silver peak™

presents

The Software–Defined WAN

The most common means for enterprises to connect branch offices into the corporate data center is predictable, reliable, and relatively secure. Yet multi-protocol label switching (MPLS) is also expensive and inflexible, often requiring months to bring up a new branch. Today's hyper-connected, cloud-based envrionments demand greater agility and efficiency. Enter the software-defined WAN, which can address this shortcoming in traditional WAN architectures by putting an overlay on top of them.

In this eGuide, *Network World* and *Computerworld* explore the trends in software-defined networks and offer in-depth advice on addressing the key limitations of today's VPNs. Read on to see how software-defined WANs could help your company maximize its investments in the cloud.

The First Place to Tackle SDN? In the WAN

Michael Elmore of Cigna argues that the best initial use case for SDN is in the wide area network

BY JOHN DIX, NETWORK WORLD | *Disruptive innovation in infrastructure is on the rise, and nowhere is that more evident than in the Software Defined Networking movement. But while much of the SDN discussion has focused on the data center, the better initial use case might be in the wide area network. One advocate of that approach is Michael Elmore, IT Senior Director of the Enterprise Network Engineering Infrastructure Group at Cigna, a global health service company headquartered in Bloomfield, Connecticut. Michael is also on the board of Open Network Users Group (ONUG). Network World Editor in Chief John Dix asked Elmore to participate in an email-based Q&A to explore the promise of Software Defined WANS.*

The members of the Open Network User Group that you are a member of have voted the WAN as the top use case for SDN twice in a row now. Why do you think that is? Consider this quote from a Wall Street firm at the recent Open Networking User Group meeting in New York: "Although much of Wall Street has focused on the 'sexy' datacenter aspect of SDN, interest in software-defined WAN has increased meaningfully and we believe SD-WAN could experience more rapid adoption than datacenter overlay technologies. SD-WAN can dramati-

cally reduce the cost of WAN deployments by enabling cheaper bit rates in both CAPEX and OPEX (i.e., less cost for the same bandwidth or more bandwidth for the same cost as compared to MPLS) and less overprovisioning for the same SLAs."

What's more, the WAN tends to be more discreet in terms of organizational teams and the technology stack itself, meaning organizations can move faster to embrace SD-WANs. So, if you're interested in building a WAN that is better, faster and cheaper, there are some key issues to consider.

What WAN issues today would encourage a company to start exploring SD-WAN options? There are many challenges and limitations with the predominant MPLS-based layer 3 VPN service offerings that have become the standard connectivity solution for many Fortune 500 companies over the past 15 years. Although these solutions have served the enterprise well in a time of limited options, the market is opening up and ripe for transformation.

Previous attempts to scale VPN overlays have not found their way to mainstream, due to protocol scalability limitations and the sheer configuration complexity required for a reasonably sized enterprise network. As more and more critical business applications—such as voice, contact center and storage applications— converge to an IP transport, a high-performing and ultra-resilient (self-healing) IP WAN fabric will become essential to the business.

If you're interested in building a WAN that is better, faster and cheaper, there are some key issues to consider.

Michael Elmore

IT Senior Director of the
Enterprise Network Engineering
Infrastructure Group at Cigna

Let's examine the WAN challenges today:

Cost: The access cost component for MPLS services provided by Tier I service providers continues to be a challenge. Global and national providers are at the mercy of their wholesale relationships with the local exchange carriers and tend to pass these costs to the consumer, with a potential mark-up. Additional cost components include everything from the number of routes, multicast support and QoS requirements, all of which further inflate costs.

Scale: It seems the MPLS provider's control plane and forwarding information base (FIB) tables are hitting scale limitations, causing providers to police the number of routes they are willing to accept from a customer. For the enterprise, this means more front-end negotiation, risk of hitting these policed thresholds, and ultimately the risk in dropping routes, as well as the cost the SPs incur (and potentially pass on) with the constant churn of hardware and perpetual maintenance to support the increased demand in Provider Edge (PE) and backbone capacity.

Service quality: WANs today are not application aware, nor do they consider different application performance thresholds. Soft failures/regional brown-outs can have catastrophic impact on real-time applications.

SLAs are only as good as the customers' ability to measure these and hold the providers accountable. Whether it's latency, jitter, packet loss or the absolute number of outages allowed per month, all of this requires significant management overhead. Although sourcing teams and enterprise service owners are focused when negotiating a predetermined financial penalty for a specific SLA breach, often these breaches render more material impact to the business, which cannot be compensated by collecting an SLA credit. How does an enterprise protect its net promoter score for a customer call they may have dropped, due to a regional outage?

Service provider maintenance is sometimes uncoordinated, resulting in unplanned business impact.

Time to detect failures and restore service is often elongated. Both hard down and soft failure detection requires synchronization between the service provider's control plane and the customer's control plane (bifurcation of control planes). Customers can tune the edge timers; however, they remain dependent on the provider's backbone to detect, hold down, withdraw and prorogate the updates. This holds true for dual-carrier MPLS architectures as well, where customers rely on carrier A to withdraw the associated prefix(s) in a hard outage situation, so the disparate topologies can converge and restore the session path. It gets worse with a brown-out or regional outage, where carrier A would never withdraw the prefix(s), yet causes application degradation.
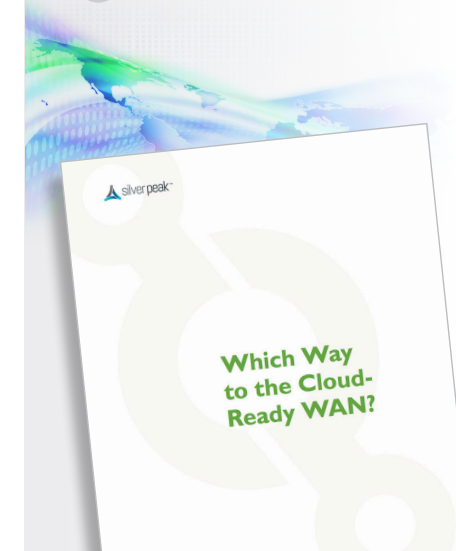
Security: There is no inherent data plane encryption. Some customers elect to implement over-the-top IPsec, which tends to impede the benefits of MPLS by decreasing overall scale, while adding an additional fault domain layer. Additionally, this requires distributed configuration steps for setup and key management.

