Hype Cycle for Enterprise Networking, 2021

Published 7 July 2021 - ID G00747511 - 105 min read

By Analyst(s): Andrew Lerner, Danellie Young

Initiatives: Cloud and Edge Infrastructure

Driven by cloud, digitalization and the pandemic, enterprises are adopting new networking technologies faster than previous years. Multicloud networking and SASE are at peak hype and experiencing real-world adoption. I&O leaders can use this research to prioritize investment and time adoption.

Additional Perspectives

- Invest Implications: Hype Cycle for Enterprise Networking, 2021
  (11 August 2021)
- Summary Translation: Hype Cycle for Enterprise Networking, 2021
  (10 August 2021)

Strategic Planning Assumptions

By 2023, 30% of enterprise locations will have internet-only WAN access, compared with approximately 15% in 2020.

By 2025, 35% of companies that use multiple public cloud providers will use a single network software stack, an increase of over 10 times from 2021.

By 2024, 30% of enterprises will adopt cloud-delivered SWG, CASB, ZTNA and branch office firewall as a service (FWaaS) capabilities from the same vendor, up from less than 5% in 2020.

Analysis

What You Need to Know

I&O networking leaders must aim to deliver the right amount of networking, at the right time and at the right cost to support their digital businesses. This is in contrast to many long-standing network practices of building out “rock solid” infrastructure to last five to 10 years. I&O networking leaders should look at the technological innovations covered in this research to help align network strategies with digital initiatives.

For more information about how peer infrastructure and operations (I&O) leaders view the technologies aligned with this Hype Cycle, see 2021-2023 Emerging Technology Roadmap for Large Enterprises.

The Hype Cycle

Users and apps are everywhere. It is now commonplace that employees access applications while their network traffic never traverses a corporate-owned location. This has altered traffic patterns and rendered long-standing networking designs outdated.

This research describes the 30 most hyped innovations in networking. For each hyped technology, we define and analyze the value to enterprises, level of adoption and anticipated rate of future growth. I&O leaders should use this research to determine if and/or when to invest in these innovations.

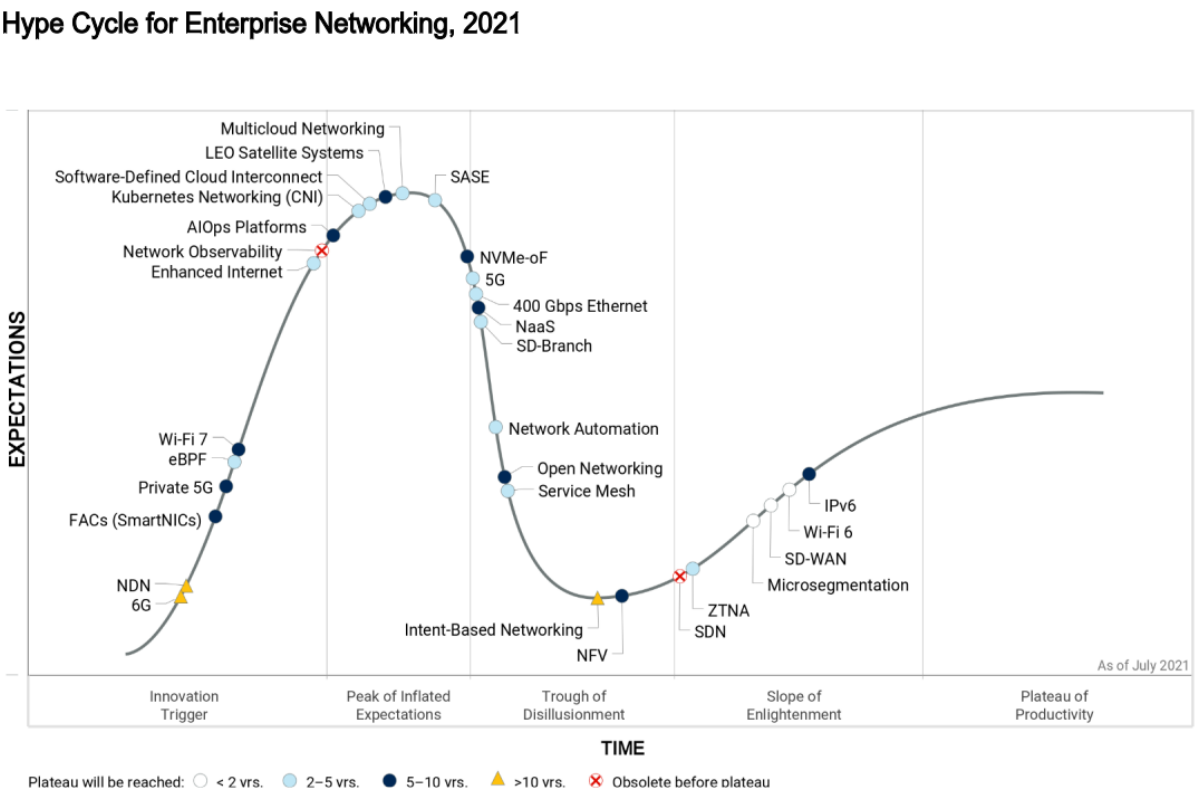
New Hype: Approximately one-third of the innovations covered in this Hype Cycle have changed from 2020, including six innovations on this Hype Cycle for the first time: including 6G, private 5G, eBPF, AIOps, network observability and NaaS.

Peak Hype: Several innovations are at peak hype, including network observability, SDCI, Kubernetes CNI, multicloud networking, 5G and SASE. These innovations have been driven by several factors, including heavy vendor/supplier marketing, the adoption of cloud-native architectures, and the increasingly distributed location of users and applications.

Fast Movers: Three innovations are moving particularly fast through the Hype Cycle: Wi-Fi 6, service mesh and SD-branch. This is a result of increasing enterprise awareness of these innovations and/or mainstream adoption.

Obsolete (or moving in that direction): Software-defined networking (SDN) is obsolete, as true SDN technologies (not just technologies marketed as SDN) have not achieved significant market traction. Similarly, intent-based networking has not gained substantial traction as a stand-alone offering from vendors.

Figure 1: Hype Cycle for Enterprise Networking, 2021



Source: Gartner (July 2021)

Downloadable graphic: Hype Cycle for Enterprise Networking, 2021

The Priority Matrix

The Priority Matrix shows networking technologies, by impact, against a timeline for the number of years until mainstream adoption. It is useful for ranking which technologies an organization should examine first based on maturity and business impact.

The following transformational and/or high-impact technologies are likely to mature during the next two years: SASE, SD-WAN, Wi-Fi 6, 5G and network automation. SASE, SD-WAN and 5G directly relate to addressing emerging traffic patterns due to cloud and digital initiatives. Network automation is a key enabling technology to help make networks more agile to align with the increasing pace of change in the enterprise.

Table 1: Priority Matrix for Enterprise Networking, 2021

(Enlarged table in Appendix)

Benefit	Years to Mainstream Adoption			
↓	Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Transformational		SASE	AIOps Platforms FACs (NextGen SmartNICs) LEO Satellite Systems	6G Named Data Networking
High	SD-WAN Wi-Fi 6 (802.11ax)	5G Network Automation	NVMe-oF Private 5G	
Moderate	Identity-Based Segmentation	400 Gbps Ethernet eBPF Enhanced Internet Kubernetes Networking (CNI) Multicloud Networking SD-Branch Service Mesh Software-Defined Cloud Interconnect ZTNA	NFV Open Networking Wi-Fi 7 (802.11be)	Intent-Based Networking
Low			IPv6 NaaS	

Source: Gartner (July 2021)

Off the Hype Cycle

- Standard private LTE — This is an important technology but not one of the most 25 hyped technologies in networking. We've added private 5G to the research, which garners more hype.
- Edge networking — This is an important and broad set of technologies but not one of the most 25 hyped terms in enterprise networking.
- Network on-demand services — This is an important technology but not one of the most 25 hyped technologies in networking.
- Telemetry-based routing — This is an important technology but not one of the most 25 hyped technologies in networking. It is a subcomponent to several other technologies on the Hype Cycle, including enhanced internet and SD-WAN.
- Ethernet switching fabric — This is an important and mature technology but not one of the most 25 hyped technologies in networking.
- Cloud-managed networks — This is an important and mature technology but not one of the most 25 hyped technologies in networking.

On the Rise

6G

Analysis By: Kosei Takiishi

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

6G is the generic name for the next-generation cellular wireless that is expected to be next in line after 5G. In 2021, the features and timetable for 6G are not clearly defined although it's expected to be commercialized in 2028 by some CSP pioneers. 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 and energy efficiency (e.g., 10 times more efficient).

Why This Is Important

The 2030 agenda including 17 sustainable development goals by the United Nations are heavily impacted by the mobile. Many of these social issues and ambitious goals will result in technologies that become part of 5G or future 6G cellular deployments. Design and research for 6G has already begun with many industrial associations, academic and commercial organizations. 5G can solve some of these challenges, but 6G is indispensable for continuous growth and problem solving in the 2030s.

Business Impact

Although there is no clear 6G definition and the telecom industry is just trying to add one generation every 10 years (same as before), many technologies and concepts from 6G research will find their way into other wireless systems (cellular and otherwise) over the next decade. 5G networks will also be modernized and democratized to become software-based networks based on client demands, and 6G will benefit from it.

Drivers

- Different from 4G and current 5G, 6G will become a sort of national network supported or impacted by countries and national policies. Some leading countries have started their initiatives: In August 2020, Korean government announced that the country plans to launch a pilot project for 6G in 2026. In October 2020, the Alliance for Telecommunications Industry Solutions (ATIS) in the U.S. launched the Next G Alliance to advance North American Leadership in 6G. In November 2020, Korean Ministry of Science and ICT hosted the first 6G Global 2020 in Seoul. In April 2021, the U.S. and Japan agreed to jointly invest $4.5 billion for the development of next-generation communication known as 6G.
- Competition for 6G leadership by local organizations has already started and this could further accelerate 6G standardization and commercialization. These major activities are: In July 2020, NTT DOCOMO hosted 5G Evolution and 6G summit and also renewed the 6G white paper published in January 2020. In November 2020, FuTURE Forum in China published 11 white papers for 6G. In May 2021, 6G Symposium Europe was held as a virtual event.
- Many commercial organizations have started their 6G research to be a part of the future 6G patent pool.

Obstacles

- The 5G journey has just started and its best practices and monetization are not clear. Success or failure of 5G will have a major impact on 6G commercialization and business.
- The telecommunications industry has formulated their own specifications and standardization (such as 2G, 3G, 4G and 5G) by themselves. It is unclear whether 6G will be able to incorporate external opinions more.
- Some 6G technologies such as THz wireless may not prove relevant or cost-effective for most cellular user's needs.

User Recommendations

CSP CIOs should:

- Check the current emerging 6G discussion carefully.
- Avoid deploying 6G commercially till late 2020s. However, there could be deliverables of the 6G research projects that emerge in other wireless areas before 6G. For example, THz wireless systems could well emerge before 2030.

- Support your regulators and government to create their new national policy by 5G evolution and 6G.

There is no action required for IT leaders as 6G commercial offerings are not available in the market.

Sample Vendors

Ericsson; Huawei; Nokia; NTT DOCOMO; SK Telecom

Gartner Recommended Reading

Predicts 2021: CSP Technology and Operations Strategy

Named Data Networking

Analysis By: Sylvain Fabre

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Named data networking (NDN) is an architecture for the future internet that associates unique names (similar to URLs) to blocks of data that can be stored, digitally signed and transmitted across nodes, rather than naming endpoints. The current system transports data containers (packets) between two endpoints using an IP address.

Why This Is Important

NDN can improve expert and citizen data scientist productivity. NDN simplifies processing and mining the huge datasets generated by new scientific fields such as climate science, genomics as well as Internet of Things (IoT) devices, across multiple repositories in various geographies, at the network layer. NDN, by performing all operations such as forwarding requests to data sources, content discovery, access and retrieval using content names, eliminates the need for a location layer.

Business Impact

NDN addresses some of the fundamental weaknesses of the Internet Protocol (IP), such as security and efficient content distribution. But it will need to support current services and applications. To succeed, NDN will need strong support not only from academia, but also from the IT and telco industries — which it would disrupt. NDN could have a major impact on the networking industry, not just routers and switches, as well as the application layers such as search, social and web browsing.

Drivers

- The National Science Foundation (NSF) began development of named data networking (NDN) in 2010 and it evolved into a consortium of academic and industry members.
- In telecom applications, the use cases, as well as the benefits of NDN could complement those of edge computing, at least regarding caching, video optimization, application acceleration and bandwidth saving, but adoption remains uncertain even within a 6G time frame.
- NDN will also provide an architecture with the ability to effectively and securely support broadcast/multicast of content (with native caching) and the IoT.
- Being a clean-slate design, NDN has the opportunity to introduce leapfrog innovation in networking, but this might also hinder its adoption.

Obstacles

- The overhead of naming everything would be onerous when looking at small nodes such as IoT devices and wearables.
- Defining and agreeing on a global naming strategy and standards would be challenging, especially with current fragmentation.
- As IPv6 has demonstrated, introducing large-scale changes in the network is not easy.
- Inertia associated with IP: even a new protocol (v6) has taken 20+ years to get to 30% adoption.
- Although the Named Data Networking Consortium has several members from the telecom industry (see Sample Vendors section below), there is no evidence of adoption of NDN in 5G commercial implementations (which started back in 2018), or investment in its future.
- There are no commercial implementations of NDN yet, only some early interest from academic researchers, and none from enterprises.
- There doesn't appear to be any strong commercial demand for NDN from any key stakeholders, probably because the disruption would be extreme and the benefits uncertain.

User Recommendations

- Evaluate how NDN could impact your networking portfolio strategy in the long term.
- Evaluate the pros and cons of playing an early innovator role in NDN development.
- Use NDN to simplify data discovery for scientific research for institutions that generate and mine large datasets (petascale and over) over multiple locations.
- Fasten data retrieval by using NDN for in-network caching of popular datasets.
- Empower your research community to create infrastructure that supports operations by using NDN to enable creation of federated content repositories, retrieval from multiple sources and remote data subsetting.

Sample Vendors

Cisco Systems; Fujitsu; Huawei; Intel; Juniper Networks; Panasonic; Viasat

FACs (NextGen SmartNICs)

Analysis By: Anushree Verma

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Function accelerator cards (FACs) are a class of devices that have dedicated hardware accelerators with programmable processors to accelerate network, security and storage functions — deployed as an ASIC, FPGA or SoC. FACs improve data operations and services, server availability and bandwidth performance besides enabling connectivity to a network. While all FACs are essentially NICs, not all NICs/SmartNICs are FACs. They come with onboard memory and peripheral interfaces and run independently.

