WHITEPAPER

WAN Transformation

Network modernization considerations for long-term success

LUMEN® TECHNOLOGIES

Abstract

Wide Area Networking for enterprises used to be simple, static, and straightforward: Businesses had physical sites where they conducted business and where employees worked, business applications ran in data center environments that were managed by in-house IT staff or via third-party contracts, and Wide Area Networks (WANs) connected users to those applications.
Fast forward to today — the pandemic drove digital transformation at a breakneck pace, and there are now many more WAN options and implementation choices muddying the waters as customers try to navigate the network landscape.

This paper takes on the perspective of an enterprise that has existing WAN services and is assessing "What's Next?". Is their current WAN optimal for their needs, or are there opportunities to improve? Here, we approach the question from the angle of business needs and outcomes, with particular focus on applications and by who and where those applications are being used. We propose a basic framework to help inform the customer and make recommendations as follows:

1. What is my current and anticipated application environment?
2. Where and how are my users accessing my enterprise applications and data?
3. What are my security considerations?

This paper also illustrates several use cases, which outline four common technology-migration paths to optimized network architectures and their respective business benefits.

LUMEN® TECHNOLOGIES

Introduction: WAN modernization drivers

Over the past decade, enterprise WAN choices have evolved from the de facto standard of IP/MPLS VPNs toward increased adoption of internet connectivity, creating public–private hybrid WANs. This has its drawbacks, however, as internet does not provide that same reliability or availability that is provided when using dedicated private links.

In addition, the application landscape has dispersed across various data center, public and private cloud, and Edge environments, with users needing to access those applications from many locations and devices. While traditional, centralized WANs were tightly managed — with every start and end location known — this is no longer the case with dispersed WAN environments, as cloud applications don't have known physical locations.

Today, Software-Defined Wide Area Networking (SD-WAN) has become mainstream as a "smart" overlay network to manage various routing and traffic policies. And Secure Access Service Edge (SASE) has emerged as a new paradigm closely integrating security (e.g., Zero Trust) and SD-WAN capabilities in the cloud.

Consider the following digital-transformation drivers and how they've framed the current WAN landscape:

From centralization to edge and cloud

The cloud dispersed applications and data from a centralized, private data center to internet-enabled software and services. Modern network topologies now resemble a tangled bowl of spaghetti with data firing along multiple paths between end devices rather than spokes of a wheel around a centralized hub.

From relative safety to zero trust

Traditional WAN architectures had perhaps one or two external entry points, so internal traffic was deemed relatively safe. With the Internet of Things (IoT), however, everything is connected, and many of those entry points are managed by third parties — meaning the safest assumption when it comes to your WAN is that nothing is safe. This is the premise of Zero Trust, a framework for securing cloud-first businesses that asserts that no user, device, network, or application can be trusted by default for access permissions.

From the office to work-from-home

It's a digital-first work world, and experts say that there's no going back. According to Microsoft's Work Trend Index 2022, 53% of workers are considering going hybrid in the year to come, and 51% of hybrid workers say they're likely to go fully remote in the year ahead[1]. This is a huge network challenge, as creating an office that works for in-office, hybrid, and remote employees requires an intentional, secure, and radically flexible WAN architecture.

Three questions to consider before updating your network architecture

A modern WAN must meet the needs of digital-first organizations, which means empowering users and optimizing applications, wherever they reside, securely and flexibly. By asking the right questions, businesses can pinpoint where exactly they need to improve their network architecture to achieve their business outcomes.

Consider the following:

1. What are my current and anticipated application environments?

- Where do my applications run — private data centers, public clouds, SaaS cloud services, Web cloud services, on business premises, at the network edge?
- What network-performance requirements do those applications have to meet to deliver the ideal user experience? Consider network latency, throughput, tolerance for packet loss, and jitter.
- What are my data and application load/bandwidth characteristics? Are bandwidth needs predictable? What does peak demand vs. average load look like?