Visibility: The customer's Layer 3 routing control plane is outsourced to the MPLS service provider, as customers are required to inject their remote site routing table into the SP's network, either statically or dynamically. At this point, the customer loses visibility with very limited access to the provider edge, not to mention the backbone.

Managing multi-homed default route selection in a single VRF requires the customer to provision site-of-origin (SOO) via a route map on the provider edge, with limited means to validate the configuration / implementation. This type of manually steering of traffic can take days, if not weeks to implement. The risk: outbound traffic destined to the closest exit point could suddenly transition to another multi-homed exit point causing latency and application lag.

Most SPs prohibit SNMP access to the premise equipment for proactive alerting and instrumentation, limiting visibility into what is happening in the MPLS "underlay."

Agility/flexibility: Time to provision is typically elongated and unpredictable when compared to the consumer market. How is it possible for consumers to provision 10 to 250Mbps service to their home in a few days or weeks, yet it takes a corporate network administrator typically 60-90 days to get similar bandwidth provisioned? This is the classic and rigid LEC problem,

represented by the wholesale dependency retail service providers have when delivering services to the enterprise customers. The retailers are often dependent on the LECs outside of their own territory. This challenge becomes exacerbated when trying to procure 'diversity' for multiple circuits.

There's no inherent application-based path selection to facilitate routing cloud-based application access via the local internet.

So if those are the WAN challenges today, what is the SDN promise? In short, the SD-WAN can enable customers to take back control from service providers, while creating new market opportunities for those service providers.

If customers could create SD-WANs that separate the underlying transport from a software-based, overlay control plane on controller(s) owned by the customer, it would empower them, among other things, to centrally manage security policies and make application-based routing decisions dynamically and based on application performance criteria—all independent of the underlying transport.

The underlay just becomes a set of common IP circuits with next hop reachability. This opens the door for customers to go direct to the local market (LEC, MSOs, etc.) to procure more cost-effective bandwidth with the right mix of transport technologies and SLAs required for the business, without compromising or fragmenting the logical routing topology.

Consider a company that has business process outsourcing, business-to-business, internal, or other WAN constructs, which increase complexity and cost. What if a network administrator could build an underlying network with various transport providers and glue the transport together with a unified overlay provid-

ing centralized policy management via a controller to create logical segmentation for multi-tenancy? Essentially, this would drive up the efficiency rate, creating a more cost-effective network.

The benefits become exponential when you couple an SD-WAN strategy with converging and centralizing/regionalizing services such as SIP voice, IP Contact Center and other services, which are often distributed and reside on edge CPE today (DSPs, SRST).

Let's dive into how each of the previous problem statements gets addressed with SD-WAN:

Cost: An SD-WAN overlay enables customers to regionalize their transport and go directly to the LEC markets to reduce the double margin effects inherent to the traditional national/global provider model. Ethernet services enable new commercial off-the-shelf CPE options.

Scale: By separating the underlying transport and the control plane with software based overlay/controller(s) owned by the customer, it reduces the dependency and scale limitations with the carriers. Essentially, the carrier becomes "next hop reachability" via IP circuits, with an intelligent overlay managed by the customer to orchestrate the enterprise routing. The scale becomes directly proportional to the SDN controller.

Service quality: WANs today are not application-aware, nor do they consider the application performance thresholds. Soft failures/regional brown-outs can have unpredictable and adverse impact to real-time applications.

Application or performance aware routing is a game-changing feature that enables customers to monitor the performance of the underlay and make real-time dynamic routing decisions by application. This dynamic detection and convergence capability will improve overall service quality by avoiding manual intervention and troubleshooting, while increasing a customer's probability to hit internal SLAs, as well as responding to unplanned carrier maintenance. This type of dynamic performance awareness has the potential to decrease the reliance on hop-by-hop QoS policy management as well.

Security: Many SD-WAN products come standard with data plane encryption and control plane security. Most enterprise security teams have stopped asking for internal WAN encryption due to cost, scale and manageability challenges. SD-WAN is an opportunity to provide a consistent authentication and transport encryption policy regardless of the underlying transport mechanism or service provider.

Central policy management and segmentation now become a reality, and multi-tenancy increases the efficiencies of the underlying transport. "Who are you" and "what do you need access to" are based on user policy.

Visibility: A carrier-agnostic approach with full visibility and unification of the routing table, inclusive of a multi-home default route scenario. Services such as QoS and multicast will be inherent to the customer controlled overlay. Alerting and management will be innate, enabling the underlay performance visibility.

Agility/flexibility: Customers can leverage non-traditional transport for connectivity, such as cable MSOs, broadband and/or business-class internet, LTE and 4G to improve delivery time

frames. Optimized path selection for cloud services, such as web conferencing, Office365, HR (workday) and other cloud-based apps via local internet links. Service chaining and NSFV become a reality through logical steering of traffic for load balancing and firewall services.

How close are we to realizing this nirvana vision?
The technology is very close, both from the traditional equipment suppliers and early stage start-ups. However, vendors are taking different approaches for prioritizing the features they will implement, and in developing their product roadmaps. Many of the approaches will overlay Internet transport in the long run. The timing seems appropriate, especially given the maturation that has taken place with real-time services and codecs moving from narrow band to wide band, driving up the tolerance for Internet performance characteristics.

So, if an organization likes the sounds of SD-WANs, what kinds of questions should they be mulling to see if it is good option for them?
1. How available is Ethernet access as it relates to your remote site foot-print? Many of the non-traditional suppliers will offer SD-WAN services with Ethernet interfaces.
2. Will the solution support TDM interfaces?
3. How will the hardware integrate with the LAN side routing (inline or via industry standard routing protocols)?
4. What is the tooling and instrumentation and strategy? Will the solution integrate with existing toolsets or move to a new operations / instrumentation model?
5. What's the pricing model? Before moving into a POC or pilot, customers should ensure they have a deep understanding for the unit pricing and financial model including subscription, licensing, maintenance and hardware costs. Much like the transition to cloud based SaaS applications; some solutions may drive new internal accounting questions.

