

Six Building Blocks of a Next-Generation Software-Defined Campus LAN

Table of Contents

Introduction	3
Six Key Components of a Next-Generation Software-Defined LAN	4
Wireless LAN	4
Ethernet LAN	6
Security	7
Management and Orchestration	8
Zero Trust	8
Artificial Intelligence and Machine Learning Integration	10
Total Cost of Ownership	12
Conclusion	13



Introduction

Digital acceleration, defined by initiatives that include ubiquitous connectivity, migration to the cloud, and investment in next-generation networking technologies, has driven many advancements in the IT industry. Wired and wireless networks are no exceptions. The local-area network (LAN) wired and wireless forms the backbone of IT, enabling next-generation applications and increasing user productivity. The LAN greatly impacts user experience and is the beginning or end of many security events that occur at the enterprise. As IT administrators look to build next-generation networks, they are focusing on ensuring a secure, seamless user experience. As such, network architects have settled on six key building blocks to achieve the next-generation software-defined LAN. It's important to consider total cost of ownership (TCO) as well as the elements listed below.



Six Key Components of a Next-Generation Software-Defined LAN

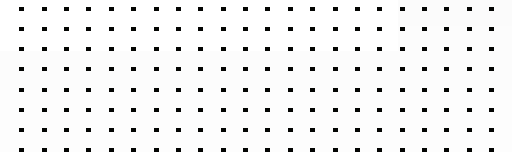
Wireless LAN

Wireless is the dominant method of access for LAN clients. This is due to the mobility and flexibility the technology affords. As administrators consider wireless solutions, reliability and performance are key metrics but not the only metrics that should be considered for next-generation LANs. Wireless networks are asked to support higher-density environments more than ever before. They must be able to utilize the latest technology to improve RF spectrum optimization to deliver both the speed and mobility users expect. Guest access is expected in all enterprise environments and is typically facilitated by guest Wi-Fi, so the need to both secure and manage this access is a must for a next-generation solution. Lastly, a wireless network should not operate in a silo. It should be part of an integrated access-layer solution to simplify and enable both the user and administrator experience.





According to recent research, many organizations (45%) planned to upgrade their Ethernet or Wi-Fi networks to newer standards over the next two years.¹



Ethernet LAN

Ethernet is the most mature of the LAN access technologies. Wireless becoming the dominant access method may lead some to mistakenly neglect to focus on Ethernet switching. The key capabilities to consider are listed below.

Scalability. The solution must grow along with the organization without increasing complexity, so scalability is very important. The demand for speed and bandwidth continues to increase as next-generation wireless technology funnels ever larger traffic flows to the wired network, which forces upgrades to meet the need. Next-generation Ethernet LANs need to support higher speeds such as 10 Gigabit and 100 Gigabit, as well as multi-Gigabit 2.5 and 5 GE access.

Power over Ethernet (PoE). Ethernet switching is increasingly being used as a power source for everything from wireless access points to Internet-of-Things (IoT) devices and smart lighting solutions. A next-generation Ethernet LAN should offer higher PoE-powered options such as PoE+ and PoE++ 803.3bt, which can offer up to 60W of power to enable business technology.

Integration. Interoperability and integration with wireless, the other dominant access method, should be a key requirement. The user experience should be the same whether connecting to wired or wireless, as should the security.

“Today, 92% of organizations use switches capable of maximum Ethernet speeds of 1 GbE or faster in the workplace; and 42% of organizations use 10 Gigabit or faster Ethernet networks.”²



Security

Many security events begin at the wired and wireless LAN edge because this is where the user and endpoint connect. Malware, phishing, and many other exploits all start with a user's click and then propagate into the network to infect other hosts or compromise valuable data.

The LAN access layer and the clients that connect are also the end for many attacks that start outside of the physical location. This means that any next-generation LAN should have advanced security integrated by default. Segmentation to limit the scope of successful attacks must be easy to implement and manage. This segmentation should not rely on just Layer 3 and 4 VLANs but be able to enforce policies through Layer 7 to ensure maximum protection at the LAN access edge.

“Many security incidents start on end-user workstations, because employees click on phishing links or their systems become compromised by other means.”³



Management and Orchestration

Deployment and day-to-day management of the wired and wireless network can be dynamic and time-consuming. Deployment can require labor-intensive individual configuration of Ethernet switches before they can be integrated into a network.

