Gartner®

Hype Cycle for Enterprise Networking, 2023

Published 12 July 2023 - ID G00790717 - 108 min read

By Analyst(s): Andrew Lerner, Nauman Raja, Karen Brown

Initiatives: I&O Platforms

There is a range of networking technologies gaining steam, including quantum networking, network sustainability, network twins, and service connectivity layer. I&O networking leaders should use this research to prioritize investment and optimize adoption of emerging network technologies.

Analysis

What You Need to Know

Technology refresh drives most enterprise network investment today. However, I&O networking leaders are being asked to deliver increasing automation and secure networks as their organizations digitally transform, regardless of whether a refresh is in-scope.

Thus, organizations must invest differently as they modernize, which requires rethinking many long-standing "best practices" derived in an era when user locations were less dynamic and distributed and most apps were in the corporate data center. In order to deliver the right amount of networking, at the right time and cost to support the business' digital objectives, I&O networking leaders should look at the technological innovations covered in this research.

The Hype Cycle

This research describes the 30 most hyped innovations in networking. For each hyped technology, we define it, describe its value, and identify adoption and drivers/inhibitors of growth. Over one-third of the technologies profiled in this research has changed from last year.

New hype: Several new hyped technologies were added this year, including:

- CBaaS (cloud backbone as a service)
- Digital network twin

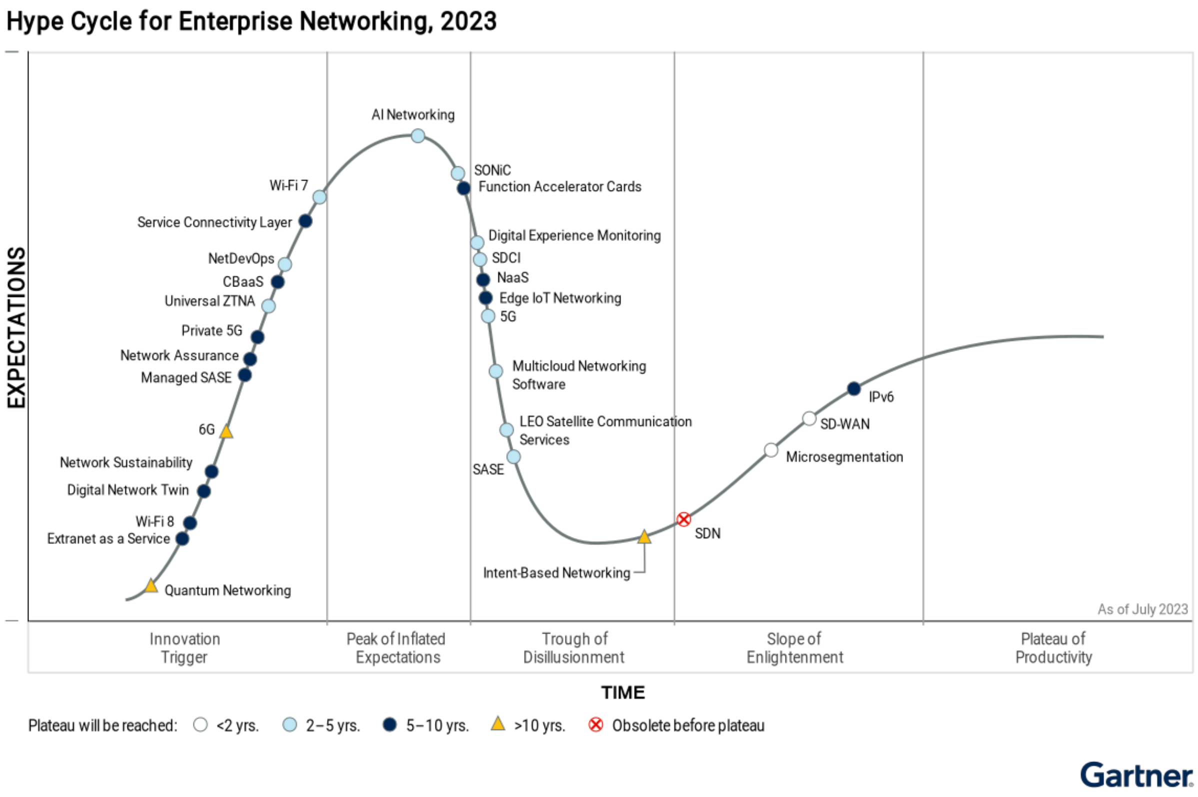
- Digital experience monitoring (DEM)
- ExtranetaaS
- Managed secure access service edge (SASE)
- Network assurance
- Network sustainability
- Quantum networking
- SONiC
- Universal zero trust network access (ZTNA)
- WiFi8

Peak hype: AI Networking is at peak hype this year, driven by multiple factors including vendors promoting AI capabilities, and the industry hype around ChatGPT and generative AI. SONiC is also near peak hype as it is often touted as the potential to be the “Linux of networking” which is enticing to enterprises.

Fast movers: Service connectivity layer (SCL) and function accelerator cards (FACs) both underwent substantial movement on the Hype Cycle as vendors and offerings emerged, driving increased interest, awareness and 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.

Figure 1: Hype Cycle for Enterprise Networking, 2023



The Priority Matrix

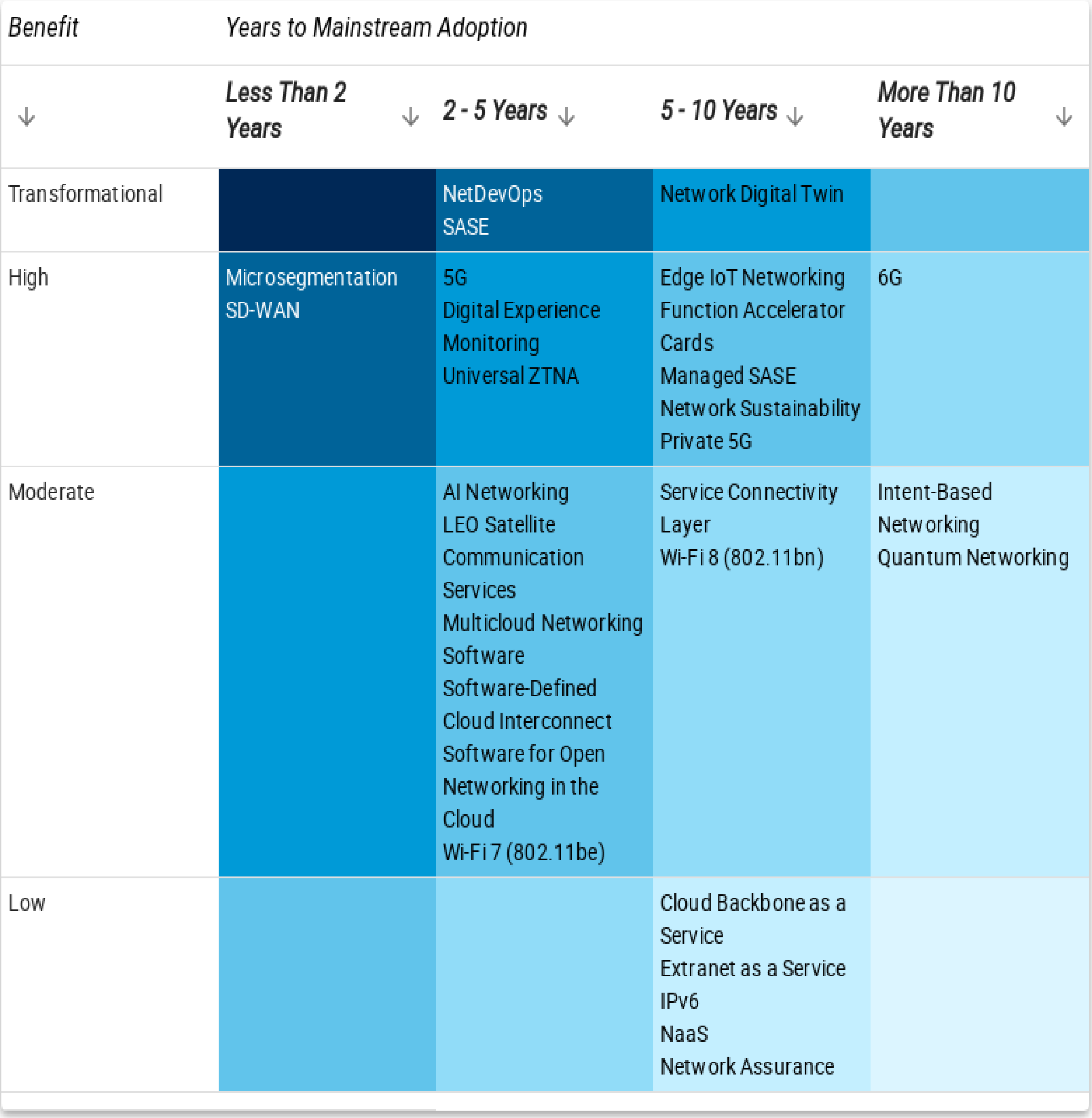
The Priority Matrix identifies networking technologies by impact against a timeline of estimated years until mainstream adoption. This helps organizations prioritize which technologies to focus on based on maturity and business impact.

Given how fundamental network infrastructure is to the modern digital business, it is difficult for enterprises to rapidly absorb new networking technologies, due to the potential impact of a network issue. Thus, there are a limited number of transformational technologies that we anticipate rapidly being adopted. SASE and NetDevOps are the two transformational technologies likely to mature in the next two to five years. Software-defined WAN (SD-WAN) and microsegmentation are high-impact technologies likely to mature during the next two years.

The remaining technologies with the highest impact that are likely to mature in two to five years are 5G, digital experience monitoring (DEM) and universal ZTNA. In the five-to-10-year maturity time frame, network digital twins has the potential to become a transformational technology, along with other high impact technologies that include edge Internet of Things (IoT), FACs, managed SASE, network sustainability and private 5G.

Table 1: Priority Matrix for Enterprise Networking, 2023

(Enlarged table in Appendix)



Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		NetDevOps SASE	Network Digital Twin	
High	Microsegmentation SD-WAN	5G Digital Experience Monitoring Universal ZTNA	Edge IoT Networking Function Accelerator Cards Managed SASE Network Sustainability Private 5G	6G
Moderate		AI Networking LEO Satellite Communication Services Multicloud Networking Software Software-Defined Cloud Interconnect Software for Open Networking in the Cloud Wi-Fi 7 (802.11be)	Service Connectivity Layer Wi-Fi 8 (802.11bn)	Intent-Based Networking Quantum Networking
Low			Cloud Backbone as a Service Extranet as a Service IPv6 NaaS Network Assurance	

Source: Gartner

Off the Hype Cycle

These technologies are still important, but have been taken off the Hype Cycle:

- 400G is maturing and consequently not one of the most hyped networking technologies.
- Enhanced internet is no longer one of the most hyped networking technologies.

- Service mesh has been replaced on this Hype Cycle with service connectivity layer, which is a related technology that garners more emerging hype.
- Kubernetes networking (container networking interface [CNI]) is a maturing technology, but has been replaced on the Hype Cycle with service connectivity layer, which is a related technology that garners more emerging hype.
- Edge networking doesn't constitute as much hype as using existing technologies to address edge requirements including SD-WAN, SASE and edge computing.
- Open networking has been replaced on the Hype Cycle with SONiC, which garners the most client interest of any open networking technology.
- Network automation has been around for over 10 years and has been dropped from the Hype Cycle. NetDevOps remains on the Hype Cycle which is a subset of network automation that garners increasing hype.
- SD-branch is maturing and consequently not one of the most hyped networking technologies and has been removed from the Hype Cycle.
- NFV has matured and is most popular among service providers, not enterprises and has been removed from the Hype Cycle.
- Wifi6e has been replaced on the Hype Cycle with WiFI7 and WiFi8.
- ZTNA is a maturing technology, but has been replaced with universal ZTNA which is garnering more emerging hype.

On the Rise

Quantum Networking

Analysis By: Andrew Lerner, Nauman Raja, Chirag Dekate

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Quantum networking — also known as quantum communications — is a way to transmit information across a network. Quantum networking (QN) sends information in the form of entangled photons (qubits), while most existing networks are based on the binary encoding of 1s and 0s. Quantum networking enables the exchange of quantum information.

Why This Is Important

Quantum networking has the potential to address new use cases and enable a platform for future innovation and discovery. Quantum networks enable organizations to securely connect quantum systems, and cannot be decrypted using existing decryption mechanisms. One of the advantages of a quantum network is that it brings together many smaller, networked quantum computers. This way, it can operate at a larger scale and helps solving problems that are beyond the reach of a single machine.

Business Impact

Quantum networks have the potential to transform the way information is transmitted by security-sensitive industries — such as financial services, healthcare, energy, defense and government. New, disruptive applications of quantum networks — such as quantum sensing and interconnecting distributed quantum computers — have the potential to create the foundations of a next-generation “quantum internet.”

Drivers

- R&D innovations like testbed networks and pilots are driving interest in and awareness of quantum networks.

- Government and military organizations are funding quantum initiatives and exploring the feasibility of quantum networking to prepare for the next generation of network connectivity. They are focused on increased security and new use cases that involve interconnecting quantum sensors for applications (for example, helping people navigate in GPS-denied environments). China and Europe have been the most aggressive to date (see the AEI article, Quantum Computing: A National Security Primer). The EU has launched several centrally funded quantum testbeds and created an open system for ease of public private collaboration. Chinese initiatives are the most advanced with ground-ground, ground-satellite and satellite-satellite quantum communication infrastructures.

- Academic institutions are exploring the feasibility of using quantum networking to solve real-world connectivity challenges around scale, performance and security. Academic institutions are also creating interest and a corresponding talent pipeline.

- U.S. initiatives associated with QN are largely being driven by academic research activities.

- Quantum-based networks are not susceptible to known decryption mechanisms that can be used on existing networks. Thus, organizations concerned about the potential to break traditional VPN encryption are investigating quantum networking.

- Standards bodies are actively working on creating standardized protocols and mechanisms to use QN.

Obstacles

- Very few commercial entities are connected to existing quantum networks, limiting the value of connecting to them.

- QN are expensive to deploy, and there is no clear commercial ROI to build them.

- QN are not compatible with Ethernet and TCP/IP, thus they cannot be integrated easily into an organization’s existing infrastructure or the internet.

- Deploying QN requires specialized infrastructures, such as photon detectors, that are hard to integrate with commercial telecom infrastructure.

- QN is in its infancy and technology stacks currently used to build QN are immature or have scalability challenges. QN require greater timing and synchronization granularity than what classical technologies can deliver, limiting growth.

- QN still have low qubit transmission rates and are sensitive to noise.

- While QN are more resistant to decryption than existing networks, applying postquantum encryption to existing networks can provide a similar functionality. This could deter or delay investments in QN.