Are there remaining concerns or potential speed bumps that enterprise customers should consider?
The SD-WAN approach could also lead to carrier proliferation. How many carriers are too many? One side of the spectrum will suggest the more carriers, the better unit pricing. However, the resources required to manage a certain number of carriers may ultimately be unsustainable, hitting a diminishing marginal utility effect.

There is also the question of open versus closed. Many of these solutions will be shrink wrapped and closed alternatives, so if you desire openness and the desire to integrate multiple suppliers across a single overlay, you may need to wait.

It's clear that the time is now for enterprises to perform a market scan and develop a detailed set of problem statements to address. As a potential SD-WAN consumer here in the early stages of this emerging market, you have an opportunity to help guide development efforts and prioritization with the core suppliers.

It's clear that the time is now for enterprises to perform a market scan and develop a detailed set of problem statements to address.

Why Communications Service Providers Need to Implement SD-WAN

Faced with commoditization of bandwidth services and declining revenue, CSPs should look to SD-WAN to deliver flexible, cost-effective managed services.

BY LEE DOYLE, NETWORK WORLD | Communications Service Providers (CSPs), including carriers, managed service providers and cable providers, are challenged to maintain business services revenue and profit streams in the face of bandwidth commoditization (e.g. high speed, inexpensive Internet services). Software defined wide area network (SD-WAN) solutions could and should enable CSPs to increase the value of their managed services for business customers.

CSPs rake in roughly $40 billion per year (with good profit margins) selling WAN services such as MPLS, frame relay, Ethernet, Internet, T-1 and leased lines to business customers. These companies have been willing to pay a premium for highly reliable, low latency, secure links from their data centers to branch offices and between data centers.

The problem is that increased use of cloud and SaaS applications has significantly altered WAN traffic flows in distributed organizations. Remote users require direct access to SaaS/Cloud-based applications such as Salesforce, Office 365, Lync, WebEx, and off premise storage. Traditional managed network services such as MPLS, which link branches to a centralized data center, can't offer low latency/high performance access to cloud applications.

Seeing an opportunity, a plethora of product suppliers, including Cisco, Riverbed, Viptela, VeloCloud, Silver Peak, Pertino and Talari, have introduced SD-WAN technologies that allow organizations to better leverage Internet circuits to solve WAN traffic challenges. SD-WAN uses software and cloud-based technologies to simplify delivery of WAN services to the branch office, and software-based virtualization enables network abstraction that results in simplification of network operations.

But that approach requires customers to acquire and manage the gear, which leaves the door open for CSPs to march in with a managed alternative, an opportunity they desperately need. After all, CSP revenues for managed business services have peaked and will slowly decline due to the commoditization of bandwidth services and, as mentioned, services like MPLS are threatened by the ability of customers to use SD-WAN technologies to leverage Internet circuits.

Internet circuits (Ethernet, DSL, cable, etc.) typically are one third to one half the cost of comparable speed MPLS links. And Internet services have the advantage of higher speeds (100MB to 1 GB), wide availability and rapid provisioning times as compared

Software defined wide area network (SD-WAN) solutions could and should enable CSPs to increase the value of their managed services for business customers.

to MPLS. The ability of SD-WAN to minimize the disadvantages of the Internet (poor reliability, unpredictable latency, and weak security) is the key threat to traditional managed business services provided by leading CSPs.

CSPs need to adopt SD-WAN technologies to remain competitive in the market for managed services. SD-WAN can help CSPs deliver flexible, cost effective managed services that meet their customers' current and future needs. A key service that CSPs can deliver is hybrid WAN. Hybrid WAN allows current MPLS customers to add managed Internet bandwidth to their branch network. The Internet circuits will handle non-critical traffic flows to the data center and the increasing amount of direct to cloud traffic (i.e. popular SaaS applications).

CSPs can offer customers managed, secure hybrid WAN services—a key benefit for organizations wishing to outsource complex WAN management to a business partner. CSPs market the reliability, security, and traffic handling benefits delivered via SD-WAN technology. A number of leading CSPs are already working with SD-WAN solutions (e.g. Verizon and SingTel) and many more are investigating the technology.

CSPs can drive the adoption of SD-WAN by reducing the risk of introducing new technology, assisting in the migration to hybrid WAN (i.e. a mix of MPLS and Internet circuits), and by providing professional and support services. By leveraging SD-WAN to deliver new, valuable services to their business customers, CSPs can avoid the likely disintermediation to their managed service business via the inevitable increased use of Internet circuit for business traffic.

Fixing Internet VPNs with Software-Defined WAN

SD-WAN promises to fix some of the key limitations of Internet VPNs. Let's look at how this works in practice.

BY CIARAN ROCHE, NETWORK WORLD | Internet VPNs have been a feature of many global enterprise WANs for the last 10 years. In a previous article I mentioned that this technology is often used out of necessity, with cost pressure forcing enterprises to just deal with Internet performance limitations.

With increasing interest in Software Defined WAN (SD-WAN) recently, many use cases have been proposed by vendors and early enterprise adopters alike. However, it is today's site-to-site Internet VPNs that should be seen as the 'low-hanging fruit' for initial SD-WAN deployments. Moving to a software-defined solution results in a topology that should be very familiar to enterprises with existing VPN deployments, while solving some of the bigger performance and management issues.

Getting organized with profiles and templates

One major limitation of traditional networks is that they are based on individual device configurations, and the concept of life cycle management doesn't really exist. Sophisticated enterprises often use third-party tools to centralize configuration management, implement version control, and use templates, but organi-

cally growing Internet VPNs in the network are often forgotten.

Most SD-WAN solutions address this by establishing a hierarchical, template-driven structure for the network in the orchestrator by default. You start by defining what each site type should look like in advance—single or dual WAN connections, VLAN settings for voice/data, SSID for internal and guest Wi-Fi, etc. Then you establish enterprise-wide settings like QoS schemes, firewall policies and private IP subnet ranges for LANs. Once this is in place, creating new sites or changing existing sites requires a minimal amount of site-specific effort. This is what is making SD-WAN intriguing for retailers; 1,000 very similar stores can be defined once and then kept perfectly in sync as business policies change.

