Brought to you by:

vmware®

Software-Defined WAN

for dummies®
A Wiley Brand

Learn the overlay architecture of SD-WAN

Understand the principles of Software-Defined WAN

Prepare to deploy an SD-WAN network

Sanjay Uppal, VMware
Steve Woo, VMware
Dan Pitt, Open Networking Foundation
Special Foreword by Lee Doyle, Doyle Research

VMware 2nd Special Edition

About VMware

VMware software powers the world's complex digital infrastructure. The company's compute, cloud, mobility, networking and security offerings provide a dynamic, consistent digital foundation to deliver the apps that power business innovation. VMware is streamlining the journey to digital business for more than 500,000 customers globally, aided by an ecosystem of 75,000 partners, by unlocking value from today's technologies while enabling the integration of tomorrow's. With VMware, organizations are empowered to flex and harness new technology quickly, without disrupting operations or introducing risk. This year, VMware celebrates 20 years of breakthrough innovation benefiting business and society.

About the Open Networking Foundation

Launched in 2011 by Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo!, the Open Networking Foundation (ONF) is a growing nonprofit organization, with more than 140 members, whose mission is to accelerate the adoption of open SDN. ONF promotes a vendor-neutral approach to open SDN and OpenFlow technologies, standards and software while fostering a vibrant market of products, services, applications, customers and users. For further details, visit the ONF website at **www.opennetworking.org**.

Software-Defined WAN

Software-Defined WAN

2nd VMware Special Edition

by Sanjay Uppal, Steve Woo and Dan Pitt

SPECIAL FOREWORD BY **Lee Doyle**

for dummies®
A Wiley Brand

Software-Defined WAN For Dummies®, 2nd VMware Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-53558-4 (pbk); ISBN 978-1-119-53555-3 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Revision edition editor: Connor O'Brien

Production editor: Siddique Shaik

Business Development Representative: Karen Hattan

Senior Acquisitions Editor: Katie Mohr

Table of Contents

Foreword

Software-Defined WAN, or *SD-WAN* for short, is at the leading edge of software-based networking deployments. SD-WAN offers significant business value for organizations with distributed branches in terms of business agility and the ability to leverage *Internet bandwidth economics* – put simply, cost savings.

This *Software-Defined WAN For Dummies* book explains the way for IT and business managers to migrate to a distributed network which is less complex, more flexible and easier to manage. With this book, VMware and Dan Pitt make an important contribution to better understanding the future of WAN implementations.

Defining SD-WAN and Understanding its Importance

SD-WAN uses software and cloud-based technologies to simplify delivery of WAN services to branch offices. Software-based virtualization enables network abstraction that results in simplification of network operations. SD-WAN enables IT and business managers to deploy Internet-based connectivity (with its benefits of ubiquity, high bandwidth and low cost) easily, quickly and with quality, reliability and security.

Changing traffic patterns: SaaS, cloud, mobile, video

The evolution of IT technologies has altered traffic flows within distributed organizations. Not only do remote users require significantly more bandwidth (for example, when using video), but they also need to directly access SaaS/cloud-based applications such as Saleforce, Office 365, Lync and off-premise storage (such as Dropbox, Evernote, and so on). Traditional MPLS networks which transmit all traffic from the branch to a centralized data center can't offer low latency/high performance access to cloud applications. In addition, the security and management requirements associated with disparate traffic flows have added to the complexity of managing branch operations – thus increasing operational (staffing) costs for many IT organizations.

SD-WAN Benefits

In contrast, SD-WAN provides a wide range of benefits for distributed organizations, including:

- **Business agility.** Rapid deployment of WAN services (such as bandwidth and firewall) to distributed branch operations without the need to send IT personnel on-site. Bandwidth can be easily added (with additional circuits) or reduced as business requirements evolve.
- **Internet economics.** Internet connectivity (including cable, DSL and ethernet) is widely available, quick to deploy and a fraction of the cost of equivalent MPLS circuits. SD-WAN provides the benefits of reliable, secure WAN service at Internet price points.
- **Optimized cloud architecture.** SD-WAN eliminates the backhaul penalties of traditional MPLS networks and leverages the Internet to provide secure, high-performance connections from the branch to cloud. With SD-WAN, remote users will see significant improvements in their experience when using the cloud/SaaS-based applications.

Highlighting SD-WAN Buying Considerations

If you're an IT or business manager, consider the following criteria when evaluating SD-WAN deployments:

- **Ease of adoption and management.** A key benefit of SD-WAN is that it makes deploying WAN services at the branch fast and simple. SD-WAN solutions must be straightforward to deploy, and they leverage centralized provisioning to eliminate the need for trained personnel to visit remote sites.
- **Ability to migrate to hybrid WAN.** The majority of distributed organizations already have MPLS deployed to the branch offices. Organizations should be able to seamlessly deploy SD-WAN solutions (Internet circuits) without changing the existing MPLS network. Those organizations can, over

time, migrate traffic growth toward cost-effective Internet bandwidth.

- **Automation – traffic steering.** SD-WAN gives organizations the ability to prioritize traffic. The key is providing managers with easy-to-use tools for setting priorities and with features that automatically changes traffic flows according to current network conditions.

Reaching Conclusions and Making Recommendations

The increased deployment of cloud, SaaS, video and mobile applications has challenged IT and business managers to provide high-quality WAN services to the branch. Deploying and managing the WAN has become more challenging and costly as traffic flows decentralize.

SD-WAN offers compelling advantages for distributed organizations with critical branch operations, including the benefits of business agility, improved application performance and lower costs of bandwidth. Distributed organizations should consider SD-WAN solutions on the basis of their ease of use and management, ability to integrate with their existing MPLS network and the intelligence to automatically adjust traffic flows to current network conditions.

– Lee Doyle

Lee Doyle is principal analyst at Doyle Research, and provides client-focused targeted analysis on the evolution of intelligent networks, including SDN and NFV. He has over 25 years' experience analyzing the IT, network and telecom markets. During his 25+ years in the industry, Lee has written extensively on such topics as SDN, NFV, enterprise adoption of networking technologies and IT-telecom convergence.

Before founding Doyle Research, Lee was Group VP for Network, Telecom and Security research at IDC. Lee contributes to such industry periodicals as *Network World, Light Reading,* and *Tech Target.* Lee holds a BA in Economics from Williams College.

Introduction

Enterprise networks are the last frontiers to be undergoing the rapid transformation ushered in by computer virtualization and the adoption of cloud delivery models. Virtualization and cloud technologies brought new levels of IT flexibility, efficiency and cost benefits while leaving the underlying networks unchanged. As mobile devices and new applications entered enterprise workloads, networks struggled to meet the demands placed upon them. Network bottlenecks arise from the traditional architecture that is based on hardware-centric, proprietary and outdated technologies.

Software-Defined Networking (SDN) promises the solution to many of these problems with a software-based solution on commercial off-the-shelf (COTS) hardware platforms. The sophisticated software platform enables a transition from the proprietary hardware devices to software-defined networks that are programmable, agile and decoupled to keep pace with the innovations in enterprise IT.

Software-Defined WAN (SD-WAN) is the extension of SDN that is transforming the enterprise branch office. With SD-WAN, no longer are the advantages of SDN limited to the data center. SD-WAN abstracts network hardware into a control plane and multiple data planes that can be used with cloud-based management and automation to simplify the delivery of services to the branch office. This work is all done with the manageability, performance and reliability assurances that enterprises expect.

SD-WAN is in the spotlight and is gaining popularity in the IT world. With any new disruptive technology, existing incumbents and many adjacent solution providers go into a frenzy to gain a piece of the market. This activity is part of the IT hype cycle. However, vendors who provide solutions with real, measurable benefits often emerge as industry leaders and go on to define the technology space.

This book aims to explain the ideal solution and the real benefits of SD-WAN, and to pick out the key information for you, like the proverbial ‘wheat from the chaff’.

