Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure

6 March 2024 - ID G00785075 - 41 min read

By Tim Zimmerman, Christian Canales, and 2 more

Automation, security and migration strategies are the primary drivers for infrastructure strategies as the market continues to move away from hardware. I&O leaders must use this research to deliver wired and wireless infrastructure to their campus, branch and remote-office environments.

Strategic Planning Assumption

Through at least 2026, over 70% of wireless local-area network (WLAN) deployments will lack a tangible use case for organizations to deploy Wi-Fi 7, as most business applications do not require the enhanced capabilities of the new standard.

By 2027, 70% of enterprises refreshing and/or expanding their WLAN will upgrade to Wi-Fi 7, due to future proofing aspirations and vendor push combined with aggressive product marketing.

Market Definition/Description

This document was revised on 11 March 2024. The document you are viewing is the corrected version. For more information, see the ***Corrections*** page on gartner.com.

Gartner defines the enterprise wired and wireless LAN infrastructure market as wired and wireless networking hardware and the related network software. Related components of the solution include enterprise switches, access points and the requisite tools to secure,

manage, test and optimize the network infrastructure that provides connectivity for users, devices and applications that may reside on the network or on other networks.

Enterprises in all vertical markets use enterprise wired and wireless networks to connect and transport data for fixed and end-user devices to applications that may be local or remote to the physical end user. In addition to physical connectivity, these solutions provide the following capabilities in diverse markets, including the ability to:

- Discover, identify, secure, manage and segment Internet of Things (IoT)/operational technology (OT) devices
- Support, test and maintain network infrastructure components
- Provide a resilience infrastructure
- Secure the network infrastructure
- Provide scalability and flexibility for management and control plane communication processes
- Provide no-touch/low-touch Day 2 environment

Must-Have Capabilities

The must-have capabilities of this market include:

- IEEE 802.11 Wi-Fi-certified access points that support 2.4GHz, 5GHz and 6GHz.
- Ethernet network switches suitable for deployment at the network access, distribution and core network layers.
- Wi-Fi process control and management plane functionality placed on a physical appliance, virtual machine, which can be located at the edge, in the data center or cloud-based.
- A network management application.
- Secured and managed third-party devices on the network.
- Security for device authentication and authorization, such as 802.1X.
- Security policy enforcement application.

- A wired and wireless intrusion detection.
- Telemetry for troubleshooting and optimization of the network.

Standard Capabilities

The standard capabilities for this market include:

- Access points that support indoor and outdoor environments with optional external antennas and that support Wi-Fi 5, 6 and 6E certifications.
- The ability to provide Power over Ethernet (PoE) to all components.
- A guest access portal that allows for guests to be directed outside of the firewall for internet connectivity.
- The ability to view network analytics for the end users and applications they use on their devices.
- A network fabric that can create dedicated channels of communication across the end-user connection to its destination that are governed by a policy. The fabric should be able to extend across competitive equipment (i.e., access points and switches).
- Network monitoring, such as user and entity behavior analytics (UEBA), that can be integrated with the network security policy to take that appropriate action.
- The ability to collect and export telemetry data that allow AI- and ML-enabled network assurance tools to troubleshoot and optimize the network.
- The ability to detect and report configuration drift.
- The ability to discover, identify, secure and manage nonuser devices (IoT/OT).
- Application visibility and/or performance management.
- The ability to manage through exported API, Simple Network Management Protocol (SNMP) and other methods of legacy competitive access points and switches.

It is important to note that this research is not inclusive of wired and wireless networking infrastructure devices that are primarily used to support adjacent markets, such as point-to-point WAN offerings.

Optional Capabilities

Optional capabilities for this market include:

- Indoor location services
- Natural language troubleshooting interface
- Consumption-based pricing models (NaaS)
- Ability to collect and use telemetry data from competitive access points and switches
- Integration with ITSM applications, including ticketing
- Private/public 5G integration and offloading
- The ability to apply full zero trust principles to all connected users and devices

Magic Quadrant

Figure 1: Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure

Vendor Strengths and Cautions

ALE

Alcatel-Lucent Enterprise (ALE) is a Niche Player in this Magic Quadrant. Its OmniSwitch switches, OmniAccess Stellar wireless access points and OmniVista management products broadly address the enterprise network market. ALE's portfolio includes on-premises and cloud-based management options with network fabric segmentation and universal network policy for IT and IoT provisioning. The company prioritizes the midsize enterprise (MSE) business market segment, and its clients are primarily in the government, healthcare and transportation verticals. Gartner expects ALE to continue investing organically in software

capabilities for network security, visibility and assurance, with inorganic investment in vendor technology partnerships to continue filling out solutions for the portfolio offering.

Strengths

- **Campus networking fabric:** Clients in ALE's key target verticals (government, healthcare, transportation and education) looking for simplified management and streamlined automation will benefit from ALE's fabric architecture and industry-specific expertise.
- **Universal network policy — UPAM/NAC:** ALE's Intelligent Fabric and OmniVista management solutions include onboarding, segmentation and secure policy provisioning across the wired and wireless network edge for customers with IT, IoT and OT requirements.
- **Technology partnerships and solutions**: ALE has strong partnerships for SASE solutions, SSE cloud security solutions, and video management systems to provide customers with extensible systems.