Is this completely new? Definitely not; automation tools have been available for years on traditional networks. Packaging it up into a turnkey solution is a helpful approach, though—especially when combined with some performance-improvement features.

Addressing link quality issues

VPNs are great when they work. The problems start when sites are in regions with poor-quality connectivity, and they are compounded

Moving to a software-defined solution results in a topology that should be very familiar to enterprises with existing VPN deployments, while solving some of the bigger performance and management issues.

when the enterprise wants to deliver high-quality voice, video, and other business-critical traffic to the site using this infrastructure.

One of the most compelling features of some SD-WAN solutions is the ability to separate the underlying infrastructure from the overlay network. This allows multiple types of connectivity to be plugged in—maybe a business-grade ADSL2+ circuit to start with, as well as a cable modem link and perhaps a 4G/LTE service also—but operate the network without worrying about which packets are being routed over each link.

The software platform is aware of the pool of connectivity. It continuously measures the performance and throughput available over each path, and makes a decision on a per-packet basis, taking QoS settings into account and duplicating critical packets across circuits if needed. It's still the Internet, but now there is a level of active traffic steering and management that can make the solution a viable option for more applications. If a link goes down or is performing too poorly, it just drops out of the available pool until it is restored.

The tools to understand what's going on
Visibility is another area where the packaged approach of SD-WAN solutions can be appealing to enterprises. There are certainly ways to get detailed visibility of application-level traffic flows in Internet VPNs, but they usually require third-party software, server infrastructure, and all the usual patch management and maintenance to keep them functional. Almost all SD-WAN offerings include built-in visibility of usage levels and performance on the network, and several combine this with an application database that includes hundreds or even thousands of traffic signatures. This can be a valuable troubleshooting and capacity management tool for an over-stretched IT team.

The next VPN
Looking at the SD-WAN feature set as a whole, it's easy to see why enterprises are already finding it compelling as a VPN replacement. Some of the 'challenger' vendors in this space have priced their solutions at a point that is comparable to the maintenance of traditional VPN routers, which can help with the business case. If you have some problem sites on VPN in a traditional network today, it could be worth evaluating SD-WAN as a potential solution to some of these issues—and then see if the technology also makes sense at other sites.

Silver Peak's SD WAN Solution Boosts Application Performance

Silver Peak is bringing its WAN acceleration expertise to the SD WAN market with a product said to deliver private line–like performance and security over regular broadband connections.

BY LINDA MUSTHALER, NETWORK WORLD | In recent weeks I've written about several vendors in the software defined wide area networking (SD WAN) space. There's one thing I've learned as I've talked with these companies: each one takes an approach to wide area networking that plays to the company's strengths. Silver Peak just had a major announcement pertaining to SD WAN, and not surprisingly, this company is building on its deep expertise in WAN acceleration.

In mid June 2015, Silver Peak announced its Unity EdgeConnect product set. This SD WAN solution brings broadband Internet into the WAN in a way that delivers private line-like performance and security. I'll get into the "how" of the solution in a moment, but first I want to discuss the "why" of software defined wide area networking.

Today, multi-protocol label switching (MPLS) is pretty much the standard way for enterprises to connect their branch offices back into the corporate data center. MPLS has been a good solution for at least the past decade. As a technology, it's predictable, reliable, and relatively secure. It allows enterprises to connect their remote users to applications in the data center in a private, secure way.

However, MPLS has its drawbacks. It's expensive and inflexible, and it can take months to bring up a new branch. Companies have limited control over their MPLS implementations because they have to be outsourced to a carrier or service provider.

But the biggest drawback to MPLS is that it's out of sync with the way that companies deploy enterprise applications today. According to Gartner, 80 percent of enterprise traffic today is destined for the Internet. In order for a branch office to reach applications in the cloud, the traffic has to go from the branch over the MPLS line to the data center to an exit point out to the Internet and then to the application, and then back again. It's inefficient but this is the way to do it if MPLS is the branch's primary point of access. Unfortunately it means that cloud-based applications are going to suffer from poor performance.

Unique solution

SD WAN solutions address this shortcoming in traditional WAN architectures. By putting an overlay on top of the WAN, companies can deploy broadband links on the network to augment or even replace the MPLS links.

SD WAN solutions address the short-comings of MPLS in traditional WAN architectures. By putting an overlay on top of the WAN, companies can deploy broadband links on the network to augment or even replace the MPLS links.

This is what Silver Peak does, but the vendor brings its WAN acceleration expertise into the mix for a unique solution that emphasizes high performance for cloud applications. Silver Peak's SD WAN solution consists of three elements:

- **Unity EdgeConnect** is a zero-touch virtual or physical appliance for branch locations. It can be deployed in minutes to create a virtual network overlay that leverages both MPLS and broadband connectivity.

- **Unity Orchestrator** provides visibility into both legacy and cloud applications, and the ability to centrally assign business intent policies. Using templates, Orchestrator can assign policies with limited or no manual intervention.

- **Unity Boost** is an optional performance pack that is an on-demand subscription. It's for applications where acceleration is really needed; for example, data replication at the end of the work day. This is a real differentiator of the Silver Peak solution.

The Unity architecture is the fabric that brings all the elements of the WAN together. Customers can take baby steps to get into SD WAN or jump into it full force. There's no need to change traditional routers, switches or connectivity; Unity can ride over all of those but in addition it's possible to bring in broadband using cable, DSL, LTE, or whatever the preference is.

I mentioned the Unity ConnectEdge appliance is zero-touch. An administrator can create templates for policies the organization wants to put in place, such as the acceptable latency rate for traffic. A company can define a couple of templates and match them to its applications. Then the Orchestrator automatically pushes out these policies to the branches based on what applications are in use.

