-off rates for some smart wearables, and the complexity of integration between various data systems.

Since bidirectional BMIs are more advanced and extreme form of wearable (in effect, an implant with bidirectional connectivity), the above trend provides some guidance as to what needs to occur to allow a wider adoption of bidirectional BMI. Namely, it will need to become more affordable and find ways to add functionality without added invasiveness.

An early application is from NYX Technologies, currently in beta testing phase, which aims to use neurotechnology to both monitor and stimulate brain function and improve sleep.

User Advice: Enterprises should be prepared for future creeping of bidirectional BMI devices into enterprises; BYOD may occur before specific legislation is in place, so business leaders should:

- Ensure customer safety and business security by implementing data anonymity and privacy (beyond GDPR) for brain-wearable data in products.
- Highlight trade-offs when promoting wellness solutions.
- Take responsibility: Set up a steering board to monitor products sold to consumers and provided for employees. Preempt potential legal liability by regularly reviewing implanted wearables features and their use cases and deciding on what is acceptable in terms of read/write from and to users' brains.
- Establish policies for unauthorized implantables: While they cannot easily be removed, users may be prohibited from some roles such as operating vehicles or machinery (as BYOD bidirectional BMI implants would pose risks similar to drugs or stimulants).

Business Impact: There are multiple form factors for devices designed to be worn or implanted to sense the human body, such as smartwatches, head-mounted displays (HMDs), ear-worn wearables or hearables, wristbands, smart rings, smart garments, smart contact lenses, exoskeletons, implants and ingestibles. Over the next three to 10 years, they will enable business use cases including: authentication, access and payment; immersive analytics and workplace; and control of power suits or exoskeletons.

What is unique about bidirectional BMI is that it is a brain-altering class of wearables/implantables. In addition to the use cases mentioned above, we now look at bidirectional connectivity for the brain. For example, stimulation applied to boost alertness in response to markers of fatigue in a worker's EEG, or relaxing cortical currents applied to the brain of a teacher or nurse showing signs of irritability. This creates very specific ethical and security challenges, because they are a direct interface to the human brain.

Bidirectional BMIs are the front line of innovation that powers human augmentation. They are designed to exhibit some level of autonomy when connection to the internet is not available or desirable. They are also designed to learn using machine learning (ML), interact with the environment around the wearer, enhance human abilities, and connect humans to the Internet of Things (IoT) and the Internet of Brains (IoB).

As a result, direct read-and-write access to brain activity creates many opportunities for workforce enablement. It also provides new vulnerabilities to individuals and their companies by adding a vector of attack and human factor issues such as altering users' perception of reality, or even their personality.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: BrainCo; Facebook; Kernel; Neuralink; Neuroelectrics; NeuroMetrix; NYX; Omron Healthcare

Recommended Reading: "Maverick* Research: Mass Adoption of Brain-Monitoring and -Altering Wearables Creates Risk of Mind Control"

"Emerging Technology Analysis: Smart Wearables"

"Venture Capital Growth Insights: Smart Wearables"

Drone Base Station

Analysis By: Kosei Takiishi

Definition: An unmanned aerial vehicle (drone) can provide a cellular signal when terrestrial cellular base stations are out of service or not available in an extreme situation such as disaster recovery. Existing disaster response solutions such as movable base stations and satellite backhauls are very expensive, large to operate and take time to prepare. A drone base station tries to fill the gap in an agile and efficient manner.

Position and Adoption Speed Justification: Cellular network, including 2G, 3G and 4G long-term evolution (LTE), has been deployed gradually over the past 30 years and most of the human-inhabited areas can be covered by itself. However, there are still uncovered areas including uninhabited rural regions and communication-disabled areas.

Drone base station can be deployed regardless of road and ground conditions, and can be operated even in areas where there are entry restrictions and prohibitions, such as disaster areas. Moreover, it is much easier to carry and operate and has shorter preparation time (e.g., as little as one hour) in comparison with existing disaster response solutions such as Verizon's Cellular on Wheels.

Consequently, some communications service providers (CSPs) in advanced markets have started testing for it, including AT&T, Verizon and Sprint in the U.S.; KT in South Korea; NTT DOCOMO, KDDI and SoftBank in Japan; China Unicom and China Telecom in China; and EE in the U.K. Yet, drone base station will move slowly through the Hype Cycle due to the challenges below and the need for further development:

- Small coverage area, such as 1 km or less.
- Short operating time, less than one hour with onboard power supply: Connection with ground power supply through cable is possible; however, increasing altitude will cause problems such as cable weight and wind pressure (existing limitation: wind speed is about 20 m, altitude is about 100 m).
- Difficulty moving horizontally with wired power supply.
- Weather also can affect the ability, like very high winds during a prolonged storm heavy rain and during a blizzard.
- Different policy and procedure to enhance the radio coverage in the air.
- Regulations such as aeronautics and radio law.

User Advice: We advise:

- Test the drone base station, and confirm its capability and effectiveness.
- Study the coverage and its radio interference in the air.
- Start developing the ecosystem with stakeholders.

Business Impact: Drone base station is mainly targeted to compensate for the cellular network coverage during emergencies, but its potential is huge, including communication distance enhancement by multihop communication over drones and automated network optimization sensing neighbor cells. Its commercialization is far into the future, but its research and study can start now.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Airspan; Ericsson; Fujitsu; Nokia; Qualcomm; ZTE

Recommended Reading: “Magic Quadrant for LTE Network Infrastructure”

Private 5G

Analysis By: Sylvain Fabre; Joe Skorupa

Definition: Private 5G is defined as a private mobile network (PMN) based on 3GPP 5G to interconnect people/things in an enterprise. CSPs and TSPs have the potential to offer 5G PMN to various verticals, such as Industry 4.0, mining, oil, utility and rail road companies; IoT service providers, university campuses, stadiums/arenas etc. Private 5G offerings provide a separate network from the public network. It can include voice, video, messaging, and broadband data and IoT/M2M use cases with higher performance requirements.

Position and Adoption Speed Justification: Most enterprises use cases that justify a need to deploy a Private Mobile Network (PMN) that requires cellular connectivity for mobility, will be adequately served with a 4G network. Where 5G is justified, a PMN can provide the required functionality earlier than what the local CSPs may have deployed on their public infrastructure. There is another class of use cases however, not focused on mobility but requiring a high performance backbone where wiring is complex and costly — as in a factory deployment. In that case, support of autonomous delivery vehicles on the shop floor, could apply, but as a complementary application. Some verticals may adopt 5G sooner as a response to the current COVID-19 pandemic, driven by cost optimization, resiliency and automation concerns.

Volkswagen is reported to plan 5G private deployments in 122 German factories in 2020.

An early implementations example is: BMW Brilliance Automotive (BBA, BMW’s JV in China) claims complete 5G coverage in all of its factories.

User Advice: Enterprises looking to deploy 5G PMN should:

- Seek out quotations not only from CSPs but also other possible providers such as large equipment vendors and smaller specialist
- Consider SIs and consultancies for design, deployment and managed services.
- Consider licensed and also unlicensed/shared spectrum options where available (for example 5G was approved for use in CBRS in February 2020 such as CBRS; German regulator Bundesnetzagentur [BNetzA] has allocated spectrum in the 3.7 GHz to 3.8GHz band for industrial local 5G).
- CSPs offering Private 5G to industrial buyers need to work with IT service providers that have the required industry skills (and knowledge of other technologies) to provide a value proposition of how 5G supports a specific use case or business KPI to justify the additional investments

required to make existing infrastructure 5G ready. For example, in manufacturing 5G is seen as a platform that combines connectivity with security and AI capabilities.

Business Impact: While 5G standard are defined by 3GPP, other bodies are contributing in order to improve applicability to connected industrial applications, for example 5G-ACIA (Alliance for Connected Industries and Automation). 5G PMN can offer enterprises improved security and independence and enable efficiency gains in several manufacturing and industrial processes.

An early implementations example is: BMW Brilliance Automotive (BBA, BMW's JV in China) claims complete 5G coverage in all of its factories.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Athonet; Ericsson; Huawei; Nokia

Recommended Reading: "4 Hype Cycle Innovations That Should Be on the Private Mobile Networks Roadmap for 5G Security, CSP Edge and Slicing"

"Market Impact: How CSPs Can Rebuild Resilience and Business Continuity During Disruption"

"Cool Vendors in Communications Service Provider Network Operations"

NR-Light

Analysis By: Kosei Takiishi

Definition: NR-Light is a new standard specification focusing on IoT by 3GPP release 17 that will be frozen in 2021. Incumbent 3GPP release 16 covers high-performance (e.g., industrial IoT) and low-complexity IoT (i.e., LTE-M/NB-IoT) but there is the gap between high-performance IoT devices and low-complexity IoT devices. NR-Light could occupy just 10MHz or 20MHz of bandwidth and deliver 100 Mbps of downlink and 50 Mbps of uplink throughput.

Position and Adoption Speed Justification: While NB-IoT and LTE-M enhancements have been covered by early 5G specifications by 3GPP release 15 and 16, these are not very new and just relatively minor improvements compared to other new functions. To broaden and optimize 5G's support for IoT, 3GPP release 17 will standardize NR-Light — a new class of devices that is more capable than eMTC/NB-IoT but supports different features and smaller bandwidth than 5G NR eMBB/URLLC. This type of requirement was not covered by previous 3GPP standards and this can make it a suitable technology for use cases such as high-end wearables or industrial IoT cameras and sensors. Especially, the telecom industry is promoting 5G to be a platform for vertical industries such as automotive and healthcare and this NR-Light capability will become the basis.

User Advice:

- Observe and participate in the 3GPP standardization related to NR-Light
- Adopt multi IoT access technologies including LTE-M, NB-IoT and NR-Light by satisfying multiple demands from clients

Business Impact: 5G evolution, the concept of the enhancement of initial 5G, becomes mature in the middle of 2020 and NR-Light will be one of the important technology components. NR-Light will not impact any businesses soon but its benefit is clear and can satisfy enterprise clients which are trying to find devices with a balance of functionality and cost.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Ericsson; Huawei; Nokia; Qualcomm

Recommended Reading: “Magic Quadrant for LTE Network Infrastructure”

Mobile Edge Zone for Public Cloud

Analysis By: Sylvain Fabre; David Wright

Definition: Mobile edge zone for public cloud covers an application platform that is both carrier-grade and public cloud managed, to be deployed at the cloud provider’s edge or within a telecom communications service provider’s network. It is suitable to host a variety of telecom workloads stretching from the telecom back office out to the mobile edge.

Position and Adoption Speed Justification: There are multiple capabilities needed to be a mobile supplier or a communications service provider (CSP), and the cloud providers moving into this space only cover some of these. They have no radio access products, or large professional services arms for installing and operating live networks, but can partner with CSPs or telecommunications service providers (TSPs) to acquire that capability. They are however making incremental moves toward some core network aspects which are well within their current capabilities and augment them. These aspects are the mobile edge as well as packet core domain, or insights on the radio access network (RAN) domain — all these options do not require actually providing RAN products. This is a systematic approach by public cloud providers to position as providers of mobile infrastructure. Lack of radio access and spectrum may not be an issue in the longer term however, with multiple initiatives working toward reducing barriers to entry for a new breed of nontraditional telecom operators. For example, network sharing such as Multi-Operator Core Network (MOCN) or Multi Operator RAN (MORAN), and unlicensed spectrum approaches such as Citizens Broadband Radio Service (CBRS).

A public cloud provider partner however brings something the telco CSPs have never been able to develop: a truly horizontal application hosting and management environment. The cloud providers bring a robust IaaS and PaaS service platform that will make it easy for telecom VNF providers and other telecom ISVs to build and deploy 5G-related solutions.

Examples so far include various incremental moves that public cloud providers are making toward building mobile network capabilities: 5G Multiaccess Edge Computing (MEC) with AWS Wavelength, Microsoft Azure Edge Zones for telco (optimized x86 plus virtual Evolved Packet Core [EPC] plus certified partner virtual network functions [VNFs]), and Google Global Mobile Edge Cloud (GMEC). Amazon Web Services (AWS) will self-OEM the hardware, Microsoft will partner for integrated certified hardware, and Google will run on a variety of third-party container-compliant hardware. Microsoft and Google are explicitly including the use of their own edge network access points and capabilities in the offering, AWS has not yet specified this aspect. In terms of workloads, GMEC is currently demonstrating mostly back-office Business Support Systems (BSS) functionality (like Amdocs and Netcracker), whereas Microsoft has purchased virtual EPC (mobile packet core) provider Affirmed Networks, and agreed to acquire Metaswitch Networks (cloud native telecom networks). AWS has been silent about VNF partnerships. In all three cases, the goal is to “tether” the mobile domains to the public cloud and manage them from there, at least partially.

The desire of telecom CSPs to sell services that monetize their 5G network and license investments will continue to propel them toward the cloud providers, and likewise the telecom VNF/app independent software vendors (ISVs) will see a scalable route to market. This combination will accelerate the adoption of this approach in market.

Finally this trend could accelerate with political initiatives that seek to promote a supply chain for 5G network infrastructure that is refocused on North American providers. Leveraging North American public cloud providers for 5G networks could be seen as an alternative to Asian vendors at a time where there are no traditional end-to-end vendors of 5G public networks left in North America (since Nortel Networks, Motorola and Lucent have left the space).

User Advice: The benefit for CSPs is a wider choice of vendors and potentially a faster route to OS innovation. But, CSPs should be mindful that using public cloud providers rather than traditional infrastructure may not reduce vendor lock-in but possibly a shift to a different set of suppliers instead.

There is also a risk for CSPs when public cloud providers compete in providing private mobile networks to enterprises.

CSPs considering partnership with cloud providers for their mobile edge should:

- Increase differentiation by integrating the edge computing offering from the public cloud provider(s) into your private mobile network solution for industries.
- Retain long-term value by designing edge architecture with edge public cloud provider(s) so that the CSP can secure most value from enterprise networks and related IoT data.
- Preempt competing offers by cloud providers for mobile private networks by offering complementary solutions such as slice as a service to cloud providers and (mobile virtual network operators [MVNOs]) (using shared as well as licensed spectrum options).

All things considered, there seems to be a bigger benefit for public cloud providers, who are positioning themselves to capture value away from both CSPs and their vendors, by gaining increased access to IoT data.

Business Impact: As the public cloud providers consolidate more network capabilities, they will over time become more of a competitor to:

- Traditional network infrastructure vendors (especially as VNFs [virtualization] and open source gain further adoption in how mobile networks are implemented).
- Existing CSPs (as unlicensed/shared spectrum options gain wider adoption for enterprise and industry use).

In a related initiative (although not a public-cloud managed solution), other nontraditional vendors of infrastructure also venture into the mobile networking space, for example VMware acquiring Uhana for RAN analytics, signaling an era of more vendor choices for CSPs.

Finally, some of the cloud providers appear to also be edging toward their own fully independent wide-area networks — Google already has most of it in fiber, Amazon is attempting a long-play through satellites. We also see signs of public cloud providers entering provision of mobile networking to enterprises, such as private LTE over CBRS supplied as connectivity as a service by AWS and Microsoft (Google is also active with the Spectrum Access System [SAS] sensing database for CBRS spectrum).

One open question is where the profit will go — with app, cloud and telecom vendors in every solution, who controls the customer, who negotiates the sale and who will capture the most margin.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Alibaba Cloud; AWS; Google; IBM Cloud; Microsoft Azure; VMware; XGVela

Recommended Reading: "Emerging Technologies: Venture Capital Growth Insights for mmWave 5G"

"Market Guide for 5G New Radio Infrastructure"

"Assessing 5G Mobile Technology for Organizations"

"Market Trends: Strategies Communications Service Providers Can Use to Address Key 5G Security Challenges"

"Reduce Privacy Risks When Using 5G Products and Services"

Open-Source Radio Access

Analysis By: Sylvain Fabre

Definition: Open-source radio access network (RAN) includes OS base station concept for low-cost wireless access points that can be used to reduce coverage costs. The concept also covers the evolution of the traditional RAN equipment and interfaces to an open, virtualized architecture. This profile mentions several forums and initiatives related to the open-source RAN station concept.

