CenturyLink Business

SOLUTION BRIEF

SD-WAN: Simplifying WAN Complexity & Improving WAN Performance

Organizations with geographically dispersed locations often struggle with variations in network service. The Software-Defined Wide Area Network (SD-WAN) has emerged as a solution to address variations in network performance across locations. In combination with Network Function Virtualization (NFV), a closely aligned technology, SD-WAN addresses many of the common pain points faced by organizations that need to provide high-speed, economical network service to numerous sites. This paper explores how SD-WAN solves common network connectivity challenges experienced by distributed organizations.

Introduction

The old saying, "If it ain't broke, don't fix it" is popular in IT because it reflects an understandable reluctance to tamper with imperfect systems that still work. This view deserves to be challenged once in a while, though. Networks that connect distributed organizations, for example, may not be "broke," but as new alternatives emerge, they start to look expensive and cumbersome.

The sweeping virtualization changes that have altered the world of infrastructure, compute and storage now affect networks. Distributed organizations are beginning to embrace what is known as the Software-Defined Wide Area Network (SD-WAN). SD-WAN reinvents the traditional WAN using the power of virtualization. Network virtualization has been transformative because it replaces purpose-built network hardware with generic compute power capable of running almost any application. The resulting value proposition is so much better: Costs get lower; bandwidth gets bigger; analytics get more detailed; installations get faster; availability is essentially everywhere globally; security gets stronger; and most importantly, critical applications work as expected.

SD-WANs ease a number of pain points that affect businesses with geographically dispersed branches. This paper looks at pressing issues with traditional WANs that can be addressed by SD-WANs. These include management of multiple vendors, a lack of visibility into performance and uneven service levels as well as high overhead and capital expense.

SD-WAN Overview

As with any new set of technologies, categories overlap and labels can be confusing. SD-WAN is often lumped together with Network Function Virtualization (NFV) and Software-Defined Network (SDN). They are related technologies but not the same thing. NFV is an emerging set of standards that makes it possible to operate networks using commodity hardware instead of the purpose-built legacy network equipment. Figure 1 shows a simple comparison between NFV and the legacy hardware network.

Networks, for good reasons, had always been constructed using routers, switches, firewalls and so forth that were designed with exacting specifications, proprietary circuits (ASICs) and performance characteristics. While it was possible to run network traffic through a basic server, this kind of hardware was not up to the job until recently.

Now, with NFV, it is possible to have an "off the shelf" server handle high-volume network traffic due to its increased compute power, built-in network cards and other network features included. Combined with parallel advances in virtual machine management and the development of cloud infrastructure, NFV enables large-scale networks using virtualized elements.

The advantages of NFV are evident in many use cases, but they can be a bit abstract. SD-WAN takes the precepts of NFV and shapes them into a commercially viable product, designed to solve real-world problems. These include inconsistent bandwidth levels, irregular network performance across multiple sites and time-consuming manual network management processes. An SD-WAN makes NFV-powered network functionality available as a service. An organization can tap into the SD-WAN's features based on its locations and available Internet service providers.

