The 2017
Guide to WAN Architecture & Design

Part 2: WAN Evolution

By Dr. Jim Metzler, Ashton Metzler & Associates
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division

Sponsored in part by:

Table of Contents

Executive Summary

The wide area network (WAN) is a critically important topic for number of reasons. Those reasons include:

- The latency, jitter and packet loss that is associated with the WAN often cause the performance of applications to degrade;
- The WAN can be a major source of security vulnerabilities;
- Unlike most of the components of IT, the price/performance of WAN services doesn't obey Moore's Law;
- The outage of a WAN link often causes one or more sites to be offline;
- The lead time to either install a new WAN link or to increase the capacity of an existing WAN link can be quite lengthy.

A discussion of wide area networking is extremely timely for two reasons. One reason is that, for the first time in well over a decade, the wired WAN is the focus of considerable innovation which is leading to the deployment of a wide range of new WAN-related products and services. The second reason is that on a going forward basis, the WAN needs to support a new set of requirements such as providing connectivity to a growing number of mobile workers and public cloud providers as well as to the Internet of Things (IoT).

The primary goals of the 2017 Guide to WAN Architecture and Design (The Guide) are to make enterprise network organizations aware of the emerging alternatives to the traditional approaches to WAN architecture, management and security and to help them understand the key differences in those alternatives. The Guide will be published both in its entirety and in a serial fashion. This document, Part 2, is the second of the serial publications. This document contains the description of a hypothetical company called NeedsToChange and it also contains how VeloCloud suggests that NeedsToChange should evolve its WAN.

The other sections of The Guide are:

- Part 1
  This section focused on providing insight into the current state of the WAN. This document contains the results of a survey that was distributed in May of 2016. Throughout The Guide the network professionals who completed the survey will be referred to as The Survey Respondents.

- Part 3
  This section will have two primary sub-sections. One sub-section will summarize the key WAN architecture, management and security considerations that were brought out in Part 2. The second sub-section will be a detailed call to action.

- Complete copy
  The final publication will consist of an executive summary and Parts 1 – 3 as described above.

Hypothetical Company: NeedsToChange

VeloCloud was given the description of a hypothetical company: NeedsToChange. The goal was to present VeloCloud with the description of a company that has a traditional WAN and ask them to provide their insight into how the company should evolve its WAN.

Even within the context of a traditional WAN, there is a wide breadth of options relative to a company's WAN topology, services, applications and goals. As a result of this breadth, it isn't feasible to cover all possible options in a reasonably sized description of NeedsToChange's WAN. In order to limit the size of the description of NeedsToChange's WAN and yet still bring out a wide array of important WAN options, VeloCloud was allowed to embellish the description of NeedsToChange's WAN. They could, for example, add additional data centers or key applications; vary the amount of traffic that was backhauled; prioritize the factors impacting NeedToChange's WAN or identify business drivers such as the need to support mergers and acquisitions.

Below is the description of NeedsToChange's WAN that VeloCloud received.

1. **Data Centers**
   NeedsToChange has a class A data center in Salt Lake City, Utah. The site has two diversely routed T3 links into an MPLS network and a 100 Mbps link to the Internet.

2. **Traffic Prioritization**
   In the current environment, traffic is prioritized in a static manner; e.g., voice traffic always gets top priority and it receives a set amount of bandwidth.

3. **Business Critical Data Applications**
   Two of NeedsToChange's business critical applications are SAP and Product Data Management (PDM). PDM is NeedsToChange's most bandwidth intensive application, however it is widely understood that NeedsToChange runs its business on SAP and so the performance of SAP is critical. In addition to the applications that NeedsToChange uses to run its business, the company uses an Infrastructure as a Service (IaaS) provider for disaster recovery (DR).

4. **Public Cloud Computing Services**
   Other than its use of an IaaS site for DR, NeedsToChange currently makes relatively modest use of public cloud computing services. However, the company has started to implement Office 365 and the decision has been made that on a going forward basis, unless there is a compelling reason not to do it, any new application that the company needs will be acquired from a Software as a Service (SaaS) provider.