Position and Adoption Speed Justification: The viability and potential wider adoption of this technology require more leading communications service providers (CSPs) to join and actually deploy the technology, and then, expand deployments beyond limited rural areas. In addition, the function of real software-defined radio in the base stations can prove difficult to realize and commercialize in the near future, although initiatives such as OpenAirInterface (OAI) may help.

OpenRAN refers to disaggregation of RAN functionality. vRAN refers to RAN implementation using VNFs. O-RAN is the open RAN alliance.

Open source related projects in the RAN include:

- Openstack
- OAI: OpenAirInterface software alliance.
- Open Cellular by TIP: An open source project that seeks to facilitate community cellular infrastructure design, build and operations for rural and under connected areas.
- OpenRAN Group: Co-founded by Facebook as part of The Telecom Infra Project's (TIP's) in 2016, includes Intel, Nokia, Deutsche Telekom and SK Telecom, and aims to define and build 3GPP vendor neutral hardware and software infrastructure.
- OIN: Open invention network (recently joined by Rakuten).
- O-RAN Alliance (founded in February 2018) has CSP members including AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO and Orange. O-RAN appears to be gaining traction as the main forum for OS Radio access with 22 mobile operators with commercial deployments as of June 2020.
- Open vRAN Ecosystem: An earlier initiative championed by Cisco, announced in February 2018, that included Reliance Jio, Altiostar, Aricent, Intel, Mavenir, PHAZR, Red Hat and Tech Mahindra.

What makes these forums attractive to CSPs is that progress can occur faster than the traditional 3rd Generation Partnership Project (3GPP) standard process.

Another driver could be the renewed ambitions from hyperscalers to position themselves as alternative suppliers of network infrastructure (e.g., acquisitions: Affirmed Networks by Microsoft or Ahana by VMware), which is easier for them with an OS framework.

User Advice: It is too early to plan for wide-scale deployment. However, the potential cost savings should be investigated by CSPs — traditional and alternative — since more economical access points could justify the coverage of underserved and rural areas, especially where current infrastructure, opex and backhaul costs make such deployment expensive. However, it is still unclear whether the open-source base station concept would prove enough to change the current views of the vast majority of CSPs. However, the trend to open-source network elements is likely to continue as other parts of the GSM infrastructure also open up.

In terms of open source base station initiatives, there is a clear momentum building based on interest from CSPs to achieve the benefits of NFV in the RAN as well as reduce vendor lock-in to some extent.

Business Impact: Historically, base stations and cellular access points have remained driven by larger vendors due to the required investments in R&D and testing, at least as far as macro, outdoors equipment for CSPs is concerned. Open-source base stations can reduce costs by making the equipment more versatile. They may also open the door to smaller vendors and open-source developers that can develop applications supporting a variety of wireless standards (such as 3GPP, Wi-Fi, iBeacon or Radar). However, if open-source base stations' volumes start ramping up, then it is likely that there would be fees involved, especially about 3GPP patents for 4G and 5G.

vRAN is based on open standards and less driven by the traditional infrastructure vendors. It will open up the CSP infrastructure market. Many smaller, software-specialist vendors— as well as larger public cloud players can now host mobile network elements VNFs on behalf of CSPs and TSPs. Open-sourced solution may not be cheaper due to the need for integration as well as potential increased vendor management overhead.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Altiostar; Aricent; China Mobile; Cisco; Ericsson; Facebook; KDDI; Mavenir; Nokia

Recommended Reading: "Magic Quadrant for LTE Network Infrastructure"

5G Security

Analysis By: Sylvain Fabre; Bernard Woo

Definition: 5G security is enabled by a set of 5G network mechanisms, and improves 4G security with:

- Unified authentication (4G authentication is access dependent).
- Flexible security policy for diverse use cases (versus single 4G policy).
- Encrypted transmission Subscription Permanent Identifier (SUPI) prevents International Mobile Subscriber Identity (IMSI) leakage for user privacy.

Position and Adoption Speed Justification: 5G security is not a priority in many deployments; standards won't cover everything — implementation will hugely influence outcomes (e.g., private network versus public infrastructure). Switching on security features is up to the CSPs.

- 5G will increase number and diversity of connected objects, potential DDoS attack vectors and entry points; this also provides more telemetry for anomaly detection.
- More 5G private, dedicated networks will be deployed by enterprises (more security conscious than consumers).
- Legacy networks and devices will interconnect with 5G.
- 5G infrastructure virtualization, automation and orchestration of a service-based architecture increases exposure.
- Slicing virtual networks across shared infrastructure impacts security due to lateral movement risk, and cross-slice permeability issues.
- Wider ecosystem delivering industrial 5G use cases, with varying security competencies and credentials, make SLAs, service assurance including E2E security, challenging.
- Backward compatibility with 4G/Long Term Evolution (LTE) means some legacy security issues persist in 5G.

User Advice: Don't rely exceedingly on network 5G security, end users will still have to continue using VPNs and identity management.

In addition, security leaders leveraging 5G, including for industries, should:

- Anticipate increased attack risk such as DDoS by improving equipment and software design of 5G network infrastructure and endpoints, and recovery procedures.
- Implement layered-DDoS defense with best of cloud scrubbing center, cloud web application firewall, bot mitigation, DNS protection, ISP and on-premises DDoS appliances. Determine effectiveness of protections from incremental add-on solutions an ISP or CDN can sell.
- Evaluate DDoS protection services from current CSP or cloud providers as a possible failover for key applications when on-premises DC is under attack.
- Initiate effective mitigation by correlating network traffic, application availability and server performance. Outages may be due to human or system error rather than attacks.
- Consider interoperability with other networks e.g., authentication of Wi-Fi devices. Ensure 5G device hardening to reduce possibility of being used as botnets.
- Segment IoT devices with different incident responses.
- Complement 5G infrastructure security with distributed anomaly detection/monitoring including edge and core slicing.

- Decide any trade-offs between secrecy, capacity, delay, quality of service (QoS), compute and energy efficiency by use case.
- Implement edge protection concepts used in application security for elasticity and focused on app-layer protection, and commonly provided via a CDN provider, SaaS or cloud provider.

Security for 5G systems encompasses need to include in network deployments:

- Cross-network layer security (e.g., between 5G macro and small cell layers)
- E2E security (e.g., managing strength of different algorithms, generating and negotiating secret keys, confidentiality protection)
- Cross-CSP 5G network domain security (e.g., in R16, several cloud service providers [CSPs] could provide slices for a given 5G service)
- Leverage user traffic integrity protection which is available now

Traffic interception may require formal and time-sensitive reporting to clients due to maturing data protection regulations.

Implement patching policies and procedures on devices used for network configuration given 5G's reliance on software.

All 5G network infrastructure vendors implement the same 3GPP standards for 5G security; however development processes may vary; concerns about specific vendors as well as geopolitical tensions have increased procurement scrutiny around 5G infrastructure.

5G network infrastructure requires more antennas, promoting sharing with different CSPs or utility providers, or multitenant scenarios. It needs the review and update of hardware protection protocols, including physical measures to address recent increases in vandalism based on fake news.

Embed privacy-protective features into endpoint/IoT devices to manage potential privacy risks.

Plan for lower security context anytime your 5G devices connect to a legacy 3G or 4G network.

Business Impact: Increased controls could impact QoS, increase latency and lower data rate due to traffic encryption overhead.

Guaranteed security levels may enable 5G use in more demanding use cases, using other improvements, like:

- Home control feature enables network to verify device location when the device is in a visited network, preventing spoofing attacks on device locations involving false signaling messages to request device identifier and location, and then intercept ongoing communications.
- 5G mitigation against bidding down attacks prevents a fake base station from making UEs believe that the BTS ("IMSI catcher") does not support a specific security feature and use a previous mobile network technology.

- Flexible security policies and other chargeable features such as slice as a service, QoS SLAs for latency etc. in 5G allow premium pricing.
- 5G security adds value for CSPs but may be adding complexity for business users.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Ericsson; Huawei; Intel; Mobileum; Netcracker; Nokia; VIAVI Solutions

Recommended Reading: "Market Trends: Strategies Communications Service Providers Can Use to Address Key 5G Security Challenges"

"Reduce Privacy Risks When Using 5G Products and Services"

"Market Guide for Mobile Threat Defense"

"Protecting Web Applications and APIs From Exploits and Abuse"

CSP Edge IaaS

Analysis By: Sylvain Fabre; Ted Chamberlin

Definition: The new category of CSP edge IaaS facilitates CSPs' edge deployment beyond their own network perimeter; this allows CSPs' connection to an edge provider, on their footprint but with the edge providers handling the edge-related infrastructure and its operations. A diverse feature set is provided by multiple providers, including stateful applications, dynamic caching, CDN, application acceleration, or games and industrial IoT applications optimized for latency. Individual CSP deployments can be federated, creating an edge cloud framework.

Position and Adoption Speed Justification: This model also allows companies to connect to, and consume edge cloud as a service for enterprise networks — including private mobile 4G and 5G networks. Initial adoption indicates that early CSP edge infrastructure as a service (IaaS) providers are operational but defining clear business models and showing their viability is the next step.

Early initiatives include:

- Ericsson Edge Gravity, started in 2016, focused on wireline operators; provides a cloud native solution on both the application and the infrastructure side. With over 85 communications service providers (CSPs) signed up, they initially focused on a few use cases to validate their business approach. This provided a preintegrated full stack solution, such as CDN (deal with Limelight), caching, SD-WAN and gaming, with an intent to support more moving forward. The goal for Edge Gravity is to mature current CDN edge nodes to intelligent points of presence (PoPs). As of publication however, Ericsson Edge Gravity appears to have ceased activities.

- Deutsche Telekom's MobiledgeX provides an abstraction layer across multiple CSPs, exposing as runtime to application developers to support gaming and industrial applications. These include Holo-Light (German, AR/VR for industrial applications); 1000 realities (Polish, AR/VR applications); Edgemesh (U.S., enhance visitors' browser); Niantic (U.S. software, started with Google); VRee (Netherlands, AR/VR suits).
- Macrometa provides a distributed database platform that can leverage CDN and data center providers to provide distributed edge capability, underpinned by a distributed database and ledger functionality. This enables workloads to run locally at the edge with low latency.
- AlefEdge provides a software stack that works with existing networks as a plug-and-play overlay, using proprietary APIs. Their cloud-native software at the edge enables multiple edge sites to form the "Edge Internet."
- Gaming/e-sports use case: E-sports and gaming experience suffer from lag time and excessive latency which impede user experience. Providers like Edgegap and Swarmio Media provide AI-based algorithms that optimize edge hosting locations with proximity to gamers.

While nascent, these approaches seem to provide a faster avenue for enterprises, and service providers, to connect and deploy edge cloud topologies at scale, beyond what traditional local solutions can deliver. However, profitability and revenue need to be demonstrated for many of these offerings, which will require wider adoption. The fact that Ericsson's Edge Gravity appears to have run into difficulties is confirmation that this approach is still unproven.

User Advice: Enterprises, service providers and CSPs should consider cloud edge providers to support use cases that require one or several of the following:

- Fast deployment and cycle times.
- Deployment of development environments and toolchains for deployments closer to end users.
- Wider area of operation (e.g., an edge supporting vehicle to infrastructure over a road network).
- Access to preoptimized edge and application offering (such as low-latency gaming).

The trend of public cloud providers stepping in to offer edge and other telecommunications-related infrastructures, is likely to continue to put significant pressure on the vendors in this space.

Business Impact: Consider the following areas of impact:

- The CSP edge IaaS provider can be beneficial for enterprises wanting to quickly connect and leverage industrially relevant applications, typically latency dependent and of an immersive nature.
- CSPs can quickly access an edge environment and focus on a specific set of use cases while leaving operational concerns to a third-party provider.
- In a market where multiple edge approaches will coexist, (such as ETSI Multi-access Edge Computing [MEC], OpenFog, ONAP etc.) this new breed of providers can enable edge cloud operation at a wider scale, sooner than that if extensive interoperability testing and integration was to occur. Skipping testing could accelerate adoption, but may not be optimal.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: AlefEdge; CloudBackend; Macrometa; MobiledgeX

Recommended Reading: "4 Hype Cycle Innovations That Should Be on the Private Mobile Networks Roadmap for 5G Security, CSP Edge and Slicing"

"Market Insight: Telecom CSP Sector Industry Product Planning, Strategy and Execution"

"Market Trends: Strategies Communications Service Providers Can Use to Address Key 5G Security Challenges"

Edge as a Service

Analysis By: Bob Gill

Definition: Edge as a service describes a model in which the edge platform, or even the edge applications themselves, are offered via provider-owned and operated assets, requiring little to no infrastructure on the part of the customer. Edge as a service can take the form of 1) "edge platform as a service" where a CSP offers development and runtime services such as within a CDNs interconnected POPs, or 2) completely managed application solutions, e.g., a hospitality package running on provider-owned hardware on the customers premise.

Position and Adoption Speed Justification: One of the greatest impediments to deploying edge computing in 2020 is the lack of broadly accepted infrastructure and operation models, leaving the enterprise to piece together solutions from still emerging technology stacks and operational models. For such critical and far reaching applications, the potential for selecting and implementing an eventual "dead end" are high, while few universal deployment models to simplify implementations exist. Edge as a service focuses on a delivery model for edge computing where a communications services provider, cloud provider, or even ISV or system integrator provides all or nearly all of the infrastructure required to deliver edge-based applications, shielding the customer from technical and market volatility. In essence, the customer is free to focus on business enabling applications rather than infrastructure building.

User Advice: While I&O must view edge infrastructure as an extension of the corporate data center or cloud, "edge as a service" allows implementers to look at edge deployments as they might a PaaS platform or hosted application model.

From the PaaS perspective, CDN and interconnection providers have begun offering "edge PaaS," whereby a customer can utilize bare metal, serverless infrastructure, or Kubernetes and containers on POP-located hardware, that is already extensively networked and interconnected on the providers' backbone networks. These platforms are particularly suitable for communications centric applications, such as optimized interactive content delivery (e.g., gaming), network path optimization (e.g., telemetry based routing), and security and management overlays.

In something akin to the traditional hosting models, "edge SaaS" packages the edge infrastructure, management, orchestration, and applications themselves into turnkey, function-specific, outcome-based application suites; examples include point of sale, restaurant or store-specific applications, and even IoT functionality, for a restaurant or QSM (Quick Service Mart) implementation. In such cases, the IT expertise of the store or franchise may be low, the number of locations high, and the application suite tightly vertically focused. Elasticity and the need for "boots on the ground" may be supplied by overnight shipment of preconfigured server/software bundles that can be simply unpacked and plugged in, allowing the systems to "phone home" and obtain configuration and update software. "Edge SaaS" provides the customer with the traditional benefits offered by a vertical-specific ISV or system integrator, for those in need of a focused and complete solution, while minimizing the technical expertise required.

Business Impact: As enterprises begin to implement edge computing, it stands to reason that long standing "build vs. buy" models will be recycled, much as they have for more traditional applications over the last four or five decades. Enterprise needs for customization and differentiation must be balanced against in-house technical expertise, their stance toward "opex vs. capex," and the breadth of the solution (targeted specific application set versus a more general distributed infrastructure platform). Edge as a service may speed the time to market for many use cases, by lowering the technical hurdles, operational expertise required, and "platform risk" present in such a nascent market.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Akamai; AlefEdge; CDNetworks; Cloudflare; Reliant Solutions; Rigado; VMware

At the Peak

Cloud-Native Telco Applications

Analysis By: Amresh Nandan

Definition: Cloud-native telco applications refer to application of cloud-native and microservices architecture to CSP operational technology applications at various levels such as virtual network functions, network management applications, operational and business support systems. These applications could be running in private or public cloud or in some cases both (hybrid cloud infrastructure).

Position and Adoption Speed Justification: Even though discussed for many years now, cloud-native is a relatively new in adoption in the telecom domain. Adoption of cloud-native architecture and principles also vary across different layers of CSP architecture. It can be seen more in BSS as compared to network functions. Across industry, it is still in early stage and on the rise in terms of interest and adoption. Inadequate benefits from earlier adoption of NFV and complexities of BSS and OSS have motivated many CSPs to adopt cloud-native approach in their operational technology. While cloud-native approach offers a number of benefits such as flexibility, agility, scalability and improved products and feature velocity; it demands new skills and new way of working. That's why cloud-native adoption will take time.