User Recommendations

- Do not use quantum networking in production environments. Technology, protocol stacks and benchmarks are nonstandardized and ad hoc. Most quantum networks are associated with R&D exploration today.
- Work with your local university or government entities and join their emerging quantum networks to build a quantum network or gain experience with quantum networking. These partnerships can enable you to tap into the emerging quantum-enabled talent pipeline and form early relationships with quantum vendors.
- Look to traditional networking alternatives before investing in quantum networking. This is recommended due to the immaturity of the technology and market.

Sample Vendors

Aliro Quantum; IonQ; nodeQ; Qasky; QuDoor; Qunnect; QuTech; WeLink

Gartner Recommended Reading

Infographic: How Use Cases Are Developed and Executed on a Quantum Computer

Cool Vendors in Quantum Computing

Preparing for the Quantum World With Crypto-Agility

Extranet as a Service

Analysis By: Andrew Lerner

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

ExtranetaaS is a networking software offering that delivers extranet as a service. An extranet is a logical network zone that connects multiple independent parties together, typically under different administrative domains, often with diverse requirements. These are sometimes also referred to as B2B networks.

Why This Is Important

ExtranetaaS can help accelerate the sharing of information between partners using cloud services. Although extranets have been around since the 1980s (and the term extranet has been in use since 1995), ExtranetaaS simplifies the ability to set up and secure operation of an extranet in the modern era, as enterprises increasingly use public cloud and SaaS services.

Business Impact

Extranets are a way for enterprises, partners, customers and other outside parties to access data and systems resident on a network. It allows these parties to connect and exchange needed information such as application components or financial transactions, and is helpful in connecting independent parties with common interests. An example is within the financial services industry where local connectivity between regulatory agencies, stock exchanges, market data companies and trade clearing is often required.

Drivers

- Traditionally, extranets were established in data centers, nearby applications and data, using dedicated circuits or IPsec VPN. As organizations are migrating applications to the public cloud and SaaS, it is causing them to rethink their existing extranet approaches.

- The native public cloud providers don't offer robust advanced networking configurations to support complex extranet connectivity scenarios, driving enterprises to entertain ExtranetaaS solutions.

- There is a desire to simplify and replace physical infrastructure, including routers, firewalls and VPN appliances, with software with solutions that are more API- and software-oriented.

- There is also a desire to remove expensive dedicated lines such as MPLS or dedicated broadband.

- Smaller and startup network vendors are aggressively targeting enterprises to help them solve the technical and security challenges as organizations migrate their applications to cloud services.

Obstacles

- ExtranetaaS is a new and unknown technology to most enterprises.
- Extranets often support mission-critical environments that lead to a desire for moderate incremental change. This is in contrast to a shift to ExtranetaaS, which entails a software-only aaS delivery from lesser-known vendors.
- The public cloud providers' native capabilities are good enough for some extranet use cases.
- Organizations can use colocation in cloud data centers to address the challenge of getting the services closer to public cloud, SaaS and partner services without using ExtranetaaS.
- Most enterprise network teams take a "set it and forget it" perspective toward extranet deployments, preferring not to rearchitect the entire deployment. This drives moderate incremental modernization of existing extranets versus conversion to ExtranetaaS.
- The ROI of ExtranetaaS is unproven.
- The supply of vendor solutions is immature as many of the vendors focused on this technology are smaller companies that are unproven.

User Recommendations

- Investigate ExtranetaaS if using the native cloud provider constructs doesn't support your B2B networking requirements.
- Look to ExtranetaaS if you're migrating an existing on-premises, hardware-based extranet or B2B network to a public cloud environment.
- Shortlist ExtranetaaS offerings as an option for connecting to a large number of customers' data in a secure fashion.

Sample Vendors

Alkira; Graphiant; Trustgrid

Gartner Recommended Reading

Market Guide for Multicloud Networking Software

Wi-Fi 8 (802.11bn)

Analysis By: Mike Leibovitz, Tim Zimmerman

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Wi-Fi 8 is a proposed standard to follow Wi-Fi 6 and Wi-Fi 7. Wi-Fi 8 IEEE 802.11bn (Ultra-High Reliability) is the next proposed amendment to IEEE 802.11 WLAN beyond Wi-Fi 7 (802.11be). Its working group is expected to be established in late 2023, and its release cycle is anticipated to last until 2028.

Why This Is Important

Wi-Fi 8 is a future wireless standard aimed to enhance the reliability of the Wi-Fi protocol with deterministic latency. It prioritizes service availability and delay guarantees by improving connectivity, spectrum availability and performance consistency. These enhancements will be critical for industries like healthcare, public safety and industrial automation, where reliable wireless communication is essential. Wi-Fi 8 is expected to become available by 2028.

Business Impact

Wi-Fi 8 promises to deliver more dependable wireless communications capable of better supporting the mobility of robots, machines, vehicles and drones. The improved reliability will enable greater support for employees, customers, Internet of Things (IoT) and operational technology (OT). This could create new use cases, including immersive communications, digital twins and cooperative robots that demand stringent levels of uptime, which are not currently enabled by existing Wi-Fi protocols.

Drivers

- Improved roaming experiences for people, devices, robots and IoT, ensuring that endpoints stay connected at all times. This is made possible through the new roaming capability of Wi-Fi 8, which includes distributed multilink operation (MLO) technology.
- Deterministic wireless communication is required to meet emerging demands across multiple industries related to automation and robotics. Wi-Fi 8 will be designed to ensure these applications perform not only in terms of data delivery, but also in terms of maximum latency.
- Full-spectrum utilization enables high-performance wireless connectivity for enterprise and industrial endpoints. By supporting multiple devices operating simultaneously across radio bands with less interference, Wi-Fi 8 will deliver consistent performance and offload opportunities for a range of use cases.

Obstacles

- There are currently no Wi-Fi 8 devices or infrastructure available on the market.
- There is no ratified Wi-Fi 8 standard yet, as it has yet to be drafted. The working group responsible for its development is set to begin its work in late 2023.
- The process of developing and ratifying a Wi-Fi standard typically takes around five years, which means we can expect Wi-Fi 8 products to become generally available around 2028.

User Recommendations

- There is no action required, as no Wi-Fi 8 commercial offerings are currently available in the market.

Network Digital Twin

Analysis By: Tim Zimmerman, Andrew Lerner

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

A network digital twin is a model of the behavior of campus, software-defined WAN (SD-WAN) or data center network components. It is usually delivered as software and provides a model that can be used for validation of the configuration or policies of a single network component or the entire network. It automatically synchronizes with the production network.

Why This Is Important

The complexity of enterprise networks continues to grow, coupled with the business demands for faster and accurate delivery of network activities, such as changes. In addition, there is an increase in network updates and the limited availability of skilled resources mandates the automation of testing to reduce the costs of shadow IT and duplicate systems. A network digital twin allows for the validation of configuration and security policies made to individual components.

Business Impact

For IT leaders, a network digital twin allows faster testing and consequent delivery of network changes with fewer personnel resources and less cost by reducing shadow IT equipment requirements. We believe a network digital twin can improve delivery times for requests by 20% across the network.

Drivers

- **Lack of time to test network component updates:** As network vendors adopt agile development processes, new versions of operating systems and applications are being delivered at a much increased pace compared to several years ago. Most IT organizations do not have the ability to completely test one version before the next version arrives.
- **Amount of configuration errors due to network complexity:** Over 80% of network problems are due to improper configuration and change management.
- **Cloud migration issues:** More than 15% of security breaches are caused by misconfigured cloud services
- **Increasing desire to improve automation:** Using an automated pipeline to deliver data center network changes.
- **Need for virtual production networks:** Organizations struggle to replicate, simulate or emulate their production networks due to cost of equipment or operational expense to keep the environment synched with production systems.
- **Training:** Organizations can use a network digital twin to train new employees in a lower-risk environment.

Obstacles

- **Amount of physical resources required:** The compute and memory resources required to model a discrete component will require that modeling and testing be completed in the cloud.

- **Ability to model existing discrete network components:** Creating network models and test suites is complex and will require skill sets that are different from those that are currently available in IT.

- **Creating composite networks:** Connecting discrete network components for a single vendor is difficult but network digital twin tools and IT skills will need to improve before multivendor composite networks can be built.

- **Lack of standards:** Standards are not yet in place and current solutions may be proprietary/vendor specific.

- **Lack of trust:** Enterprise network teams lack trust in digital twins either due to immaturity of the technology, or their lack of experience with it.

- **Lack of awareness:** The technology is relatively new and immature.

- **Lack of a clear business case:** To justify spending on the new technology.

User Recommendations

- Pilot a network digital twin if you're looking to roll out data center networking changes in an automated CI/CD pipeline.

- Prefer a network digital twin that is delivered as a service, offers subscription-based pricing and supports multiple vendors.

- Deploy a campus network digital twin to validate changes to existing campus network configuration, changes in security policies or application migration to the cloud.

- Calculate ROI for network digital twin saving resulting from preventing security and configuration issues.

- Educate senior management on the value of discrete and composite network digital twin modeling.

Sample Vendors

Ericsson; Extreme Networks; Forward Networks; Intentionet; Keysight; Nokia; NetBrain

Gartner Recommended Reading

Quick Answer: What Is a Digital Twin?

Emerging Tech: Venture Capital Growth Insights for Digital Twins

Network Sustainability

Analysis By: Marissa Schmidt, Tushar Jain

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Network sustainability is an attribute of networking products and architectures that optimize space, materials and energy efficiency. This includes (but not limited to) networking hardware and/or software that is designed to improve energy efficiency while the product is idle and running. Network sustainability also needs to show an optimized network and use products that apply circular economy practices and/or source from renewable energy to ultimately reduce the environment carbon footprint.

Why This Is Important

Networking products have been around for decades as the base conduit for any users to access cloud or on-premises applications. As companies expand quickly, existing network architecture grows without assessing a more optimized network. Networking products have a material environmental footprint in the data centers and in cloud networks, and are critical to the everyday business. Due to their vast footprint, network products typically constitute about 10% of IT GHG emissions in most enterprises.

Business Impact

Improving network sustainability can reduce power, waste and space requirements, improve recycling and lower greenhouse gas emissions. All these improvements can serve the main benefits of reducing costs and boosting IT operations, and in some cases can improve costs of capital and stock performance. Secondarily, improved network sustainability can help protect the business from both reputational and regulatory risk.

Drivers

- Senior leaders are increasingly pressuring the IT organization to contribute to the sustainability goals for the enterprise.

- Organizations need to ensure their data centers are power-efficient to meet data center and cloud sustainability targets and bring down costs.

- Within the next 10 years, data centers are likely to be more power-constrained than from 15 years ago. Hence, energy efficiency will be even more critical beyond just saving money and reducing greenhouse gas (GHG) emissions.

- Network sustainability protects against the short- and long-term variability of fossil fuel energy costs.

- Organizations that have power reduction goals still have the need to continue to enhance hybrid work and drive more power efficiency due to back-in-the-office initiatives.

- Workloads continue to move out of traditional data centers and into cloud environments. Many organizations operate with hybrid environments, which further increases depending on networking.

- Depending on functionality, networking software running on any hardware may still need equivalent hardware resources as the traditional network appliance.

Obstacles

- Analytics and toolsets to dynamically manage and optimize multivendor network energy, utilization and GHG emissions are very limited.
- Enterprises buy the networking product based on need of features or capabilities, and on energy efficiency as a secondary consideration, with other sustainability characteristics as tertiary.
- While moving to the cloud is generally a more sustainable choice, it will likely increase network load and associated energy and GHG emissions.
- Networking vendors may see networking sustainability as nice to have and not make it a priority in their product life cycle.
- Many people see sustainability as a “global citizen” initiative versus actually being a financial benefit to the enterprise.
- There is limited awareness or not yet top priority of networking sustainability in the enterprise, as evidenced by the small number of inquiries Gartner has received on the topic to date.

User Recommendations

- Review current data architecture for better efficiency and data thinning at the edge to obviate the need for high-bandwidth connections.
- Shortlist vendors that demonstrate sustainability by hardware buyback programs or trade-in programs with proven and demonstrable circular economy best practices in place.
- Select vendors that have user tools to benchmark networking designs and routes in terms of their carbon impact to optimize network design and/or use fewer networking products.
- Require sustainability targets from vendors during the RFP process.
- Look for energy-efficient power ratings and grades for server hardware asks, and PLCM software design choices such as low-power mode, virtualization, idle/service core usage and analytics.
- Use components such as hardware casing, plastic components that leverage renewable energy, and recycled material.
- Choose enterprises with liquid and immersion cooling, as well as chassis/server airflow and printed circuit board (PCB) design choices.

Gartner Recommended Reading

Quick Answer: What's the Difference Between Sustainability, ESG and CSR?

Quick Answer: How Can Sustainability Drive Data Center Infrastructure Cost Optimization?

Unlock the Business Benefits of Sustainable IT Infrastructure

6G

Analysis By: Kosei Takiishi

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

6G is the generic name for the next-generation cellular wireless, also called Beyond 5G. In 2023, the features and timetable for 6G are not clearly defined, although it's expected to be commercialized in 2028 by some communications service provider (CSP) pioneers. 6G will enhance 5G capabilities and is intended to provide higher peak data rate (e.g., 100 Gbps to 1 Tbps), lower latency (e.g., 0.1 ms) and much more connection density and energy efficiency (e.g., 10 times more efficient).

Why This Is Important

The U.N.'s 2030 Agenda for Sustainable Development, including 17 goals, is heavily impacted by the mobile industry. Many of these social issues and ambitious goals will result in technologies that will become a part of 5G or future 6G cellular deployments. Design and research for 6G is already underway by many industrial associations and academic and commercial organizations. 5G can solve some of these challenges; however, 6G is indispensable for continuous growth and problem solving in the 2030s.

Business Impact

6G will enable end users, including consumers and enterprises, to transfer and process large volumes of data in real time, which enables true immersive experiences as well as more mission-critical human machine communications. Much richer and advanced connectivity of the physical world with the digital world — digital-physical fusion — is expected. There is no clear 6G definition, but 6G is aiming to improve 5G capabilities by adding one generation every 10 years (same as before).

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, which will drive further research and discussions. In February 2023, the South Korean Minister for Science and ICT unveiled the K-Network 2030 plan, calling for South Korean tech firms to lead the way in developing world-class 6G technologies and software-based networks. The Chinese government has nominated 6G as one of its priority projects for 2023. In March 2023, the Beyond 5G Promotion Consortium in Japan published its B5G White Paper 2.0.

- Academics and commercial organizations want to be part of the 6G process, and active research has already begun. Working group one6G in Europe hosted a summit and held related open webinars in 2022. In February 2023, NTT DOCOMO hosted Open House'23, where 6G was one of the main topics. In November 2022, NTT DOCOMO published the 6G White Paper 5.0.

- Many commercial organizations and academic institutions have started their 6G research to be a part of the future 6G patent pool.

