Digital Transformation Demands a Next-Generation Wide-Area Network

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Cisco

December 2016

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Digital Transformation Demands a Next-Generation Wide-Area Network

Table of Contents

Digital Transformation Demands a Next-Generation Wide-Area Network

Executive Summary

With enterprises becoming more and more distributed, the wide-area network (WAN) is the foundation of any digital transformation effort. For that reason, digital transformation requires WAN transformation. Enterprises need to leverage network automation, network virtualization, embedded security, advanced analytics and centralized services to hit this target. This paper offers a roadmap for WAN transformation and examines Cisco's end-to-end solution for network transformation, Digital Network Architecture.

Digital Transformation Requires WAN Transformation

In today's world, the network is the foundation of any digital transformation effort. The wide-area network (WAN), in particular, must evolve to support digital transformation. In fact, already 29% of network infrastructure teams say that digital transformation initiatives currently drive their decision-making. Even those teams not yet impacted by digital transformation are adopting and supporting technology initiatives that are commonly viewed as essential elements of digital transformation initiatives. For instance, 87% of network infrastructure teams are currently providing connectivity to at least one Internet of Things (IoT) initiative, and 35% of network teams are supporting a hybrid cloud architecture.[1]

Network infrastructure teams are also seeing rapid changes in traffic patterns as a result of digital transformation. Applications that are indicative of digital transformation are emerging as major WAN bandwidth consumers. According to Enterprise Management Associates (EMA) research, big data traffic now tops the list of applications that consume the most WAN bandwidth. It was cited as a top source of traffic by 30% of network infrastructure teams. Cloud-native applications and external cloud applications were each cited as the top consumer by 24% of respondents, placing them third on the list of top bandwidth hogs.[2]

Branch offices and remote sites are also emerging as major engines of transformation. Device growth in these remote sites is ubiquitous. Eighty-four percent (84%) of enterprises are experiencing endpoint device growth in remote sites, and 28% describe this growth as "significant." The leading sources of this device growth are PCs and laptops (60% of enterprises), IoT devices (59%), and smartphones and tablets (57%). The strategic value of these remote sites is highlighted by the fact that most enterprises (55%) have abandoned centralized architectures in favor of allowing remote sites to connect directly to public cloud services.[3] Unfettered cloud access is now simply more important than centralized control.

One significant way in which enterprises are transforming their WANs is hybrid connectivity. Among enterprises that are investing in more internet connectivity, 74% plan to replace MPLS and other managed WAN services with the internet for primary network connectivity. Also, 96% of enterprises are using wireless technology for primary WAN connectivity in some sites, including 82% that use 4G/LTE and 50% that use carrier/municipal Wi-Fi. However, this changeover to the internet isn't universal. On average, these companies are replacing MPLS with the internet at only 45% of their sites.[4] Network teams will be maintaining a diverse network architecture for quite some time.

[1] EMA, "Network Management Megatrends 2016: Managing Networks in the Age of the Internet of Things, Hybrid Clouds, and Advanced Network Analytics," April 2016.
[2] EMA, "Next-Generation Wide-Area Networking," July 2016.
[3] Ibid.
[4] Ibid.

In the context of all this change, the network infrastructure team will need to reinvent its approach to the WAN. These new demands are putting pressuring on legacy WAN architectures. Existing technologies will fail to address these new requirements, and the network will become too complex and costly to maintain. In fact, the top three challenges to success with an enterprise WAN are "a lack of skills and knowledge" (32%), "problems with network hardware and software solutions" (32%), and "rising costs and a lack of budget" (30%). These challenges point to the need for WAN transformation.[5]

A Roadmap for WAN Transformation

Network infrastructure teams clearly face a variety of challenges when trying to deliver a WAN that supports digital transformation. Many enterprises are responding to these challenges by adopting software-defined WAN (SD-WAN), but network infrastructure teams should consider a more comprehensive and strategic approach to WAN transformation.

In particular, the WAN should be treated as part of an end-to-end network architecture, where application policies, user privileges, quality of service, security, and other services are delivered in a unified manner across campus, branch, and WAN infrastructure. Several design principles can guide network teams to success with their WAN transformation efforts: automation, virtualization, security, service assurance through analytics, and centralized service delivery.

Automation

WAN technology is traditionally complex and distributed. Hundreds, if not thousands, of individual routers require manual provisioning and configuration. As new applications, devices, and users join the WAN, network engineers and administrators find their time consumed by making additional manual changes to network devices.

EMA research has found that 82% of enterprises are actually increasing the number of network-connected sites on their WANs, including 22% that are growing their number of connected remote sites by more than 25% over the next 12 months. With a traditional, highly manual WAN, IT organizations will lack the personnel to manage this rapid growth and dynamism. In fact, these enterprises would rather apply talented network engineers to more strategic tasks, like network optimization and network planning. Whether part of an SD-WAN solution or part of a larger solution, network automation is essential. Solutions that can automate activation, provisioning, and change management can streamline WAN transformation.

Virtualization

New breakthroughs in software and hardware engineering have made it possible for enterprises to virtualize a wide variety of network functions that were traditionally delivered to branch offices via specialized hardware appliances. This virtualization of branch infrastructure lowers overhead, reduces complexity, and accelerates change. For instance, several network functions can now be consolidated as software running on off-the-shelf hardware, and the networking team can add or subtract network functions and services via software changes.