User Advice: CSPs are advised to adopt cloud-native architecture and principles in phases — so that operational readiness in terms of DevOps, CI/CD, container orchestration and automation tool chain can be assured. BSS, OSS and NFV MANO applications are good candidates for cloud-native adoption before cloud-native VNFs are implemented. Network functions differ from IT applications as they process control plane and data plane in addition to other functional requirements, with often specific performance, capacity and latency requirements. These must be understood in detail. In addition, cloud-native application management is best in an open environment — with open APIs and open tool chain. CSPs moving to cloud-native approach also need a roadmap of balancing monolithic applications and decomposed microservices-based functionalities. Such decisions require careful selection and prioritization of operational technology functions. CSPs must work with suppliers in this change process to balance the complexity and benefits of moving to cloud-native approach.

It should be noted that cloud-native mean fundamental changes and impacts both — architecture as well as operating model. Therefore relevant tools, skills, adequate structure and new processes are prerequisite to gaining efficiency. As CSPs implement cloud-native across various layers of their technology stack, they should align it to their automation goals — zero touch provisioning, service creation and closed loop service management.

Business Impact: Cloud-native approach promises a transformational impact on operations and business — helping CSPs invest and scale as per market demand instead of preprovisioning of capacity and capabilities. It can allow emulating web-scale operations as well as provide flexibility in sourcing and technology change management. A cloud-native approach can also address some of the legacy issues associated with infrastructure — network planning, design and deployment; by allowing platform as a service. Eventually CSPs can look at network infrastructure such as 5G core as a service from vendors. In operations, it can help develop a layered architecture separating core functionalities of BSS and OSS with capabilities needed for product changes and customer experience/journey management.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Cisco; Ericsson; Huawei; Mavenir; Microsoft; Nokia; ZTE

Low Earth Orbit Satellite Systems

Analysis By: Bill Menezes

Definition: Low earth orbit satellites currently provide global or regional narrowband voice and data network services, including to areas with little or no existing terrestrial network coverage. LEO systems operate at lower altitudes (1,200 miles or less) than predominant geostationary systems (about 22,000 miles). Planned LEO broadband systems of up to thousands of satellites could support significantly lower latency and, depending on system technology, broadband data speeds that are greater than throughput of current GEO and LEO systems.

Position and Adoption Speed Justification: Demand for low earth orbit (LEO) services is well-defined. A further growth driver is the lower cost of launching smaller LEO satellites, which can cost around $1 million compared with the $50 to $100 million cost of a geostationary (GEO) satellite, and can be clustered on a single launch rocket. But newer and planned systems will move slowly through the Hype Cycle given the lengthy time frames to plan and deploy them and to develop inexpensive directional antennas. Only about 53% of households globally had internet access at YE19, according to the International Telecommunication Union. Lack of broadband access hinders economic growth, thereby limiting enterprise business potential in underserved regions. However, not all of the next-generation LEO systems planned for extending broadband to at least 60% of the world's population in the coming decade will come to fruition. One of the systems closest to commercial deployment — OneWeb's 648-satellite, LEO constellation — halted with OneWeb's March 27 bankruptcy filing.

User Advice: Enterprises with current or planned business interests in remote or underserved global regions should closely follow LEO system development to align narrowband and broadband connectivity requirements for IoT and general data networking with technology capabilities and service availability. Among planned systems:

- OneWeb had launched 74 of its satellites by the time it declared bankruptcy. During 2Q19 the company began the process of trying to sell its radio spectrum, potentially enabling a successor to take over its plan. The system targets downlink speeds of multiple Gbps at round-trip latency of 10 ms to 30 ms. Terminals for fixed and mobile applications would provide a broadband satellite connection plus 2G, 3G and 4G LTE device connections.
- SpaceX venture Starlink as of 2Q19 had launched about 350 of its satellites, with plans to operate a 4,425-satcom LEO constellation providing global broadband internet access. The company scheduled launches of 180 additional satellites in 2020, targeting possible initial commercial service to North America by year's end. Global commercial broadband coverage is targeted for 2024. The full constellation will require more than 100 successful launches.
- Telesat, which already operates a number of GEO satellites, plans a constellation of 300 LEO satellites to provide global broadband connectivity. The Canadian company launched a test satellite in January 2018, targeting full commercial service in 2023.
- Amazon's "Project Kuiper" is seeking regulatory permission for a LEO constellation of 3,236 satellites to provide broadband internet access to underserved areas as well as to Amazon data-dependent services such as AWS. As of 2Q20, there was no announced service date.

Other planned or existing LEO services include those supporting narrowband data for IoT and digital imaging, or satellite phone and messaging services.

Business Impact: Planned LEO satellites will enable broadband connectivity for all remote or underserved geographies for consumer or enterprise use cases. These services also will be able to provide low-latency backhaul for terrestrial technologies such as remote cellular towers and Wi-Fi hotspots. It will possibly spur new development of those networks in areas where high costs have prevented fiber or other wired WAN backhaul connections. These systems will require customer infrastructure such as directional or phased-array antennas at manufacturing volumes large enough to make them cost-effective.

Just as significant is the use case for narrowband IoT, which requires simpler, less expensive ground antennas and only intermittent connectivity to endpoints or gateways that may be served with a small number of satellites rather than global constellations. Enterprise also may benefit for LEO backhaul for private networking in use cases such as manufacturing, healthcare or natural resources.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Amazon; Iridium; ORBCOMM; SpaceX; Telesat

Recommended Reading: “Market Insight: New Satellite Constellations Enable Revenue Opportunity for CSPs to Complement IoT Connectivity Services”

“Satellite Communications Strengthen Resilience Planning”

“Market Trends: New Satellite Constellations Will Provide Revolutionary Opportunities for Connecting the IoT”

Edge AI

Analysis By: Alan Priestley; Erick Brethenoux; Eric Goodness

Definition: Edge AI refers to the use of AI techniques embedded in IoT endpoints, gateways and edge servers, in applications ranging from autonomous vehicles to streaming analytics. While predominantly focused on AI Inference, more sophisticated system may include a local training capability to provide in-situ optimization of the AI models.

Position and Adoption Speed Justification: Edge AI will be implemented in a range of different ways, depending on the application and design constraints of the equipment being deployed — form factor, power budget (i.e., battery powered vs. mains powered), data volume, decision latency, location, security requirements etc.:

- Data captured at an IoT endpoint and transferred to an AI system hosted within an edge computer, gateway or aggregation point: In this architecture, the IoT endpoint is a peripheral to the AI system. The endpoint acts as a data gatherer that feeds this data to the AI system. An example of this is environmental sensors deployed for a smart agriculture application.

- AI embedded in the IoT endpoint: In this architecture, the IoT endpoint is capable of running AI models to interpret data captured by the endpoint and drives some of the endpoints' functions. In this case, the AI model (e.g., a machine learning model) is trained (and updated) on a central system and deployed to the IoT endpoint. An example is a medical wearable that leverages sensor data and AI to help visually impaired people navigate the world in their daily lives.

The applications that are starting to see increasing adoption of edge AI include those that are latency sensitive (e.g., autonomous navigation), data intensive (e.g., video analytics), and require an increasing amount of autonomy for local decision making. While many of these applications are still in R&D or trial phases, and widespread adoption is at least a few years away, other such as video analytics (leveraging deep learning methods and deployed as deep learning models at the endpoints or in edge servers) are starting to see adoption — driven by the rapid growth in deployment of surveillance cameras and the need for real-time interpretation of captured video streams.

User Advice: Enterprise architecture and technology innovation leaders should:

- Determine whether the new AI developments in machine learning (ML) are applicable to their IoT deployments, or whether traditional centralized data analytics and AI methodologies are adequate.
- Evaluate when to consider AI at the edge vs. a centralized solution. Applications that have high-communications costs are sensitive to latency, or ingest high volumes of data at the edge are good candidates for AI.
- Assess the different technologies available to support edge AI and the viability of the vendors offering them — many potential vendors are startups, which may have interesting products but limited support capabilities.
- Estimate carefully and pragmatically the appropriate level of autonomy and trustworthiness for AI systems deployed on edge systems.
- Assess the risk associated with the nondeterministic nature of many AI techniques where it may not be possible to control or replicate the analysis results.
- Use edge gateways and servers as the aggregation and filtering point to perform most of the edge analytics functions. Make an exception for compute-intensive endpoints, where AI-based analytics can be performed on the devices themselves.

Business Impact: By incorporating AI techniques at the edge, enterprises may be positively impacted as follows:

- Improved operational efficiency, such as enhanced visual inspection systems in a manufacturing setting.
- Enhanced customer experience, with faster execution time, performed at the edge.

- Reduced latency in decision-making, with the use of streaming analytics and migration to an event-based architecture.,
- Communication cost reduction, with less data traffic between the edge and the cloud.
- Increased availability even when the edge is disconnected from the network.
- Enhanced local decision autonomy for edge systems.
- Reduced storage demand through a more reactive exploitation of the data and a better estimate of its potential obsolescence.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Amazon; Baidu; Google; Huawei; Intel; Matroid; Microsoft; Neurala; NVIDIA; Qualcomm

Recommended Reading: "Exploring the Edge: 12 Frontiers of Edge Computing"

"5 Questions a Product Manager Must Ask When Creating an AI-Enabled Edge Product Strategy"

"Use Edge AI to Drive Revenue Growth, Forecasting, Customer Engagement and Workforce Planning"

"Cool Vendors in AI Semiconductors"

Network Slicing

Analysis By: Peter Liu

Definition: Network slicing is a form of virtual network technology. It allows a network-based CSP to create multiple virtual networks in the form of a "network slice," on top of a common shared physical infrastructure. Each slice can be customized to have its own network architecture, engineering mechanism, network provisioning methodology, configuration and service quality profile based on the requirements that it serves.

Position and Adoption Speed Justification: Network slicing emerges as an essential technique in 5G networks to accommodate different and possibly contrasting quality of service (QoS) requirement (5G Network Slicing). The realization of this service-oriented view of the network leverages on the concepts of software defined network (SDN) and network function virtualization (NFV) that allow the implementation of flexible and scalable network slices on top of a common Infrastructure.

From a business model perspective, each network slice can be administrated by a mobile network operator (MNO), mobile virtual network operator (MVNO) or a solution provider. The infrastructure provider (the owner of the telecommunication infrastructure) can also leases its physical resources to the MVNOs that share the underlying physical network. According to the availability of the assigned resources, a MVNO can autonomously deploy multiple network slices that are customized to the various applications provided to its own users.

Key characteristics of network slicing include the following:

- Each network slice comprises an independent set of visualized network functions that support a particular use case.
- Each slice is completely isolated in operations so that no slice can interfere with the traffic in another slice.
- Each slice is configured with its own network topology, engineering mechanism and network provisioning. It normally contains a slice management function that may be controlled by the CSP or the customer, depending on the use case.

Network slicing always link with 5G and especially a stand along (SA) 5G deployment as well as Edge computing. As the 5G commercial rollout has begun in various countries, network slicing has become a hot differentiating feature. More CSPs have started evaluations and trials of network slicing. They include BT, China Mobile, Deutsche Telekom (DT), SK Telecom (SKT) and Vodafone U.K. CSPs in China will start deploying the stand-alone 5G and MEC in large scale in 2020, which we believe will accelerate the network slice maturity and enable more innovation opportunities.

Network slicing and related management activities are being trialed by some CSPs and their vendor partners. In the beginning of 5G SA deployment, commercial cases will mainly focus on the core network slicing. Full Dynamic network slicing and end-to-end slicing (including RAN) will take longer time.

User Advice:

- CSPs should focus now on infrastructure transformation, including NFV, SDN, cloud RAN, edge computing and cloudification initiatives, since those are the fundamental technologies that enable network slicing.
- Network slicing management requires certain new components in the technology stack. CSPs should identify the architectural changes well in advance, while adopting NFV technologies to facilitate network slicing even at a later stage.
- Network slicing is one of the key technologies in the 5G era, and CSPs should evaluate and trial network slicing by working closely with vendors.
- CSPs should be practical and plan static network slicing with a focus on core network and key vertical use cases, such as entertainment, manufacturing and connected car.

Business Impact: Network slicing offers a more efficient approach to building a mobile network, which is essential in creating multiple networks on a single common platform that potentially disrupts the traditional single network for all business models. CSPs can run multiple independent business operations or business models on a common physical infrastructure. This increases infrastructure utilization and economic efficiency, and it also helps generate new business models, especially for vertical industries.

With network slicing, business customers will be able to access highly customized network slices tailored to specific requirements in a cost-effective, timely and efficient way. It will also allow businesses to optimize their current services and create new offers that otherwise wouldn't have been possible.

Long-term, network slicing will create a new type of service provider that doesn't have a physical infrastructure, but purchases a virtual network slice from a single network-based CSP that has been optimized for the services it provides.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Ciena; Cisco; Ericsson; Huawei; Intel; Mavenir; Nokia; Samsung; ZTE

Recommended Reading: "CSP CIOs' Role in 5G Platforms as Accelerators for New Value Creation Across Industries"

"Market Guide for 5G New Radio Infrastructure"

"Innovation Opportunities Will Be Enabled as 5G Evolves Through 2025"

"3 Key Enterprise Networking Hype Cycle Innovations in CSPs' Roadmap for Manufacturing"

vRAN

Analysis By: Kosei Takiishi

Definition: Virtualized radio access network (vRAN) is a next-generation architecture that aggregates baseband processing functions to the server cloud, for many radio access nodes. While current distributed RAN (dRAN) and centralized RAN (cRAN) use dedicated bare-metal hardware for base band unit (BBU) in a base station, vRAN usually uses software including virtualized BBU which can run on white-box hardware servers.

Position and Adoption Speed Justification: cRAN (where the dedicated hardware's BBUs for each base station are moved to a shared, centralized pool) has been deployed by several leading communication service providers (CSPs) (including SK Telecom, KT and NTT DOCOMO). Although, they are yet to launch vRAN, for the most part: SK Telecom announced the successful implementation of the world's first vRAN in a 4G LTE commercial network in 2016, and Nokia published that the world's first commercially deployed cloud-based 5G radio access network is live in North America in 2019. Gartner estimates that these initiatives would be focusing on providing advanced marketing message for their branding rather than pursuing the real benefit of vRAN adoption.

As a vision and a long-term strategy for CSPs, cRAN will evolve to vRAN because CSPs can use their central offices for vRAN as new micro data centers which can host not only for their network enhancement such as vEPC and virtualized Internet of Things (IoT) gateways but also for mobile edge computing for new business opportunities. Mobile edge computing will provide for newer services that can leverage lower latency and geographic presence.

One early example is Rakuten's 4G LTE vRAN in Japan, which could be the first commercial deployment in the world. Rakuten has a lofty ideal to innovate the telecom sector by adopting fully virtualized cloud-native network and plan to sell its platform and best practices to other CSPs.

The software-based nature of vRAN is treated as a cost-effective approach to replace the traditional, distributed RAN architecture to enable new serviceability and simplified deployment approach.

- vRAN is treated as a cost-effective approach to replace the traditional bare-metal hardware base stations but this has not yet achieved the conclusive evidence.
- Interoperability issues between different radio equipment vendors.
- Performance concerns related to white box especially power consumption by external FPGA board.
- Cloud-based (software) processing is inherently less efficient than using dedicated hardware using application-specific integrated circuit (ASIC) chips.

User Advice: vRAN is now attracting incumbent mobile CSPs but what Rakuten is doing mostly cannot be acceptable for most of mobile CSPs, because Rakuten is a new greenfield CSP and can adopt state-of-the-art techniques from scratch. On the other hand, incumbent CSPs possess siloed massive network resources locked in by their vendors. these CSPs should:

- Prioritize new technologies that are most needed for sustainable development and operational efficiency. vRAN is one of the candidates.
- Clarify bottlenecks, difficulties and immaturity in case you follow Rakuten by discussing feasibility with your incumbent vendors

As a vision, this vRAN and virtualization of other access components also provide an option for fixed-mobile convergence and CSPs should look at evolving their network architecture while adopting vRAN.