Blazing new paths

Dynamic path steering over SD WAN is a common feature for all solutions. Typically, if one path to/from a branch goes down, another one takes over so there is no loss of traffic. Silver Peak kicks this feature up a notch and calls it dynamic path control. It's not just based on downtime of a path, but also on quality of service (QoS) and better performance on one path over the other. This is where Silver Peak's years of experience in driving the WAN based on optimized performance comes into play.

Silver Peak also uses path conditioning on broadband, similar to that which MPLS uses. The vendor is able to condition the network tunnels to make sure they provide the best possible performance. The company claims to have a "secret sauce" to keep track of packets to give private line-like performance over the Internet lines. A cloud intelligence service that is part of Unity EdgeConnect assures that Silver Peak knows the best, most optimized route on the WAN to take.

Silver Peak also claims to provide better security over broadband through WAN hardening than MPLS provides with its private line connection. It starts at the point of IPSec tunneling. Silver Peak uses a 256 AES encrypted tunnel so that every packet on the WAN is completely encrypted. Traffic can only be read at the other end of the WAN by another Silver Peak device. No unauthorized traffic is allowed to enter; the WAN only carries traffic from trusted devices on either end.

The final piece to this solution is the monitoring and reporting that provide more control and understanding of what's happening on the network.

Silver Peak has tossed its hat in the SD WAN ring and it's bringing to bear all the lessons it has learned over years of providing WAN acceleration solutions.
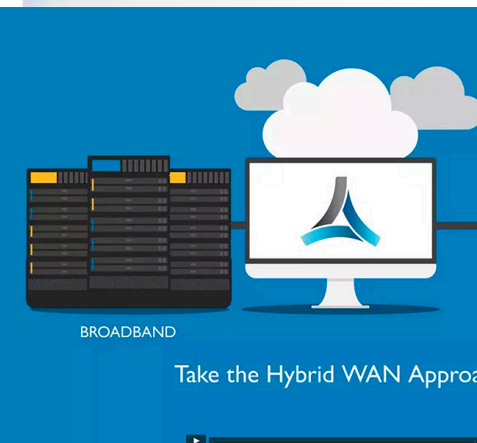
What Does a Next–Generation WAN Look Like?

The WAN is changing faster than ever before, but what will it look like?

BY CIARAN ROCHE, NETWORK WORLD | After years of sitting in the shadow of virtualization, SaaS, containers, and all the other exciting IT trends, the wide area network is finally getting some attention. These other trends are actually drivers for this change in many cases; while WAN architectures have remained relatively static in recent years, the applications they need to support have changed beyond recognition. This is driving the need to re-think what the WAN looks like and how it operates.

The phrase 'next-generation WAN' will mean different things to different enterprises, but let's identify some of the characteristics that are starting to become more common. Some of these are new, but in many cases the next-generation WAN is a new network methodology or mindset. This can impact the technologies used, insourcing/outsourcing decisions, and functionality provided by the network.

It will probably include more Internet

Let's start with one of the more controversial aspects of the WAN. Private connectivity between sites is a prerequisite for many global enterprises. This has been true since the concept of a WAN was invented. The concept of a 'closed user group' has always applied to private WAN technologies; it is a natural fit for many traditional applications. Even today, technologies like Microsoft's Active Directory assume a private network exists between sites by default.

Where enterprises have deviated from natively private connectivity, it is usually for cost, coverage, or bandwidth reasons. Site-to-site VPNs are a mature technology, allowing an enterprise to extend its private network to all locations, but there are trad-eoffs. Performance has always been the biggest perceived issue, closely followed by accountability and lack of SLAs. For many enterprises, these weaknesses have resulted in Internet VPNs being used as a last resort.

The application mix in many enterprises is driving the need for a re-think of this approach. In many cases, 70% to 90% of the traffic carried over the private network is destined for the Internet. This isn't all critical SaaS or IaaS traffic going to AWS, Office 365, Salesforce.com or Azure, of course; it also includes the regular Internet browsing traffic for each location.

The natural concern is that the highly engineered private MPLS network has become an expensive conduit to centralized Internet breakout points—the enterprise pays for the private network bandwidth and then pays again for the Internet break-out capacity. In most enterprises, non-Internet traffic is becoming an ever-smaller percentage of the total WAN traffic. This can impact capacity planning, application performance, and user satisfaction. This trend is resulting in enterprises considering a greater adoption of Internet technology, along with the neces-

For many enterprises, weak performance, accountability, and lack of SLAs have resulted in Internet VPNs being used as a last resort.

sary intelligence in the network to deliver traffic to its destination using the most appropriate path.

Abstraction is changing network infrastructure

Deploying an enterprise WAN with a mix of public and private technologies, with prioritized connectivity to on-net and off-net destinations, is somewhat of a nightmare using traditional network architecture techniques. Policy-based routing, split tunneling, access control lists, IP SLA for link performance monitoring, object tracking to detect state changes—these are all features available in traditional networks but combining them to deliver a cohesive solution, and troubleshooting them when something goes wrong is a major challenge.

One of the key technologies that is driving the next-generation WAN is Software Defined WAN (SD-WAN). This can mean many things, and in future posts I'll discuss these in detail, but from a practical perspective one of the key features of SD-WAN is the ability to abstract the virtual, software-controlled network fabric from the underlying network components. This results in network architecture definitions that can be based on creating a path from site A to site B, regardless of whether sites A and B are connected using MPLS, point-to-point Ethernet, 4G mobile, DSL connections from local ISPs, or any combination of these. This is a huge mind-set change for enterprises, and it finally opens up the possibility of treating the underlying bandwidth as a true commodity.

Think network services, not device configurations

In the same way that abstraction is changing site-to-site connectivity, services are replacing traditional complex configurations. Take a piece of functionality that is common to all (or most) sites like a security policy: this could consist of hundreds of lines of configuration deployed on the routers at every location. Changing the policy means editing configuration lines on each device, checking for errors, and then testing.

Next-generation WAN architectures allow network-wide services to be managed at the policy level. The policy is held centrally, with version control and audit capabilities, and automatically pushed to devices. This is a powerful new capability for IT teams, especially when extended to include more complex services like cloud-based web filtering, WAN optimization, and IDS/IPS services.