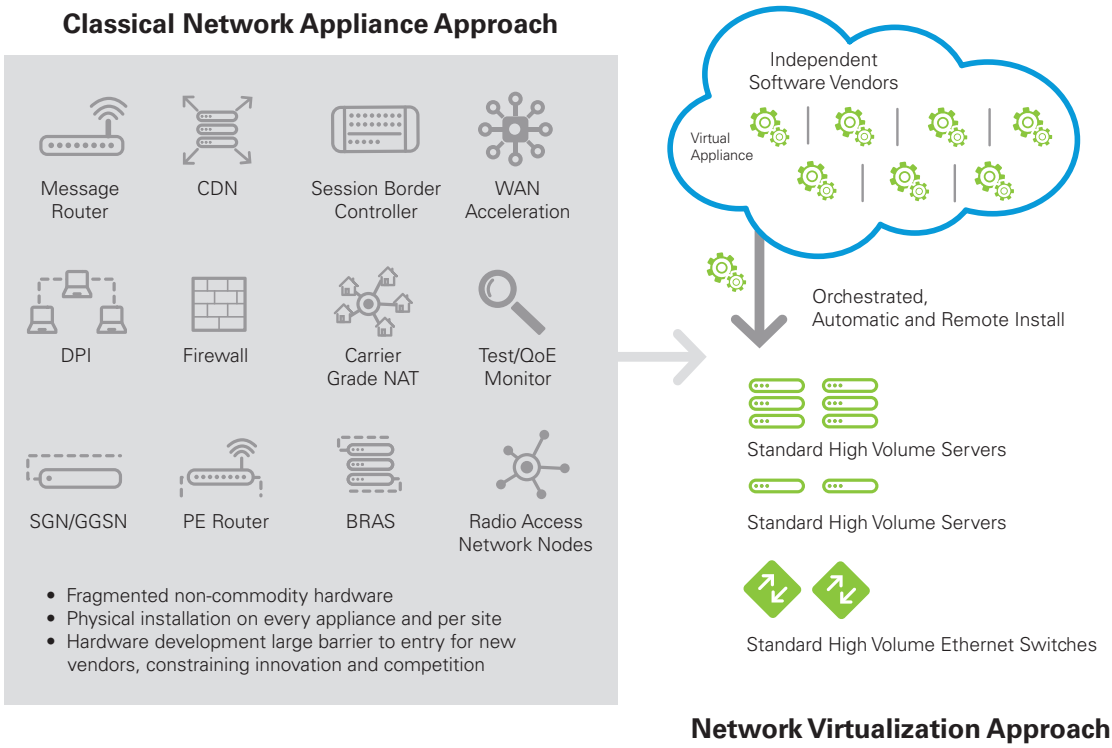

Figure 1 – Comparison between NFV and the legacy appliance-based approach to networks.

Wide-Area Network Pain Points

Traditional wide area networks can be challenging and resource intensive to manage. To illustrate common pain points addressed by SD-WAN, consider the simplified example of a distributed organizational network shown in Figure 2. This might be a retail chain or a business with branch offices. They have a WAN for locations near headquarters. Remote locations need to use a broadband connection and VPN to reach the main corporate data center.