Cautions

- **Lack of parity between cloud and on-premises offerings:** OmniVista 2500 Network Manager System and OmniVista Cirrus do not ship with feature parity. ALE plans continued investment in development, however, customers must ensure that the required functionality is available in their preferred deployment model today..
- **Limited AIOps functionality:** ALE is trailing leaders in this research for advanced visibility and assurance functions. The OmniVista Network Advisor, and separate Rainbow collaboration platform, have limited use-case outputs and autoremediation. Customers are advised to test functionality as part of a proof of concept before buying.
- **NaaS product offering**: ALE offers a buying model for customers that includes some capex in the initial purchase. This product offering doesn't not meet Gartner's definition for NaaS; however, it may appeal to buyers that seek some reduction in initial capital outlay.

Allied Telesis

Allied Telesis is a Niche Player in this Magic Quadrant. The company has a broad switching portfolio led by the x9x0 series switches and a WLAN offering that can address most use cases, but is currently missing a Wi-Fi 6E model. The portfolio is governed by Vista Manager

EX, the Autonomous Management Framework Plus (AMF Plus), the AMF-Security Controller and the Autonomous Wave Control (AWC) wireless controller. Allied Telesis focuses on customers in the healthcare, education, government and healthcare sectors, and its operations are geographically diverse. Gartner expects Allied Telesis to start adding AI/ML-based analytics to its network management solution in 2024, to ease off network operations with features such as guided troubleshooting.

Strengths

- **Enterprise-grade network management features:** AMF Plus and the AMF Security Controller are optional add-ons to Vista Manager EX, resulting in a breadth of features that include quality of service (QoS) traffic prioritization, endpoint policy enforcement and malware protection.
- **Multivendor management:** AMF Plus provides support for third-party network devices, simplifying the administration of wired and wireless infrastructure.
- **Unified operating system:** Allied Telesis has a single OS, AlliedWare Plus, which eases management and configuration capabilities across all products, including routers and firewalls.

Cautions

- **Lack of network fabric:** Allied Telesis lacks a native network fabric, which limits segmentation and policy enforcement and may require a partner product.
- **Lack of AIOps features:** Allied Telesis does not yet have AI/ML-based analytics for network assurance services, such as root cause analysis of issues arising from baselined application performance, guided troubleshooting and a natural language interface.
- **Limited market visibility:** Allied Telesis has limited wired and wireless LAN market visibility among customers and prospects outside of Japan, based on end-user Gartner interactions, gartner.com searches and social media conversations.

Arista Networks

Arista Networks is a Visionary in this Magic Quadrant. The company addresses the enterprise networking market with its 700 series leaf switches and 7000 series enterprise spine switches; Cognitive Wi-Fi access points that include Wi-Fi 6E; and its CloudVision management platform. Most of Arista's customers are located in North America and are in

the financial, healthcare and higher education sectors. Gartner expects Arista to continue to invest in its CloudVision integrated security and AI and ML capabilities, with functionality further extending to the data center. This architecture expansion will aim to deliver proactive network performance monitoring, application visibility and policy enforcement across the campus, WAN and data center.

Strengths

- **Network management tools that simplify operations:** Arista's CloudVision platform is unified for both campus and data center management; it also supports digital twin capabilities for testing and validation of configuration/connectivity changes to the campus network.
- **Differentiated network security strategy:** Arista is one of the few vendors in this research with a NDR offering for advanced threat detection and incident response use cases. The launch of CloudVision Arista Guardian for Network Identity (AGNI) in 2Q23, a NAC product, adds risk and behavior assessment of endpoints.
- **Advanced AI and ML capabilities:** Arista's CloudVision AIOps includes the Autonomous Virtual Assist (AVA) platform for natural language processing, in addition to automated trouble ticketing, incident severity classification and issue remediation, and predictive analytics.

Cautions

- **Limited exposure outside its data center customer base:** Arista's strategy targets its data center customer base to grow its campus networking business, limiting market visibility, especially in the midmarket.
- **Price premiums:** Arista's campus switching portfolio, predominantly targeted at large enterprises, has a price premium. Measured in the average revenue per port, it is among the highest in the industry.
- **Limited exposure outside North America:** This region accounted for more than 60% of Arista's wired and wireless LAN revenue in 2023. Organizations considering Arista should verify product and service availability in their geography.

Cambium Networks

Cambium Networks is a Niche Player in this Magic Quadrant. Cambium's ONE Network solution addresses the enterprise market with wired switches (via its cnMatrix product line) and access points with software-defined radios. cnMaestro X manages the entire Cambium product family. Cambium focuses on customers in the hospitality, education, government and healthcare sectors, and its operations are geographically diverse. Gartner expects Cambium to enhance its ePSK technology for simplified device onboarding, including IoT endpoints, and to continue to invest in its AIOps capabilities.