Obstacles

- The 5G journey is still in its early years, and its best practices and monetization are not clear. Success or failure of 5G to drive revenue and new business opportunities will have a major impact on 6G commercialization and business.

- The telecommunications industry has formulated its own specifications and standardization (such as 2G, 3G, 4G and 5G). It is unclear whether 6G will be able to incorporate external opinions, extending the start provided by some other industries' participation in developing 5G standards.

- Some 6G technologies, such as THz wireless, may not prove to be technically viable or cost-effective for most cellular users' needs.

User Recommendations

- Monitor discussion of the currently emerging 6G carefully.
- Prepare early trials and proofs of concept (POCs) in the late 2020s with vendors to learn more about the capabilities of 6G and early use cases, and begin building skill sets.
- Support your regulators and government to create their new national policy for 5G-Advanced and 6G. Technology innovation and strategy leaders should look at evolving 6G standards to get an early idea of future networking technologies.

Sample Vendors

Ericsson; Huawei; Nokia; NTT DOCOMO; Qualcomm; Samsung Electronics; SK Telecom

Gartner Recommended Reading

Emerging Tech Impact Radar: Communications

Managed SASE

Analysis By: Ted Corbett, Lisa Pierce, Jon Dressel

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Managed secure access service edge (MSASE) delivers the full life cycle of SASE functionality as a managed service. This includes design, migrations, configuration, installation, operations and management. These services cover the core SASE components of SD-WAN, SWG, CASB, firewall, zero trust network access (ZTNA) elements, and security posture and vulnerability assessments.

Why This Is Important

SASE management is often performed by the enterprise, making SASE only suitable for clients with mature security engineering and operations capabilities. Many enterprises lack the expertise to manage and secure networks, indicating that MSASE is a better choice for them. Sixty to 70% of SD-WAN buyers use managed services (e.g., MNS); we expect MSASE to increasingly align the same way. Gartner client interest in SASE is solid, with thousands of inquiries in the last two years.

Business Impact

MSASE can speed time to value for enterprises, and reduces strain on internal resources while reducing operational risk in order to reap SASE benefits. Currently, the vast majority of SASE offerings assume skilled and experienced client networking and security teams in emerging technologies, which many clients lack. MSASE services help these clients to more rapidly adopt SASE and achieve comparable benefits as organizations with solid internal network and security expertise.

Drivers

- There is strong client interest in SASE because it allows them to reduce the number of security vendors they employ, decreasing complexity while supporting key transformation initiatives, including cloud and hybrid work.

- Most enterprises cannot hire and retain enough employees that are skilled enough to support the demands of expanding security operations.

- Enterprise interest in MSASE is robust, as it optimizes their security architecture and reduces investments in internal resources.

- MSASE providers view the high interest in SASE and vendor consolidation as a prime opportunity to capitalize on the trend, resulting in a proliferation of choices for customers.

- The increase in MSASE vendors has resulted in downward pricing pressure, making it a more attractive alternative for customers considering buying SASE without a managed component.

- Enterprises clearly see the efficiency and performance by subscribing to an MSASE service that provides a single platform view of their security posture, due to the market's current lack of a consolidated platform and single portal interface.

Obstacles

- SASE solutions are available from an array of network and security vendors, yet few viable offerings exist in the market with a single management plane, unified data model, data lake and simplified pricing.
- Vendors have yet to fulfill Gartner's full vision of SASE, leaving some clients disillusioned and seeking more capabilities more quickly from their providers.
- Vendors commonly generalize specific enterprise use cases and lead with their solution first.
- Today, few fully deployed MSASE services exist. Vendor offers are expanding, but solution proof points in production environments are limited at this stage of market adoption.
- Client adoption is constrained by current commitments — either a capex commitment with remaining depreciation, or opex commitments constrained by contract terms.
- Client-aligned migration plans are lacking.
- The lack of productized life cycle process (days 0-2) standardization for MSASE will result in fragmented SLA experiences.

User Recommendations

- Evaluate MSASE providers if networking and security labor is the primary constraint to adopting SASE for the organization.
- Invest in MSASE to accelerate deployment, streamline security integrations, enable life cycle management and reduce staffing risk.
- Seek MSASE vendors who align their underlying SASE products with your organization's primary use cases, such as branch transformation, hybrid work support, or best-in-class security capabilities.
- When assessing MSASE services versus SASE offers, set realistic expectations about your organization's needed time and assets for both configuration and operations, since the managed services elements would require internal resources.
- When assessing MSASE offers, prioritize operational simplicity, unified management, ease of procurement and reduced overhead.
- Judge MSASE services by the level of standardization of their key network and security functions and life cycle processes, the maturity of SLAs, and commercial terms.

Gartner Recommended Reading

Forecast Analysis: Secure Access Service Edge, Worldwide

How to Align SD-WAN Projects With SASE Initiatives

2022 Strategic Roadmap for SASE Convergence

Market Guide for Single-Vendor SASE

Quick Answer: How Can Midsize Enterprises Benefit From Security Vendor Consolidation?

Network Assurance

Analysis By: Gregg Siegfried, Simon Richard

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Network assurance tools enable users to verify that a network behaves as intended. These tools are delivered as software, and typically discover and model a network environment.

Why This Is Important

Networks are increasing in complexity, and are changed repeatedly. Changes in configuration, use case or consumption should not degrade or have unintended side effects. Network assurance is of key interest to network and infrastructure leaders responsible for the health and performance of their network. The techniques that network assurance tools use facilitate testing and validation, and can support self-healing.

Business Impact

For network operations, it is not easy to answer the question as to whether the network behaves the way it is expected to. But this is what network assurance addresses by modeling the network and its traffic and running validation tests. Having a model of the network that validates applications and network changes accelerates the delivery of applications and increases reliability. The visibility gained by deploying network assurance will also decrease mean time to resolution (MTTR).

Drivers

- Networks are becoming more dynamic, and network changes are more frequent. Network operations are running out of resources to manually validate current state and upcoming changes.
- Modern applications are increasingly distributed and rely on external services as application workloads span the administration domain, making networks more difficult to assess.
- Network complexity increases the effort in maintaining an awareness of network health.
- The rise of digital experience monitoring exposes application performance issues at the same time, and modern applications are placing greater demands on the network.
- Improved compliance and simplified auditing, due to the algorithmic correctness of configurations, direct mapping to business intent and ongoing, dynamic and real-time validation.
- There are a handful of vendors that are actively investing in and promoting these capabilities in the market.
- Vendors are marketing network “digital twins” as a safe environment to test and validate network activities in support of networking and security use cases.

Obstacles

- Network assurance is an addition to an organization’s existing network toolkit, not a replacement. Tool sprawl is already a challenge for most network teams.
- Net assurance needs integration with network discovery and source of truth tooling, which increases complexity and can’t be used off the shelf.
- Network assurance tools build a model assuming that network devices, such as switches and router firewalls are bug free and that there are no cable or hardware issues. Unless they ingest and process live data, they only represent a partial state of the network.
- Organizations will need to design, create and deploy custom validation tests fit for their network, and face high costs of operation.

User Recommendations

- Include network assurance tooling to validate proposed network change.
- Integrate network assurance with network discovery and network source of truth.
- Pilot the network assurance solution offered by your network vendor, if any.

Sample Vendors

Cisco; Forward Networks; IP Fabric; Juniper Networks; NetBrain

Private 5G

Analysis By: Sylvain Fabre

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

A private 5G network is based on 3rd Generation Partnership Project (3GPP) standard R15 or above to provide unified connectivity, optimized services and security for enterprises. A 5G private mobile network (PMN) is specific to the enterprise and used to interconnect people and things. Deployments can be entirely on-premises, with local breakout, or linked to a public cloud or local telco.

Why This Is Important

Multiple verticals will require 5G PMN deployments to realize the full effect of their digital transformation initiatives. Adopting new 5G standards earlier than communications service providers (CSPs) can offer on their public infrastructure can provide access to additional functionality. Distinct from the public network, private 5G supports voice, video, messaging, data and Internet of Things (IoT) with higher performance requirements. It can optimize cost or connectivity (for example, less expensive than Wi-Fi for large area coverage).

Business Impact

Private 5G enables transformational digital use cases for industry, especially in conjunction with other technologies, such as factory digital twin or edge AI for computer vision. 5G PMN can offer enterprises improved security, independence and enable efficiency gains; for example, complete 5G coverage in factories, with speeds over 1 Gbps, and support for edge and AI use cases with guaranteed performance levels.

Drivers

- Applicability and vertical specific integration are increasing. Beyond 3GPP, other bodies are now contributing, such as 5G Alliance for Connected Industries and Automation (5G-ACIA) or 5G Automotive Association (5GAA).
- Liberalization of the radio spectrum has opened up standard radio bands, often around 3.5 GHz, for use by private 5G networks.
- Requirement for full, reliable network coverage for machines, sensors and equipment, including indoor, outdoor, office and large industrial areas at lower cost than Wi-Fi.
- Performance profile for demanding industrial use cases, in particular when low-latency, high-bandwidth (especially uplink), and reliability are required and exceed the capabilities of the shared public infrastructure.
- Private 5G has 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.
- Interest from telecommunications service providers (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 and so on are thereby expanding into industries and generating new revenue.
- Alternative provider types beyond the CSPs, such as integrators, infrastructure vendors and hyperscalers, are driving new deployments and proofs of concept.
- Some enterprises deploy private networks because they want to run their network more independently, as their own infrastructure, with limited outside dependency. One example is long-term commitment from public network operators; also, data privacy can be a key concern, with data loss prevention security controls in place to ensure sensitive information does not leave the enterprise perimeter.
- Some defense and government clients have indicated a wish to have more control and visibility into the vendors involved in the mobile services provision, which can be an issue over a shared public network built and managed by a CSP.
- Low-latency applications using processing embedded in network infrastructure are logistically easier if the application, and infrastructure are owned by the same entity.

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 are still a work in progress; for example, with network slicing.
- Complex deployment and operation.
- Limited availability and cost of equipment designed to use the radio bands available for private network use.
- Module availability and pricing for R16 and up.
- 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 NarrowBand-Internet of Things (NB-IoT) and other low-power wide-area networks (LPWA networks), such as LoRaWAN.

User Recommendations

- Differentiate from other providers, like large equipment vendors, systems integrators (SIs), resellers, smaller specialist network vendors and hyperscalers, by integrating PMN with other functions like supplier information management (SIM), IoT platforms, edge computing, design and managed services, and national roaming.
- Co-create networks by partnering with SIs and consultancies that have the required industry skills for design, deployment, and managed services engineering headcount and evaluation test bed environments. For example, build manufacturing 5G PMN with connectivity, security and AI capabilities.
- Design licensed and unlicensed/shared spectrum options where available.
- Supplement your engineering teams by working with IT service providers. Do not expect or plan on public 5G replacing WLAN in large portions of your environment. Instead, IT leaders should select private 5G for specialized use cases with large coverage areas and known application performance requirements.
- Identify use cases and their requirements to establish where 5G can be implemented — for example, in applications using HD wireless cameras.

Sample Vendors

AT&T; Celona; China Mobile; Ericsson; HPE (Athonet); Huawei; Nokia; T-Mobile; Verizon; Vodafone

Gartner Recommended Reading

Infographic: 5 Steps for Vendors to Scope and Run Successful POCs for Enterprise 5G PMNs

Market Guide for 4G and 5G Private Mobile Networks

3 Go-to-Market Strategies for Product Leaders in Private Mobile Networks

Research Roundup: How to Build Winning Propositions in 5G Private Mobile Networks

Quick Answer: What Metrics Can TSPs Consider for Their Private Mobile Network Solution Development?

Universal ZTNA

Analysis By: Andrew Lerner, John Watts

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Universal zero trust network access (ZTNA) extends existing ZTNA technologies to use cases beyond remote access, to support local enforcement in campus and branch "on-premises" locations. "Universal ZTNA" is a marketing term, as the original ZTNA definition was not limited to remote access use cases. Universal ZTNA centralizes a user or device zero-trust-access policy to enable a single access policy definition.

Why This Is Important

Extending ZTNA products to campus environments creates several benefits for enterprises, including security gap elimination, unified policy, enhanced visibility, simplified operations and modernized pricing models.

Business Impact

Although remote work surged in recent years, the future of work is hybrid. Hybrid working creates challenges for employees due to inconsistent network access implementations, which can lead to lost productivity and increase the likelihood of security and networking incidents. Universal ZTNA helps to streamline network and security policies across multiple environments.

Drivers

- Organizations that have deployed ZTNA for remote workers and are looking to extend the same technology for users while on-premises.
- Organizations are looking to develop a unified security policy to allow access to resources regardless of the user or device's physical location.
- Vendors are starting to aggressively market universal ZTNA.
- When done in conjunction with retiring duplicate systems for on-premises or remote access security, extending existing ZTNA implementations beyond remote access allows enterprises to achieve lower total cost of ownership (TCO).
- There is a desire for a consistent end-user experience when accessing corporate resources, whether in the office or remote.
- Organizations are looking for simplified administration of campus networks, via reducing the amount of switching configuration (e.g., between VLANs, 802.1X, MACsec, private VLANs, access control lists [ACLs] and microsegmentation) or reducing the need for network access control (NAC).
- Organizations are looking for improved visibility and control of end-user devices both on and off the local network.
- Organizations are looking to enable near-real-time adaptive access controls based on the risk of the user and device, beyond relying on the physical location or IP address of a user or device.

Obstacles

- Siloed network and security teams mean organizations overlook the opportunity to unify remote access and campus security using a single tool — with each silo picking their own product.
- There is a limited number of vendors with robust universal ZTNA offerings. Specifically, shortcomings include unmanaged devices and unauthenticated users, including unmanaged operational technology (OT) and Internet of Things (IoT).
- Steering traffic to enforcement points may require network redesign, or create latency or complexity and impact performance.
- IT management tools for patching and software distribution may need modernization to support reaching isolated endpoints, even in campus locations.
- There is an increased concentration risk of ZTNA failures due to poor policies, vulnerabilities or operational downtime in ZTNA infrastructure. There is increased risk of account takeover attacks applied to both remote and campus workers.
- Organizations have not defined what adaptive signals are important and what actions to take when adaptive signals fall below a certain threshold.

User Recommendations

- Start with secure remote user access use cases before extending to on-premises use cases.
- Pilot universal ZTNA deployments by extending existing remote access ZTNA deployments to campus environments in order to determine feasibility.
- Prefer universal ZTNA vendors who offer both on-premises and cloud-hosted enforcement points, to help avoid suboptimal traffic routing.
- Prefer cloud-based management for universal ZTNA deployments to gain faster access to new capabilities from the vendor, and avoid having to manage the management system.
- Align universal ZTNA with the need for web and SaaS security through secure access service edge (SASE) and security service edge (SSE) products, which, in addition to remote access, enable security and better networking performance on-premises.
- Create and test a resiliency plan for what happens when enforcement points are unavailable and resources are not reachable (for example, local policy caching when cloud resources are not available).