About This Book

This book describes a networking world that is less complex, more flexible and easier to manage. So is this book going to be a difficult read? Not at all! The brilliant engineers that have implemented the many layers of software that form SD-WAN have done all the hard work. This abstract view of the networking world means that you no longer have to worry about the multitude of details needed to manage a variety of networking hardware. Instead, you can just sit back and enjoy this quick read through the structure and advantages of SD-WAN.

Foolish Assumptions

We assume that you understand general data center and WAN networking concepts and that you have a passing knowledge of virtualization. We also assume that you have an interest in networking and network administration and that you are interested in providing benefits to your enterprise.

How This Book Is Organized

This book is organized into six chapters, which you can read in order or skip wherever you like. That's the great thing about *For Dummies* books. You can read only the parts you need or want to and don't have to read the rest. Or you can read it cover to cover. This book is written to suit all types of readers, including you.

- **Chapter 1: Taking an Overview of Software-Defined WAN:** This chapter gives you a soft introduction to SD-WAN.
- **Chapter 2: Surveying SD-WAN Architecture:** This chapter details the layers and elements comprising the SD-WAN architecture.
- **Chapter 3: Deploying SD-WAN:** This chapter describes many of the options for deploying SD-WAN – Internet-as-WAN, hybrid WAN and interoperation with traditional WAN.

- **Chapter 4: Counting the Benefits of SD-WAN for Enterprises:** This chapter elaborates the benefits for enterprises and the reasons for the fast adoption of SD-WAN.
- **Chapter 5: Looking to the SD-WAN Future:** This chapter assesses the impact that SD-WAN has had on the connected world.
- **Chapter 6: Top Ten Considerations for Enterprise Adoption of SD-WAN:** As the transition from tradition WAN to SD-WAN accelerates, this chapter points out the top things to consider.

Icons Used in This Book

To make it easy to navigate to the most useful information in this book, we use icons to highlight key text:

TIP

The target draws your attention to top-notch advice.

REMEMBER

The knotted string highlights important information to bear in mind.

WARNING

The bomb alerts you to potential pitfalls to watch out for.

Where to Go from Here

As with all *For Dummies* books, you can either take the traditional route and read this book straight through from front to back, or you can dip in and out at any point you like. Just use the headings as your guide for pinpointing the information you need. Whichever approach you choose, you can't go wrong. Either way, you'll gain a better understanding of Software-Defined WAN. Dive right in!

IN THIS CHAPTER

- Figuring out what Software-Defined WAN is
- Discovering the need for SD-WAN
- Exploring SD-WAN features

Chapter 1
Taking an Overview of Software-Defined WAN

In this chapter, you discover what Software-Defined Wide Area Network (or Software-Defined WAN, or SD-WAN) is. You find out why you may need this network solution and what it can and can't do for you. You also explore the features of Software-Defined WAN.

Defining Software-Defined WAN

Software-Defined WAN provides the advantages typically associated with Software-Defined Networking (SDN) in data centers but for wide area network solutions for enterprise branch offices. Both SDN and SD-WAN virtualize resources to provide accelerated services delivery, better performance and improved availability by automating network deployment and management while improving return on investment and reducing the total cost of ownership.

SDN in general applies to any networking environment. Web-scale Internet companies have led its adoption, primarily in massive data centers and secondarily in the links between them, followed by telecom service providers in a variety of scenarios: radio access

networks, virtual evolved packet core, virtual customer premises equipment, multilayer integration of optical and packet networks, and more.

Meeting the SDN principle of network abstraction

The basic principle underlying SDN is that it abstracts the network to a set of capabilities that are independent of how those capabilities are provided. As a result, applications that use the network don't have to include specific details of the network equipment, details that change over time. SD-WAN provides a software abstraction to create a network overlay and decouple network software services from underlying hardware WAN circuits.


REMEMBER

With the new abstraction, IT managers can control and manage their network more easily than has been possible with managing underlying hardware for WAN networks. This network overlay provides a common interface across different physical components to ease the overall network administration and enable network owners to develop their own infrastructure-independent applications.

Separating functionality into control and data planes

SD-WAN separates functionality into a control plane layer and a data plane layer. The *control plane* is the part of the network that is responsible for signaling traffic and making packet routing decisions. It also includes device system configuration and management. The *data plane* is part of the network that carries application and user data.

Essential to this concept is that one logical instance of the control plane serves multiple instances of the data plane (typically switches and routers). In traditional networks, each instance of the data plane contains its own control plane, making programming of the network impossible.


REMEMBER

This separation of layers has several benefits:

- Network service agility is increased as more of the intelligence is moved from the data plane into the more abstract and programmable control plane.

- The control plane provides management of an ever-larger and more diverse set of data plane components or physical resources and devices.
- A communication protocol, such as the standard OpenFlow protocol, enables the communication between the control plane and the various data plane components. (This protocol is often called the *Southbound Interface* (SBI) because it is south of the control plane in an architectural diagram.)
- An API, or application-programming interface, enables applications to program the network as an abstraction. (This API is often called the *Northbound Interface* (NBI) because it is north of the control plane in an architectural diagram.)
- Various options for both the NBI and SBI give operators choices, but eventually the industry will settle on a few open standards for these interfaces to facilitate multivendor interoperability.

Understanding the Need for SD-WAN

Businesses and their IT teams face three major challenges:

- Increased access cost for MPLS-based bandwidth to support application performance
- High complexity in branch deployments
- Architectural issues with traditional WAN that is both static and private, inhibiting the migration to dynamic and public cloud environments.

We explore each of these challenges in the following sections.

Dealing with applications hindered by expensive bandwidth

Businesses must ensure that their most critical applications, whether customer-facing or productivity tools for their employees, run continuously and perform well. However, businesses increasingly deploy distributed architectures and business structures in their quest to be close to their customers and partners. And, they expect their application experience at the most remote

branch site, connected by a wide area network, to offer the same performance and robustness as if the user accessed the application at the company headquarters or data center.

To achieve this local area network (LAN)-like performance, enterprises have traditionally purchased and operated private networks, such as private T1 access to an MPLS service with service level assurances. Often, multiple, dedicated private networks are deployed – one for each different application. However, these private networks are expensive, costing anywhere from $200 to $800 and more per month for just 1.5Mbps of capacity. This cost hinders the ability of the enterprise to support more demanding real-time applications, such as VOIP, video conferencing, collaboration and virtual desktops.

Internet services, including broadband that offers ever-increasing amounts of bandwidth at low cost, offer an attractive resource. However, Internet services generally fail to perform at business grade as they do not come with the manageability, performance and reliability assurances that businesses desire. Instead of using the Internet for primary access to applications and data, business often use it only for backup and less critical applications.

Tackling branch deployments delayed by IT complexity

Businesses need to be close to their customers and to respond to market demand as quickly as possible, which means supporting both workers and customer-facing services in distributed branches, such as a new retail site, sales office, call center or logistics depot. However, branch deployments from an IT perspective are correctly reputed to be cumbersome and slow.

Typically, multiple network appliances must be delivered to a branch and installed by a skilled network engineer. Whether the appliance or other IT resource is provided by the enterprise itself or by a partner, the necessity of these on-site visits adds considerable cost and takes considerable time. The lead-time for the procurement and installation of private networks can extend to two to three months. In addition, skilled staff must configure the various components, not just for the remote site appliances but also for the supporting connections at the application data centers and headquarter locations. Often, the skills to perform these configurations depend on a thorough understanding of different equipment and carrier services provisioned at each remote site.

Considering cloud migration not supported by static architectures

As enterprise applications move to cloud data centers, such as Amazon AWS and Microsoft Azure, and increasingly adopt Software-as-a-Service (SaaS) applications such as Microsoft Lync, Salesforce and Box, businesses must choose the right architecture to access these applications. Not only must IT worry about day-to-day application and branch deployment issues, they must now prepare for a fundamental shift in the computing environment.

Businesses have relied on traditional private networks to provide secure, high performance and highly available access to applications residing within the walls of an enterprise's own headquarters and private data centers. Too often, the chosen architecture requires *backhauling* traffic intended for the cloud across the private network before reaching its destination (that is, sending network data over an out-of-the-way route to reach its destination). This backhaul does provide both the enterprise level of service as well as services delivered in the corporate data centers, but at a high cost. It imposes a performance penalty and consumes excessive amounts of the limited and expensive private bandwidth.