Putting it all together

The new mindset behind next-generation WANs encompasses many sub-themes, and there is an increasing level of hype in the industry behind some of the promises of the emerging technologies and methodologies. Cutting through this and arriving at a realistic assessment of what options are best suited for each type of enterprise is essential.

Silver Peak CEO: We're Re-imagining the WAN for a Cloud World

CEO and founder David Hughes sees huge opportunities in software-defined WAN.

BY JOHN GALLANT, NETWORK WORLD | *Silver Peak, Inc., made its name as a top provider of wide-area network optimization capabilities. But the company has its sights set on a loftier goal today: Completely changing the way you build your entire WAN. Silver Peak is moving rapidly to support so-called software-defined WANs, which make it easier and cheaper to connect branches and end users to cloud applications.*

David Hughes founded Silver Peak and became CEO in 2013. In this conversation with John Gallant, Chief Content Officer of

IDG US Media, he talks about the customer pressures driving this strategic change. He also discusses how the move distances Silver Peak from competitors like Cisco and Riverbed, and describes new tools from Silver Peak that enable customers to build networks based on real business goals versus arcane tech specs.

How do you define your market and what differentiates you from competitors? Traditionally, we've been seen as a WAN optimization player. That's certainly where we made our name. We've been able to satisfy some of the largest customers in the world. Now, we're looking beyond WAN optimization, looking at how to rethink the way you build a wide-area network. We're hearing from customers that the current way of building a WAN using MPLS, for instance, just isn't satisfactory as they move to the cloud. They want to be able to use the Internet more effectively than they can today. Where we see our future differentiation is around providing very ready access, very easy connectivity to broadband services so people can build a wide-area network much more quickly and efficiently.

Let's talk about those customer pressures. Customers are actively working on their own private and hybrid clouds, there's

growing use of software-as-a-service, as well as infrastructure-as-a-service and platform-as-a-service. What kind of strains does all that put on the typical wide-area network? Where are the pinch points and what do you see as the solution to those problems? If we look back 10 years to the peak of MPLS, it was really designed well for the problem that people had in those days of communication from branch-to-branch and branch-to-data center, where most applications were in the data center. The challenge customers are facing now is that more and more of their applications are migrating from the data center to the cloud, either to be hosted in IaaS or even more likely to be a SaaS service like Salesforce.com or Office 365 or Box. The fundamental traffic flow is no longer branch-to-data center. It's really branch-to-cloud and the MPLS networks are generally built to primarily send everything back to a data center or headquarters or backup data center and then out to the Internet. That really doesn't make sense anymore. People want to find a shortcut to get the user in the branch connected to the app in the cloud. It's this move to the cloud that's making people rethink their wide-area networks.

Talk about the solutions there, David. What WAN architecture should customers be building? The fundamental thing that people need to think about is how to build a virtual WAN, a WAN that's an overlay so they can mix and match services anywhere. They're comfortable from an SLA point of view with MPLS today but they want to add broadband. They want to be able to use Comcast or they want to be able to use LTE services from Verizon or whomever to give them more cost-effective and more agile connectivity in the branch. An overlay lets them mix and match those services in a very easy way. They're no longer tied to a single service provider.

Think about VMware virtualization. The hypervisor provided a way for people to quickly migrate software from a Dell server to an HP server to a Dell server as they went through an upgrade path and they didn't have to reinstall everything or have any downtime because the abstraction layer, the hypervisor, let you mix and match your underlying infrastructure. In the same way going forward, virtual wide-area networks with an overlay will let you mix and match what's underneath. That really gives you agility and the ability to take advantage of lower cost services.

I want people to understand exactly what you mean by a virtual WAN. Talk to me about what that is and how you help them build that? Perhaps as an example to get an idea of how someone starts using a virtual WAN, anywhere you could Skype from you could potentially build a branch. All you need is an IP address on an Ethernet port. From there, a device can automatically register and become part of that customer's network so it's signing into an overlay which runs over the top of any kind of IP network, be it MPLS or a cable-based system or wireless LTE.

What's the role of WAN optimization in this virtual environment? People understand that today as two devices at the ends of a link. There is a name that some people use, SD-WAN or software-defined WAN which embodies some of this. Both SD-WAN and WAN optimization are addressing problems that people have in the wide-area network. The fundamental value proposition of WAN optimization is about performance, performance at a distance, making sure applications work just as well if I'm coming from Singapore or San Francisco. For virtual WANs and SD-WAN, the primary value proposition is about connectivity. I want to easily connect my branch with a minimum of fuss and I want to be

People want to find a shortcut to get the user in the branch connected to the app in the cloud. It's this move to the cloud that's making people rethink their wide–area networks.

able to do that cost effectively and reliably, securely. We obviously have our WAN optimization family and we've recently announced an added product family focused on SD-WAN. We see that both those value propositions apply for a number of customers. The intersection between these two worlds is actually pretty big.

That makes sense. Is that product that you referenced the Unity product? Unity is the umbrella architecture and the new product is called EdgeConnect.

Let's talk first about Unity. Help people understand what it is. Unity is our name for an overlay, our fabric which lets you connect branches, headquarters, IaaS services, SaaS services all together. You don't have to think about it being attached to one carrier. You can use however many carriers you want and it's not just physical locations but physical and virtual locations.

Is this similar to the concept that Cisco was talking about recently with the Intercloud? I'm not sure. There may be some similarities there. I think for Cisco, they have their IWAN [Intelligent WAN], which is their way of taking the legacy routing infrastructure and trying to add things like performance routing to be able to use multiple links cost effectively. But it's not really an overlay technology. It's more a way of tweaking routing to try to solve some of the problems with using multiple links. An overlay is different in that you're not really using all those old protocols like EGP and OSPF. You're using SDN-influenced technology with end-to-end connectivity and single-hop routing. It's really a different way of thinking about things. It's more influenced by the work in the data center around SDN than by the routing protocols of the last two or three decades.

Customers can't put a device at a cloud provider so how do you create that kind of overlay with all those cloud providers? There are really two cases. The first case is when it's an IaaS service like Amazon. In that case, yes, we can be inside running as an AMI (Amazon Machine Image).

