Magic Quadrant for the Wired and Wireless LAN Access Infrastructure

Published 11 July 2018 - ID G00345275 - 56 min read

By Analysts Bill Menezes, Christian Canales, Tim Zimmerman, Mike Toussaint

Evolving enterprise requirements for greater access layer intelligence and automation continue challenging networking vendors. Infrastructure and operations leaders should evaluate wired and wireless LAN infrastructure based on increasingly complex needs for access network services and management.

Strategic Planning Assumptions

By 2020, only 40% of network operations teams will use the command line interface (CLI) as their primary interface, down from 75% in 2018.

Adoption of cloud-managed networks by businesses of all sizes will double, from less than 10% in 2018 to more than 20% by year-end 2023.

Market Definition/Description

Gartner defines the wired and wireless access LAN Infrastructure market as comprising vendors supplying wired and wireless networking hardware and software that enables devices to connect to the enterprise wired LAN or Wi-Fi network. These devices may include:

- Laptops
- Smartphones, tablets and other mobile smart devices
- Networked office equipment
- Sensors and other Internet of Things (IoT) endpoints
- Other fixed or mobile devices communicating to a wired switch port or a wireless access point (AP) at the edge of the enterprise infrastructure

This research does not cover wired and wireless access networking infrastructure for adjacent markets such as public venues; small office/home office; commercial and industrial settings; or point-to-point solutions. It also does not evaluate vendor capabilities in "service provider Wi-Fi," such

as public hot spots operated by a communications service provider for mass-market access or offloading of cellular device data traffic.

Enterprise wired and wireless local-area networking components include:

- Hardware — Physical network elements including:
  - Wireless access points
  - Wired switches
  - Controllers (physical or virtual), if needed
- Software — Network service applications that are cloud-based, appliance or virtual appliance, including but not limited to:
  - Network management, monitoring
  - Performance management
  - Guest access
  - Onboarding services
  - Authentication, authorization and accounting (AAA) security/authentication
  - Policy enforcement
  - Intrusion detection systems/wireless intrusion detection systems
  - Location services
  - Application visibility
  - Network and vertical market analytics
  - Security, including behavioral analysis

This market includes these typical vendor types:

- *Vendors providing their own wired and wireless infrastructure components, network applications and services*
- *Vendors primarily providing a specific connectivity option, such as either wired or wireless components.* These vendors often focus on solutions addressing a unique set of market

requirements, such as cloud-based management of a predominantly wireless LAN, or a vertical market such as retail or healthcare.

- *Vendors using a strategic partner to provide some or all of the hardware or software components of an end-to-end access solution, including network services applications.* The combined solution these vendors offer should provide differentiating functionality, in order to be considered a better option for enterprises that might otherwise buy solution components directly from the strategic partner.

Magic Quadrant

Figure 1. Magic Quadrant for the Wired and Wireless LAN Access Infrastructure

Source: Gartner (July 2018)

Vendor Strengths and Cautions

Aerohive

Aerohive's wireless-focused access network portfolio comprises stand-alone and stackable campus switches, access points and branch office routers, with a cloud-managed distributed control architecture. Organizations typically employ HiveManager network management as a public or private cloud solution, although it also may be deployed on-premises. To manage a multivendor unified access network, the enterprise can use HiveManager to configure, provision and monitor Aerohive APs in conjunction with switches from Aerohive or with N-Series switches from OEM

partner Dell EMC. Organizations managing Juniper Networks' wired switches with the Juniper Sky Enterprise solution can get visibility of Aerohive APs through Juniper's integration with Aerohive Cloud Services Platform APIs. Aerohive also enables unified policy management of its wired and wireless LAN and its own software-defined WAN (SD-WAN) VPN routers through HiveManager.

After the evaluation period for this Magic Quadrant, Aerohive began shipping A3, a stand-alone access management solution sold independently of the vendor's switches and APs, for onboarding, authentication, access control, and guest access of wired and wireless clients on any vendor network.

Aerohive's focus is primarily distributed enterprises, including healthcare, retail, and hospitality, followed by the primary/secondary education vertical market and higher education. Aerohive generates most of its business in North America and EMEA, with Asia/Pacific markets addressed primarily by its strategic partners. Midsize enterprises in those regions seeking cost-competitive solutions should evaluate Aerohive as an option for cloud or on-premises-managed wireless LANs (WLANs); global enterprises deploying compatible Dell or Juniper switches should evaluate Aerohive as part of a unified access network.

Strengths

- Aerohive bundles a basic version of HiveManager with all its campus switches and APs as Aerohive Connect. This provides organizations seeking simple access network connectivity with basic cloud network configuration and monitoring for no additional subscription cost, with an upgrade path to expanded features for policy management, guest access, security and network device visibility.
- Organizations have options for third-party campus switches that integrate with HiveManager, since Aerohive added Juniper as a partner. Organizations looking beyond Aerohive's own limited wired switching portfolio and its core territories of North America and EMEA now have more global options for integration with Aerohive APs in Dell EMC and Juniper.
- HiveManager includes Aerohive's Insight platform of open APIs, enabling developers to create solutions accessing information about network and client devices and applications connecting with the enterprise LAN.

Cautions

- Aerohive relied on the Americas region for 63% of its access-network-related revenue in 2017, with 9% coming from what is currently its smallest region, Asia/Pacific. Customers must perform due diligence to ensure Aerohive or its partners provide sufficient postsale service and support in regions where it does less business.
- Aerohive global WLAN revenue declined 9.9% in 2017. Customers should monitor the company's ongoing product development and improvements in areas such as machine learning capabilities

for network management and assurance.

- Aerohive customers must rely on the vendor's partners for wired switching hardware beyond its own basic branch switching product line, which, during the evaluation period for this research, did not include 802.3bz multigig campus switches.

ALE

ALE provides a broad portfolio of wired and wireless access networking products under the Alcatel-Lucent Enterprise brand. It utilizes its own OmniSwitch wired switches combined with its cost-competitive OmniAccess Stellar wireless access points for midsize enterprise campus and branch office deployments, managed via its on-premises OmniVista 2500 network management system. ALE also now offers OmniVista Cirrus, a multitenant cloud management solution with an entry-level "freemium" service tier that provides limited functionality, such as a dashboard for viewing basic network and device inventory, and available software and firmware updates for its registered network devices. The premium version, available as a SaaS subscription, enables network provisioning, unified management of ALE switches and Stellar APs, network heat mapping, and network performance monitoring.

ALE targets primarily the hospitality, healthcare, transportation, education and government vertical markets. Organizations in its primary business regions of EMEA, North America and Asia/Pacific outside of China should include ALE in their access layer vendor evaluations.

Strengths

- In addition to its Stellar wireless APs, ALE supports campus unified access layer deployments using APs from its OEM partner HPE (Aruba), managed with OmniVista 2500. Clients can deploy access control and guest access or bring your own device (BYOD) management via OmniVista 2500 or Aruba's ClearPass Policy Manager solution.
- ALE's core access layer technology includes its Intelligent Fabric, which enables automated configuration or reconfiguration of ALE network devices or applications, helping to reduce deployment time and potential configuration errors by automating network protocol configurations.
- ALE provides wireless mesh networking functionality for all of its OmniAccess Stellar APs, as a no-cost software upgrade. The function enables the APs to connect with each other via the low band of the 5GHz radio, using the 5GHz high band and 2.4GHz bands for client connectivity to the APs.