Cloud applications reside outside private enterprise sites. A cloud-based dynamic architecture can access multiple rapidly changing locations and deliver the flexibility and agility that most businesses require. No business can afford to sacrifice the same levels of security, performance and availability of a private network, so an Internet-based cloud solution offers a nearly ideal way to enable direct access from each branch to the many cloud application destinations.

Figuring Out What SD-WAN Is Not

REMEMBER

SD-WAN is a comprehensive solution comprised of many components, but

- It does not include the traditional, book-ended WAN optimization that is applicable for only the private-MPLS links and for TCP only connections.
- It is not just multilink WAN bonding with path control.

- It is not just the last mile solution with a cloud gateway to provide caching and acceleration techniques to applications.
- It is not multilayer integration of packet and optical networks in a telco backbone.
- It is not private, dark-fiber networking that avoids telco services.

Discovering the Features of SD-WAN


REMEMBER

In a nutshell, SD-WAN

- Virtualizes the network
- Enables a secure overlay
- Simplifies services delivery
- Provides interoperability
- Leverages cost effective hardware
- Supports automation with business policy framework
- Monitors usage and performance
- Supports interoperable and open networking
- Enables managed services

The following sections describe these functions in more detail.

Virtualizing the network

SD-WAN as a network overlay enables application traffic to be carried independently of the underlying physical or transport layer, offering a transport-independent overlay. Multiple links, even from different service providers, constitute a unified pool of resources, often referred to as a *virtual WAN.*


REMEMBER

This capability enables SD-WAN to provide high availability and performance for applications. It also increases the utilization of resources and simplifies the network.

Network operators can add new links and applications easily because no static tie exists between the application and the link it must use – a key benefit of the abstraction principle. The virtualization also provides self-healing as links experience degraded performance.

Enabling a secure overlay

SD-WAN provides a secure overlay that is independent of the underlying transport components. SD-WAN devices are authenticated before they participate in the overlay.


REMEMBER

Any combination of circuits and service providers can support secure, encrypted transmission, and the separated control plane enables automated configuration and key management across the multitude of branches. Additionally, a network designer can include segmentation as an overlay that is both independent and consistent across the various underlying components.

Simplifying services delivery

SD-WAN programmability does not just cover connectivity policy, it also extends to the insertion of network services, whether on the branch customer premise equipment (CPE), in the cloud or in regional and enterprise data centers.


REMEMBER

The business-level abstraction simplifies configurations to both route the traffic to the service delivery node and to configure the policy. Business-level abstraction simplifies complex configurations of traffic routing and policy definitions.

Providing interoperability

SD-WAN provides the ability to incrementally add resources and interoperate with existing devices and circuits. This capability follows directly from the separation and abstraction of the control plane from the data plane.


REMEMBER

SD-WAN also satisfies a key design goal to enable multiple circuits, devices and services to coexist and interoperate. APIs enable integration into existing and different management and reporting systems deployed by enterprises.

Leveraging cost-effective hardware


REMEMBER

SD-WAN improves cost effectiveness and flexibility by leveraging commercially available hardware and network appliances or servers. The separation of the control plane from the data plane enables the use of standard hardware for the data plane.

Virtual appliances can be remotely delivered and take advantage of existing or standard commercial off-the shelf (COTS) servers. However, the initial installation and configuration of these servers typically requires on-site IT installations. This form factor is likely well suited to larger branches as well as campuses and/or data centers. Virtual appliances are also deployable in hosted cloud environments.

Custom-designed network appliances based on standard CPUs, memory and other components can still capture the cost benefits of commercially available silicon, yet provide the advantages of purpose-built hardware. Custom-designed appliances will come with just the right configuration out of the box, thus enabling deployment in sites without IT support, which can be a significant advantage for smaller and remote branches without on-site IT resources.

Supporting automation with business policy framework


REMEMBER

SD-WAN enables the abstraction of configuration into business-level policy definitions that span multiple data plane components and also remain stable over time, even as the network changes. The control plane provides the programming flexibility and centralization over a diverse and distributed data plane. Enterprises can expect application awareness and smart defaults to provide further abstraction from the detailed transport level details. Policy definitions can refer to users and groups, the applications they should use and what level of service they should receive.

Notably, this abstraction from the physical layer enables the self-provisioning delivery model. Devices no longer require preconfiguration on a per-device basis; instead, they inherit the configurations and policies based on their assigned role in the network.

Monitoring usage and performance


REMEMBER

SD-WAN provides consolidated monitoring and visibility across the variety of physical transports and service providers, as well as across all remote sites. This monitoring capability offers business-level visibility, such as application usage and network resource utilization. SD-WAN adds detailed performance monitoring across all components of the data plane. Coupled with the

business policies, performance monitoring enables intelligent steering of application traffic across different paths and resources within the virtual WAN network.

Supporting interoperable and open networking

REMEMBER

SD-WAN further improves agility, cost effectiveness and incremental migration via its approach of open networking, interoperability and evolving standards.

Two organizations at the forefront of SDN and open networking are

- **Open Networking Foundation (ONF):** The Open Networking Foundation champions open, vendor-neutral SDN architecture, interfaces, protocols and open-source software with the goal of accelerating SDN's commercial adoption.
- **Open Networking User Group (ONUG):** The Open Networking User Group (ONUG) is a community of IT business leaders who exchange ideas and best practices for implementing open networking and SDN designs. There is an ONUG Working Group for SD-WAN.

Enabling managed services

Many enterprises, even the largest, outsource the management of their branch networks and WAN to either managed IT providers or to their network service providers. Additionally, some cloud application providers, such as Unified Communications as a Service (UCaaS) providers, provision and manage the circuits needed for accessing their applications.

REMEMBER

To address this business requirement, SD-WAN should enable managed service providers (MSPs) to manage the WAN networks of their clients with a multi-tenant infrastructure. In addition to the management and orchestration functions, the data center networking components should also be designed for multi-tenancy and scalable virtual deployment in providers' cloud data centers.

IN THIS CHAPTER

- Comparing traditional WAN and SD-WAN solutions
- Exploring the SD-WAN architecture
- Understanding the SD-WAN layers

Chapter 2
Surveying SD-WAN Architecture

Traditional WAN has lagged behind the proliferation of applications, especially online and collaboration applications, and major IT trends, including migration to the cloud. Businesses focus on being close to the customer, and agility and cost consciousness have also outpaced traditional WAN that has traditionally been static and slow to change.

Identifying the Challenges that Face a Traditional WAN

The following sections describe WAN requirements and how each requirement has challenges when using traditional WAN.

Need to simplify WAN for enterprise branch offices

WARNING

Providing WAN solutions for enterprise branch offices using traditional techniques has several challenges:

- Box-by-box manual configurations are complex.
- QoS configurations are created manually. Parameters like bandwidth are manually entered and do not adapt to changes in link conditions.
- Management is on-premise only.

Inefficient WAN utilization

WARNING

Providing WAN solutions for enterprise branch offices using traditional techniques has the following challenges:

- Manual routing protocol tuning required to load balance traffic.
- Ineffective use of all available WAN resources. WAN circuits are often in passive standby for use only in hard failover situations.
- Use of Layer 3 and Layer 4 aware routing. Decisions are based on only availability and distance, which is often manually tuned.
- When a link failure occurs on WAN, routing protocol takes several seconds to converge, resulting in a poor experience for the end user. Traditional WAN uses active-standby deployments as active-active deployments are complex to manage and scale.

Secure communications

WARNING

Internet Protocol Security (IPSec) VPN is commonly used to secure corporate traffic over Internet/broadband or private links. However, traditional VPN solutions have the following challenges:

- A pre-shared key is used to authenticate IPSec devices. It is easy to deploy, but managing large number of pre-shared keys across multiple devices does not scale and is less secure.

- Public Key Infrastructure (PKI)-based authentication meets the scale for IPSec; however, it is complex to deploy as it requires setting up and involves managing another system called Certificate Authority (CA).

