2025 Strategic Roadmap for Enterprise Networking

22 October 2024 - ID G00818377 - 23 min read

By Analyst(s): Karen Brown, Tim Zimmerman, Andrew Lerner, Mike Leibovitz

Initiatives:I&O Platforms

Network technology is rapidly changing as cloud, compute and security demands grow. This creates a challenge for infrastructure and operations leaders, requiring a comprehensive network strategy to make better investment decisions.

Overview

Key Findings

- Although network operations are largely manual, emerging technological advances will shift dramatically to more-automated processes enabled by artificial intelligence (AI) during the next three to five years.
- AI language model workloads, including training and inference models, require higher-performance network connectivity and constitute only a small percentage of enterprise compute resources in data centers and in the cloud. However, we expect this to grow dramatically near-term.
- Adoption of SD-WAN and SASE, along with hybrid work policies, are driving increased investments in internet connectivity and cloud-based security and, to a much lesser extent, consumption-based services.
- Enterprise network and security operations are largely siloed, but we expect this to shift as organizations increasingly implement zero-trust principles.

Recommendations

- At every network infrastructure refresh, mandate automation and open APIs, pilot AI-enabled capabilities and add sustainability as an evaluation criterion.
- Network teams must be included in data center, cloud, edge and AI initiatives and must be trained regarding AI compute requirements.
- For new infrastructure or service contracts, evaluate usage-based/network as a service (NaaS) alternatives for cost and flexibility advantages.
- Include SASE platforms on the shortlist when making software-defined WAN (SD-WAN), secure web gateway (SWG), next-generation firewall (NGFW), zero-trust network access (ZTNA) and cloud access security broker (CASB) investment decisions.

Strategic Planning Assumptions

By 2027, generative AI (GenAI) technology will account for 25% of initial network configuration, which is an increase from less than 3% in 2024.

By the end of 2028, Ethernet will be as influential a network transport for meeting AI infrastructure requirements as InfiniBand, which currently dominates the market.

By 2027, 70% of enterprises will select a broader platform solution for new multicloud networking software (MCNS) deployments, which is an increase from 10% in early 2024.

By 2027, 65% of new SD-WAN purchases will be part of a single-vendor SASE offering, which is an increase from 20% in 2024.

By 2028, on-premises NaaS will be adopted by 15% of all enterprises, which is an increase from less than 2% in 2023.