5. **Voice and Video**
   NeedsToChange supports a modest but rapidly growing amount of real time IP traffic, including voice, traditional video and telepresence.

6. **Internet Access**
   NeedsToChange currently backhauls over half of its Internet traffic to its data center in Salt Lake City. The company is looking to enable direct Internet access from their branch offices but they are concerned about security. NeedsToChange is also concerned that it is supporting non-business related Internet traffic that is negatively impacting business traffic.

7. **Mobile Workers**
   Roughly half of NeedsToChange's employees regularly work somewhere other than a company facility.

8. **Guest Workers**
   NeedsToChange's network organization is considering offering guest WiFi access from at least some of its facilities.

9. **Branch Offices**
   NeedsToChange categorizes its branch offices into three categories: small, medium and large.
   - A small office/site has between 5 and 25 employees. These sites are connected by an MPLS network with each site having either a single T1 link or multiple T1 links that are bonded. All of its Internet traffic is backhauled.
   - A medium office/site has between 25 and 100 employees. These sites are connected by an MPLS network with each site having capacity between a single T1 link and a link running at 10 Mbps. All of its Internet traffic is backhauled.
   - A large office/site has more than 100 employees. These sites are connected to an MPLS network either by using bonded T1 links or by a T3 link. They also have direct Internet connectivity which in most cases runs at 10 Mbps over DSL.

10. **Branch Office Availability**
    NeedsToChange wants to improve the availability of the WAN access at its branch offices and has established a goal of 99.99% availability.

11. **IoT**
    The company has begun a smart business initiative which the company believes is just the first in a number of initiatives that will quickly drive the need for them to support thousands, if not tens of thousands, of devices.

12. **Visibility**
    In the majority of instances in which the performance of one of NeedsToChange's business critical applications begins to degrade, the degradation is noticed first by the end users. In addition, the time it takes to identify and resolve performance problems has been increasing.

13. **Regulations**
    NeedsToChange is subject to PCI compliance. That is just one factor driving NeedsToChange to seek out ways to increase its security.

14. Factors Driving Change

While not in priority order, the following factors are driving NeedsToChange to seek alternative WAN designs:

- Improve application performance, notably for SAP;
- Reduce cost;
- Increase uptime;
- Reduce the time it takes to identify and remediate performance problems;
- Increase security;
- Reduce complexity;
- Provide access to public cloud computing services in general and Office 365 in particular;
- Provide better support for real time applications;
- Reduce the time it takes to implement new network services;
- Increased agility both in terms of supporting new facilities and in supporting growth within existing facilities

Balancing off the factors driving NeedsToChange to seek alternative WAN designs is the fact that NeedsToChange will not be allowed to increase the size of its network organization.

NTC Tackles the Future with VeloCloud Cloud-Delivered SD-WAN: Fast. Agile. Secure.

Speed has become the currency of business, and security threats have multiplied and soared in sophistication. Internet-connected devices (IoT) are growing explosively and has been an integral part of NTC's network traffic growth. They have already investigated the cloud-based application industry trend and confirmed that NTC's IT strategy should leverage this direction to gain agility and cost savings.

NeedsToChange (NTC) is aggressively rolling out Office365 to boost productivity and enable mobile users—but it plays havoc with visibility into traditional traffic patterns. While NTC is still a reasonable-sized company—3000 employees across 50 sites—there is a distinct possibility that a near-term acquisition will double the number of sites and headcount, as well as add another data center.

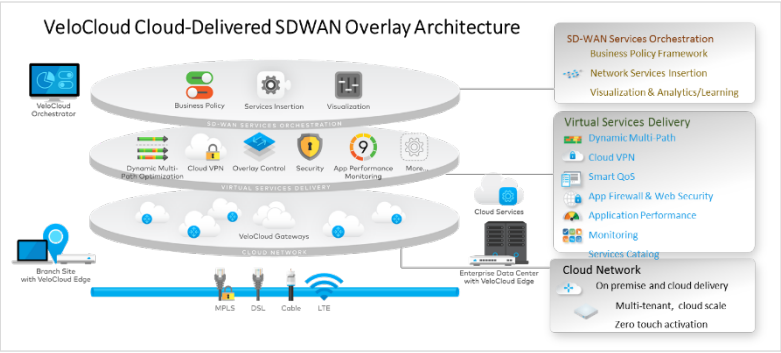
IT staff is concerned that the current WAN architecture—static traffic management, distributed policy enforcement, fixed-bandwidth access links, MPLS contracts—cannot prepare NTC adequately to support digital business imperatives and general network upgrades at current funding and staffing levels. There is no time for a slow evolution of equipment and connectivity, and there is no funding or staffing for a replacement.