Business Impact:

Future applications, such as content delivery network (CDN) services at the mobile edge, are emerging within cloud-based offerings, as well as localized caching and location-based service applications — aggregating signaling from such platforms. As network functions become virtualized under NFV, watch for further radio applications within cloud-based systems, including controllers providing seamless roaming and mobile video optimization functions. This may form the architecture of choice for future 5G standards.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Altiostar; Cisco; Mavenir; Nokia; ZTE

Recommended Reading: "Lessons Learned From Rakuten's Fully Virtualized and Cloud-Native 4G Network"

5G

Analysis By: Sylvain Fabre

Definition: 5G is the next-generation cellular standard by the 3rd Generation Partnership Project (3GPP). The standard targets maximum downlink and uplink throughputs of 20 Gbps and 10 Gbps respectively, latency below 5 milliseconds and massive scalability. New system architecture includes core slicing as well as wireless edge.

Position and Adoption Speed Justification: Seventy-three operators have announced 5G rollouts (Source: Global mobile Suppliers Association [GSA], April 2020), just under 9% (up from 5% one year ago) of mobile networks.

3GPP Release 16 freeze date has been postponed due to the COVID-19 pandemic, with a freeze target date of mid-2020.

5G encompasses a range of 3GPP standards focused on different functionality:

- R15: Extreme broadband (5G NSA and then 5G SA)
- R16: Augmentations for Industrial IoT (massive IoT, slicing and security improvements)
- R17: Augmentations for wider ecosystem expansion (freeze target date end of 2021)
- R18: Additional augmentations (e.g., extra territorial 5G systems, railway smart station services)

Due to this phased introduction, and the time required from the vendors' ecosystem to build standard compliant networks and grow silicon and device availability, Gartner expects the full potential for 5G use cases to materialize first in 2022.

Use of higher frequencies and massive capacity, will require very dense deployments with higher frequency reuse. Here we see regional differences, whereby mmWave will be leveraged in the U.S. and South Korea, but may not see initial adoption elsewhere.

Gartner expects many 5G deployments to initially focus on islands of deployment, without continuous national coverage.

Less than 45% of CSPs globally will have launched a commercial 5G network by 2025. Uncertainty about the nature of the use cases and business models that may drive 5G is currently a source of uncertainty for many CSPs, enterprises, and technology and service providers (TSPs). Gartner estimates that 5G capable handset penetration will reach 50% in 2023 in Western Europe, and could be a little faster in North America.

We are seeing different dynamics by regions, where in many parts of Africa for example, 5G would not be the next step to lower bandwidth services, and handset cost may be an inhibitor for lower income subscribers. Adoption is more aggressive in APAC and NAR, with Europe cautiously enthusiastic — and the developing world lagging.

User Advice: TSP product managers should:

- Focus mobile infrastructure planning on LTE, LTE-A, LTE-A Pro, small cells and heterogeneous networks (HetNets), as part of a planned transition toward 5G.
- Ensure backward compatibility to preceding generation (LTE) devices and networks. This is necessary because 5G coverage may be limited, so new 5G devices need to be able to seamlessly transition to 4G fallback infrastructure for uninterrupted service.
- Focus on related architecture initiatives — such as software-defined network (SDN), network function virtualization (NFV), CSP edge computing, distributed cloud architectures and cloud native containerization, as well as end-to-end security in preparation for 5G.
- Provide solutions where new frequency allocations (preferably) should be used for the latest technology — 5G — to benefit from lower cost per byte, higher bandwidth and more capacity.
- Help CSPs refine generic services to vertical-focused solutions (B2B) for 5G.
- Have a clear understanding of specific verticals and their use cases for more effective consultative selling of their 5G solutions.
- Build their ecosystem of partners to target verticals more effectively with 5G.

Enterprise business leaders should:

- Identify use cases that definitely require the high-end performance of 5G; these may be few or even nonexistent for many verticals.
- Evaluate the multiple IoT alternatives available that may prove adequate, more available and more cost-effective than 5G for many use cases (e.g., low-power wide-area [LPWA] such as NarrowBand Internet of Things [NB-IoT], long-range [LoRa], Wireless Smart Ubiquitous Networks [Wi-SUN]).
- Clarify the level of complexity involved in operating a private 5G network.
- Evaluate options for CSPs or other providers to be involved in running the 5G network.

Business Impact: Gartner Enterprise 5G Surveys indicate that vertical use cases with 5G would be first motivated by operational cost savings. Another driver is agility — in particular, in oil and gas and manufacturing.

In addition, the vertical users for 5G appear to value lower latency from ultrareliable and low-latency communications (URLLC) and expect 5G to outperform rivals in this area.

With massive machine-type communications (mMTC), scenarios of very dense deployments can occur, supported by the 5G target of 1 million connected sensors per square kilometer.

5G enables, principally, three technology deployment and business scenarios, which each support distinct new services, and possibly new business models (such as latency as a service):

- Enhanced mobile broadband (eMBB) supports high-definition video.
- mMTC supports large sensor and IoT deployments.
- URLLC covers high availability and very low latency use cases, such as remote vehicle/drone operations.

URLLC and mMTC will be implemented after eMBB. Only eMBB addresses the traditional mobile handset requirement of ever higher throughput. URLLC addresses time critical industrial applications such as automation, with latency around 1ms over a limited range for a limited number of connections — where reliability and latency requirements surpass bandwidth needs. Finally, mMTC addresses the scale requirements of IoT. Apart from some smart city scenarios, mMTC may not be required in most locations for some years, with NB-IoT and other LPWA such as LoRa being sufficient for a while.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Cisco; Ericsson; Huawei; NEC; Nokia; Samsung; ZTE

Recommended Reading: “Market Guide for 5G New Radio Infrastructure”

“Assessing 5G Mobile Technology for Organizations”

“How to Select 5G NSA/SA Migration Paths”

“Forecast: Communications Service Provider Operational Technology, 1Q20 Update”

“Market Trends: Strategies Communications Service Providers Can Use to Address Key 5G Security Challenges”

“Reduce Privacy Risks When Using 5G Products and Services”

mmWave

Analysis By: Bill Ray

Definition: mmWave is the frequency band between 30GHz and 300GHz, where the wavelength varies between 10 mm and 1 mm, respectively. However, nearby bands including 24 and 28GHz are also commonly referred to as "mmWave." The 5G mobile telephony standard extends into several mmWave bands, which are also used for point-to-point wireless communication and satellites links.

Position and Adoption Speed Justification: The addition of mmWave bands to the 5G standard has focused a great deal of attention, and investment, on what was (hitherto) a band used only by specialists and niche applications. The U.S., in particular, has been active in deploying 5G networks into mmWave and China has announced plans to allocate mmWave frequencies to its domestic operators. mmWave is attractive because it is largely unoccupied, so it can provide very high capacity, but it's poor penetration and propagation makes deployment of blanket coverage expensive and complicated.

The WiGig standard (802.11ad and 802.11ay) uses mmWave at 60GHz but has achieved little commercial success despite being available for more than a decade. The limited range, and the increasing speed of Wi-Fi, prevented WiGig from being adopted outside a few niche applications (such as wireless VR headsets). However, the adoption of mmWave in 5G has triggered investment in, and mass production of, mmWave antennas and transceivers, reducing the cost of equipment capable of operating in the band.

This innovation is further driven by the release of large blocks of mmWave into the public domain. In 2019 the U.K. regulator Ofcom has released 2.24GHz of spectrum around 24GHz for unlicensed use indoors, while the U.S. regulator Federal Communications Commission (FCC) released 14GHz of spectrum at 60GHz (including the band used by WiGig). These allocations are intended to spur development of new standards, and new applications, for high-speed, short-range, wireless connections.

Investment in 5G is creating new antenna designs and beamforming techniques which will benefit all applications of mmWave, increasing the utility while decreasing the cost of deployment. Phased-array mmWave antennas capable of accurately directing radio signals are a necessity for the next generation LEO satellite constellations. The technology can also be used for highly-accurate location tracking and for using reflected signals to improve the coverage of mmWave systems.

The publicity around 5G has driven mmWave to the top of the Hype Cycle very quickly, and it is now descending as 5G customers find that the bandwidth they get does not match with what was promised by network operator. This, combined with spurious concerns over the safety of mmWave, will push the technology into the trough of disillusion over the next year or two.

User Advice: Anyone looking for point-to-point, or point-to-multipoint, links should include mmWave in the technologies being evaluated. The limited range, and highly-directional, nature of mmWave means that license-free (or light license) systems can operate without fear of interference, and at much lower cost, than licensed systems. Campus networks should consider mmWave point-to-multipoint systems for backhaul of private LTE cells or Wi-Fi access points, especially where clear line of sight is available.

Equipment to run such links is already available but is also developing quickly as enhancements created for 5G networks filter into the rest of the industry. Users should expect to see costs falling rapidly over the next couple of years (following a similar path to the drop in pricing of equipment using microwave frequencies, once that was incorporated into the 4G standard).

Business Impact: The availability of mmWave bands provides plenty of bandwidth. In many instances mmWave will be able to replace wired connections, with ultra-reliable connectivity (using simultaneous connections to multiple access points) making it as reliable (if not more reliable) than wired connectivity. This will enable production lines to reduce the cable loom, increasing flexibility and reducing maintenance costs. Stationary equipment is ideally suited for highly directional mmWave signaling, but with beamforming and other optimization techniques mmWave rapidly becomes suitable for robots and other mobile endpoints.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Metawave; Qualcomm; Renesas Electronics; Texas Instruments

Recommended Reading: “Market Trends: mmWave Opportunities Outside Smartphones”

“Don’t Expect 5G to Replace Wired Access WANs Anytime Soon”

Sliding Into the Trough

Network as a Service (NaaS)

Analysis By: Gaspar Valdivia; To Chee Eng

Definition: Network as a service (NaaS) is a standardized, highly automated offering, where network products, services and operations are consumed by enterprises as a service. NaaS can be offered across the LAN, WAN and/or data center by communication service providers that may own or not the network. NaaS offers often leverage SDN and network automation and are combined with VNF marketplaces enlarging value to enterprise customers. Provider’s web portal is used by customers to self-provision the NaaS components, often charged on a pay per usage basis.

Position and Adoption Speed Justification: A growing number of global communications service providers (CSPs) are investing in NaaS and virtual network function (VNF) marketplaces. These CSPs are evolving to a platform approach for service management for their NaaS offers and have adopted software-defined network (SDN) and network function virtualization (NFV) to decouple data plane for control plane and network hardware from software.

TM Forum and Metro Ethernet Forum (MEF) have carried out initiatives joined by carriers and technology vendors to define a common framework on how telecom service providers build and deliver NaaS. They assess what elements needs to be homogenized in the industry and provide definitions on elements such as service metrics and service orchestration and standardize service information models and application programming interfaces (APIs) to enable interconnection of services across networks. However, intercarrier connections are still mostly pending.

Today, most CSPs still lack a comprehensive NaaS platform. They have limited offers in their VNF marketplaces in breadth (just some network functions), depth (limited pretested services chains) or geographic reach (offering bandwidth on demand [BoD] but only for some connectivity services in selected countries). Legacy and complex systems (BSS and OSS) and processes, siloed organizational structures, lack of appropriate skills are among the most common barriers.

Enterprise's uptake of CSP's NaaS offering is still rather limited. Over time, as CSP's capabilities develop aligned with standards and enable end-to-end service orchestration across networks and technologies, and service catalogs get populated, Gartner expects NaaS will gain further market traction.

User Advice: Deploying NaaS requires end-to-end automation of service orchestration and life cycle management across cloud-based and hybrid infrastructure, both in IT and network domains. NaaS includes processes such as endpoint authentication and authorization, service provisioning and QoS management. A master service catalog together with a common information model framework across domains and standards-based APIs are key components of a CSP's NaaS implementation.

For CSPs, operational success of NaaS, VNF as a service (VNFaaS), and increasingly containerized network functions (CNF), will require the adoption of a digital business technology platform approachable to meet internal and external requirements from customers and ecosystem partners. As CSPs evolve their NaaS portfolios, they must provide partners with modules, tools and processes to test, certify and onboard VNFs. If not yet deployed, CSPs should build NaaS platform capabilities to enable on-demand enterprise service delivery and consumption-based commercial models for network services. Typically starting with bandwidth on demand on MPLS, Ethernet and/or internet services and cloud connects. CSPs should:

- Adopt NaaS using a platform approach for enterprise services design, deliver and support a service factory model for operations. Begin by developing a blueprint of target services architecture and deploying specific modules to that target architecture.
- Expose network APIs for partners and developers so they can leverage underlying platform capabilities to add to your offerings or build their own services.
- Combine NaaS platform capabilities with a VNF marketplace for enterprise network services that customers can consume on as-a-service commercial model either directly from the NFV network POPs or onboarded on on-premises universal CPEs.
- NaaS and VNF marketplace platforms should include service/VNF catalogs, license management, revenue management, self-service and support and robust life cycle management process and tools.

Business Impact: Deploying NaaS requires from CSPs upfront investments in network and operation transformation for increased agility, automation and cost-efficiency in service delivery. CSPs can use NaaS to offer more flexible, consumption-based commercial models such as bandwidth on demand on WAN connections as well as to enhance the user experience they offer to their enterprise customers. Flexible and scalable services, real-time configuration, ease of management through service web portals and full-service automation become key service attributes. The combination with VNF marketplaces allows for easy consumption of value-added services such as security, WAN optimization or SD-WAN services.

Advanced analytics, cloud, virtualization, microservices, open source will also bring opportunities for CSPs to untap new revenue streams with NaaS. An example could be mobile private networks including NaaS orchestration of service life cycle for 5G network slicing capability. Usage of AI in network operation and maintenance, and self-optimization, self-healing capabilities will also build into the NaaS-enhanced services.

CSP's exposure of network APIs can allow partners and developers to add to CSP's offering as well as to leverage and combine underlying platform capabilities with others from third-party providers (such as Amazon or The Walt Disney Co.) to build their own services. That would create new revenue streams for CSPs.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Arista Networks; Arista Networks (Big Switch Networks); Cisco; Dell; Ericsson; Hewlett Packard Enterprise (HPE); Huawei; Juniper Networks; Nokia; VMware

Recommended Reading: "2019 Strategic Roadmap for Networking"

"Market Guide for CSP Operations Support System Solutions"

"Market Opportunity Map: Enterprise Network Services, Worldwide"

"Magic Quadrant for Network Services, Global"

"Debunk the Misperceptions About Network as a Service"

CSP AI

Analysis By: Peter Liu

Definition: Artificial intelligence (AI) applies advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions. "CSP AI" refers to how communications service providers (CSPs) leverage AI and machine learning technology to improve customer experience, reduce costs, generate new revenue opportunities, and optimize their IT and infrastructure operations.

Position and Adoption Speed Justification: AI promises to be one of the most disruptive and innovative classes of technologies in the next 10 years and has been identified as top game-changer technology by CSP CIOs (refer to "2019 CIO Agenda: A CSP Perspective"). Further, 40% of the CSP CIO respondents are already implementing or plan to implement AI within 12 months. The disruptive nature of AI is a result of the increasing demand for vendors to create insights and outcomes from advances in emerging AI technologies and techniques.

The early promise and function of the AI technology in telecom industry are mostly focused on improving existing operations, enhanced audience analysis and segmentation.

CSPs have been using virtual assistant (VA), analytics and machine learning-related technologies for years, mostly focused on improving existing operations, and enhancing audience analysis and segmentation. Major CSPs in developed markets have, to some extent, been leveraging advanced analytics, artificial intelligence and automation (AAA)-related technologies, aiming to empower and enable various capabilities, process and technologies such as network optimization, self-organizing network (SON), and customer engagement.

An increasing number of CSPs are exploring use cases for AI, and many are already in the initial phases of a pilot or proof of concept. Leading CSPs, such as AT&T, Orange, Telefonica and Vodafone, are combining data analytics capabilities with AI and automation to differentiate themselves further.

However, the legitimate excitement about the transformative power of AI leads to unrealistic expectations within the CSPs (further buttressed through hype by solution providers) and the loose link between theoretical/conceptual frameworks and their business value fuels a deepening skepticism. Therefore, very few of the AI projects make it to live deployment. The industry is at risk of getting stuck in “proof-of-concept purgatory” — a limbo state where AI stalls and never reaches its full potential. Subsequently these lead to lack of leadership support for AI initiatives and competing priorities for investment.