Rigid WAN circuit requirements

WARNING

Traditional WAN delivers reliable application experience only over private circuits. However, private circuits often run into these challenges:

- New or additional private circuits involve lengthy provisioning times.
- Circuits are often very expensive and can't support the bandwidth needs for newer applications.
- Turning sites up and down (for example, on construction sites or pop-up retail stores) is extremely difficult.

Complex service delivery

WARNING

New services at the branch often require manual installation of additional appliances at the enterprise branch. This often leads to a complex stack of appliances at the enterprise branch and a need for additional racks and IT management of the equipment.

Cloud migration

WARNING

Providing WAN solutions for enterprise branch offices using traditional techniques has the following challenges:

- Internet, SaaS and cloud-hosted applications are still backhauled over private networks and through the centralized corporate data center.
- Expensive private networks are congested.
- Backhauling leads to performance penalties.
- Configuring encryption to cloud data centers is a repetitive manual process.

Managed Service Provider ready

While many enterprise businesses look for solutions deployed by in-house IT, many rely on managed service providers to offer WAN solutions. However, traditional WAN solutions are not purpose built for MSPs and have the following challenges:

- Managed Service Providers (MSPs) are in a unique situation of needing to manage multiple distinct customer organizations, often in a single dashboard, and to look for systems that are not only role based and multi-tenant but scaled typically to thousands of end customers.
- MSPs need to avoid truck rolls and costly overheads. Complex CLI-based troubleshooting requires lengthy training cycles for network operations staff.
- MSPs like to reduce lengthy cycles in order to deploy expensive private circuits.

Analyzing SD-WAN Architecture

The SD-WAN architecture has these three layers (from bottom to top), which you can see in Figure 2-1:

- Secure cloud network
- Virtual services delivery
- Orchestration and analytics

The following sections describe each of the layers in more detail.

Secure cloud network

Secure overlay is a transport-independent overlay that can work across any combination of public or private circuits. This layer should enable connectivity to both enterprise data centers and SaaS applications.

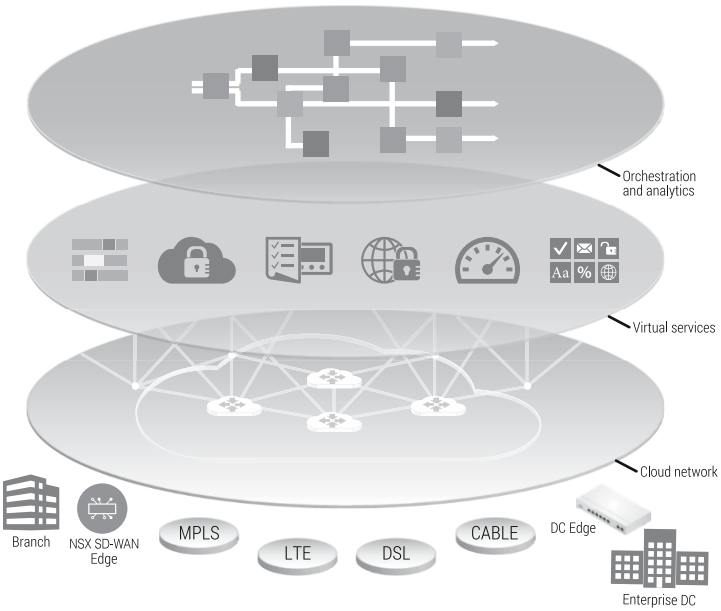

FIGURE 2-1: SD-WAN architecture.

Address the issues with traditional WAN

WARNING

Traditional WAN delivers security and performance across private links to applications that reside on a customer data center, an arrangement that has two issues:

- Traditional WAN ties a customer to a private circuit for enterprise grade security and performance. In this scenario, the customer loses the flexibility of transport independence.
- Backhauled SaaS applications experience performance penalties because of the traditional WAN.

REMEMBER

SD-WAN addresses these issues by delivering transport independence that is both secure and reliable across a combination of private-only, hybrid, dual Internet and Internet-only sites. SD-WAN should optimize access to both on-premise and SaaS applications. At the core, SaaS applications should have the ability to go direct to Internet with security to reduce impact of backhaul. For enterprise SaaS applications like mission-critical collaboration applications that require a highly resilient WAN with dynamic path forwarding, it is optimal to have dual-ended service

with the node hosted in the cloud, often close to the SaaS application that could offer per-packet application steering.

Branches should automatically multi-home and establish secure connectivity to multiple cloud and on-premise gateways. Multi-homing to multiple gateways enables direct access to cloud data centers and applications while still enabling assured performance, monitoring and additional dual-ended services, and thus eliminates backhaul penalties.

Transport-independent secure overlay also helps MSPs to bring up new sites quickly by leveraging ordinary broadband links and thus helping customers to get sites up and running before private circuits come in. To achieve this goal, MSPs should ideally look for solutions that can offer reliability for voice and video even over inexpensive public Internet links. Once the private circuit comes in, hybrid transport gets added as a part of the virtual resource pool automatically, thus offering even better WAN availability.

Create a scalable, secure cloud network

SD-WAN uses standard based encryption, such as AES, to provide secure connectivity over any type of transport, thus forming a secure cloud network.

Before a new SD-WAN device can participate in the secure cloud network, it needs to be first authenticated to the SD-WAN management plane. Once authenticated and authorized, the SD-WAN device downloads its assigned policy and is granted access to the secure cloud network. Based on the policy, sensitive traffic can have separate encryption keys to isolate itself from the rest of the traffic.

REMEMBER

Security and optimization services can be delivered at a cloud node or on-premise node based on the traffic type. Additionally, the network layer picks the best combination of links and gateways based on security criteria and performance requirements of the applications and users.

Virtual service delivery

A rich set of services, including those from ecosystem partners, should be easily deployable from a list or catalog of applications. Based on the type of service, these could be delivered at the branch, in the data center or in the cloud. These options help to reduce device sprawl in the branch.

Services in the branch

Some services, like a firewall, could run only in the branch, while others, like WAN optimization, need to be bookended at the destination, such as the data center. SD-WAN should simplify how these services are delivered in the branch. Customers can also benefit from a self-service application catalog. In addition to end customers, service providers can leverage the platform to deliver managed CPE offerings with dynamic services often called network functions or services virtualization.

Services delivered from a regional data center

Enterprise on-premise services, such as firewalls and Web security gateways, among others, can be partially or completely centralized rather than deployed at every branch. Centralizing reduces the number of devices and IT effort required to provision every branch with these functions. However, the appropriate traffic from each branch must then be forwarded to one of multiple regional data centers or a centralized data center.

REMEMBER

Rather than setting up complex and static policy-based routing rules, SD-WAN enables one to easily orchestrate a business policy-based backhaul to a regional branch with a simple single click. However, instead of leveraging private only for backhaul, enterprise should also consider backhaul over a reliable and secure SD-WAN enabled overlay, thus enabling cost savings on expensive private links.

Services in the cloud

Traditionally, customers have chosen to backhaul data for security reasons or because Internet links were not reliable. Backhauling results in degraded SaaS application performance and inefficient use of expensive private link bandwidth.

Leveraging a direct-to-Internet path to access SaaS doesn't resolve Internet reliability and security concerns. One could leverage a combination of per-packet application steering with cloud Web security to deliver direct, secure, optimized access to cloud applications. This approach helps to eliminate backhaul penalties to a SaaS application and frees up private links for other corporate traffic.

REMEMBER

It is important to have a powerful orchestrator that has a business policy framework to easily orchestrate these services in the branch, regional data center or in the cloud.

Orchestration and analytics

SDN uses a control plane separate from the data plane to leverage commodity hardware, improve agility and avoid vendor lock-in.

The SD-WAN architecture uses a similar principle. The orchestration layer provides the control plane for forwarding traffic to and from the on-premise and cloud nodes, flexibly across the multiple underlying transports and with the policy-driven insertion of distributed network services.