A Network for the Future

VeloCloud Cloud-Delivered SD-WAN, overlaying NTC's existing traditional WAN, immediately delivers many benefits and positions NTC favorably for growth, industry trends and the potential acquisition, while also leveraging existing WAN infrastructure investments. **Cloud-based applications are seamlessly integrated** and immediately rolled out with equal access to mobile and branch-site users. Traffic is routed via the **shortest path** to either the NTC data center or cloud-based applications. **Adding a broadband link per site** relieves bandwidth limitations, delivers the goal of direct Internet access, supports IoT, increases application performance, and improves branch uptime. **Security is simplified and strengthened** by inserting VNF firewalling and traffic inspection in each network site, and using VeloCloud built-in automated VPN technology. VeloCloud **cloud-delivered orchestration** provides network-wide dashboards, traffic and performance visibility, as well as centralized policy control.

A VeloCloud Cloud-Delivered SD-WAN for NTC

The illustration shows the VeloCloud overlay architecture. Transport-independence works across ***any*** combination of circuits that NTC deploys. Branch offices and data centers may be equipped with virtual or hardware-based VeloCloud platforms, replacing or augmenting legacy equipment.

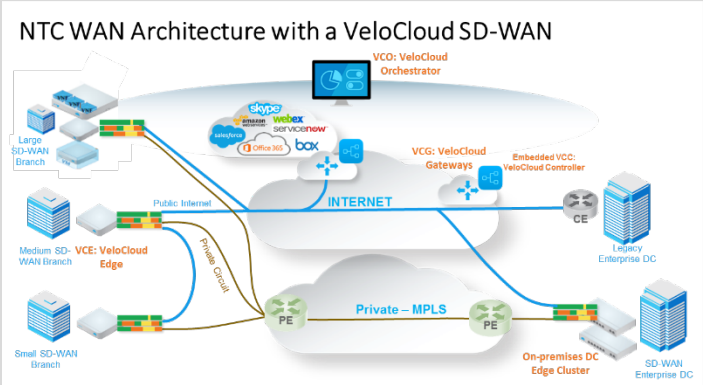


The network layer—consisting of VeloCloud Gateways, either on-premises or provider-based—enables connectivity to both enterprise data centers and IaaS/SaaS applications. A rich set of

virtual services, including those from ecosystems partners, are easily deployable from an application catalog. One essential service dynamically optimizes traffic over multiple links. At the top of the figure, the orchestration layer covers monitoring, configuration, policy coordination and unprecedented network visibility.

NTC Network Architecture: SD-WAN at Work

NTC's network architecture after implementing a VeloCloud Cloud-Delivered SD-WAN is shown below. Every site has broadband Internet and traditional MPLS connectivity. New sites do not require MPLS, and older sites may migrate to broadband when the MPLS contract expires, or both link types may co-exist indefinitely. NTC can make the most cost-effective decision per site. VeloCloud Dynamic Multi-path Optimization ensures a superior grade of service over any type of link.



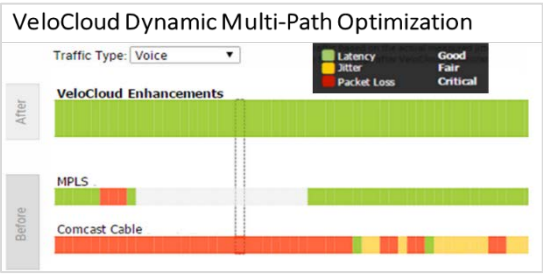
Most branch sites would be equipped with a hardware-based VeloCloud Edge platform (automatically deployed via the Zero-Touch capability), although larger sites that already support VM-hosting could be deployed with a VNF Edge. Data centers can be connected no-touch with legacy equipment, or with VeloCloud Hub Edges (virtual or hardware-based) when the time for site refresh is optimal.

