



Prepared for



Hybrid Work Requires Network Transformation

May 2022 EMA White Paper
By Shamus McGillicuddy, Vice President of Research

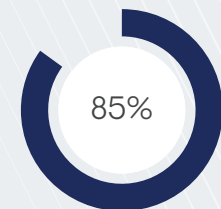
The Rise of the Hybrid Work Era

Hybrid work, or working from anywhere, is the future, and the future has arrived. The pandemic mainstreamed it, but the benefits of hybrid work will ensure it sticks around. According to Enterprise Management Associates (EMA) research, 85% of companies have experienced a permanent increase in the number of employees who work from home at least part time.¹ Note the word “permanent.” Companies have clearly recognized that hybrid work has business benefits that deliver value indefinitely.

In the world of hybrid work, many people split their time between working from home and the office, as one network engineer with a large American insurance company explained to EMA. “After the pandemic, we expect about 70% of people will go into the office only two or three days a week.”

The pandemic has changed more than where people work. It’s changed how they work—specifically, the applications they use and the space they work within. It’s changed their tolerance for health risk, too.

With hybrid work as the new normal, network infrastructure and operations teams must adapt their corporate networks and their network management tools and practices to support this reality. They must upgrade and optimize their networks to address more bandwidth demand, mobility, and cloud access. They must also transform operations with automation, a focus on security beyond corporate borders, and insights into the work-from-home user experience.



of companies have experienced a permanent increase in the number of employees who work from home.

¹ Unless otherwise noted, all statistics cited in this paper were originally published by EMA in the July 2021 research report, “Post-Pandemic Networking: Enabling the Work-From-Anywhere Enterprise.”

The Impact of Hybrid Work on Corporate LANs

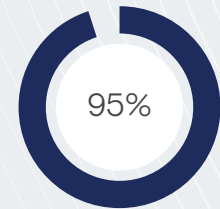
New Applications

The massive shift to hybrid work changed how people collaborate and communicate. Voice, video, and screen-sharing applications are now essential to collaboration, no matter where a person is working. In fact, 95% of enterprises report that hybrid work has increased the volume of real-time communication traffic on their networks.²

EMA expects usage of real-time applications to remain elevated, even as people return to office settings. Hybrid work created a permanent culture of collaboration via real-time applications as a person's location becomes less predictable. This shift in application usage goes beyond information workers who traditionally worked in carpeted enterprises. Doctors are embracing telemedicine. Retailers are communicating with customers via video. Schools and universities are embracing hybrid learning.

Cloud applications also have exploded with hybrid work. More than 70% of enterprises report that the pandemic accelerated the migration of applications to the cloud. Because latency can increase when applications migrate from on-premises data centers to the cloud, enterprises must modernize their networks to mitigate its impact. Local-area networks need to be optimized to efficiently deliver traffic to the WAN edge, and the WAN must be optimized to get traffic to the cloud. Any minor local network issue can have a major impact on cloud application performance compared to applications delivered via a local or regional data center.

Networks must also account for the fact that on-premises workspaces are fundamentally different in the hybrid work era. Hot desks are replacing permanent desks, which creates an opportunity for location-based services to help manage desk availability. Increased mobility is also a factor, and EMA expects hybrid workers to bring multiple devices to the office, which will demand higher-density network connections and improved access management. Finally, workspaces must be sustainable from an environmental perspective, but also from a public health perspective. For instance, infrastructure should address the increased health and safety awareness of workers.



of enterprises report that hybrid work has increased the volume of real-time communication traffic on their networks.

² EMA, "Enterprise WAN transformation: SD-WAN, SASE, and the Pandemic," December 2020.

New Infrastructure Requirements

EMA research found that the pandemic prompted 71% of enterprises to increase investment in on-premises LAN infrastructure. One might have expected the opposite, given that many corporate sites were empty during the first years of the pandemic. This investment suggested that hybrid work drives change in the LAN.

Another big driver of LAN investment, according to 46% of companies, is increased bandwidth demand. This includes high bandwidth Wi-Fi that can support real-time applications and high-density connectivity. It also includes high-density, multi-gigabit switch upgrades with the latest generation of Power over Ethernet (PoE) to power the next-generation Wi-Fi access points and other devices and sensors.