Sample Vendors

Appgate; Elisity; Fortinet; Versa Networks; Zscaler

Gartner Recommended Reading

Emerging Tech: How to Differentiate in the Fast-Growing but Crowded ZTNA Market

Campus Network Security and NAC Are Ripe for Market Disruption

Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure

Market Guide for Single-Vendor SASE

Cloud Backbone as a Service

Analysis By: Lisa Pierce, Andrew Lerner

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cloud backbone as a service (CBaaS) uses a public cloud provider's backbone for WAN transport, allowing network traffic to traverse that backbone to connect enterprise users, devices and locations. CBaaS offerings are delivered as a cloud service to customers and are occasionally marketed as WANaaS. Customers are responsible for ingress to the provider, typically via VPN or private WAN service. CBaaS can be delivered by a cloud provider or by a software vendor utilizing a cloud provider.

Why This Is Important

Heavy cloud users continue to seek out alternative WAN services to connect public cloud services. CBaaS is another example. But typically, the traffic transiting the particular cloud provider's backbone is limited to customer traffic that the particular IaaS provider and node(s) serve.

Business Impact

These offerings provide an alternative to existing WAN services to support cloud node to cloud node use cases. However, CBaaS typically doesn't support the full set of WAN requirements for most enterprises.

Drivers

- Aggressive marketing and sales from public cloud providers, including Amazon Web Services (AWS), are urging enterprise clients to discard their legacy WANs.
- The shift of enterprise workloads to public cloud providers makes the cloud provider's backbone a more logical choice for transport.
- As an architecture, CBaaS is compelling for organizations heavily focused on one public cloud provider, and that lack data center investments.
- CBaaS provides additional route diversity for clients seeking to enhance their WAN business continuity architectures.
- There also has been aggressive marketing from value-added resellers that acquire multiple CBaaS offerings and repackage them to sell to enterprises seeking CBaaS from multiple cloud service providers (CSPs).

Obstacles

- Prices from some CBaaS providers are multiple times more expensive than traditional WAN services.
- Because CBaaS is typically tied to a particular CSP, it is less attractive to clients whose traffic is significantly distributed across multiple CSPs.
- Offers are not end to end because access is excluded, as is WAN transport to the CBaaS node, forcing clients to procure separately.
- Compared with facilities-based carriers, the number of CBaaS nodes is very small.
- SLAs focus mainly on availability, and apply only between the CBaaS provider's nodes.
- Limited CBaaS telemetry data makes it less attractive to traditional network personnel, and to clients that operate their own SD-WAN networks.
- CBaaS offerings are fairly narrow. They do not seek to rival common carrier services, which serve all customers. Thus, customers must procure WAN transport for other use cases.
- These types of offerings continue to fracture the WAN, so clients must secure alternate WAN transport and employ consistent performance monitoring across all WAN providers.

User Recommendations

- Evaluate CBaaS offerings as a complement to your existing WAN, but don't expect CBaaS to replace your WAN.
- When applicable, use CBaaS selectively as part of your larger business continuity plan.
- Look at CBaas offerings if you're heavily invested with a particular IaaS provider for the mid to long term (three to five years or longer).
- Given their siloed nature, recognize that CBaaS maturation and price declines will be introduced at a very slow pace. I&O clients should assess the attractiveness of CBaaS offerings accordingly.

Sample Vendors

Alkira; Amazon Web Services; Microsoft

Gartner Recommended Reading

Optimize WAN Architectures for Workloads That Span the Hybrid Cloud and the Multicloud

How to Architect Your Network to Optimize Internet Performance and Reliability

NetDevOps

Analysis By: Andrew Lerner

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

NetDevOps entails applying DevOps and/or continuous integration/continuous deployment (CI/CD) practices to networking activities. This requires an automated pipeline that includes staging, pre/postvalidation, and testing of networking activities such as provisioning. Similar terms used to describe this approach include "NetOps 2.0" and "network as code."

Why This Is Important

NetDevOps can improve agility, reduce toil and increase reliability. It is particularly valuable for organizations implementing infrastructure as code (IaC) for other portions of their infrastructure, because the network is often a bottleneck. We estimate that less than 10% of enterprises actively use NetDevOps practices currently. Thus, there are ample opportunities to further improve agility while reducing human error within network provisioning and ongoing operations.

Business Impact

The use of NetDevOps practices helps to deliver networking functionality to the business faster, and increase overall network uptime, and aid with compliance.

Drivers

- As organizations implement IaC, GitOps and/or DevOps, traditional approaches to network provisioning are not sufficiently agile or reliable. NetDevOps helps to bring the network up to speed with other infrastructure and application processes.
- There is very limited tolerance for network outages/downtime. The practices associated with NetDevOps, such as automated testing, reduce the likelihood of a production impact because of increased testing, peer review, validation and automated rollback.
- NetDevOps practices drive clear workflows and documentation, which helps with auditing and governance, and troubleshooting.
- Network infrastructure and automation vendors are increasingly integrating their workflows with IaC and CI/CD tools, and marketing these concepts.
- For organizations embracing public cloud and cloud-native concepts, networks are typically built and provisioned with the application. Thus, it makes sense to integrate network, infrastructure and app provisioning using the same (or similar) processes.

Obstacles

- Many network teams aren't aware of NetDevOps.
- The skills and expertise required for NetDevOps (i.e., software development practices, Ansible, Terraform, Nornir, Python, APIs) are different from common network engineering skills, and in limited supply.
- NetDevOps requires highly accurate up-to-date network information (inventory, location, etc.), which is uncommon in many enterprises.
- Network teams are risk-averse and lack confidence in automating data center networks, because the business impact of outages are massive.
- There are few commercial network automation offerings that provide multivendor breadth and feature depth across data center, cloud, campus, WAN and security domains.
- Inconsistent or undocumented workflows limit adoption.
- Most enterprises do not have "development" or "test" network environment(s) which prevents or limits the effectiveness of NetDevOps practices.

User Recommendations

- Apply NetDevOps practices opportunistically, including as part of broader IaC practices. NetDevOps is not a fit for all networking activities; don't try to use NetDevOps techniques for all changes.
- Invest in personnel by shifting hiring and training focus toward specific software competencies, including Ansible and Python, community forums and cross-pollinating networking teams with adjacent DevOps personnel.
- Capture and store both device configurations and operational network state (for example, active routing tables) in a version control system.
- Invest in network infrastructure and network automation tools that offer published, open, restful APIs that expose more than 90% of functionality.
- Create standard templates for device types, apply versioning, and track configuration drift.
- Automate pre- and post-change validation, and configuration rollback.
- Automate pre- and post-environmental testing, such as latency/availability checks.

Sample Vendors

Arista; Amazon Web Services; HashiCorp; Itential; Network to Code; Red Hat

Gartner Recommended Reading

Market Guide for Network Automation Tools

The Top 5 Trends in Enterprise Networking and Why They Matter: A Gartner Trend Insight Report

3 Actions to Retain Customers and Grow Revenue in the Enterprise Network Hardware Market

Service Connectivity Layer

Analysis By: Simon Richard

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

The service connectivity layer (SCL) abstracts the necessary network plumbing and security controls required to connect application services together regardless of location or IP address. The technology simplifies the stitching of services for developers who are not networking experts, and can provide facilities such as discovery and registry, connectivity, authorization, identity and observability.

Why This Is Important

SCL technologies (such as service meshes, cloud private endpoints and service connectivity fabrics) allow developers and application architects to configure their services assuming that the network is flat, and that services are reachable, without having to be concerned about details of the underlying network infrastructure.

Business Impact

Organizations that are building or operating modern distributed applications will benefit from decreased cycle time, increased productivity and operational simplicity. The SCL will help deliver software faster by abstracting services and connectivity between them. Developers can concentrate more on business functionality, and less on networking minutiae.

Drivers

- The increasing use of cloud services benefits from secure, transparent and controlled connectivity. The adoption of mesh app and service architecture (MASA) relies on ubiquitous connectivity between apps and services and between services.
- New offerings such as Amazon VPC Lattice validate the emergence of the SCL.
- Kubernetes service mesh users want to extend the service mesh benefits outside their clusters into more static environments. The SCL can bridge the gap between highly dynamic and static environments.
- Organizations are increasingly leveraging cloud private endpoints to communicate to service in public clouds.
- The SCL establishes some of the foundation for zero trust security architectures by pushing enforcement out to the service endpoints.
- The technology that extends identity to services and processes is gaining traction.
- The SCL is aligned to platform engineering efforts, as it reduces application developers' networking cognitive load.

Obstacles

- Vendor ecosystems are nascent and immature, with some emanating from the service layer and some from the network layer.
- The lack of clear buyer persona between networking, security, platform and developers makes it difficult for vendors to gain customers. Consensus needs to be reached among many teams, including networking, security and application architects for every sale.
- Integration with existing legacy networks' construct, architecture and operational processes makes it difficult to operationalize the SCL.
- The SCL works better for organizations that have a platform operations team and have adopted infrastructure as code. Some developers and infrastructure and operations (I&O) teams are unaware that SCL technologies can address some of their issues.

User Recommendations

- Deploy a service connectivity solution to insulate application development from complex network technologies when necessary.
- Work with I&O and platform operations teams to ensure service connectivity is at the right level of abstraction.
- Include security, platform, development and network teams in the product evaluation and architecture processes.
- Try your public cloud offering's service connectivity before looking at third parties' offerings.

Sample Vendors

Amazon Web Services; Google; greymatter.io; HashiCorp; Solo.io; Tetrate

Gartner Recommended Reading

Using Emerging Service Connectivity Technology to Optimize Microservice Application Networking

Adopt a Mesh App and Service Architecture to Power Your Digital Business

Managing Machine Identities, Secrets, Keys and Certificates

Wi-Fi 7 (802.11be)

Analysis By: Tim Zimmerman, Mike Leibovitz

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Wi-Fi 7 (802.11be) is a proposed wireless LAN (WLAN) standard. IEEE 802.11be (very high throughput) is the next amendment proposal to IEEE 802.11 for advances in WLAN and is expected to be ratified in early 2024. The amendment is expected to provide more efficient usage of noncontiguous spectrum, support up to 40 Gbps performance and increase the number of spatial streams from eight to 16. Moreover, it will introduce TSN capabilities for low-latency traffic as well as standardize 6 GHz support.

Why This Is Important

New high performance applications like 8K video streams, as well as augmented reality/virtual reality, are driving user performance requirements. The introduction of Wi-Fi 7 (802.11be) provides new unused spectrum in many geographies for additional performance and allows time-sensitive networking (TSN) capabilities that will address low-latency and real-time traffic requirements.

Business Impact

For IT leaders, the introduction of low-latency real-time capabilities will help with the integration of operational technology (OT) applications onto the IT infrastructure. This is needed for industry 4.0 initiatives as well as for closed-loop applications, including the deployment of robots and drones, while providing over 40 Gbps performance for wireless connectivity in a single coverage area.

Drivers

- **Higher performance for video and lower latency:** This will boost theoretical performance with higher speeds upward of 40 Gbps, offer increased WLAN capacities and the integration of TSN for wireless applications addresses. Address low-latency requirements (potentially less than 2 ms for critical traffic) and eliminate congestion.

- **Increases number of radio streams to 16 and introduces coordinated multiuser multiple in, multiple out (CMU-MIMO):** Enabling support for more discrete endpoints within a coverage area, coordinated with allocated capacity based on endpoint type and application. This functionality will also increase the efficiency and resilience of mesh networks with allocated bandwidth.

- **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 cover legacy devices that could slow the overall performance.

Obstacles

- **Surplus performance for many enterprises:** Wi-Fi 7 (IEEE 802.11be) will theoretically provide performance of up to 40 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 intermediate distribution frame (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 Wi-Fi (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 prestandards 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.
- Be aware of access points' product end-of-life status as we do not expect Wi-Fi 7 before 2024, 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.
- Review the 6 GHz coverage area since it may differ from 2.4 GHz or 5GHz and result in coverage holes.
- Be prepared to update LAN switching to address higher power over Ethernet (PoE) requirements for access point as well as accommodate the higher performance wireless connectivity.

Sample Vendors

Cisco; Extreme Networks; Hewlett Packard Enterprise (Aruba); Huawei; Juniper Networks

Gartner Recommended Reading

Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure

Critical Capabilities for Enterprise Wired and Wireless LAN Infrastructure

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

I&O Platforms Primer for 2023

At the Peak

AI Networking

Analysis By: Jonathan Forest

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Adolescent

Definition:

AI networking uses AI and machine learning (ML) to deliver granular and specific actionable network insights. AI networking can be a feature within a network vendor's management platform, a stand-alone multivendor platform or a part of an AIOps platform. It can also be delivered as part of a managed network service. AI networking primarily delivers Day 2 network insights. Further, it offers recommendations to accelerate incident resolution, and prevent outages and trouble tickets.

Why This Is Important

AI networking can improve network availability and end-user experience, reduce operational resources required to manage networks, and decrease time to resolve incidents. Stronger AI networking products offer predictive management and simplified troubleshooting recommendations. They improve network performance which can't reasonably be achieved through manual resources. Ultimately, the goal is to provide a better experience for end users and more efficient network management for organizations.

Business Impact

AI networking drives operational management savings of up to 25% by reducing the number of support calls, enabling a quicker incident response, improving network availability and optimizing the end-user experience. It simplifies network management so that the network team won't need deep configuration and troubleshooting skills. However, new data science skills may be needed. The adoption rate within campus networks appears to be higher than it is for other networking domains such as SD-WAN.

Drivers

- There are a handful of vendors that are actively investing in and promoting AI networking capabilities in the market.

- Many networking capabilities are becoming commoditized. In order to differentiate their offerings, some vendors are overhyping their capabilities and claiming that predictive analytics can eliminate most trouble tickets.

- Organizations are looking at how to optimize Day 2 operations by reducing incidents and accelerating the resolution of network incidents.

- Organizations want to improve network availability and network or application performance to enhance end-user application experience.

- Organizations seek to simplify networking and reduce reliance on deep skills by networking teams. They have had trouble finding staff to manage their network in-house and often choose to source network operations with a managed network services (MNS) provider. For some organizations, AI networking offers an alternative approach that allows organizations to manage the network in-house with fewer networking skills required.

- AI networking is seen as an approach to reduce the management costs of network operations, because it can reduce the amount of personnel required to manage the network. Since many recommendations are done automatically, the time to resolve incidents is shortened, which translates to fewer resources required.

- Platform teams and cloud teams are having a greater influence on networking decisions. They are preferring to use modern automation and data science techniques versus traditional approaches to network operations.

- AI networking helps to simplify managing increasingly complex network, security and application infrastructures. They now come with heterogeneous environments — think multicloud, data center, colocation and edge — and more layers of abstraction, such as containers and Kubernetes.