Security services such as VNF firewalling are hosted in each site to secure the broadband connections. This eliminates the need to backhaul traffic to the data center—resulting in a better end-user experience and cost savings when the freed-up bandwidth is reused for PDM or other application traffic.

Essential Network Capabilities

Transport-Independent Branch Connectivity

VeloCloud's unique technology bundles traffic across multiple links and ensures enterprise-quality performance and security. A broadband link per site provides for NTC's desired Internet connectivity, relieving the backhauling of traffic through the data center, and also delivers critically-needed cost-effective bandwidth for IoT growth and convenient access for mobile users.

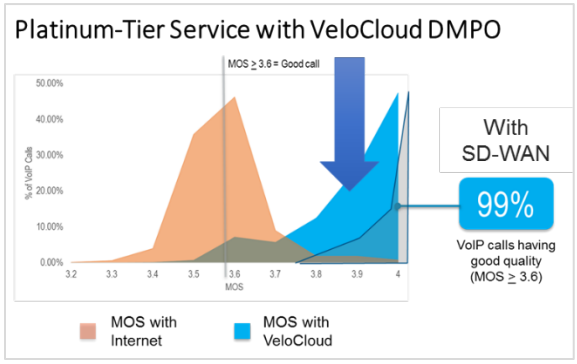


Links are auto-selected for traffic steering on a per-packet basis, based on (1) policy-driven priorities and business preferences, (2) auto-detection of application type, and (3) currently measured link performance. Mid-flow re-steering happens dynamically when changing link conditions are detected.

The illustration shows how VeloCloud technology achieves excellent performance across multiple links, each individually of lesser quality. The bundled multi-link connections (MPLS, broadband, LTE) provide increased branch uptime, headroom for IoT traffic, and elastic increases in cost-effective bandwidth.

Real-time Traffic—Superior QoS over Broadband

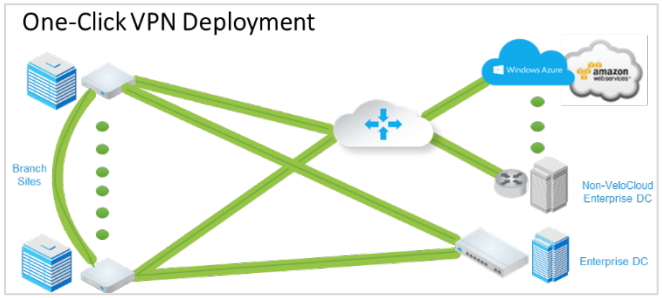
VeloCloud Dynamic Multi-path Optimization (DMPO) is a unique VeloCloud capability that assures application performance over any link types. A MOS score exceeding 3.6 (a good call) is maintained for 99% of calls with VeloCloud DMPO, while only 60% of calls achieve this without VeloCloud.



DMPO includes (1) *Continuous Monitoring and Analytics*: automatic capacity testing, link and path quality monitoring, tracking bandwidth, quality, packet loss, delay, and jitter; (2) *Dynamic Application Steering:* application-aware packet steering, aggregated bandwidth for single flows, maximizing throughput, sub-second reactions to network glitches ensuring no application impact; (3) *On-Demand Remediation*: error and jitter correction, automatic steering around brownouts/blackouts, link repair. DMPO maintains exceptional call quality and call success rates, and keeps video smooth and visible. IoT devices often reply on real-time-sensitive traffic that can be safely supported by deploying DMPO over broadband links.

Security

VPN deployment is significantly simplified with a VeloCloud SD-WAN. VPN any-site-to-any-site tunnels are automatically set up and secure all connections with strong PKI end-to-end encryption. Interoperable IPsec is supported directly to NTC's existing data center, and also connects to cloud-hosted data centers which may be a future NTC direction.