Cautions

- ALE continues to rely on HPE (Aruba) as a strategic partner for large WLAN deployments with complex requirements, limiting the control it has over technology development to serve organizations with those needs.

- ALE's network automation capabilities remain limited, with machine learning currently used for functions such as generating predictive analysis reports through the OmniVista management solution, or identifying potential network configuration change issues via the ProActive Lifecycle Management (PALM) solution.

- ALE's indoor location solution, Stellar LBS, utilizes only Bluetooth low energy (BLE) technology that Gartner believes renders it too limited for some advanced enterprise location service uses requiring more precise asset location than BLE may provide.

Allied Telesis

Allied Telesis offers an end-to-end wired and wireless LAN portfolio, but did not begin shipping more recent functional capabilities such as campus switches supporting 802.3bz multigig technology until 2Q18 and planned availability of 802.11ac Wave 2 access point is 3Q18.

Enterprises can manage the switching and WLAN product portfolio on-premises with Vista Manager EX or in the private or public cloud using Autonomous Management Framework (AMF) Cloud. Customers requiring a controller-based architecture must use the Autonomous Wave Control (AWC) plug-in with the vendor's Vista Manager EX unified management solution or integrated with Allied's AR-Series Firewall products. Allied Telesis' Unified Wireless Controller (UWC), deployable as hardware or a virtual appliance, was scheduled for end of sales in 2H18. The Allied Telesis AMF delivers a suite of features to optimize reporting, network management and automation. The xSeries switches and TQ access points are Open Networking Foundation (ONF)-certified products, leveraging software-defined networking (SDN) and firewall integration for device access control.

Allied Telesis sells predominantly through channels, generating more than 50% of its revenue in Japan. The company rarely appears in Gartner inquires, although it has a global footprint. Allied Telesis mainly targets the public-sector, education, healthcare and hospitality vertical markets. Predominantly small and midsize enterprises in the Asia/Pacific region, North America and EMEA should assess Allied Telesis for its wired and wireless LAN infrastructure needs.

Strengths

- All products, including industrial-grade switches, use the same operating system (AlliedWare Plus) for uniform functionality, support, migration and upgradability.

- Vista Manager EX/AMF can be deployed on-premises or as a multitenant cloud option, providing deployment flexibility while simplifying network management and automation. Vista Manager EX supports multivendor monitoring, requiring SNMP configuration for visibility and monitoring of other vendor network devices.

- Vista Manager EX/AMF can also be integrated via an API with Allied Telesis Secure Enterprise Software Defined Networking (SES), an SDN controller that integrates with the firewall to manage policy enforcement.

Cautions

- Allied Telesis has limited functionality for basic applications, such as guest access. It does not provide a captive portal that automatically issues guest access through SMS or email.
- Allied Telesis does not provide location-based services and has limited capabilities for IoT segmentation, real-time traffic analysis and security behavioral analytics. This impairs its near-term ability to deliver on advanced enterprise requirements.
- Allied Telesis operates globally, but 60% of its revenue is derived from the Asia/Pacific region. Clients should validate that the reselling partner has the ability to provide sufficient local support capabilities.

ARRIS (Ruckus)

ARRIS International completed its acquisition of the former Ruckus Wireless and the Brocade ICX wired switch business of Broadcom in December 2017. Those operations now provide enterprise access networking solutions as "Ruckus Networks, an ARRIS Company." ARRIS' strategy is to grow its enterprise access networking sales via Ruckus, diversifying beyond a legacy business that focused on service provider networking solutions primarily for cable multisystem operators and telcos that provide consumer, public venue and multidwelling unit Wi-Fi.

Ruckus provides full enterprise-portfolio-enabling unified management of a wired and wireless access network using either a controller-based or controllerless architecture, with on-premises or cloud-based management. In late 2017, the vendor expanded its ICX campus switch portfolio with the new ICX 7650 fixed form factor stackable switch lineup that included an access switch supporting up to 24 1/2.5/5/10GbE multigigabit ports.

Ruckus' foremost enterprise vertical focuses are in hospitality, retailing, education, and national, state, and municipal government, served through ARRIS and Ruckus channel partners. Enterprises in these markets in North America, EMEA and Asia/Pacific with access layer requirements should evaluate Ruckus as a potential solution.

Strengths

- Ruckus Cloud Wi-Fi platform enables remote configuration and management of compatible wireless APs, plus the ability to switch to an on-premises management solution using the same APs.
- Ruckus' Cloudpath Enrollment System provides wired and wireless network access management, policy management, onboarding and guest access for user or IoT devices, as either a cloud-based or on-premises solution, available as a software purchase or SaaS.
- Ruckus offers a versatile IoT solution via its IoT Suite that comprises the vendor's SmartZone controller, compatible Ruckus APs and IoT Modules that attach to the APs. These modules enable

connection to the WLAN of non-Wi-Fi IoT endpoints using connectivity standards such as Zigbee, BLE or LoRa. The controller enables a single management interface for both the WLAN and the IoT access network.

Cautions

- Current and potential customers should require details of the ICX development roadmap as well as integration between ICX and the Ruckus cloud management platform to determine if these products can meet their unified network requirements.
- Ruckus trails its large-enterprise competitors in delivering advanced enterprise capabilities, such as network automation, and in the accuracy of location-based services supported by its Smart Positioning Technology (SPoT) location engine and analytics software.
- Ruckus does not support multivendor management of the enterprise access layer through its cloud management platform. The vendor has an OEM relationship with Dell EMC for access networking, aimed primarily at enterprise verticals and service provider customers.

Cisco

Cisco continues to provide the broadest portfolio of access wired switching and WLAN products. In 2H17, Cisco began delivering its intent-based networking architecture for campus solution, which included the launch of the Catalyst 9000 switching product line, and, in 1H18, new Aironet 4800 access points.

Customers must choose between two separate access layer solutions — Aironet/Catalyst and Meraki — which are loosely tied together through the Digital Network Architecture Center (DNA-C) network monitoring dashboard. The DNA-C offering provides management and automation capabilities for Cisco Aironet and Catalyst product lines that are not available in the Meraki cloud platform. DNA Center version 1.1 enables a single dashboard for visibility and control for both Meraki and Aironet/Catalyst product families, even though Cisco continues to maintain the Meraki Dashboard for full management of Cisco Meraki switches and APs.

In 2017, Cisco grew its revenue year over year for both campus switches and enterprise WLAN equipment, but at a slower rate than the overall market. Clients should consider Cisco globally for all enterprise on-premises and cloud-based access layer opportunities.

Strengths

- For organizations with hybrid environments, Cisco's roadmap for 2H18 is to continue developing DNA Center as a platform that is a single touchpoint providing automation, analytics, and the ability to tie the Aironet/Catalyst and Meraki product lines together.

