ESG BRIEF

Networking Predictions for 2022

Date: December 2021 **Author:** Bob Laliberte, Principal Analyst

ABSTRACT: 2021 is headed for the history books, and we now turn our attention towards the new year. The last year—well to be more precise, the last two years—have brought about significant changes in network environments as digital transformation initiatives, cloud computing adoption, edge computing and hybrid work models impact how networks are acquired, deployed, and managed. The rate of change has only been matched by the pace of innovation as network technologies rapidly evolve to deliver enhanced functionality and secure experiences. As a result, there are a number of key technologies and architectures to follow in 2022.

Introduction

Moving into 2022, there will be a number of key trends to watch. As organizations accelerate digital transformation initiatives and build out highly distributed environments, it will be important to ensure that the network is an enabler of these efforts and not an anchor holding the company back.

2022 Predictions

1. **Cloud-based network management becomes the de facto standard.**

    With remote work and highly distributed environments here to stay, it is becoming more important for organizations to become operationally efficient. In fact, that has been ESG research respondents' most-cited goal for their digital transformation (DX) initiatives for the last several years.[1] To accomplish this, operations teams need fewer dashboards to manage and tighter integration between network domains, with the ultimate goal being a unified end-to-end network management solution. We have already witnessed a lot of progress in this regard with unified wired and wireless management, with some vendors now offering unified wired, wireless, and WAN capabilities. One of the keys to enabling a unified end-to-end network management solution is to host the management software in the cloud. As organizations continue to adopt the internet as their corporate network, it will be important for them to gain visibility into this space as well.

    These cloud-based network management solutions are typically offered as SaaS solutions and as such, deliver a number of benefits to organizations. They do not need to buy servers and storage to host applications and data, and all patches and upgrades are handled by the vendor. Leveraging modern application architectures will allow network vendors to roll out new capabilities quickly and easily.

    The other significant advantage to cloud-based network management is that all network data is collected and can be leveraged to drive intelligence back into the management solution. Typically, this is done using AI/ML technologies to ensure accelerated troubleshooting and self-healing/optimization capabilities.

---

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

Vendors should expect that not every customer will be able to adopt cloud-based solutions and, as such, should architect their cloud-based network management solutions so they can be deployed in on-premises private cloud environments when required.

2. **AI/ML technologies play a more important role in network management and automation solutions.**

Providing network intelligence via AI/ML technologies will be important since, as application and worker environments become more distributed and complex, it will become increasingly difficult to effectively manage these environments manually. In no way does this imply that network operations teams are at risk of losing their jobs. Indeed, this is more about providing them with the tools to manage increasingly distributed and complex environments more efficiently.

It is also important to note that human intervention is key to ensuring AI/ML-enabled technologies are functioning properly. ESG sees organizations progress through four stages of adoption to become comfortable with the technology.

I.　**Alert.** In this stage, organizations can leverage AI/ML technologies to rapidly correlate all the network telemetry and alert operations teams immediately. The staff is then responsible for determining the best resolution to the problem.

II.　**Alert and recommend.** In this stage, the operations team is not only alerted to an issue, but is also provided with the recommended solution to fix the problem. This should dramatically reduce the amount of time spent troubleshooting—if the recommendation is correct. This is where human intervention and a feedback loop play critical roles in advancing the technology.

III.　**Alert, recommend, and automate.** After manually fixing the problem several times, operations teams should be more comfortable leveraging automation to fix the problem (when possible; this doesn't work for a bad cable). This step enables the management software to orchestrate the changes and validate that the problem is fixed. The last step is to notify the operations team (closed loop).

IV.　**Automate.** The last stage comes after the operations team is comfortable with certain tasks being fully automated. That is, when a problem is detected, the system determines the corrective action and automatically makes the changes. However, it is imperative in this stage to provide the operations teams with information about the fault, the steps taken, and a validation that the service is back online or performance has been restored.

Keep in mind that there will always be faults that require manual intervention, especially related to physical infrastructure (hardware and cabling), but the goal of leveraging intelligence is to drive greater operational efficiencies. It is also important to note that applying this technology to additional network domains (DC, campus, branch, WAN, wired, and wireless) will add more context and value.

3. **Campus and branch networks are rearchitected to support hybrid work.**

The shift to adopting hybrid work models will have a dramatic impact on how campus and branch offices are architected. Previously, organizations aimed for architecting their spaces with a mix of 80% cubicles/desk space and 20% collaboration or meeting rooms. Hybrid work has flipped that model on its head and organizations are now minimizing cube/desk space in favor of creating more collaboration areas. Also, because office workers will likely need to interact with remote workers, I would expect that supporting video and audio collaboration/unified

communication apps will play a significant role. To provide flexible connectivity, organizations will deploy Wi-Fi 6 and new 6 solutions (specifically to provide investment protection as Wi-Fi 6e-enabled devices come to market), which make use of the newly available spectrum and can accommodate those collaboration applications. Depending on organizations' existing wired infrastructure, this shift may require an upgrade to support the additional power requirements for not only Wi-Fi 6 and 6e (tri-band antennas) but also for IoT devices. The changes to the campus will also include the deployment of additional IoT sensors and cameras to ensure employee safety and compliance with any mask or distancing requirements.