Why This Is Important

FACs can accelerate a whole variety of functions, like networking, security and storage functions, by offloading these functions from the server and dedicated appliances. For example, they improve server performance as much as 10% to 50% by offloading RAID, data compression, block management, encryption and session management for TLS.

FACs are primarily adopted by hyperscale CSPs like Microsoft, AWS and Baidu to improve server performance and enable bare metal provisioning of instances.

Business Impact

FACs enable more cost-efficient data center environments while improving performance. By offloading high overhead functions, they allow the server to host more workloads, hence the direct cost of additional servers and infrastructure software is saved as well in some cases. In addition, they can provide NVMe over Fabrics and GPUDirect storage to facilitate data transmission between remote resources — necessary for hybrid and cloud computing setups with off-site servers.

Drivers

FACs have started growing in popularity since 2019 with hyperscale offering services to customers who are using AWS Nitro and Microsoft AccelNet. However, in 2020, with the ecosystem support, it has gone further in popularity, moving ahead in terms of adoption and justifying its advancement in this Hype Cycle. In addition, vendors are actively and aggressively marketing FACs, which are also referred to as data Processing Unit (DPU), SmartNICs, Distributed Services Card (DSC) or Programmable NICs. Gartner estimates that FACs will grow to $1 billion in 2024 from less than $10 million in 2019, at an estimated rate of 155% CAGR during the time period. Some of the drivers for this transformative innovation include:

- The rise of AI/ML workloads, solid modeling, seismic analysis and advanced analytics has created unprecedented demand on storage and network, resulting in latency and bandwidth issues (fueled by COVID-19).
- Frequency and sophistication of cyberthreats make it imperative to have security functions offloaded and run in an independent, isolated manner in a secure way, specifically in bare metal use cases or microservices-based applications.
- Telecommunication networks are moving toward virtualizing the network edge with 5G adoption, which leads to offloading 5G user plane function (UPF) and 5G network slicing to the FACs to achieve low latency and high throughput.
- 2020 saw FACs getting ecosystem support with server virtualization vendors such as VMware porting its ESXi hypervisor to ARM ISA. This enables the cores on a FAC to offload the core hypervisor functions, adding new levels of hardware-enabled isolation and security within virtualized systems. Another benefit is network consolidation for less demanding workloads.

Obstacles

- Hyperscale CSPs are able to justify the incremental price with the large scale order and customization benefits they have by adopting FACs — their per month revenue saving is passed on to the customer. However, enterprises are yet unable to justify the incremental price, thereby hindering rapid adoption.
- This market is very price sensitive; enterprises need a clear use case and benefit given the higher price point, to drive SmartNICs and FACs.
- Silos in the organization (compute, storage and networking) create challenges in the combined benefit that FACs provide.
- Data plane programmability is high risk and has limited value and interest for enterprises.
- Form factor and power consumption are also an obstacle to adoption. While some FACs consume less than 45 watts and are smaller form factor, some FACs consume as much as 75 watts, blowing up rack, power and cooling budgets, and may have to occupy the only full-size PCIe slot in the server, preventing the installation of a GPU add-in card.

User Recommendations

- Bring in short-term value with FACs, but plan to eventually migrate more functions to drive long-term value.
- Engage with your vendor to not only generate incremental performance benefits, but — more importantly — replace legacy components like aggregation switches and reduce the number of application licenses. Most licenses are for per core, but eliminating the number of server and hypervisor licenses by 30% and the number of network security licenses can drive huge incremental benefits in terms of cost benefits and increasing performance.
- Evaluate FAC-based storage offerings if you are an enterprise with applications that require microsecond latency performance when processing large data sets.
- Engage with FAC vendors if you are a large DCN operator to address network scale/security needs. Enterprises should pilot FAC as an option to support extremely network sensitive workloads.
- Exercise careful evaluation according to use case; not all SmartNICs available in the market are FACs.

Sample Vendors

Broadcom; Ethernity Networks; Fungible; Nebulon; NVIDIA; Pensando; Pliops; VMware; XILINX

Gartner Recommended Reading

Market Trends: Function Accelerator Cards Disrupting Traditional Ethernet Adapter Market

Your Server Is Eating Your Network — Time to Rethink Data Center Network Architectures

Market Trends: Arm in the Data Center: Act Now to Develop Plans to Address This Shifting Market

Private 5G

Analysis By: Sylvain Fabre, Joe Skorupa

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Adolescent

Definition:

A private 5G network is based on 3GPP technology and spectrum to provide unified connectivity, optimized services and security for enterprise. A 5G PMN is used to interconnect people and also things in an enterprise, and can consist of a mix of public and private infrastructure (e.g., private slice over public network). Deployments can be hybrid with on-premises radio and local breakout and connections to the telco core, and/or a public cloud or fully on-premises implementations.

Why This Is Important

Multiple verticals will require 5G private mobile network (PMN) deployments to realize the full effect of their digital transformation initiatives. It can provide the required functionality, with guaranteed performance levels, earlier than CSPs can offer on their public infrastructure. Distinct from the public network, it supports voice, video, messaging, data and IoT with higher performance requirements and can optimize cost or connectivity (e.g., cheaper than Wi-Fi for large area coverage).

Business Impact

5G PMN enables truly transformational digital use cases for industry, especially in conjunction with other technologies such as edge computing, such as factory digital twin, or edge AI for computer vision.

5G PMN can offer enterprises improved security and independence and enable efficiency gains in several manufacturing and industrial processes. For example, BMW Brilliance Automotive (BBA, BMW's joint venture in China) claims complete 5G coverage in all of its factories.

Drivers

- Improved applicability to connected industrial applications: while 5G standards are defined by 3GPP, other bodies are now contributing, for example 5G Alliance for Connected Industries and Automation (5G-ACIA) or 5G Automotive Association (5GAA).
- Requirement for full, reliable network coverage of buildings, machines, sensors and equipment, including indoor, outdoor, office and industrial areas at lower cost than Wi-Fi.
- Need to meet the performance profile for demanding industrial use cases is a key justification for deploying a private 5G network, in particular when low-latency, high-bandwidth and reliability are required.
- A private set up is required if network performance requirements exceed the capabilities of the shared public infrastructure.
- There is also another class of use cases, not focused on mobility initially but requiring a high-performance backbone where wiring is complex and costly — such as in a factory deployment.
- In addition, there is a lot of interest from TSPs that can offer 5G PMN to various verticals, such as I4.0 factory automation, mining, oil, utility and railroad companies; IoT providers, universities, stadiums etc. thereby expanding into industries and generating new revenue.
- We also see an influx of alternative provider types beyond the CSPs, such as integrators, infrastructure vendors and hyperscalers, all of which are driving new deployments and POCs.

- Enterprises deploy private networks because data privacy is a key concern. They require more control and visibility of their data, with security controls, and ensure that sensitive information does not leave the enterprise perimeter.
- Some enterprises want to run their network more independently as their own infrastructure, with limited outside dependency.
- Some defence and government clients have also indicated a wish to have more control and visibility into the vendors involved in the provision of mobile services, which can be an issue over a shared public network built and managed by a CSP.

Obstacles

- Unclear business models and value justification vs. alternatives (e.g., 4G PMN).
- Perception that real value begins from 3GPP R16, and that maturity and availability of R16 solutions is still a work in progress.
- Complex deployment and operation.
- Networks and endpoints cost.
- Lack of outcome-based pricing models.
- Spectrum availability and/or cost in some countries.
- Perception of risk regarding timing and relevance of private 5G.
- Feedback from some industrial clients mentioned that the majority of their use cases could be serviced by a 4G private network, and/or NB-IoT and other LPWA such as LoRa.

User Recommendations

- Enable networks differentiated from other possible providers such as large equipment vendors, system integrators, resellers and smaller specialist network vendors — and more recently hyperscalers, by integrating PMN with other functions such as SIM management, IoT platform, edge computing, design and managed services, and national roaming.
- Co-create networks by partnering with SIs and consultancies for design, deployment and managed services engineering headcount and evaluation test bed environments. For example, build manufacturing 5G PMN as a platform that combines connectivity with security and AI capabilities.
- Design licensed and unlicensed/shared spectrum options where available.
- Supplement your engineering teams by working with IT service providers that have the required industry skills.

Sample Vendors

AT&T; Athonet; China Mobile; Druid Software; Ericsson; Huawei; Nokia; Vodafone; ZTE

Gartner Recommended Reading

Creating Your Enterprise 4G and 5G Private Mobile Network Procurement Strategy and RFQ

Architecting a Reference Framework for 5G Private Mobile Networks

Market Guide for 4G and 5G Private Mobile Networks

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

Market Guide for 5G Network Ecosystem Platform Providers

eBPF

Analysis By: Andrew Lerner, Simon Richard

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Extended Berkeley Packet Filter (eBPF) is an enhancement to the Linux operating system kernel that allows specific instruction sets to run (sandboxed) inside the kernel. It allows companies to add features to Linux without changing kernel source code or requiring kernel modules.

Why This Is Important

eBPF allows users to create hooks that are triggered by Linux kernel events, which offers a safer and simpler way to add/enhance capabilities (such as performance and visibility enhancements) in Linux than was previously available. Technology vendors can use eBPF to avoid kernel-level modules, which carry inherent risks. Also, eBPF is already in production use at scale by hyperscalers, including Amazon Web Services (AWS), Facebook and Netflix, and is being used by technology vendors.

Business Impact

eBPF allows companies to safely and quickly make changes to Linux, compared to using alternative approaches such as Linux kernel modules or upstreaming to the Linux distribution. Currently, much eBPF work is focused on improving observability and performance for applications. Most enterprises will not use eBPF directly, but instead technology vendors will use eBPF as an underpinning technology in their products and services to improve the performance and safety of programs that run on Linux.

Drivers

- Early usage of eBPF is by hyperscalers using it to deliver more efficient cloud offerings, and networking and network security vendors that are using it in their products.
- Hyperscalers use eBPF to remediate kernel vulnerabilities without patching to address Day 0 vulnerabilities, and to more efficiently handle distributed denial of service (DDoS) attacks.
- eBPF is an option for organizations looking to avoid the risk associated with Linux kernel modules, which can destabilize the Linux kernel.
- Organizations are looking at eBPF to accelerate the development speed of software that runs on Linux, via avoidance of the requirement for upstream inclusion into the Linux distribution.
- Organizations are looking to eBPF to improve the performance and monitoring capabilities of software running on Linux.
- eBPF is popular among technologically advanced companies including technology vendors and hyperscalers, because it provides a standardized interface and requires less in-depth kernel programming knowledge.
- eBPF helps to overcome scale and visibility limitations of iptables, which is the default networking stack in Linux. eBPF helps to optimize and customize Linux network packet handling by processing them earlier in the cycle.

Obstacles

- Many older Linux kernels don’t support eBPF.
- Most enterprises do not have the awareness, need or risk tolerance to tackle Linux kernel challenges directly.
- Security and system reliability concerns will severely limit what organizations are willing to deploy using eBPF, as poorly written eBPF programs can directly impact the operation of the Linux kernel.
- Technology vendors will face integration challenges and backward compatibility with existing non-eBPF-enabled products.
- While it is realistic for technology vendors and hyperscalers, most enterprises lack the expertise and skills necessary to use eBPF.

User Recommendations

- Enterprises investing in network visibility and network security products that either run Linux or support Linux should require eBPF support for newer Linux variants.
- Technologically advanced enterprises that are comfortable coding in the Linux kernel should explore whether eBPF can address performance or visibility challenges that are meaningful for their organization.
- Networking and network security vendors should invest in eBPF to improve performance and visibility, and ultimately to avoid falling behind competitors.

Sample Vendors

Cloudflare; Isovalent; Netronome; Sysdig; Tigera

Gartner Recommended Reading

Cool Vendors in Cloud Networking

Wi-Fi 7 (802.11be)

Analysis By: Tim Zimmerman, Mike Toussaint, Bill Menezes

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

IEEE 802.11be (Extremely High Throughput) is the next amendment proposal to IEEE 802.11 for advances in WLAN. The amendment builds upon the existing IEEE 802.11ax standard and potentially will be called Wi-Fi 7.

Why This Is Important

New applications like 8K video streams, as well as augmented reality/virtual reality, are driving user performance requirements of greater than 200 Mbps. Increasing density of people and things for both indoor and outdoor environments also contribute to demand.

Business Impact

For IT leaders, Wi-Fi 7 (802.11be) builds on 802.11ax and focuses on 2.4 GHz, 5 GHz and 6 GHz bands. Advancements to the standard increase the bandwidth and number of differing streams that communicate to multiple devices simultaneously while maintaining backward compatibility.

Drivers

- **Higher performance for video and lower latency:** This will boost theoretical performance with higher speeds upward of 30 Gbps, increased WLAN capacities and lower latency, while maintaining backward compatibility with existing 802.11 standards.
- **Increases number of radio streams to 16 and introduces CMU-MIMO:** The amendment not only allows for more spatial streams to coexist. It is also supposed to support “coordinated” multiuser multiple in, multiple out which will allow multiple access points and better mesh networks.
- **Expand to 6 GHz increasing available spectrum:** The new amendment will use the unlicensed spectrum newly allocated at 6 GHz to create more efficient use of noncontiguous spectrum and allow 320 MHz bandwidth and 16 spatial streams. Additionally, since 6 GHz is a new spectrum, it will not contain legacy devices that could slow the overall performance.

Obstacles

- **Surplus performance for many enterprises:** IEEE 802.11be will theoretically provide performance of up to 30 Gbps in a single coverage area, which is more than three times greater than 802.11ax. The applications needing this much performance are in the future.
- **Required wired infrastructure upgrade:** The uplink ports of IDF switches will need to be upgraded beyond the 1 Gbps ports that are currently available, since the radio performance of one or more access points will exceed the wired connection.
- **Price:** The list price for 802.11be access points is expected to be more expensive than earlier generations and enterprises will need to justify the value.

User Recommendations

- Do not pay a premium for any adoption of Wi-Fi 7 (802.11be) unless existing wireless solutions are unable to provide the performance and functionality needed to meet defined end-user requirements.
- We do not expect Wi-Fi 7 before 2024 so be aware of product end-of-life status of access points, since silicon vendors will limit the production of previous versions of radio chips. These will cause vendors to shorten the availability of some models and only offer newer access point versions.

Sample Vendors

Aruba; Cisco; Extreme Networks; Juniper Networks

Gartner Recommended Reading

Magic Quadrant for Wired and Wireless LAN Access Infrastructure

Critical Capabilities for Wired and Wireless LAN Access Infrastructure

Next-Gen Campus Connectivity Must Start by Defining the End-User Experience

Cloud and Edge Infrastructure Primer for 2021

Enhanced Internet

Analysis By: Mark Fabbi

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Enhanced internet is a collection of internet-based service offerings to improve the reliability and performance of internet-based traffic. Enhanced internet services include features such as telemetry-based routing, performance optimization, and secure and automated tunnel creation. Enhanced internet services may be sourced by enterprise customers or built into SaaS services, and are increasingly relevant due to growing cloud adoption.