“We’re going to have smaller cubicles in smaller offices, so we’ll need more switching capacity and port density,” said a network engineer with a large insurance company.

“A lot of our doctor’s offices and satellite offices were having bandwidth issues because telemedicine was pumping so much video onto the network. Our [Wi-Fi] site surveys weren’t set up for that,” a network engineer with a regional hospital network recently told EMA. “Doctors were also bringing in their own devices to do telemedicine, so our BYOD program really exploded. We have to figure out how we can safely—from a compliance perspective—support and bring on all these devices. We have some pending upgrades for our wireless LAN controls and for network segmentation. Access point density needs to be increased, too.”

Forty-three percent of IT organizations said increased office mobility was driving LAN investment. This translates to high-density deployments of Wi-Fi access points with seamless handoffs as users move from hot desks to private rooms for phone calls and to conference rooms for meetings. The investments must also focus on adequate coverage throughout offices, not just conference rooms.

Internet of Things (IoT) connectivity requirements drive LAN investment for 38% of companies. This starts with Wi-Fi and switch upgrades, but it also includes additional security and compliance capabilities. Many companies need new authentication and segmentation technology, since simple IoT VLANs will no longer cover the growing complexity of IoT environments. Smart building controls need network access privileges that are quite different from industrial control systems or medical monitoring equipment. This IoT activity may also drive investment in private 5G, particularly to support the low-latency connectivity needs and network slicing demands of robotic controls and vehicle guidance systems.



46%

of companies are investing in high bandwidth Wi-Fi to support real-time applications and high-density connectivity.

Finally, 30% of companies said their need for new location-based services that support sustainable work environments drive their LAN investment. They need Wi-Fi access points with accurate location capabilities. In fact, 88% of IT organizations say the pandemic made them interested in the long-term use of location technology for addressing public health issues.

“Location-based services will be interesting for social distancing. The fear of a pandemic surge happening again is there,” a network engineer with a large insurance company recently told EMA.

The top use cases for this interest in location technology are optimizing productivity for managing desk and conference room availability (55%), enforcing room occupancy (39%), and controlling smart HVAC, such as increasing ventilation in occupied rooms (32%).

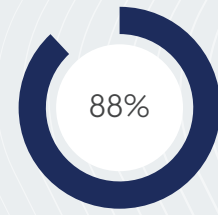
This modernization of the network requires a commensurate transformation of network management. For instance, network teams are also hybrid workers, so they need cloud-based tools that are accessible from anywhere and easy to use. They also require automation to reduce complexity and AIOps insights that allow them to be more proactive with dynamic and complex hybrid work environments.

New Security Requirements

Forty-two percent of organizations told EMA that new compliance and security requirements are their biggest challenge with hybrid work. Their policy design and implementation processes and tools are outdated. Their access controls are too rigid for flexible work environments. Also, the home office opens a whole new attack surface that must be secured.

Among enterprises that have increased their LAN investments during the pandemic, 63% told EMA that they are addressing security and compliance requirements with this spending. For instance, office mobility and bring-your-own-device policies require modern authentication, access control, and segmentation technology, along with network automation, to mitigate the complexity that comes with all this change. New network security technology may also be required.

These security and compliance investments should be easy to implement and manage, and they should support a seamless experience for users no matter where they are working.



88% of IT organizations say the pandemic made them interested in the long-term use of location technology for addressing public health issues.

Optimizing the LAN for Hybrid Work

Infrastructure Upgrades to Consider

Every company will determine its own network requirements for hybrid work, but EMA assumes that most upgrades involve the latest generation of available technology. This section explores the capabilities that will best help network architects optimize their infrastructure.

Access Layers Based on Wi-Fi 6E

Wi-Fi 6E, an extension of the Wi-Fi 6 standard for Wi-Fi technology, is now generally available from all leading vendors. Premium Wi-Fi 6E access points have triband radios that offer maximum wireless air-space for hybrid work. Wi-Fi solutions have used the 2.4 and 5 GHz frequency band for years. These frequency bands offered a relatively narrow spectrum that required overlapping channels that were prone to interference. Wi-Fi 6E triband radios support the newly opened 6 GHz frequency band, which effectively quadruples the amount of radio frequency spectrum that Wi-Fi operates within and eliminates overlapping channels. Experts expect these access points to deliver real-world throughput of 2 Gbps.