- For customers requiring an access networking strategy for IoT, Cisco has created a fully featured solution by integrating its IoT capabilities with its Enterprise Networks organization. Components include the analytics of DNA-C; Time-Sensitive Networking capabilities supported by the IE 4000 industrial switch line; and virtual segmentation supported by Software-Defined Access (SD-Access).

- For enterprises deploying iOS client devices, Cisco's relationship with Apple allows its infrastructure to uniquely acquire telemetry data directly from Apple clients with iOS Wi-Fi analytics.

Cautions

- Organizations with hybrid cloud and on-premises management requirements should realize that although DNA Center provides central management functionality for Catalyst/Aironet and Meraki, there are differences in how some features might be implemented, rendering hardware components and some software functionality incompatible. These differences are a consideration for migration between platforms if needs or requirements change.

- Clients report that Cisco ONE/DNA bundling options are a shift from previous licensing and include in the subscription components for automation and assurance capabilities that they find complex and that may provide overlapping or unneeded services. Mandatory term licenses for some products also create uncertainty and can increase ongoing costs. Enterprises must review the capabilities and pricing in each licensing tier before making purchase decisions.

- Clients report that implementing IoT segmentation using SD-Access is complex and difficult to deploy. Enterprises should confirm that they have adequate resources and training to ensure that they achieve the intended business functionality.

Dell EMC

Dell EMC provides unified access networking solutions based on its own N-Series stackable campus switches combined with WLAN infrastructure from strategic partners Aerohive and ARRIS (Ruckus). Enterprises specifying on-premises or cloud-based management will use Aerohive, which provides an OEM solution comprising Dell EMC-branded wireless APs and a version of Aerohive's HiveManager NG network access and control suite enabling unified management of the wired and wireless network. Dell EMC provides basic access management, policy enforcement, onboarding and security functions using its branded version of HiveManager NG, or additional multifactor network access control through its own Impulse SafeConnect solution.

Dell EMC also has continued developing open networking capabilities, launching its N2128PX-ON and N3132PX-ON 802.3bz switches with an Open Network Install Environment boot loader enabling third-party operating system vendors to support the hardware with their OSs.

Dell EMC's primary enterprise focus is on midsize organizations, with additional vertical market targets globally that include public education, healthcare, hospitality and government. Organizations with unified access network requirements should include this vendor in their evaluations.

Strengths

- Dell EMC provides a large ecosystem for access network services, including AirWatch for unified endpoint management; Impulse SafeConnect for network access control (NAC); and Dell's RSA NetWitness suite for security behavioral analytics.
- The vendor supports IoT device management with VMware's Pulse IoT Center solution, which used an open-source agent to identify and then onboard "things," with policy enforcement at the access switch or AP.
- Customers buying Dell EMC's unified access network infrastructure benefit from the company's global support infrastructure, which is more developed than those of its OEM partners in such regions as Latin America and Asia/Pacific.

Cautions

- Dell relies on Aerohive and Ruckus for wireless technology development in applications such as wireless network analytics and location-based services, raising the risk that having no direct control over partner roadmaps hinders its ability to respond quickly to changing WLAN market requirements.
- Dell has indicated its relatively new OEM relationship with Ruckus is focused on service provider and public venue networking. The companies have not outlined any plans to leverage the relationship for product development specific to enterprise campus and branch office use cases.
- Dell EMC lags its major competitors in delivering advanced enterprise capabilities such as network automation and location services, which rely heavily on the capabilities of its OEM partners in those areas.

D-Link

D-Link provides unified wired and wireless access network infrastructure for enterprise customers that have basic connectivity requirements and a priority of cost control. The vendor's enterprise business portfolio includes dual radio 802.11ac indoor and outdoor access points plus stackable managed Ethernet switches. This includes the DMS-1100 switch line with 802.3bz multigig ports to support fully Wave 2-capable uplinks, although during the evaluation period for this Magic Quadrant, D-Link did not offer APs with 802.3bz capabilities. Most D-Link enterprise customers utilize the Central WiFiManager wireless controller software available as an on-premises or cloud-hosted solution at no additional cost, with its campus switch and wireless AP products, for basic network management and guest access features. In February 2018, the vendor introduced its Nuclias cloud-

managed network platform, available as IaaS and providing a more fully featured solution than Central WiFiManager for network configuration, monitoring, guest access, and unified management of a D-Link wired and wireless access network.

D-Link's enterprise offerings focus on small to midsize organizations primarily in the education vertical market. Cost-conscious prospects with basic campus access networking requirements in regions such as EMEA and North America, where D-Link has its largest business presence, can evaluate this vendor for small branch office and remote location deployments.

Strengths

- D-Link is a low-priced solution offering a broad range of indoor and outdoor wireless APs, plus managed and unmanaged wired campus switches suitable for basic networking use cases.
- Basic guest access features are included at no additional cost with D-Link's DAP and DWL access points, DWC wireless controller and DES, DGS and DXS managed switch models.
- D-Link's Auto Surveillance VLAN (ASV) utility for its Smart and SmartPro managed switches enables customers to route both data and video from IP surveillance cameras through the same switch, instead of requiring a dedicated switch just for the video feed.

Cautions

- D-Link's business is concentrated in emerging markets, Asia/Pacific and Europe, and in the consumer and service provider markets, which account for about 80% of its business. Enterprise customers outside of those domains should ensure the vendor provides an appropriate level of support both geographically and for their specific networking requirements.
- D-Link's web-based, subscription network management solution, D-View 7, does not support multivendor deployments, only the vendor's switches and access points, limiting its utility for mixed-vendor environments.
- D-Link's portfolio does not provide location-based service applications or support machine learning features for automating access layer connectivity, limiting its utility to basic enterprise connectivity and management requirements.

Extreme Networks

Extreme Networks is a wired/wireless LAN access layer vendor that continues to expand globally. In the past year, we have seen Extreme demonstrate its ability to deploy and support clients globally with a portfolio that allows it to address all enterprise access layer opportunities. Extreme has edge-to-core infrastructure solutions that can be optimized from on-premises, cloud or hybrid network service applications. Extreme customers have licensing flexibility — instead of a "one size fits all" model — for applications needed for their business requirements, such as ExtremeManagement,

ExtremeControl and ExtremeAnalytics. Extreme Fabric Connect also addresses the growing need for IoT segmentation and ExtremeAI uses network data and machine learning to automatically tune the wired and wireless access network. Extreme is one of only three vendors covered by this research that supports Time-Sensitive Networking services across a number of its switching platforms.

Extreme continues to provide strong customer service through a 100% insourced service and support team. While still a relatively small campus switch and WLAN vendor, 2018 revenue jumped 36% and WLAN revenue doubled. Most of the growth was due to acquisitions, although the company reported organic revenue growth as well.

Clients should assess Extreme Networks globally for all wired/WLAN access layer opportunities.

Strengths

- Extreme's management team continues to provide strong leadership, and the sales management team has extended the vendor's reach geographically as well as across vertical markets.
- Extreme Fabric Attach provides an access layer fabric that also addresses the need for enterprise IoT segmentation across its wired and wireless LAN product portfolio.
- Extreme's Product Management organization has done an excellent job integrating the access networking products of its recent acquisitions, Avaya and Zebra, into a cohesive roadmap focused on common hardware and a unified operating system, which is important to clients developing a three- to five-year strategy.