Why This Is Important

As enterprises increase the use of cloud services, the internet becomes the mission-critical component of the WAN. While internet services have become more reliable over time, they do not come with the same service levels and consistency found in business-class WAN services on a global basis. Enhanced internet services attempt to bridge the gap.

Business Impact

Enhanced internet services enable enterprises to improve reliability and performance for cloud-resident applications. It is particularly relevant for organizations using multiple cloud services with a distributed user footprint (global or panregion) and for apps that are particularly impacted by performance variations, such as real-time traffic. These services may also be of value to midsize enterprises moving to an all-internet-based WAN transport.

Drivers

- We are observing increasing interest in enhanced internet services, as a growing proportion of enterprise applications are deployed in the cloud and rely on internet services for access.
- The internet is not good enough in all regions or for all applications. Thus, there is a need for a more assured, consistent internet experience.

Obstacles

Enhanced internet faces a number of hurdles to achieve status as a stand-alone market:

- Integrating an additional component from new, unknown suppliers can complicate enterprise cloud transitions.
- Some SaaS providers integrate enhanced internet into their services, and it is likely that SASE providers will include enhanced delivery features into their offerings.
- New services have to fit a very narrow financial window to ensure enhanced internet services remain cheaper than traditional MPLS services.
- Several on-premises functions in other markets would make sense to deliver OTT, such as IPv6 gateways, WAF, DNS and global redirection services. We expect to see more service consolidation across OTT service offerings via acquisition or internal development. While there is a clear need for a more assured and optimized delivery of internet-based applications, enhanced internet services may be better served as an integrated component in SaaS, SASE or SD-WAN solutions.

User Recommendations

Enterprises with global or extended regional footprints that are increasing their usage of public cloud-based applications:

- Add OTT enhanced internet services to the evaluation, at least for those locations and applications that need additional assurance and performance. Any migration of WAN architecture or evaluation of the end-to-end network security architecture is an ideal time to consider enhanced internet services requirements as part of a larger evaluation.
- Enhanced internet capabilities can provide differentiation when considering SASE or SD-WAN solutions. So, include enhanced internet features in the evaluation of these technologies.

Sample Vendors

Anapaya; Teridion

Gartner Recommended Reading

Cool Vendors in Enhanced Internet Services and Cloud Connectivity

Network Observability

Analysis By: Josh Chessman, Andrew Lerner

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

"Network observability" is largely a buzzword, with no concrete definition beyond "network visibility." It's not meaningfully different from what has long been available in NPMD products. Observability (by itself) is a key application monitoring construct, particularly for transitioning from external monitoring to both internal and external instrumentation. Networks have existed in an "observable" state for many years; thus, the term "network observability" is largely meaningless.

Why This Is Important

While the term “network observability” is mostly a marketing buzzword, it is important because overhype and aggressive marketing by vendors can drive false expectations and lead to suboptimal investments.

Also, for many organizations “network monitoring” has negative connotations as something legacy and not relevant to modern businesses. By reframing the discussion as observability, IT operations teams are able to involve a wider audience in what we might otherwise call modern monitoring.

Business Impact

Many network monitoring vendors have started marketing their products using “network observability” to attempt to latch on to the APM trends and hype around observability. Prospective buyers of products marketed as “network observability” may be led to believe that the tool(s) they are acquiring provide some additional functionality, which is not accurate. This can lead to selection of suboptimal solutions and/or overpaying for functionality.

Drivers

- Vendors and users are using “network observability” terminology as a modern synonym for “network monitoring/visibility.” This is largely because “network monitoring” has negative connotations as something legacy and not relevant to modern businesses. By reframing the discussion as “observability,” IT operations teams are able to involve a wider audience in what we might otherwise call “modern monitoring.”
- Network observability is driven by the broader construct of observability.
- Vendors are aligning networking products with this buzzword. Buzzwords are strong terms that can help drive sales for vendors. Because observability is being used successfully in the APM space, vendors in a variety of other IT monitoring areas have begun using the term to describe their products.
- Observability (by itself) is driven by modern applications, their inherent complexity, and the rise of new practices and methodologies (such as DevOps) that left many organizations frustrated with legacy monitoring tools and techniques. However, in practice today, applying “observability” to networking products is of limited value beyond visibility. Networks have, for the most part, always been observable — consisting of packets and flow data from various devices all of which can be collected and analyzed. For example, SNMP data is easy to extract and analyze without requiring any additional instrumentation or agents on the infrastructure side. For public networks, routing and BGP “looking glasses” have been providing routing and pathing information since the 1990s.
- The important difference between today’s “observability” and network visibility is the requirement that telemetry from the network (whether via ITIM or NPMD products) needs to support the broader observability objectives — not just be visible to the network team. The tools must provide the observer with the ability to glean the necessary insights to accomplish their objective using available telemetry.

Obstacles

The concept of network observability is a false promise focused on leveraging the growing cache around the term “observability” without providing any new functionality.

User Recommendations

- Avoid selecting or paying a premium for products because they're marketed as network observability. Investing in such tools and expecting that they will provide more or better functionality/visibility than traditional visibility/monitoring solutions is unrealistic and unnecessary. The functionality they offer is not different or unique from those provided by network monitoring tools.
- Focus on identifying tools that meet your specific needs for network monitoring based on specific features, functionality and workflows. Specific examples of tools that offer more tangible benefits include NPMD and APM.
- When investing in "true" observability initiatives, focus on customer/digital experience, rather than a single technology area.

Gartner Recommended Reading

Market Guide for Network Performance Monitoring and Diagnostics

Magic Quadrant for Application Performance Monitoring

Market Guide for AIOps Platforms

At the Peak

AIOps Platforms

Analysis By: Gregory Murray, Pankaj Prasad, Josh Chessman

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Artificial Intelligence for IT operations (AIOps) platforms analyze telemetry to improve IT operations and have five characteristics: data ingestion across telemetry domains; topology assembly from network flows, application traces, hypervisor, container and cloud; event correlation to reduce the number of redundant events associated with an incident; pattern recognition to predict incidents or probable root cause; association of probable remediation to augment, accelerate or automate resolution.

Why This Is Important

The combination of increasing application complexity, monitoring tool proliferation, and increasing volumes and varieties of telemetry has shifted complexity from gathering the data to interpreting the data. AIOps capitalizes on machine learning and analytics techniques to classify and cluster diverse telemetry signals in near-real time, at scale, and in ways that exceed human capacity. Even where automated remediation is not possible, this analysis can augment and accelerate human response.

Business Impact

AIOps platforms deliver value through:

- Agility and productivity — by reducing alert fatigue through correlation of related events, operators can focus on fewer, more critical events.
- Service availability and triage cost — by reducing the time and effort required to identify root cause and augmenting, accelerating, or automating remediation.
- Compounded value of existing monitoring tools — by unifying the events from siloed monitoring tools and learning actionable event patterns across domains.

Drivers

Demand for AIOps platform capabilities is accelerating and is fueled by:

- Increasing complexity — organizations use an increasingly complex mix of modern, hybrid IT that relies on a complex, highly integrated mix of on-premises assets, cloud IaaS/PaaS providers and SaaS solutions to deliver their missions.
- Increasing monitoring expectations — investments and improvements in monitoring and the pursuit of observability are generating more data from more sources. Emerging monitoring platforms and practices, like application performance management (APM) and digital experience monitoring (DEM) present operators with extremely detailed views into their business applications and the end-user experience. Effective use of this additional data requires near-real time analysis and rationalization against other adjacent telemetry.
- Demands for reliability — shifts in roles and responsibilities from newer operating models, like DevOps and SRE, in the pursuit of greater availability and faster incident resolution. AIOps platforms enable agility by offloading some of the mechanical tasks of event triage, root cause analysis and solution identification. This both accelerates response for common issues and frees up human creative capacity for novel events and business priorities.

As these trends, themselves, are accelerating, expect for the case for AIOps platforms to continue to accelerate.

Obstacles

AIOps platform adoption must overcome the following obstacles:

- Expectations mask real opportunities — Hype is a prolific obstacle to AIOps adoption. It is hard to separate claims of intelligence and magical automation from practical, achievable use-cases. Success with AIOps platforms requires clarity on the capabilities and limitations of available solutions.
- Time-to-value for high-value use-cases — AIOps platforms learn through observation. They learn everything from normal ranges and patterns of data to which automation resolves which issue. Learning requires time because rare events can take months to develop accurate detection models.

- Market shifts and maturity — AIOps is evolving and the market is in flux. Monitoring vendors are moving up the stack, AIOps platform vendors are reaching into monitoring domains, and ITSM vendors see AIOps capabilities as a way to extend their reach. Expect both technology advancements and market shifts to change state-of-the-art and go-to-market.

User Recommendations

- Establish clear, realistic use cases for an AIOps platform pilot. This fundamental step underpins an eventual strategy, while scoping the vendor landscape, clarifying the telemetry requirements and separating hype from reality.
- Integrate single-domain AIOps features with an AIOps platform. This approach allows for efficient data ingestion and analysis, and surfacing of insights across domains.
- Mature toward automation integration, ensuring that core benefits of AIOps are realized before expecting full automation. High risk cases are not ideal for automation but benefit from AIOps accelerating or augmenting human response.
- Shift mechanical operations to analytics and automated execution, while developing creative skills in integration and automation development. Prepare for disruption and adapt to a highly integrated environment. Tackle silos that can create blind spots in your AIOps platform coverage.

Sample Vendors

BigPanda; IBM; Moogsoft; ServiceNow; Splunk

Gartner Recommended Reading

Market Guide for AIOps Platforms

Infographic: Artificial Intelligence Use-Case Prism for AIOps

Solution Path for Adopting AIOps

Understanding the Application of AIOps Disciplines Within IT Operations

Kubernetes Networking (CNI)

Analysis By: Simon Richard, Andrew Lerner

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Kubernetes networking addresses the following three requirements: pod to pod communications, external entities to services communications (often referred to as north south traffic) and pod to service traffic communication, often referred as east-west traffic. Container Networking Interface (CNI) plug-ins handle pod-to-pod networking, ingress controllers handle north-south traffic and service mesh handles east-west traffic.

Why This Is Important

Kubernetes has become the de facto standard system for container orchestration. The native networking capabilities within K8s don't suffice for most enterprise production workloads at scale. CNI software and ingress controllers bridge this gap.

Business Impact

Many organizations are investing in Kubernetes as a foundational technology to their digital business strategies. To securely scale networking within K8s, a CNI and an ingress controller are needed. K8s' CNIs enable developers to implement network policies and multitenancy without requiring developers to concern themselves with lower-level network tasks.

Drivers

- Kubernetes ingress controllers provide several benefits, including automatically encrypting traffic and increasing network performance and visibility.
- The default networking capabilities in K8s do not scale to meet production enterprise requirements and/or fall short from a security/visibility and management-at-scale perspective.
- Open source options, such as Cilium and Calico, reduce acquisition friction and initial cost (compared to dealing with commercial vendors), and align with the culture of many advanced customers who prefer OSS.
- Public cloud providers offer their own natively integrated CNI plug-ins and ingress controllers that integrate with their cloud platform and load balancers.
- For on-premises Kubernetes deployments, third-party CNI plug-ins and ingress controllers are necessary. However, most commercial platforms include support for a default CNI plug-ins.
- Network virtualization vendors and data center networking vendors have CNI plug-ins that extend their policy model to Kubernetes applications and are supported by commercial Kubernetes platforms.
- On the ingress-controller side, most load-balancing as well as some API gateway solutions extend their offerings to provide ingress controller functionality.
- Most cloud providers include a CNI that integrates with their platform without any additional cost.

Obstacles

- Organizations not using K8s don’t need networking capabilities for it.
- Many enterprises lack deep K8s expertise.
- Commercial vendors offering CNIs have difficulty maintaining pace with the K8s releases, which can limit the value to enterprises.
- The technology landscape associated with container networking solutions is fragmented, with many commercial vendor and open-source CNI plug-ins — which can confuse customers — and delay adoption for fear of making a wrong choice.

User Recommendations

- Avoid making Kubernetes-networking decisions in isolation. When sourcing, designing and deploying container networking solutions, ensure that the networking, cloud and development teams are involved as part of a cross-functional effort.
- Hide network complexity from the application team. For example, an ingress controller exposes Layer 7 policy rules to the application team, but hides the load balancing minutia.
- Eliminate manual network provisioning in Kubernetes-based environments. The automation and self-service provisioning of network resources will be required.
- When deploying Kubernetes, look first to extend your deployed network virtualization or data center fabric vendors/solutions from the cloud or data center networking.
- Prefer ingress controllers that extend your existing load balancing or API gateway vendors.Include requirements for turnkey Kubernetes network integration in network RFPs.

Sample Vendors

Cisco; Isovalent; Rancher Labs; Tigera; VMware

Gartner Recommended Reading

Best Practices for Running Containers and Kubernetes in Production

Software-Defined Cloud Interconnect

Analysis By: Lisa Pierce

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Software-defined cloud interconnect (SDCI) provides private network connectivity between enterprises and public cloud service providers (CSPs). SDCIs pre-provision physical connectivity from their hubs to public CSPs, internet service providers (ISPs) and network service providers (NSPs). SDCIs serve as aggregators and intermediaries to quickly provision logical connectivity to CSPs and complement this with billing, monitoring/management, security and administrative functions.

Why This Is Important

Capabilities provided by SDCIs reduce complexity by providing enterprises with a single interface to potentially dozens of CSPs (IaaS, PaaS and SaaS providers), ISPs and NSPs. These functions are also useful when a CSP site experiences either an interim or prolonged/catastrophic outage. SDCI services are key enablers of private, high-performance connectivity to public cloud services and are simpler than dealing with individual cloud services providers on a one-off basis.

Business Impact

Simplifying the method of connecting into multiple public CSPs is essential to optimizing the end-user experience, performance, security and cost. Because it supports rapid provisioning and modification of configurations via a centralized dashboard and programmable controls, SDCI is the most agile of private methods to connect into CSPs. In addition, many SDCI offers also include other services, such as security features, SD-WAN gateways and inter-SDCI hub WAN transport.