The orchestration layer is failsafe and highly resilient, and additionally the data plane functions independent of the control plane. A cloud-delivered orchestration layer also simplifies end user deployments so that no IT administrator installation is required.

The orchestration layer has three functions:

- **Management plane:** The management plane has a consolidated dashboard for zero-touch deployments, configuration monitoring, troubleshooting and reporting.

  Zero-touch deployment extends zero-touch provisioning of a branch CPE to zero-touch WAN configuration by automatically performing WAN capacity and link characteristic measurements, including latency, jitter and loss, so that manual configurations of link characteristics are not required for configurations. Ideally, QoS policies should automatically adjust as the link conditions change.

  The management plane is also responsible for authenticating and authorizing new SD-WAN devices into the network. PKI is built into the orchestration layer to facilitate the identification of SD-WAN devices and the distribution of identity information. It also enables SD-WAN devices to securely authenticate each other and exchange encryption keys. The orchestration layer can stop a SD-WAN device from being able to participate in the secure cloud overlay by revoking the device identity.

- **Highly available and resilient control plane:** A highly scalable, resilient control plane that can be offered on a commodity hardware is a requirement of SD-WAN. The control plane itself could be on-premise or optionally cloud hosted. An SD-WAN control plane should allow for customer migration from legacy WAN to SD-WAN by interoperating with existing L2/L3 infrastructure with minimum configuration changes.
- **Business policy framework:** A business policy framework defines policies at the business level, meeting service assurance, security and corporate governance requirements.


REMEMBER

Scalability and multi-tenancy of SD-WAN control and the management plane helps MSPs to manage multiple customers with a single unified dashboard.

Appreciating the Advantages of SD-WAN over Traditional WAN


REMEMBER

An SD-WAN has several advantages over a traditional WAN.

- **Simplified WAN:**
  - Rapid deployment and automation
  - Quality-of-Service (QoS) that adjusts with automated link and capacity monitoring
  - Scalable secure communications over any transport
  - Management and orchestration that can be cloud delivered or on-premise
- **Efficient WAN utilization:**
  - Unification of all available WAN links to provide aggregate capacity
  - Distributed, cloud-based services with simple policy-based insertion
- **Assured application performance:**
  - Forwarding based on real-time evaluation of WAN characteristics, including quality and capacity of the link

- Dynamic reactions to meet business policy based on performance or security criteria
- Active-Active support to provide subsecond reaction to WAN blackouts or brownouts so that application flow can be continued

» **Highly available WAN:**

- A physical transport-independent overlay for managing user connectivity and experience to different applications
- Greater flexibility in choosing and changing service providers
- Faster provisioning times and automated configurations
- Delivery of performance and security for on-premise and cloud applications. No backhaul performance penalty

» **MSP ready:**

- Central management and troubleshooting of complex customer environments
- MSPs move from connectivity play to service delivery offerings
- Elimination of expensive truck rolls and lengthy deployment cycles

IN THIS CHAPTER

- Using SD-WAN and cloud
- Using SD-WAN with Internet links
- Using SD-WAN with hybrid WAN

Chapter 3
Deploying SD-WAN

In this chapter, we explore different deployment options available for connecting branches with SD-WAN. Unlike traditional WAN networks, which relied solely on private links based on MPLS protocol, SD-WAN offers different flexible link options for accessing cloud applications and data center-hosted applications.

Connecting Enterprise to Cloud Services with SD-WAN

One of the main drivers for utilizing Internet/broadband links to connect branch sites is the adoption of cloud services, from Infrastructure-as-a-Service (IaaS) providers, such as Amazon Web Services (AWS), to Software-as-a-Service (SaaS) providers, such as Salesforce.com, Office 365 and WebEx.

The traditional WAN architecture does not lend itself well to connecting enterprise branches to cloud services. Why? Typically, all Internet-bound traffic gets backhauled to a central site via expensive private WAN links, for several reasons:

- The traffic to the SaaS is still required to go through centralized services, such as security scanning, filtering and monitoring.

- The branch typically does not have robust connectivity to the Internet and needs to rely on the Internet connectivity at the central site.
- The traffic backhauling, typically referred to as the *hair-pinning* or the *trombone,* makes inefficient use of private WAN bandwidth while introducing unnecessary latency that affects application performance and the end-user experience.
- The promise of SD-WAN rests with the flexibility to utilize Internet/broadband links to augment or, in some cases, to replace expensive private WAN links. It also enables traffic to be sent directly to cloud services over Internet/broadband. SD-WAN business policy specifies whether the selected cloud applications should be sent directly to the Internet, redirected to other cloud services for additional network services or backhauled to a central site – for example, sending trusted SaaS applications, such as Salesforce.com, direct via a broadband/Internet link instead of backhauling through a central site.
- The need to send Web traffic over a broadband/Internet link to a cloud Web security service.
- The need to backhaul email traffic to a central site to be scanned by a data-loss prevention (DLP) appliance.

As shown in Figure 3-1, Without SD-WAN, combining Internet/broadband and private WAN links requires complex setup and, even then, only rigid traffic patterns are allowed. It is an administrative nightmare to keep track of all the IP addresses of each application and manually tune the routing across each link based on the application and the condition of the links.

REMEMBER

SD-WAN simplifies the WAN by using business policies and automation. How? For SaaS applications, an enterprise chooses applications and decides whether to send the applications directly to the cloud, insert additional cloud service or backhaul to a central site, with a specified business priority: high, medium or low. For enterprise applications hosted in an enterprise data center, an enterprise can just specify the business priority. The SD-WAN solution selects the most appropriate link to deliver the applications based on the business priority and the real-time link conditions.

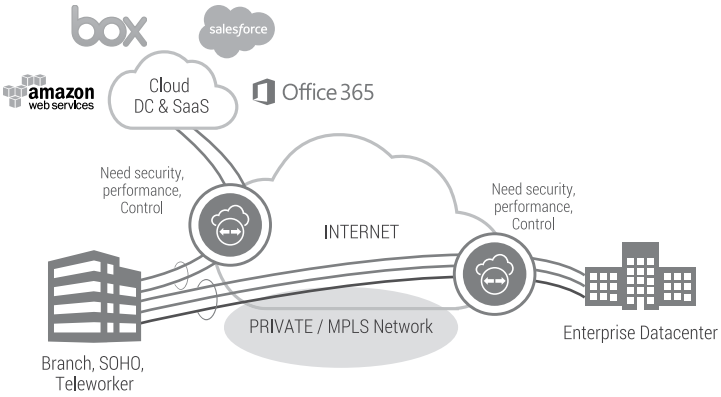

FIGURE 3-1: The SD-WAN solution.

WARNING

There are two issues with sending traffic directly over the Internet/broadband links without SD-WAN:

- The enterprise cannot easily guarantee the availability or performance of these applications at the levels achieved when traversing private corporate networks. The Internet/broadband link fails to deliver the performance required by applications – for example, it fails to deliver good real-time application performance 25 per cent of the time, according to *VeloCloud Internet Quality Report* 2H/2014.
- When sending the traffic direct, enterprises have no place to deploy additional security and visibility services.

REMEMBER

SD-WAN enables the enterprise to send SaaS applications and Internet Web traffic directly over Internet/broadband while maintaining visibility, control and performance. This can be accomplished only by having additional footprint in the cloud, and the software nature of SD-WAN makes this possible. In addition, SD-WAN can insert network services regardless of where the traffic is sent.

Looking at Deployment Options

Enterprises that have already starting using the Internet/broadband are often still using it for less critical purposes, such as a backup link. However, with the increase in cloud adoption

and video applications, the demand for WAN bandwidth increases drastically. The ability of SD-WAN to fully leverage Internet/broadband links enables additional branch architectures that can fully utilize Internet/broadband links as part of enterprise WAN, while still maintaining the reliability and performance that private links can deliver. Figure 3-2 and Table 3-1 show examples of the SD-WAN deployment options.