- The hype around ChatGPT promises to expand AI networking to include Day 0 and Day 1 operational tasks.

Obstacles

- Overzealous marketing creates confusion and makes it more difficult to select an offering that adds demonstrable value, slowing down overall adoption.

- Network operations personnel are generally risk-averse. They do not fully trust the AI networking recommended actions to remediate network incidents, or they need to validate the outcomes first, which minimizes the value.

- Core networking features and capabilities remain more important in customer buying decisions than AI networking.
- Many AI networking products or features are nascent, unproven and rather immature.
- AI networking vendors generally struggle to link capabilities to strong business cases, and enterprises struggle to determine a clear ROI.
- Enterprises already have trouble managing existing tools. Adding more tools will just exacerbate tool sprawl.
- Some network personnel are concerned about losing their jobs or having to change their way of working.

User Recommendations

- Start small and iterate your use of AI networking solutions by validating and tracking the accuracy of the recommendations. When more recommendations and predictions prove accurate, you can start using the more automated recommendations over time.
- Start with a handful of high-priority use cases, such as ticketing or hardware. Minimize the risk by starting with noncritical production tasks or processes with a high chance of success.
- Investigate AI networking solutions that are integrated with broader network vendor offerings. Most mainstream networking vendors will have meaningful offerings in the next 12 months.
- Require vendors to deliver a concrete roadmap over the next one to two years, with specific details such as feature descriptions and timelines.
- Prefer multivendor solutions to avoid siloed tools and address broader use cases.
- Focus on the business case you are trying to solve by evaluating potential cost savings, time savings, agility benefits and end-user performance improvements.

Sample Vendors

BigPanda; Cisco Systems; HCLTech; Hewlett Packard Enterprise (HPE); Huawei; Juniper Networks; MetTel; Palo Alto Networks; ScienceLogic; VMware

Gartner Recommended Reading

Quick Answer: What Functionality Should I Expect From Network AIOPs Features?

Market Guide for AIOps Platforms

Function Accelerator Cards

Analysis By: Anushree Verma

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

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 — known as DPUs/IPUs and/or SmartNICs. FACs improve data operations and services, server availability, and network performance and security, besides enabling connectivity to a network. They have onboard memory and peripheral interfaces, and can run independently.

Why This Is Important

FACs can improve server performance by up to 50%, via offloading functions such as virtual switching, security and application delivery controller (ADC). They can host dedicated network appliances, including firewalls. They can also improve security by placing security functions onto a securely booted, locked-down environment. Today, FACs are primarily adopted by hyperscalers and large cloud providers, and we estimate they will grow at a five-year CAGR of 65% through 2027.

Business Impact

FACs enable cost-efficient and energy-efficient data center environments, while improving performance. By offloading high overhead functions, they allow the server to host more workloads, which reduces the direct cost of additional servers and, in some cases, infrastructure software. In addition, they can facilitate data transmission between remote resources — primarily for HPC and artificial intelligence/machine learning (AI/ML) workloads.

Drivers

- Hyperscale cloud providers such as AWS, Microsoft Azure and Tencent, and other large cloud providers are using FACs today, and growing their implementation to achieve price/performance improvements.

- Vendors are aggressively marketing FACs, which are also referred to as data processing unit (DPU), infrastructure processing unit (IPU), SmartNICs, distributed services card (DSC) or programmable NICs.

- 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.

- FACs can reduce the number of servers and hypervisor licenses by 10% to 30%, and may also decrease the number of application software licenses.

- Pulling security out of the server reduces the software-based surface area for attack.

- 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.

- FACs are increasingly bundled in high-performance solid-state storage systems to boost IOPS and minimize latency.

- FACs provide an alternative platform to host network appliances, such as firewalls and ADCs, with price/performance benefits in specific usage scenarios.

- Vendors with a large enterprise-installed base, including Hewlett Packard Enterprise (HPE) and VMware, have invested heavily in the technology and marketed it to organizations with specific usage scenarios until 2022. However, there has been a slowdown in the past few months.

- Increased consolidation in the market with AMD acquiring Xilinx and Pensando Systems, and Microsoft acquiring Fungible.

Obstacles

- Enterprises perceive FACs as a disruptive and dramatic departure from typical data center networking patterns, which limits adoption due to concerns over risk.
- There is confusion in the market due to vendors using different terminology, and providing different capabilities and architectures.
- Data plane programmability is high-risk, and has limited value and interest for enterprises.
- Hyperscale CSPs are able to justify the incremental price with the large-scale order and customization benefits they get by adopting FACs. However, enterprises are so far unable to do so, thereby hindering rapid adoption.
- Form factor and power consumption can impact rack, power and cooling budget, or occupy a full-size PCIe slot.
- Broadcom's pending acquisition of VMware creates uncertainty for potential buyers because Broadcom doesn't currently offer a FAC.

User Recommendations

- Use FACs for specific use cases, such as acceleration of NVMe-oF and AI/ML.
- Engage your existing data center infrastructure vendors on their plans for multivendor interoperability for offload on FACs, prior to your next server refresh.
- Investigate FACs to replace legacy components like physical firewalls and reduce the number of application licenses.
- Pilot FAC offerings to improve scale/security needs in the context of a large-scale data center network (1,000 switches), or to support extremely network sensitive workloads.
- Select FAC-based storage offerings, if you are an enterprise with applications that require microsecond latency performance when processing large datasets.
- Use a cross-functional team that includes networking, compute, storage and security personnel to evaluate FAC offerings.
- Focus on management and orchestration when evaluating FACs, as they are key differentiating factors.

Sample Vendors

AMD; Ethernity Networks; Intel; Kalray; Microsoft; Napatech; Nebulon; NVIDIA; Pliops; VMware

Gartner Recommended Reading

Emerging Technologies: Adoption Growth Insights — Function Accelerator Cards (Next-Gen SmartNICs, DPUs, IPUs)

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

Software for Open Networking in the Cloud

Analysis By: Andrew Lerner, Simon Richard

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Software for open networking (SONiC) is a modular, open-source network operating system (NOS). The SONiC NOS is primarily run on network switches in data center environments. SONiC was written and open sourced by Microsoft, and is now under The Linux Foundation.

Why This Is Important

SONiC is an open-source NOS that can run on network devices. It is commercially supported by several suppliers and is being adopted in larger-scale network environments, including cloud providers and very large enterprises. The open-source software (OSS) nature of SONiC enables users to influence the development of new features or directly code them. SONiC is accelerating the disaggregation of hardware and software, because it offers a viable software option, with a number of vendors behind it.

Business Impact

As an open-source initiative with increasing commercial support, SONiC offers strong potential for network innovation, in the same manner that Linux offered in the server OS market. SONiC can reduce reliance on vendor-proprietary approaches, which enables enterprise network teams to evolve at a pace that is not determined by a specific vendor.

Drivers

- Organizations that operate large networks, including service providers, cloud providers and large enterprises, are looking to avoid vendor lock-in and/or leverage the pace of innovation associated with open source and are increasingly interested in SONiC.
- Because SONiC is open source, it has low barriers to acquisition (no software licensing cost upfront), compared with commercial software, which limits friction of initial testing and deployment.
- 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.
- Vendor marketing is driving increased interest and awareness of SONiC among enterprises and service providers.
- SONiC has emerged as the most notable and prominent open-source NOS option in terms of interest, adoption, features and commercial vendor support.

Obstacles

- Support concerns regarding noncommercial software and disaggregating hardware from software.
- A strong culture of risk aversion among enterprise network teams causes them to prefer vendor-proprietary commercial solutions with branded support.
- Nearly all commercial switching vendors lead with integrated switches running their proprietary OSs when selling to enterprises. Vendors that offer SONiC typically do so only in corner-case or one-off scenarios.
- Lack of awareness, especially in midmarket enterprises and small and midsize businesses (SMBs).
- Lack of commercially supported SONiC options from incumbent enterprise vendors.
- SONiC has limited capabilities regarding certain networking features, such as OSPFv3, port mirroring and centralized management.

User Recommendations

- In large (more than 250 switches) environments and/or within forward-leaning organizations, pilot SONiC as an NOS to drive innovation and reduce lock-in.
- Use commercially supported distribution of SONiC for mission-critical production data centers.
- When introducing SONiC, look for logically and/or physically isolated use cases, such as a new application, rack or physical location.
- Stay as close as possible to the main open-source version (trunk). Avoid implementing features that will not be added upstream to the main trunk.
- Use SONiC for simple, VxLAN-based CLOS fabrics in the data center, where the architecture is straightforward and requirements for proprietary features are minimal.

Sample Vendors

Dell, Aviz Networks, Hedgehog, BeyondEdge, Dorado, Netris

Gartner Recommended Reading

Market Guide for Data Center Switching

Sliding into the Trough

Digital Experience Monitoring

Analysis By: Mrudula Bangera, Padraig Byrne

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Digital experience monitoring (DEM) technologies monitor the availability, performance and quality of experience for an end user or digital agent as they interact with an application and the supporting infrastructure. Users can be external consumers of a service, internal employees accessing corporate tools, or a combination of both. DEM technologies seek to observe and model the behavior of users as a continuous flow of interactions in the form of “user journeys.”

Why This Is Important

DEM helps organizations address visibility in two key areas:

- **Remote employees’ experience:** Instrumenting the corporate network is relatively easy. Doing the same for a home or coffee shop network ranges from challenging to impossible.
- **Web applications:** Visibility into the performance of as-a-service-based applications (including e-commerce) presents a unique challenge, due to the location of the application and difficulty in instrumenting cloud-based environments.

Business Impact

RUM and STM technologies in DEM allow businesses to understand how the users (customers) are interacting with the brand across mobile and web. The endpoint monitoring technology gives organizations increased flexibility to gain visibility into the endpoint, network and service of the user, irrespective of where workers are located, and without requiring extensive instrumentation of the physical environment.

Drivers

- **User experience:** Organizations are coming to the realization that metrics tell only part of the story. If the user is having a less-than-ideal experience, then whatever the metrics say are meaningless. DEM can help provide visibility into not just the metric-based performance, but also the subjective portion of the user experience.

- **SaaS:** As organizations move from on-premises-based applications to SaaS-based applications, they lose visibility into, and control over, the performance of these applications. A user of a SaaS-based application in one location using a specific endpoint (such as a laptop or mobile) may have a totally different experience from a different user at a different location using a different endpoint. Even the same user at the same endpoint may have very different experiences, depending on where they are located at the time. DEM enables organizations to understand where the performance bottlenecks are, so they can be addressed.

- **Work from anywhere:** The massive changes in workforce location brought on by the COVID-19 pandemic are driving infrastructure and operations (I&O) teams to adopt endpoint monitoring technologies to analyze and optimize remote workers' access to, and use of, applications.

- **"Last mile" in full-stack observability:** Monitoring of applications from the server side is important, but I&O teams need to understand the end-user journey and the corollary experience. Endpoint monitoring through DEM tools allows I&O teams to track performance from the endpoint's connectivity to Wi-Fi through service provider networks and beyond.

- **Commercial off-the-shelf (COTS) and virtual desktop infrastructure:** Organizations often rely on COTS applications for critical business operations. The very nature of these solutions makes them difficult (if not impossible) to instrument from an application perspective. I&O teams rely on the visibility provided by DEM tools to provide information on performance from the end user's perspective.

Obstacles

- There are very few DEM vendors that provide functionality across all three pillars of DEM (synthetic monitoring, endpoint visibility and real-user monitoring), making it difficult to choose a vendor that can provide a complete solution.

- Most DEM visibility comes from an agent installed on the endpoint, which can represent a challenge for organizations that are already running numerous endpoint agents.

- Large organizations may struggle with the management of tens or hundreds of thousands of endpoints via a DEM tool user interface.
- Due to the sheer volume of data generated by DEM tools, organizations without a robust analytics approach may struggle to make sense of all the data. Few vendors use analytics to enable a proactive approach in this space.
- User experience can be enhanced through autorectification of anomalies. However, very few DEM vendors provide the ability to automate remediation.

User Recommendations

- Gain a holistic view of digital experience by choosing and deploying DEM solutions that gather sentiment alongside other data points.
- Minimize endpoint performance impacts by evaluating DEM capabilities from vendors and tools you already own (for example, DEM capabilities from a unified endpoint management , security or remote access vendor).
- Enable insight-driven automation by choosing DEM solutions that provide analytics and remediation functions.
- Measure SaaS application performance by choosing DEM solutions that can perform real-user monitoring and synthetic transaction monitoring.
- Gain transparency into employee experience by monitoring as many endpoints as possible.

Sample Vendors

Apica; Catchpoint; Cisco; Fortinet; Kadiska; Lakeside Software

Gartner Recommended Reading

Market Guide for Digital Experience Monitoring

How to Monitor and Troubleshoot Remote Workers' Application Performance

3 Ways to Optimize Observability and Monitoring of Digital Services in the Cloud

Use DEM to Understand and Enhance Your Employees' Work-From-Home Experience

Use Synthetic Monitoring to Enhance User Experience for Hosted and SaaS Applications

Software-Defined Cloud Interconnect

Analysis By: Lisa Pierce, Karen Brown

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Software-defined cloud interconnect (SDCI) provides private network connectivity between enterprise sites and public cloud service providers (CSPs). SDCI providers preprovision physical connectivity from their hubs to public CSPs, internet service providers (ISPs) and network service providers (NSPs). They serve as intermediaries to quickly provision logical connectivity to CSPs and add in billing, application and network performance monitoring/management, security and administrative functions.

Why This Is Important

SDCI services are key enablers of private, high-performance connectivity to public cloud services and are operationally simpler than dealing with individual cloud service providers on a one-off basis. They reduce enterprise complexity by providing a single interface to dozens of CSPs (IaaS, PaaS and SaaS providers), ISPs and NSPs. In a well-designed edge architecture, these same functions are also useful when a CSP site experiences either an interim or prolonged/catastrophic outage.

Business Impact

Simplifying the method of connecting into multiple public CSPs serves to optimize 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 include other services, such as security features, SD-WAN gateways and inter-SDCI hub WAN transport.

Drivers

- Most enterprises are best served by employing two types of connectivity to cloud providers, one is Internet and the other is private port connectivity, which requires private WAN services like MPLS, Ethernet or wavelength. Gartner estimates that enterprise spending on private/dedicated connections to the cloud will grow at 20.5% CAGR in the period 2020-2025 to reach almost $3 billion (see Forecast: Communications Services, Worldwide, 2020-2026, 1Q22 Update). SDCI is one form of private cloud connectivity.

- Today, 80% of enterprises connect to multiple CSPs; in fact, most enterprises connect to 40+ public CSPs. In addition to internet connectivity, private cloud ports aren't scalable (need one WAN connection and private cloud port per CSP) and typically require backhaul, which adds latency. SDCI offers a turnkey managed approach to simplify complex cloud connectivity requirements from enterprise sites to CSPs.