Drivers

- Gartner clients often assume they will employ one method to connect into all CSPs, but most enterprises are best served by employing at least two types of connectivity. Direct internet access into CSP ports doesn't scale well, since each CSP has unique administrative and management portals, billing, SLA and security requirements.
- The global COVID-19 pandemic exacerbated this scaling problem by accelerating enterprise migration to CSPs, which will grow at a compound annual growth rate (CAGR) of more than 24% from 2021 through 2024 (see Forecast: Public Cloud Services, Worldwide, 2018-2024, 4Q20 Update). Today, most enterprises connect to 20+ public CSPs. In addition to internet connectivity, clients can employ carrier cloud connect services like AT&T NetBond and cloud hubs like Equinix or SDCI. With the exception of internet connectivity, all of the remaining connectivity choices into CSPs are private — and they connect into CSP private ports like Amazon Web Services (AWS) Direct Connect. Gartner anticipates enterprise spending on cloud connectivity will grow by over 17% year over year between 2019 and 2024, with 75% of enterprises employing private WAN cloud connectivity services (see Forecast Analysis: Enterprise Networking Connectivity Growth Trends, Worldwide).
- Simplifying the method of connecting into multiple CSPs is essential to continued adoption of CSP services. In addition, I&O leaders must optimize the end-user experience, performance, security and cost — and this is where SDCI excels. SDCIs are the most flexible private method, both to connect to multiple CSPs and to manage that connectivity going forward; by the end of 2024, we anticipate that 30% of enterprises will use SDCI services to connect into public CSPs — up from less than 10% in 2020.

Obstacles

- The largest obstacle to SDCI adoption is the widely held perception by many I&O leaders that they only need to employ internet connectivity directly into CSPs.
- Many I&O leaders are unaware of the availability of private connectivity options.
- I&O leaders often are unfamiliar with the differences between the types of private connections into CSPs, and the use cases that best align with each type of connection.
- SDCI functions are evolving over time, which makes it difficult for some clients to decide the best time to jump in.
- Current SDCI market leaders are smaller companies that are often unknown to enterprise clients, which increases perceived risk.

User Recommendations

Today, four considerations enterprises must address include:

- Assess basic functions: Clients who want SDCI providers to connect into CSPs and also provide WAN and access should use MSPs for SDCI. Clients who only want connectivity into CSPs can also assess SDCI from non-MSPs.
- Availability and maturity of other functions: Assess SDCI offer breadth with other services like security, monitoring/management, billing, UCaaS and SD-WAN. As to their level of integration with the foundational SDCI service, favor in-line/integrated services versus bolt-ons.
- Hybrid computing needs: Assure that end-end reliability, security and performance meet your requirements in hybrid environments like mixed computing and applications environments, and multicloud use cases.
- Assess alternatives: A growing number of providers offer connectivity to multiple cloud providers, enhanced internet backbone providers and carriers. Carefully assess both your own needs and the changing provider landscape.

Sample Vendors

Alkira; CoreSite; Epsilon; PacketFabric; Unitas Global

Gartner Recommended Reading

How to Optimize Network Connectivity Into Public Cloud Providers

Innovation Insight for Software-Defined Cloud Interconnection

How to Architect Network Connectivity Across Multiple IaaS Cloud Providers and Regions

How to Architect Your WAN for Hybrid Cloud and Multicloud

How to Interconnect With Azure, AWS and Google Backbones

LEO Satellite Systems

Analysis By: Bill Ray

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Low Earth orbit (LEO) extends to around 1,300 km, significantly closer than geostationary orbit, which is more than 35,000 km from Earth. Connecting to satellites in LEO uses significantly less power, supporting low latency and faster data. However, coverage may require a large number of satellites, most of which will have a limited life span (around five years). Several companies are in the process of launching LEO services for broadband internet access and low-speed IoT connectivity.

Why This Is Important

Companies like Amazon and SpaceX have invested heavily in satellite services intended to provide internet access to consumers and enterprises. Innovations from the smartphone industry have reduced the price of satellites significantly, and the cost of launch is also declining, making these constellations economically viable. As of 2Q21, Starlink was already providing internet access to tens of thousands of users, with plans to rapidly scale up the service and exploit its first-mover advantage.

Business Impact

LEO services will make broadband internet, and IoT data gathering, globally available. Companies and employees can assume that internet access will always be available, removing network access as a limit on locations to work or live. Remote offices will always be able to get a reliable connection, and home workers will be able to live where they like. In time, this connectivity will extend to include aeroplanes, ships and sea platforms, creating a ubiquitous internet (and corporate intranet).

Drivers

- LEO satellite constellations are being launched to address two, distinct, markets: broadband internet access, and low-power IoT connectivity. These markets are being addressed by different companies using different constellations, as the requirements are quite distinct.
- Despite the widescale deployment of terrestrial wired and wireless services, there are still millions of homes and businesses that lack sufficient internet access, even in developed markets. Satellite broadband is relatively expensive (SpaceX's Starlink is charging $99 per month plus $499 installation) and won't compete with already-installed fibre to the cabinet or home. However, Gartner has calculated that there are enough homes without connectivity in the U.S., Europe and Australasia to sustain the Starlink service.
- Other customers will include airlines, ships and the military. LEO satellites can also provide backhaul for cellular services — a single satellite uplink can provide connectivity to a cell tower providing 5G, 4G, Wi-Fi or any other local access technologies. This reduces the cost of network deployment for cellular operators, extending coverage into areas that have previously been economically impossible.
- Starlink is the first mover, with more than 1,000 satellites deployed by 2Q21. However, in time, it will need to compete with offerings from Amazon as well as regionally-backed projects including OneWeb (U.K.), Telesat (Canada), Sfera (Russia) and Hongyan (China).
- IoT connectivity is a different market, focusing on low cost and low power to provide global asset monitoring and tracking. Companies like Myriota already offer a sensor with a five-year battery life and satellite connectivity, while Lacuna Space uses chips and radios conforming to the existing Lora standard, reducing the cost of a satellite-connected IoT sensor to a few dollars. Asset tracking is certainly the killer application, but condition and environmental monitoring will also be an important use case.

Obstacles

- To provide oceanic and remote region coverage (needed by military customers), links from satellite to satellite are required. Only the Iridium narrowband constellation currently has such links, although other companies are testing and designing them.
- Customer equipment currently costs more than $2,000. Developments in antenna design and mass production should reduce that cost, which needs to get below $500 for widespread adoption.
- Maintaining 30,000 satellites, with a life of five years, requires 500 new satellites per month. Current launch vehicles, such as the SpaceX Falcon 9, can launch 60 satellites at a time. This will not be sufficient, so larger launch vehicles (such as the SpaceX Starship or Blue Origin's New Glenn) will be needed.
- Satellite operators are required to avoid interfering with incumbent deployments, limiting the radio spectrum they can use. We expect that radio spectrum access will become a key point of negotiation, and perhaps litigation, in the next five years.

User Recommendations

- Exploit the rapid development of LEO services by adding satellite connectivity into future and strategic planning.
- Check the location of teleports to predict early-service availability; early services will only be available within 500 km of a teleport (earth station).
- Prepare for international availability by liaising with local regulators and resellers. LEO services are inherently global, so will spread internationally as quickly as regulators will allow.
- Protect investment by validating the technical and financial ability of your provider to launch and maintain its constellation.

Sample Vendors

OneWeb; Starlink; Telesat Canada

Gartner Recommended Reading

Market Trends: LEO Satellites Will Provide Practical Connectivity to Remote and Mobile Offices

Emerging Technologies: LEO Mega Constellations — Market Disruption Ahead

Multicloud Networking

Analysis By: Jonathan Forest

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Multicloud networking products primarily address networking requirements across multiple public cloud environments and often extend to private clouds as well. They provide simplified and consistent networking policy, network security, governance and network visibility across multiple clouds from a single console. We consider transport to and between clouds as adjacent functions. Multicloud networking products are often delivered as software and can be self-managed and/or delivered as a service.

Why This Is Important

Multicloud networking solutions offer the ability to manage various private and public cloud environments from a single console to ensure network consistency, scalability, reliability, security and simplicity. Beyond managing various clouds, we also have seen examples of enterprises leveraging multicloud networking solutions for single cloud environments (such as offering more configuration granularity) to address limitations from the cloud service providers.

Business Impact

Multicloud networking solutions ensure consistent and simplified network and security configuration management and policy enforcement, which reduces complexity and ultimately results in better management, control and governance. In addition, the solutions offer network visibility which simplifies troubleshooting, lowers operational support costs, improves reliability and makes it easier to pass audits.

Drivers

- Enables networking policy management across different cloud environments (private or public) as well as on-premises data centers. While some workloads remain on-premises, multicloud networking is primarily driven by more workloads in the public cloud.
- Ensures consistent networking policies, configurations, visibility, security and governance across various cloud environments and on-premises data centers.
- Reduces troubleshooting by simplifying decentralized and complex architectures across different cloud environments.
- Enables ease of connecting from enterprise locations to multiple private/public cloud providers and across cloud providers.
- Simplifies and maintains Day 2 operations.
- Provides enhanced functionality, scalability and simplicity compared to what a single public cloud provider can offer. Clients have used multicloud networking products within a single cloud provider's environment when specific cloud-native functionality was inadequate.
- While the intent of most enterprises is to use multicloud networking across multiple clouds, at times they initially use it within a single cloud to solve a feature gap within a specific cloud provider.

Obstacles

- Multicloud networking is seen as a "nice to have" and not a "must have" as there are alternatives that are good enough for most use cases. Many clients use existing data center solutions or the cloud-native vendors' capabilities. In fact, a recent Gartner survey states that approximately 60% of enterprises use cloud-native vendors' capabilities.
- Time required to certify, integrate and support delays multicloud networking support for new features from public cloud providers.
- Multicloud networking vendors add purchasing complexity and operational expense (via additional software, configurations and installations to manage).
- Increased risk of vendor lock-in at the networking orchestration layer because enterprises rely on the common networking stack provided by the multicloud networking vendor.

- There are some smaller vendors in this market with immature offerings and limited customer base, which may set back customers' buying decisions.

User Recommendations

- Choose lighter-weight functionality by focusing on solutions that use native cloud provider APIs versus solutions that require the installation of heavy agents or overlays.
- Avoid public-cloud-native networking service gaps by validating full visibility, troubleshooting and configuration management support for segmentation, firewalling, ACLs and routing.
- Fill gaps or give preference to multicloud networking solutions when cloud-native capabilities do not suffice. This can be valuable even for a single cloud.
- Include your private and public clouds as part of your overall network strategy by combining requirements for a consistent management framework.
- Choose the appropriate multicloud network connectivity option by evaluating cost, performance and security, and checking vendor references.

Sample Vendors

Alkira; Aviatrix; Cisco; Cohesive Solutions; VMware

Gartner Recommended Reading

Technology Insight for Multicloud Networking

Magic Quadrant for Data Center and Cloud Networking

Critical Capabilities for Data Center and Cloud Networking

SASE

Analysis By: Joe Skorupa, Neil MacDonald

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Secure access service edge (SASE) delivers multiple converged network and security as a service capabilities, such as SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). SASE supports branch office, remote worker and on-premises general internet security use cases. SASE is delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

Why This Is Important

SASE is a key enabler of modern digital business transformation, including work from anywhere and the adoption of edge computing and cloud-delivered applications. It increases visibility, agility, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and network security services mainly via a cloud-delivered model. SASE can reduce the number of vendors required for secure access from four to six today to one to two over the next several years.

Business Impact

SASE enables:

- New digital business use cases (such as digital ecosystem and mobile workforce enablement) with increased ease of use, while reducing costs and complexity via vendor consolidation and dedicated circuit offload
- Infrastructure and operations and security teams to deliver a rich set of networking and network security services in a consistent and integrated manner to support the needs of digital business transformation, edge computing and work from anywhere

Drivers

- SASE is driven by enterprise digital business transformation: the adoption of cloud-based services by distributed and mobile workforces, edge computing and business continuity plans that must include flexible, anywhere, anytime, secure remote access and use of the internet and cloud services.
- The need to flexibly support digital business transformation efforts with a zero trust security architecture while keeping complexity manageable is a significant factor for the adoption of SASE, primarily delivered as a cloud-based service (see The Future of Network Security Is in the Cloud). The COVID-19 pandemic accelerated these trends.
- For IT, SASE can reduce the deployment time for new users, locations, applications and devices as well as reduce attack surface and shorten remediation times by as much as 95%.
- Network security models based on data center perimeter security are ill-suited to address the dynamic needs of a modern digital business and its distributed digital workforce. This is forcing a transformation of the legacy perimeter into a set of cloud-based, converged capabilities created when and where an enterprise needs them — that is, a dynamically created, policy-based secure access service edge, or SASE.

Obstacles

- **Organizational silos, existing investments and skills gaps:** A full SASE implementation requires a coordinated and cohesive approach across network security and networking teams.
- **Organizational bias and regulatory requirements that drive continued on-premises deployment:** Some customers have an aversion to the cloud and want to maintain control.
- **Global coverage.** SASE depends upon cloud-delivery, and a vendor's cloud footprint may prevent deployments in certain geographies, such as China, Russia and the Middle East, where vendors may have limited cloud presence.
- **SASE security services maturity:** For the next several years, SASE capabilities will vary widely. Sensitive-data visibility and control is often a high-priority capability, but it is difficult for most SASE vendors to address. Your preferred vendor may lack the capabilities you require but two-vendor partnerships can be a viable approach.

User Recommendations

- Involve the CISO and network architect when evaluating offerings and roadmaps from incumbent and emerging vendors to ensure an integrated approach.
- Leverage WAN, firewall, VPN refresh or SD-WAN to update network and network security architectures.
- Strive for not more than two vendors for all core services to minimize complexity and improve performance.
- Identify required capabilities for networking and security, including latency, throughput, geographic coverage and endpoint types to develop evaluation criteria.
- Focus on vendors that include CASB if DLP is a priority. They have the most experience in this area.
- Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the numbers of vendors required. Deploy ZTNA to augment or replace legacy VPN to limit investment in legacy technology.
- Consolidate vendors to cut complexity and cost as contracts renew.
- Leverage branch office transformation and MPLS offload to adopt SASE for security services.

Sample Vendors

Cato Networks; Fortinet; Palo Alto Networks; Versa Networks; VMware; Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Market Guide for Zero Trust Network Access

The Future of Network Security Is in the Cloud

Magic Quadrant for WAN Edge Infrastructure

Magic Quadrant for Cloud Access Security Brokers

Market Guide for Zero Trust Network Access

Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge

NVMe-oF

Analysis By: Julia Palmer, Joseph Unsworth, Joe Skorupa

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Nonvolatile memory express over fabrics (NVMe-oF) is a network protocol that takes advantage of the parallel-access and low-latency features of NVMe Peripheral Component Interconnect Express (PCIe) devices. NVMe-oF tunnels the NVMe command to the remote subsystems. The specification defines a protocol interface and is designed to work with high-performance fabric technology, including remote directory memory access (RDMA) over Fibre Channel, InfiniBand or Ethernet with RoCEv2, iWARP or TCP.

Why This Is Important

NVMe-oF is a method of extending access to nonvolatile memory (NVM) devices, using the NVMe protocol to remote storage systems. This enables a front-end interface into storage systems, scaling out to large numbers of NVMe devices and extending the distance within a data center over which NVMe subsystems can be accessed. The goal of NVMe-oF is to significantly improve data center network latency and to provide comparable-to-local latency for remote NVMe devices.