Cautions

- Customers with hybrid deployments may not initially be able to deploy newer Extreme Network applications both on-premises and in the cloud. For example, Extreme's user and entity behavior analytics (UEBA) offering was initially released as a cloud offering with an additional release for on-premises flexibility. Organizations need to validate applications can be deployed in the specified location.
- Extreme continues to lag behind providing location capabilities that lack the location precision of competitive offerings. Organizations using location solutions from ExtremeWireless or ExtremeWireless WiNG should specify their requirements and test to ensure that the technology addresses the use case.
- Customers purchasing Extreme products or that continue to own legacy products from the companies it has acquired must be aware of the challenges in combining the access layer offerings of several organizations. Organizations with existing Avaya or Zebra products need to ensure that they have a migration and product integration plan and that any new products or applications meet their solution needs.

Fortinet

Fortinet provides a portfolio of wired and wireless access networking infrastructure integrated closely with security hardware that reflects the vendor's core business. Clients control this infrastructure via the Security Fabric umbrella that provides simplified management and configuration of Fortinet switches and wireless APs through a single pane of glass, plus security, identification, policy application and enforcement.

Enterprises can manage Fortinet's Secure Wi-Fi and Secure Switching as a unified fabric from their FortiGate, reducing the time needed for configuring wireless LANs by treating them as extensions of their network security firewall. Access points can be managed via dedicated controllers, which offer WLAN control and scalability into the tens of thousands of APs. Fortinet's FortiCloud provides AP management and control with zero-touch deployment and client analytics. Fortinet also offers free location analytics that can be adopted with any of their management solutions.

Fortinet continues to focus on the distributed enterprise and branch office, retail, healthcare, and education verticals in the North America and EMEA markets. Global prospects should include Fortinet when they have requirements for enterprise-class unified wired and wireless network features and functionality.

Strengths

- Fortinet integration of security hardware into its access layer infrastructure provides the architecture with seamless network security without overly complex configuration and operation.
- FortiManager offers unified management tools for single-pane-of-glass management of thousands of devices across security, wireless and wired network devices.
- Fortinet's extensive use of GUI configuration tools can reduce requirements for learning new CLI commands for full functionality. Look and feel is similar across devices, which should reduce total cost related to adoption and ownership over the long term.

Cautions

- Gartner clients do not commonly report end-to-end Fortinet deployments; the lack of cross-vendor network equipment management in Fortinet's unified management platform does not account for the multivendor environments in which it may be deployed.
- Overlapping FortiGate and FortiWLC positioning can be a potential source of confusion regarding the targeted scale of deployment. Both products offer "enterprise-class" features and functionality, but Fortinet positions them to small and large enterprises respectively. This lack of clarity in positioning and use cases also extends to the Fortinet large offering of access points.
- FortiSwitches are targeted at small to midsize enterprises, while Fortinet wireless products can be scaled to support large enterprises, a difference that large enterprises looking to consolidate their

networks around the Security Fabric platform should be aware of.

HPE (Aruba)

Aruba, a Hewlett Packard Enterprise company, is one of the leading global providers of wired and wireless access networking products for campus and branch office deployments, with few notable exceptions. Enterprise customers with hybrid requirements for on-premises or cloud-managed network architectures choose from essentially the same portfolio of wired switches, wireless LAN controllers and access points. Although there remain feature and functionality differences, organizations have largely similar choices for unified access network management using ClearPass access control and policy management solutions via either the AirWave on-premises management or Aruba Central cloud management system.

HPE (Aruba) offers integrated security through its 360 Secure Fabric, which leverages ClearPass for NAC with IntroSpect for continuous monitoring of network and client devices to collect data for user and entity behavior analytics. IntroSpect uses more than 100 supervised and unsupervised machine learning models to identify anomalous behavior indicating potential or actual attacks, providing dynamic risk scoring that enables either manual response or an automatic response trigger in ClearPass.

HPE (Aruba) campus switching and WLAN revenue in 2017 grew less than overall market rates. Aruba's wired and wireless LAN solutions are suitable for consideration globally for all access layer opportunities.

Strengths

- The basic license for AirWave includes basic connectivity analytics, while AP licenses include ClearPass guest access software, mirroring similar offers from other vendors aiming to keep costs competitive for basic networking requirements.
- For campus aggregation and core switching, the 8400/8320 chassis switches include network analytics and policy-based integration with monitoring and security tools.
- HPE (Aruba) updated development of its capabilities for network service assurance with NetInsight, a new cloud-based offering feeding 400 data points into a machine learning engine to provide user connectivity and radio frequency insights for recommended network configuration changes.

Cautions

- Aruba has progressed slowly in developing products for IT/operational technology (OT) convergence. This will limit its utility for customers in the OT space, especially with Time-Sensitive Networking functionality.

- Customers interested in cloud-managed access networks are limited by the current focus of Aruba Central cloud management suite on branch network deployments. It lacks the same complete functionality as its on-premises ClearPass and AirWave offerings to support campus switches, controllers and APs while the company continues developing the product.

- HPE (Aruba)'s Meridian product line has not extended yet beyond Wi-Fi and BLE functionality, which leaves some end users, for some use cases in target markets such as healthcare and retail malls, looking for more robust solutions. Clients continue to explain that location service applications require the use of Meridian APIs to allow integration with other technologies and applications, to create an expanded end-user experience.

Huawei

Huawei provides access layer networking through its Enterprise Business Group (Enterprise BG) global solution provider that generated nearly 60% of its switching and WLAN revenue in 2017 in the vendor's home market of China. Huawei continues product development in areas such as unified network management, location-based services and advanced analytics for network assurance, with a portfolio and roadmap that generally keep pace with market requirements.

Enterprises seeking a unified wired and wireless campus networking solution utilize the Agile Campus Network Solution, which represents Huawei's end-to-end flagship offering for campus networking. Network service functions such as access control, policy enforcement, traffic monitoring, application visibility, WLAN configuration and deployment, location services, and guest access are provided through the Agile Controller-Campus (Agile Controller) solution. For integrated management of wired and wireless networks and for network quality analysis, enterprises must deploy the eSight software suite that utilizes SNMP.

Huawei is the third-largest vendor in the wired/wireless LAN access layer worldwide market, growing well above market rates. Clients should evaluate Huawei for all wired/WLAN access layer opportunities, especially for locations in China and EMEA, where it has a sizable installed base.

Strengths

- Agile Controller can be deployed on-premises and in the cloud, scaling to up to 6,000 APs and more than 1,000 switches. Software licensing options deliver functionality encompassing AAA security, onboarding, guest access management and security orchestration.

- Huawei has added 2.5/5 Gbps switches to its S6720-SI fixed-form campus switch portfolio, supporting its already strong foundation in fixed and modular switches that generally are priced lower than comparable products from its largest competitors.

- Huawei's Cloud Managed Network (CMN) solution allows management of wired and wireless LAN infrastructure in a private or public cloud, including firewalls and access routers. Organizations that require a change from an on-premises to a cloud-managed deployment can do so by

upgrading their software and their hardware licenses, without having to change hardware such as access points or switches.