Introduction

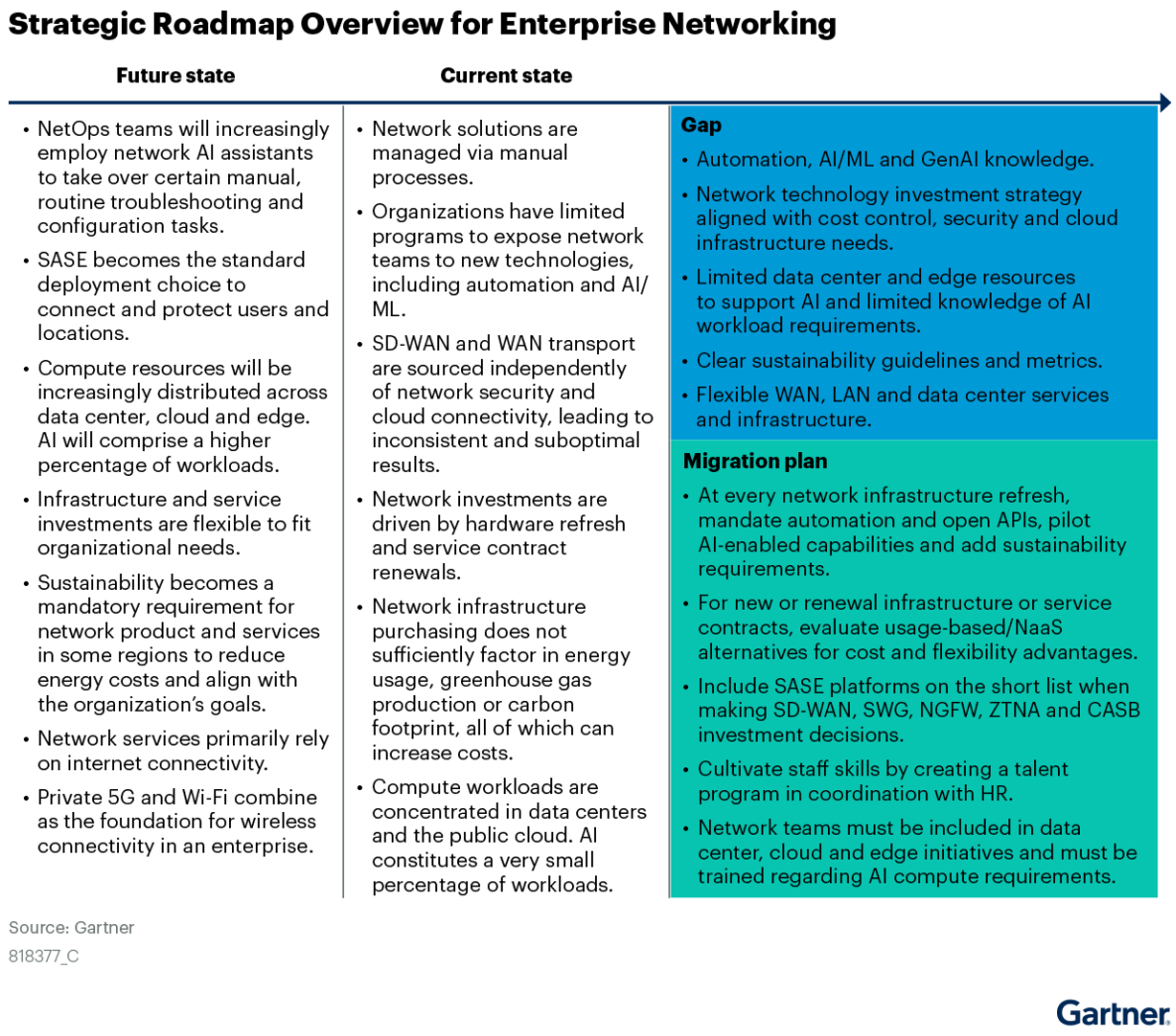
Enterprise network technology will shift materially during the next three to five years, as adoption of AI and the continued breakdown of network and security siloes impact network operations. This will force infrastructure and operations (I&O) leaders to rethink their networking strategies and team skills for:

- Network infrastructure, including hardware, software and associated support services

- Networking services, including network infrastructure and transport services operations and life cycle management

To guide this process, the strategic roadmap in Figure 1 will identify the key enabling network services and infrastructure components, as well as procurement and operational best practices to manage and drive network transformation.

Figure 1: Strategic Roadmap Overview for Enterprise Networking



Source: Gartner
818377_C

Future State

In the future, enterprise networks will be increasingly automated, AI-assisted and more tightly integrated with security across LAN, data center and WAN domains. This future-state network roadmap is a vision of how the strategy for enterprise WAN, campus and data center networks will evolve to meet organizations' changing business objectives. Meanwhile, this strategy will address budget realities, existing infrastructure, network consumption needs and legacy organizational culture. The biggest difference from the current state of enterprise networking will be described in the following sections.

Network Operations Will Be Digitally Augmented

Nearly all network vendors across LAN, WAN and data center environments will deliver AI-enabled/GenAI-enabled capabilities within their existing network management suites. These AI-enabled/GenAI-enabled AI networking assistants use natural language conversations to dynamically interact with network teams. They will help network teams navigate and interact with vendor documentation, initial design and new build-out configuration in a more simplified and automated fashion.

They also will increasingly provide troubleshooting assistance. For example, a network technician can ask the AI networking assistant to display the path between a user and a specific server. The assistant will then provide that mapping as a meaningful, useful output, rather than requiring the technician to run traceroute queries on endpoints. This will not only improve initial provisioning, but also support reactive troubleshooting.

Further, automation technology will increasingly take over networking tasks such as configuration and incident detection. In campus environments, this also will extend to issue resolution, as enterprises gain more trust in AI-powered remediation capabilities. This will lead to faster resolution of service issues. AI/machine learning (ML) capabilities built into WAN and LAN offerings will increasingly track compliance with service-level agreement (SLA) commitments.