Business Impact

- NVMe-oF offerings impact business use cases where low-latency application and workload requirements are critical to the bottom line.
- Though requiring potential infrastructure changes and upgrades, the clear benefits these technologies can provide will immediately attract high-performance computing customers who can quickly show a positive ROI.
- NVMe flash media with the combination of NVMe-oF protocols can deliver architectures that extend and enhance the capabilities of storage arrays.

Drivers

- NVMe is a storage protocol that is used within solid-state arrays and servers. It takes advantage of the latest NVM to address the needs of extremely-low-latency workloads and is now broadly deployed. However, the NVMe-oF data center storage protocol is still emerging and developing at different rates depending on the network encapsulation method.
- The NVMe-oF protocol can take advantage of high-speed networks and accelerate the adoption of next-generation storage architectures, such as disaggregated compute, scale-out software-defined storage, and hyperconverged and composable infrastructures, bringing super-low-latency application access to the mainstream enterprise.
- Unlike server-attached flash storage, shared accelerated NVMe and NVMe-oF can scale out to high capacity with high-availability features and be managed from a central location, serving dozens of compute clients.
- Most storage array vendors have already debuted at least one NVMe-oF capable product with nearly all vendors expected to do so within a year.
- In 2018, the NVMe standards body ratified NVMe/TCP as a new transport mechanism. In the future, it's likely that TCP/IP will evolve to be a very important data center transport mechanism for NVMe-oF.
- The application layer also plays a role in driving adoption. Support for NVMe-oF in 2020 (both FC-NVMe and RDMA over converged Ethernet) by VMware vSphere v.7.0 will help drive more mainstream usage; however, Microsoft is yet to make a similar announcement.

Obstacles

- Implementation of end-to-end NVMe-oF infrastructure could require substantial changes to not only storage platforms but also networking and servers depending on the existing infrastructure.
- I&O leaders are struggling to justify ROI for end-to-end NVMe deployments as only a small percentage of workloads will benefit from such uplift.
- The cost and complexity have impeded the adoption of NVMe-oF solutions in mainstream enterprises.
- Software support for NVMe-oF is still nascent but as it will expand and mature, I&O leaders will have an additional choice of either deploying NVMe-oF with RDMA RoCEv2 or NVMe-oF over TCP/IP-based products to leverage latest Ethernet deployment, thereby easing the transition and providing investment protection.

User Recommendations

- Identify workloads where the scalability and performance of NVMe and NVMe-oF-based solutions justify the premium cost of such deployment. Target it for AI/ML, high-performance computing (HPC), in-memory databases or transaction processing.
- Users should investigate any other potential infrastructure bottlenecks, and consult existing suppliers on potential performance and TCO gains to justify the ROI.
- Identify a potential storage platform, network interface controller, host bus adapter and network fabric suppliers to verify that interoperability testing has been performed and that references are available.
- Verify the availability of NVMe-oF networks for HCI deployments to see performance improvement.

Sample Vendors

Dell Technologies; Excelero; Hitachi Vantara; IBM; Lightbits; NetApp; Pavilion Data; Pure Storage; Vast Data; WekaIO

Gartner Recommended Reading

Emerging Technology Horizon for Communications

2020 Strategic Roadmap for Storage

Prepare Your Storage and Data Management Strategy for the Impact of Artificial Intelligence Workloads

Critical Capabilities for Solid-State Arrays

Your Server Is Eating Your Network — Time to Rethink Data Center Network Architectures

Sliding into the Trough

5G

Analysis By: Sylvain Fabre

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

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 is as low as 4 milliseconds in a mobile scenario and can be as low as 1 millisecond in ultra-reliable low-latency communication scenarios, and massive scalability. New system architecture includes core slicing as well as wireless edge.

Why This Is Important

5G is key for industry digital transformation, with 162 operators rollouts (Source: GSA, April 2021), 20% of mobile networks (up from 9% one year ago). 3GPP 5G standards releases deliver incremental functionality:

- R15: Extreme mobile broadband
- R16: Industrial IoT (massive IoT, slicing and security
- R17: MIMO enhancement of MIMO, Sidelink, DSS, IIoT/URLLC, bands up to 71GHz, nonterrestrial networks and RedCap
- R18: Under definition

Business Impact

- Material impact on multiple industries and use cases by enabling digital transformation.

- 5G enables three main technology deployment and business scenarios, which each support distinct new services, and possibly new business models (such as latency as a service), namely enhanced mobile broadband (eMBB) supports high-definition video, mMTC supports large sensor and IoT deployments, and URLLC covers high-availability and very low-latency use cases, such as remote vehicle/drone operations.

Drivers

- Increasing device penetration: Gartner estimates that 5G-capable handset penetration will reach 87% in 2023 in Western Europe, similar to North America.
- Operational cost savings for industry use cases.
- Agility — in particular, in oil and gas and manufacturing.
- Requirements from industrial users value 5G lower latency from ultra-reliable and low-latency communications (URLLC) and expect 5G to outperform rivals in this area.
- Demand for massive machine-type communications (mMTC), to support scenarios of very dense deployments up to 5G target of 1 million connected sensors per square kilometer.
- Increased availability of industry-specific spectrum options (e.g., CBRS).
- mMTC addresses the massive scale requirements of IoT.

Obstacles

- Availability of spectrum, in particular for industrial private networks, in some countries.
- Security concerns over certain vendors, and when using 5G in critical industrial scenarios.
- Readiness of R16 solutions; availability and pricing of networks and modules.
- Use of higher frequencies and massive capacity requires very dense deployments with higher frequency reuse.
- Uncertainty about use cases and business models that may drive 5G for many CSPs, enterprises, and technology and service providers (TSPs).

- Different dynamics by regions: where in many parts of Africa for example, 5G would not be the next step up from 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.
- Feedback from some industrial clients mentioned that the majority of their use cases could be serviced by a 4G private network, and/or NB-IoT and other LPWA such as LoRa.

User Recommendations

- Enable a diverse network that can offer adequate and cost-effective alternatives to 5G for many use cases (e.g., LPWA, NB-IoT, LoRa, Wi-SUN).
- Enable 5G for temporary enterprise connectivity, mobile and FWA secondary/tertiary use cases for branch location redundancy, as long as 5G is not the primary link for high-volume or mission-critical sites, unless there are no other options.
- Provide clear SLAs for network performance by testing installation quality for sufficient and consistent signal strength, signal-to-noise ratio, video experience, throughput and coverage for branch locations.
- Ensure backward compatibility to 4G devices and networks, so 5G devices can fallback to 4G infrastructure.
- Focus on architecture readiness — such as SDN, NFV, CSP edge computing and distributed cloud architectures, and end-to-end security — in preparation for 5G.
- Build their ecosystem of partners to target industry verticals more effectively with 5G.

Sample Vendors

Cisco; Ericsson; Huawei; Mavenir; Nokia; Qualcomm; Samsung; ZTE

Gartner Recommended Reading

U.S. Telco 5G Plans Take Shape

Emerging Technologies: 5G Technology Spending, 2020 Survey Trends

5G as a Service: Deployment Scenarios of Private Networks in the 5G Era

Market Guide for 5G Network Ecosystem Platform Providers

Creating Your Enterprise 4G and 5G Private Mobile Network Procurement Strategy and RFQ

400 Gbps Ethernet

Analysis By: Naresh Singh

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Adolescent

Definition:

IEEE 802.3bs Ethernet standard, that transmits Ethernet frames at 400 Gbps through a combination of four-level pulse amplitude modulation or traditional non-return-to-zero methods transmitting at four lanes of 100 Gbps, eight lanes of 50 Gbps or 16 lanes of 25 Gbps.

Why This Is Important

This is a logical upgrade from 100 Gbps for high-speed Ethernet networks. Although 800 Gbps standards are being developed, it is likely that 400 Gbps will be the go-to Ethernet high speed for the foreseeable future for users needing to go beyond 100 Gbps to maximize bandwidth in their data center and beyond for a number of reasons including demand and efficiencies.

Business Impact

400 Gbps Ethernet will be a niche technology for at least the next three years, mainly relevant to hyperscale cloud service providers and bandwidth-intensive communication service providers.

It is a critical requirement to address I/O-intensive applications such as artificial intelligence (AI)/machine learning (ML) and 8K media streaming preferably needing 25 Gbps and higher server access.

400 Gbps is increasingly needed for heavy-traffic data center interconnects and dense WAN transport legs.

Drivers

- Increasing bandwidth need is felt in both service provider and enterprise data centers as a result of users and applications becoming more bandwidth-hungry and demanding. And so 400 Gbps serves best where the economics justifies and demands the highest available packet per second Ethernet transport.
- 400 Gbps switches and optics have been available from a host of vendors for a few years. Although relatively new, it has been able to achieve early, but moderate, level adoption among mega cloud providers like Amazon, Alibaba, Apple, Facebook, Google and Microsoft, mostly in their data center spine layer and for their global backbone and interconnect usage.
- Large telcos like AT&T, Verizon, NTT, and Telstra have also been trialing 400 Gbps capabilities in their global optical backbones and in some cases providing Ethernet services based on it. Major data center interconnect vendors such as PacketFabric and Zayo have also started offering 400 Gbps as an option for their customers.*
- In January 2020, IEEE 802.3cm that enables 400 Gbps over multimode fiber for shorter distance use cases was ratified. This paves the way for a greater proliferation of 400G in intra DC east-to-west use cases in the leaf and spine layers of the Ethernet fabric.
- Multiple groups including OIF and OpenZR+ have been working to define a standard and testing for a coherent WDM-based 400G module targeting mid and long distances usage in data center interconnects and communications service provider (CSP) metro access and interconnects. Switch OEMs are testing these with large cloud and CSP operators. This is likely to open up more use cases for 400 Gbps in the short and midterm, making it more versatile as an option for high-speed Ethernet.

Obstacles

One of the biggest challenges for 400 Gbps is the lack of use case for it in the mainstream enterprise market. It is estimated that over 90% of the demand for 400 Gbps comes from hyperscale cloud providers and, to an extent, CSPs. Although there is increased shipment of 400 Gbps due to growth in demand from these sectors, it is forecast to remain niche for the rest of the market through 2023.

Cost-effective optics remain an issue with customers although a number of transceiver modules and cables (both active and passive) are available and supported by the leading Ethernet component and switch vendors. For some key cloud customers, this is leading to delayed deployments — as new options like 800 Gbps get ready to show up in the midhorizon, giving hopes of a better value vis-a-vis the cost.

User Recommendations

I&O leaders must:

- Prioritize 400 Gbps for their data center core if they plan to implement I/O-intensive applications like AI/ML and 8K streaming media. The technology is backward-compatible with 200 Gbps, 100s, 50 and 25 Gbps.
- Choose 400 Gbps for their intradata center aggregation and spine layer needs if they have an overgrown optical cable footprint and want to optimize cable runs.
- Check availability and roadmap for 400 Gbps links with the data center/cloud interconnect provider they are looking to work with or are already working with. Even if they don't require such high-speed links, they can expect more competitive offers for their links due to the efficiencies they achieve through their 400 Gbps links.
- Explore relevant third-party optical transceiver providers to bring down costs if optics costs have been the main hurdle for delaying deployments. Choose wisely from vendors that conduct rigorous testing with multiple OEM equipment and have a good track record for support.

Sample Vendors

Arista Networks; Edgecore Networks; Huawei; Juniper Networks

Gartner Recommended Reading

40G Is Dead — Embrace 100G in Your Data CenterHow to Avoid the Biggest Rip-Off in Networking

NaaS

Analysis By: Ted Corbett, Gaspar Valdivia, Jonathan Forest

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

NaaS is a delivery model for networking products. NaaS offerings deliver network functionality as a service, which include the following capabilities: self-service capability, on-demand usage, including dynamic scaling up and scaling down. It is billed on an opex model that is consumption-based, via a metered metric (such as ports, bandwidth or users), and not based on network devices/appliances. Its offerings may include elements such as network switches, routers, gateways and firewalls.

Why This Is Important

Many NSPs and non-NSPs are creating NaaS offers, while enterprises seek consumption-based spending for networking akin to what cloud offers for compute. Thus TSPs are investing to bring offerings to market to match these needs — marketed as NaaS. Globally, enterprise networking annual spending is $240 billion for 2020, and each provider wants their share. New entrants see huge enterprise spending, while many incumbents seek to hold on, invest in their NaaS strategy and grow amid emergent competition.

Business Impact

- Many enterprises pursue a flexible, consumption-based networking model regardless of user or application location. NaaS seeks to provide enterprises with agility, service delivery quality, automation and end-to-end customer experience — with up/down scalability and predictable all-opex spending.
- Emerging NaaS providers seek to disrupt current NSP vs. non-NSP customer consumption norms. Over time, this disruption is expected to expand enterprise buyer options and pricing models.

Drivers

- Many enterprises envision a future where their end-to-end networking estate spans LAN, data center and WAN edge cloud-based network functions, WAN services and life cycle network operations delivered in a consumption-based, predictable spending model.
- Though historically common, the all-opex network product procurement model where operational leases (rentals) turn an all-capex purchasing model into opex has long served the purpose of amortizing payment for networking products. However, they are not significantly more flexible than common capex-based approaches.
- Currently, the key drivers for an all-opex model for the enterprise have evolved: Enterprise buyers seek a greater focus on end users and their applications for improved service delivery quality, automation and predictable customer experience from the market. Also, WAN services from NSPs have increasingly evolved from enterprise locations to virtually any cloud-based provider or hosted endpoints. These continue to drive enterprise objectives for increased agility, more flexible consumption models and a seamless experience across their network consumption life cycle. Finally, NaaS providers see these bundled, opex-driven services as very "sticky," making it more difficult for enterprise clients to peel off individual components to seek out those with better value (cost and/or performance)
- More recently, in response to evolving enterprise needs, non-NSPs are seeking to drive revenue by pursuing their own emergent offers for NaaS.

Obstacles

- There is no evidence that buyers will pay less for any NaaS proposition from providers.
- Return on investment (ROI) models for a NaaS proposition do not exist from providers.
- Enterprises entering into NaaS agreements relinquish control over their network design and face full replacement of NaaS components upon early or end of term based exit events.
- Enterprises that sweat their network assets to reduce refreshes lose this flexibility, since NaaS providers become the entity sweating any assets included in their offers.
- NaaS offers currently in the market (primarily from NSPs) are not comprehensive solutions. These offers are focused on the provider's PoP where many NaaS components reside, such as gateways and cloud connectivity bandwidth on demand.
- The all-opex procurement is complicated by scaling, life cycle operations and refreshes of network product technologies.

User Recommendations

Exert caution with NaaS at this emerging market stage.

I&O leaders should:

- Avoid NaaS offers if you want to retain network design control or prefer to sweat assets beyond typical refresh cycles — smooth spending via financial leasing.
- Create a before and after ROI calculation by capturing all relevant in-scope costs and uniformly comparing proposals to identify the economic differences before further consideration.
- Choose NaaS to achieve operational, lease-based network spending when this is your primary goal and have a predictable consumption pattern.