Cautions

- Huawei generated more than 87% of its access networking revenue from the China and EMEA regions in 2017. Risk-averse organizations, especially in areas such as North America where Huawei has faced political headwinds, should conduct due diligence to ensure sufficient support for implementation and service of Huawei solutions.
- Huawei's end-to-end location services rely on partnerships that complement its broader customer value proposition. Organizations should ask for proof points and review Huawei's ecosystem of partners for additional capabilities.
- Huawei trailed its major competitors in providing advanced automation for network service assurance, having just introduced its CampusInsight solution using analytics leveraging AI technology in March 2018.

Juniper Networks

Juniper introduced its subscription-based Juniper Sky Enterprise cloud-based management platform in January 2018. Juniper Sky Enterprise introduces new cloud managed capabilities for the entire suite of Juniper networking and security products and addresses the industry shift from complex CLI-based management to simplification, automation, and consolidated graphical management of network and security assets. Juniper Sky Enterprise enables zero-touch provisioning with drastically decreased requirements for learning Junos OS. However, clients with existing Junos skill sets have full access to the CLI. Juniper continues to align its products with a security focus under the Software-Defined Secure Networks (SDSN) banner, which provides automated and centralized security policy definitions through the Juniper Policy Enforcer engine. SDSN utilizes all Juniper switches, routers, and firewalls for security profiling and threat detection, while integrating directly into Juniper Sky Enterprise cloud platform. Juniper offers campus switching under the EX product line, although its campus switch revenue grew only 0.7% in 2017. Juniper continues to expand its ecosystem of partners, which includes Aerohive and HPE (Aruba) for wireless LAN infrastructure. Wireless device profiling is supported via third-party ecosystem that includes Aruba ClearPass, Cisco Identity Services Engine (ISE), ForeScout, and others; however, security behavioral analytics are available through Juniper Sky ATP.

Juniper's consolidation of its product portfolio into a cloud management platform and integration of automated security structures across its products provide for a suitable network architecture at both the midsize- and large-enterprise levels. Midsize and large enterprises should evaluate Juniper for wired switching opportunities or for unified access networking for organizations whose WLAN

requirements can be met by Juniper's WLAN partners, including Aerohive, Samsung, Mist Systems, LANCOM Systems or HPE (Aruba).

Strengths

- Juniper Sky Enterprise provides much needed cloud-managed management and configuration capabilities such as zero-touch provisioning to SRX, NFX and EX Series devices.
- SDSN functionality extends across networking products thereby centralizing and automating security policy in addition to providing real-time threat detection.
- Junos Fusion provides switch aggregation to support integrated management of multiple campus switches as a single logical device.

Cautions

- Juniper's wireless strategy relies on partners such as Aerohive and Aruba. This strategy limits the control Juniper has over its wireless technology roadmap, potentially delaying integration of customer-required features into its management tools such as SDSN and Juniper Sky Enterprise.
- Customers requiring a unified wired and wireless access experience cannot get it from Juniper due to its lack of in-house-branded wireless products.
- Customers adopting the new Sky Enterprise platform will be among the first to put it through varying production scenarios and scales, often for the first time until the platform builds up a solid in-production track record.

LANCOM Systems

LANCOM Systems' wired and wireless access layer portfolio provides basic connectivity plus most essential management features, (such as automated network configuration, monitoring, onboarding and guest access) running on the company's proprietary LCOS operating system. Enterprises can operate a unified access network using either stand-alone, controller-based or controllerless architecture, managed by the LANCOM Management Cloud (LMC) solution, deployed either on-premises or in LANCOM's multitenant public cloud.

LANCOM provides limited multivendor functionality. LANCOM provides a REST API enabling third-party developers to access monitoring data gathered by LMC to use for advanced network analytics and other functionality.

Unlike the larger vendors in this research, LANCOM does not provide a dedicated policy enforcement application or security appliance. This requires enterprises to implement policy enforcement using a combination of LCOS features included with all LANCOM devices, such as dynamic VLAN

assignment, LANCOM Enhanced Passphrase Security (LEPS) feature, RADIUS client and RADIUS server.

Organizations in LANCOM's primary vertical markets of retailing, education and hospitality, and located in its core EMEA region, can consider the vendor for basic unified access layer requirements.

Strengths

- LANCOM's wired and wireless LAN portfolio is competitively priced with larger competitors for comparable hardware or network application capabilities.
- LANCOM's LN-830E Wireless APs with integrated Bluetooth and proprietary Zigbee radios are the basis of the vendor's IoT containment technology, using the AP as a gateway aggregating and segregating traffic from IoT endpoints. The solution currently is limited to LANCOM's ePaper digital signage and labeling solution.
- The vendor includes software updates for its wireless APs, switches and controllers in the purchase price.

Cautions

- LANCOM's business is concentrated almost exclusively in EMEA. Enterprise customers outside of this region should ensure the vendor will be able to provide an appropriate level of support both geographically and for their specific networking requirements.
- LANCOM's product strategy emphasizes integration of SD-WAN and wired/wireless LAN through its Management Cloud. This may limit the appeal of its solutions to organizations whose roadmaps do not prioritize this integration.
- LANCOM does not currently support 802.3bz. Organizations that require full performance from an 802.11ac Wave 2 solution using existing cabling will have to wait until LANCOM releases its 802.3bz switches and wireless APs, currently scheduled for year-end 2018.

Mist Systems

Mist Systems continues to be one of the smaller vendors covered by this research, while growing its total revenue tenfold in 2017. Mist offers a portfolio of wireless components that are typically delivered as a service in the cloud. Customers requiring wired switching for a unified access layer solution must buy compatible, partner-supplied switches through Mist. Mist dual radio access points have 16 integrated antenna elements for BLE and collect more than 100 different user states, which are processed through an unsupervised machine learning engine. Mist's AI-driven Wi-Fi provides guest access, network management, policy applications and a virtual network assistant as well as analytics, IoT segmentation, and behavioral analysis at scale. Mist provides indoor location capabilities and virtual BLE beacon functionality for wayfaring applications and asset management.

The Mist architecture also allows it to leverage artificial intelligence technology for proactive operations, predictive recommendations, and rapid troubleshooting required to provide network assurance and automation.

Given Mist's sixfold expansion of its global sales organization and a reseller channel with more than 200 partners, enterprises can assess Mist's capabilities for meeting wireless-focused access layer opportunities globally.

Strengths

- The Mist management team's vision matches Gartner's view of emerging customer requirements, with a strong product strategy, and has executed strong revenue growth and sales expansion to support global opportunities.
- The Mist wired and wireless access layer solution uses an in-line AI engine called Marvis, which includes a patented dynamic packet capture and unsupervised machine learning to automatically identify, adapt and fix network issues.
- Mist has an indoor location solution that provides one-meter to three-meter granularity and virtualizes BLE beacons, eliminating the need for physical battery-powered beacons.