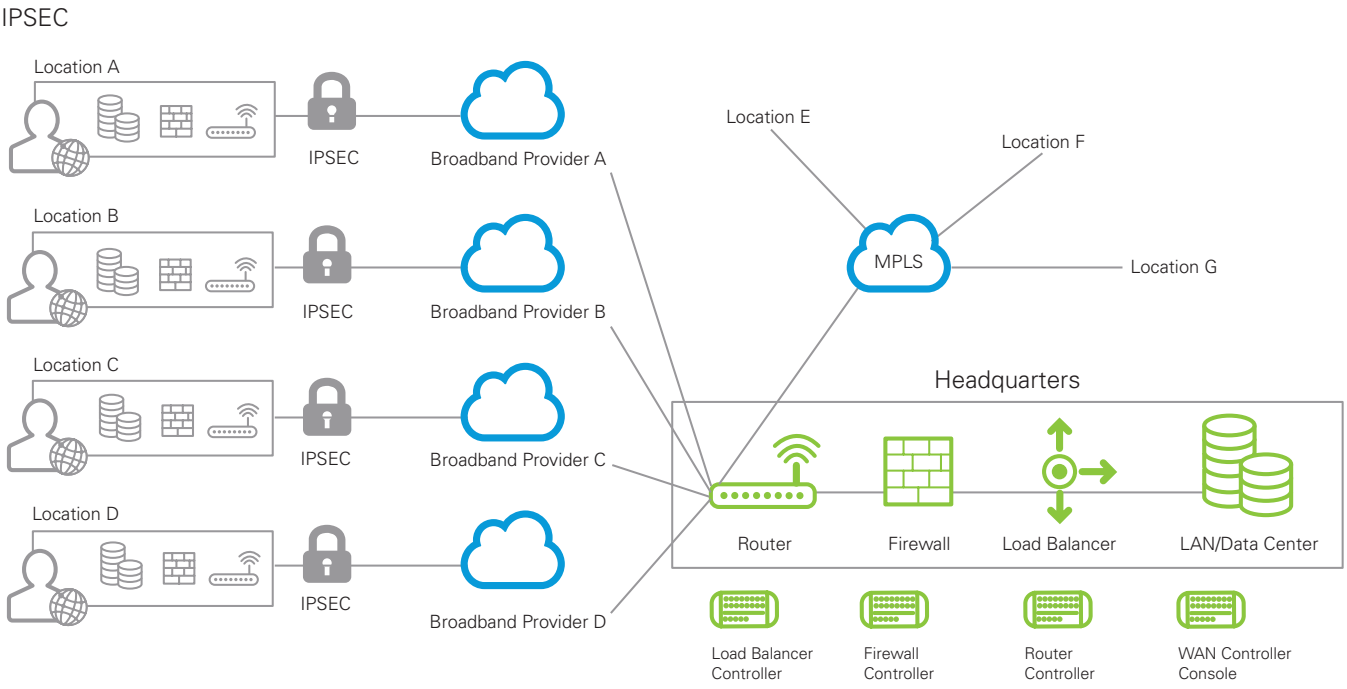

Figure 2 – Network architecture for distributed organization that relies on multiple broadband networks to reach remote locations.

This networking approach can cause pain for the organization. While the network functions, perhaps even well, it is slow and costly to operate. Challenges include the following:

- **Managing multiple vendors and network types**: The organization has to stay on top of multiple network vendors. If it were a large retail chain, there might be dozens of vendors, including cable broadband providers, metro Ethernet services, telcos and so forth. Each vendor would have its own service contract, service levels, and terms and conditions. The manager at each remote location, who likely handles the network as just one small part of a much bigger role, is responsible for dealing with any immediate network issues.
- **Lack of visibility for network and application performance**: In this scenario, headquarters does not have good visibility into how the scattered third party networks are performing. Application performance, which may be subject to an enterprise-wide service level agreement (SLA) by IT, can suffer from slowdowns that headquarters will not be able to see. Or, if they see them, they will not be able to explain or remediate them.
- **Difficulty managing a large number of endpoints**: Each endpoint in this network requires its own dedicated setup, with a firewall and router. These purpose-built hardware elements need to be installed manually. Specialized equipment for the broadband provider may also be required. Managing these endpoints is resource-intensive. Network specialists must visit the sites to install equipment and make changes to configurations.
- **Lack of agility for new site turn ups and service adds**: Organizations are not static, especially retail chains with multiple locations. They open new stores, close underperformers, lose their leases and change sites. With the setup shown in Figure 2, each physical move requires reinstalling physical network equipment and perhaps dealing with yet another network carrier. This is not an insurmountable challenge, of course, but it slows down the process of moving or updating network capacity. It is also expensive, with trained technicians needed to make each change in person.