This augmentation encompasses technologies such as digital twins, which creates a dynamic virtual representation of a network to safely apply changes and predict their impacts. AI and GenAI also will augment other products such as digital experience monitoring (DEM) tools, resulting in more consistent applications performance for all end users.

Overall, network automation levels will improve from the current state, where most enterprises have automated less than 50% of their Day 0 and Day 1 network activities. There is reason for optimism, given recent growth (see Market Guide for Network Automation Platforms).

These network automation levels will be driven by the increasing automation being embedded into infrastructure. This will include SASE, data center fabrics, campus fabrics and the deployment of more workloads into the edge and public clouds and/or the adoption of infrastructure as code (IaC) principles.

In addition, organizations will increasingly turn to AI-powered NetDevOps to make network upgrades more efficient and reliable. As the name implies, NetDevOps applies DevOps and/or continuous integration/continuous deployment (CI/CD) practices to networking activities. This requires an automated pipeline that includes staging, prevalidation/postvalidation and the testing of networking activities such as provisioning. NetDevOps can improve agility, reduce toil and increase reliability. It is particularly valuable for organizations implementing IaC for other portions of their infrastructure because the network is often a bottleneck.

SASE Will Be Standard

In this future state, self-managed or managed SASE — either single-vendor or dual-vendor with tightly integrated components from two partners — will be the preferred technology to securely and uniformly connect remote and branch users to applications.

Capitalizing on SASE nodes embedded in core WAN service offerings, a subset of SASE vendors will offer private, middle-mile backbone transport services. These services offer enhanced networking performance compared with standard WAN options that rely on congested public internet routes. The customer will then secure access circuits separately to complete endpoint connections.

Similar to WAN transport, SASE providers also will add direct cloud peering capabilities to their offerings to support efficient cloud traffic flows. Such additional WAN backbone and cloud connectivity features will benefit organizations for two reasons:

- Integrated WAN transport efficiencies and cloud connectivity support will improve overall network and applications performance.
- The packaging of these elements can simplify procurement, planning and deployment.

Compute Resources Are More Distributed

In the enterprise network of the future, the ongoing de-emphasis on location for data center operations will accelerate. Compute resources will be distributed more broadly across company-owned data centers, colocation facilities, cloud hyperscale environments and the edge locations. This will require consistent, high-quality connectivity linking edge locations and on-premises, colocation and cloud points of presence (POPs). Further, workloads can move more flexibly between these environments as enterprises evolve their applications strategy from on-premises-centric to more cloud-native and distributed edge environments.

Meanwhile, the evolution of AI will influence data center operations. As enterprises adopt AI, the required support training models that rely more on graphic processing units (GPUs) than central processing units (CPUs) will find a home in data centers. AI technology in the data center requires 400 Gbps and greater switches to connect GPUs without packet loss.

While InfiniBand has been the early preferred technology to meet this need, we predict AI Ethernet fabric technology will increasingly be used in AI-centric data center environments, taking advantage of Ethernet's larger vendor ecosystem. At the same time, data center support teams in turn will be trained to support this AI-centric network infrastructure.

Infrastructure Costs Are More Predictable and Aligned With Usage

Enterprises in the future state will have options beyond traditional upfront purchase and flat-rate service (and support) pricing. This will be driven in part by established hybrid work policies where employees split time between the office and remote locations, eliminating the need to maintain fixed-usage connectivity at many corporate facilities. Meanwhile, enterprises will have access to better network analytics data derived from automation-enhanced technologies such as SASE. With the change in connectivity needs and better analytics data, enterprises will increasingly turn to subscription and consumption options that are better aligned with functionality and usage.

In campus networking, we see emerging demand and supply of true NaaS offerings whereby the pricing is based on square footage and number of users (see Note 1). In these scenarios, absent future staff or applications increases at a location, this utility pricing model can offer cost savings compared to fixed-rate connectivity, which is usually based on the maximum network usage estimates. Longer term, we expect such offers will evolve and become a more viable enterprise option.