Essentially a virtual instantiation of the product? Yes, and we have similar capabilities for Microsoft Azure and VMware vCloud Air. In all those cases you can run Silver Peak software inside your virtual private cloud. The second case is that of the SaaS service where, unless you're a very large customer, if you go to Salesforce or Office 365 and ask them to take your piece of hardware, the most likely answer is going to be no. For that, we take a different approach, which is while you can't be inside that service provider, you can certainly be very close. If you look at the way the network and the cloud are evolving, there are a few interconnect points which are one hop away from a lot of people. To the extent that you can build a network hub that is either at or close to that location, you can be very close to those SaaS providers. We track where all the SaaS providers are providing their services from and we'll route your traffic to the egress point from your network that's closest to that provider, basically getting you to the doorstep of Salesforce or Office 365.

That makes sense. I was reading a piece by Zeus Kerravala in Network World where he was talking about Unity actually having the ability to determine, based on traffic patterns, what is the optimal route. Can you talk a little bit about that? Essentially, we know where all the Office 365 data centers are around the world and we have a service with that information so our customers are able to measure from each gateway the distance

to each of those services. That provides the customer—it's all automated—the information needed to take the best route for that service.

Based on collective intelligence from all your customers? Yes, both the measurements that the individual customers are making as well as collective information that's coming from our Unity intelligence service.

Can you talk to me about a customer and what they've seen from using the Unity product? Sure, we have a number of customers, but one of them is Interrol in Europe. They've used us to augment an MPLS network and build out using the Internet with roughly five times as much bandwidth for the same cost as what they had before. We've got a lot of other customers in the midst of making the same transition. It's a very common path right now to be looking at: How do I take my MPLS network and augment it with Internet connectivity? That's the main driving use case we see with our customers at present.

There's a lot of talk lately about software-defined networks. How does SDN match up with the wide-area network trends that you're talking about? Do these two things synch up? SDN has been a buzz topic in the data center for probably five years now. Some people see it as a solution in search of a problem. There are certainly some niche applications but for a lot of enterprises, there's not a compelling reason to implement SDN today. Maybe soon. The difference that I see in the wide-area network is that we are solving a real problem customers have. They want to be able to leverage multiple networks. They want to get agility. They want the automation that comes with SDN

and that's where this SD-WAN piece comes in. It's one of the first instances of SDN where it's driven by a real problem. You're probably familiar with the Open Network User Group that grew up in New York. They've been pushing the open networking SDN angle for a while. They've recently started to look at SD-WAN. It's been voted two or three sessions in a row now as the top use case because it's applying a lot of the ideas—the overlay ideas, the automation ideas—to a real and present problem.

Is there a role for the carriers in this or do they see it as a threat? They see it as a threat but I think there is a role. For every customer that wants to take the network into their own hands and wrest control back from the carrier, there are other customers that really want to have someone handle their networking soup to nuts. While SD-WAN is sometimes looked at as a way of giving the customer leverage to mix and match carriers, it's also a very good way of building your managed service. We've been engaging with some forward thinking service providers who are looking at how to leverage SD-WAN technology to be able to provide managed services more cost effectively. I think it's definitely a threat but it's absolutely an opportunity for service providers that are willing to think a little bit outside the box.

It would seem that they are the ones who are ideally situated because they're located near all of the cloud providers. Whether you have an office or not they have something close to the cloud provider. Yes.

And they can be that point of egress that you talked about. Yes, they certainly have multiple points of presence so they can provide a regional hub service, for instance. There was an an-

nouncement we had with Equinix about a year ago where they provide Performance Hub service because they've got all of those locations. They are a real estate-driven service provider but even for the traditional service providers there are opportunities for them to do some really creative things.

How does this change the competitive dynamic for Silver Peak? There are a lot of companies in your space. There's Cisco, Riverbed, Dell. I'm sure I'm forgetting a few other folks that you compete with. Where do they stand on this transition? As we move beyond WAN optimization, we face a different set of competitors. Some of those competitors that are in the WAN optimization space like Riverbed don't appear to be making a transition into this new world of SD-WAN and virtual WAN overlays. From a competitive point of view, there's always Cisco. Cisco has pretty much a stranglehold on branch infrastructure in enterprises and, of course, they also hear what customers are asking for in terms of the problems they're facing. But they have continued to sell branch routers and to continue things along the [current] lines. When you look at the landscape, it's us and some brand new companies that I think provide the innovation in this space and really provide the true overlay technology to build a virtual WAN.

How many months or years lead do you think you have on this versus competitors? I think that's the hard way to measure things. How are we uniquely positioned? For 10 years we've been building overlay networks. A little known secret is that we've always been an overlay. Right from version 1.0 of our WAN optimization software we used tunnels to build an overlay between all of our devices, where almost all the other vendors were [using] PCP proxies. They were proxies at heart. We used to get beaten

up because we were using these tunnels and building an overlay. What's really interesting is that as the requirements have changed, as people have come to understand that the currency of SD-anything is building this virtualization layer, our heritage is really becoming a strength. That puts us in a unique position. Having 2,000 customers where we've deployed our software and hardware appliances running some of the biggest wide-area networks in the world, means we're bringing to bear mature software and experience with WANs that puts us at an advantage with respect to someone coming out with version 1.0 of their solution. Even if they've got some great ideas, it's going to take some time to mature.

What percentage of your products are delivered as hardware versus software? More than half of our business is pure software, people buying virtual appliances either by subscription or on a perpetual basis. Less than half now is the same software delivered on hardware that we supply. We've seen that transition happen pretty swiftly. I think it's probably about four or five years ago, we shipped everything as hardware and in those years the business has moved really dramatically. It's pretty exciting to see that and certainly as we moved into that software world we learned a lot about the way the world has changed and where the world is going. It's much more about agility and automation than about some of the things that traditional networking people worry about.

Do you envision a point in the future where it's 100% software based? Possibly, but I think there are always customers that are looking for a complete turnkey, off-the-shelf solution and so we don't want to force the customers down a path they don't want

to go. Better to let the customers choose. There is definitely a minority going with hardware but I'm not sure it ever gets to 100% software.