- **Uneven service levels between locations**: It is not guaranteed that different locations served by separate carriers will have varying service levels, but it is quite likely. Some locations will suffer from slow networks. This is not just a technical issue. Slow downs beget service desk calls and customer complaints. Outages and network difficulties can even have an impact on employee morale. Poor service ripples through the business and creates hidden costs.
- **High network costs for some locations**: A heterogeneous network is going to result in higher costs for some locations. This is unavoidable under the scenario shown in Figure 2. And, it's not even just a matter of pure cost. There will be striking differences in costs for different levels of service. In some locations, great service will seem like a bargain. In other places, the company will be overpaying for inferior service.
- **High administrative overhead at headquarters**: Networks with so many moving parts take a lot of people hours to manage. The multiple control consoles translate into multiple administrators and skillsets. Multiple providers mean numerous contracts, service agreements and invoices to process. Legal and procurement overhead will be (or should be) allocated to managing the network shown in Figure 2. In addition, the need to acquire and install large volumes of hardware adds administrative hours to the IT department and related business departments.
- **Hardware obsolescence / hardware footprint**: Networks that rely on purpose-built hardware have to deal with the inevitability of obsolescence. The network owners are in a constant mode of upgrading and replacing network hardware components. This accounts for more administrative overhead that has to be factored into cost. Adding new hardware may also create unforeseen conflicts which could require people, time and money to resolve. The actual physical footprint of the network at each location may cause problems as well. Setting up and maintaining dedicated network rooms in remote locations further drains resources and time.
- **High CapEx**: Hardware is a capital expense (CapEx). The practice of buying network hardware is so routine that the cash outlay may not register as anything out of the ordinary. To be fair, there wasn't much of an alternative until recently. Now, though, as network options proliferate, it is possible to see the CapEx of constant network hardware acquisition as a point of pain in IT management.
- **Securing the network**: While there is considerable value to be gained by the efficiencies SD-WAN delivers, improved security capabilities are an equally important benefit. Traditional Multi-Protocol Label Switching (MPLS) WANs have limited visibility into the types of traffic that traverse it, which masks vulnerabilities to security breaches. SD-WAN brings sweeping improvements in awareness of traffic that crosses WANs, improving the detection of anomalies and remediating them. SD-WAN also delivers a comprehensive framework for delivering security at the edge over broadband connectivity. This translates to a vastly improved and more efficient means of providing security at the premise versus today's patchwork security mix of broadband and IPSec.
- **Lack of guaranteed uptime**: Under traditional networking models, engineering for 100% availability was a costly proposition involving redundant circuits and service provider router diversity. In contrast, SD-WAN is designed to allow simultaneous use of multiple connections per site. With low cost, high bandwidth options readily available from wireless LTE or cable broadband providers, "always on" connectivity goes from "nice to have" to "easy to have."
- **Having to connect to a single network provider to receive maximum benefit**: MPLS has been used to build most of the private networks over the past decade. This robust technology is well-understood, with predictable performance and reliable architectures. The downside to MPLS is that customers need to connect all of their locations to a single network provider to effectively use features; e.g., multicast for video streaming, fast-reroute for backbone link failures, multiple closed user community configurations, traffic prioritization to make sure voice conversations have the highest quality possible, etc. Depending on where customer locations are located, there can often be expensive backhaul to get remote sites connected to the service provider network. Because Internet is available everywhere, and SD-WAN can leverage public connectivity, SD-WAN coverage is both more ubiquitous and more cost effective.

Benefits of SD-WAN

Moving the organization to SD-WAN will result in a network architecture like the one shown in Figure 3. Now, instead of dedicated hardware at each location, there is a connection to a provider's SD-WAN appliance. The SD-WAN appliances use open hardware standards to run NFV features that mimic the VPNs, routers and firewalls of the traditional network.

All of the network's purpose-built hardware is replaced by commodity hardware running virtualized network functions. Even though different carriers are providing the connectivity in certain places, they are transparent to the users and administrators of the SD-WAN. A single management console gives the administrators a unified point of control over the SD-WAN and a way to monitor its functioning across the entire network.