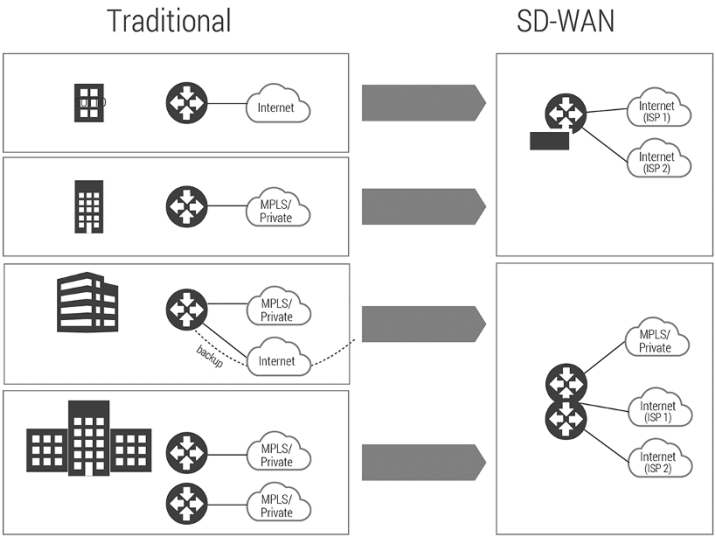

FIGURE 3-2: SD-WAN deployment options.

TABLE 3-1 Deployment options by branch type

Branch Type	Traditional WAN	SD-WAN
SOHO, Small office	Single Internet branch	Dual-Internet WAN branch
Small office	Single private WAN	
Medium office	Private WAN with backup link	Hybrid WAN branch using one or more private WAN and Internet
Large office	Multiple private WAN	

Internet WAN branch using SD-WAN

This type of branch terminates one or more Internet links, which can be any combination of broadband, wireless (3G, 4G LTE) and fiber. It provides a reliable, secure connection to the enterprise data center and differentiated access to public cloud services. Critical business applications and low priority traffic traverse the same Internet links, though at different service levels.


REMEMBER

With two Internet/broadband links, the ability of SD-WAN to dynamically steer application on a per-packet basis, in the middle of the active sessions, can greatly improve the reliability and performance of the applications.


REMEMBER

In addition to steering, to overcome transient performance issues seen in Internet/broadband links, SD-WAN can perform on-demand remediation, such as Forward Error Correction (FEC), to mitigate the underlying performance issue. The end result is having an Internet WAN branch that is capable of supporting enterprise real-time applications more than 99 per cent of the time, according to *VeloCloud Internet Quality Report* 2H/2014.

Hybrid WAN branch using SD-WAN

Hybrid WAN utilizes a combination of private WAN and Internet links. While enterprises do utilize dual private WAN links, increasing private WAN bandwidth can be cost prohibitive or slow due to the circuit availability. A properly designed SD-WAN overcomes the challenge of managing the application performance across heterogeneous networks.


REMEMBER

SD-WAN business policy abstraction provides full utilization of all the available links without requiring an operator to manually tune the routing protocol for every application over each link. As an example, high priority real-time applications can traverse the more reliable private WAN links while still being able to use the Internet/broadband links for bursts. File transfer applications can utilize the aggregate bandwidth across all links. If enterprises require an application to be pinned to a specific link for compliance or security reason, SD-WAN provides a very easy option to control the link selection on a per-application basis.

Maximizing the Performance Benefits of Using Heterogeneous Networks

SD-WAN deployment supports heterogeneous networks, including dual Internet/broadband links, wired and wireless links and private and public links. These different links have great variation in performance characteristics based on type of links and even the time.

Most of these links are also asymmetric in nature. For example, DSL, cable and wireless links typically have different upload and download speeds; wireless links have different latency in upstream and downstream directions. Performance degradation, such as jitter, packet loss and increase in latency, is typically a result of network congestion that is also unidirectional in nature. In other words, network congestion in the upstream direction is independent of the downstream direction.

REMEMBER

To maximize the benefits of having multiple links in heterogeneous networks, SD-WAN measures performance of upstream and downstream directions separately. In addition, it makes steering and remediation decisions for each direction independently. Why? If a congestion in the upstream direction significantly increases the latency or packet loss in the upstream direction, measuring just the Round Trip Time (RTT) or overall packet loss will render the whole link unusable, while it is still possible in this case to use the downstream direction of the link. It is desirable for SD-WAN to send the upstream traffic of the same flow on one link and the downstream traffic on another link if these are the link and direction that deliver the performance that application requires. SD-WAN overlay makes the using of different links and directions transparent to the end user and the application.

In order for solution to be Managed Service Provider (MSP) ready, all layers should have multitenancy with partitioned data storage with reliable design that doesn't have any single point of failure. It should be scalable at multiple levels to hundreds of thousands of branches.

Migrating to SD-WAN

REMEMBER

Enterprises should be able to migrate to SD-WAN without having to rip out and replace their traditional WAN devices. It is imperative that an SD-WAN solution be deployable on an incremental basis and interoperates with existing enterprise devices. Here are some examples:

- **Example 1: Connect the new SD-WAN branches to the data center:** Adding SD-WAN sites should not mean replacing the WAN headend or requiring a new datacenter device. The SD-WAN solution should not mandate a SD-WAN headend but support standard IPSec, which is already widely used by enterprises. This does not mean every SD-WAN device should establish IPSec connectivity to enterprise VPN headend as doing so defeats the simplicity that SD-WAN promises to deliver. Instead, SD-WAN can provide a footprint in the cloud that terminates the connectivity from SD-WAN devices. Then only one IPSec VPN is needed from the SD-WAN cloud into enterprise VPN headend.
- **Example 2: SD-WAN device and branch firewall:** At a branch location where an enterprise already has an existing firewall, an SD-WAN device sits in front of the firewall's public interface. It terminates the WAN connectivity and presents the aggregate bandwidth to the branch firewall. Enterprises can maintain the same security policies they already have on their firewall but now with more bandwidth, ease of management and the reliable connectivity that SD-WAN provides. Because the SD-WAN device faces the Internet directly, it should be locked down or have basic firewall capability to accept only applicable traffic.
- **Example 3: Existing MPLS WAN router with SD-WAN offload:** Enterprises want to offload certain traffic to the SD-WAN device without having to make significant configuration changes to the existing infrastructure, which may include the WAN router and layer 3 LAN switch. The SD-WAN device should be able to attract the portion of the traffic it wants to be sent through SD-WAN overlay. Through routing protocol such as OSPF, an SD-WAN device advertises the subnets to or from which it wants to process the traffic. Once the specified traffic arrives on an SD-WAN device, SD-WAN policy decides whether the traffic should be forwarded through the SD-WAN overlay or handled by the traditional WAN device.

- **Example 4: Secure and optimized communication between SD-WAN branches:** Enterprises should ensure that they have secure and optimized communication between SD-WAN branches. Traditional hub-and-spoke architectures are static and can result in non-optimal application performance. As an example, a video call between employees in two branch offices in Florida with their data center in California typically needs to hairpin via California. To circumvent this problem, traditional WAN sets up another static tunnel between branch offices in Florida. However, as the number of branch offices increases, not only do their customers run into scalability and management challenges, but also the statically defined WAN wouldn't perform reliably if these remote branches are connected over Internet VPN. An SD-WAN device should solve scalability, manageability, reliability and security for branch-to-branch communications.

IN THIS CHAPTER

- Accelerating enterprises to the cloud
- Improving business agility with lean branch offices
- Creating a better IT budget management

Chapter 4
Counting the Benefits of SD-WAN for Enterprises

Disruptions in IT are primarily driven by the unmet needs in the enterprises that hinder growth. For the enterprises with significant numbers of branch offices, stitching multiple WAN-related technologies together is an onerous commitment. SD-WAN delivers a strong set of business results to fulfill many of the unmet needs of enterprises, both large and small. This chapter walks you through those results.

Improving Business Agility with a Software-Defined Solution

Businesses need to be close to their customers at the branches and to support the organization's growth. Enterprises grow by adding more branches to serve customers where they are, and every branch is growing bigger to be the hub of multiple services for the customers. Both types of growth require enterprises to be agile to expand current network infrastructure and be able to provision more services per branch.