With all of the available spectrum in Wi-Fi 6E, premium access points can do more to optimize signals, provide a higher density of concurrent connections, and steer 6 GHz-capable devices to the new band while steering older devices into lower frequency bands, leading to less interference and better performance.

High-Density Switching Behind the Wireless LAN

With Wi-Fi connections set to multiply and overall throughput ready to explode, the wired network must also be modernized.

Enterprises will require high-density, multi-gigabit (2.5 and 5 Gbps) switches to provide connectivity to Wi-Fi access points. These new switches have the capacity to backhaul traffic from access points that deliver gigabit connections to clients. These switches also need to support universal PoE so they can power Wi-Fi 6E access points and IoT devices and sensors.

Most networks will also require an upgrade to the core and aggregation layer, since multi-gigabit access switches will require 100 Gbps or even 400 Gbps uplinks to handle traffic coming off the wireless LAN.

The Dual Potential of 5G

Emerging 5G solutions offer a couple of benefits to hybrid work networking. First, private 5G is an emerging class of technologies that complements and integrates with Wi-Fi for a more versatile wireless LAN. Private 5G offers lower-latency connectivity, network slicing, SIM-based security, and resiliency capabilities that are important to critical communications, such as medical equipment, industrial control systems, and public safety communications. Given the potential overlap with Wi-Fi, many network teams will look to existing switching and Wi-Fi vendors for a trusted solution.

Fixed-mobile 5G wireless services from mobile network operators can address connectivity issues in home offices, especially in regions where terrestrial internet service providers are substandard. Network teams should consider installing 5G routers in the homes of employees who are struggling with poor internet connectivity.

EMA research found that 72% of companies are considering mobile internet solutions for some home offices. Many SD-WAN vendors now offer 5G-enabled devices that extend the WAN underlay to home offices.

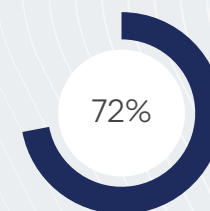
Optimize Network Management

Hybrid work requires network operations to be more agile and efficient because networks are more complex and difficult to manage. A new approach to network management is essential.

Cloud-Based Management

Optimized network management starts with cloud-based management tools. EMA research has found growing interest in cloud-based network management models. Cloud-based network management offers reduced overhead at a time when resources are constrained. No onsite hardware is needed, and the vendor manages patches and upgrades. Cloud-based tools are also easy to scale as networks grow, since no onsite tool upgrades are required.

Most cloud-based network management solutions are also extensible, with APIs and partner ecosystems enabling integrations into third-party security solutions, cloud service providers, and more. Finally, these tools are accessible from anywhere. Network managers do not have to be in a specific location to access them, allowing them to work from anywhere.



72% of companies are considering mobile internet solutions for some home offices.

Network Automation

Network teams should also embrace automation to mitigate any complexity associated with hybrid work. EMA research found that 91% of IT organizations expanded their use of network automation in response to hybrid work. This network automation spanned design, provisioning, configuration, change management, and assurance workflows. Workflows for automating segmentation and security policy design are especially critical.

These are the top six network automation use cases for IT organizations that expanded their use of automation to support hybrid work:

1. Monitoring and troubleshooting (47%)
2. Configuration and change management (33%)
3. Infrastructure provisioning (30%)
4. Device lifecycle management (29%)
5. Network design (23%)
6. Policy management (22%)

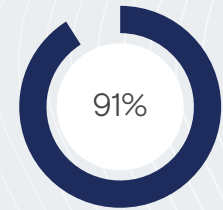
AI Ops-Driven Assurance

Network teams need better network data and actionable insights to support hybrid work. It starts with collecting the right telemetry. Home offices are hard to monitor because options for collecting telemetry are limited. Many network operations teams have adopted active, synthetic monitoring tools that can provide insight into internet and cloud performance.