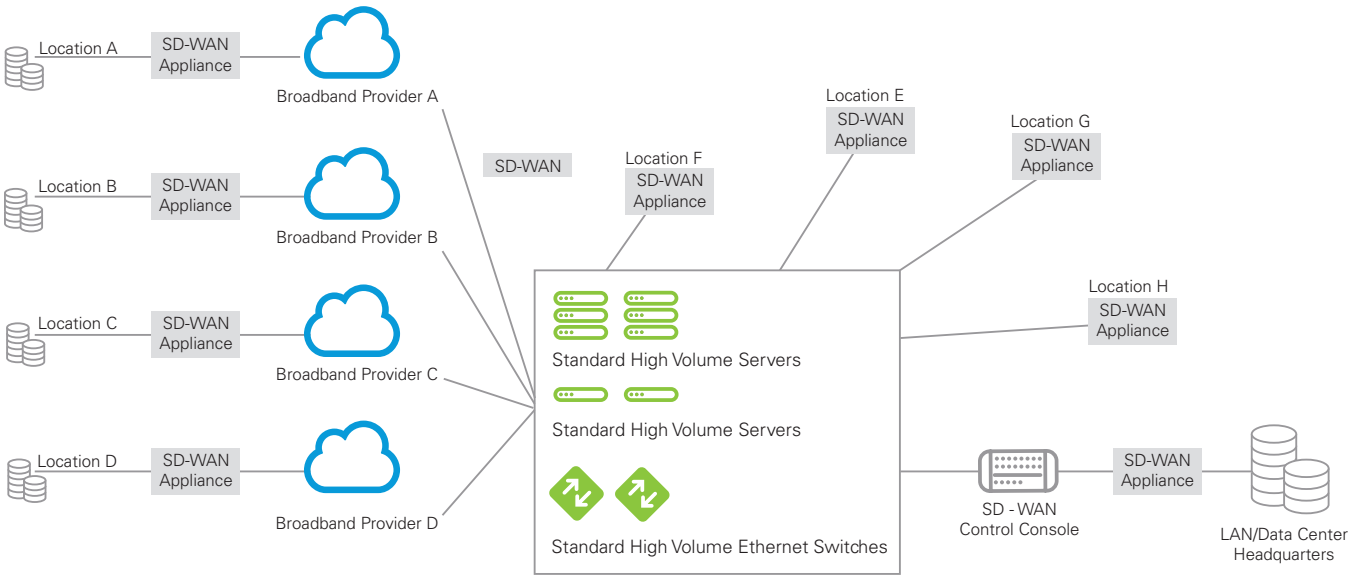

Figure 3 – An SD-WAN approach to the distributed organization.

SD-WAN is not a magic bullet, but it provides a solution for many of the traditional network pain points described above. The benefits of SD-WAN include:

- **One network type from multiple carriers**: With SD-WAN, there may still be multiple network vendors used across locations, but there is just one network type as far as the organization is concerned. It is easier to change network vendors with SD-WAN. The potential selection of carriers is also broader.
- **Clear visibility for network and application performance**: The SD-WAN's single console and uniform hardware and software deployment makes it possible to monitor network and application performance at any point in the network. Most SD-WAN solutions include a highly granular level of analytical reporting that covers typical network performance characteristics as well as application level performance, usage, and service level policies.
- **Simplified management of endpoints**: While it is still necessary to manage each endpoint in the SD-WAN, the uniformity of the endpoints makes the process much less administratively burdensome.
- **Ability to quickly turn up new site service adds**: With the use of software, rather than hardware, to make the network function, it becomes easier and faster to turn on new end points or change locations.
- **Even service levels between locations**: SD-WAN makes it possible to mitigate uneven service levels through its flexibility in carrier choice and its ability to scale services using NFV.
- **Streamlined network costs across locations**: With greater vendor choice and uniform hardware, SD-WAN evens out the cost differences between locations.

- **Lower administrative costs**: An SD-WAN's single "pane of glass" administrative console will result in lower administrative costs compared to the multi-site, multi-console approach required in the traditional setup.
- **Hardware obsolescence / hardware footprint**: Hardware obsolescence doesn't disappear with SD-WAN, but the process of dealing with it changes. Instead of having to replace purpose-built, specialized hardware on an erratic cycle that depends on the age of equipment at various locations, SD-WAN makes it possible to upgrade open standard hardware in bulk — along with other hardware upgrades — across the data center. It's a far more streamlined, cost effective acquisition process. On a local level, the hardware footprint shrinks substantially. Each location should have a single appliance that connects it to the SD-WAN, as opposed to the router/firewall configuration required previously. A switch is still needed, however.
- **Reduced CapEx**: CapEx falls dramatically with SD-WAN. There is no hardware for the customer to buy in most cases. In a service provider based SD-WAN model, the appliance at each location is usually provided and managed as part of the SD-WAN service agreement.

Conclusion

Every organization has its own potential level of fit with the SD-WAN concept. Some will find the technology more appealing than others. For distributed organizations, especially ones that rely on multiple carriers and network types in order to maintain connectivity with branch outlets, SD-WAN presents some major advantages. These include CapEx savings, simplified control and administration, and more reliable and visible service levels. For organizations that use aggregators, or function like "do it yourself" aggregators, SD-WAN presents an opportunity to take control of the aggregation process and manage it more efficiently and cost effectively.

About CenturyLink Business

CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America's largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.

Global Headquarters
Monroe, LA
(800) 784-2105

EMEA Headquarters
United Kingdom
+44 (0)118 322 6000

Asia Pacific Headquarters
Singapore
+65 6768 8098

Canada Headquarters
Toronto, ON
1-877-387-3764

©2016 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners. Services not available everywhere. Business customers only. CenturyLink may change or cancel services or substitute similar services at its sole discretion without notice.
789050916 -2- sd-wan-simplifying-wan-complexity-improving-wan-performance-solution-brief-CM160141

CenturyLink® Business