Sustainability Will Play an Important Role in Network Investments

Chronic and sometimes acute local energy shortages will result in rising energy costs across all parts of organizations' operations, including enterprise networking. Furthermore, governments, particularly in Europe, are expected to establish or expand regulatory requirements for sustainable, energy-efficient business operations to address systemic regional and national power shortages during the next few years. In response, energy efficiency initiatives will become important to curb operating costs and sustain growth in certain geographies, including Europe and parts of Asia/Pacific.

Although enterprise IT energy costs will be affected by power-hungry data center servers and environmental temperature control, I&O leaders will also focus on power-efficient infrastructures. These will include data center switches, SD-WAN appliances, LAN switches and wireless LAN access points to curb operational expenses.

In response, enterprises will source networking equipment with lower power consumption ratings, as well as reducing less-efficient copper cabling in structured wiring. They also will require that equipment be compatible with energy-efficient Ethernet (802.3az) for wired connectivity or intelligent power over Ethernet (PoE) to reduce network switch power consumption during low-traffic periods.

Circular economy mandates will also have an impact on network equipment procurement. The European Union Corporate Sustainability Reporting Directive, which was adopted in early 2023, requires more than 50,000 companies to comply with new environmental, social and governance (ESG) reporting requirements by 2028. Meanwhile, regulations in France require a percentage of recycled or refurbished components in hardware products and tighten regulations on the disposal of equipment during infrastructure refresh cycles, and other countries may mandate similar requirements. In response, enterprises will incorporate recyclability and modularity requirements into their hardware RFPs.

Wi-Fi and Private 5G Drive Campus Infrastructure

Campus networking decisions will be driven by software functionality, rather than hardware capabilities. With use cases that expand beyond IT-centric laptops, tablets and phones, to include Internet of Things (IoT) devices and operating technology (OT) systems, the number of wireless devices accessing the LAN network will increase significantly.

Enterprises will rely on wireless LAN (WLAN) infrastructure that can integrate private cellular, public cellular (including 5G) and Wi-Fi technologies. They also will increasingly adopt Wi-Fi 7 (802.11be) to provide better coverage, lower latency, increased over-the-air capacity, support for 6 GHz bands and reduced interference. Wi-Fi 7 products will offer theoretical performance at speeds as high as 40 Gbps, along with integrated time-sensitive networking (TSN) that will improve latency and reduce traffic congestion.

5G private mobile network (PMN) technology will offer connections with larger coverage areas and better density, improved performance, resilience and supporting low latency. This will support a wider range of use cases in the manufacturing and healthcare verticals. Wireless bandwidth capacity for private 5G will shift focus from high-band millimeter wave (above 24 GHz) to midband frequency blocks, such as 3.7 GHz.

Zero-Trust Concepts Rule Network Designs

Currently, we see interest in applying zero-trust concepts to networking, often driven by IT security/chief information security officer (CISO) teams mandating zero-trust strategies. In the future network state, zero-trust networking (ZTN) will become a pervasive implemented technology. ZTN applies zero-trust concepts to network infrastructure. Specifically, this means user and/or device access to the network is based on identity and context and is then continuously reassessed in real time, based on calculated risk.

A full ZTN infrastructure meets the following three requirements:

- Access to the network is granted only after identity is authenticated and authorized.
- Network access is restricted only to necessary resources.
- Network access is continuously adjusted in near real time, based on risk derived from identity and context.

Most enterprises are early in their ZTN journeys. Gartner estimates 63% of organizations have at least partially adopted ZTN, but only 16% have implemented full ZTN (meeting all three requirements described above) in more than 75% of their network infrastructure. [1] In particular, the third requirement is rare in enterprise network deployments. However, driven by security mandates, budgets and improving sets of technology platforms, including security service edge (SSE) and SASE, we expect this number to triple during the next three years.

WAN Services Are Flexible and Primarily Internet-Based

In the future enterprise network, increased reliance on cloud applications and workloads will drive further evolution of SD-WAN to support better traffic flow between enterprise locations and cloud service providers (CSPs). Importantly, stand-alone SD-WAN will give way to secure SD-WAN that incorporates a NGFW, often as part of a larger SASE adoption strategy.