- User interviews confirm that another common SDCI use case is to move data between CSPs.

- Clients with dispersed operations who heavily rely on CSP public (internet) ports can aggregate internet traffic from multiple sources through SDCI to CSP private cloud ports.

- SDCI hubs are ideal for serving as cloud edge onramps — and addressing growing client requirements to optimize packet and applications performance to multiple CPS, along with addressing security requirements.

- SDCIs are the most flexible private method to connect to multiple CSPs and to manage that connectivity going forward; by the end of 2027, we anticipate that 30% of enterprises will use SDCI services to connect into public CSPs — up from less than 10% in 2022.

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 and benefits of private connectivity options into CSPs.
- 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, making 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.
- SDCI, CBaaS, carrier connect and cloud hub vendors all offer private cloud connectivity services that have some functional overlap, making it difficult for enterprises to determine which option is best to use.

User Recommendations

- Use SDCI managed services to support multicloud CSP use cases and also bundle in WAN and access. Alternatively, you may employ SDCI just for CSP connectivity if you have secured WAN and access by other means.
- Compare the availability and maturity of other functions, like edge architecture, security, application and network monitoring/management, billing, UCaaS, SD-WAN and cloud networking software.·
- Favor SDCI service integration versus bolt-ons. For example, prefer offers where the provider truly integrates security into the offer versus simply routing traffic to a security provider’s cage.
- Verify that end-end reliability, security and performance meet your needs in hybrid environments like mixed computing and applications environments and multicloud use cases.·
- Survey emerging alternatives: A growing number of SDCI providers offer connectivity to multiple cloud providers, enhanced internet backbone providers and carriers. Carefully assess your own needs and the changing provider landscape.

Sample Vendors

Console Connect; CoreSite; Epsilon Data Management; InterCloud; Stateless

Gartner Recommended Reading

How to Optimize Network Connectivity Into Public Cloud Providers

Optimize WAN Architectures for Workloads That Span the Hybrid Cloud and the Multicloud

Infographic: How to Best Connect to Public Cloud Services

NaaS

Analysis By: Ted Corbett, Gaspar Valdivia, Jonathan Forest, Lisa Pierce

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Network as a service (NaaS) is a standardized and highly automated delivery model for networking functionality. It offers support for dynamic scaling up and down of network resources. The NaaS vendor primarily owns and operates NaaS offerings. Pricing is on a pay-for-use basis, or as a subscription based on usage metrics. Typically, self-service interfaces — including an API and a user portal — are exposed directly to customers.

Why This Is Important

Many network service providers (NSPs) and non-NSPs are creating NaaS offerings for enterprises seeking consumption-based spending for networking — similar to what cloud offers for compute. Enterprise network equipment market spending is projected to reach $94 billion in 2023. This reflects a 6.1% five-year CAGR through 2027. New entrants see growing enterprise spending, while many incumbents seek to hold on, invest in their NaaS strategy and grow amid emergent competition.

Business Impact

Currently, some 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 adaptive billing based on usage amid all-opex spending. Emerging NaaS providers' goal is to disrupt current customer sourcing norms. Over time, this disruption may expand enterprise buyer options and pricing models.

Drivers

- Many enterprises envision a future where complete life cycle network operations are delivered via a consumption-based, predictable spending model. This future would include their end-to-end networking estate spanning LAN, wireless-LAN, data center and WAN edge, for both on-premises or cloud-based network functions — including private 5G and other emerging network services.

- Buyers increasingly seek full life cycle management of their network estate, not simply all-opex network product procurement where operational leases (rentals) have long served the purpose of amortizing payment for networking products.

- 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 evolved from enterprise locations to virtually any cloud-based provider or hosted endpoint. These continue to drive enterprise objectives for increased agility, more flexible consumption models and a seamless experience across their network consumption life cycle.

- In response to evolving enterprise needs, non-NSPs are seeking to drive revenue by pursuing their own emergent offers for NaaS.

Obstacles

- Most NaaS offerings in the market are limited to pricing/licensing changes. This confuses and frustrates customers, limiting true adoption.
- Compared to traditional pricing models, positive ROI models for a NaaS proposition do not yet exist.
- Enterprises entering into NaaS agreements hand over control of their network design and face full replacement of NaaS product components upon early or end-of-term-based exit events.
- Current NaaS offerings (primarily from NSPs) are not comprehensive, focusing on the provider's points of presence, where many NaaS components such as gateways and cloud connectivity bandwidth on demand reside.
- All-opex procurement is complicated by refresh timing of different network product technologies.
- Most NaaS offerings include network hardware, but do not meet the definition of NaaS and are not different from the vendor's labeling of current offerings as new; these packages are not owned and operated by the network vendor in this case, and are not NaaS offerings.

User Recommendations

IT leaders:

- Exert caution with NaaS due to widespread confusion created by the provider community.
- Procure network products more traditionally with financial leasing methods to smooth spending.
- Retain network design control by separately procuring kit as an operations lease and add managed operations.
- Calculate before and after ROI by capturing all in-scope costs and uniformly comparing proposals to identify the differences.
- Choose NaaS to achieve operational, lease-based network product spending when this is the primary goal, and you have a predictable consumption pattern.

Technology service providers:

- 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 value of NaaS offers by disaggregating proposals and providing detailed comparisons against alternative options.

Sample Vendors

Nile

Gartner Recommended Reading

What Is NaaS, and Should I Adopt It?

Magic Quadrant for Managed Network Services

Magic Quadrant for Network Services, Global

Navigating Emerging Network-as-a-Service Promises and Challenges

Early NaaS Pricing Lessons to Drive Adoption

5G

Analysis By: Sylvain Fabre

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

5G is the fifth generation cellular technology 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, down to centimeter-level location accuracy indoors, and massive IoT scalability. New system architecture includes core slicing and wireless edge.

Why This Is Important

5G supports the 4th industrial revolution and IoT. Its fast and reliable real-time data transfer will benefit many industries. 5G supports eMBB, URLLC and MIoT — vital for enterprise transformation. 3GPP 5G standards releases deliver incremental functionality in: R15, extreme mobile broadband; R16, industrial IoT (massive IoT, slicing and security) — latest commercially available release; R17, MIMO enhancements, sidelink, DSS, IIoT/URLLC, bands up to 71GHz, nonterrestrial networks; and RedCap R18 is under definition with a planned freeze date in 1Q24.

Business Impact

- 5G enables three main technology deployments; each supports distinct new services for multiple industries and use cases of digital transformation, and possibly new business models (such as latency as a service). These are enhanced mobile broadband (eMBB) for HD video, mMTC for large IoT deployments, and URLLC for high-availability and very low-latency use cases, such as remote vehicle operations.
- Promising applications for 5G use include fixed wireless access, IoT support and private mobile networks.

Drivers

- Over 249 operators have rolled out 5G (see GSA), 30% of public mobile networks, and some form of 5G capability is penetrating lower cost smartphones in vendors' portfolios (with over nine versions of the technology depending on the band and the 3GPP release).
- Gartner estimates that 5G-capable handset penetration in 2025 will reach 54% worldwide, and 78% in Western Europe, with 5G-capable handset share of sales reaching 80% in 2023 in Western Europe from 51% in 2021. North America share will rise to close to 87%.
- 5G capability is starting to deliver value in emerging always-on wearables use cases.
- Increased data usage per user and device requires a more efficient infrastructure.
- 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 continues for massive machine-type communications (mMTC) to support scenarios of very dense deployments up to the 5G target of one million connected sensors per square kilometer. While diverse networks can offer adequate and cost-effective alternatives to 5G for many use cases (e.g., LPWA, NB-IoT, LoRa, Wi-SUN), overall total cost of ownership (TCO) and future proofness may not be as good.
- Availability has increased for industry-specific spectrum options (e.g., CBRS).
- Competitive pressures continue, for example, if one CSP launches 5G in the market others usually have to follow or risk losing market share — this includes both public as well as private 5G offerings.

Obstacles

- Issues with availability and cost of spectrum, in particular for industrial private networks, occur in some countries.
- Security concerns arise when using 5G in critical industrial scenarios.
- Availability and pricing of networks and modules for R16 and beyond solutions.
- Upgrade to 5G SA (stand-alone) core is needed for more advanced R16 releases (such as slicing), and commit to the continuous evolution of 5G releases over R17, R18 and beyond.
- Cost of radio network upgrades for 5G coverage and availability may require additional sites.
- Use of higher frequencies and massive capacity requires denser deployments with higher frequency reuse, which could raise network costs.
- Uncertainty exists about use cases and business models that may drive 5G for many CSPs, enterprises, and technology and service providers (TSPs).
- Feedback from some industrial clients mentioned that the majority of their use cases could be serviced by a 4G private network, Wi-Fi and/or NB-IoT, and other LPWA such as LoRa.

User Recommendations

- Enable R16 and above 5G for enterprise connectivity for mobile, nomadic 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 and 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 fall back 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 an ecosystem of partners to target industry verticals more effectively with 5G before your competition.

Sample Vendors

Ericsson; Huawei; Mavenir; Nokia; Qualcomm; Rakuten Symphony; Samsung Electronics; ZTE

Gartner Recommended Reading

Emerging Tech: 5G mmWave at a Crossroads

Infographic: 5 Steps for Vendors to Scope and Run Successful POCs for Enterprise 5G PMNs

Invest Implications: Magic Quadrant for 5G Network Infrastructure for Communications Service Providers

Market Guide for 4G and 5G Private Mobile Networks

Quick Answer: What Vendor Product Leaders Need to Know About MWC Barcelona 2023

Edge IoT Networking

Analysis By: Tim Zimmerman, Bill Ray, Nick Jones

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Edge Internet of Things (IoT) networking represents a diverse set of communication technologies that connect end-user devices and sensors to edge computing platforms or to the cloud. For WAN-connected devices, this includes cellular (public and private), low-power wide-area (LPWA) and satellite technologies. For on-premises, connectivity includes traditional Ethernet and Wi-Fi, but also over 40 industrial and building automation protocols for wired and wireless infrastructures.

Why This Is Important

Edge (IoT) networking has traditionally been siloed because the end-to-end solutions require transporting the data to different application platforms — on-premises servers, edge computing platforms or to the cloud. Therefore, many edge IoT devices now have multiple communication technologies integrated. Wired cabling provides RS-232 or other connectivity where wireless is not available. LPWA provides private, low-bandwidth connectivity for remote devices where cellular provides public connectivity. Wi-Fi provides high performance, in-building connectivity, while others address low latency.

Business Impact

As 18 billion devices connect to the network, visibility of IoT for security risk and discovery is now mandatory for any IT strategy. As responsibility converges from other organizations to IT, edge IoT networking will lead to simplified deployment and operation. The longer-term value will be the commoditization of the hardware and lower connectivity prices across all vertical markets, since performance and pricing may not be needed by all applications to achieve the desired business outcome.

Drivers

- **Standardization of technology —** Advances in cellular, LPWA, 5G, Wi-Fi and BLE. Both 5G and Wi-Fi (802.11be) allow them to meet performance requirements, and offer coverage and low-latency “wireless” connectivity.

- **Shrinking number of OT teams —** As more technologies converge onto a single IT infrastructure, a growing number of operational technology (OT) teams continues to merge into IT.

- **Security —** Historically siloed connectivity technologies provided security by obscurity while newer, standards-based options provide authentication and data encryption options to address use-case requirements.

- **Pricing —** The ability for the market to focus on a discrete set of solutions will drive pricing for overall connectivity down.

Obstacles

- **Refresh rates of devices —** Edge IoT business solution refresh rates are very slow — often 10 years or longer — which means the opportunity window to update them to standardized technologies is drawn out.

- **Proprietary protocols —** Many communication protocols at the edge are proprietary and the move to IP-based protocols for these solutions is slow.

- **Slow deployment of connectivity options —** The ability for newer connectivity options to be deployed is also drawn out, since the implementation of time-sensitive networking (TSN) for low-latency Wi-Fi requirements will be standardized. Also, the rollout of 5G/NB-IoT to reach nonmetropolitan/rural areas will take years.

- **Limited migration capabilities —** Unfortunately, moving from LPWA or WirelessHART means replacing the communication infrastructure with limited or no path for migration to newer technologies. This will impact deployment timeframes for end users that need to use the existing assets to address business case ROI requirements.

User Recommendations

- Document any organization changes to ensure that the information about legacy OT networks or any inherited network and associated assets is well known.
- Beware that WAN and WLAN/LAN solutions today require different and separate communication infrastructures.
- Invest in public (5G, NB-IoT) or private cellular technology for large, open environments that could be indoor (utilities or manufacturing plants) or outdoor. Evaluate if the solution attributes for throughput, latency and device density are required by your applications.
- Invest in Wi-Fi 6 for indoor enterprise applications or defined outdoor environments such as stadiums or parks. Monitor the technology for 802.11be, do not pay any premiums for the new functionality (Wi-Fi 6E) due to limited device availability at 6 GHz.
- Mandate support for 802.11u to allow migration of applications connectivity from WAN to WLAN infrastructures and upgradability to any new standards that provide Wi-Fi 6E.
- Choose vendors that provide IoT platform connectivity — e.g., IoT ports or multiple radio options — to address edge solution requirements.

Sample Vendors

AT&T; Belden (Hirschmann); Cisco; Extreme Networks; HPE (Aruba); Juniper Networks; Siemens; Sierra Wireless; Verizon Communications; Vodafone

Gartner Recommended Reading

Despite the 5G Hype, 3GPP LPWA Is the Emerging Workhorse of IoT Connectivity

Forecast: Internet of Things, Endpoints and Communications, Worldwide, 2022-2032, 1Q23 Update

Important and Compelling Innovations for Commercial IoT Use Cases

Multicloud Networking Software

Analysis By: Andrew Lerner, Marissa Schmidt

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Early mainstream

Definition:

Multicloud networking software (MCNS) enables the design, deployment and operation of a network within multiple public cloud environments. MCNS enables unified networking policy, network security and network visibility across multiple cloud environments. These products address traffic routing, secure ingress and egress, and integrate with public cloud services. MCNS can be self-managed and/or delivered as a service. It is accessible via APIs and UIs.

Why This Is Important

MCNS improves networking within public cloud environments. Enhancements include consistent management and visibility across multiple cloud environments, and/or feature depth within public cloud environments, beyond what the cloud provider offers natively.

Business Impact

Enterprises are heavily investing in public cloud services to modernize and digitally transform. Public cloud providers' native networking capabilities are "good enough" for many use cases, but have some notable gaps. MCNS directly addresses these gaps.