Cautions

- Mist continues to grow rapidly and can deploy updates as often as weekly, which may disrupt network performance or operations. Clients should set up testing environments to ensure there are no changes to functionality that require additional process changes or training.
- The focus of the Mist solution is cloud-based service delivery. Organizations that need on-premises or private cloud capabilities should test the functionality as part of the evaluation process.
- Mist uses partners to provide vertical market functionality for IoT or OT solutions such as Time-Sensitive Networking. Organizations in these vertical markets should test the end-to-end solution.

Mojo Networks

Mojo Networks offers a wireless-focused, cloud-managed access layer infrastructure with its portfolio of access points, access layer applications and a limited lineup of wired switches. While focused in North America, Mojo has a global customer base, direct sales staff and distribution partners. The cloud-managed Cognitive WiFi solution has been optimized for large-enterprise networks, as well as higher education and K-12 markets, but has the ability to be deployed on-premises if needed. As a software-defined solution, Mojo has the industry-leading ability to create a digital twin of an existing client network in the cloud and test configuration changes or new code revisions in a digital "sandbox." Clients will find their options limited with Mojo, however, if they

require more features than offered by Mojo's basic portfolio of three fixed-format Ethernet switches, or require an on-premises access network management solution.

As one of the smaller vendors covered in this research, Mojo Networks shipments increased approximately 25% year over year in fiscal-year 2017.

Evaluate Mojo Networks in North America for all wireless cloud-based access layer connectivity projects and globally through distribution partners that provide the required ability to support installations.

Strengths

- The ability to deploy the solution in the cloud or on-premises provides the flexibility that is needed by many organizations.
- Federal Information Processing Standard (FIPS), Common Criteria and Federal Risk and Authorization Management Program (FedRAMP) certifications provide the ability for Mojo to be used for U.S. Federal opportunities that have these requirements.
- Network analytics is provided within Mojo Cognitive WiFi, with the machine learning and big data platform tracking more than 300 KPIs.

Cautions

- Mojo has a limited IoT segmentation/containment strategy and limited UEBA for discovery, onboarding and management. Organizations must evaluate Mojo's capabilities and whether ecosystem partners can provide an end-to-end solution.
- Mojo does not currently support 802.3bz and has no short-term plans to fill this gap. Organizations looking to do switch refreshes as part of an 802.11ac Wave 2 solution will have to look to other switch offerings.
- Many of the Mojo network and security applications are targeted toward "wireless" clients including wireless intrusion prevention system (WIPS), network analytics and management. Clients deploying an end-to-end solution using Mojo's limited portfolio of campus switches need to ensure that the appropriate functionality is also available for wired clients.

New H3C

New H3C provides a full portfolio of access layer networking hardware and software primarily to customers in its home market of China. The company was formed by the 2016 acquisition of a 51% stake in HPE's former H3C subsidiary by Unisplendour, a subsidiary of Tsinghua Holdings.

A full range of products includes the WA5600 802.11ac Wave 2 access point and the S5150-EI fixed-format campus switch, each with a 2.5G Power over Ethernet (PoE) port to support full Wave 2

uplinks. Users employing the intelligent Management Center (iMC) for unified wired/wireless management add further functionality with a series of modules for applications such as user and device profiling, policy enforcement, network traffic analysis, and management of quality of service (QoS) configurations. Network analytics and assurance monitoring for on-premises deployment also requires the vendor's WBC access controller.

Although its target customer base includes service providers and smart city deployments, New H3C corporate vertical markets include education, healthcare and government sectors. Clients with Asia/Pacific access layer opportunities can consider New H3C for enterprise campus and branch office deployments.

Strengths

- The Oasis platform provides wireless management from the cloud, including data analytics and basic device/user behavior analysis in a multitenant environment.
- New H3C has grown substantially faster than the market for both campus Ethernet switch and WLAN revenue, despite being restricted, so far, primarily to sales in China.
- New H3C has a strong foundation in switching, with a broad portfolio of fixed form and modular switches at competitive pricing.

Cautions

- Under the agreement with HPE creating New H3C, the vendor is largely limited to selling networking solutions in Greater China. Organizations outside of that market should require detailed documentation regarding the level of vendor or partner support for implementation and postsale service and support available at their locations.
- The Oasis cloud managed network platform is offered only in China, with a lack of overseas application cases for private cloud that limits its appeal to organizations outside the region.
- Clients will find that, despite updates to New H3C's CUPID indoor location service platform to integrate data from both Bluetooth beacons and Wi-Fi, the vendor has few partners outside of China, limiting the development of location applications outside of the region.

Riverbed

Riverbed acquired Xirrus in April 2017 and has integrated that vendor's wireless capabilities into its existing application-focused network infrastructure and performance management portfolio. Postintegration into Riverbed, wireless management is maintained through the pre-existing Xirrus Management System Cloud (XMS-Cloud) or on-premises with the XMS-Enterprise platform. Xirrus now has been integrated into the SteelConnect switch platform, which aligns the wireless suite with Riverbed's SD-WAN application routing engine to offer application prioritization and routing

capabilities seamlessly from the edge into the campus wireless network. Xirrus WLAN is also integrated with SteelCentral Aternity for end-user experience visibility. With a history of deployments in different verticals, Xirrus access points can be deployed via zero touch, thereby reducing time to deploy and optimizing large wireless networks. Xirrus' EasyPass integration enables intuitive self-registration of BYO devices for enterprise users as well as guest device access requiring no intervention from network administrators. Additionally, organizations can onboard headless IoT devices via EasyPass. EasyPass also provides native integration with Microsoft Office 365 and Google App accounts for single sign-on (SSO) functionality for enterprise users.

Riverbed can be considered globally as an enterprise branch office wired and wireless access networking option.

Strengths

- Xirrus aligns well with Riverbed's historical deep application visibility by providing similar application management functionality on the WLAN portfolio. Applications can be prioritized, throttled and excluded according to policy. Configuration is via the XMS-Cloud-based management or the SteelConnect cloud and on-premises management platforms.
- Riverbed provides strong automated onboarding tools for enterprise end users, guests, BYOD, and IoT devices via EasyPass, which has native integration via Office 365 and Google SSO.
- The vendor's WLAN access points have a proven track record in high-density and challenging wireless environments and now provide complementary application prioritization functionality to Riverbed's SD-WAN product through the common SteelConnect interface.

Cautions

- Clients with legacy Xirrus WLAN deployments predating the Riverbed acquisition must ensure the vendor provides sufficient product integration support, given these are the initial set of integrations between Riverbed Xirrus and SteelConnect product families.
- Despite offering some attractive features, SteelConnect access layer switches do not offer the robust backplane bandwidth required to support higher-demand application traffic at high port densities.
- To ensure the ongoing integration of SteelConnect with legacy products meets their requirements, legacy Xirrus customers must exercise due diligence in monitoring Riverbed's sales, future support and product roadmaps.

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

LANCOM was added for the first time this year.

Dropped

No vendors were dropped from the 2017 Magic Quadrant. The entry for Brocade (Ruckus) has changed to ARRIS (Ruckus), given that ARRIS completed its acquisition of Ruckus in 2017.