Technology service providers should:

- Build NaaS capabilities by investing in consumption-based, commercial models across LAN, WAN and cloud connect services.

- Build trust in NaaS by providing itemized pricing, standardized service definitions, and scale up and down commercial flexibility.
- Prove to prospective buyers the commercial value of NaaS offers by disaggregating proposals and providing detailed comparison against alternative options.

Sample Vendors

Aryaka; AT&T; BT; Hewlett Packard Enterprise (HPE); Juniper; Microsoft; Open Systems; Orange; PacketFabric; Verizon

Gartner Recommended Reading

2020 Strategic Roadmap for Enterprise Networking

Magic Quadrant for Managed Network Services

Magic Quadrant for Network Services, GlobalDebunk the Misperceptions About Network as a Service

SD-Branch

Analysis By: Andrew Lerner

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Early mainstream

Definition:

SD-branch products allow multiple branch network functions to be managed as a single construct. They cover four network functions (WAN gateways, LAN switches, WLAN, firewalls), with unified configuration, policy, reporting, visibility and automation across the four functions via a single console. They offer zero-touch configuration for provisioning; automated operational tasks (e.g., troubleshooting, reporting, moves/adds/changes); and fully supported, documented and published APIs.

Why This Is Important

SD-branch enables simplified management of branch networking equipment. SD-branch enables enterprises to deploy a single policy via a central console that is automatically deployed to multiple devices. This concept of managing branch network devices via a single console is not new and has previously been referred to as BOB (branch office in a box). However, we are seeing renewed interest in this concept, including Gartner clients and vendors who promote the term extensively.

Business Impact

With SD-branch, IT staff can manage branch infrastructure in a simple, efficient manner. This can reduce opex for branch networking/security equipment, and increase uptime/availability in branches due to the simplified and integrated policy and UI. Organizations can then quickly and easily add new locations and new apps/user groups.

Drivers

- The enterprise need for SD-branch generally stems from the need for greater simplicity, agility and increased security via consistent policies across branch devices.
- SD-branch products are most compelling for smaller, distributed branch locations where it is challenging to get network personnel on-site.
- SD-branch solutions are being pushed by both product vendors and service providers who offer it as a turnkey managed service.
- We expect enterprises will seek single-vendor SD-branch deployments due to integration simplicity. However, in theory, SD-branch solutions can be single vendor or multivendor.

Obstacles

- Limited multivendor management support for organizations that use different vendors for SD-WAN, switching, security and WLAN
- Mismatched refresh cycles for switches, WLAN, WAN devices and security
- Limited budget and/or difficulty in identifying concrete ROI
- Lack of support from certain vendors
- A desire to limit or reduce branch network infrastructure, often in conjunction with a broader initiative to support WFA

User Recommendations

- Use SD-branch products if operational changes to branch networking equipment such as SD-WAN, firewalls, WLAN or switches are a substantial challenge or drain on personnel.
- Shortlist multiple suppliers and run a real-world pilot to validate functionality within your environment before making a long-term or strategic purchase from any specific vendor.
- When evaluating SD-branch solutions, prioritize the specific network function that is of highest importance for your environment, and focus on that function. Not all vendors have equal feature capability across all functions.
- Prefer SD-branch products that allow for management of multivendor environments to aid with transition and/or to protect existing investments.
- Include SD-branch solutions when refreshing branch equipment, but do not require that all functions be replaced at once.

Sample Vendors

Cisco; Fortinet; Hewlett Packard Enterprise (HPE); LANCOM Systems; Versa Networks

Gartner Recommended Reading

Magic Quadrant for WAN Edge Infrastructure

Network Automation

Analysis By: Josh Chessman, Andrew Lerner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Network automation tools automate the configuration, visibility, troubleshooting, reporting, and maintenance of physical and virtual network devices and services. Network automation tools can improve agility and operational efficiency, lower costs, reduce human error, and improve compliance with configuration policies.

Why This Is Important

We estimate that greater than 70% of enterprise networking activities are manual as of late 2020 (outside of public cloud environments). This lack of automation can create bottlenecks in provisioning/operations and increases likelihood of human errors, which in turn may drive outages and impact uptime. This can ultimately delay time to deliver services to lines of business (LOBs) and reduce availability of services.

Business Impact

Organizations, whether in the middle of digital transformation initiatives or not, are seeing a need for the network to become more responsive. Network automation (NA) tools allow organizations to ensure their networks meet high standards including reduced errors and support costs, improved uptime, and enhanced agility, to which users have become accustomed.

Drivers

- While organizations have been undergoing digital transformation for years, the acceleration seen in the past 12 months has drastically increased. In conjunction with this acceleration, organizations are becoming ever-more dependent on these digital initiatives to drive business value. A significant part of digital transformation is the ability for I&O to update its environment at ever-increasing rates.
- The traditional approach of manually updating each device with the appropriate settings is too slow, fraught with danger from typos and missed devices, and expensive due to increased personnel needs. Network automation tools allow organizations to make network changes across tens, hundreds, thousands, or more devices in short periods of time.
- As organizations grow, their tolerance for network outages decreases significantly. Making network changes, even with proper planning and change windows, can introduce unexpected issues that may have impacts beyond just the expected change areas. Organizations require scalable, high-quality NA tools that can effectively manage network change cycles where high change volumes and the risks of costly errors render manual changes impractical or ineffective, resulting in a need for NA tools.

Obstacles

- The skills required to implement and use these tools (such as Python or coding APIs) are often different from those traditionally associated with network engineering (such as CLI), potentially requiring additional training and staffing changes.
- Very few vendors offer NA tools that provide broad multivendor support for both Day 0/1 and Day 2 activities and strong support for WAN, campus, data center and cloud environments simultaneously. Thus, organizations struggle with tool sprawl, budget and suboptimal tools.
- While most NA tools provide support for a variety of vendor devices, there are times where vendors, products, or software or hardware revisions lack support, impacting the overall success of a deployment.
- The benefits of really good NA (versus mediocre) are apparent at the practitioner level, but can be very difficult to cost-justify the upstream investment.
- Testing and validation automation are only emerging in the NA space and are difficult to integrate with configuration change automation.

User Recommendations

- Create and maintain an accurate list of network devices with hardware and software revisions.
- Start small and iterate. Focus on nonchange/nonproduction activities first. Focus initially on tasks with less complex workflows that the network team has greater control over.
- Provide engineers appropriate time and training resources to learn the technology. Encourage them to familiarize themselves with common NA building blocks.
- Automate testing and change configuration rollback.
- Deploy NA in a practical fashion with a focus on both specific, contained areas within the organization along with nonchange activities (such as reporting and troubleshooting) before moving onto more robust functions.
- Identify tools that work with the skills within your organization and that match your organization's existing culture and workflows. For example, if your organization uses UIs for configuration changes, look for tools that do the same; if it uses CLIs for configuration changes, look for tools that operate similarly.

Sample Vendors

Cisco; Itential; Micro Focus; NetBrain; Network to Code; Red Hat

Gartner Recommended Reading

Market Guide for Network Automation and Orchestration Tools

Best Networking Practices in a DevOps WorldNetOps 2.0: Embrace Network Automation and Analytics to Win in the Era of ContinuousNext

Solution Path for Evolving to Next-Generation Enterprise Networks

Open Networking

Analysis By: Andrew Lerner, Mark Fabbi

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Open networking refers to: (a) the disaggregation of hardware and software on networking devices, and/or (b) the use of open-source networking software. Examples include disaggregated physical switches that conform to OCP specifications, and software such as SONiC and FRR. Most open networking technologies are based on Linux, and designed for data center environments, but are expanding into campus and WAN.

Why This Is Important

Open networking can reduce expenditures and increase flexibility while reducing vendor lock-in, which, when combined, can enable faster network innovation. Open-based networking is still in its early adoption phase for enterprise deployments, but is well-established in cloud and service provider networks.

Business Impact

Open networking options reduce reliance on tightly integrated vendor-proprietary approaches, which enables enterprise network teams to evolve at a pace that is not determined by a specific vendor. Ultimately, this can drive more-flexible and agile networking capabilities to support the business, and at a reduced acquisition cost.

Drivers

- In data center environments, there is increasing interest in Software for Open Networking in the Cloud (SONiC) as an open-source NOS, driven by a desire to move away from vendor-proprietary stack and/or leverage the pace of innovation associated with popular open-source initiatives. Technologically advanced organizations seek to standardize on an NOS that is supported across hardware vendors, creating the potential for innovation in the same manner that Linux offered in the server OS market.
- A strong commercial ecosystem is forming around SONiC. Dell Technologies, NVIDIA, Arista Networks, Juniper Networks and nearly all white-box vendors are on the official SONiC hardware compatibility list. Multiple vendors, including Dell Technologies and NVIDIA, provide commercial support and/or a commercial distribution for SONiC. This drives increasing customer interest.
- Brite-box switches offer disaggregated hardware and software, but are supported via a single commercial supplier and thus represent a more mainstream approach to leveraging the open networking movement. Brite-box solutions from vendors such as Dell Technologies and NVIDIA have over 4,000 production customers. These brite-box solutions are 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.
- Vendors are increasingly allowing modules to be loaded on supported NOSs, which enables organizations to run open-source software for specific features such as Border Gateway Protocol (BGP).
- In very large campus switching environments (100+ switches), technologically advanced enterprises are looking at brite boxes to reduce initial switching costs.
- Data center original design manufacturer (ODM) or white-box switches have an average selling price that is 76% less than traditional OEM switches. ODM switches are highly aligned with disaggregated switching, and accounted for 29% of unit shipments of data center switches in 2020.

Obstacles

- Many vendors lead with integrated switches, instead of brite-box offerings.
- The number of open-source software options (i.e., SONiC, OS10 Open Edition, OpenSwitch, etc.) could fragment efforts and delay broader adoption.
- A strong culture of risk aversion among enterprise network teams results in them preferring vendor-proprietary solutions.
- There is a perception that brite-box and/or open-source software will create new support challenges and/or increase support costs.
- Competition and acquisitions between vendors are limiting availability of brite-box options.

User Recommendations

- Organizations with larger data centers (100-plus switches) should include SONiC and brite-box options on their shortlist for refresh and build-out opportunities.
- Organizations with a strong cultural preference for open-source software should prefer SONiC in their data centers.
- Any organization pursuing a disaggregated open-source approach must have advanced technical expertise to deal with the support and integration requirements.

Sample Vendors

Dell Technologies; Edgecore Networks; IP Infusion; NVIDIA; Pica8

Gartner Recommended Reading

Market Guide for Data Center Switching

Service Mesh

Analysis By: Anne Thomas

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

A service mesh is a distributed computing middleware that optimizes communications between application services within managed container systems. It provides lightweight mediation for service-to-service communications, and supports functions such as authentication, authorization, encryption, service discovery, request routing, load balancing, self-healing recovery and service instrumentation.

Why This Is Important

A service mesh is lightweight middleware for managing and monitoring service-to-service (east-west) communications, especially among microservices running in ephemeral managed container systems, such as Kubernetes. It provides visibility into service interactions, enabling proactive operations and faster diagnostics. It automates complex communication concerns, thereby improving developer productivity and ensuring that certain standards and policies are enforced consistently across applications.

Business Impact

- A service mesh helps ensure resilient and secure request-response communication between services deployed in Kubernetes and other managed container systems.
- Service mesh middleware is one of many management technologies that provide software infrastructure for distributed applications deployed in managed container systems.
- This type of middleware, along with other management and security middleware, helps provide a stable environment that supports “Day 2” operations of containerized workloads.

Drivers

- Service mesh adoption is closely aligned with microservices architectures and managed container systems like Kubernetes. Service mesh supports needed functionality in ephemeral environments, such as service discovery and mutual Transport Layer Security between services.
- As microservice deployments scale and grow more complex, DevOps teams need better ways to track operations, anticipate problems and trace errors. Service mesh automatically instruments the services and feeds logs to visualization dashboards.
- A service mesh implements the various communication stability patterns (including retries, circuit breakers and bulkheads) that enable applications to be more self-healing.
- Many managed container systems now include a service mesh, inspiring DevOps teams to use it. The hyperscale cloud vendors provide a service mesh that is also integrated with their other cloud-native services.
- Independent vendors, such as Buoyant, HashiCorp and Kong provide service meshes that support multiple environments.

Obstacles

- Service mesh technology is immature and complex, and most development teams don’t need it. It can be useful when deploying microservices in Kubernetes, but it’s never required.
- Users are confused by the overlap in functionality among service meshes, ingress controllers, API gateways and other API proxies. Management and interoperability among these technologies hasn’t yet been addressed by the vendor community.
- Many people associate service mesh exclusively with Istio, even though it isn’t the most mature product in the market and has a reputation for complexity.
- Independent service mesh solutions face challenges from the availability of platform-integrated service meshes from the major cloud and platform providers.

User Recommendations

- Delay adoption of service mesh until your teams start building applications that will get value from a mesh, such as applications deployed in managed container systems with a large number of service-to-service (east-west) interactions.
- Favor the service meshes that come integrated with your managed container system unless you have a requirement to support a federated model.
- Reduce cultural issues and turf wars by assigning service mesh ownership to a cross-functional PlatformOps team that solicits input and collaborates with networking, security and development teams.
- Accelerate knowledge transfer and consistent application of security policies by collaborating with I&O and security teams that manage existing API gateways and application delivery controllers.

Sample Vendors

Amazon Web Services; Buoyant; Decipher Technology Studios; Envoy; F5; Google; HashiCorp; Istio; Kong; Microsoft; Red Hat; Solo.io; Tetrate; VMware

Gartner Recommended Reading

How a Service Mesh Fits Into Your API Mediation Strategy

Assessing Service Mesh for Use in Microservices Architectures

Emerging Technology Analysis: Service Mesh

Intent-Based Networking

Analysis By: Andrew Lerner

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

An intent-based networking system (IBNS) is a closed-loop system to help design, provision and operate a network based on business policies. It is typically packaged as software. A full IBNS includes four key subcomponents: (1) translating higher-level business policies to network configurations; (2) automating network activities across network components; (3) having awareness of network state/health; and (4) providing continuous assurance and enabling dynamic optimization.

Why This Is Important

IBNSs simultaneously improve network agility and reliability, while enabling unified policy across multiple infrastructures.

Business Impact

A full IBNS implementation can reduce the time to deliver network infrastructure to business leaders by 50% to 90%, while simultaneously reducing the number and duration of outages by 50%.

There has been limited impact to date, due to low real-world adoption and lack of viable, easy-to-use full IBNS products. Instead, there is incremental adoption of subcomponents of IBNS, including network automation and assurance. These subcomponents are sold and implemented independent of a full IBNS.