Drivers

- Many organizations are looking for consistent networking features and management across multiple cloud environments.
- MCNS simplifies Day 2 network operations within public cloud environments, including visibility and troubleshooting.
- Enterprises look to MCNS when cloud-native functionality is inadequate. For example, enterprises invest in MCNS to address overlapping IP addresses, higher VPN bandwidth, "full stack" networking and security (e.g., web application firewall [WAF] and distributed denial of service [DDoS]), advanced routing, encryption, and inadequate troubleshooting and visibility.
- MCNS can be used as an alternative to native transit services such as AWS Transit Gateway or Azure Virtual WAN.
- Enterprises use MCNS to address complicated networking requirements associated with B2B extranet environments where there are multiple parties connected.

Obstacles

- Enterprises start with their cloud providers' native stack, which is often good enough for initial use cases, and then becomes very "sticky," limiting their ability to use MCNS.
- Enterprises view MCNS as a "nice to have" and not a "must have," making it difficult to justify large or long-term investments.
- Enterprises wanting to deploy MCNS for existing workloads must perform a network cutover, which is tedious, creates risk, and requires downtime and often professional services. This deters investments and slows deployments.
- Since 2022, prominent MCNS vendors have scaled back investments in sales and marketing, elevating enterprise concerns and reducing awareness around and access to the technology.
- MCNS products add purchasing complexity and operational expense, as a result of the additional software, configurations and installations that must be managed.
- Most vendors that are heavily focused on this market are lesser-known. This prevents, deters or delays investment.
- Many midsize enterprises and SMBs aren't aware of MCNS.

User Recommendations

- Use the native network capabilities of the cloud providers, until they do not sufficiently address business needs.
- Invest in MCNS when networking feature depth or operational network consistency across clouds is critical to the business.
- Require that MCNS vendors heavily assist with the migration to their MCNS product, via migration tools, automation and professional services.
- Prefer MCNS offerings that are API-first and "cloud-fluent" (meaning they dynamically interact with their surrounding environment, using the cloud platform API).
- Prefer MCNS vendors that offer consumption-based pricing if your needs are unpredictable or highly dynamic.

- Invest in MCNS offerings that offer strong security features (e.g., segmentation, encryption and firewall) or provide turnkey integration with your selected security vendors.
- Avoid replicating existing on-premises data center networking designs and vendors when deploying workloads in the public cloud.

Sample Vendors

Alkira; Aviatrix; Cisco Systems; F5; Prosimo

Gartner Recommended Reading

Market Guide for Multicloud Networking Software

LEO Satellite Communication Services

Analysis By: Bill Ray

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Low earth orbit (LEO) satellites operate at an altitude of less than 4% of the distance compared to a traditional communication satellite. Connecting to satellites in LEO uses significantly less power, supporting low latency and faster data. However, coverage requires a large number of satellites, most of which will have a limited life span. Several companies have launched LEO services for broadband internet access, while others are focused on low-speed (and low-power) IoT connectivity.

Why This Is Important

Innovations from the smartphone industry, along with lower launch costs, make LEO constellations economically viable. The orbit makes power consumption and latency comparable to terrestrial services. As of 2Q23, Starlink is providing internet access to a million customers and OneWeb is providing global connectivity to enterprises. Other operators (including Amazon) are still working toward commercial services.

Business Impact

LEO services make broadband internet and IoT data globally available. Companies and employees can assume that internet access and IoT sensing will always be available, which would remove network access as a limit on locations to work or live. Geography will cease to be a factor in recruiting the best staff and supporting the most profitable customers. This connectivity is extending to include airplanes, 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. Other customers include airlines, ships and the military.

- Satellite broadband is relatively expensive (SpaceX's Starlink charges $99 per month, plus $499 for installation) and won't compete with already installed fiber to the cabinet or home. However, we have calculated that there are enough homes without connectivity to sustain the Starlink service with reasonable penetration.

- 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.

- As of 2Q23, Starlink and OneWeb are both offering commercial services. But these will need to compete with offerings from Amazon's Project Kuiper network, as well as competing projects such as E-Space, SATNet and Telesat.

- The 3rd Generation Partnership Project (3GPP) is creating standards for integrating LEO services with terrestrial networks, initially for narrowband (IoT and messaging), but in recognition that supplementary coverage from space (SCS) will become an increasingly important factor in providing global connectivity.

- IoT connectivity is a different market, focusing on low cost and low power to provide global asset monitoring and tracking. While asset tracking remains the primary application, condition and environmental monitoring will also be an important use case.

Obstacles

- To provide oceanic and remote region coverage (needed by military customers), satellite-to-satellite (intraconstellation) links are required. Starlink is testing such connections, but other constellations are still at the planning stage.
- Customer equipment currently costs more than $1,000, and subscription costs will vary widely between providers.
- Maintaining 30,000 satellites, with a life of five years, requires 500 new satellites per month. Current launch vehicles, such as SpaceX's Falcon 9, can launch 60 satellites at a time. This will not be sufficient, so larger launch vehicles (such as SpaceX's 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 strategic workforce and business planning.
- Prepare for international availability by liaising with local regulators and resellers. LEO services are inherently global, so these 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.
- Mitigate against requirements for proprietary equipment by planning for a reinstallation in five years, allowing for updated equipment or a change of satellite service provider.

Sample Vendors

Astrocast; Myriota; OneWeb; SpaceX

Gartner Recommended Reading

Maverick* Research: LEO Satellites Will Trigger the Revolution That 5G Has Failed to Deliver

3 World-Changing Opportunities Emerged While You Were Fighting COVID-19

SASE

Analysis By: Neil MacDonald, Andrew Lerner

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Secure access service edge (SASE) delivers converged network and security capabilities, including SD-WAN, SWG, CASB, firewall and zero trust network access (ZTNA). SASE supports branch office, remote worker and on-premises secure access use cases. SASE is primarily 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, performance, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and security services mainly via a cloud-delivered model. SASE reduces the number of vendors required for secure access to one or two explicitly partnered vendors.

Business Impact

SASE enables:

- Digital business use cases (such as branch office transformation and hybrid 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

- Digital business transformation including the adoption of cloud-based services by mobile workforces, edge computing and business continuity plans that must include a flexible, anywhere, anytime, secure, identity-based logical perimeter model of SASE.

- The need to flexibly support digital business transformation efforts with a zero trust security architecture while managing complexity is a significant factor for the adoption of SASE, primarily delivered as a cloud-based service.

- For IT, SASE can reduce the deployment time for new users, locations, applications and devices.

- For information security, SASE enables a single way to set policy enforcement consistently across all types of access — internet, web applications and private applications, reducing the attack surface and shortening remediation times.

- Enterprise desire to simplify network and network security deployments via the reduction of policy engines and management consoles.

Obstacles

- **Organizational silos, existing investments and skills gaps**: A full SASE implementation requires a coordinated and cohesive approach across security and networking teams, which is challenging given refresh/renewal cycles, silos and existing staff expertise.

- **Organizational bias and regulatory requirements for 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, Africa, South America and the Middle East.

- **SASE maturity:** SASE capabilities vary widely. Sensitive data visibility and control is often a high-priority capability, but it is difficult for many SASE vendors to address. While your preferred single vendor may lack the capabilities you require, two-vendor partnerships can be a viable approach.

User Recommendations

- Involve the security architect and network architect when evaluating offerings and roadmaps from the incumbent and emerging vendors to ensure an integrated approach.
- Leverage WAN, firewall, VPN hardware refresh cycles or software-defined WAN (SD-WAN) deployments to update network and network security architectures.
- Explore single-vendor SASE, dual-vendor SASE and managed SASE options when investing, but avoid deploying SASE with more than two vendors, regardless of vendor marketing for all core services to minimize complexity and improve performance.
- Use vendor combinations — when selecting a dual-vendor solution — that have explicit integration including turnkey automation and visibility, and ideally management and data plane integration.
- Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the number of vendors required.
- Leverage branch office transformation and dedicated circuit offload projects to adopt SASE.

Sample Vendors

Cato Networks; Cisco Systems; Cloudflare; Forcepoint; Fortinet; Juniper Networks; Netskope; Palo Alto Networks; Versa Networks; Zscaler

Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Market Guide for Single-Vendor SASE

The Future of Network Security Is in the Cloud

Magic Quadrant for SD-WAN

Magic Quadrant for Security Service Edge

Intent-Based Networking

Analysis By: Andrew Lerner

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

The IETF defines intent-based networking (IBN) as a set of operational goals and outcomes defined in a declarative manner without specifying how to achieve or implement them. Gartner further specifies IBN as a closed-loop system to design, provision and operate a network based on business policies. IBNs translate business policies to network configurations, automate network activities, maintain an awareness of network health and provide continuous network assurance and dynamic optimization.

Why This Is Important

Intent-based networks simultaneously improve network agility and reliability while enabling a common policy across multiple infrastructures. Unfortunately, the term is used loosely by network vendors. Thus, most offerings marketed as intent-based fall short of the complete functionalities of intent-based networking. Instead, we observe an incremental adoption of the subcomponents of an IBN, including network automation, configuration validation and network assurance.

Business Impact

A complete IBN implementation can reduce the time taken to deliver network infrastructure to business leaders by an estimated 50% to 90%. It can simultaneously reduce the number and duration of outages by an approximate 50%. However, there has been limited impact to date due to low real-world adoption and a lack of viable, easy-to-use full IBN products.

Drivers

- There is a desire to make networks more agile in conjunction with cloud deployments and digital business.

- Intent-based networking offers a reduced operating expenditure (opex) associated with managing networks. Therefore, more senior-level network resources are free to focus on more important strategic tasks.

- There is a desire to simplify network administration amid the increasing complexity of networking with overlays, cloud environments and containers.

- IBN allows real-time self-documentation, which also includes the rationale — that is, the intent behind design or configuration decisions.

- IBN can lead to improved compliance and simplified auditing. This is due to the algorithmic correctness of configurations that provide self-validation, direct mapping to the business intent and ongoing, dynamic and real-time validation.

- IBN can help to reduce the impact of enterprises that are not able to hire or retain senior-level network engineers and architects.

- In October 2022, the IETF published the informational document, RFC9315, which helps to streamline IBN terminology and definition. This research document can reduce confusion, foster consistency and consequently clear hurdles to adoption.

Obstacles

- Only a limited number of vendors offer complete IBN capabilities. Very few offerings translate a higher-level intent into network configuration — we estimate that there are fewer than 1,000 full deployments.
- Network automation, AI networking and AIOps all deliver some of the value intent-based networks offer, and are often simpler to implement. This limits, prevents or delays IBN.
- Vendors are increasingly delivering recommendation engines and predictive capabilities in their management products, which limits or delays IBN.
- Very few vendors provide full intent-based networks. Instead, vendors release products that deliver some discrete individual benefits, often with limited integration between them.
- Full IBN is restricted to greenfield or very homogeneous environments that are deployed in a very prescriptive, structured and specific way. This inflexibility limits adoption.
- It is challenging to define intent for preexisting network deployments.

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 or prescriptive predictions with specific recommendations.
- Invest in network products that provide specific and 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.

Sample Vendors

Gluware; Juniper Networks; NetBrain

Gartner Recommended Reading

Market Guide for Network Automation Tools

Climbing the Slope

Software-Defined Networking

Analysis By: Andrew Lerner, 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. The Open Networking Foundation specifically defines SDN as “the physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices.”

Why This Is Important

SDN products that separate the network control plane from the forwarding plane never achieved mainstream enterprise adoption. Unfortunately, with time, SDN has evolved into an overused marketing term, essentially meaning “new stuff in networking.” However, interest in SDN led to innovations in automation, orchestration and programmability. It paved the way for innovations like software-defined WAN (SD-WAN), microsegmentation, brite-box switching and SD-branch products.

Business Impact

Products that meet the true technical definition of SDN are rare in the enterprise. However, products that are marketed as SDN — but that do not meet the architectural definition of SDN — can have many benefits. They 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 initially driven by academia, along with large network operators that were looking to innovate on traditional proprietary networking solutions.
- Early SDN drivers aligned with the idea of separating hardware from software, with a view to fostering innovation in both, while increasing agility in order to lower costs.

- Although SDN technology is obsolete, SDN terminology is widely used in vendors' marketing efforts. This use is the main driver of discussions about SDN today.

Obstacles

- There are almost no SDN technologies available in the enterprise that meet the technical definition of SDN. True SDN technologies have not achieved any significant traction in the enterprise market.
- Vendors widely market non-SDN technologies as SDN, which misleads and confuses customers.
- The hope that SDN would enable decoupling of the control plane from network hardware and foster independent software innovation was never fulfilled.

User Recommendations

- Do not fall for vendors' misleading claims that their commercial products are SDN products, nor should you engage in any discussions about deploying them.
- Focus on reducing or eliminating the "human middleware" — that is, manual operation — problem that has plagued traditional network solutions for two decades.
- Execute on SD-WAN, SASE and network automation initiatives to reduce human error, increase quality, improve agility and cut costs.

Gartner Recommended Reading

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

Microsegmentation

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

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Microsegmentation — also referred to as identity-based segmentation or zero trust network segmentation — can create more granular and dynamic access policies than traditional network segmentation, which is limited to internet protocol/virtual LAN (IP/VLAN) circuits.

Why This Is Important

Once a system is breached, attackers move laterally (including in ransomware attacks), which can cause serious damage. Microsegmentation seeks to limit the propagation of such attacks. It can greatly reduce the initial attack surface as well.

Business Impact

Microsegmentation can mitigate the risk and impact of cyberattacks. It is a form of zero trust networking that controls the access between workloads and is used to limit lateral movement, if and when an attacker breaches the enterprise network. Microsegmentation also enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads, including those that host containers.

Drivers

- As servers are being virtualized, containerized or moved to infrastructure as a service (IaaS), existing safeguards such as traditional firewalls, intrusion prevention solutions and antivirus software struggle 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.

- Zero trust is becoming a requirement in data center design, and microsegmentation is a practical way to accomplish this.

- The increasingly dynamic nature of data center workloads makes traditional network-centric segmentation strategies difficult to manage at scale, if not impossible to apply.

- Some microsegmentation products provide rich application communication mapping and visualization, allowing data center teams to identify which 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 restricted the ability of network-centric firewalls to provide this segmentation.

- The extension of data centers into IaaS has placed a focus on software-based approaches for segmentation — in many cases, using the built-in segmentation capabilities of 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

- Complexity — If not planned and scoped correctly, microsegmentation 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 protection 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 when policies overlap or conflict.
- 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 microsegmentation to be a net new budget item.

User Recommendations

- Select zones to microsegment based on the highest risk. Oversegmentation is the leading cause of failure and an unnecessary expense for segmentation projects.
- Seek a solution that maps application communication paths and makes policy recommendations, using AI to make policy recommendations.
- 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 microsegmentation style (network overlay, host-based, cloud-native, API-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).
- Target the most critical assets and segment them first.
- Plan for coexistence of traditional firewalls and microsegmentation approaches for the next five years, and seek products that can support both.

