Q3 2015

WAN Key Trends

By John E. Burke,
CIO and Principal Research Analyst, Nemertes Research

Executive Summary

The rapid spread of enterprises to many, smaller branches, coupled with the rise in good, cheap broadband Internet and the use of cloud resources, is driving enterprises to shift to a new 3-tier WAN that replaces much MPLS connectivity with commodity broadband Internet. This in turn is driving the rise of many solutions that reshape how enterprises provision and manage WANs: Software-Defined WAN (SDWAN) and Virtual WAN (vWAN) technologies focused on providing a centralized, virtualized set of WAN connections over an infrastructure that freely substitutes Internet for private WAN connections; Network as a Service solutions that make WAN connectivity just another cloud-provisioned solution consumed as needed; and WAN-to-Cloud eXchanges (WAN-CXes), that plumb direct links from an enterprise WAN edge to a public cloud service provider network, bypassing the public Internet. In combination, these changes and solutions provide the enterprise with a way to reshape their WANs in ways that make them more agile, more flexible, and better able to meet the current and future needs of the business at lower cost and with greater resilience.

The Legacy Enterprise WAN

Originally, an enterprise WAN generally consisted of enterprise locations (HQ, branches, data centers, etc.) connected to each other with dedicated TDM links. Links traversed either owned (e.g. fiber stretching between locations in the same metro area) or leased (T1s, T3s, etc) infrastructure. Internet connectivity was concentrated in the data centers, and Internet access for users elsewhere was all backhauled across the WAN. WAN bandwidth was expensive, and making optimal use of it gave birth to optimization technologies.

In the last few decades, that model gave way gradually to the now-dominant 3-tier architecture. (Please see Figure 1).