Strengths

- **Broadened network management capabilities:** Cambium's recently introduced Network Service Edge (NSE) solution extends cnMaestro's network management to include SD-WAN, network security and outdoor fixed wireless.
- **Cambium's "assists" feature:** This application provides a security auditing capability that continually scans the network, and reports and provides resolution of misconfigured products, as well as identification of the potential risk.
- **Flexible software-defined radios:** The software-defined radios in Cambium's access points allow for enterprises to change the radio frequencies (2.4 GHz, 5 GHz or 6 GHz). Up to five radios can be configured for high-density requirements or for the need to simultaneously support different WLAN installations.

Cautions

- **Fragmented IoT segmentation capabilities:** NSE supports segmentation of wired IoT endpoints, while cnMaestro X leverages Cambium's ePSK technology for wireless IoT onboarding. Additionally, Cambium does not have a campus fabric, limiting its ability to segment devices as a unified construct to the access layer, with no support of VXLAN.
- **Limited enterprise vertical exposure:** Cambium has limited visibility in the enterprise space outside the hospitality, education and healthcare verticals. Cambium's exposure at deployment scales above MSE is also very limited.
- **Lack of modular chassis switch:** This portfolio gap prevents Cambium from adequately addressing high-density access or high-speed core/distribution use cases, in which a common high-speed backplane and redundant management and power supplies in a single chassis are highly desirable.

Cisco

Cisco is a Leader in this Magic Quadrant. Its Catalyst and Meraki products deliver a broad portfolio of wired and wireless access products, network applications and services. Its operations are geographically diversified, and Cisco services clients in all markets, from small and midsize businesses (SMBs) to large enterprises. Cisco's vision for Networking Cloud is to unify the on-premises catalyst hardware with the simplicity of the cloud-based Meraki management to deliver flexible options for its customers. Gartner expects Cisco will continue to invest in its on-premises management (DNA Center, now Catalyst Center), NAC (Identity Services Engine [ISE]), and SDA Fabric solutions as they strive to achieve use-case parity and experience consistency across the two portfolios.

Strengths

- **Portfolio breadth:** The scope of Cisco's wired and wireless hardware and software product portfolio addresses use cases across market verticals, business organizations of all sizes and network deployment scenarios of any type.
- **Advanced network assurance:** Cisco's integration of ThousandEyes throughout the portfolio, along with its deep relationship with device vendors (Apple, Intel, Samsung), is delivering real-world insights for IT and security operational use cases.
- **Geographic reach:** Cisco's extensive global reach within direct and indirect sales channels positions it as a campus networking vendor capable of delivering and supporting effective solutions to clients worldwide.

Cautions

- **Rising prices:** Cisco customers cite high prices to obtain, refresh and maintain Cisco wired and wireless infrastructure.
- **On-premises and cloud lack parity:** Cisco buyers must make a decision on the management solution they intend to deploy — Meraki in the cloud, or Catalyst Center on-premises. Differences in solutions create a buying gap for key generative AI, AIOps and security analytics features.
- **Security portfolio decision:** Cisco's vast security portfolio creates buyer confusion, with an increase in the total cost of ownership (TCO), as customers choose from optional software components such as XDR, ISE, Umbrella and Secure Network Analytics.

CommScope (RUCKUS)

RUCKUS Networks, owned by CommScope, is a Visionary in this Magic Quadrant. The company addresses the market with its RUCKUS brand ICX wired switches, R series wireless access points and RUCKUS One — its network management and AIOps platform. RUCKUS operates globally and focuses primarily on the federal, state and local government segments of the enterprise network market, as well as the education segment. Gartner expects that RUCKUS will continue to invest in the AIOps capabilities of its RUCKUS One platform, its network security and segmentation capabilities, and in expanding its integration with WAN edge capabilities.

Strengths

- **Network management with AIOps features:** The RUCKUS One platform has several strong capabilities, including network assurance services, profiling and policy enforcement of endpoints (including IoT), and digital twin features for testing and validation of Wi-Fi upgrades.
- **Detailed root cause analysis tools:** RUCKUS AI, the AI engine of RUCKUS One, offers detailed analysis across the wired and wireless network. Users can see the root cause assessment data and apply resolution suggestions.
- **Security strategy:** RUCKUS One comes with integrated NAC functionality at no extra cost, and the RUCKUS WAN Gateway provides network services such as microsegmentation, DNS and firewalling to switches and WLAN access points.

Cautions

- **Limited experience in large complex network requirements:** RUCKUS has limited experience in large enterprise network environments, especially in complex core layer network deployments.
- **Digital twin functionality gaps:** RUCKUS One does not support the verification of switching network configurations in a virtual testing environment, since its digital twin capabilities are limited to wireless.
- **Lack of modular chassis switch:** This portfolio gap prevents RUCKUS from adequately addressing high-density access or high-speed core/distribution use cases, in which a common high-speed backplane and redundant management and power supplies in a single chassis are highly desirable.