Inclusion and Exclusion Criteria

To qualify for inclusion, the vendor needs to:

- Demonstrate relevance to Gartner clients in the enterprise access layer market by offering switching and WLAN hardware to address enterprise access layer networking requirements outlined in the Market Definition section.
- Demonstrate relevance to Gartner clients in the enterprise access layer market by providing one or more network service applications as outlined in the Market Definition section, with an annual network service application revenue exceeding $10 million.
- Produce and release enterprise access layer networking products for general availability as of 15 February 2018. All components must be publicly available, shipping and included on the vendor's published price list. Products shipping after this date will only have an influence on the Completeness of Vision axis.
- Have at least 50 enterprise customers that use its access layer networking products in production environments as of 15 February 2018.
- Demonstrate production enterprise customers with at least five reference customers supporting access layer networks of more than 100 access points.

Additional Vendors

There are several additional vendors that garner interest from Gartner clients or that could impact this market over time. These vendors do not currently meet our inclusion criteria, but they can address enterprise access layer connectivity in certain usage scenarios. In some cases, these vendors sell to customers outside the traditional IT organization. Specific players we track include:

- ADTRAN
- Arista Networks

- Cloud4Wi
- Pica8
- Sundray Technologies
- TP-Link
- Ubiquiti Networks
- Zyxel Communications

Evaluation Criteria

Ability to Execute

Gartner evaluates technology providers on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to have a positive effect on revenue, retention and reputation within Gartner's view of the market. Technology providers are ultimately judged on their ability and success in capitalizing on their vision.

Product/Service: We evaluate vendors for completeness of their access layer infrastructure products and services consisting of switches, access points and related components such as external antennas and outdoor enclosures needed for the end-to-end solutions in various vertical markets. We evaluate network service applications such as management, monitoring, guest access, policy enforcement, location, network analytics and security applications. We consider product differentiation and architectural migration strategies from legacy implementations, whether there is an incumbent vendor or a new solution provider. We also look at maintenance and deployment service capabilities across the global landscape.

Overall Viability (Business Unit, Financial, Strategy and Organization): Viability includes an assessment of the organization's overall financial health, and the financial and practical success of the business. We also evaluate whether the organization continues to invest in access-layer-related business, including technology and product development, as well as solution delivery to the market, including sales channels, marketing communication and service delivery.

Sales Execution/Pricing: This involves the vendor's capabilities to understand client needs and communicate differentiation, as well as the direct and indirect channel sales structure to support client opportunities. This criterion includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel, both direct and indirect.

Marketing Responsiveness and Track Record: This includes the ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, and customer

needs evolve, and market dynamics change. This criterion also considers the vendor's history of responsiveness to changing market demands.

Marketing Execution: This criterion focuses on how the vendor is perceived in the market, and how well its marketing programs are recognized. For access layer infrastructure, the evaluation focused on the clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. An additional indicator for this criterion is how often Gartner clients consider a vendor as a possible supplier in a shortlist evaluation. The change in momentum in this indicator is particularly important.

Customer Experience: How do customers view this vendor? This evaluation includes significant input from Gartner clients in the form of inquiries, face-to-face meetings and written responses about the vendors. A key component in this category is the vendor's ability to provide strong presales and postsales support, especially aligned with vertical requirements.

Operations: This criterion was not ranked.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	High
Customer Experience	High
Operations	Not Rated

Source: Gartner (July 2018)

Completeness of Vision

Gartner evaluates technology providers on their ability to convincingly articulate logical statements about current and future market directions, innovation, customer needs and competitive forces, as

well as how they map onto the Gartner position. Technology providers are ultimately rated on their understanding of how to exploit market forces to create opportunities for themselves.

Market Understanding: Does this vendor's marketing message articulate a clear, understandable message that answers the market requirements for technologies and services? Do the vendor's message and supporting products lead the access layer market requirements or merely fulfill them? Are vendors focusing on building their core competencies, or are they investing in random technologies?

Market Strategy: We evaluate the vendor's ability to look into the future and drive/influence the direction of the market through product roadmaps and offerings. We also look at its ability to provide clear, differentiated messaging consistently communicated internally, externalized through social media, advertising, customer programs, and positioning statements. Are the issues that are being addressed meeting the trends in the market and the needs of end users?

Sales Strategy: Does the vendor have a sound strategy for selling that uses the appropriate networks, including direct and indirect sales, marketing, service, and communication? Does it have partners that extend the scope and depth of market reach, expertise, technologies, services and the customer base?

Offering (Product) Strategy: Does the current and future planned product line meet the needs of buyers now with differentiable functionality, and how will it do so in the future? Is the vendor simply building products that the buyer is asking for, or is it anticipating the issues that those buyers will face and allocating resources to address them?

Business Model: We evaluate the design, logic and execution of the organization's business proposition to achieve continued success. Specifically, we look for whether the business model meets the needs of the target market and provides growth for the vendor.

Vertical/Industry Strategy: Do the vendor's strategy, direct resources, skills and offerings meet the needs of market segments, including vertical industries? In this market, can the vendor differentiate itself with solutions that are specifically developed for the unique requirements of targeted verticals, such as healthcare, logistics, manufacturing, retail and hospitality?

Innovation: What has the vendor done to address the future requirements of access layer infrastructure, including the need for tighter integration with wired networking products, voice, video and application visibility support? Is there innovation in the access layer applications that address client needs for easier installation or onboarding, as well as better management? Has the vendor successfully differentiated the current and future product lines to better address customer requirements, both now and two to five years out?

Geographic Strategy: Can the vendor meet the needs of global enterprises for products and support?

Table 2: Completeness of Vision Evaluation Criteria

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

Source: Gartner (July 2018)

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 access layer product family. Leaders will have the ability to shape the market and provide complete and differentiating access layer 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 no obvious gaps in their portfolios.

Challengers

A vendor in the Challengers quadrant will have demonstrated sustained execution in the marketplace, and will have clear and long-term viability in the market, but may not have a complete access layer product portfolio for either products or network applications. Additionally, Challengers may not have shown the ability to shape and transform the market with differentiating functionality.

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 access layer technologies within the enterprise (for example, security,

management or operational efficiency). The ability to apply differentiating functionality across the entire access layer 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 solution, 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

The enterprise access layer is a critical component for enabling organizations to respond rapidly to the demands of digital business. Gartner clients consistently report that the wireless LAN, especially, has moved well beyond "nice to have" connectivity to become increasingly the user's first or primary connection with the enterprise network. Organizations now require the campus or branch office access network to support an increasing number of devices per user for corporate applications, video or voice services, plus a growing number of Internet of Things endpoints. The WLAN provides greater deployment flexibility than the wired LAN for expanding the network's reach and quickly providing connectivity for new users, devices and usage scenarios.