We do, however, forecast that CSP AI and machine learning technologies will take a relatively long time to reach the Plateau of Productivity. Barriers include the nascent and expensive nature of the technology and the execution strategy. CSP AI also requires specific expertise and rare skill sets, which most CSPs lack. Other challenges include a lack of good-quality data for training sets and process changes to enable new automations.

User Advice: Expect effective adoption of AI to be a learning journey. Don’t be afraid to start small with modest, straightforward projects, such as simple algorithms in network planning and next-best offers or including automation in areas with a lot of manual, repetitive work. At the same time, think big. Plan for an architecture that supports AI across all business functions in the organization, and use early projects as learning platforms for more-complex midterm projects.

Obtain senior management and business support for projects needed to underpin AI and machine learning, since there will be many personnel hours needed to complete data cleansing, system integration and process fixes.

Invite sourcing to participate in business outcome meetings. This can help ensure that supplier RFPs minimize the chance of vendor lock-in by including questions that uncover the supplier’s attitude to risk sharing and co-creation on projects that include nascent technologies.

Business Impact: The benefit of AI is very wide, and almost all CSP functions can benefit from it.

AI drives improvements and new solutions to business problems across a vast array of business, consumer and operation areas. Key applications include:

- **Intelligent network operations.** AI makes it possible to derive value from this network data and to shift network operations from being reactive to being data-driven, predictive and proactive operations. This results in higher efficiency and lower operating expenditure.
- **Process automation.** Larger CSPs already have multiple small robotic process automation initiatives, but the delivery of truly "intelligent" automation of major processes is still some years away. CSPs are evaluating early products that provide machine learning to find the root cause of issues and to determine the simple next best action in individual parts of a process.
- **Virtual customer assistant (VCA) and augmented cognition.** Leading CSPs have already implemented VCAs to help them improve their customer engagement. By using AI algorithms that analyze vast amounts of customer data and through natural language processing, intelligent chatbots can gain a better understanding of the customer. They can also combine historic and behavioral patterns with ongoing real-time engagement data to determine the best action at the best moment of the customer journey.
- **Personalization service design.** New pattern detection techniques can improve adoption of campaigns and enhance the ability to understand and respond to customer experience needs.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Aria Networks; Ericsson; Guavus; Huawei; IBM; Mavenir; Nokia; Nuance Communications; Oracle; P.I. Works

Recommended Reading: "Market Insight: Unleash the Potential of AI in Telecom 5G Era"

"Top 10 Trends for the Communications Service Provider Industry in 2020"

"CSP CIOs Enable Business Outcomes Through AI Augmented Talent and Decision Making"

eSIM

Analysis By: Pablo Arriandiaga

Definition: The embedded SIM (also called eSIM or eUICC) is a programmable subscriber identity module (SIM) that is physically embedded into a mobile device. It is designed to remotely manage multiple CSPs profiles and be compliant with GSMA specifications. An eSIM is provisioned over-the-air (OTA) with operator credentials, giving users the ability to change providers. eSIMs should not be confused with "soft" SIMs (iSIMs or virtual SIMs) that store operator secret credentials in software. These are not included here.

Position and Adoption Speed Justification: GSM Association (GSMA) standards' work, first in IoT and later with consumer sectors, has increased potential innovation for OEMs and other players. More than 200 MNOs worldwide support eSIM and adoption is accelerating, mainly in consumer devices, driven by cases such as wearables, trackers or tablets where size and/or placement, mobility, update frequency, and life cycle are important. In consumer devices, the increasing support of main OEMs for eSIMs in their new 4G and 5G smartphones will also act as a trigger for accelerating adoption.

In IoT, the main driver is the connected car, but other areas such as utilities and logistics are also driving adoption as well. In IoT most use cases are using eSIM as insurance to avoid future lock-in. However, MNOs are reporting low use compared to their IoT installed base. Additional challenges are that GSMA needs to evolve the standards to solve battery problems for NB-IoT that are required for use cases such as utilities as an alternative to 2G networks.

User Advice: Enterprises using IoT solutions need to evaluate the eSIM service offer by CSPs or IoT MVNOs acting as prime contractors by assessing MNOs supporting each by country including version of the standard supported, and interoperability with other eSIM subscription management platforms. In 3GPP LPWA IoT solution users need to understand the impact of updating profiles OTA on the battery life and the feasibility of doing it using the data throughputs that those technologies support. Other solutions such as iSIM or nuSIm (not covered in this profile) could be an alternative if providers show commitment to support future standardize versions.

OEMs should continue to promote eSIM in designs where its advantages are attractive, for example use cases swapping cellular providers regularly across countries and with big amounts of data. OEMs should also work with the GSMA and CSPs to present end users with a superior solution and a balanced playing field for new and innovative offers.

CSPs must craft an evolution plan to efficiently support the shift to eSIM and take advantage of emerging opportunities leading to competitive differentiation. Leverage the flexibility of eSIM to attract new customers with superior service offerings that also motivate existing users to stay (for example, by eliminating per-device fees and instead bundling in content, wearables and more).

CSPs must ensure that their eSIM technology is compatible with a variety of different handset manufactures and eSIM vendors, to ensure they can support multiple download and activation methods. In addition, evolve their billing support systems with advanced eSIM management capabilities.

Business Impact: Businesses with a large number of mobile devices used by their employees will also benefit from the convenience of eSIM for minimizing roaming tariffs when roaming. eSIM can deliver a streamlined user experience for managing cellular connectivity, enabling IT teams to provision and deploy new devices in a rapid and convenient fashion.

For OEMs, eSIM uses less space and is cheaper than traditional SIM technology. This means that mobile connectivity can now be introduced into hardware where it was previously not feasible due to cost or space restrictions.

CSPs can gain new business opportunities from a world of intelligently connected services and devices, reduce the logistical costs associated with handling traditional SIM cards and retain existing SIM security. In addition, eSIM is the vital enabler for the future growth of the IoT market allowing CSPs and IoT MVNOs to provide local connectivity worldwide in a cost-effective way and move from a pure connectivity play to a platform play.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Apple; Arm; EMnify; Ericsson; Gemalto; Giesecke+Devrient; IDEMIA; Samsung Electronics; Sierra Wireless; Truphone

Recommended Reading: “Magic Quadrant for Managed IoT Connectivity Services, Worldwide”

“Critical Capabilities for Managed IoT Connectivity Services, Worldwide”

“3 Automotive Hype Cycle Innovations That Should Be on Your Connected Vehicle Roadmap”

“Market Guide for Internet of Things Mobile Virtual Network Enablers”

NB-IoT

Analysis By: Kosei Takiishi

Definition: Narrowband-Internet of Things (NB-IoT) is a low-power wide-area (LPWA) wireless connectivity protocol designed to coexist with LTE and 5G networks. It is a 3GPP standard, first standardized on its Release 13 in 2016; its key features include bidirectional communications and throughput of several tens of Kbps using licensed spectrum. Officially known as “LTE Cat NB1,” it enables more-economical module cost and a greater maximum power efficiency than LTE-M Cat M1. This analysis of the technology also covers further Cat NB specifications.

Position and Adoption Speed Justification: NB-IoT, along with Long Term Evolution for machine-type communications (LTE-M; also known as “LTE Cat M1”), is the 3rd Generation Partnership Project’s (3GPP’s) effort to address the emerging LPWA market for supporting use cases for IoT in a WAN setting.

As with other LPWA technologies, its key focus areas include low data rate, low power consumption and low module cost. This is because the target use case is for connected devices that typically have a long life, low data rate and volume, together with a sporadic transmission frequency.

One of the advantages of NB-IoT is that it can use the existing LTE spectrum that mobile network operators (MNOs) have been allocated. In addition, NB-IoT can mainly be rolled out via a simple software upgrade on existing LTE infrastructure. LTE Cat NB2 is also standardized by 3GPP Release 14 in 2017. Major upgrades from Cat NB1 include peak data rate improvement up to 120 Kbps, supporting positioning and single-cell multicast and energy/latency optimization. Cat NB2 enhancement is covered by 3GPP Release 15 in 2018 by adding new wake-up signal to decrease power consumption and TDD support. Globally, 93 CSPs have already commercialized NB-IoT based on GSMA as of January 2020. Among them, China is moving much faster in terms of NB-IoT adoption than the rest of the world. Given the size of the Chinese market, this affects the global overall speed of adoption as well.

User Advice: Product leaders in mobile CSPs should:

- Focus LPWA efforts on NB-IoT and LTE-M. Though it is worth noting that NTT DOCOMO in Japan shut down its NB-IoT service in 2020, so there is a need to observe major CSPs' decisions carefully.
- Test NB-IoT for more-demanding industrial use cases, as NB-IoT supports authentication (which is supported by the SIM card on mobile devices in 3GPP) and also boasts high reliability, which a licensed spectrum operation supports better than unlicensed alternatives.
- For IoT deployments involving the Chinese market, give NB-IoT a high priority in the near term.
- For deployments outside of China, use NB-IoT on the basis that investing in the standard will be a long-term play but a low-risk strategy — while planning for continuous evolution (such as 5G massive machine-type communications [mMTC] and Cat NB2).

Business Impact: No IoT connectivity protocol is necessarily better than another, but each caters to a different set of business requirements. Among LPWA alternatives, NB-IoT will address the needs of use cases with higher requirements for reliable connectivity, higher SLAs and robust 3GPP security. The main difference between NB-IoT and other fully or partially proprietary LPWA technologies (such as long-range [LoRa] and Sigfox) is that NB-IoT is a 3GPP standard. It will be deployed in a majority of mobile CSPs, which will benefit from the stronger and richer 3GPP ecosystem; though it is worth noting that interoperability is not guaranteed as different network operators are deploying NB-IoT in different frequency blocks. Finally, as an extension of LTE, NB-IoT will be deployed within mature networks, with established operational and customer experience management key performance indicators (KPIs) and practices, along with mature systems such as self-organizing networks (SONs) and IT support systems.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Arm; China Mobile; Ericsson; Huawei; Nokia; Qualcomm; Quectel; u-blox; Vodafone; ZTE

Recommended Reading: "Market Trends: CSPs Must Focus on NB-IoT and LTE-M for Their LPWA Strategies"

"Exploit LPWA Networks Now — 5G Won't Change Them"

Shared Spectrum Access

Analysis By: Kosei Takiishi

Definition: Shared spectrum access is based on the concept of sharing licensed access to a currently infrequently-used piece of spectrum by adopting IT to find unused radio spectrum and optimize its usage. In the U.S., the current shared band is citizens broadband radio service (CBRS) and opens a 150 MHz piece of spectrum in the 3.5 GHz band and plans are in place for 6 GHz. Other country regulators are considering shared spectrum licenses, often for 5G use.

Position and Adoption Speed Justification: While any incumbent users of this shared spectrum frequency bands have priority (for example, the Navy in the U.S.), other license holders are permitted, providing they do not create interference. Portions of the frequency allocation can be licensed to registered service providers or enterprises at a particular location (such as a campus environment, a city environment or indoors) and other parties may be allowed a third grade of access if spectrum is available. A spectrum access system (SAS) manages any potential conflict between authorized users. CBRS, followed by other licensed shared access (LSA) long-term evolution (LTE) frequency schemes, could have been described as the hot small cell technology at the beginning of 2017. Delays in the Federal Communications Commission (FCC) certification and auction process have put things on hold, but CBRS auction will finally start in July 2020. In the meantime, momentum has been building up with cellular operators, cable multiple-system operators (MSOs), wireless internet service providers (WISPs), neutral hosts and system integrators all keen to exploit opportunities. CBRS capable devices such as iPhone 11 series are in the market already. Other country regulators are examining similar concepts. In Europe, the European Telecommunications Standards Institute (ETSI) standards body has completed specifications for LSA, which would operate in the 2.3 GHz frequency band, but was not commercially adopted. Evolved LSA is coming next with more focus on private network usage. CBRS alliance has standardized its latest release 3 in February 2020 finally covers some 5G specifications (3GPP release 15).

User Advice: The following user types should consider CBRS and similar shared license solutions:

- Property owners who require good cellular connectivity for the public, but have been unwilling to fund distributed antenna system (DAS) installation would be able to provide coverage and operate a gateway to MNO cellular networks, for which they could potentially charge.
- Cities and enterprises could operate their own private LTE-based networks.
- WISPs can migrate to LTE protocols and move away from proprietary solutions.
- Neutral hosts can build a one-frequency-band small cell installation instead of trying to accommodate multiple licensed frequencies from all the MNOs.
- MNOs can overcome the high cost of deploying small cells at many locations by connecting to CBRS gateways.

Business Impact:

- CBRS has gained a wide range of interested parties in the U.S. and opens the potential for new types of small cell networks. Other country regulators are expected to follow with shared spectrum access provisioning.
- Investigate shared spectrum access opportunities, for example, the use of these frequency bands for neutral host small cells and private LTE networks.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: CommScope; Ericsson; Federated Wireless; Google; Nokia; Samsung Electronics

Recommended Reading: "Market Trends: New Opportunities and Business Models Will Arise From the Growth of Dynamic and Shared Radio Spectrum"

Standard Private LTE

Analysis By: Sylvain Fabre; Tim Zimmerman

Definition: Private LTE is defined as a private wireless network based on Long Term Evolution (LTE) technology infrastructure to interconnect people/things in an enterprise business. Private LTE offering can include voice, video, messaging, broadband data and IoT/M2M features. Access is only available to the enterprise own devices with authorized SIM cards, increasing security, with better and predictable performance as the infrastructure is not publicly shared. .

Position and Adoption Speed Justification: Private LTE is the 16th most-searched term among networking technologies considered for Gartner Hype Cycle, which is a composite metric based on Gartner search, Gartner inquiry and Google trends.

There is an increasing interest in deploying private LTE networks by enterprise business customers in various vertical industries, such as manufacturing, mining, oil, utility and railroad companies, IoT services, university campuses, stadiums/arenas, and so on, to support their growing business and emergency services.

Private LTE networks are designed and deployed with a focus on high capacity, high speed and high security capabilities to increase operational efficiencies of business customers. Enterprise customers are using private LTE networks to either complement or replace Wi-Fi or their traditional private radio technologies such as PMR, VHF/UHF and others. Private LTE is also being deployed to replace traditional wireline technologies such as Ethernet and Multiprotocol Label Switching (MPLS) for remote office connectivity. Unlike the traditional private radio networks, private LTE can also support growing M2M/IoT communications. CSPs are increasingly focused on investing in private LTE networks. CSP suppliers are also focused in developing private LTE solutions to offer directly to enterprise customers or offer through CSPs. With the introduction of LTE-U and Citizens Broadband Radio Service (CBRS, a spectrum band from 3.5 GHz to 3.7 GHz in the U.S.) shared public spectrum, private LTE is shaping up as a major scenario for enterprise mobility. CBRS testing started in a number of U.S. cities across 36 states; unlike other unlicensed spectrum options that can get crowded, access is dynamically managed by the Spectrum Access System to minimize interference.

The U.K. and Germany have already allocated spectrum in the same band as CBRS, and other bands are expected (such as 6GHz).

From an IoT/M2M perspective, the roadmap from 4G to 5G promised capabilities requires a much higher density of endpoints, up to 1 million per sq. km.

User Advice: Private LTE is one of the opportunities for CSPs to grow their revenue. CSPs should prepare a strategic plan to invest in private LTE infrastructure and grow revenue over the next several years. A major advantage for CSPs is that private LTE networks can be deployed using their existing LTE infrastructure with very minimal additional investments. Private LTE service should have the following features: On-demand high-speed LTE access, on-demand high capacity LTE access, high-security features such as data encryption, eliminating internet-based traffic when needed, multifactor authentication (MFA), and secure/encrypted devices. Private LTE offerings should also have features like mobile worker management, push-to-talk, push-to-video, and other business applications targeting various vertical enterprise customers. Private LTE offering should also have dedicated networks such as LTE-M, etc., to support IoT/M2M business requirements.

With the introduction of LTE-U and Citizens Broadband Radio Service (CBRS) shared public spectrum, the private LTE market sees CSPs and their suppliers competing directly. CSPs used to have the upper hand in this market thanks to licensed ownership of spectrum resources, and they should use those assets to offer a differentiated private LTE service.