Extreme Networks

Extreme Networks is a Leader in this Magic Quadrant. Extreme Network's Infinite Enterprise portfolio ties wired, wireless and SD-WAN products together into a single end-to-end solution underpinned by Extreme Fabric, a zero touch, automated network fabric. This fabric is managed by a unified management platform available in the cloud or on-premises. Extreme's operations are geographically diversified and the company services clients in all markets, from SMBs to large enterprises, with a specific focus on state and local government, education, healthcare, manufacturing, and retail. Gartner expects Extreme Networks to continue to invest in its ExtremeCloud IQ CoPilot AI capabilities, as well as cloud-based universal ZTNA, fabric innovation and digital twin initiatives.

Strengths

- **Zero touch network fabric:** Extreme Networks has continued investment in Extreme Fabric, its single secure end-to-end fabric technology. Zero touch provisioning and automation reduces the deployment burden for customers.
- **Universal licensing**: Extreme's universal licensing gives the customer a flexible licensing approach. Licenses are not tied to specific hardware and can be moved from one device to another, irrespective of device type. The licenses are tied to the network.
- **Third-party network management:** Multivendor integration streamlines deployment into brownfield environments. Configuration, firmware updates, backups, alarms and events can all be handled by ExtremeCloud IQ.

Cautions

- **Global reach challenges:** Extreme Networks has gaps in its presence in regions such as Asia and Latin America.
- **Pricing:** Extreme Networks' pricing for switches is higher compared to most vendors in this research, based on our market statistics that measure the average revenue per port (after discount).
- **No NaaS offering:** Extreme does not directly offer a consumption-based NaaS offering, with pricing delivered on a pay-for-use basis or as a subscription based on usage metrics.

Fortinet

Fortinet is a Leader in this Magic Quadrant. The Fortinet Security Fabric, unified by FortiOS, allows extremely tight integration between its wired and wireless products. Through its

proprietary FortiLink protocol, FortiAPs and FortiSwitches can become an extension of the FortiGate security appliance. Fortinet's operations are geographically diversified, and its clients range from MSEs to large enterprises across various sectors. Gartner expects Fortinet to continue to invest in its network AIOps capabilities, including incorporating enhanced third-party management and network performance monitoring. We also expect Fortinet to improve its threat detection capabilities through correlation and user and entity behavior analytics (UEBA) at the network level.

Strengths

- **Differentiated LAN offering with a strong security focus**: Fortinet delivers an architecture in which wired, wireless and security are integrated under a single unified operating system (FortiOS) and cloud management platform.
- **Dedicated AI operations module:** The FortiAIOps AI engine provides network assurance (event correlation and issue remediation) across security, wired and wireless by leveraging data feeds from the FortiGate portfolio.
- **Effective microbranch solution**: Fortinet has a well-thought-out solution for microbranch sites. The solution allows FortiAP to act as an endpoint for Unified SASE. Unified SASE, together with digital experience monitoring (DEM), provides converged access for a hybrid workforce.

Cautions

- **Lagging influence with security buyers:** Most of Fortinet's firewall customer base deploys switches and WLAN products from a competitor, since security and networking are commonly separate buyer centers. Fortinet's revenue market share in campus networking is almost 10 times smaller than that in the firewall market.
- **Multiple management interfaces**: Fortinet has several management options: FortiGate manager, FortiManager (on-premises and cloud), FortiLAN and FortiMonitor, which are used to manage the different deployment architectures. This can result in a confusing mix of management options.
- **Lack of modular chassis switch:** This portfolio gap prevents Fortinet from adequately addressing high-density access or high-speed core/distribution use cases, in which a common high-speed backplane and redundant management and power supplies in a single chassis are highly desirable.

HPE (Aruba)

Hewlett Packard Enterprise (HPE) (Aruba) is a Leader in this Magic Quadrant. The company offers a comprehensive approach to enterprise networking through the Aruba Edge Services Platform (ESP) of wired and wireless solutions. Aruba Central, available both on-premises and via the cloud, has received a welcomed UI refresh to the cloud platform, inclusive of most key capabilities, such as the NetConductor fabric orchestrator. Its operations are geographically diversified, and Aruba services clients in all markets, from SMB to large enterprise. Aruba has been aggressively expanding its NaaS offering through its channel, including new offerings that encompass the broader HPE GreenLake ecosystem. Gartner expects Aruba to continue investing in advanced networking solutions, while integrating its two recent acquisitions of Axis Security (SSE security cloud), and Athonet (private wireless core software) into a single management cloud system.

HPE announced its intention to acquire Juniper Networks on 9 January 2024. At the date of publication, HPE met the inclusion criteria for this Magic Quadrant, and both HPE and Juniper continue to operate as independent entities. Gartner will provide additional insight and research to clients as more detail becomes available.

Strengths

- **Campus fabric and security management:** Aruba ESP delivers an automated and secure wired and wireless fabric incorporating device onboarding, policy assignment and UEBA client monitoring that offers key capabilities to deploy a zero trust architecture.
- **Switching advancements:** Aruba has delivered two key features that separates its switching hardware from competitors: in-service software upgrades (ISSUs) for switch stacks, and Layer 7 application control on access ports.
- **Inclusive AI features:** Aruba Central's standard license includes key management functionality, such as AIOps, that provides significant value out of the box. Customers will benefit without increasing costs for advanced licenses, as required with the competition.