As they adopt secure SD-WAN and cloud applications, enterprises will continue to transition away from traditional, private IP multiprotocol label switching (MPLS) transport circuits to internet-based alternatives, including dedicated internet access, wireline broadband and wireless. Although some organizations will rely entirely on internet transport for their core WAN design, others will still use private MPLS and Ethernet in specific use cases. Hence, MPLS will not disappear from many WANs in the next five years but rather be used selectively for routing high-sensitivity applications traffic within the private company intranet or in specific geographies, such as China, to address government internet restrictions.

Cloud connectivity also will play an increased role in enterprise network design. Enterprises will increasingly turn to MCNS, which enables consistent and secure network design, deployment and operation in multiple network cloud environments. To support increased cloud applications traffic, network service providers (NSPs) will enhance internet services to optimize routing, improve performance and support stronger SLAs.

Enterprise NSPs also will offer more sophisticated managed network services. This includes upgraded bandwidth on demand (BOD), expanded cloud management and increased security offerings and updated customer portals.

Current State

Enterprise Networking Is Primarily Manual

Gartner estimates that most enterprise networks are managed via manual activities. As of mid-2024, only about 20% of organizations have automated at least 50% of their network activities, while 50% have automated less than 25% of network activities. This is an increase from 2021 levels, in which 10% of organizations had automated at least 50% of their network activities, and 72% had automated less than 25%.

Network, Security and Cloud Teams Are Loosely Integrated

In many enterprises, the traditional network, security and cloud organizational silos still exist. As a result, network investment decisions are not always aligned with network security priorities, and vice versa. Meanwhile, cloud development teams are not always consulted by network teams that are assessing cloud networking infrastructure or services investments. Therefore, network investments can be misaligned with the organization's security and cloud applications needs.

Sustainability Has Limited Impact on Infrastructure Investments

Although they vary by region and country, overall energy costs remain elevated worldwide, driven by ongoing surges in oil and natural gas prices that were influenced by geopolitical and market factors. Estimates are that, by 2026, huge electricity price increases will be needed to fund decarbonization initiatives.

Energy pricing is of particular concern in the data center due to growth in compute resources to support AI technologies. AI compute resources consume up to 10 times the energy of traditional data center servers. This infrastructure could increase data center power consumption by 165%, according to a Goldman Sachs estimate. [2] As of mid-2024, governments are increasingly establishing sustainability mandates, including the EU's Corporate Sustainability Reporting Directive (CSRD). Faced with energy shortages, governments are likely to enact laws requiring energy-efficient, sustainable business IT operations. This will force enterprises to retrofit their network infrastructure by specific deadlines (see The Impact of CSRD on Enterprise Sustainability Strategies).

And yet, based on Gartner inquiry, focus on power efficiency and sustainability, including use of recycled components or refurbished equipment, is in data center environments and are not significant factors for enterprise network teams when evaluating network infrastructure purchases. This can result in higher operating costs for networking equipment.

Compute Resources Are in Data Centers and the Public Cloud

Enterprise applications are primarily hosted in corporate data centers (including colocation facilities) or in public cloud environments. While enterprises use application delivery controllers (ADCs) or load balancers to manage applications traffic on-premises or in the cloud, these environments must be maintained separately. As a result, there is limited ability to shift resources between environments.

Meanwhile, AI compute resources while growing are mostly in cloud environments and constitute a small percentage of overall workloads in corporate data centers or colocation facilities.

Campus Network Investments Are Driven by Hardware Refresh

The enterprise LAN environment is hardware-centric and includes a mix of wired and wireless connectivity that can be difficult to modify to meet changing user connectivity needs. Wireless LAN and campus networks rely primarily on unlicensed spectrum in the 2.4 GHz, 5 GHz and 6 GHz bands, which can quickly become congested with increased user traffic.

Organizations Do Not Prioritize New Technology Skills Acquisition

Organizations' technical enrichment programs often focus on certifications to support current network operations. Rarely do they offer enrichment programs that expose network teams to new technologies, such as software development processes, automation, AI/ML and GenAI. Similarly, new hires are primarily selected for their traditional technical skills to support current operations and are rarely required to have new technology training or skills.

WAN Infrastructure and Services Are Inflexible

Enterprises tend to purchase WAN connectivity services and infrastructure that lacks flexibility to adapt to organizations' changing needs. Wireline WAN connectivity services usually include unlimited data usage at set port data speeds and fixed or burst access data speeds. Wireless data services offer best-effort data speeds, but unlike wireline services, usage is usually capped or throttled and SLAs are virtually nonexistent.