Wireless LAN controllers centralize configuration of wireless access points, but are rarely integrated with or have visibility into the wired network to which it, and the access points it supports, are connected. Next-generation software-defined LAN should offer unified management and orchestration, not only of the wired and wireless access layer, but for the security controls that make that network safe.

Zero-touch provisioning is also required to create a solution that is simple and agile to deploy and manage. To meet the promise of “software-defined,” a centralized controller with a common interface must be able to deploy and manage the core features of the network. These include wired, wireless, and security.

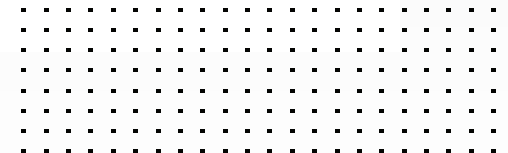
Zero Trust

The ability of a next-generation LAN to identify what is connected to the network is key in implementing zero trust. The LAN must be able to identify corporate and IoT devices and determine their level of privilege or network access. While users can have their roles determined through authentication, IoT and other headless devices (which compose a large share of attached network devices) often do not have the ability to authenticate. A next-generation LAN should be able to automate identification and onboarding of these devices, implementing least-privileged access segmentation to minimize their threat and maximize their potential benefits.





Of the 21.7 billion active connected devices worldwide in 2020, 11.7 billion (54%) are estimated to be IoT device connections.⁴



Artificial Intelligence and Machine Learning Integration

The latest innovations at the LAN edge involve the use of artificial intelligence (AI) and machine learning (ML). AI/ML can automate the more tedious tasks of an IT administrator or help desk. By gathering data from network elements, AI/ML can shorten the time to resolution or prevent issues before they occur, through proactive tuning. These enable IT teams to be more strategic and proactive rather than reactive. However, not all of these tools are made equal and the success of AI/ML is directly tied to the type and quality of information it receives. AIOps is a valuable, and for some, necessary tool for managing enterprise networks. Use of this technology should be a consideration during the evaluation stage.

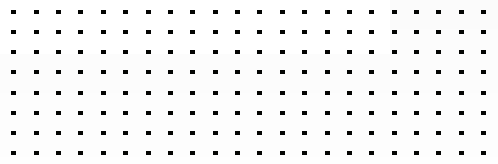

IDC predicts that over 60% of large enterprises worldwide will rely on advanced AI capabilities to automate at least one part of their enterprise network by 2024.⁵





52%

of [infrastructure and operations] I&O organizations selected “lower costs” as one of the top three important goals for the next 12 months.⁶



Total Cost of Ownership

The LAN is the backbone of IT infrastructure and includes some of its most mature technologies. Historically, the initial capital expenditures were to purchase and deploy hardware, but as demands and requirements have changed, LAN vendors increasingly commodify all aspects of the LAN—even the operating systems.

Careful consideration must be made not just for the cost of the hardware, but the ongoing costs of licensing and support that accompany many of today's solutions. Things to avoid include:

- Licensing without clear value
- Complex licensing that does not make sense
- Licensing fees that change over time
- Licensing fee lock-in

Any quote for a next-generation LAN solution should offer a clear and easy-to-understand quote for both hardware and licensing.



Conclusion

Digital acceleration is making today's LAN work harder and smarter. To achieve a next-generation software-defined LAN, the building blocks listed above must be included. Ensuring the LAN is secure and keeps up with user demand for a fast and seamless experience is key. At the same time, it must be easy to manage and maintain a low total cost of ownership.

¹ ["Networking Technology Trends in 2020 and Beyond,"](#) Spiceworks Ziff Davis, accessed February 10, 2022.

² Ibid.

³ John Edwards, ["How microsegmentation can limit the damage that hackers do,"](#) Network World, April 16, 2020.

⁴ Knud Lasse Lueth, ["State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time,"](#) IoT Analytics, November 19, 2020.

⁵ Brandon Butler, et al., ["IDC FutureScape: Worldwide Enterprise Network Infrastructure 2020 Predictions,"](#) IDC, October 2019.

⁶ Chris Howard, ["Top Priorities for IT: Leadership Vision for 2021,"](#) Gartner, 2020.



www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.