Cautions

- **Cloud NAC:** Aruba's Cloud Auth solution is new and lacks parity with Aruba's ClearPass. Buyers need to consider their requirements carefully, and calculate TCO if buying additional software components.

- **Lack of third-party network management:** Aruba has focused investment in their Central cloud and on-prem management solution instead of AirWave, their legacy on-premises network infrastructure management system. Although HPE does offer OpsRamp for third-party management, this has left a portfolio gap without complete parity.
- **Confusing NaaS offering:** Aruba has multiple NaaS offerings for both end customers and its channel, which have been cited as confusing when prospective buyers consider licensing options and service packs.

Huawei

Huawei is a Leader in this Magic Quadrant. Huawei's CloudCampus solution consists of CloudEngine S-series switches, AirEngine wireless APs and iMaster NCE applications that are broadly focused on addressing a wide range of use cases. Huawei's operations are globally diverse, with clients across multiple verticals and significant growth in Europe, the Middle East and Africa. However, geopolitical issues cause Huawei to have virtually no presence in North America and limited penetration in a few other countries, such as Australia and the U.K., where it ceased operations of its own accord. Gartner expects Huawei to continue to invest in its Wi-Fi 7 portfolio and antenna technology, and in its network assurance capabilities for high-quality user experience in popular audio and video applications.

Strengths

- **Strong product portfolio:** Huawei has a robust wired and wireless product portfolio that continuously monitors connectivity to increase performance and stability.
- **Experience-centric network configuration and management:** The iMaster NCE-Campus network management platform provides experience-centric wired and wireless LAN service quality and network assurance services.
- **Simplified architecture for OT to IT migration:** Huawei has introduced a converged campus network architecture that integrates OT capabilities into traditional enterprise products and simplifies the migration of OT to IT.

Cautions

- **Global sales reach challenges:** Huawei continues to have ongoing geopolitical issues that limit Huawei's exposure in some geographies and vertical markets. Its presence in North America, the U.K. and Australia is limited.

- **Limited market messaging:** Compared to other vendors in the market, Huawei marketing focuses on its technical capabilities and less on client business values and issues.
- **No NaaS offering:** Huawei does not have a NaaS offering, with pricing delivered on a pay-for-use basis or as a subscription based on usage metrics.

Juniper

Juniper Networks is a Leader in this Magic Quadrant. Its wired and wireless LAN offering includes EX series switches, QFX series switches and wireless access points driven by Mist AI, which address most use cases across large-enterprise and MSE markets. Juniper's client base is globally diverse, with particular focus on the general enterprise market, as well as retail, education, government and healthcare. The company continues to invest in integrated AI and ML operations, as well as cloud-based security capabilities. Gartner expects that Juniper will invest in GenAI integration for enhanced capabilities in its natural language processing interface.

HPE announced its intention to acquire Juniper Networks on 9 January 2024. At the date of publication, Juniper Networks met the inclusion criteria for this Magic Quadrant, and both HPE and Juniper continue to operate as independent entities. Gartner will provide additional insight and research to clients as more detail becomes available.

Strengths

- **AI-driven automation:** Juniper leads with AI/ML-driven capabilities, including performance monitoring based on customizable SLEs, to deliver improved end-user experience. Guided troubleshooting and the ability to automatically fix routine issues simplify network operations.
- **Strong security:** Juniper's WxLAN framework provides networkwide policy enforcement for users and IoT endpoints, and the recently introduced Juniper Mist Access Assurance service further provides agentless NAC capabilities.
- **Simplified network management with fabric technology:** Juniper's Campus Fabric, based on a VXLAN overlay with an EVPN control plane, can ease campus and branch management of Juniper devices by reducing network complexity and deployment inconsistencies.

Cautions

- **Cloud-dependent management platform:** While Mist Edge handles some network functions on-premises, to get the most value (e.g., access to real-time statistics and device updates) it requires a connection to the Mist Cloud. The legacy Junos Space Network Management Platform lags functionality as a fully centralized (on-premises) alternative.
- **Campus fabric lacks third-party support:** While Juniper's fabric is built on a standards-based EVPN-VXLAN architecture and interoperates with third-party infrastructure, it does not manage third-party network devices natively.
- **Limited customer traction of NaaS solution:** Juniper has announced its NaaS offering, but Gartner barely sees it come up during inquiry.

TP-Link

TP-Link is a Niche Player in this Magic Quadrant. Its Omada, Omada Pro and associated network software products mainly focus on addressing the needs of the small and midsize enterprises (SMEs). Its operations are geographically diversified, with the bulk of its revenue generated from EMEA, followed by Asia/Pacific and North America. Gartner expects that TP-Link will continue to invest in SME customers' requirements for ease of configuration and operations by adding to the capabilities of its GUI web-based configuration and cloud management platforms.