WAN service contracts are frequently renewed with no competitive RFP, so the incumbent carrier has no incentive to offer market-competitive pricing.

Most enterprises also purchase network infrastructure equipment, including SD-WAN appliances and on-premises firewalls outright, resulting in high upfront costs. They then face additional expenses when this equipment reaches its end of life and must be replaced.

Network providers are offering NaaS alternatives that do not require high upfront investment, but these offers have seen limited adoption among enterprises. Key challenges include the fact that NaaS offers vary dramatically in features and availability, and they often prove more expensive long-term compared to traditional offers.

Remote Access and Corporate Access Are Secured Separately

Although many enterprises have shifted back to in-office work, they have maintained remote work options, albeit on a more limited basis. However, remote and in-office user access is secured separately. While many enterprises have transitioned from products based on legacy virtual private network (VPN) to securely manage remote users, corporate offices still often rely on traditional network access control (NAC) security. This creates uneven security policy control and inconsistent user experience for workers who split their time between remote and in-office work.

Gap Analysis and Interdependencies

Enterprise networking can better meet organizational business needs by becoming more integrated, cross-platform-aware and responsive. To do so, several gaps must be closed:

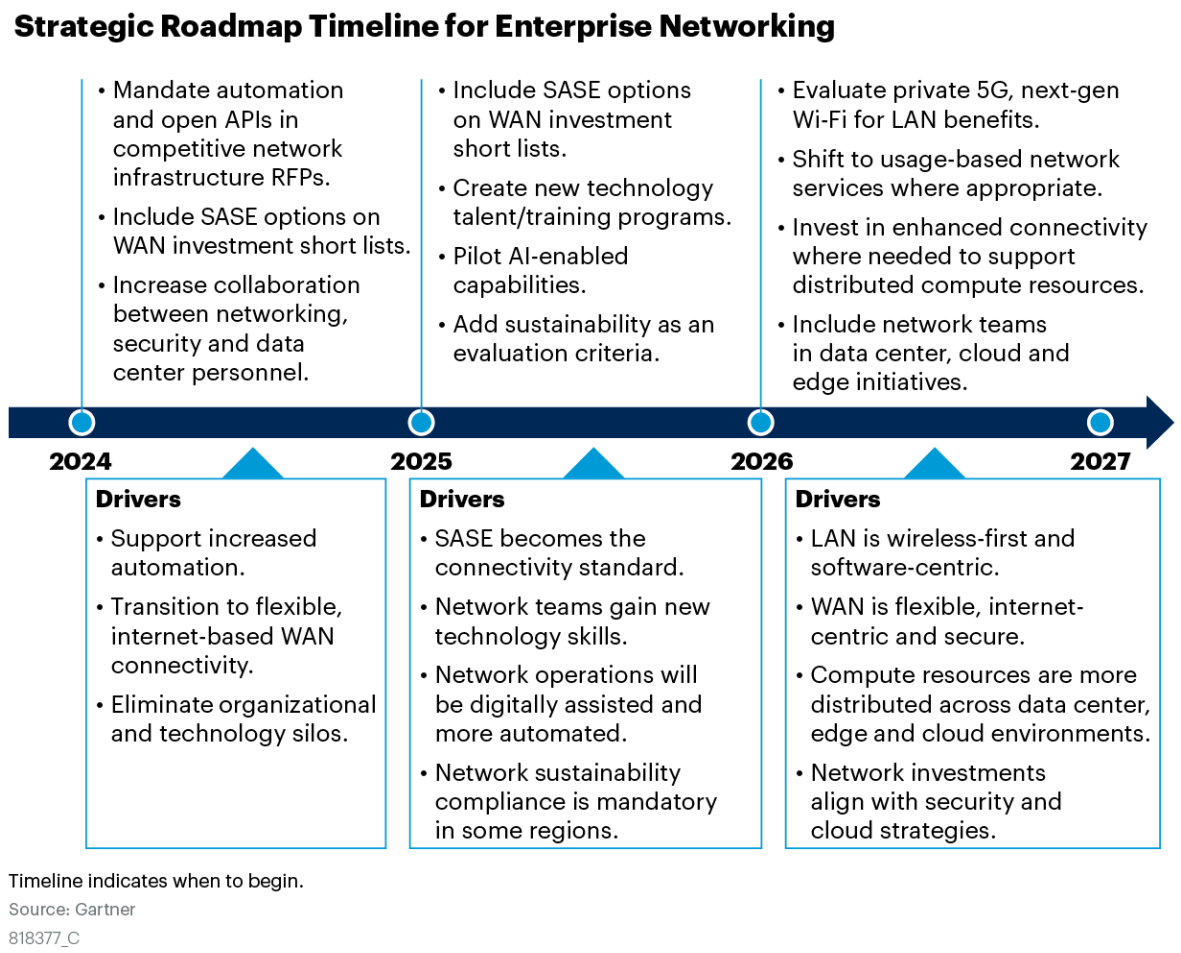
- **Limited cross-vendor, cross-functional automation tools:** Despite having plenty of automation tools, there is little integration or ability to extend beyond individual vendor products or automation functions. Tool vendors also do not effectively market the value of their offerings.
- **Limited AI/ML and GenAI knowledge:** AI/ML technology development is in an adolescent stage, and most I&O organizations have limited knowledge or experience applying it to their operations.
- **Enterprise network strategy doesn't align with security and cloud needs:** Enterprises' procurement of services and infrastructure across the WAN, cloud and security domains is rarely coordinated, despite cross-functional interdependencies.
- **Organization structures limit coordination between network, security and cloud teams:** Network, security and cloud teams operate independently, with limited cross-team coordination.
- **Enterprise network investment focuses on refresh and/or immediate needs:** Enterprise network investments target individual infrastructure or service upgrades to meet an acute, immediate need, rather than multifunction or flexible usage offerings that would provide greater long-term organizational benefits.
- **Siloed on-premises and cloud compute resources:** Enterprises must maintain legacy applications hosted on-premises while separately managing newer applications hosted in cloud environments.