I&O enterprise leaders should:

- Take advantage of the widening choice of suppliers by including CSPs, vendors and integrators in your RFQ for private LTE
- Consider the need for off-site mobility and national roaming

For CSPs delivering private LTE, we recommend:

- Include VoLTE, VoWiFi, video, messaging, RCS, fixed-mobile convergence, etc. in their private LTE offering
- Use licensed ownership of spectrum resources to offer a differentiated private LTE service
- Differentiate offering by bundling other value-added services, such as agile and scalable network, with features such as SIM management, self-healing, closed loop automation, national roaming, etc.

Business Impact: The need for private connectivity in industry verticals is growing, as seen in the volume of Gartner inquiries on this topic. Verticals such as mining, oil, railroad, health, logistics, land development and banking are seeking private connectivity on demand to support their premises. Such connectivity is not just human-to-human; it also includes human-to-things, things-to-things, etc. A private LTE network is perceived as one aspect of increasing productivity and cost reduction. CSPs should invest in private LTE networks and develop customized offerings for various vertical industries with an ecosystem of partners.

For enterprise IT leaders, we recommend:

- Consider deploying an LTE PMN if don't have on-premises access to cellular wireless coverage or wish an alternative supplier to CSPs
- Include CSP suppliers in your RFQs, as they are now competitors to operators for private LTE solutions
- Consider CBRS from noncellular vendors to provide local coverage or additional network capacity for indoor and outdoor wireless services for both rural and urban environments
- Get vendors to clarify their roadmap from 4G to 5G, such that disruption is minimal and interference managed during coexistence of these technologies

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Athonet; Cambium Networks; Cisco; CommScope; Druid Software; Ericsson; Huawei; Mavenir; NEC; Nokia

Recommended Reading: "Autonomous Things Ecosystems Open Opportunities for IT Services Providers in Telecom"

"Emerging Technologies: Venture Capital Growth Insights for mmWave 5G"

"Magic Quadrant for LTE Network Infrastructure"

"Industry Focus Can Expand Private LTE Footprint"

"Market Insight: Public Safety, First Responder and Mission-Critical Networks Migrate Toward LTE"

Wi-Fi 6 (802.11ax)

Analysis By: Tim Zimmerman

Definition: Wi-Fi 6 (802.11ax) is the latest iteration of the IEEE 802.11 WLAN family. Its main enhancements are allowing the network to control device connectivity for the first time and to improve the efficiency of existing 2.4GHz and 5GHz spectrum, thereby increasing throughput in densely populated areas. As such, its goal is to support a larger number of devices including IoT that are properly connected to the network.

Position and Adoption Speed Justification: IEEE, the standards body of 802.11-based technologies, started the High Efficiency WLAN (HEW) Study Group in May 2013 to examine the most pressing needs for the next-generation Wi-Fi technology. Ratification of the new Wi-Fi 6 (802.11ax) standard was expected in late 2019 but was delayed until 2020 and perhaps longer due to COVID-19. Prestandards-based networking equipment has already been released by a majority of the key/leading vendors. Successive Wi-Fi technologies have increased per-device throughput at an impressive rate through the years (from 802.11b's 11 Mbps to 10 Gbps expected from the new standard).

The number of IoT devices and the convergence of building automation and line of business devices onto the enterprise communication infrastructure continues to contribute to congestion. 802.11ax will be able to more intelligently use network resources instead of letting the device make connectivity decision as previous versions of the standard allowed. Advancements allow differing streams to communicate to multiple devices simultaneously as well as cutting latency by as much as 75%.

User Advice:

- We advise clients not to pay a premium for any adoption of Wi-Fi 6 (802.11ax) unless existing wireless solution do not provide the performance and functionality needed to meet defined end-user requirements.
- For IT leaders, Wi-Fi 6 (802.11ax) represents an opportunity to significantly improve performance for special use cases such as dense device deployments, they are advised to monitor the standardization timeline and product availability to find the right entry point for future infrastructure upgrades as well as availability of client devices that will support the new standard.
- We advise clients that "Wi-Fi 6 certification" currently does not mean 802.11ax compliant since the standard is not ratified. Any organization that purchases prestandard products should have the ability to upgrade or update their product at no cost to be standards compliant.

Business Impact: Wi-Fi 6 (802.11ax) is the first Wi-Fi technology that will be able to support large-scale IoT usage scenarios and other high density environments using existing 2.4GHz and 5GHz spectrum via its use of OFDMA.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Broadcom; Cisco; Extreme Networks; Hewlett Packard Enterprise (Aruba); Huawei; Intel; Juniper Networks (Mist Systems); Qualcomm

Recommended Reading: "Magic Quadrant for Wired and Wireless LAN Access Infrastructure"

"Critical Capabilities for Wired and Wireless LAN Access Infrastructure"

Communications Platform as a Service (cPaaS)

Analysis By: Daniel O'Connell

Definition: Communications platform as a service (CPaaS) is a cloud-based middleware on which organizations can develop, run and distribute communication software. The platform offers APIs that simplify the integration of communication capabilities — including SMS, voice, messaging apps, social and video — into applications, services and business processes, complemented with development tools and documentation. A CPaaS vendor may also offer off-the-shelf modules as programmable components and complete solutions.

Position and Adoption Speed Justification: Initial CPaaS adoption was largely driven by digital-native companies, such as Uber, Lyft, and Airbnb. Some CPaaS providers are building solutions for specific industry use cases (such as healthcare appointment reminders or e-commerce payments). Awareness of CPaaS is now quickly expanding into traditional enterprises that see software as a means toward digitalization. As these enterprises embrace CPaaS, they face several challenges, which include:

- A fragmented vendor landscape — With new entrants from different backgrounds participating in the market.
- Different levels of platform capabilities — Some CPaaS providers focus on baseline offerings centered on API-enabled SMS, voice, and two-factor authentication (2FA). While others possess a much richer set of capabilities that expands into messaging apps, payments, video and advanced voice capabilities.
- Varying global reach — Some of the CPaaS vendors have global reach and can support local numbers for voice and messaging in 150+ countries while others are more regional or country specific.
- Enterprise-grade capabilities — Most of the CPaaS vendors have invested on well-developed sales and service capabilities, and started to offer enterprise security, admin, control and compliance.
- Pricing models — Most of the CPaaS vendors offer a broad set of pricing options that suit enterprise needs.

User Advice: Enterprises start small but often find their CPaaS adoption accelerating much faster than expected. In some cases, a given use case finds adoption far more popular than expected. In other cases, the CPaaS tool starts in one business unit, but is quickly embraced across other business units. IT leaders adopting CPaaS should:

- Identify software development skills and competency gaps in your organization to implement CPaaS. Backfill with third-party developers to learn new skills if necessary.
- Start with one or two basic use cases then expand into new business units for greater enterprise adoption.
- Do not evaluate vendors solely on price. Rather focus on the developer experience, including APIs, SDKs, documentation, and training.

- Expand CPaaS usage outside the developer community by learning how to use visual builders.
- Experiment with the newer CPaaS offerings in such areas as messaging apps, security, payments, video, IoT, and contact center. Such tools can be used to address complex use cases.
- Understand how your vendor can fulfill address vertical compliances, country/regional requirements, and industry standards. They are increasingly important when more complex business solutions are addressed.

Business Impact: The majority of CPaaS projects continue to focus on the foundational elements of CPaaS — namely SMS, voice, security, and authentication. These elements are used in such areas as customer engagement, alerts and notifications, mobile marketing, and secure transactions. They have proven highly capable with regards to automation, scaling, global deployments, and value for the investment. Businesses have seen the greatest impact in terms of:

- Improvements in customer satisfaction, Net Promoter Scores (NPS) and loyalty as result of using intelligent omnichannel customer engagement systems based on CPaaS.
- Increased business agility through the ability to rapidly design, test and deploy new product features and capabilities on the vendor's platform, using their APIs and SDKs.
- A reduction in fraud through authentication and two-factor authentication.
- Operational efficiency gains through optimized resource scheduling and by easily setting up appointment reminders, order/delivery notifications and ticket booking systems.
- Global scalability by not having to redo CPaaS deployments when expanding into new regions and countries.

We expect CPaaS adoption to further accelerate in 2020 and beyond as some of the new services mature. Particularly in the area of messaging apps such as WhatsApp, Google RCS, and Apple Business Chat. These apps will allow richer, two-way conversations that can include pictures, videos, and menu selections, from which payments can be attached. Other capabilities now starting to gain adoption include contact center, biometric security, mobile IoT, AI, bots, and NLP.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Bandwidth; CM.com; IMImobile; Infobip; MessageBird; Plivo; Sinch; Twilio; Vonage

Recommended Reading: "Market Guide for Communications Platform as a Service"

"Market Guide for Emergency/Mass Notification Services"

"Adopt a Pace-Layering Application Approach to Evaluate Your Cloud Contact Center Options"

Massive MIMO

Analysis By: Kosei Takiishi

Definition: MIMO stands for multiple input/multiple output. MIMO can multiply the capacity of a radio link by transmitting and receiving more than one data signal simultaneously over the same radio channel. MIMO is an essential technology element for 4G and 5G, and it can improve the data throughput as the number of antennas is increased. Existing MIMO is mainly composed of two or four antenna elements at a base station but massive MIMO is supposed to utilize dozens or more than 100 antenna elements.

Position and Adoption Speed Justification: By increasing the signal-to-noise ratio of transmissions, massive MIMO enables transmissions to travel greater distances within a given transmit power. It also increases channel capacity through the use of sophisticated adaptive properties that enable automatic signal direction lock-in and optimization of radiation patterns. Massive MIMO for communications service provider (CSP) networks operates by controlling the amplitude and phase of each antenna in both the network array and the device array. In addition, to reduce interference, both the network and the device need to know where, and where not, to radiate.

Despite the promised benefits, massive MIMO with beamforming in macrocells has not really taken off because CSPs either haven't needed it or have considered it too expensive or too big and heavy to deploy commercially. It appears, however, that antenna prices are now coming down. Also, massive MIMO becomes far more practical at higher frequencies, such as those planned for many 5G deployments, because of smaller antenna array, lower cost and lower weight for pole mounting.

On the cellular networks, SoftBank's Time Division-Long Term Evolution (TD-LTE) and China Mobile's TD-LTE have implemented massive MIMO on base stations with 128 transmitters and 128 receivers (128T128R). The arrival of 5G will usher in massive MIMO technology, but the technical limitations of massive MIMO such as its size, weight and power consumption will still force CSPs to introduce more-realistic less-antenna elements (such as 3.5GHz's 32T32R) in early 5G.

User Advice: Adding more arrays with smaller-beam-width antennas will help increase channel capacity. However, it will also significantly increase the complexity of signal processing. CSPs should take advantage of massive MIMO to maximize spectral efficiency and provide improved coverage and quality of service. Massive MIMO will play a significant role in improving the performance of data throughput and the spectral efficiency in LTE and 5G.

Business Impact: From a network perspective, massive MIMO has been very useful in increasing channel capacity and reducing interference. Massive MIMO is an addition to CSPs' efforts to address traffic-related mobile communications issues and can help reduce a radio access network's energy consumption — an important contributor to network operating expenses.

Also, massive MIMO can provide excellent spectral efficiency achieved by spatial multiplexing of many terminals in the same time-frequency resource (so-called multiuser MIMO).

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Antenova; ArrayComm; CommScope; Ericsson; Huawei; NEC; Nokia; Westell Technologies; ZTE

Recommended Reading: "Market Guide for 5G New Radio Infrastructure"

"Top 10 Technologies That Are Defining the Future of Mobility, 2019 Update"

Open Networking/OCP Networking

Analysis By: Mark Fabbi

Definition: Open networking concepts originated in the data center to support the disaggregation of hardware and software networking platforms. This leveraged Open Compute Project (OCP) efforts promoting open-source network hardware and software designs and the commercial, brite-box, offerings of vendors such as Dell EMC and Mellanox Technologies. Open software solutions are based on Linux network operating systems and tools. More recent work expands the focus beyond data center networking to campus switching and wireless access points.

Position and Adoption Speed Justification: OCP-based networking is still in its early adoption phase for enterprise deployments, but is well established in cloud and service provider networks. However, open, brite-box networking solutions, which bundle disaggregated hardware and software into a single supported package represent a more mainstream approach to leveraging the open networking movement. Brite-box solutions from vendors such as Dell EMC and Mellanox have over 4000 production customers. On the other hand, Hewlett Packard Enterprise (HPE) abandoned their Altoline open switch portfolio which contributes to the uncertainty in the market. Recent acquisitions of Mellanox and Cumulus Networks (both by NVIDIA) contribute both hope and uncertainty in the market. In the broad data center market, original design manufacturer (ODM) (or white-box) switches (of which OCP designs represent a significant portion) accounted for 28.4% of unit shipments of data center switches in 2019 (up from 19.8% in 2018). This is with an average selling price 74% less than traditional OEM switches. OCP-compliant hardware is available from many white-box switch providers, either as stand-alone switches or coupled with commercial software, often as part of branded (brite-box) offerings. Brite-box solutions will be much more attractive to enterprise buyers as the complexity of integrating hardware and software as well as support is dealt with by the brite-box provider. Software components such as the Open Network Install Evironment (ONIE), SAI and Open Network Linux (ONL) promote further abstraction of the underlying hardware, making switch OS functions more transportable across switches using different underlying switch silicon.

OCP-compliant switches are available to support a wide range of 10/25/40/50/100G applications for both leaf and spine requirements, including chassis options. Standard network components should become available in a number of Linux distributions to further the efforts of the open-networking movement. Such contributions lower the barrier to entry for new network innovation. However, the growing number of open-source software options (Open Network Linux, SONiC, OS10 Open

Edition, FBOSS, OPX, etc.) could potentially fragment efforts and delay broader adoption, though during the past year we have seen an increased focus on the Microsoft contributed SONiC switch OS software.

Most of the initial work under OCP networking has focused on data center products with a very broad set of possible commercial applications. However we have observed expansion of OCP networking into new areas, such as WLAN access points and campus (with designs for a stacking, PoE capable access layer switch now available), branch and optical networking platforms.

User Advice: We recommend the following:

- Large data center and service provider operators should demand support for OCP networking for future purchases to help reduce operating costs, as they offer competitive and more flexible alternatives to OEM hardware and software.
- Organizations considering open-source hardware options can gain further leverage by assessing SAI-based software options as they become available, as these will further lower their dependency on hardware components.
- In addition, support for specific APIs that are aligned with chosen orchestration and operational environments is key.
- Any organization pursuing a disaggregated open-source approach must have advanced technical expertise to deal with the support and integration requirements.
- Enterprises wanting to lower their network expenditure or create a customized operational environment should evaluate the commercial offerings of vendors targeting open networking and brite-box switching, rather than focusing on the open-source foundational technologies.
- Include brite-box switching on shortlists in specific usage scenarios, such as new application deployments — e.g., analytics cluster and virtual desktop infrastructure (VDI) pods — and to drive new operational initiatives, such as automated development/test and DevOps.

Business Impact: Open networking and OCP initiatives will help reduce related capital expenditure costs by as much as 70%, increase operational flexibility when compared with traditional network approaches while reducing vendor lock-in. Decoupling of hardware and software can allow for changing deployments as use cases or demand shifts as changes can be made in software rather than hardware replacements which lowers the investment risk. OCP software should lower the barriers to entry for innovation in hardware and software, which will benefit the broader networking market and allow for more customization as required.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Alpha Networks; Arista Networks (Mojo Networks); Cumulus Networks; Dell EMC; Edgecore Networks; Mellanox Technologies; Microsoft; Nephos Technologies; Quanta Computer

Recommended Reading: "Magic Quadrant for Data Center and Cloud Networking"

LTE-A Pro

Analysis By: Kosei Takiishi

Definition: Long-term evolution advanced (LTE-A) Pro, defined by Third-Generation Partnership Project (3GPP) Release 13 and later, is intended to mark the point in time when the LTE platform was dramatically enhanced to address new markets as well as add functionality to improve efficiency. This release 13 standardization was frozen in 2Q16. Its technical targets are a peak rate of more than 3 Gbps and delay of less than 2 ms.