Strengths

- **Scalable network management offering:** The Omada network management offering is bundled with its access network hardware, which provides unified monitoring for an unlimited number of TP-Link APs, campus switches and security gateway products.
- **Wi-Fi 6 and 7 portfolio:** TP-Link has a comprehensive portfolio of Wi-Fi 6 access points, all of which are supported by RF optimization features, which can improve overall end-user experience and the ability to troubleshoot the wireless network infrastructure. It has also introduced Wi-Fi 7 access points to its portfolio.
- **Competitive pricing:** TP-Link's pricing is among the lowest of its competitors, which aligns with the needs of most MSEs. More broadly, this strategy is particularly attractive to organizations with basic network connectivity needs and where cost is the primary determinant.

Cautions

- **Lack of enterprise focus on software innovation:** Despite products that meet all traditional levels of enterprise network technology, TP-Link lags behind other vendors in its support of advanced network operations technologies, such as network assurance, automation and AIOps functionality.
- **Basic network security and location features:** TP-Link provides only basic network policy enforcement, and limited IoT containment and indoor location services.
- **Limited product capabilities:** TP-Link's enterprise network portfolio lags the competition, with limited AI/ML capabilities. Additionally, TP-Link's portfolio lacks support for next-generation networking features such as network fabrics, leaf-spine topologies and dynamic segmentation.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

Allied Telesis was added to this Magic Quadrant.

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

For Gartner clients, Magic Quadrant and Critical Capabilities research identifies and then analyzes the most relevant providers and their products in a market. Gartner uses by default an upper limit of 20 providers to support the identification of the most relevant providers in a market. On some specific occasions, the upper limit may be extended by Methodologies where the intended research value to our clients might otherwise be diminished. The

inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, providers must:

- Demonstrate relevance to Gartner clients in the wired and wireless networking market by offering an Ethernet switching and wireless LAN (Wi-Fi) hardware portfolio that minimally addresses the “must-have” capabilities identified in the market definition.
- Produce or OEM networking products that provide mechanical and/or virtual stackable wired networking for general availability as of 31 July 2023. All components must be publicly available for purchase, exist in inventory, be available for shipping and be included on the vendor’s publicly published price list. Products shipping after this date will only have an influence on the Completeness of Vision axis.
- Vendors are required to meet one of the following (reported as constant currency):
    - At least $200 million in annual revenue and have at least 200 customers that use its enterprise wired and wireless LAN solution in the twelve months from 1 July 2022 to 1 July 2023, where “customer” is defined (per Gartner Methodologies) as a net new installed logo that has paid for the equipment and/or is additionally paying (for subscription services), depending on the purchasing model.
    - At least $10 million in revenue in the twelve months from 1 July 2022 to 1 July 2023, and 50% growth compared to the previous 12 months.
- Have a cloud- and on-premises-capable network discovery, identification, configuration, security, management, and monitoring platform that includes integrated network automation tools.
- Offer integrated network security tools that offer, at a minimum, device and user segmentation, with specific remediation for guest users/devices and IoT devices.
- Have no more than 70% of revenue generated in a single region (of the seven regions mentioned below).
- Have customers in at least four of the seven global regional sales (APAC/Japan, North America, South America, Western Europe, Eastern Europe, Middle East, Africa).

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate vendors on their ability to deliver products or services that meet the requirements of the market. We also evaluate the vendor's ability to articulate differentiation and core competencies in their market message and the receptivity of the market. As a more mature market, criteria such as operations are not rated because we feel that it does not affect the ability of vendors to deliver solutions to the market, compared to the other criteria.

Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	Low
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	High
Customer Experience	Medium
Operations	NotRated

Source: Gartner (March 2024)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to communicate that they understand client business issues in their target markets and have the products, services, vision and strategies to address these issues.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Low

Source: Gartner (March 2024)

Quadrant Descriptions

Leaders

A vendor in the Leaders quadrant will have demonstrated an ability to fulfill a broad variety of customer requirements through the breadth of its enterprise network product family. Leaders will have the ability to shape the market and provide complete and differentiating enterprise network applications, as well as global service and support. Leaders should have

demonstrated the ability to maintain strong relationships with their channels and customers, and have limited gaps in their portfolios or are very strong in specific areas.

Challengers

A vendor in the Challengers quadrant demonstrates sustained execution in the marketplace. It will have clear and long-term viability in the market, but may not have a complete enterprise network portfolio for either products or network applications. Additionally, Challengers may not have shown the ability to shape and transform the market with differentiating innovation or functionality, or have the ability to serve a broad, global customer base.

Visionaries

A vendor in the Visionaries quadrant demonstrates an ability to increase features in its offering to provide a unique and differentiated approach to the market. A Visionary will have innovated in one or more of the key areas of enterprise network technologies (for example, security, management or operational efficiency). The ability to apply differentiating functionality across an entire enterprise network infrastructure will affect its position.

Niche Players

A vendor in the Niche Players quadrant demonstrates a near-complete product offering. However, it may not be able to control development or provide differentiating functionality because it relies on a strategic partner to offer part of the offering, whether it is a hardware component or a network application. Niche Players may also lack strong go-to-market capabilities that would enhance their regional or global reach or service capabilities in their product offerings. Niche Players often have deep vertical knowledge and will be an appropriate choice for users in the specific vertical markets where they have specialized offerings and knowledge.