EMA research has found that virtual network functions (VNFs) are the preferred consumption model for most remote site network functions and services. For instance, more enterprises prefer to deploy VPN endpoints as a VNF rather than via dedicated appliances (48% vs. 26%), and these numbers are similar for WAN optimization controllers. Forty-six percent (46%) of enterprises prefer to deploy WAN optimization controllers as VNFs compared to only 25% that prefer to deploy them as appliances. Enterprises were split their approach to WAN routing, with 37% preferring virtual routers and 36% prefering hardware-based routers.[6]

[5] EMA, "Next-Generation Wide-Area Networking," July 2016.
[6] Ibid.

Security

WAN transformation involves rapid change, an expansion of connected devices, and an increasingly distributed infrastructure. IT organizations need a security architecture that can support encompass and protect all of these elements. In fact, network infrastructure teams have identified security as a top networking initiative, with 47% of all survey participants indicating that security most impacted their decision-making this year.[7] Furthermore, 38% of enterprises say they are adding new security controls to address the growth of connected devices in remote sites, and 34% of SD-WAN adopters say improved network security was a top business driver for their implementation of the technology.[8]

When enterprises transform the WAN, they will need solutions that integrate security into the fabric of the architecture. Security policies should be applicable across clouds and by application type, user, device, location, connectivity choice, and much more.

Service Assurance Through Analytics

The network is a rich source of data that can reveal insights into infrastructure performance and business performance. When an organization applies advanced analytics to that data, it can reap many benefits. IT can align the network more closely with the needs of the business and support digital transformation. In other words, advanced analytics of this rich data set enables better service assurance. Today, 49% of network infrastructure teams apply advanced analytics to network data. Their top use cases for this analysis are network security monitoring (36%), network optimization (30%), and business process optimization (27%). By integrating advanced analytics technologies into the transformed WAN, an IT organization can ensure that the network is supporting the business adequately today and into the future.

Centralized Service Delivery

This final design tenet is critical. Centralized service delivery, whether enabled through on-premises tools or via the cloud, are what unites all the other pieces together into a truly transformed WAN. These are tools and technologies that pull data from the network, analyze it, and create digital services that enhance the value of the network and create new business opportunities.

Cisco Digital Network Architecture: An End-to-End Solution for WAN and Branch Network Transformation

Digital Network Architecture (DNA) is Cisco's solution for building networks that support digital transformation. Many enterprises view SD-WAN solutions as the key enabler of WAN transformations, but Cisco takes a broader view. While Cisco DNA encompasses an end-to-end architecture from the campus to the WAN and through to the branch office, Branch network and WAN transformation are foundational elements addressed by the architecture.

The first two pillars of Cisco DNA are Automation and Management, which Cisco enables with its APIC Enterprise Module (APIC-EM), an SDN controller that automates Cisco's entire network infrastructure product portfolio. APIC-EM offers an open, programmable software driven platform for managing Cisco WAN and branch infrastructure, both hardware and software. Cisco offers individual applications on top of APIC-EM to enable automation and troubleshooting capabilities. These applications include:

[7] EMA, "Network Management Megatrends 2016: Managing Networks in the Age of the Internet of Things, Hybrid Clouds, and Advanced Network Analytics," April 2016.
[8] EMA, "Next-Generation Wide-Area Networking," July 2016.

- Cisco Plug and Play, a day zero deployment application for provisioning network devices
- IWAN App includes a set of SD-WAN services that include hybrid WAN connectivity, performance-based routing, WAN optimization, and network security. They enable enterprises to build a hybrid WAN with best-path selection, integrated security, and optimized application performance.
- EasyQoS, which allows engineers to set quality of service settings for applications based on business intent. Rather than set QoS on each branch router one by one, EasyQoS can make the appropriate changes on all routers at once to set QoS across the entire network.

The second element of DNA is Virtualization. Cisco offers a couple of options for virtualizing and consolidating network functions and services in the branch. The first is IOS-XE, a network operating system optimized for programmability, centralized control, and support for third-party applications via API integration. Enterprises can run third-party network functions as virtual services on Cisco branch platforms that run IOS-XE, which include Cisco 3850 and 3650 switches, the ASR 1000 Series routers, and the ISR 4000 Series routers. Cisco also offers Cisco Enterprise NFV, a network functions virtualization software architecture that enables the delivery of network services like routing, WAN optimization, wireless LAN controller (WLC), and next generation firewall (NGFW) on x86 server platforms. IT organizations can use Enterprise NFV to consolidate devices in the branch into virtualized network functions on a single off-the-shelf server.

The third, DNA pillar includes Analytics, a series of services that can deliver added value to adopters of DNA by pulling data from the network, applying analytics, and creating new digital business opportunities in branch offices. One of the first examples is CMX Cloud, a cloud-based analytics service for location- and presence-based services. Leveraging data from Wi-Fi access points, this service can provide insight into wireless network user behavior in branch locations, such as retail stores, clinics, and restaurants. Enterprises can use this insight to optimize customer engagement in these locations.

Finally, DNA includes a trusted security architecture to protect branch networks in real-time. DNA's advanced threat defense capability delivers perimeter control protection, intrusion prevention, web security, and malware protection. DNA also offers dynamic multipoint VPN (DMVPN) services that secure connectivity through site-to-site and remote access technologies to protect sensitive enterprise communications. DNA users can also acquire a Stealthwatch Learning Network License, which provides security operations with visibility and analytics of network traffic and establishes a baseline for machine learning to detect anomalous behavior. Finally, DNA offers Umbrella (OpenDNS) for visibility at the DNS layer to protect direct internet access at the branch .

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Its people, products and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at thenetwork.cisco.com and follow them on Twitter at @Cisco.

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 or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3499.121516