Drivers

- The desire to make networks more agile in conjunction with cloud deployments and digital business.
- Reduced operating expenditure (opex) associated with managing networks, and more senior-level network resources free to focus on more important strategic tasks.
- Performance optimization: Intent-based algorithms provide better traffic engineering versus traditional approaches, such as routing protocols. This can improve application performance.
- Reduction in dedicated tooling costs as automation and orchestration are embedded in IBNS.
- Real-time self-documentation, which also includes the rationale (intent) behind design/configuration decisions.
- Improved compliance and simplified auditing, due to the algorithmic correctness of configurations, direct mapping to business intent, and ongoing, dynamic and real-time validation.

Obstacles

- Very few vendors provide full IBNSs. One of the reasons for this is that IBNSs are very hard for vendors to build and generalize. Instead, vendors release products that deliver some discrete benefits individually, often with limited integration between them.
- Nearly all products that are marketed by vendors as “intent based” fall short of the full capabilities of an IBNS. As of early 2021, real-world enterprise adoption of full IBNSs is nascent. We estimate fewer than 100 full deployments that meet all aspects of the definition.

User Recommendations

- Tune out vendor marketing of products listed as “intent-based” or “intent-driven.” Instead, invest in products that enable network automation and provide network assurance, AIOps and/or predictive analytics.
- Invest in network products that provide specific actionable recommendations (down to the device and configuration level) when purchasing equipment and tooling solutions. The combination of these investments can help to enable closed-loop automation and operations.

Gartner Recommended Reading

Market Guide for Network Automation and Orchestration Tools

NFV

Analysis By: Bjarne Munch, Mike Toussaint

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Network function virtualization (NFV) virtualizes network functions (such as firewalls, WAN optimization, SD-WAN and routing) that can be deployed as software on open server platforms or universal customer premises equipment (uCPE) platforms, as opposed to dedicated physical appliances. Virtual network functionality can be deployed both on-site and off-site, in branch offices, internal data centers, providers' point of presence, cloud services, or hosting facilities.

Why This Is Important

NFV and related uCPE are important because these technologies offer enterprises an opportunity to improve their WAN architectures by making their WAN more agile, flexible and scalable.

Business Impact

There are three main value propositions of NFV:

- Off-site-deployed NFV can improve enterprise network agility because it enables enterprises to rapidly deploy new functionality where needed.
- Off-site-deployed NFV can facilitate simplification of branch office designs.
- For branch office uCPE-based NFV, business impacts are mainly due to the ability to consolidate functionality on fewer appliances, and to enhance deployment flexibility and ability to move functions to different platforms if needed.

Drivers

- NFV has grown out of the requirement to support and consolidate multiple network functions at the WAN edge. However, the ability to move functions out of branch office and centralized data centers to off-site provider nodes is now a key driver as it enables simpler branch office design as well as more scalable solutions.

Obstacles

- Lack of best practices and standardized dimensioning of the uCPE platform to suit multiple NFV, leading to performance issues due to lack of procession power or memory
- Insufficient guidelines from the vendors that specify what type of virtual network functions (VNFs) can work together on specific platforms
- Limitations of standard orchestration systems, leading to cumbersome processes when deploying VNFs on remote uCPE platforms

User Recommendations

- Prefer off-site NFV services, as opposed to on-site, for optimum scalability and cost-efficiency, and establish strategies to evolve these services to SASE.
- For on-site deployments, do not deploy uCPE in-house without following VNF vendors' precertified configurations, unless there are sufficient IT resources to perform detailed technical evaluations and full load testing. Ensure that any proof of concept or pilot is performed with all functionality required on the uCPE to ensure these functions operate acceptably together on the chosen hardware, at the required traffic load.
- For off-site NFV, ensure that virtual functionality is located close to the enterprise locations (ideally not more than a 10 ms to 20 ms round-trip delay). Also ensure that providers offer sufficient resilience in their NFV node design, such as redundant nodes.

Sample Vendors

AT&T; BT; Cisco; NTT; OBS; VMware

Gartner Recommended Reading

Pump the Brakes on Network Function Virtualization Services

Climbing the Slope

SDN

Analysis By: Andrew Lerner, Joe Skorupa, Mark Fabbi

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Obsolete

Definition:

Software-defined networking (SDN) is an architectural approach to designing, building and operating networks that promised increased agility and extensibility by decoupling the network topology from the control plane.

Why This Is Important

SDN products never made it to mainstream enterprise adoption. Rather, SDN spawned innovations in automation, orchestration and programmability. This paved the way for things like SD-WAN, microsegmentation, brite-box switching and SD-branch.

Business Impact

There is very little direct commercial impact of full SDN solutions. However, products that are marketed as “SDN” (but don’t meet the architectural definition) can increase network agility, simplify management, improve security and lead to reductions in operational and capital expenses, while fostering cross-functional collaboration.

Drivers

- SDN was driven initially by academia, combined with large network operators that were looking to drive innovation into traditional proprietary networking solutions.
- Early SDN drivers were aligned with separating hardware from software, to foster innovation in both hardware and software, while increasing agility with the potential to lower costs.
- While technologically obsolete, SDN terminology is widely used by vendor marketing efforts. This remains the top driver behind SDN discussions today.

Obstacles

- There are effectively no SDN technologies available in the mainstream marketplace today. Thus, true SDN technologies have not achieved any significant enterprise market traction.
- Vendors widely market non-SDN technologies as SDN, leading to customer confusion and misinformation.
- The hope that SDN would allow the decoupling of the control plane from network hardware and foster independent software innovation never came to fruition.

User Recommendations

- Don't get caught up in the hype and vendor claims that commercial products are SDN or engage in any discussions/planning to deploy it. SDN is not the answer to any enterprise networking challenge today.
- Focus on reducing or eliminating the "human middleware" (i.e., manual operations) problem that has plagued traditional network solutions for the past two decades. This can be achieved by executing network automation initiatives to reduce human errors, increase quality, improve agility and cut costs.

Sample Vendors

NEC

Gartner Recommended Reading

State of SDN: If You Think SDN Is the Answer, You're Asking the Wrong Question

ZTNA

Analysis By: John Watts, Lawrence Orans, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Zero trust network access (ZTNA) creates an identity- and context-based logical access boundary around applications. Applications are hidden from discovery and access is restricted via a trust broker to a set of named entities. The broker verifies identity, context and policy adherence of specified participants and devices before allowing access, and prohibits lateral movement in the network. This removes public visibility of applications and significantly reduces the attack surface area.

Why This Is Important

ZTNA is a key technology for enabling user-to-application segmentation through a trust broker, to enforce a security policy that allows organizations to hide private applications and services and enforces a least-privilege access model for applications. It is a synthesis of concepts in the Cloud Security Alliance's Software-Defined Perimeter (SDP) guide, Google's BeyondCorp vision and O'Reilly's Zero Trust Networks book.

Business Impact

ZTNA yields immediate benefits by shielding services from attackers. In contrast to basic VPN products, ZTNA removes full network access and improves user experience, flexibility and adaptability. It enables more granular user-to-application segmentation through simplified policy management. Cloud-based ZTNA offerings improve scalability and ease of adoption. Early products on the market focused on web applications, but have expanded to work with a wider range of applications and protocols.

Drivers

- The need to support digital business transformation scenarios ill-suited to legacy access approaches, such as access to applications, services and data located outside the enterprise.
- Need for flexibility to quickly expand capacity as the sudden shift to remote work in 2020, with the onset of the COVID-19 pandemic, strained legacy on-premises VPN infrastructure.
- The rise of zero trust initiatives within organizations, which resulted in the need for more precise access and session control in on-premises and cloud applications.
- A desire for vendor consolidation, to remove point solutions and adopt more products from vendors with SASE frameworks, resulting in ZTNA additions to existing SWG or CASB services.
- A need to connect third parties such as suppliers, vendors and contractors to applications securely without exposing the network over VPN, or to connect the application to the internet for access.
- Mergers and acquisitions enabled by the ability to extend application access to acquired companies preclosure without needing to deploy endpoints or connect networks directly between the two companies.

Obstacles

- Cost: ZTNA is typically licensed per named user on a per user per year basis and may cost more than traditional VPNs.
- Limited support: Not all products support all applications. For example, some only support web, RDP and SSH protocols.
- Agent or agentless ZTNA: Some providers only offer one way to consume ZTNA. This limits applicable use cases.
- Weak identity management: Organizations with no federated identity support in the cloud find limitations with use cases as many providers rely on third-party identity providers for user authentication.
- Lack of on-premises trust brokers: Cloud-based trust brokers work well for remote access, but may not be preferred to extend the same policies on-premises. While providers exist that have both cloud and on-premises trust brokers, they are far and few between.
- Limited knowledge of acceptable application access rights for users: Organizations must map the correct application accesses upfront to get full benefit of ZTNA.

User Recommendations

- Open applications and services without requiring the use of a VPN or DMZ.
- Normalize the user experience for application access both on and off the corporate network.
- Implement application-specific access for employees and IT contractors as an alternative to VPN-based access.
- Extend access to systems prior to a merger, without having to configure site-to-site VPN and firewall rules.
- Allow access on personal devices by reducing full bring your own device (BYOD) management requirements and enabling more secure direct application access.
- Cloak systems from hostile networks, such as collaboration systems exposed to the internet.
- Permit users in potentially dangerous areas of the world to interact with applications and data to reduce or eliminate risk.
- Secure access to enclaves of Internet of Things (IoT) devices if the device can support a lightweight SDP agent or a virtual-appliance-based connector on the IoT network segment for connection.

Sample Vendors

Akamai; Appgate; Cato Networks; Ivanti; Netskope; Perimeter 81; Proofpoint; SAIFE; Zscaler

Gartner Recommended Reading

Market Guide for Zero Trust Network Access

Solving the Challenges of Modern Remote Access

Quick Answer: Cost Effectively Scaling Secure Access While Preparing for a Remote Workforce

Quick Answer: How to Securely Enable Access for Unmanaged Devices

2021 Strategic Roadmap for SASE Convergence

Identity-Based Segmentation

Analysis By: Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, Shilpi Handa

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Identity-based segmentation (also referred to as microsegmentation, zero-trust network segmentation or logical segmentation) can create more granular and dynamic policies than traditional network segmentation, which is limited to IP/VLAN circuits. “Identity-based” refers to workload identity, not user identity.

Why This Is Important

Certain attacks — such as ransomware attacks — can cause serious damage if allowed to spread laterally. Identity-based segmentation seeks to limit the propagation of such attacks.

Business Impact

Identity-based segmentation can reduce the risk and impact of cyberattacks. Identity-based segmentation is a form of zero-trust networking and is used to reduce the damage if and when an attacker breaches the enterprise network. This is done by reducing the ability of the attacker to spread laterally. Identity-based segmentation also enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads, including workloads that host containers that meet compliance requirements.

Drivers

- As more servers are being virtualized or moved to infrastructure as a service (IaaS), traditional firewall, intrusion prevention, and antivirus are rarely able to follow the fast pace of deployment for new assets. This leaves the enterprise vulnerable to attackers gaining a foothold and then moving laterally within enterprise networks. This has created increased interest in visibility and granular segmentation for east-west traffic between applications, servers and services in modern data centers.
- The increasingly dynamic nature of data center workloads makes traditional network-centric segmentation strategies operationally complex, if not impossible to apply.
- Some identity-based segmentation solutions provide rich application communication mapping, allowing data center teams to identify where communication paths are valid and secure.
- The shift to microservices container architectures for applications has also increased the amount of east-west traffic and further complicated the ability of network-centric firewalls to provide this segmentation.
- The extension of data centers into public cloud has also placed a focus on software-based approaches for segmentation — in many cases, using the built-in segmentation capabilities of the cloud providers.
- Growing interest in zero-trust networking approaches has also increased interest in using application and service identities as the foundation for adaptive application segmentation policies. This is critical to enforcing segmentation policies in the dynamic networking environments used within container-based environments.

Obstacles

The most frequent obstacles to identity-based segmentation are:

- Complexity: If not planned and scoped correctly, identity-based segmentation projects can lose organizational support before completion.
- Lack of knowledge: Security and risk leaders don’t know which applications should be communicating with others, sowing doubt in automatically-generated firewall rules.

- Legacy network firewalls: Some data centers have network firewalls for broader east-west traffic segmentation, which is adequate for some organizations. Traditional firewalls can also present operational challenges to some identity-based segmentation solutions.
- Organizational dynamics: Cloud-centric organizations employing DevOps may value agility more than security, believing that any additional security controls will introduce operational friction.
- Expense: Full microsegmentation can come at a high price. Many organizations consider identity-based segmentation to be a net new budget item.

User Recommendations

- Use a network flow mapping project to understand application and server flows.
- Start small and iterate with basic policies. Oversegmentation is the leading cause of failure and an unnecessary expense for segmentation projects.
- Do not use IP addresses or network location as the foundation for east-west segmentation policies. Use the identities of applications, workloads and services — either via logical tags, labels, fingerprints or stronger identity mechanisms.
- Use the ID-based segmentation style (agent-, network- or hypervisor-based) that covers both the location of the workloads (on-premises, hybrid and IaaS) and the type of environment in which workloads are hosted (containers and virtual machines).
- Apply continuous adaptive segmentation. Start with new assets, then close existing gaps. Identify quick wins, and mix zoning governing principles when needed.
- Adopt a risk-based approach and look beyond technical considerations.
- Consider products with established security expertise. Isolation alone isn't segmentation. If mediated communication is needed between zones, different functionality is required.
- Plan for coexistence of traditional firewalls and ID-based segmentation approaches for the next five years, and seek products that can support using both.

Sample Vendors

Amazon Web Services; Cisco; ColorTokens; Guardicore; Illumio; Microsoft; Palo Alto Networks; vArmour; VMware; Zscaler

Gartner Recommended Reading

Three Styles of Identity-Based Segmentation

SD-WAN

Analysis By: Andrew Lerner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Software-defined wide-area network (SD-WAN) products replace traditional branch routers. They provide dynamic path selection based on business or application policy, centralized policy and management of appliances, VPN, 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.

Why This Is Important

SD-WAN improves site availability, cost and performance for enterprise WANs, and is aligned with the broader shift of applications to public cloud workloads. There is high client interest in SD-WAN products, and we estimate that more than 50,000 customers have deployed SD-WAN products in production networks. Further, we expect continued rapid growth of SD-WAN deployments, and forecast vendor revenue to grow at a more than 20% compound annual growth rate (CAGR) for the next three years.

Business Impact

SD-WAN products create simpler and more cost-effective branch office WANs that map to modern application and cloud architectures. These products are significantly faster, easier to deploy and more manageable than traditional, router-based solutions. The benefits of an SD-WAN include reduced capital and operational expenditures (capex/opex) at the WAN edge, reduced device provisioning times, easier alignment with applications, and enhanced branch availability, compared with traditional routers.