Context

Gartner’s perspective on the enterprise wired and wireless LAN infrastructure marketplace emphasizes the continued and accelerating shift from merely providing foundational network connectivity to applications and technologies that address business issues such as technical debt, lack of IT resources and digital transformation. It also includes application

performance, end-user experience and the overall support of business requirements across the entire network fabric. This market view is based on the preceding 12-month time period ending August 2023.

Gartner's research indicates that investments in campus-switching products have slowed down in the past year, with global port shipments registering a decline of 1% in the period 1Q23 through 3Q23, year over year (see **Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 3Q23**). Worldwide unit shipments of WLAN APs, however, increased by 10%. This indicates that organizations continue to "rightsize" investments in wired infrastructure, while favoring a more aggressive push to Wi-Fi connectivity. The increase in work-from-anywhere initiatives is creating opportunities for enterprises to reduce their footprint of switching and cabling infrastructure, since Wi-Fi connectivity better suits flexible office space arrangements.

From a global market revenue perspective, campus switching grew 31% and WLAN 27% in the period 1Q23 through 3Q23, year over year, hence significantly outpacing shipment growth. This was predominantly due to price increases, as a result of the supply issues that have been impacting the market since late 2021. Most vendors have raised their pricing to counterbalance higher component and freight costs, albeit these increases have also impacted software licensing. The outlook for 2024 is that of supply conditions continuing to improve, as most vendors have voiced, allowing them to carry on releasing backlog as inventory levels normalize. While it is unlikely that vendors will reduce their pricing in the next 12 months as supply conditions stabilize, today's economic environment will foster more aggressive price competition. The value proposition of more attractive lead times has begun to slowly fade away as a differentiator, and we expect will force vendors to more aggressive discounts.

Even though core connectivity technologies are also driving network refresh projects, the most visible of the connection-oriented technologies is Wi-Fi 6 (802.11ax), which operates at 2.4 and 5 GHz, and Wi-Fi 6e (802.11ax; 6 GHz), which is still a draft standard and operates in the less-crowded 6 GHz spectrum. It is important to note that the majority of contemporary end-user devices, such as laptops, tablets and smartphones, are still limited to 802.11ac and 802.11ax, and cannot use the 6 GHz spectrum.

Wi-Fi 6E APs accounted for 1.7 million units shipped in the period 1Q23 through 3Q23, equivalent to 6% of overall AP shipments. Wi-Fi 6E adoption is led by customer interest in the performance improvements from the newly allocated 6 GHz band, combined with future-

proofing aspirations. We believe that some of these deployments have been influenced (and will continue to be, in the short term) by the supply issues affecting the market. Gartner has observed Wi-Fi 6E AP sales benefiting from shorter lead times. This is because Wi-Fi 6E APs have new semiconductor components, altering supply differently, and shipments only started to pick up at the end of 2022, limiting the impact on inventory levels. The arrival of Wi-Fi 7 will change many of these dynamics, diminishing the value proposition of Wi-Fi 6E.

The reliance on diverse suites of technologies to support digital business has placed significant emphasis on understanding application performance, user experience requirements and security postures across the entire network fabric. Disruptive network technologies that focus on application performance and end-user experience continue to drive the majority of innovations in the overall enterprise networking market.

What Has Changed?

Focus on Business Outcomes

Gartner inquiries indicate that organizations have grown weary of complex, perpetual network projects and the associated high operational costs of enterprise networks. Enterprises want the network to "get out of the way" so they can focus on running their business and not running the network. Therefore, the shift from delivering only network connectivity to actually supporting business outcomes continues to accelerate. Network equipment vendors are responding by introducing AIOps, GUI and natural language interfaces, and cloud-native platforms that speed time to deployment and drastically reduce operational tasks, even across complex enterprise networks.

Lack of Personnel and Skills Continue to Drive a Push to Automate

In the last couple of years, Gartner's Leadership Vision for Infrastructure and Operations survey has found that enterprises continue to have personnel shortages and skill deficiencies in their organizations. From client inquiries, enterprises are using automation to not only provision equipment and monitor but also to troubleshoot issues when the network functionality is not meeting defined service levels.

ZTNA Creates New Experiences

Remote clients are using the connectivity that is available, such as public internet, in conjunction with cloud-based zero trust network access (ZTNA) services to provide security, visibility and flexibility in an as-a-service model. This allows vendors to deliver the same

offering in their on-premises campus and branch environments that they're using to secure connectivity to their remote employees. The result would be a single software offering, versus disparate offerings for campus and remote workers, with the goal to deliver a "coffee shop" network, whereby the user experience is: grab a seat, connect and work.

Market Overview

The enterprise wired and wireless LAN infrastructure market is now composed of vendors not only delivering wired and wireless Ethernet networking hardware, but also tightly integrating network management applications that reside on-premises or in the cloud. This combination of network hardware and powerful software is integral for addressing organizational mission agility, the need to automate, pervasive security and the increased levels of performance required by end users across all categories of connected applications and devices.