- **Limited visibility across network, security and cloud environments:** Most organizations lack the ability to monitor the status and performance of network, security and cloud environments in sufficient and granular detail.
- **LAN is hardware-dependent, mixing wired and wireless components:** To provide greater connection flexibility and improved management, LAN and campus network functions need to be "wireless-first" to support greater device portability. They also must be managed and controlled by AI-powered software that offers better visibility and can be more easily modified than hardware, the latter of which will increasingly become commoditized.
- **Inconsistent user experience across all devices and locations:** When users move between devices and locations, there is no way to guarantee consistent applications performance or access to corporate digital assets.
- **Rigid WAN services and infrastructure with unpredictable price fluctuations:** WAN network services and infrastructure investments are often made without competitive RFPs, and they lack the ability to make capacity, bandwidth and performance adjustments.
- **Lack of clear sustainability guidelines and metrics:** Enterprise network teams are not given sustainability goals, so selecting services and infrastructure that are energy-efficient or sustainable are nice, but not necessary factors.

Migration Plan

Based on the gap analysis, we propose the following migration plan for enterprise networking. This will require multiple steps, prioritized by near-term, midterm and longer-term actions (see Figure 2).

Figure 2: Strategic Roadmap Timeline for Enterprise Networking



Timeline indicates when to begin.

Source: Gartner

818377_C

Gartner

Higher Priority

At every network infrastructure refresh, mandate automation and open APIs as evaluation criteria:

- For automation, start small and iterate, focusing first on simpler, nonchange workflows, such as backup configurations or routing table updates databases.
- Build automation progressively, automating such activities as network status verification and auto-populating trouble tickets with event data, including error messages or time of occurrence.
- At every network equipment and services refresh, prioritize automation functionality when selecting vendors. This includes proving common activities are readily automated, as well as mandating open published RESTful APIs.

Pilot emerging AI-enabled capabilities, and add sustainability as an evaluation criterion:

- Test AI/ML technology to verify its value-added benefits, as well as ease of integration with existing network IT service management (ITSM) operations.
- Start small and iterate with GenAI solutions by testing functionality in a proof of concept (POC) to validate capabilities and verify recommendations before moving to production.
- To support AI and GenAI clusters in the data center, build out a dedicated network to connect GPUs. Favor Ethernet over InfinBand for GPU clusters up to 2,000 GPUs.
- Mandate sustainability requirements for networking equipment. This includes power usage limits and power management features such as intelligent PoE, with a focus on operational expenditure (opex) savings benefits. Require infrastructure vendors to provide sustainability certification that aligns with organizational objectives.