Drivers

- Digitalization and cloud adoption are driving more applications out of private data centers and to public Internet, including SaaS and public cloud providers.
- In conjunction with hybrid or all-internet WAN topologies, SD-WAN improves availability, cost and performance for enterprise WANs.
- Organizations moving to hybrid or internet-only WAN transport are driven toward SD-WAN products because of their improved path-selection functionality and manageability.
- Several dozen vendors are competing in the market, including incumbent network and security vendors, startup vendors and smaller vendors with a regional or vertical focus. These vendors are aggressively pushing SD-WAN products and services to enterprises.

Obstacles

- Inability to get out of an existing equipment or service provider contract.
- WAN architecture is not hybrid and/or branch locations have only a single connection.
- Lack of budget.
- Closure of remote locations due to broader business reasons.
- Lack of cloud adoption, which reduces the benefits of hybrid WAN architectures.
- Limited need for increased branch availability.
- Inability to utilize the internet as transport, often due to compliance or security concerns, or lack of reliable connectivity.
- Existing WAN edge products (firewalls/routers) are good enough to meet business requirements.

User Recommendations

- Refresh your branch WAN equipment by implementing SD-WAN when you're migrating apps to the public cloud, building hybrid WANs, equipment is at end of life, or managed network service/MPLS contracts are renewing.
- Follow a thorough SD-WAN selection process by shortlisting a diverse set of vendors/providers and running a pilot.
- Include network security teams in the design, planning and implementation, because SD-WAN-enabled hybrid WANs directly affect placement of security controls, such as firewalls and secure web gateways (SWGs). SD-WAN should be designed in conjunction with a SASE architecture.

Sample Vendors

Cisco; Citrix; Fortinet; Hewlett Packard Enterprise (HPE); Palo Alto Networks; Versa Networks; VMware

Gartner Recommended Reading

Magic Quadrant for WAN Edge Infrastructure

Critical Capabilities for WAN Edge Infrastructure

Magic Quadrant for Network Services, Global

Toolkit: RFP Template for Managed and DIY SD-WAN Products and Services

2021 Strategic Roadmap for SASE Convergence

IPv6

Analysis By: Neil Rickard

Benefit Rating: Low

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Internet Protocol version 6 (IPv6) is the next version of Internet Protocol (IP). It's designed to overcome several key limitations of Internet Protocol version 4 (IPv4) — in particular, the exhaustion of new public IPv4 addresses.

Why This Is Important

New allocations of public IPv4 addresses are no longer available from the internet registrars, so new public IP addresses will be IPv6 only. The continued growth of the internet, including new consumer internet access in emerging markets, mobile devices and the Internet of Things (IoT), will increasingly be accommodated using IPv6, while existing IPv4 addresses will continue in use.

Business Impact

Enterprises that do not enable IPv6 for their external-facing services risk a poor user experience for IPv6-based end users, including their own work-from-home users, as the traffic will have to flow through carrier network address translation (NAT) engines, degrading performance and obscuring end-to-end visibility.

Large-scale specialist networks, such as some IoT networks, need more addresses than can be easily accommodated with IPv4 and so require IPv6.

Drivers

- The continued growth of the internet, especially IoT, will be accommodated using IPv6. Google IPv6 statistics show nearly 35% of users accessing Google do so using IPv6.
- Supporting IPv6 for external-facing applications will improve performance and visibility for enterprises' customers, partners and remote employees connecting via an IPv6-only internet provider or from IPv6-only devices, as it will avoid the need for that traffic to flow through carrier-scale NAT-degrading performance and obscuring end-to-end visibility.
- Enterprises are increasingly discovering pockets of IPv6 appearing within their organizations, especially in IoT use cases. These include sensor networks, process automation systems and building environmental control networks, as many of these systems will only support IPv6 or require such a large number of endpoints that IPv4 addresses cannot easily accommodate them.
- Selling unused publicly registered IPv4 addresses can help offset the costs of IPv6 migration.
- Some governments have mandated IPv6 adoption by public-sector organizations.

Obstacles

- The installed base of IPv4 infrastructure is massive and operational migration costs are high.
- Many systems have lower performance running IPv6 compared with their IPv4 performance.
- IPv6 represents a greater security risk than IPv4, as there is much less practical experience with securing IPv6 networks.
- Most enterprises have public IPv4 addresses for their external services and use private IP addressing internally (using the RFC 1918 standard). In addition, there is an active market for IPv4 address transfers between organizations, resulting in less urgency to adopt IPv6.

User Recommendations

- Enable IPv6 on the enterprise public internet presence. Supporting external IPv6 connectivity will improve performance and visibility for enterprises' IPv6-only customers, partners and remote employees connecting via an IPv6-only internet provider or IPv6-only mobile device.
- Undertake IPv6 planning, including determining which systems and equipment are IPv6-ready and which are not and establishing a transition roadmap. We do not currently recommend migrating to IPv6 for all internal systems.
- Build new greenfield networks to support both protocols from the outset. Every new item of network and IT hardware or software with network capability should have IPv6 support.
- Implement IPv6 for specialty networks where it provides a specific advantage (for example, when scale is critical, intercompany/interagency addressing is required, or networks are frequently set up and torn down).
- Support both IPv4 and IPv6 through at least 2026.

Gartner Recommended Reading

Best Practices for IPv4 Trading and the Move to IPv6

Wi-Fi 6 (802.11ax)

Analysis By: Tim Zimmerman

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Wi-Fi 6 (802.11ax), ratified in February 2021, is the latest iteration of the IEEE 802.11 WLAN family. It allows the network to control device connectivity and improves the efficiency of how Wi-Fi uses existing 2.4GHz and 5GHz spectrums. This increases throughput in densely populated areas. Its goal is to support a larger number of devices, including Internet of Things (IoT) devices, that are properly connected to the network.

Why This Is Important

The accumulation of 15 billion IoT devices and the convergence of building automation and line-of-business devices onto the enterprise infrastructure continue to contribute to congestion. It will be important for the network to utilize resources more intelligently instead of letting the device make connectivity decisions. This means that the issue of "sticky" clients is resolved because the network will automatically move the client to a new access point.

Business Impact

For IT leaders, Wi-Fi 6 (802.11ax) represents an opportunity to significantly improve performance for use cases such as dense device deployments. Advancements allowing differing streams to communicate to multiple devices simultaneously will assist in cutting latency by as much as 75% from previous versions while maintaining backward compatibility. With better control of the physical network, we expect enterprise network vendors to offer service-level agreements (SLAs) for client performance.

Drivers

- **The need for better network control:** The ability for access points to control client association helps with client connectivity and steering but also allows the network to address congestion for the campus infrastructure as a whole rather than from the view of a single client.
- **The ability to separate clients into differing radio streams:** This allows the access point to separate one-stream and two-stream client devices from clients with four or more streams, while providing simultaneous client communication.
- **Better battery life for mobile clients:** Higher performance provided by Wi-Fi 6 (802.11x) means that the radio, which consumes a lot of energy in transmission, is on less, implying better battery life for mobile clients.

Obstacles

- **Surplus performance:** IEEE Wi-Fi 6 (802.11ax) theoretically provides performance of up to 10 Gbps in a single coverage area. High-definition unicast video is often 2 Mbps to 3 Mbps per client and 4K streaming requires only 25 Mbps. This means 802.11ax has the ability to address the performance needs of approximately 400 simultaneous users in a single coverage area, even though it is difficult for that many people to be in a single coverage area at one time.
- **Required wired infrastructure upgrade:** The uplink ports of IDF switches will need to be upgraded either to 802.3bz or something higher than the 1 Gbps ports since the radio performance of one or more access points will exceed the wired connection.
- **Price:** The list price for 802.11ax access points ranges between $700 and $2,000, which is significantly higher than IEEE 802.11ac.

User Recommendations

- Do not pay a premium for any adoption of Wi-Fi 6 (802.11ax) unless existing wireless solutions are unable to provide the performance and functionality needed to meet defined end-user requirements.
- Require vendors to upgrade or update to be standards-compliant at no cost when purchasing a prestandard Wi-Fi-6-certified product.
- Be aware of product end-of-life status of access points since silicon vendors will limit the production of previous versions of radio chips, which will cause vendors to shorten the availability of some models and only offer newer access point versions.

Sample Vendors

Aruba; Broadcom; Cisco; Extreme Networks; Huawei; Juniper Networks; Qualcomm

Gartner Recommended Reading

Magic Quadrant for Wired and Wireless LAN Access Infrastructure

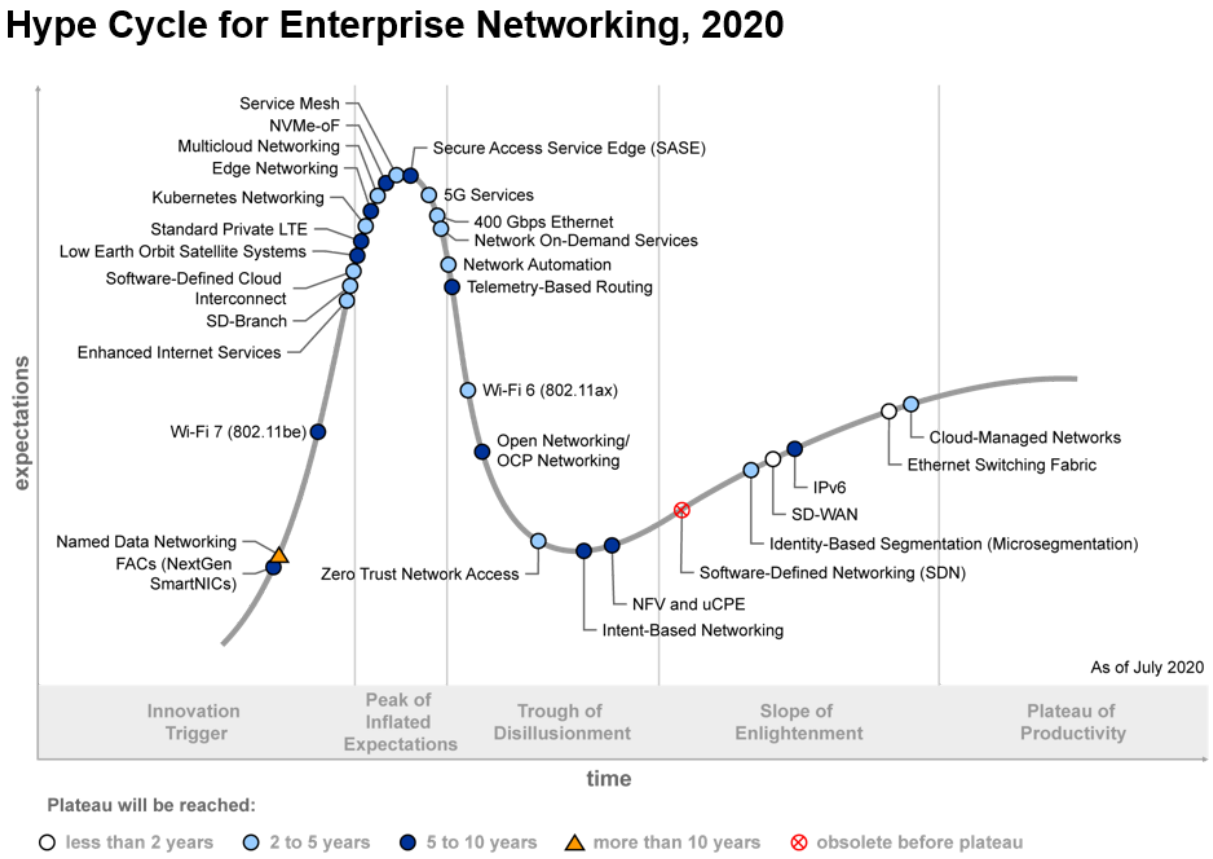
Critical Capabilities for Wired and Wireless LAN Access Infrastructure

Next-Gen Campus Connectivity Must Start by Defining the End-User Experience

Cloud and Edge Infrastructure Primer for 2021

Appendixes

Figure 2: Hype Cycle for Enterprise Networking, 2020



Source: Gartner (July 2020)

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media 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 innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation 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 innovation'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 innovation 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 innovation to reach the Plateau of Productivity.

Source: Gartner (July 2021)

Table 3: 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 (July 2021)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	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 (July 2021)

Evidence

Gartner analysts have taken over 5,000 inquiries on the topic of networking from 20 May 2020 through 19 May 2021.

Networking Hype Index — To help identify and select the most hyped networking terms, Gartner researchers compiled a hype index that measures the overall hype associated with specific networking technologies. This hype index was a composite metric that included client interest (inquiry and search), Google trends, articles in popular periodicals, analyst opinion and social media impressions.

Document Revision History

Hype Cycle for Enterprise Networking, 2020 - 8 July 2020

Hype Cycle for Enterprise Networking, 2019 - 9 July 2019

Hype Cycle for Enterprise Networking and Communications, 2018 - 13 July 2018

Hype Cycle for Enterprise Networking and Communications, 2017 - 20 July 2017

Hype Cycle for Networking and Communications, 2016 - 27 July 2016

Hype Cycle for Networking and Communications, 2015 - 27 July 2015

Hype Cycle for Networking and Communications, 2014 - 22 July 2014

Hype Cycle for Networking and Communications, 2013 - 26 July 2013

Hype Cycle for Networking and Communications, 2012 - 27 July 2012

Hype Cycle for Networking and Communications, 2011 - 24 August 2011

Hype Cycle for Networking and Communications, 2010 - 4 August 2010

Hype Cycle for Networking and Communications, 2009 - 28 July 2009

Hype Cycle for Networking and Communications, 2008 - 9 July 2008

Hype Cycle for Networking and Communications, 2007 - 26 July 2007

Hype Cycle for Networking and Communications, 2006 - 14 July 2006

Recommended by the Authors

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

Understanding Gartner's Hype Cycles

Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

2020 Strategic Roadmap for Enterprise Networking

Table 1: Priority Matrix for Enterprise Networking, 2021

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		SASE	AIOps Platforms FACs (NextGen SmartNICs) LEO Satellite Systems	6G Named Data Networking
High	SD-WAN Wi-Fi 6 (802.11ax)	5G Network Automation	NVMe-oF Private 5G	
Moderate	Identity-Based Segmentation	400 Gbps Ethernet eBPF Enhanced Internet Kubernetes Networking (CNI) Multicloud Networking SD-Branch Service Mesh Software-Defined Cloud Interconnect ZTNA	NFV Open Networking Wi-Fi 7 (802.11be)	Intent-Based Networking
Low			IPv6 NaaS	

Source: Gartner (July 2021)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media 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 innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation 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 innovation'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 innovation 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 innovation to reach the Plateau of Productivity.

Phase ↓	Definition ↓

Source: Gartner (July 2021)

Table 3: 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 (July 2021)

Table 4: Maturity Levels

Maturity Levels ↓	*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 (July 2021)