Position and Adoption Speed Justification: As of April 2020, there are around 80 mobile communications service providers (CSPs) that commercialized LTE-A Pro based on the Global Mobile Suppliers Association (GSA). These CSPs' network supports three major functions: carrier aggregation, 4x4 MIMO and 256 QAM in the downlink. Same as LTE-A's smooth migration from LTE, LTE-A Pro will be introduced gradually. LTE-A Pro could also be a bridge between 4G LTE and 5G that have been commercialized by many advanced leading CSPs in the world.

The major advances achieved with the completion of release 13 include: machine-type communications enhancements, such as LTE-MTC and NB-IoT; public safety features, such as device-to-device (D2D) and D2D proximity services (ProSe); small cell dual connectivity and architecture; carrier aggregation enhancements; interworking with Wi-Fi; licensed assisted access (at 5 GHz); 3D/full dimension (FD) MIMO; indoor positioning; single-cell point to multipoint; and work on latency reduction. Many of these features were started in previous releases, but will become mature in release 13 and following specifications. Concerning the data throughput improvement, carrier aggregation enhancements can support up to 32 carriers and FD MIMO can support 8-, 12- and 16-antenna elements.

User Advice: We advise:

- Confirm that equipment can be upgraded to LTE-A Pro at minimal additional cost.
- When introducing LTE-A Pro functionality in the network, ensure that adequate backward-compatibility testing with LTE, LTE-A and existing 3G networks is undertaken by vendors during acceptance and interoperability testing.
- Acquire a new frequency asset for LTE-A Pro, and improve user experience continuously.

Business Impact: The focus of LTE-A Pro for existing smartphone users is to aggregate many more frequency bands, deploy more antennas at base stations or devices, and obtain higher speeds and better capacity. LTE-A Pro is only useful for CSPs, either when they have licenses on several frequencies that they want to aggregate or when they want to increase LTE bandwidth by refarming a separate spectrum that had been previously used for 2G, 3G or LTE networks.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Ericsson; Huawei; NEC; Nokia; Samsung Electronics; ZTE

Recommended Reading: “Magic Quadrant for LTE Network Infrastructure”

“How to Select 5G NSA/SA Migration Paths”

AI-Based Mobile Network Optimization

Analysis By: Sylvain Fabre

Definition: AI-based mobile network optimization (AI-based MNO) goes beyond traditional self-organizing networks (SON), leverages AI to automate planning and operations for mobile networks. It resides partly in the operations support system framework and partly in the radio access network (RAN) eNodeB, and is an adjunct to human operators for planning, alarm management and maintenance, self-configuration, and self-optimization for the mobile network to help communications service providers (CSPs) automate RAN operations.

Position and Adoption Speed Justification: Cost-optimized automated operations, maintenance and planning are necessary because:

- CSP wireless infrastructure becomes more heterogeneous, which include (2G, 3G, 4G, alongside Wi-Fi). The forthcoming 5G will make the situation more complex and challenging.
- These layers need to be managed and optimized simultaneously. Self-organizing network functionalities are traditionally divided into three major subfunctional groups: self-configuration, self-optimization and self-healing.

They are specified in 3GPP and NGMN. The use of AI is a new area for these tools, and we have actually seen in the last couple of years vendors that were SON-focused, move into AI and optimization.

Primarily, SONs are a key feature of small cells. The increasing use of small cells will mean that a much larger quantity of sites will need to be managed. The rise in connected endpoints driven by the Internet of Things (IoT), as well as 5G, will also require automation to improves network KPIs and allows automation of maintenance tasks and energy saving.

With over 7 million base stations worldwide, and the need to densify networks for 5G, a larger role for AI is required for scaling operations.

CSP IT I&O leaders must include factors such as the NFV approach, orchestration approach, deep packet inspection (DPI), big data analytics and solution architecture changes in their implementation roadmap. They must also identify their partners with a well-defined, holistic roadmap. As a result, the need for continual significant investment in the development of AI Automation capabilities into 5G has proven more difficult to sustain for smaller vendors, who confront much larger infrastructure vendors with greater and more substantial budgets. These difficulties for small vendors will intensify unless they quickly transform.

User Advice: CSPs should:

- Invest in value-adding SON features based on savings in operations, administration and maintenance, as well as network planning and head count.
- Select AI Optimization vendors that can integrate network elements into SONs beyond the RAN. For example, incorporating the core network should become a logical requirement for SON vendors.
- Require multivendor, multitechnology (including Wi-Fi) support. Most vendors propose features that give control of the SON to the vendor — while operators would prefer this to be interworking between different vendors and administered by the operator.
- Use a SON vendor that is different from the installed RAN vendor(s) to provide better key performance indicators (this can be a SON from another RAN vendor or a RAN-independent supplier).
- Use SON to optimizes network conditions on a per-subscriber basis, with user revenue/value information supplied by the BSS.
- Request the inclusion of artificial intelligence (AI) and automation with SON systems, which is starting to occur in some vendors and is a requirement to fully extract value from SON.
- Consider including smaller vendors that are not also providers of RAN infrastructure; but, knowing that while innovative and independent from RAN, they are also more likely to shift focus in the longer term; for example there are several vendors that exited the SON space recently (such as Amdocs, Continual, RADCOM, TEOCO, VIAVI) but then refocused on other aspects such as analytics, automation and optimization. Cisco also sold their SON technology to HCL Technologies.

Business Impact: SON has moved beyond operations and maintenance function. Some vendors now include a more comprehensive network view, adding core and transport networks. Predictive maintenance capability as well as customer experience optimization and value-based optimization (toward higher-paying/higher-tenured customers) can also be added as differentiators. Yet, a full and all-encompassing network SON — able to automatically tune end-to-end networks in a dynamic fashion, with several vendors and radio protocols, while dynamically taking individual customer value into account — remains a moving target. Increasingly, virtualized network functions will make this all-encompassing SON more achievable, and indeed an integral element to service assurance.

AI-based mobile network optimization:

- Provides significant savings in operations and greatly automate the way future wireless networks are set up, managed and planned.
- Is integral to advanced RAN architectures, such as cloud-based RANs.
- Has also been applied to managing mobile core networks.
- Leverages new approaches, such as analytics, machine learning (ML) and AI to add more value to network quality and customer experience in an increasingly predictive manner.

- Should move to closer integration and service assurance solutions.
- Should integrate with BSS information about the value of the user needs to drive how resources are optimized.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Cellwize; Huawei; NEC; Nokia; P.I. Works; ZTE

Recommended Reading: “Magic Quadrant for LTE Network Infrastructure”

VoLTE

Analysis By: Kosei Takiishi

Definition: Voice as an application can be run as an all-IP end-to-end service on Long Term Evolution (LTE) networks. VoLTE is based on the IP Multimedia Subsystem (IMS) network, with specific profiles for control and media planes of voice service on LTE defined by GSMA PRD IR.92. Advantages include very fast call setup, as well as higher definition and simultaneous voice and video, with the possibility to include voice features in IMS and, later, non-IMS applications.

Position and Adoption Speed Justification: Out of 791 commercial LTE networks worldwide, there are 260 commercial voice over LTE (VoLTE) offerings that have been launched (25.8% of all commercial rollouts) as of February 2020 (according to GSA).

This reveals continued rapid growth, and many initial issues that slowed down initial uptake having been resolved, such as:

- The need for quality, countrywide LTE coverage.
- The need to refarm 2G spectrum (and 3G in the U.S.) for 4G, so that communication service providers (CSPs) don’t need to use 2G or 3G for voice with circuit-switched fallback (CSFB).
- Widescale and bilateral roaming agreements (increasingly, the IP exchange [IPX] addresses this requirement).
- On a regulatory note, VoLTE would generate demand from government or law enforcement for legal interception facilities. Usually such mandates are an extra cost for CSPs, not a revenue generator.
- The business model for VoLTE has also been an issue, since voice in most markets is no longer a revenue generator for CSPs.

IMS will be used continuously on the next generation: 5G. Voice over 5G includes Voice over New Radio (VoNR), voice/video communication solutions EPS fallback (EPS FB), RAT fallback (RAT FB) and Voice over eLTE (VoeLTE).

User Advice: We advise:

- Plan network evolution alongside your service roadmap. Multimedia telephony is needed, and video calling (among other types), advanced messaging and presence applications can be added.
- Differentiate CSP VoIP so that the branded VoLTE stands out clearly from over-the-top alternatives (like WhatsApp), such as HD-quality VoLTE.
- While there may not always be a clear business case for VoLTE as a service, there is a business case in using VoLTE to release 2G and 3G spectrum for more LTE capacity.
- Network function virtualization (NFV)-based IMS or virtual infrastructure management (VIM) may be the architecture of choice for VoLTE, since CSPs favor using virtualized architectures for new features first.
- Promote IMS adoption in anticipation of voice service introduction after 5G commercialization.

Business Impact:

- As the usage of voice and SMS is decreasing, revenue sources for CSPs' data are starting to take over in many places. Unlimited voice is common on consumer contracts around mostly any country. In that context, HD voice quality would be of more interest.
- Another issue, which is partly technology-related and partly service-related, is migrating users away from legacy 2G/3G onto the 4G platform. This can be one motivation for moving to VoLTE — not just as a new service, but simply as a replacement for the legacy circuit-switched voice being retired (for example, as the old network is phased out and spectrum is refarmed).

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Cisco; Ericsson; Huawei; Mavenir; Maveric Systems; NEC; Nokia; Samsung Electronics; ZTE

Climbing the Slope

LTE-M

Analysis By: Kosei Takiishi

Definition: Long Term Evolution for machine-type communications (LTE-M) is aimed at providing a cellular communications infrastructure that is able to support the Internet of Things (IoT). It is specified by the 3rd Generation Partnership Project (3GPP) standards, first developed and published in 3GPP Release 13 (2016). The first specification is so-called LTE Cat M1 and has added capabilities with new 3GPP releases. This analysis of the technology also covers further LTE-M specifications.

Position and Adoption Speed Justification: Standards-compliant LTE-M devices are now being produced and improvements continue in power consumption, cost and performance.

Following LTE-M, IoT wide-area connectivity standards continued to be developed with the emergence of narrowband-IoT (NB-IoT) as an alternative technology choice that has lower bandwidth capability, but a wider area coverage, lower device power consumption and potentially, lower device cost. Differentiators for LTE-M are bigger throughput, supporting limited to full mobility and voice communication by VoLTE.

Cat M2 is also standardized by 3GPP Release 14 in 2017. Major upgrades from Cat M1 include peak data rate improvement up to 2.5 Mbps, enhanced mobility and half-duplex voice, supporting positioning and single-cell multicast. Cat M2 enhancement is covered by 3GPP Release 15 in 2018 by adding new use cases, including support for higher UE velocity, a lower UE power class and TDD support. Globally, 36 CSPs have already commercialized LTE-M based on GSMA as of January 2020.

User Advice: Communications service providers (CSPs) planning to expand their IoT communications services business should consider incorporating LTE-M into their LTE networks alongside alternatives such as standards-based NB-IoT or long-range WAN (LoRaWAN).

Business Impact: Attention to LTE-M has mainly been based in North America, while CSPs in Asia/Pacific are tending to favor the alternative NB-IoT standard (also supported in 3GPP Release 13), which uses a much smaller slice of spectrum. Europe is split between LTE-M, NB-IoT and LoRaWAN. It remains to be seen how LTE-M will compete with the industrial, scientific and medical (ISM) band solutions such as LoRaWAN.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Ericsson; Huawei; Nokia; Sierra Wireless; ZTE

Recommended Reading: “Exploit LPWA Networks Now — 5G Won’t Change Them”

LTE-U

Analysis By: Kosei Takiishi

Definition: Long Term Evolution Advanced over unlicensed spectrum (LTE-U) is LTE operating in the unlicensed spectrum bands. The aim is to supplement the licensed narrow LTE frequency bands with larger amounts of unlicensed spectrum — thereby significantly increasing available bandwidth. The first two LTE-U standards supplement licensed LTE frequency downlinks with part of the 5GHz

Wi-Fi spectrum — known as LTE license-assisted access (LTE-LAA) and LTE Wi-Fi aggregation (LWA).

Position and Adoption Speed Justification: An increasing number of communications service providers (CSPs) are conducting trials of Long Term Evolution (LTE) in unlicensed spectrum and perceive this as a potential way to increase available spectrum for LTE services. License-assisted access (LAA) and LWA standards are part of the 3rd Generation Partnership Project (3GPP) Release 13, which was completed in 2016. Products are now starting to be deployed in volume across North America and Asia/Pacific.

3GPP Release 16, to be finished during 1H20, is standardizing 5G for unlicensed spectrum operation and the usage of unlicensed spectrum will continue on the next generation too.

User Advice: Since LAA is perceived more as an opportunity to cost-effectively increase cellular capacity (particularly indoors), consider using this technology in conjunction with LTE small cells. In fact, CSPs who have managed Wi-Fi services could leverage these locations to deploy LTE-LAA and effectively result in deploying a cellular small cell at minimum cost.

The first standard will use a licensed LTE frequency for call authentication and control plus upstream data traffic; while part of the 5GHz unlicensed Wi-Fi frequency band can be used for downstream traffic. LAA may be easier to integrate with the cellular core network than carrier-class Wi-Fi, but new standards-based equipment and software will be required both on the small-cell equipment side and on user devices for LAA to work. There are plans for support of upstream traffic in unlicensed bands too. In addition, there is still industry support for the MulteFire Alliance promoting the use of LTE in some unlicensed frequency bands such as sXGP 1.9GHz in Japan — without the need for a supporting licensed band. Note that prestandard LTE-U products do not have a “listen before talk” functionality that is mandatory in most countries.

Business Impact: In the past several years, the telecom industry witnessed an uptake in LTE-LAA products with a growing — but still relatively small — number of CSPs adopting this network-capacity-enabling solution. As of April 2020, there are 9 mobile CSPs that commercialized LAA and 1 mobile CSP that commercialized LWA based on the Global mobile Suppliers Association (GSA). It will not be particularly straightforward though, since property owners/enterprises must be willing to sacrifice some of their Wi-Fi bandwidth.

The overall business impact will be to increase the available bandwidth for LTE data transmission — a protocol that is more efficient and also potentially more secure than public Wi-Fi.

LTE-U can currently be used by cellular operators, 3GPP Release 14 and MulteFire continue to open up bandwidth to LTE protocols — providing opportunities for not only traditional cellular operators, but also for mobile virtual network operators (MVNOs) and new entrants.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Ericsson; Huawei; Nokia; Qualcomm; Samsung Electronics; ZTE

Recommended Reading: "Industry Focus Can Expand Private LTE Footprint"

Software-Defined Wide-Area Network (SD-WAN)

Analysis By: Gaspar Valdivia; Andrew Lerner

Definition: Software-defined wide-area network (SD-WAN) products replace traditional branch routers. They provide several features: dynamic path selection, based on business or application policy; centralized policy and management of WAN edge devices; and zero-touch configuration. SD-WAN products are WAN transport/carrier-agnostic and can create secure paths across multiple WAN connections. SD-WAN products can be hardware- or software-based and managed directly by enterprises or embedded in a managed service offering.

Position and Adoption Speed Justification: Over the last five years, CSPs have increasingly partnered with SD-WAN product vendors and deployed managed SD-WAN services, often with some option for bring your own access. CSPs' enterprise customers across markets continue adopting SD-WAN. Gartner estimates that more than 25,000 customers have deployed SD-WAN products in production networks (some in do-it-yourself mode), which is over 600,000 branch locations. CSPs compete with a large variety of service providers such as system integrators, technology vendors offering services, managed service providers specialists, or internet aggregators. Gartner expects managed SD-WAN services opportunity to grow at a 42% compound annual growth rate (CAGR) for the next three years. The primary drivers for SD-WAN adoption are improved network agility and flexibility, operational simplification, and better utilization of all available bandwidth in an enterprise site when deployed with a hybrid WAN topology, yielding cost improvements and performance improvements. More than 40 technology vendors compete in the market today, including pure play startup vendors, incumbent routing vendors and pivoting optimization and security vendors.

User Advice: CSPs need to differentiate their offerings from over-the-top (OTT) solutions beyond offering choice of SD-WAN technology and support third-party provided underlay connectivity. Adding advanced features such as application specific policies and controls, advanced analytics, traffic monitoring and optimization, and co-management approaches is one option. CSPs should also compete with segmented propositions offering segment-specific SD-WAN gears and service bundles that might include services such as internet connectivity, security and workplace communication services. More flexible terms and conditions (for instance, on individual link contract terminations), and proactive SLA payments will be hard to replicate by other types of providers and will help build enterprises' trust in CSPs. CSP can also differentiate their SD-WAN service from overlay deployments with network integrated approaches that bypass the internet for long hops, enhance connections to the cloud and ease phased and partial SD-WAN deployments across enterprise locations.