These integrated software tools speed time to completion for enterprise network deployments, reduce time to identify and resolve network and application issues, and deliver pervasive automation tools that reduce network administrator workloads.

Additionally, core integration of AI and ML is integral to organizing the flood of telemetry data, thereby presenting key data points necessary to optimize the network in support of digital business requirements. This technology is also becoming a valuable source of business-relevant data that is useful to I&O and overall business leadership.

How Buyers Shape Their Buying Decisions

Traditional Network Technology Capabilities

Enterprise networking has been shaped by more than 30 years of primarily delivering connectivity and resiliency at Layer 2 and Layer 3 of the OSI network model. As a result, buyers expect robust traditional Layer 2 switching features, appropriate power over Ethernet to support VoIP and AP hardware, QoS, and sufficient uplink speeds to support various traffic requirements. At the wired access layer of the network, customers expect the Wi-Fi power, performance and throughput that is necessary to support the client connection densities and bandwidth requirements. Finally, the network core and distribution layers must deliver the redundancy and high-speed routing and switching capacity to support dramatically

increased north-south traffic, much of which is destined for the cloud and other off-network locations.

Perpetual and Subscription License Pricing

Network hardware continues to be relatively commoditized, and true differentiation across vendors is reliant on the capabilities of network software features and functionality. However, as network vendors adopt the stance of software vendors, there are diminishing options for traditional perpetual licensing. Vendors realize new revenue streams by shifting to subscription-based licensing, but the shift is often confusing and continues to be a source of frustration for I&O leaders. Subscription licensing may make sense for some organizations. However, a preponderance of Gartner clients continue to express a preference for having a choice of licensing options, instead of being forced into licensing that is often inclusive of features they don't need.

AI, ML and Automation

Enterprise network vendors now offer tools using various degrees of artificial intelligence, machine learning, a natural language interface, automatic issue identification, and remediation to reduce network administration and operational workloads. However, adoption of these essential toolsets in production environments is very slow. Initially, there were concerns about the maturity of the tools, as well as their ability to increase the productivity of network operations teams. As tools mature, there is less concern about their capabilities to operate in the production network environment.

Currently, there are varying degrees of self-driving capabilities enabled by machine learning (see **Quick Answer: What Functionality Should I Expect From Network AIOPs Features?**). Artificial intelligence will drive more business-relevant network outcomes as routine issues are quickly and automatically resolved. Therefore, vendors that successfully deliver products with meaningful automation of network functions enable network teams to meet SLAs for increased overall network availability, application performance and user satisfaction.

Management Suite

As managing technical debt is one of the top challenges that IT infrastructure and operations organizations face. Per the 2023 Gartner I&O Leaders Signature Role Survey, the ability to provide a migration strategy that includes managing the legacy solution, if applicable, is an important decision criterion. [1] Clients have expressed through inquiry that

they don't want two or three different management applications for their equipment. The mantra of a "single pane of glass" extends to the entire campus environment.

Incumbency

Organizations tend to stay with their current enterprise network vendor if it offers a technology portfolio that is "good enough" to meet their needs and functions within reasonable expectations. Since the network market is relatively conservative and risk-averse, incumbent relationships often survive even when technology alignment is suboptimal. Clients that switch vendors tell us through inquiries that a significant difference in pricing from the average market price, especially on hardware such as access points and switches, will affect their decision to move to another vendor. Additionally, an often-unseen driver is the support that is received during the relationship. Clients who have bad support experiences, whether it is directly with the vendor or through a reseller, are often motivated to switch vendors.

How Providers Package, Market and Deliver

Traditional Consumption

Buyers generally source their wired and wireless LAN infrastructure through an authorized vendor channel partner, with relatively few purchases occurring directly from the network vendor. Hardware expenditures are usually a one-time cost, which is inclusive of a firmware end-user licensing agreement. These initial costs include updates to resolve certain firmware bugs that adversely affect the use of the hardware, or security vulnerabilities that would expose the end user to significant damage if left unpatched. Future operating system updates, feature upgrades or security patches are functions of a firmware maintenance contract that is purchased separately, either at the time of purchase or at a future date. Vendors charge for hardware and software licenses either as a perpetual license or as a subscription license but, as mentioned previously, the market is trending away from perpetual licensing.

Network management platforms have become ubiquitous, so access usually requires separate management licensing with various functionalities assigned to higher levels. However, some vendors offer enterprise networking solutions that are 100% reliant on the management platform for all functionalities. In such cases, the network management platform is included, and various security and/or feature license levels are offered.

Network as a Service

NaaS has slowly emerged in the enterprise networking market over the last 18 months. NaaS is based on a term subscription consumption model and includes deployment and managed services, flexible feature licensing and specific performance SLAs, and the vendor or partner maintains ownership of the equipment throughout the subscription period. True NaaS should present a transparent backbone infrastructure model, similar to cloud, thereby making the network device models, topologies and protocols behind the scenes irrelevant, as long as they meet the business outcome and SLA requirements.

⊕ Evidence

Note 1: Gartner’s Definition of 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 use metrics.

⊕ Evaluation Criteria Definitions