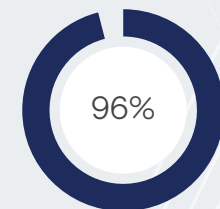
As one network engineer with a large bank said, “I don’t think we have enough visibility to support working from home. A lot of it comes down to fighting fires as they come up and not being able to get ahead. We need to fix monitoring for all users, but instead, we’re focused on fixing monitoring for just one person at a time.”

In fact, 96% of network teams have allocated budget to improve the ability of their monitoring tools to support work-from-home operations and visibility, and 42% of them said that budget would be partially spent on the collection of new types of data.

In addition to new telemetry, EMA research found that network teams need new security insights, new dashboards and reporting focused on home offices, and increased tool scalability.



91%
of IT organizations expanded their use of network automation in response to hybrid work.



96%
of network teams have allocated budget to improve the ability of their monitoring tools to support work-from-home operations and visibility.

AIOps insights are also essential to hybrid work. Hybrid workers expect a consistent user experience with their real-time communications applications as they shift back and forth from the home office to the corporate office. AIOps-derived insights can streamline and optimize operations, especially for network teams with complex toolsets.

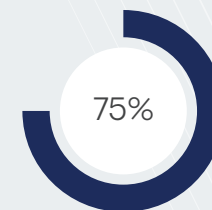
“We have lots of [diverse infrastructure] that pumps out metrics that go to various monitoring tools of varying levels of value, scalability, and usability,” said a network architect with a large retail company. “They all produce trends, alerts, and reports. It’s a massive mess. AIOps has the ability to look at all these toolsets, dump it all into machine learning, alert on it, act on it, and fix things.”

EMA research found that network managers primarily expect AIOps to help them with network optimization, operational efficiency, improved security and compliance, and network resiliency. With network operations teams increasingly focused on proactive problem prevention, they also want predictive analytics solutions that identify emerging problems before those problems impact the business.

Cross-Team Collaboration

Finally, an upgraded network management toolset should enable IT teams to work together, supporting cross-silo decision-making and workflows. One key collaboration target is cybersecurity to ensure that investments in technology, like secure access service edge (SASE) and zero trust network access, are successful. EMA research found that 75% of IT organizations have experienced increased collaboration between their network operations and security teams.³

EMA found that network and security teams collaborate most on technology, network planning and design, network implementation, and operational monitoring—all essential areas of building and operating a new network for hybrid work. Network management tools with integrated security workflows and insights are essential.



75% of IT organizations have experienced increased collaboration between their network operations and security teams.

³ EMA, “NetSecOps: Aligning Networking and Security Teams to Ensure Digital Transformation,” October 2021.

EMA Perspective

For millions of people, the nature of work has forever changed. Network teams must adapt to the new hybrid work model, allowing employees to be productive from wherever they are. Network teams need to know that it isn't just the home office that requires special attention. The corporate LAN needs an update, too.

Real-time and cloud-based applications demand more bandwidth and lower latency. The LAN must support high-density connections as users return to the office with more devices. This connectivity must be secure in response to the blurring of the network perimeter that hybrid work caused.

Managing all of this is a challenge. Network operations teams need easy-to-use tools with automation, data, and insights to ensure successful design, implementation, and management of these new networks. Network teams should also explore the opportunity of cloud-based network management tools, which are less resource-intensive and accessible from anywhere. Even if an organization isn't ready for cloud-based management today, it should plan for it in the future. Network teams should look for infrastructure solutions that can be managed via on-premises and cloud-based tools, so a future transition to cloud-based management is possible.

This white paper offers a rough blueprint for how to get started, and EMA recommends that you work closely with your trusted vendors to transform your networks for hybrid work. **Cisco Access Networking** offers many of the essential building blocks, including multi-gigabit Catalyst 9000 Series switches, Cisco Catalyst 9100 and Meraki MR57 Wi-Fi 6E Access Points, its cloud-based Meraki management solution, Cisco Catalyst 9800 Wireless Controllers, Cisco DNA Center for on-premises network automation and assurance, and Cisco's new private 5G as a service offering.

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more on [The Newsroom](#) and follow Cisco on [Twitter](#).



About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com. You can also follow EMA on [Twitter](#) or [LinkedIn](#).

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2022 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.