So many ways to WAN

How the most essential technology for distributed enterprises has evolved, and where it’s headed

Digital transformation has revolutionized the ways in which we communicate and collaborate.

Over the past few years, organizations within all industries have evolved new ways of doing business, while the global pandemic has accelerated trends such as remote working and touchless consumerism.

Consequently, enterprises have evolved to the point where their network perimeters are highly dispersed. Fixed office locations are giving way to remote and mobile users. Applications and servers are moving to the cloud, multi-cloud and SaaS providers. And security threats have increased. Now there is no longer a “safe corporate network” and “dangerous Internet”—there is only “the network.”

Throughout this evolution, the wide area network (WAN) has been the primary foundation of digital transformation, emerging as the vital link between enabling a new business model and driving the bottom line.

That’s why WAN quality is the pressing issue for IT managers, who want to maximize network performance and uptime to support new applications, support closer workplace collaboration and deliver outstanding customer service.

At the same time, technology budgets have stagnated. Managers need to be innovative in order to support the business vision while controlling costs. As a result, many organizations have looked at changing their network designs to Internet-based networks as a way to reduce costs while increasing capacity for their business-critical, cloud-based applications.
Let’s look at the various types of WANs in use today and how wide area networking is evolving to support digital transformation.

89% of all companies have already adopted a digital-first business strategy or plan to do so.¹

60% of companies that have undergone a digital transformation have created new business models.²

Striking the right balance for your network from a wide array of options

While one type of network can work for some companies, most enterprises are best served by selecting a flexible network design that includes SD-WAN, MPLS, hybrid (MPLS/SD-WAN) and Internet access.

The goal is to strike the right balance of network options, realizing that business-critical applications can and should be handled differently from less essential functions.

The impact of this multifaceted network architecture can be significant, as the organization no longer needs to trade performance for cost and can satisfy the needs of all the sites on the network. Common questions to consider for many multi-location companies include:

- Are you shifting application workloads to the cloud?
- Does the network need to support remote working?
- Is redundancy required for failover and ~100% uptime?
- Is maximizing available bandwidth a consideration?
- Do data breaches pose a catastrophic threat to the business?

To determine the best network design, it’s important to understand and evaluate all available options based on requirements for scalability, availability, Quality of Service (QoS) and security.
SD-WAN

Software-defined WAN (SD-WAN) is an application-aware service that intelligently routes traffic in real time based on established business policies, along with network quality and availability.

SD-WAN is used to connect multiple locations in a network to each other, to a data center, to applications and data in the cloud, or to SaaS platforms. Leveraging multiple, cost-effective access types at each location in an active-active configuration, an SD-WAN network routes application traffic over the best-performing network elements in real time and ensures automated failover for resiliency.

SD-WAN enables an organization to prioritize applications on an individual basis, eliminating the need for establishing CoS (Class of Service) policies. An SD-WAN can also rate limit or block unauthorized applications—ensuring that the business critical applications are not impaired by unimportant traffic.

As a software-defined overlay network, SD-WAN works on top of the other types of networks. Network management is centralized, allowing simplified visibility and control from a single pane of glass. IT personnel can view application performance as well as set network, security and application policies across all locations according to their specific goals. New sites can rapidly be turned up, dramatically reducing the need for on-site IT support.

Adding WiFi, video and cloud-based applications such as UCaaS, Office 365®, Salesforce® and others drives the need for more bandwidth. SD-WAN enables additional, low-cost broadband connections to be added to the network rapidly—without the need to reconfigure edge devices.

Sample SD-WAN network
Multiprotocol label switching (MPLS)

MPLS VPNs are operated and managed by a single carrier, with connections that are isolated from the public Internet. Because the traffic within the MPLS network is kept private, the carrier is able to enforce QoS and Class of Service (CoS) policies on individual traffic flows.

From its introduction, MPLS has been a good option for organizations that run multiple business-critical applications and need control over application performance. Voice and data traffic can converge into one network infrastructure, which enables cost-effective management by right-sizing connectivity at each location.

Over the years, many larger companies have chosen to add a back-up MPLS VPN from a different service provider to enable redundancy and achieve greater availability. While MPLS has been the network of choice from a security perspective, it’s also the most expensive option and the least flexible. What’s more, the explosion in bandwidth demand driven by cloud-based apps has put a significant strain on MPLS designs—many of which still have only one or two Internet uplinks at the data center or headquarters. To enable cost-effective bandwidth, many businesses have begun to augment their MPLS networks with hybrid WANs and SD-WANs.
Hybrid WAN

Over time, the hybrid WAN has evolved to combine features of both MPLS and broadband or Ethernet Internet to leverage the benefits of each solution. Using this network architecture, IT can maintain an existing MPLS network to run real-time applications, such as voice and video with built-in CoS, as well as use broadband or Ethernet Internet to support cost-effective higher bandwidths.

The Hybrid WAN is controlled by an SD-WAN overlay in an active/active configuration—thus improving performance and resiliency. Hybrid WANs can also be deployed with cellular broadband in an active/standby configuration to support locations that have lower bandwidth requirements.

Not only does this approach strike a balance between cost and performance requirements, but having multiple access solutions controlled by SD-WAN also enables maximum utilization of the available bandwidth. In a hybrid WAN with an active/active network design, there is no longer a concept of primary and backup—all the network circuits are used simultaneously as the SD-WAN overlay evaluates the performance of each connection in real time and routes traffic according to the best available path. As you add more network circuits to your hybrid WAN you increase the number of paths the traffic can take and add to the overall quality of the application experience.