Once you've fully sketched out your application environment and anticipated needs, it's much easier to design a network to meet those needs.

Dispersed application environments require businesses to align their cloud, data center, and edge use cases with their WAN environments to minimize network latency and jitter.

Applications	Characteristics	Network considerations
Email	A foundational communications application running across all businesses. Non-real time, so it can work over a range of different networking types, speeds and conditions.	• Email is latency and jitter tolerant; with bursty traffic based on user interactions, availability is a highconcern. • Low-speed internet connections will not materially affect performance
Real-time collaboration tools, i.e., VoIP, UCC, etc.	As dispersed workforces typically rely on voice and video to perform critical business functions, these applications are mission-critical and require a consistent network performance	• Sufficient bandwidth for data needs and simultaneous voice or video calls. • Consider high availability with redundant paths. • UCaaS apps are well-suited for simultaneous high-quality internet-based networking, but for intra-business communication, they'll benefit from managed private networking.
CRM, i.e., Salesforce, Oracle, etc.	These apps are typically considered mission-critical, thus it's important for them to be "always on" and highly available	• Redundant and diverse networking will help to achieve high availability. • Geographic load balancing will help ensure consistent performance for all users.

2. Where and how are my users accessing my enterprise applications and data?

- Who are my users — employees, customers, partners, contractors?
- Where are users based — fixed locations vs mobile, known office locations vs. home or work-from-anywhere environments?
- What options do users have for connectivity — connections from private network locations vs. access via public internet.

Once you know your application needs, think about your network users — who they are, where they're based, and how they access your applications and data. Hybrid or remote employees accessing your WAN from home via VPN, public networks, and mobile devices will have different needs than on-site employees.

A great user experience means enabling your users to interact with your business on their terms — from any device, anywhere, at any time. This level of flexibility requires deep visibility into your network, smart automation, and precise control, which is where WAN virtualization comes into play. Layering SD-WAN, for example, over a hybrid WAN architecture will coordinate workloads securely across various connectivity types using centralized software-based orchestration control of application policies.

3. What are my security considerations?

- How would security threats and related downtime impact my business?
- How would a data-privacy breach impact business financials and customer trust?

While outlining your enterprise application and user needs, think of security. The pandemic accelerated companies' digital transformations, spurring an associated uptick in cybercrimes. Lumen mitigated more than 20,000 DDoS attacks in 2021 alone[2], and the average cost of a data breach is now US$3.6 million per incident according to IBM[3].

Dispersed enterprises with applications, managed and unmanaged endpoints, and cloud services are more vulnerable to security threats, which is why many enterprises are adopting a zero-trust framework. In fact, the federal government is required to deploy zero trust by the end of the 2024 fiscal year[4].

Even if your network has built-in threat protection, as the Lumen Platform does, security should be a top priority as organizations modernize their WAN. SASE is one option for unifying network access, security, and management across a distributed enterprise. The framework's end-to-end visibility provides a unified view of network traffic and security options to nip threats in the bud, while simplifying operations for managing equipment and policies for on-site and remote workers.

Network modernization scenarios

After sketching out your application, user, and security needs, you're ready to outline your ideal WAN — and plan your migration journey. Of course, not every company needs to modernize its network — for many that already rely on a private, secure, and reliable IP VPN/MPLS architecture, their network may already be optimized for their needs, while others would benefit from a flexible hybrid design. Here, we've outlined four use cases, demonstrating common network migrations that align various WAN technologies with desired business outcomes.

Secure, private networking with MPLS

READ MORE →

Flexible hybrid networking with SD-WAN

READ MORE →

Secure hybrid networking with SASE

READ MORE →

Cost-effective, cloud-first networking with IP and SD-WAN

READ MORE →

Secure, private networking with MPLS

In this scenario, a large multinational and regional finance firm is interested in upgrading their IP/MPLS network to accommodate some hybrid work, although in-office work remains significant. The company employs a well-staffed and experienced IT team, and since it works with sensitive data, network security, uptime, and performance are top priorities for the business.