What about the mix between this new software-defined WAN focus versus traditional optimization capabilities? Where does that stand today? I don't so much think of them as opposed to each other.

I didn't mean to imply that you were but just in terms of what's driving the business. I think that for WAN optimization it's about performance and the performance over distance, as I said before. For SD-WAN it's about connectivity. Those are two different problems. The WAN optimization market is mature and people have a sense of the size of it, more than $1 billion. SD-WAN is an emerging opportunity. It disrupts the branch infrastructure market and the MPLS services market. Both of those markets are worth multiple billions of dollars so we expect SD-WAN or virtual WANs to be a multiple billion dollar market. Over the long run we expect that business will be bigger than WAN optimization.

Would you ever offer SD-WAN as a service? Ever is a strong word, but at Silver Peak we're really focused on being a software company, a leading software company. It's not in our plans to become a service provider. We are working with service providers, letting them use our technology to provide services.

You took over as CEO in 2013. How did you change the path of the company? I stepped up as CEO because I was very excited about the future. I saw that with the SDN movement coupled with what was happening with cloud, coupled with what we

had seen in terms of the adoption of software, there was a big opportunity for us to move beyond WAN optimization. The key objectives I shared with the company were twofold: We wanted to continue to execute in WAN optimization to be able to deliver to our customers scalable acceleration; but at the same time invest into what we saw coming beyond WAN optimization, which is culminating in what we're doing with Unity and Edge Connect.

Where do you go from here? What will we see in 2015 and beyond? With the launch of our EdgeConnect portfolio, we move from a one-product-family company to having two product families, one for WAN optimization opportunities and problems and the other for this emerging branch connectivity SD-WAN opportunity. You'll see us continue to build and innovate in both areas but particularly on the SD-WAN side. This is a very new industry, a new opportunity and so there's a lot of room for innovation. While we're extremely proud of what we have right now and we think we're leading the industry, there's a lot more that can be done to drive automation, to drive flexibility, to make these networks easier to scale, more rapid to deploy and that's the path forward.

Talk about the EdgeConnect announcement. Unity, as I said, is the overlay. The announcement was about EdgeConnect, which is a very specific product family. It's all about being able to take a box or a piece of software, plug it in a branch and be up and running as a full branch within minutes instead of months. It's about being able to use whatever service is available in that location, whether it's plugging in a 4G LTE stick to get going while you're waiting for MPLS to arrive or plugging into a consumer broadband cable circuit. You can be up and running

While we're extremely proud of what we have right now and we think we're leading the industry, there's a lot more that can be done to drive auto–mation, to drive flexibility, to make these networks easier to scale, more rapid to deploy and that's the path forward.

straightaway. Part of it is about that zero-touch provisioning, really easy to get up and running.

The other aspect is about being able to provision with business intent policies. For most of the history of networking, network management and automation has been looking at devices at an element level and how do I configure all of these elements. But the customers' problems aren't really about elements. They're really about services at a network level. A WAN fundamentally is about connecting users to apps. If you can let a customer describe their problem in that way, then you can actually reduce building a network to filling out just a single set of forms on one screen. So, I want to build a voiceover layer, I want it to have mesh connectivity, I want it to meet these quality of service goals, etc. Once you've said that, now every time you add a branch we automatically provision it. There's no need to go back and do any extra work as you add incremental branches. That ability to specify things with a business intent policy at a level way above the individual elements, I think, is something which will provide savings not just from a bandwidth point of view. When you say savings, sometimes people jump to the bandwidth savings or Internet versus MPLS. There are really three kinds of savings: there's bandwidth; there's OpEx, because you can make this network much easier to run; and then—looking a bit farther forward—there's CapEx savings, because as you implement a virtual WAN like EdgeConnect, you ultimately can implement a thin branch architecture. You don't need routers and firewalls in all of these branches. You end up with a much lower CapEx cost for building your wide-area network.

How do you handle security in this new WAN? We're partnering with a number of security vendors because there are many as-

pects to security which go beyond what we're talking about. The fundamental thing that we do with EdgeConnect is enable you to deploy directly onto the wide-area network without a router or a firewall in front of you. If you think about the traditional WAN optimization deployment, it was always behind a firewall or router and you're trying to be transparent and fit into the existing network architecture. With EdgeConnect and with a virtual WAN you can plug straight into the Internet and in order to do that we need to be hardened against attacks coming in and we need to encrypt everything. The overlay is encrypted with 256-bit encryption edge-to-edge and that provides the secure fabric regardless of whether you're running over the Internet or MPLS. You've got an infrastructure that is very secure.

What about management tools? In terms of components in the solution, there's the EdgeConnect devices which go in the branch and there's the Unity Orchestrator. The orchestrator or controller is a thing that manages the network. It's the place where you apply policies and where you get a little reporting—reporting on applications, reporting on the destination, not just saying it's HTTP traffic but is it traffic for Facebook or is it to Salesforce or is it to someplace in the middle of China where we don't think we've got any business going? That kind of visibility you get with our orchestration. As far as integrating with third-party devices, as well as networking-based things like SNMP, which is standard, we have a full set of REST APIs that are there for automation, both for controlling our devices and applying policy as well as for extracting information like all of the statistics that we collect.

David, what else should we know? We're very excited at Silver Peak about the change that's happening in the industry and being able

to partner with customers as they look to move beyond MPLS and build these new virtual WANs. We think that there's a lot of value that can be provided with flexible solutions, being able to use whatever network you want, to do it securely, getting control and visibility, being able to get performance. You don't sacrifice performance using the Internet. Of course, there are the three aspects of savings that we talked about. We're very excited about what's happening.

So you want people to know Silver Peak not as a WAN optimization company but as an SD-WAN company? Yes, or even more broadly as a WAN company. Helping people with their WAN challenges is where I see us going forward. It's about how we build the best possible WAN with our customers.

Download

blog

Dear MPLS, We Need to Break Up

In this blog, System Engineering Manager at Silver Peak, Adam Fuoss, discusses why it is time to ditch your old network and discover SD WAN.

read it now