Infrastructure vendors are attempting to keep pace with this evolving market, but their capabilities for providing unified wired and wireless solutions for doing so can be inconsistent. Over the past year, Gartner has seen a relatively low level of execution on access layer innovation in key areas such as IoT-specific support and automation of network management. This, in the context of the Magic Quadrant, means many vendors currently are positioned as Niche Players (see the Niche Players section). All vendors can support basic access layer connectivity via their campus network switches and wireless access points. They vary in providing "check the box" capabilities — such as access control, management and monitoring, basic guest access, security and policy enforcement — through their network services applications. However, enterprises are differentiating vendors based not only on the features and functionality of those applications, but also on a vendor's currently ability and its roadmap for incorporating more intelligence in the access layer. This enables collection of data not only from the network but also from user devices and applications. This data will be used:

- To feed machine learning engines that will drive more efficient or automated solutions for monitoring and assuring local access network performance
- For enabling more agile security in the face of growing threats
- For supporting the required user experience for applications such as voice and location-based services

Vendors also can meet enterprise requirements for providing LAN management tools as cloud-based or on-premises solutions, but face challenges in supporting hybrid environments that may require an organization to use cloud for some locations and on-premises for others.

Market Overview

Gartner's view of the market is focused on transformational technologies or approaches delivering on the future needs of end users. It is not focused on the market as it is today. Gartner research shows that global enterprise wired and wireless campus networking revenue grew by 7.78% in 2017, driven by 10.7% growth in WLAN hardware and software (see "Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q17 and 2017"). Gartner forecasts that WLAN will continue growing at high single-digit compounded rates through 2022, as organizations continue to seek more network agility given proliferating numbers of devices connecting to the enterprise network due to BYOD policies and implementation of IoT initiatives (see "Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2015-2022, 1Q18 Update"). During the evaluation period for this Magic Quadrant, few products were available supporting 802.11ax. This latest iteration of IEEE standards for WLAN increases throughput speeds in densely populated areas by improving the efficiency of existing 2.4GHz and 5GHz spectrum over 802.11ac Wave 2 (see "Hype Cycle for Mobile Device Technologies, 2017"). Wave 2 access points accounted for 92% of global revenue in 2017.

Machine Learning and Automation

Gartner is seeing an emerging trend of vendors incorporating machine learning algorithms in network management and monitoring tools to automate access layer connectivity. Increasingly, vendors are adding value to the access network infrastructure with applications that consume data generated at the network edge and feed it into machine learning engines that can extract knowledge from that data. The long-term vision vendors are beginning to execute now is to utilize this knowledge to incorporate more automation into the access layer. This will support: more rapid service delivery (such as deployment or expansion of branch office Wi-Fi); location-based applications with improved location granularity; and proactive, potentially automated management of the network fabric to meet enterprise user requirements for high performance and availability. Mining big data to identify patterns indicative of potential security threats is another key potential use case. Automation enabled by machine learning and network configurations based on network and business policies eventually will drive intent-based solutions that will be self-monitoring to ensure that the network actually meets the intent of the policies set at configuration time.

Cloud-Managed LAN/WLAN

Architectures with cloud-managed networking capabilities have become a standard element of vendor infrastructure portfolios to meet client preferences for the ability to deploy network service applications on-premises, or in a public or private cloud. However, specifications for many client access network greenfield deployments and network refreshes do not necessarily mandate a cloud-

managed solution; clients still widely require on-premises options. There is also inconsistency in how closely vendor cloud architectures map to the features and functionality of their on-premises options. Further, Gartner continues to see client preference for cloud-managed architectures to serve branch office rather than campus deployments. When cloud-managed is the choice, many clients want to look beyond proprietary products that create vendor lock-in and integration challenges. Vendor differentiation is also apparent in whether the cloud versions of network service applications share all the features and functionality of the on-premises versions.

IoT and IT/OT Convergence Drive Client Requirements

Enterprise demands for access network performance, manageability and availability are increasing as more attach large numbers of new endpoints for Internet of Things implementations. Gartner estimates that, by 2020, 80% of new IoT projects will require wireless connectivity, with many of those "things" attaching via the WLAN. This is continuing to drive vendor innovation for software services to enable these deployments, including:

- Virtual segmentation and access control of "headless" IoT endpoints to ensure security
- Network management for configuration and onboarding of potentially large numbers of devices
- Monitoring of the devices' impact on network performance

The capability of a vendor's network management solution to effectively contain IoT devices from the access network connection to the data center has become a key focus area for software development. Simultaneously, customers will require vendor strategies to serve the need for unprecedented cooperation between IT and OT organizations that will be necessary to efficiently manage and secure operational things attached to the LAN, while analyzing and monetizing the new sensor data they produce.

Enterprise Requirements Focus on Network Application Services

Software has created greater vendor differentiation than hardware, which provides similar basic connectivity from all vendors. This places greater client value on the end user-facing applications needed to configure, secure, manage and automate the infrastructure. Network service application choices made for the wired and wireless LAN impact other enterprise end-user applications, such as unified communications and collaboration platforms, as increasingly mobile work styles depend on wireless access to those platforms and are affected by network performance. Enterprises also want greater insight into security and monitoring due to the diversity of client devices using the network, which started with BYOD and guest access scenarios but expanded to IoT devices.

The focus on network service applications is becoming especially true in outsourced managed LAN scenarios. The customer may focus more on the network assurance capabilities that the provider

offers — and the SLAs for supporting a specific user experience — than on the listed throughput, capacity or antenna specs for the deployed infrastructure.

Consolidation Positions New Enterprise Vendors

The corporate consolidation wave that accelerated in 2016 saw numerous combinations completed in 2017 as vendors began integrating their acquisitions and targeting new or expanded enterprise business. ARRIS completed its acquisition of Ruckus Wireless and the Brocade ICX switch business and stated a goal of growing enterprise networking business beyond its core cable multisystem operator (MSO) segment. Extreme Networks acquired Avaya's networking business from that company's parent bankruptcy reorganization. And Riverbed Technology acquired Xirrus in April 2017, significantly expanding its WLAN portfolio.

Software-Defined Access Network Is Not Here Yet

Several network infrastructure vendors have begun using the terms SD-LAN or SD-WLAN to describe their approach to or the capabilities of their access network product portfolio. However, Gartner has not yet defined SD-LAN as a distinct product or architecture (see "State of SDN: If You Think SDN is the Answer, You're Asking the Wrong Question"). Currently, it is primarily a marketing term by vendors in describing how they have (or plan to) incorporate software-centric attributes into their access networking solution.

Our research so far indicates that what a vendor calls "SD-LAN" may or may not actually be based on an SDN architecture. Many products described as SD-LAN are not based on an SDN architecture, but are instead using SD-LAN to describe some combination of attributes, often including

- API-based manageability
- Cloud-based management
- Virtualization of controller functions
- Automated network configuration and management features, such as self-optimization/healing
- Policy-based management

Gartner clients express interest in solutions that utilize automation and zero-touch configuration to reduce management overhead in deploying and operating the LAN; but, in 1H18, they generally were not asking for the wired/wireless LAN equivalent of SD-WAN. Nevertheless, we expect vendors to continue developing greater integration of the infrastructure to manage the both the access network and the WAN via a single hardware and software platform.

Evidence

This Magic Quadrant is a reflection of a broad-based research effort involving:

- More than 500 inquiries during the evaluation period with Gartner clients about their needs and requirements for wired and wireless access network infrastructure; their vendors; RFPs and purchase proposals.
- In-person discussions and other interactions with the vendors within this Magic Quadrant.
- A detailed vendor survey requiring responses to more than 50 questions.
- A Gartner survey of client references provided by the vendors.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."