The key is to ensure that workers have a positive experience regardless of where they are physically working. To ensure that the operations team can work more effectively, I expect that organizations will look to deploy unified wired and wireless management solutions (based in the cloud) to ensure operational efficiencies.

4. **As interest in 5G continues to grow, real world solutions are tested.**

Will 2022 be the year that 5G lives up to its hype and takes hold in the enterprise? ESG research has shown that there is tremendous interest in 5G and how it may play a role in not just the consumer space, but in organizations as a legitimate business tool. In fact, 91% of mid-market and enterprise respondents cited they were interested in deploying 5G technology.[2] It should be noted that 4G/LTE already has made a meaningful impact in the enterprise as a backup link for SD-WAN solutions and for many industrial settings (4G for mines, oil and gas, etc.). The enhanced capabilities of 5G have the potential to be primary connections for edge locations within proximity to data centers. However, the promise of 5G for the enterprise extends far beyond just fixed wireless broadband.

5G has the potential for use in modular manufacturing plants, mines, oil and gas environments, augmented reality in retail locations, fleet management (trucks, planes, trains), etc. A lot of work remains to be done from the major providers (telco, NEM and cloud) to deliver 5G standalone environments that provide the advanced network slicing capabilities required. Private deployments will be forthcoming, but are organizations ready to take on the management of a completely different technology and additional complexity? Will these enterprises have the skill sets to deploy and operate it?

I look forward to following some of the leading-edge adopters such as John Deere and others to see how their private 5G deployments leveraging the available citizen band radio system (CBRS) spectrum progress. Also, with AWS and Azure rolling out private solutions, the process should become simplified. While some have predicted that private 5G will has the potential to completely replace Wi-Fi, I don't see that happening in 2022, if ever. I do like the fact that 5G is pushing Wi-Fi technology to deliver more capabilities. The competition will benefit organizations by providing them with more compelling solutions from both technologies and I look forward to seeing the 5G use cases that take hold in 2022.

5. **Consuming on-premises networks "as a service" gains momentum.**

An ongoing shift to convert on-premises CapEx purchases to OpEx is taking place. ESG research has been tracking this growing trend as organizations continue to adopt cloud-based services and want to provide a similar experience across their on-premises data center, campus, and edge locations. In fact, for 2022, more than half of the respondents (54%) cite a preference to apply a consumption-based cloud model in data centers.[3] Major IT vendors are now offering or rolling out as-a-service options for most, if not all, of their products. Network vendors

---

[2] Source: ESG Research Report, *Network Modernization in Highly Distributed Environments*, November 2021.
[3] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021

appear to be following suit, with Aruba offerings included in HPE GreenLake, and Cisco announcing Cisco Plus. This should be a natural transition for network vendors as organizations have been consuming network services from telcos. In fact, ESG research indicates that the vast majority of SD-WAN technology (73%) is now consumed as a managed service.[4] The fact that unified management for the wired, wireless, and WAN space is becoming more prevalent provides a natural path to consume those solutions as a service as well. The data center poses a more interesting as-a-service model, but with servers and storage increasingly delivered in that manner (Dell APEX, Hitachi, Lenovo), it would be only natural to include the network. I believe there are still some details to be worked out, including SLAs, scalability and, most importantly, determination of the correct shared responsibility model to put in place.

6.   Network and security convergence continues.

Secure access service edge, or SASE, was a really hot topic in 2021 and likely will continue to be in 2022. Virtually everyone agrees that a highly distributed application and worker environment creates more risk and an expanded attack surface. Network and security teams and functions need to become more tightly aligned to ensure secure connectivity to every employee and application. However, this becomes more difficult when the internet becomes organizations' corporate networks. Organizations must also take care to ensure that security and network performance are appropriately balanced. We continually see examples of this shift to ensure balance as organizations start to replace legacy VPN solutions, making sure that all users leverage the data center security stack—but doing this greatly increase latency to cloud-based applications —which negatively impacts performance.

Cloud-based zero trust network access (ZTNA) solutions are steadily gaining ground to ensure secure and performant cloud application connections. SD-WAN solutions are also being deployed (as managed services, as previously mentioned), which opens up the potential to consume SASE functionality as a managed service as well, enabling organizations to control network and security policies while leaving lifecycle management and maintenance to the MSP. There are also signs of more convergence in the data center as well, with distributed services architectures driving stateful security applications into network interface cards (NICs) and top-of-rack (ToR) switches.

 While much of this cloud-based technology can be easily deployed, many organizations will likely opt for a hybrid model to start, with technology both on-premises (definitely for the data center) and in the cloud. The key to a successful convergence will be for organizations to overcome internal cultural hurdles and drive collaborative and unified net/sec operations teams.

The Bigger Truth

Organizations have made significant changes over the last two years, accelerating digital transformation initiatives and creating highly distributed application and worker environments. As a result, the network environment has become increasingly complex while also playing a more critical role in delivering positive user experiences. Organizations will need to focus on adopting operationally efficient and intelligent network management solutions to ensure that operations teams can deploy and maintain always available, secure, and optimized networks.

---

[4] Source: ESG Survey Results, *Network Modernization Trends*, August 2021.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com   contact@esg-global.com   508.482.0188