WARNING

Traditional branch networks with hardware-based static architectures have hindered the agility required by modern enterprise organizations. Every new branch requires elaborate IT planning to scope the capacity and impact on the current data center network, complex deployment and provisioning plans and multiple truck rolls prior to installation to prepare the branch. Current static architecture not only consumes inordinate IT planning and resources, but also consumes a significant portion of the budget.

REMEMBER

SD-WAN solutions include features to eliminate the bottlenecks of hardware-based static architectures:

- Flexibility and automation from decoupling of the hardware-centric data plane functionality from the software-centric control plane
- Faster deployment, on-demand bandwidth elasticity and faster disaster recovery with virtualization of the transport links into a unified pool of resources enables IT to mix-and-match transport links of different types from different ISPs
- On-demand network services instantiation, such as security services like VPN, or a firewall based on business-defined policies, with a virtual service delivery platform from the secure cloud gateways

A combination of these features enables IT to provision branches faster, modify bandwidth and services on-demand at the branches without complex configuration changes and respond to business growth needs faster without extensive network redesign and capacity planning.

Driving IT Efficiency with Automation and Cloud Management

Traditional branch network solutions have not met the IT requirement to improve and maintain high efficiency. With the need for every new branch or branch expansion comes a long list of requirements at every stage: pre-deployment, deployment and ongoing management in both data center and branch network. These requirements are manual, time-consuming and repetitive with the current architecture, resulting in an inefficient IT management.

REMEMBER

SD-WAN solutions include features to solve these problems and usher in new levels of IT efficiency with automation and cloud benefits:

- Does not need data center scalability or capacity redesign in the pre-deployment phase to meet the needs of the additional branches. With SD-WAN, data center headend is a cloud gateway that is horizontally scalable, multi-tenant with high availability and redundancy built-in.
- Zero IT touch deployment and thin provisioning from the centralized SD-WAN management edges are designed so that a non-IT person in the remote branches can simply connect and power it up. Edge then calls home to the orchestrator for the recent software update, network configuration and the relevant business policy. There is no pre-staged configuration of the Edge or need to have central IT walk through an installation live with remote IT personnel.
- Automation and the intelligence-in-the-cloud gateway headend eliminate the bottleneck of network traffic hair pinning (or the trombone effect). Once the Edge is deployed, it connects to multiple cloud gateways based on the traffic destination, specific application, governing policy and the best path for end-to-end performance. Unlike traditional branch network solutions with hardcoded paths, SD-WAN dynamically routes the traffic to go directly to SaaS portals or public cloud infrastructure, such as Amazon AWS or Microsoft Azure, without going through the data center.
- The last piece of the puzzle that improves enterprise IT efficiency is the single pane of glass management that is business policy driven. A unified policy framework enables SD-WAN to orchestrate custom policies across hundreds and thousands of branches efficiently from an intuitive, UI-based portals. The same portal provides consolidated visibility across all branches and WAN links, making it efficient for IT to manage multiple ISPs. Additionally, it includes complete application recognition and visibility to fine-tune link utilization and proactively troubleshoot application performance issues.
- The SD-WAN solution includes real-time monitoring, historical reporting and troubleshooting tools as part of the management portal. These features help IT to manage and troubleshoot issues centrally and avoid expensive onsite visits.

Enabling the Migration to Cloud Services and Applications

REMEMBER

As the adoption of cloud applications and the proliferation of mobile devices accelerate in the enterprises, IT needs features and tools to meet end-user expectations and aid business growth:

- Cloud deployment or service options allow the delivery of services even when directly accessing cloud data centers and applications. Cloud deployment in combination with an on-premise footprint at the branch enables dual-ended services covering the last mile between the branch and any cloud destinations.
- SD-WAN's ability to add broadband/Internet as part of the enterprise WAN, yet with assured performance and availability for the most demanding real-time applications, enables direct access to cloud applications.
- Application recognition and visibility helps IT to fine-tune WAN link management and proactively mitigate performance issues.
- SD-WAN simplifies the configuration of traffic forwarding to utilize cloud-based network services, such as Web security, WAN optimization and others. SD-WAN also optimizes the performance of the overlay network across the Internet to provide the same confidence as if using services within the enterprise's private network.
- Rapid deployment and Internet-as-WAN options enable IT to connect users in pop-up, temporary branches with reliable connectivity.

Reducing Overall Costs and Helping IT Budget Management

REMEMBER

All the benefits of a solution do not mean much if they do not reduce costs. The SD-WAN solution with the software-centric approach optimizes the IT cost, leveraging the benefits of virtualization and cloud:

- Cloud gateway-based SD-WAN architecture eliminates data center upgrades or redesign costs. It reduces or eliminates data center reconfiguration and equipment replacement costs with SD-WAN solutions that provide multiple options for integrating into existing architectures, including cloud deployment options.
- Leveraging a virtual service delivery platform eliminates the branch costs associated with single-function devices.
- WAN upgrade costs are reduced with the option to mix private/MPLS and ordinary broadband/Internet links.
- Branch edge cost is reduced via the availability of a virtual device to install on any COTS-based branch server.
- Automated and zero IT touch deployment eliminates all costs associated with truck rolls to the branches.
- Cloud-based orchestration, configuration and business-policy enforcement automates the deployment of numerous branches from a central location. No need for remote IT in the branches.
- Single pane of glass management console manages all the edges, WAN links, application performance and security policies and eliminates silo network management consoles and associated costs.
- In addition to incremental, flexible and interoperable deployment options, some SD-WAN solutions may also lower costs with available pay-as-you-go subscription models.

IN THIS CHAPTER

- Understanding the scope of SD-WAN
- Understanding the relationship of SD-WAN to mobility, the Internet of Things and NFV

Chapter 5
Looking to the SD-WAN Future

The technological shift from the current hardware-centric static WAN to a software-defined WAN is in its early stages. Eventually, SD-WAN will have a far-reaching impact on the connected world; this chapter explores the extent of that impact.

Surveying the Current Scope of SD-WAN

SD-WAN is currently being considered by enterprises for deployment to their remote sites and branch offices. These sites are physical structures but are quite varied, ranging from office buildings to construction trailers, pop-up retail locations inside malls and home-office locations for teleworkers.

The users in these sites are three-fold:

- The enterprises' employees work at these sites.
- Customers, especially in retail locations, such as pharmacies or financial organizations, visit these sites.

» Partner users also inhabit these sites – for example, at a construction site when a supplier needs to get access to her applications that are back in the data center or in the cloud.

The number of SD-WAN end points under this scope of users in physical branch sites would number in the millions to tens of millions.

Extending SD-WAN for Mobility

With the dramatic growth of smartphones, tablets and laptops, each individual user can now be considered to be their own branch office or remote site. Often called *micro branches*, the physical location of this branch office is not stationary. There is an incredible diversity of these locations, from coffee shops to a telecommuter on a train to a user on a remote oilrig.

In the mobile case, the users' end device is also the location of their SD-WAN edge. Therefore, there is the need for the SD-WAN edge software to be deployed on a smartphone, tablet or laptop. Because the physical location can change dynamically, so does the addressing of the WAN links.

For example, a user at a coffee shop may be on the coffee shop's Wi-Fi as well as on his LTE connection. The network address of each of these links can be dynamic, yet session persistence is required back to the data center and the cloud applications that the user wants to access.


REMEMBER

One of the benefits of SD-WAN for this end user is the ability to use both the Wi-Fi and LTE connections based on business policy. The business policy can state that the user can send highly secure traffic only through the use of the LTE connection, but that the user's voice calls use the Wi-Fi if the link quality is good or else jump over to LTE for that same call.

The number of SD-WAN end points under this scope of mobile users will number from the hundreds of millions to billions.

Pairing SD-WAN and the Internet of Things

As of the writing of this book (in 2018), there is tremendous and understandable excitement surrounding the interconnecting of things to the Internet. No longer are the end points human users but devices ranging from an exercise sensor to an industrial refrigerator.