WAN outcome

- Maintain core IP/MPLS network to prioritize security and application performance with global consistency
- Low-priority web traffic could be more cost-effectively managed with local internet access
- Evaluate some regional sites for broadband with SD-WAN

Flexible hybrid networking with SD-WAN

In this scenario, a domestic U.S. manufacturer wants to accommodate an increasing number of work-from-home employees and is considering office closures. The company currently has multi-site IP/MPLS and VoIP services running across VPN and outsources its IT and network management to a third party. The manufacturer leverages advanced robotics during production, making network uptime critical.

WAN outcome

- Keep core IP VPN in support of main business functions and VoIP network
- Add internet break-out at key branch locations for guest Wi-Fi access
- Add managed SD-WAN for application-based routing and back-up
- Begin evaluation of modern remote access/ZTNA solutions

LUMEN® TECHNOLOGIES

Secure hybrid networking with SASE

In this scenario, a national retailer with many locations and thousands of employees is looking for network scalability for its busy season, consistent in-store Wi-Fi across its locations, and additional security to protect online sales. Currently the retailer, which has centralized IT and network management staff, has multi-site IP/MPLS with hub-and-spoke connectivity back to national data centers and in-store guest Wi-Fi.

WAN outcome

- Upgrade in-store IP to consistent Dedicated Internet Access links and enable dynamic capacity to scale bandwidth as needed.
- Converge and simplify network and security elements into a SASE framework.
- Use SD-WAN within a SASE framework for application-based routing and cloud-based security for in-store guest Wi-Fi. SD-WAN provides local internet breakout.
- Re-architect core IP links for online ecommerce platform with redundancy and full DDoS mitigation.

Cost-effective, cloud-first networking with IP and SD-WAN

In this scenario, a local accounting firm with a small in-house IT staff is struggling to manage its work-from-home employees. The company is cost conscious and working with limited IT resources as it considers changing its network architecture from a small IP VPN network connecting several offices and a data center for basic email and data-storage applications.

WAN outcome

- Implement a cloud-first strategy by transitioning WAN to internet and SD-WAN to lower total cost of ownership.
- Host office and business apps in the cloud and leverage SaaS; retire data center infrastructure.
- Leverage SD-WAN to encrypt traffic and secure transmission of sensitive apps.

Five things to look for in a WAN provider

There are countless connectivity and provider combinations for network technologies. Consider the following criteria as you choose a provider to advise on, implement, and manage your network-migration journey:

Authority: Lumen has a proven track record as a leading provider of network, voice, and security services, with the fastest, most secure platform for next-gen apps and data.

Expert guidance: Overhauling your network infrastructure is a daunting task. Lumen provides managed and professional services to help you build, deploy, and manage business-wide network topologies.

Solution variety: Lumen employs a product-agnostic approach when advising on WAN architecture. As providers of everything from internet and MPLS, to SD-WAN and SASE, to cloud ecosystems, we'll match your business needs to your ideal mix of solutions.

Visibility and control: Lumen's portal makes managing billing, repairs, orders, product configurations, and reporting both accessible and easy, so you get the most from your products and services.

Customer centricity: Lumen was the first in the telecom industry to adopt a Customer Success model. Our dedicated Customer Success teams understand your business, know how to optimize your solutions, and will help you achieve your business outcomes.

EXPLORE OUR SERVICES

Footnote(s)/Disclaimer(s)

1. Microsoft Work Trend Index 2022
2. https://assets.lumen.com/is/content/Lumen/lumen-quarterly-ddos-report-q-4?Creativeid=a1a675ca-a7c6-4574-9174-4f3a3eb737d7
3. Cost of a Data Breach Report 2021
4. Executive Order on Improving the Nation's Cybersecurity

866-352-0291 | lumen.com | info@lumen.com

LUMEN® TECHNOLOGIES