Include SASE offerings on the shortlist when making SD-WAN, SWG, NGFW, ZTNA and CASB investment decisions:

- Prioritize vendors' SASE offerings over individual SD-WAN or security products and assess whether they align with the organization's long-term network technology strategy.
- Favor vendors with unified SASE offerings that also meet performance requirements for individual networking or security components.

Medium Priority

Drive increased collaboration and integration between networking, data center and security teams, particularly when planning or deploying ZTN technologies:

- Require security and network teams to participate in the RFP/RFI process for SSE and SASE investments.
- Establish configuration criteria for ZTNA and microsegmentation technologies that reflect networking and security performance priorities.
- Foster and encourage periodic collaboration meetings between security, data center and network teams to review performance analytics, technology migration updates, ongoing service issues and new technology adoption plans.

Cultivate skills in new and existing staff by creating a talent program in coordination with HR:

- Invest in personnel.
- Shift hiring and training focus toward specific automation competencies such as Python coding and AI capabilities such as large language models.

Set aside 10% of I&O staff time per week for new technology training and testing, including pilots of automation tools. These evaluations must focus on delivering business value, such as improved efficiency and management or cost reduction.

- Change network team performance evaluations to include business-oriented goals, such as faster service delivery, improved network availability and response and reduced operating expenses. This will motivate team members to explore and use automation tools.

Lower Priority

Support core and edge compute resources by investing in enhanced connectivity products and services:

- To support compute resources in multicloud environments, strategically deploy cloud onramp solutions such as cloud hubs and software-defined cloud interconnect (SDCI).
- Selectively adopt MCNS where advanced networking features and/or a consistent network and security operations model across multiple public cloud environments is required.
- To serve compute resources across all locations, require strong connection SLAs, including high availability with low latency, packet loss and jitter.

To improve enterprise LAN reliability, scale and performance, evaluate private 5G and next-generation Wi-Fi technologies:

- Focus private 5G investments on industrial, manufacturing and healthcare use cases when IoT capabilities and data security are a priority.

- Focus Wi-Fi investment options on use cases for which traditional device connectivity (e.g., laptop, mobile phone, tablet) is the priority.
- For both technologies, identify spectrum availability at a given location to determine whether the capacity will support the use case.

Evidence

[1] **2023 Gartner State of Zero-Trust Strategy Adoption Survey.** This survey was conducted to understand the current state of zero-trust strategy adoption across the industry and to reduce confusion about the scope and maturity of zero-trust strategies across industries and verticals worldwide. The survey was conducted online from 23 October to 24 November 2023 among 303 respondents from North America (n = 134 in the U.S. and Canada), EMEA (n = 98 in France, Germany and the U.K.) and Asia/Pacific (n = 71 in Australia, India, the Philippines and Singapore). Respondents' organizations had $500 million or more in 2022 enterprisewide annual revenue, and 2,500 or more employees. Respondents were qualified if their organization had already implemented (fully or partially) or was planning to implement a zero-trust strategy. Respondents were also required to have visibility into the strategies or investment decisions related to zero-trust strategy. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[2] Bullish expectations for US electricity are attracting new power traders, Goldman Sachs.

Note 1: NaaS

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 (see Hype Cycle for CSP Networks Infrastructure, 2024).

Document Revision History

Strategic Roadmap for Enterprise Networking - 11 October 2023

Recommended by the Authors

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

Innovation Insight: AI Networking Has the Potential to Revolutionize Network Operations

Where Do I Start With SASE Evaluations: SD-WAN, SSE, Single-Vendor SASE, or Managed SASE?

Adopt a Software-First Approach When Building a NextGen Campus Network

Unlock the Business Benefits of Sustainable IT Infrastructure

Hype Cycle for Enterprise Networking, 2024

Quick Answer: Do I Still Need MPLS?

Prepare for Generative AI in Network Operations