Business Impact: SD-WAN is changing the market dynamics of enterprise network business for CSPs by moving WAN traffic from private to public connectivity services and by favoring further decoupling of enterprise sourcing of network management services, WAN edge products and connectivity. Limited growth or decline in enterprise's demand for private connections and increased competition on managed services challenge CSP's longtime established revenue stream in WAN services. Service differentiation and augmentation with enhanced functionalities and capabilities such as application performance management (APM), service bundling, segmented offerings and commercial flexibility are key levers to better compete.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Cisco; Fortinet; Huawei; Juniper Networks; Nuage Networks; Palo Alto Networks; Silver Peak; Versa; VMware (VeloCloud)

Recommended Reading: "Magic Quadrant for WAN Edge Infrastructure"

"Market Trends: SD-WAN and NFV for Enterprise Network Services"

"Competitive Landscape: Managed SD-WAN Services"

"Market Opportunity Map: Enterprise Network Services, Worldwide"

vEPC

Analysis By: Peter Liu

Definition: Virtual evolved packet core (vEPC) is the virtualization of Long Term Evolution (LTE) core network functions, which traditionally run on dedicated hardware, in virtual machines implemented on commercial off-the-shelf (COTS) servers. These services include mobility management entity (MME), serving gateway (SGW) and packet data node gateway (PGW). It can further expand the definition by including home subscriber server (HSS), and policy and charging rules function (PCRF).

Position and Adoption Speed Justification: Communications service providers (CSPs) like AT&T, Telefónica, NTT DOCOMO, Verizon, BT China Mobile and others have rolled out their network function virtualization (NFV) projects. vEPC has become one of the most feasible examples for demonstrating the benefit of NFV. CSPs are convinced that vEPC is both financially and technically viable for their networks and have started their vEPC commercial rollout in large scale.

Key motivation behind vEPC adoption can be summarized as:

- Lowers infrastructure cost by replacing proprietary hardware with common COTS hardware.
- Scales economically to meet the growing user traffic on LTE network.
- Enables higher service velocity and agility.
- Supports affordable and fast service innovation and expansion such as the Internet of Things (IoT).

- Supports evolution to 5G and its 5G next generation core, since network slicing and the inclusion of very-low-latency applications will necessitate a virtual core network.

As technology evolves, traditional concerns, such as security and performance, have been well addressed by technologies such as data plane development kits (DPDK) and single root input/output virtualization (SR-IOV), as well as new orchestration and security tools. Large-scale commercial rollout from Tier 1 CSPs eased the concern, and we see most of the new EPC procurements were involving vEPC as a mandatory. More than 100 CSPs have commercially launched vEPC with different business purposes such as capacity on demand, cloud-based core, multitenant core to support “vEPC-as-a-service,” or new business (e.g., IoT, enterprise) support.

Looking forward, containerized open-source orchestration systems such as Kubernetes are often a preferred method for greenfield deployments because of their lighter compute and storage footprints, portability, faster time to deployment, and other benefits. Container network functions (CNF) are the new trend and beginning to replace VNFs in VMs with CNFs in containers to rapidly, efficiently deliver microservices across cloud and data center architectures. There are lots of CSPs are evaluating vEPC solution with a combinations of containers and microdevices architectures.

User Advice: We recommend CSPs to:

- Identify the lead use cases and a clear set of objectives for vEPC implementation that are in alignment with the intended business outcome. Make this central to your EPC virtualization strategy.
- Do not rush to containerized based EPC solution if you already start a virtual-machine-based transformation, but make sure the infrastructure itself able to support both methodologies.
- Include investment in new orchestration architectures and management tools to achieve operational efficiency in the multivendor, heterogeneous network environment enabled by vEPC.
- Evaluate the organizational impact in terms of required skill set, initial goals and responsibilities. Create an open and cross-organizational structure that enables and champions the vEPC deployment.

Business Impact: CSP chief technology and information officers (CTIOs) are convinced that NFV is the right direction. The maturity of vEPC always makes it the pilot project in a CSP NFV roadmap. Greater scalability, elasticity, flexibility, service velocity/agility and newer pay-as-you-grow business models are the targets from this technology. Additional benefits from virtualizing LTE core network functions on COTS include:

- Reduce total cost of ownership
- Streamline asset utilization
- Support new business such as IoT and video in an effective and efficient way
- Enable fast service innovation and expansion

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Affirmed Networks; Athonet; Broadcom; Cisco; Ericsson; Huawei; Mavenir; Nokia; ZTE

Recommended Reading: "Changing CSPs' NFV and SDN Budgets and Implications for Technology Suppliers"

"Assessing 5G Mobile Technology for Organizations"

"Market Guide for 5G New Radio Infrastructure"

Small Cells

Analysis By: Peter Liu

Definition: Small cells are radio access nodes with low radio frequency power output. They are operating in the licensed and unlicensed spectrum, with a cell radius of a few tens to a couple of hundred meters. They can be deployed in variety of places including in-building, lampposts, street furniture, walls, rooftops and so on. This profile is focused on non-5G small cells that include LTE, Wi-Fi, and earlier wireless generation standards. Picocell and femtocells are two classic examples that are included in the Gartner definition.

Position and Adoption Speed Justification: Pre-5G small cell development will continue over the next few years. Traffic over cellular mobile networks continues to grow at a fast pace, placing a tremendous strain on traditional macrocell architectures. Macrocell coverage alone is providing inadequate to meet the subscriber needs in defined areas and small cells can provide additional coverage and bandwidth without having to deploy additional costly cellular tower resources. Therefore, CSPs around the world have substantially adopt small cells as a low-cost way to improve the transmission coverage and density. Small cell will become more critical in post 4G era. Increasingly, CSPs are beginning to view small cell as a strategic enabler instead of a complementary solution of macrocell. For larger communications service providers (CSPs), small cells can offer a strategic path to market solidification while helping to reduce costs associated with capacity growth in targeted areas with high population density. For smaller CSPs, small cells offer a rapid and potentially cost-effective way to grow networks efficiently and strategically.

As the market moves to 5G, CSPs are facing more challenges in terms of coverage, network capacity as well as fulfilling diversified services economically. Therefore, small cells can play an important role in the 5G era for both indoor and outdoor environment. 5G small cells are forecast to start large commercial deployment in 2020 but it will be discussed as a separated IP due to the new technology, architecture and ecosystem.

User Advice: For CSPs, consider deploying small cells within the following environments:

- Outdoors — in areas of high user density.
- Outdoors — to improve coverage in rural communities.

- Indoors — in public places such as shopping malls, transportation hubs and hospitality/hotel locations which have extremely high mobile user density. Small cell can provide enhanced coverage and capacity.
- Indoors — within office environments for enterprises where more and more employees actively use their smartphone for personal and business communication.

Form partnerships with property owners, IT service suppliers, neutral host and system integrator companies as well as local governments, to maximize opportunities and develop ecosystems while minimizing costs and the time to deploy small-cell solutions.

Adopt new ways of network planning, installation and operations support to enable large-scale, small-cell developments.

Use small cells to improve coverage, meet capacity demands and build a platform for value-added services and enhanced subscriber experience.

There are two alternatives to small cells — Wi-Fi offload and distributed antenna systems (DAS). The former is a best-efforts solution that utilizes 802.11u, and the latter is an expensive alternative with capacity issues.

Business Impact: The mobile communications industry is in a state of transformation. An increasing number of smart devices are connecting and traffic volumes are growing at a high rate. New technology is being introduced and new heterogeneous mobile network architectures are being considered by CSPs. This, in turn, is creating new business plans for new opportunities with an increasingly diverse set of service providers.

The emergence of small cells continues to significantly expand the radio access network (RAN) vendor landscape, while the small-cell equipment market is expected to reach a value of over $6.5 billion by 2021. Small cells will enable CSPs to improve coverage and increase capacity. They aim to improve subscriber experience while accommodating high-volume traffic growth.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Airspan; Comba Telecom; CommScope; Ericsson; Huawei; ip.access; Nokia; Samsung Electronics; ZTE

Recommended Reading: “Magic Quadrant for LTE Network Infrastructure”

“Forecast: Communications Service Provider Operational Technology, 1Q20 Update”

“Market Insight: Accelerate 5G Adoption Through In-Depth Indoor Coverage”

“Market Trends: Wireless Technologies for Connecting Augmented Reality to the Real World”

LTE Roaming (IPX)

Analysis By: Kosei Takiishi

Definition: Since almost 791 communications service providers (CSPs) have launched long-term evolution (LTE) services commercially, it is natural for CSPs to deploy LTE roaming, too. Internet Protocol (IP) exchange (IPX) — the successor of general packet radio service (GPRS) roaming exchange — is needed because it was developed to foster open, standardized IP interconnectivity. This migration makes CSPs deploy diameter routers and session border controllers. It allows end-to-end quality of service (QoS) in support of both roaming and interworking.

Position and Adoption Speed Justification: With CSPs emphasizing customer experience quality, LTE roaming promises QoS, quality of experience and the ability to differentiate services. LTE roaming has become more widely rolled out by many CSPs globally, and its coverage is growing rapidly year over year.

Based on how LTE has mushroomed since 2013, it is likely that LTE roaming will reach the Plateau of Productivity in approximately two years and will see wider adoption in other regions. Progress to the Plateau of Productivity may become slower due to:

- A resurgence of interest in Wi-Fi roaming and voice over LTE (VoLTE).
- Video roaming with new applications, such as unified communications as a service.
- Exchanging profiles and enforcing tiered services over diameter.

LTE frequency fragmentation will also confuse CSPs and their clients, as they will find it difficult to understand which devices can benefit from LTE roaming in foreign countries.

User Advice: We advise:

- Target to have at least two roaming partners in each country to lead better agreements including pricing and data usage.
- When negotiating agreements, sign up to a security code of conduct to help create a trusted community.

If the LTE roaming preparation is complete, this could be an advantageous position when in negotiations with a potential partner. That is because LTE users will benefit from greater data traffic availability.

Business Impact: EU's roaming annulment has increased usage for European CSPs as subscribers no longer need to be anxious over the high cost of roaming premiums. In addition, user confidence in LTE roaming charge caps may also pose an issue. For example, there are cases where unsuspecting or uninformed subscribers using 3G have been known to run up bills of over $10,000 in data roaming charges. The potential for LTE roaming charges may increase tenfold, despite "bill shock" prevention efforts by CSPs.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

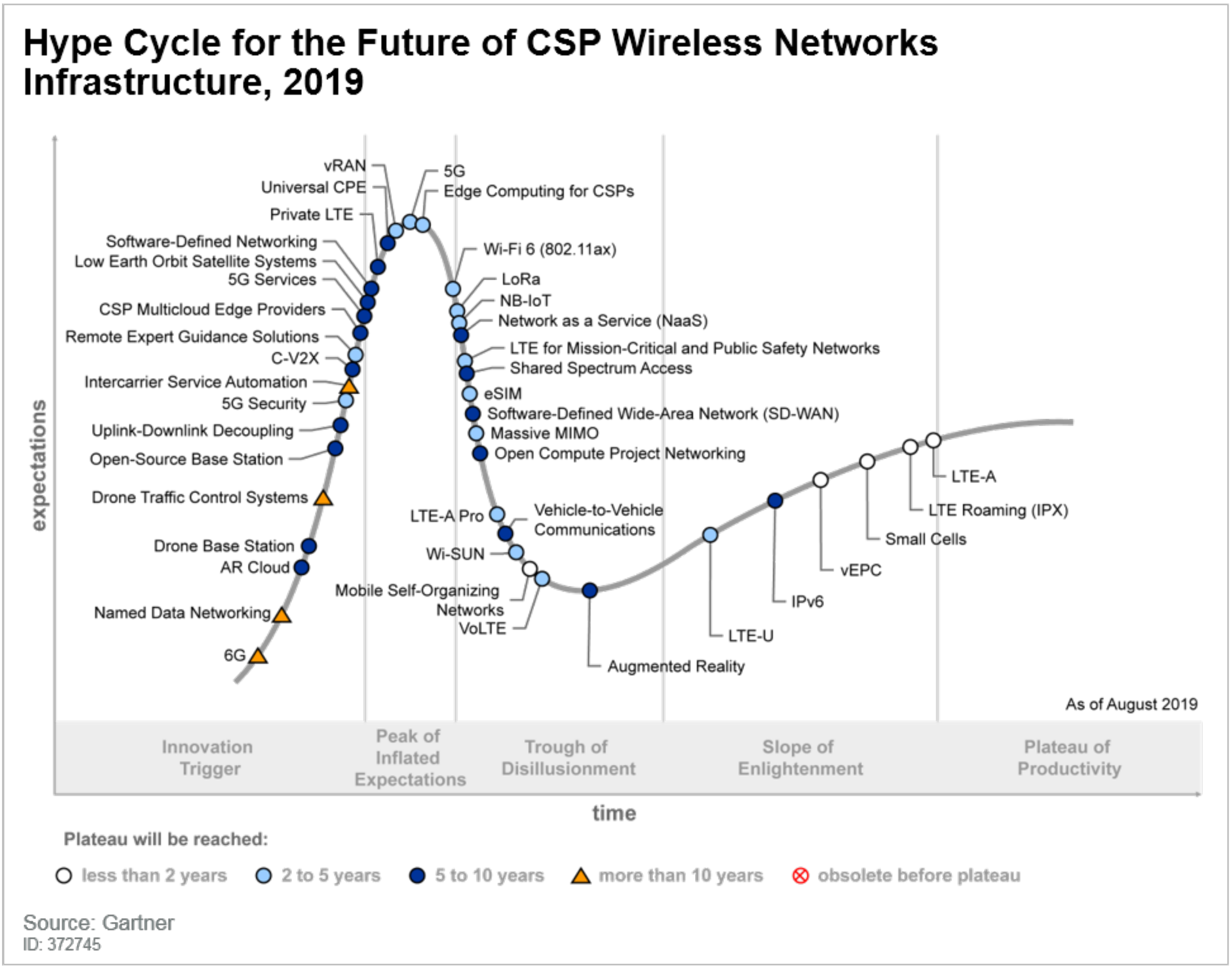
Maturity: Mature mainstream

Sample Vendors: Amdocs; Deutsche Telekom; Dialogic; F5; Oracle; SAP; Syniverse; Tata Communications; TIM Group

Recommended Reading: "Magic Quadrant for LTE Network Infrastructure"

Appendixes

Figure 3. Hype Cycle for the Future of CSP Wireless Networks Infrastructure, 2019



Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough public demonstration, product launch or other event generates significant press and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.
Trough of Disillusionment	Because the technology does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the technology's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the technology to reach the Plateau of Productivity.

Source: Gartner (August 2020)

Table 2. Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (August 2020)

Table 3. Maturity Levels

Maturity Level	Status	Products/Vendors
Embryonic	■ In labs	■ None
Emerging	■ Commercialization by vendors ■ Pilots and deployments by industry leaders	■ First generation ■ High price ■ Much customization
Adolescent	■ Maturing technology capabilities and process understanding ■ Uptake beyond early adopters	■ Second generation ■ Less customization
Early mainstream	■ Proven technology ■ Vendors, technology and adoption rapidly evolving	■ Third generation ■ More out-of-box methodologies
Mature mainstream	■ Robust technology ■ Not much evolution in vendors or technology	■ Several dominant vendors
Legacy	■ Not appropriate for new developments ■ Cost of migration constrains replacement	■ Maintenance revenue focus
Obsolete	■ Rarely used	■ Used/resale market only

Source: Gartner (August 2020)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

4 Hype Cycle Innovations That Should Be on the Private Mobile Networks Roadmap for 5G Security, CSP Edge and Slicing

Hype Cycle for Communications Service Provider Operations, 2020

Market Insight: Telecom CSP Sector Industry Product Planning, Strategy and Execution

Market Insight: Accelerate 5G Adoption Through In-Depth Indoor Coverage

Cool Vendors in Communications Service Provider Network Operations

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp