

Evolving Enterprise Networks: The Journey to Cloud, SDN, and the Edge

= TC-BLZ

A fundamental change in data networking has begun.

hat change involves moving away from hardware-based network appliances and proprietary management to open-standards-based, software-defined networks (SDNs). These networks promise to be more dynamic, scalable, agile, and resilient than their predecessors; they will be crucial for modern, scalable computing, management, and security across the cloud, wide-area networks (WANs), and local-area networks (LANs).

When coupled with high-availability, lowlatency 5G cellular or Wi-Fi 6, they will usher in scores of "core-to-edge" applications and services.

This e-book explores the benefits, key technologies, and use cases of these nextgeneration software-defined networks, which will offer a powerful competitive advantage for businesses that deploy them correctly. Simply put: Network modernization through virtualization and automation is essential to enterprise success in the digital era. Networks touch everything from distributed data centers to on-premises or colocation facilities; infrastructure-as-a-service (IaaS) public clouds and software as a service (SaaS); and the edge, which includes employees at branch offices, customers, and partners worldwide.

More flexible and robust network infrastructure — one that is easier to provision, modify, monitor, and secure.

Click here to learn more.

SDNs with enabled edge services hold much promise, yet it is undeniable that this transition to core-to-edge networking will be challenging. Why? Because no business will simply rip and replace its existing LANs, WANs, and mobile networks. In other words, deployment will involve a mix of old and new technologies that must be managed together. (The same can be said for the transition to cloud. Any number of operational, regulatory, and/or security imperatives may force an enterprise to keep its on-premises compute power and applications in the mix, resulting in hybrid cloud/multicloud configurations, with resulting deployment/management complexity.)

This e-book also offers best-practice recommendations on where and how to start this digital transition and deploy network solutions for maximum benefit with minimum risk.



Why Is Change Needed?

The need for a more flexible and robust network infrastructure — one that is easier to provision, modify, monitor, and secure — has been underscored by recent disruptions, as businesses around the globe have raced to support work-from-home and work-fromanywhere arrangements and/or revamp their supply chain.

Digital transformation requires upgrading the network, the underlying platform for everything else. The network connects distributed data centers — on-premises, in colocation facilities, in IaaS public clouds, and/or in SaaS services — to the network edge, including employees, suppliers, customers, and partners worldwide.

Network modernization extends core services (those residing in data centers or clouds) through the enterprise campus (think WAN) and out to remote sites on the edge. But many organizations confront a management morass when they try to coordinate a hodgepodge of legacy hardware, software, and networking vendors. Organizations that want to embrace new ideas (IaaS and edge computing, for instance) must continue to manage and secure their existing infrastructure. Such mixed environments cause increased complexity, in both planning and maintenance, and increased vulnerability, due to deliberate attacks or errant configurations.

Indeed, organizations can be forgiven for choosing not to upgrade key infrastructure for fear that this activity itself could cause negative consequences. In Tanium's 2019 "<u>Global Resilience Gap</u>" study of 500 global CIOs and CSOs, 81% of the respondents indicated that they had refrained from adopting an important security update or patch due to concerns about the impact it might have on business operations. Even auditing the existing network can be a major undertaking, given the explosion of network endpoints. The number of worldwide devices on the <u>internet of things (IoT)</u> is forecast to almost triple, from 8.74 billion in 2020 to more than 25.4 billion devices in 2030.

According to Flexera's 2021 "<u>State of the</u> <u>Cloud Report</u>," which surveyed 750 global cloud decision-makers and users:

- 92% of enterprises have a multicloud strategy; 80% have a hybrid cloud strategy.
- **49%** silo workloads by cloud; **45%** integrate data between clouds.
- Respondents use an average of **2.6** public and **2.7** private clouds.

Certainly wide-scale adoption of cloud has made enterprises more agile, with the ability to add or remove compute and storage resources as needed. For instance, using cloud services is an ideal way to support elastic applications, which allocate and deallocate resources on demand for specific application components. Cloud is more resilient too, in that organizations can span

compute, development, storage, disaster recovery (DR), and business continuity (BC) across a virtualized on-demand environment.

66 We've seen that companies that had already embraced cloud were able to sustain, and even innovate and extend, their business models.

Michelle Weston, Director and Global Portfolio Leader for Security and Resiliency at Kyndryl





Enter the Cloud: A Mix of Benefits and Challenges

Although moving to cloud offers benefits, it carries its own set of burdens.

yperscalers such as Amazon AWS and Microsoft Azure, which provide cloud, networking, and internet services at scale, each have slightly different feature sets. This results in a complicated management environment.

That makes it hard to move critical workloads completely into an integrated hybrid or multicloud, he says. The practical result is that private clouds are not going away. Another reason why private clouds are not

"

going away, according to Mike Lyons, chief technology officer of the Network and Edge Global Practice at Kyndryl: These onpremises solutions provide "clear control of your crown jewels applications."

Compounding complex systems management is an ongoing staffing and skills gap. This is especially true with regard to network engineers, analysts, and cybersecurity professionals. In the Global Knowledge "<u>2021 IT Skills and</u> <u>Salary Report</u>," more than half of the surveyed IT decision-makers reported that hiring for essential IT positions is "somewhat difficult or extremely difficult."

Cybersecurity personnel are in especially high demand — not surprising, given the epidemic of cybercrime. For example, Check Point Research (CPR) <u>reported</u> in October 2021 that there were 40% more attacks weekly on organizations in 2021 than in 2020. And there is still a worldwide skills shortage. According to the "(ISC²) <u>Cybersecurity</u> <u>Workforce Study, 2021</u>," published by the nonprofit ISC² (International Information Systems Security Certification Consortium), the global cybersecurity workforce is still about 65% below what organizations need in order to fill all the current open positions worldwide.

Hyperscalers have no compelling reason for consistency [with their competitors], so if you've got particular feature sets that you're interested in for workloads, you have to use that vendor's cloud and API [application programming interface].

Mike Lyons, Chief Technology Officer of the Network and Edge Global Practice at Kyndryl

This is a perfect storm: a complex patchwork of legacy and SDN-based networks connecting LANs, WANs, and enterprise data centers as well as hybrid clouds and multiclouds, but without sufficient personnel on staff to protect and thoroughly manage these vital enterprise assets.

Is there a bright spot? Perhaps. Old architectures and inefficient approaches that were slow to adapt to disruptive change in the past two years may have set the stage for organizations to accelerate their network modernization and emerge stronger.





Ball tail and

1999 🖗

kyndryl

SPONSORED BY

Network Transformation: SDN/NFV/Network Automation

Network modernization involves three areas:

- Software-defined networking (SDN)/network functions virtualization (NFV)
- Edge computing (4G/5G and Wi-Fi 6)
- Network automation

SDN centralized management enables network managers to automate changes across a large fleet of network devices. In Cisco Systems' definition, SDN has the following elements:

- A controller, the core element of an SDN architecture, that enables centralized management and control, automation, and policy enforcement across physical and virtual network environments
- Southbound APIs that relay information between the controller and the individual network devices (such as switches, access points, routers, and firewalls)

• Northbound APIs that relay information between the controller and the applications and policy engines, to which an SDN looks like a single logical network device

Software-defined networking (SDN) centralizes management and uses software-based controllers or APIs to communicate with underlying hardware infrastructure and direct traffic on a network. This way many network devices operating as a group can be controlled and managed from a single logical console. Network functions virtualization (NFV) decouples network functions from proprietary hardware appliances (routers, firewalls, virtual private network [VPN] terminators), so it can deliver equivalent network functionality without specialized hardware. The most commonly referenced advantages of SDN are traffic programmability, agility, and the ability to create policy-driven network supervision and implement network automation.



"

The major advantage of SDN is it brings agility through network abstraction and automation. Historically, a network has always been cables and wires and a big reliance on physical infrastructure. With SDN, by comparison, we can leverage the ubiquitous network carriage, primarily the internet, and effectively overlay functions on top of that.

Mike Lyons, Chief Technology Officer of the Network and Edge Global Practice at Kyndryl

This is game-changing, in that as business requirements change, the network can be changed, Lyons says. "Sometimes you hear the term *infrastructure as code*. I think that that's a good description of the way it works."

Network functions can be added or removed on-demand, much as cloud compute or storage resources can be added as needed. This elasticity removes friction, enabling services to be turned on or modified quickly.

Another advantage of SDN's programmability is how it streamlines life cycle management. Take a legacy firewall, which may have 100,000 rules in it, built up over time and always in force. With SDN, the firewall rules are established at the time of provisioning, so when that workload is retired, the firewall's rules are torn down with it.

"To me, of all the features of SDN, it's that ability to automate life cycle management that has the biggest benefit for security and governance generally," says Lyons.

Further automating network provisioning, several vendors are working on so-called intent-based networking. Essentially, intentbased networking proposes using AI and machine learning to adapt and adjust the network dynamically to the user, device, or use case. Rather than defining a detailed set of network configurations, which can be very arcane, the idea is to describe an intent and let the automation make the changes necessary to deliver it.

So if the "intent" is to set up a web server in a particular environment, a semiautomatic script will create the server, set up its rules, establish the port translations, register a Domain Name System (DNS) name, and so forth. Taking this automation up a notch, some foresee software engineers' using machine learning to "teach" the platform to perform these functions on its own.

"Intent-based networking sounds really impressive," says Lyons. "But I would suspect that there's a significant challenge to it, and one of the reasons that network engineers are well sought after these days is that it's not simple to do."

Lyons says human beings are still needed to create patterns and conduct quality assurance to make sure the resulting configuration "does what it does properly and doesn't have unintended consequences."

Broadly, however, SDN is not a panacea. "You have to be very clear about why you've got functions in place at any given time, and life cycle management is a big part of it," Lyons says. Thoughtful governance still matters, he adds. "A shortcut can expose a security vulnerability," he says. "That's possible in any environment, and it's absolutely true with SDN. Having a technology does not absolve you of the requirement to govern how you use it, which is an important part of our ethos as a provider."





Understanding the Common Core-to-Edge Use Cases

Core-to-edge networks covering end user device integration, cloud-based application delivery, highsecurity options, and innovative network services will be applied in several scenarios.

From an enterprise perspective, here are the major categories of core-to-edge systems and their advantages:





SD-WAN

Provides independence from carriers' premium Multiprotocol Label Switching (MPLS) services, using the ubiquitous public internet for transporting routine bulk data, which is dynamically managed via software. Such WANs are both less expensive (price-leveraging low-cost carriers) and more agile/resilient.



Data centers and cloud (SDN-DC) Virtualizing the data center and delivering it "as-a-service" is accomplished with a combination of software-defined networking, softwaredefined compute, and software-defined storage. This provides workloads that are more agile and resilient.





Branch networks and local-area networks (SD-LAN) Avoid physically cabling buildings

with copper to the desktop by leveraging ubiquitous wireless networks, controlling network segmentation and features with software rather than on-premises hardware.





Real-time monitoring and insight at the network edge Conducting data analysis and

storage near where the data is generated, rather than sending data to the data center for processing, is more efficient and may be essential for real-time applications, such as the control of data-intensive industrial processes.





Multicloud Connects multiple cloud computing and storage services as one heterogeneous architecture. Avoids

vendor lock-in.



Software-defined cloud 5. interconnect

Provides secure, automated connectivity to any IaaS environment. Importantly, it is provided as a service, so its deployment and management can be integrated into existing software-defined workflows.



Secure access service edge (SASE) 7. Consolidates numerous vendorspecific networking and security functions, such as standalone point products - firewalls and secure web gateways, for instance – with SD-WAN. Reduces costs and complexity.



Working on the Edge: The Role of 5G and Wi-Fi 6

Completing the puzzle of network transformation are high-capacity, low-latency wireless technologies such as 5G cellular and Wi-Fi 6, which will spread core network functions to the network's edge.

<u>Ericsson</u> predicts that by 2023, 5G will make up around one-fifth of all mobile data traffic. But this is the tip of the iceberg. 5G has a role to play in cloud, WAN, and even LAN deployments. Note that 5G is not one thing. There is standalone architecture (SA), which connects directly to the 5G core network without reliance on 4G, and nonstandalone architecture (NSA) 5G, which is built on top of existing 4G infrastructure, which still handles control signaling.

What does 5G promise enterprise users?

- Easier-to-deploy remote access
- Secure remote access
- Redundancy for WANs
- Higher-bandwidth, more secure replacement for campus-wide Wi-Fi
- A fallback infrastructure for data backup
- An infrastructure for IoT applications requiring 5G's lessthan-10-millisecond latency

The last of these uses, an infrastructure for IoT applications, is an immediately promising one and heralds the transformation at the network edge for data-intensive industrial processes.

"There's value in having very short latency between data gathering, data processing, and action in the field," says Lyons, adding that "that's a powerful argument for edge computing generally." Healthcare is another industry where this design makes sense, Lyons says. "We know that [healthcare] is very data-intensive, with high-resolution scanners and such, which can generate vast amounts of data." Asked if every industry will use edge computing, Lyon said, "I would say every industry is going to develop use cases."

Even so, there won't be one-size-fits-all. For example, not all edge deployments will require high-bandwidth, low-latency systems. In an IoT scenario featuring a swarm of lowpowered devices that only occasionally beacon, 5G or Wi-Fi 6 will be overkill.

Another real-world obstacle to using 5G everywhere is that telcos may not offer 5G in some areas. In such cases, campus-wide private 5G networks are an option, although every country has a different spectrum management authority, which may limit such private deployments. Edge computing is and will continue to be an integral part of Industry 4.0, also known as the Fourth Industrial Revolution. (See "<u>How</u> <u>Industry 4.0 Will Leverage Edge Networking</u> <u>and IoT</u>."



Overcoming Transition Challenges

At the very moment when agility and flexibility have become critical priorities, organizations are weighed down by a plethora of point solutions and technical debt, creating unwieldy complexity and hesitancy for already-stretched IT teams.

Organizations may not know where to begin and find themselves daunted by the breadth and depth of the challenge of digital transformation. Some may know where they want to be in terms of an application environment but are unsure how this maps to new requirements in network infrastructure and network operations.

In response, many are turning to service providers and partners to help them build and manage diverse vendor-agnostic environments that leverage cloud, SDN, and edge computing. As discussed, this network transformation will involve changes to existing infrastructure, deployment of SDN/NFV, and making choices about different wireless transport options at the edge (4G/5G, Wi-Fi, Wi-Fi 6). With that in mind, Kyndryl experts offer several recommendations on how and where enterprises can begin their journey to SDN/ NFV and 5G deployment.





Cloud, Network, and Edge Deployment Recommendations

Transformed enterprise networks will impact every industry, business, and network-based application and process. How should today's organizations prepare? Here are Kyndryl's top-level recommendations:

- Embrace a technology governance mindset that puts business first. Understand the business and the business drivers. Business needs should drive technology choices.
- Invest in latent capacity (compute, storage, and network). Conduct operational planning to know how much reserve capacity is needed. This should include how much of this capacity should be onpremises and how much can be acquired from the market on-demand.



- Use SDN/NFV to deploy and control network functionality.
- Evaluate how edge computing will be relevant to the business.
- Consider harnessing private cloud as a service and managed infrastructure as a service, offloading management to a partner.
- Work with a partner with demonstrated expertise and experience in end-to-end platform-agnostic enterprise IT management at scale. This partner will be able to reproduce consistent solutions quickly, because it follows a reference architecture.

Request a free 30-minute consultation with an expert or get answers to your questions about anything Kyndryl here:

Click here to learn more.



How Industry 4.0 Will Leverage Edge Networking and IoT

SPONSORED BY KYNORY

Data-intensive industrial processes present unique data networking challenges. Fortunately, the move to intelligent, interconnected, and autonomous networking schemes can solve many of these difficulties.

For a data networking perspective, the difficulty with the Industry 4.0 Revolution starts with geography. Factories tend to be in isolated locations away from city centers, where high-speed infrastructure is more commonly available. Remote locations impact how easily and affordably IT services can be provisioned, modified, monitored, and maintained.

A second difficulty is that some industrial processes demand low latency. Given the unavoidable problem of network latency, a distant data center cannot control a real-time process, for instance. (Instead of sending all data off to the cloud or a remote data center, edge storage sends only relevant data offsite. This creates a gateway, analyzing data locally and sending only results or summarized data to the cloud.)

A third difficulty is provisioning, monitoring, and securing a profusion of heterogeneous network-connected devices on the factory floor.



Enter Edge and IoT Solutions

Solving Industry 4.0's difficulties are edge computing and internet of things (IoT). Both push functionality out to the network's edge, where work is being done or data is being collected and acted on. Network transport will be provided by low-latency technologies such as 5G and Wi-Fi 6.

That's not to say IoT is without issues, particularly in terms of cybersecurity concerns. In a 2021 report, "<u>The State of IoT</u> <u>and OT Cybersecurity in the</u> <u>Enterprise</u>," produced by Microsoft and its partner the Ponemon Institute:

- 55% of the survey respondents indicated that they do not believe that IoT and operational technology (OT) devices have been designed with security in mind.
- 60% of the respondents said IoT and OT security is one of the least secured aspects of their IT and OT infrastructure.

Nevertheless, companies are pushing ahead with IoT, the research found. A large majority of the respondents believe that IoT and OT adoption is critical to future business success. Specifically, 68% of the respondents said senior management believes that IoT and OT are critical to supporting business innovation and other strategic goals. Some 65% of the respondents also said that senior management has made it a priority for IT and OT security practitioners to plan, develop, or deploy IoT and OT projects to advance business interests.



Thank you for reading.

Visit Kyndryl for more information on our Network and Edge services

www.kyndryl.com/us/en/services/network

TC-BLZ