A hybrid WAN controlled by SD-WAN is an improvement over a primary and passive secondary backup network design because both connections can deliver traffic simultaneously. Hybrid WAN with SD-WAN will provide the application visibility and intelligent dynamic routing to maximize application performance.
Internet WAN

The fundamental underlay network, Internet service provides business with access to remote resources and applications over a wide variety of access options—Ethernet, broadband/cable and cellular, just to mention a few.

An Internet WAN has no inherent prioritization, security or private transport capabilities—which may be a good solution for businesses that have no site-to-site connectivity options and run very limited applications in their network. Internet WANs are simple to use and are also cost effective, as businesses can leverage broadband at their sites to bring down the cost per Mbps of the network. As businesses grow in network and application complexity, Internet-only WANs will struggle to meet the needs and additional technologies will have to be deployed to provide the intended results.

Running multiple applications over an Internet connection creates contention for bandwidth. Without a prioritization function, those cat videos your team is uploading to YouTube may cause a high-priority customer service call to drop, or at the least have poor quality—which will reflect on the business. This is especially acute on broadband connections where the upstream bandwidth is more constrained than the download bandwidth. Lacking site-to-site connectivity options in the Internet WAN can necessitate client-based VPN options, which are cumbersome for the end user and the support teams.

Internet WANs typically need additional technologies to accomplish business-to-business needs by ensuring that the right applications have access to network resources, as well as securely connecting the end user to the application and data. Which is why they work so well in a hybrid WAN solution.

Sample IPSec network
Other considerations in choosing the right WAN

**Service level agreements (SLAs)**

Businesses want maximum uptime from their networks so all traffic gets to the right destinations quickly. While both IPSec and MPLS offer excellent availability, the private nature of MPLS offers more stringency in SLAs, while IPSec is a best-effort over-the-top service. The active-active design of SD-WAN enables a higher degree of resiliency, allowing providers to offer near 100% availability SLAs and performance metrics that are much higher than Internet-only networks.

**Network security**

IPSec VPNs, MPLS and SD-WANs all keep data private: IPSec with encryption and firewalls; MPLS by being a dedicated network that doesn’t touch the Internet; and SD-WAN by encrypting all traffic with IPSec and typically offering a firewall so any access type becomes a secure connection. Service providers employ a number of additional methods to protect business data from being accessed by unauthorized users. Typically, these solutions include cloud-based, premises-based or virtual next generation firewalls. In some industries, this is necessary to demonstrate regulatory compliance. For businesses that transmit credit or debit card data over their VPNs, some IPSec VPN and SD-WAN providers offer the built-in convenience of PCI compliance, which helps reduce the burden on the business.

**Visibility and control**

The ability to determine traffic prioritization across the entire WAN is essential. SD-WAN offers a distinct advantage. Since it utilizes an overlay network to separate the networking hardware from the network control layer, SD-WAN relies on a centralized controller to set policies. SD-WAN then acts on these policies in concert with the real-time performance of the network connections to determine the best path for each application’s traffic. This ensures that application performance is optimized.

**Class of Service (CoS)**

Network applications are subject to jitter, packet loss and latency. The collective measure of these characteristics across a connection forms the definition of Quality of Service (QoS). With an MPLS network, CoS is used to prioritize different types of traffic (e.g., voice, data and video) according to the relative importance of QoS to each. CoS is inherent in MPLS networks, while IPSec VPNs don’t offer CoS prioritization. SD-WAN can prioritize specific applications on a location or end-user basis, providing much more granularity and control than setting priorities for an entire class of service.

**Professional services**

Running an IT department is a full-time job. Finding the time to run day-to-day networking activities can be daunting—especially when the team has been tasked with developing strategic innovation for the business. An external team of technology experts, offering anything from network concierge services to specific skillsets (security, for example), can augment an in-house IT and give it the freedom to focus on higher-value responsibilities.
What to look for in a WAN provider

While enterprises now have a wealth of WAN options available, choosing the right WAN design for an organization can be tricky. That’s especially true for IT leaders seeking to leverage newer options such as SD-WAN.

Select a provider who

Has a proven track record of successful deployments in a variety of networking types and technologies.

Provides experts to offer guidance in selecting the appropriate technologies that will achieve the organization’s business goals and differentiate it from the competition.

Takes the guesswork out of network capacity planning and design so you can support your company’s digital transformation roadmap.

Enables the flexibility to provide the best available access options to satisfy unique location requirements while keeping costs down by paying only for the access and capacity needed.

Offers tools to provide application visibility and control to maximize bandwidth utilization for a cost-optimized WAN to drive the customer experience initiatives that will help the business succeed.

Doesn’t limit themselves to what their technology can do but builds on that technology to deliver what your business needs.

Specializes in managed network, security and cloud solutions for multi-location businesses.

Helps you embrace the technology for what it has to offer, rather than simply upgrade what you have today.

---


---

About Windstream Enterprise

Windstream Enterprise collaborates with businesses across the U.S. to drive digital transformation by delivering solutions that solve today’s most complex networking and communication challenges.

To learn more about Windstream Enterprise, visit windstreamenterprise.com

---

0230 I 07.20 ©2020 Windstream Services, LLC. All Rights Reserved.