Scalability is achieved by eliminating the need for static hub-and-spoke VPN tunnels, and cost savings and simplicity derive from the automatic and dynamic set up of required tunnels.

Additional security services can be easily inserted with virtual instances of firewalls or other inspection engines. The cloud-delivered nature of a VeloCloud SD-WAN provides easy leveraging of cloud-based security providers offering sophisticated and cost-effective security with less demand on NTC IT staff.

Cloud Migration

Cloud applications can be accessed via the most direct path between the VeloCloud Edge and Gateway—a dynamic VPN tunnel ensures secure access with the Gateway dynamically bookending and aggregating connections on the cloud side. NTC can leverage VeloCloud or partner providers' multi-tenant Gateways already in place for IaaS and SaaS .

Orchestration

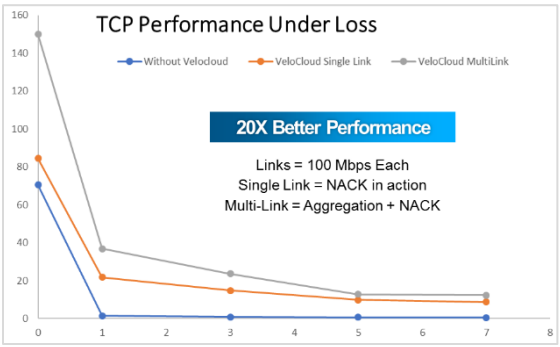
Cloud orchestration and controllers eliminate complexity and provide network-wide visibility and

control of policies and traffic patterns. Orchestration is hosted in the cloud or installed on-premises. As NTC commences rolling out SD-WAN capability, a hosted solution provides an easy entry point, while installing an on-premises solution may be preferable as deployment expands and the network hardens, especially if the expected acquisition takes place.

The VeloCloud orchestrator provides a consolidated dashboard for complete lifecycle management, including SLA measurements, remote diagnostics, link quality views, application analytics and bandwidth usage, network-wide business policy automation for traffic including voice and video, granular application and security policies, and multi-tenancy. The Zero-touch capability dramatically accelerates provisioning of new sites, while also significantly reducing IT staffing and costs.

Application Performance

Using the shortest path between the user and the accessed cloud site, in conjunction with VeloCloud Inbound Multi-source QoS and TCP Link Optimization capabilities, ensure optimal application performance. VeloCloud's Dynamic Application Steering and On-Demand Remediation capabilities allow sub-second packet steering around network problems to provide optimized performance for all traffic, and delivers a superior grade of service for real-time traffic to IaaS/SaaS sites as well as legacy data center applications.



Conclusion

VeloCloud Cloud-Delivered SD-WAN offers an overlay network architecture allowing flexible, cost-effective incremental migration, and legacy interoperability. Cost reduction results from Zero-touch site deployment, multi-link bandwidth aggregation and optimization, technologies ensuring enterprise-grade service over broadband links, virtual and hardware options for Edge and Gateway services, and dramatic simplifications in cloud application access and VPN tunnel configurations. Security is always up-to-date with the options of virtual service insertion or using a cloud security provider. The transport independent connectivity (including MPLS, Broadband, LTE, and cable) allows for cost-effective link redundancy and increased branch uptime, agility in connectivity, ready access for mobile users, and economical incremental bandwidth for IoT.

VeloCloud SD-WAN customers have realized many benefits, including migrating successfully to 100% Internet links without network redesign, achieving enterprise-quality connectivity with capacity better than the prior MPLS service, reducing branch migration to thirty minutes, meeting PCI 3.0 compliance, significantly reducing OPEX costs with VNF and Zero-Touch deployment, maintaining exceptional voice quality with greatly improved call completion, one-click propagation of services and policies across the WAN, lowering bandwidth costs, and improving performance for real-time cloud applications

VeloCloud can help NTC address enterprise IT challenges with a fast, simple, secure Cloud-Delivered SD-WAN to achieve reduced complexity, easy migration to cloud applications and services, simplified traffic patterns, and distributed Internet access.

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim's current interests include cloud networking and application delivery.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler or Steven Taylor.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer

All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.