REMEMBER

The emerging three-tier architecture of the Internet of Things (IoT) comprising sensors, gateways and the cloud fits very well with the SD-WAN framework. Each sensor would correspond to an end point in the SD-WAN context with the IoT Gateway being usually co-located with the SD-WAN edge.

Several IoT cloud services are already available both for the consumer IoT as well as industrial IoT. These cloud services can be inserted or chained into the SD-WAN framework, making the task of setting up an IoT network incredibly simple.

The IoT will cause the number of SD-WAN end points to be in the billions to tens of billions. IoT promises to bring not just a mass market for IoT services, but also significantly broaden the number of IoT developers. The open hardware movement has close parallels to the growth of cloud software in making formerly complex technology and processes available to a wide swath of the public. For example, the popularity of the Arduino microcontroller and the Raspberry Pi Linux computer have their underpinnings in simplifying computing and control for the masses. Extending this simplicity into the network is the end goal of SD-WAN.

Extending the scale of the WAN to billions of endpoints has interesting scale challenges. One of those is in the collection of analytics. The killer app for IoT is the incredibly rich information also known as *big data* that will tell us how each system in this world operates. Just the human body itself can easily contribute a thousand variables that would be useful – from the obvious ones like heartbeats to the more specific like foot pressure points of a runner. Each of these sensors will produce a time-series that will need to be aggregated across the SD-WAN to the orchestrator and then acted upon by automated functions with alerts for the human operator. The throughput required may be small, but the real-time nature of the information will require the SD-WAN

overlay to manage latency and jitter across a variety of wireless and wired networks.

Comparing SD-WAN and NFV

SD-WAN is a relatively recent development compared to the Network Functions Virtualization (NFV) push from the Communications Service Providers (CSPs). Close parallels exist between SD-WAN and NFV, and they intersect in at least a couple of use cases.

NFV use cases are quite broad, and include

- Virtualizing the Packet Core (vEPC)
- Virtualizing the Radio Access Network (vRAN)
- Virtualizing the Mobile Core Network and IMS (vMCN)
- Virtualizing CDNs (vDCN)
- Virtual Network Functions as a Service (VNFaaS)

Of these cases, VNFaaS is closely related to SD-WAN. One of the Virtual Network Functions that is being considered by ETSI (`www.etsi.org`) in their group specification is vE-CPE or vCPE.

The ETSI GS NFV 001 document states, '*today's enterprises are deploying multiple services at the edge-of-branch offices. Many enterprises find the cost of a dedicated standalone appliance per-feature prohibitive, inflexible, slow to install and difficult to maintain'.* Essentially, this use case is about virtualizing the Customer Premises Equipment (CPE) and replacing the hardware with a set of virtual functions. The vCPE use case for NFV can be implemented with an SD-WAN architecture that has a few key attributes:

- **Multi-tenancy:** Both the control and data planes should be multi-tenant and allow sharing.
- **Flexible location of virtual functions:** VNFs should be possible at the CPE or in the network (cloud), or at both locations.
- **Network or cloud-delivered services:** Services should be delivered from the cloud and not just from premises-based functions.

IN THIS CHAPTER

- Understanding the best practices with SD-WAN adoption
- Understanding the mandatory features of a SD-WAN solution
- Migrating successfully from traditional WAN to SD-WAN

Chapter 6
Top Ten Considerations for Enterprise Adoption of SD-WAN

This chapter is a handy ten-point checklist of best practices and the mandatory needs for enterprise IT considering the transition to SD-WAN architecture. As many enterprises grapple with the issues of traditional WAN and ponder where to begin the transition, this top ten-consideration checklist provides the jumpstart to get the process underway.


TIP

In case you're reading this chapter first, be advised that (in our humble opinion) there are no shortcuts to migrating from the traditional WAN to SD-WAN. Prior chapters describe the key architecture elements, key feature sets and subsection of details to plan for a smooth transition. This chapter is a checklist to understand the top considerations but is not the full recommendation by itself.

Also consider a purpose-built SD-WAN solution. As the need for SD-WAN gains momentum, many incumbent vendors with a solution like WAN optimization, multi-link bonding will bolt on a solution and call it an SD-WAN solution. Our recommendation is

to look for a purpose-built SD-WAN solution based on the top ten considerations in this chapter.

SD-WAN Considerations

The SD-WAN solution should steer application flows around network problems automatically based on the actual link conditions including both performance and capacity. More advanced implementations can provide per-packet steering on a sub-second basis that can move single application flows mid-session without any degradation.

Additional mitigation techniques can further improve performance, especially over broadband/Internet, when steering alone cannot avoid network problems.

Flexible Deployment Options

Flexible deployment options include a CPE, controller and orchestrator in physical or virtual form factor.

A cloud-hosted option enables ease-of-service rollout and optimized access to SaaS applications.

In addition, multi-tenancy should include both control and data plane separation to support security and enable service providers to deliver SD-WAN as a service for end customers.

Transport-Independent Design

Transport-independent design supports private, hybrid and Internet-only options. SD-WAN as a network overlay enables application traffic to be carried independent of the underlying physical or transport layer, offering a transport-independent overlay.

Network Service Insertion

You can reduce branch sprawl by insertion of network services in branch customer premise equipment (CPE), in the cloud, or in regional and enterprise data centers. Business-level abstraction simplifies complex configurations of traffic routing and policy definitions.

Incremental Migration and Interoperability


TIP

Look for a solution that provides the ability to incrementally add both sites as well as functions to a site and that can interoperate with existing devices and circuits. Both technical architectures as well as business models can enhance incremental migration to SD-WAN.

Optimized and Secure Access to SaaS and Enterprise Applications

SD-WAN should enable policy-driven direct access to SaaS and cloud data centers to avoid backhauling penalties while simplifying configurations. A data plane node in the cloud can enable optimization, such as dynamic path steering as well as the insertion of other services, even when directly accessing cloud destinations.

Scalable, Redundant and Resilient Control and Data Plane

Multiple links, even from different service providers, constitute a unified pool of resources, often referred to as a *virtual WAN.* The SD-WAN overlay infrastructure should also provide for a highly available architecture that is further enhanced with distributed cloud-hosted options.

Ease of ICOM (Installation, Configuration, Operations and Management)

SD-WAN eliminates box-by-box configurations and offers zero-touch deployments for branch sites. SD-WAN provides consolidated monitoring and visibility across applications, users and hosts, a variety of physical transports and service providers, as well as across all remote sites. This monitoring capability offers business-level visibility, such as application usage and network resource utilization.

Programmability

The programmability and ability to interoperate with other solution providers through APIs enables integration into different existing management and reporting systems deployed by enterprises and helps enterprises to integrate an SD-WAN solution.

A Secure and Encrypted Overlay

SD-WAN provides a secure and encrypted overlay that is independent of the underlying transport components. An SD-WAN solution should offer segmentation of sensitive traffic across both the local area network (LAN) and WAN. SD-WAN can avoid expensive backhaul by offering cloud-based security and optimization for SaaS applications.

Consider a Purpose-Built SD-WAN Solution


TIP

As the need for SD-WAN gains momentum, many incumbent vendors with branch network solutions like WAN optimization and multi-link bonding will bolt on a solution and call it an SD-WAN solution. Our recommendation is to look for a purpose-built SD-WAN solution based on these top ten considerations.

Notes

Notes

Notes

Notes

Notes

Notes

Simplify your enterprise branch network with Software-Defined WAN!

Deploying a wide area network, or WAN, may seem like a complex, daunting task. To help, this book is your quick, easy-to-read guide to understanding Software-Defined WAN, a technology that enables enterprises to migrate to a flexible, simple-to-deploy and easy-to-manage WAN solution. SD-WAN is a transformational approach to simplify branch WAN networking by automating deployment and improving performance over private, broadband Internet and LTE links for today's increasingly distributed enterprises.

vmware®

Inside...

- Understand the need for SD-WAN adoption for branch networking
- Learn the benefits of migrating to an SD-WAN solution
- Familiarize yourself with the key features of SD-WAN
- Learn about SD-WAN options
- Customize an SD-WAN adoption plan to your enterprise

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-53558-4
Not For Resale

for dummies® A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.