Sample Vendors

Akamai Technologies; Aqua Security Software; Cisco; ColorTokens; Fortinet; Illumio; Palo Alto Networks; VMware; Zero Networks; Zscaler

Gartner Recommended Reading

2023 Strategic Roadmap for Zero Trust Security Program Implementation

SD-WAN

Analysis By: Jonathan Forest

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Software-defined wide-area network (SD-WAN) products are primarily used to connect branch offices. They provide dynamic path selection, based on business or application policy, routing, centralized orchestration of policy and management of appliances, and virtual private network (VPN) and zero-touch configuration. SD-WAN products are WAN transport/carrier-agnostic and create secure paths across physical WAN connections.

Why This Is Important

SD-WAN products optimize site availability, performance, cost and agility for enterprise WANs, and are aligned with the broader shift of applications to public cloud workloads. Client demand remains high, and we estimate that approximately 120,000 customers have deployed SD-WAN products in their production networks.

Business Impact

SD-WAN products create simpler, more cost-effective branch-office WANs that support modern application and cloud architectures. They are much easier to deploy, offer more agility and deliver better performance than traditional, router-based or next-generation firewall (NGFW) solutions. Other benefits include easier operational management at the WAN edge, simpler connectivity to the cloud, better application-specific performance and greater branch availability than traditional routers.

Drivers

- Digitalization and cloud adoption are driving more applications from private data centers to the public internet, including public clouds (SaaS and IaaS). The desire to have direct connectivity to applications (without backhauling to a data center) in order to minimize latency continues to drive SD-WAN adoption.
- The renewal of first-generation SD-WAN service contracts provides an opportunity for organizations to reevaluate vendor offerings.
- With path selection functionality and manageability, SD-WAN technology can deliver better performance and availability of applications than static policy-based routing.
- Organizations are increasingly investing in secure access service edge (SASE) offerings, which drives SD-WAN deployments.
- The expiration of Multiprotocol Label Switching (MPLS) contracts makes organizations rethink their WAN architectures.
- Organizations worry that they may lag behind in the adoption of SD-WAN technology.

Obstacles

- Some vendors are promoting the myth that enterprise WANs and SD-WANs are no longer required. Some vendors claim that internet access and cloud-delivered security are all that is needed.
- The fact that some employees of organizations are working remotely reduces the demand for SD-WAN solutions.
- A lack of cloud adoption in certain industries and geographies reduces the benefits of SD-WAN solutions.
- Enterprises that backhaul traffic within a metropolitan area do not benefit from a local internet breakout to reduce latency when connecting to the cloud.

User Recommendations

- Involve security teams and cloud teams in the vendor selection process.
- Compare on-premises security with cloud-delivered security to determine the best security architecture.
- Confirm SD-WAN cloud onramp capabilities by involving cloud teams and validating orchestration with cloud service providers such as Microsoft (Azure) and Amazon Web Services (AWS), and carrier-neutral facilities such as Equinix. Confirm virtual image compatibility with various cloud platforms, for cloud-first organizations.
- Shortlist and execute a proof of concept based on desired functionality by focusing on ease of use, application performance, cloud connectivity and security functionality use cases, as opposed to perceived leadership in the market or incumbency.

Sample Vendors

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

Gartner Recommended Reading

Magic Quadrant for Network Services, Global

Critical Capabilities for Managed Network Services

Magic Quadrant for SD-WAN

Critical Capabilities for SD-WAN

Magic Quadrant for Managed Network Services

IPv6

Analysis By: Nauman Raja

Benefit Rating: Low

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Internet Protocol version 6 (IPv6) is the successor to the current Internet Protocol version 4 (IPv4). IPv6 has been standardized under RFC 2469. It was primarily developed to overcome IPv4's limitations and the exhaustion of public IPv4 addresses. IPv6 uses 128-bit addresses vs. 32-bit for IPv4, and includes new functionality, such as quality of service (QoS) and IP security (IPsec).

Why This Is Important

Since 2020, there has been a circa 5% increment each year in the number of users accessing internet services using IPv6. Allocations of public IPv4 addresses were exhausted in November 2019, therefore, new public IP addresses are either allocated from instances of returned IPv4 blocks or are IPv6 addresses. IPv6 will eliminate overlapping addresses and the need from complex network address translation (NAT) techniques.

Business Impact

The immediate impact of IPv4 address exhaustion is minimal because NAT techniques enable the connection of millions of internet-connected devices through the use of a single public IPv4 address. The migration of data centers to the public cloud and the shift from private WANs to internet circuits have decreased the requirements for public IPv4 addresses for the enterprise.

Drivers

- The allocation of new public IPv4 addresses is exhausted. However, companies can still obtain IPv4 address blocks through various secondary sources, such as brokers, and designated IP address registries (ARIN, IANA, etc.). Single, noncontiguous and smaller contiguous IPv4 address blocks are also still readily available from primary sources.

- Acquiring public IPv4 addresses is expensive and costs between $40-60 per IP address on the open market vs. as little as $500 for an IPv6/40 address block. This makes IPv6 fiscally more attractive for companies who provide public-facing native IPv6 services.

- China, India, the Netherlands and the U.S. governments have mandated IPv6 adoption. The European Commision has IPv6 as one of its six key categories in the EU Internet Standards.

- Many government agencies and higher education institutions are mandating greater adoption of IPv6 on backbone and public internet facing servers and devices at a minimum.

- Tech vendors, including communication service providers are keen to simplify their infrastructure by reducing the need to use CGNAT gateways. Therefore, they are aggressively enabling IPv6 on their IPv4 products giving their customers a choice.

Obstacles

- The cost, maintenance, mitigation risks and training burden of converting existing IPv4 network infrastructure to support IPv6 is high, while immediate short- and medium-term return on investment is low.

- Support features and performance parity for IPv6 is still variable across applications, devices and network infrastructure components.

- Claims of increased performance of native IPv6 routing vs. legacy NAT-enabled IPv4 have not been validated and vary widely based on other factors.

- There are many instances where disabling IPv6 on the network actually increases the overall network and application performance.

- Lack of dual stack support on installed infrastructure is a barrier for IPv6 adoption for some organizations.

User Recommendations

- Limit IPv6 deployments to essential public-facing services, such as DNS, web and email servers, and internet-facing network segments. Gartner does not recommend migrating to IPv6 for all internal systems.
- Develop a detailed IPv6 migration plan and roadmap, which indicates which servers, infrastructure devices (end user and IoT), applications and network equipment are fully IPv6 compatible.
- Implement an IPv4, IPv6 dual stack during the migration to IPv6 only.
- Ensure that all new network infrastructure hardware and software fully support IPv6.
- Plan to operationally support dual stack routing (both IPv4 and IPv6) for the foreseeable future.
- As a precaution, validate corporate applications for IPv4 literals and hard-coded IP addresses, in application code.
- Determine IPv6 block size requirement for your organization and submit an IPv6 allocation request.
- Create a basic lab environment to test the organization’s applications with DNS64 and NAT64.

Gartner Recommended Reading

Prepare Your Cloud Connectivity Services for More-Demanding Requirements

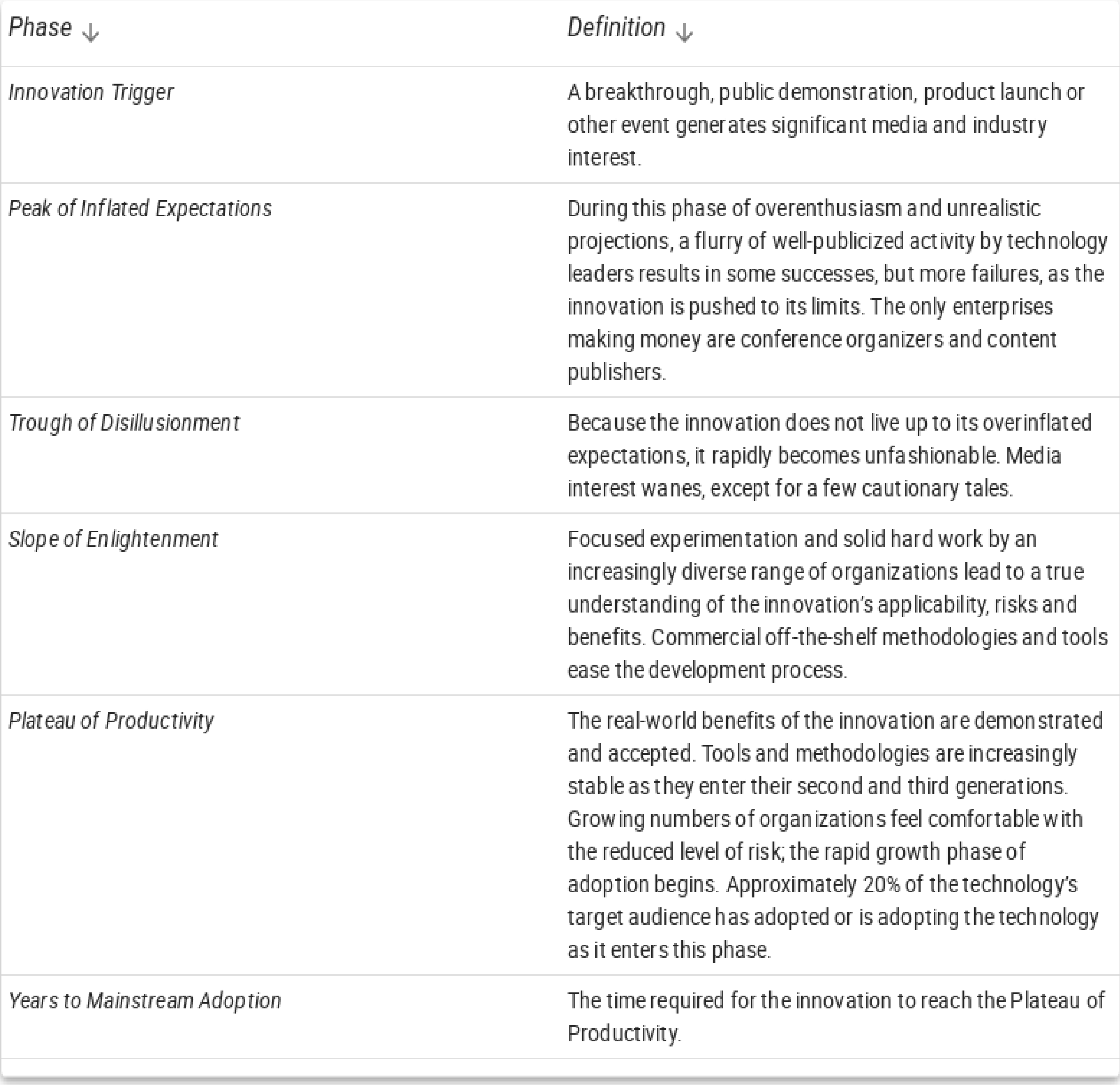
Appendixes

See the previous Hype Cycle: Hype Cycle for Enterprise Networking, 2022

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 2023)

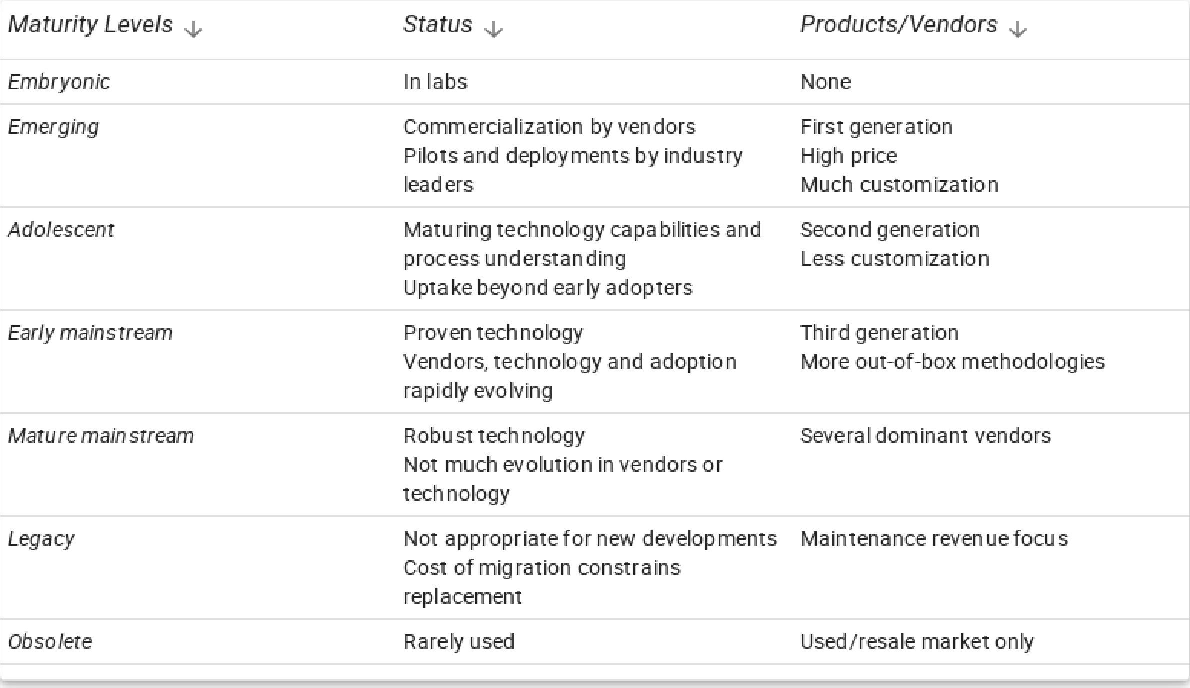
Table 3: Benefit Ratings

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 2023)

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 2023)

Evidence

Gartner analysts have taken over 5,000 inquiries on the topic of networking from 12 May 2022 through 15 May 2023.

Networking Hype Index — To help identify and select the most hyped networking terms, Gartner researchers compiled a "hype index." This hype index is a composite metric that includes client interest (inquiry and portal search), Google trends, articles in popular periodicals and analyst opinion.

Document Revision History

Hype Cycle for Enterprise Networking, 2022 - 29 June 2022

Hype Cycle for Enterprise Networking, 2021 - 7 July 2021

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

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

Table 1: Priority Matrix for Enterprise Networking, 2023

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		NetDevOps SASE	Network Digital Twin	
High	Microsegmentation SD-WAN	5G Digital Experience Monitoring Universal ZTNA	Edge IoT Networking Function Accelerator Cards Managed SASE Network Sustainability Private 5G	6G
Moderate		AI Networking LEO Satellite Communication Services Multicloud Networking Software Software-Defined Cloud Interconnect Software for Open Networking in the Cloud Wi-Fi 7 (802.11be)	Service Connectivity Layer Wi-Fi 8 (802.11bn)	Intent-Based Networking Quantum Networking

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Low			Cloud Backbone as a Service Extranet as a Service IPv6 NaaS Network Assurance	

Source: Gartner

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 2023)

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 2023)

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 2023)