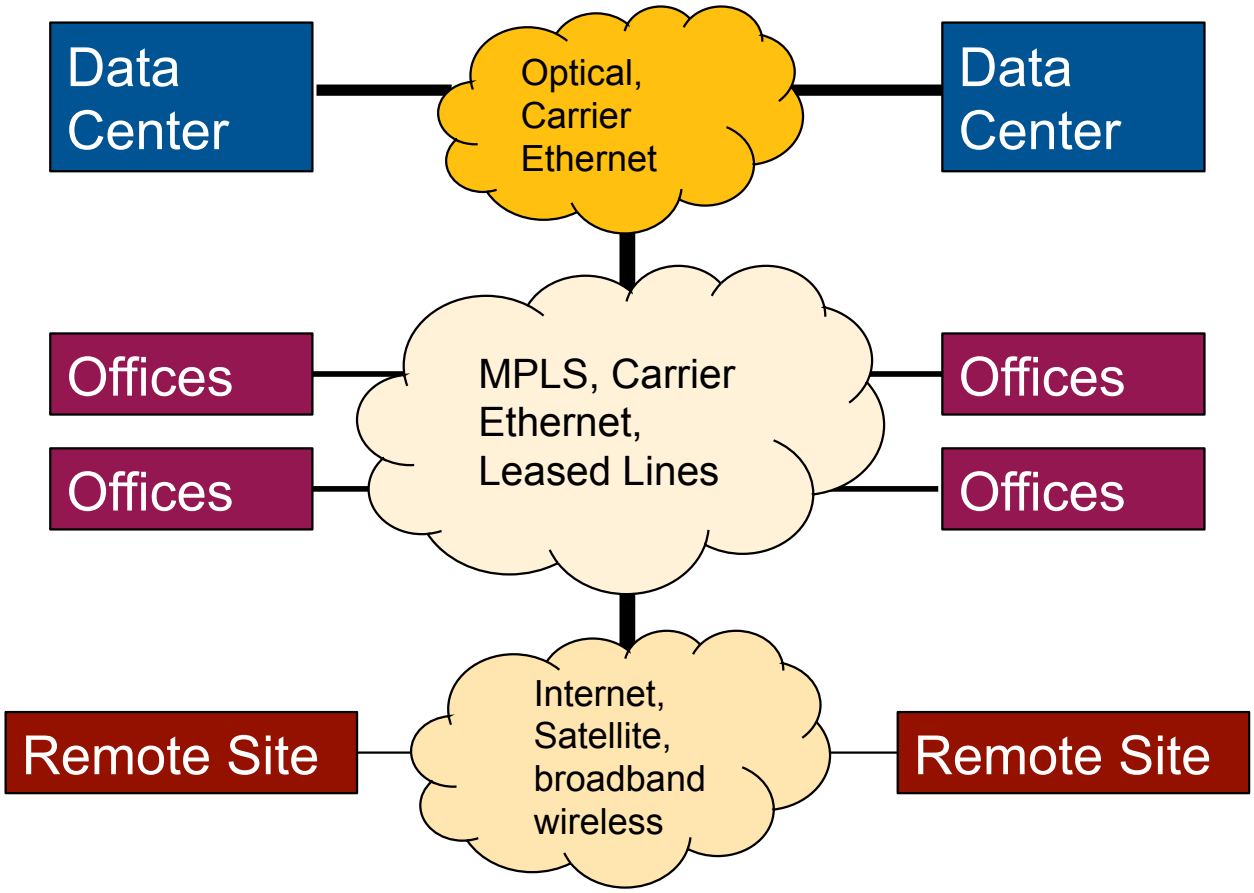

Figure 1: The Current Dominant 3-Tier WAN Model

- Ethernet links or fiber among close-clustered data centers
- MPLS WANs (either at layer 3 as IP-VPNs or at layer 2 as Virtual Private LAN Services) connecting the majority of branches to the enterprise, sometimes supplemented by non-MPLS carrier Ethernet links and largely supplanting older TDM leased lines
- Internet-based IP VPN, or satellite links, where MPLS was impossible or impractical economically.

Breaking the Old Model

The WAN is key to service delivery for many new initiatives. From location-aware discounting for shoppers in a big-box retailer, to collaboration tools unifying account teams across branch offices to virtualized, distributed contact centers, new business initiatives that center on getting closer to clients and customers, both digitally and physically, make branch strategy a key piece of the overall business plan. Agile businesses require agile branching.

For IT, supporting branches is about more than basic connectivity—bandwidth is not enough, and IT can't solve branch challenges just by throwing bigger WAN pipes at them.

As applications evolve to consume more bandwidth, in larger chunks, and with less tolerance for packet losses and variable latencies, the network must get smarter about managing traffic to meet the needs of specific applications and to fulfill the expectations of their users. At the same time, it has to assist in the overall management and mitigation of risk by providing robust security, e.g. by allowing fine-grain segmentation of traffic streams. And, of course, it has to do all this in a resilient, supportable, sustainable, and affordable way.

Expanding the traditional MPLS WAN to more locations or by ramping up bandwidth can be prohibitively costly, and 90- to 120-day wait times (more than a quarter of a year!) to connect up new branches are increasingly unworkable for the business.

In order to be a platform on which businesses can innovate quickly and easily, supporting just-in-time branching and low-risk, high-performing connectivity for any and all services, the WAN has to be smart, simple, and secure. Agile branching requires a smarter WAN.

The New WAN Requires Simplicity, Intelligence

Organizations continue to increase their number of physical locations, often by breaking up large ones into multiple smaller ones. At the same time, they continue to expand service portfolios both through offering new services out of their own data centers and by utilizing SaaS and other cloud services. Greater reliance on IT services, and especially on network-sensitive applications such as VDI, Unified Communications (UC), and real-time collaboration tools, drives the increasingly common need not just for rock-solid reliability and high throughput, but also for application intelligence in the network. The intelligent network preserves and improves the performance for business-critical applications. More than 58% of organizations use VDI, for example; more than 74% have a UC initiative; 57% use social collaboration tools. Such real-time tools are extremely sensitive to packet loss, latency, and jitter, and staff have high (and rising) expectations for good user experiences with them. So, the network must optimize and prioritize traffic to ensure its behavior reflects organizational needs, priorities, and policies in how it allocates bandwidth. Already, 56% of organizations deploy some application delivery optimization (ADO) tools, to deal with everything from bandwidth growth to streaming video. Adding optimization to the branch stack increases the cost and effort involved in spinning up a new branch.

Employees in branch offices also increasingly utilize multiple mobile devices and connect them via the branch WLAN to internal and external services. This puts increased stress on the WAN connection. IT needs a branch network that knows how to optimize performance for users on both computers and mobile devices, using either internally or externally sourced services.

More branches, more services, more devices, but not more IT staff overall—and ever fewer in the branches! So, the WAN must be easily, centrally managed: ideally, it will comprise a single network platform offering multiple services rather than a deep stack of layered devices; single-pane-of-glass monitoring rather than a collection of monitoring tools

looking at different layers of function; and deeply automated management that makes on-site, hands-on attention from IT staff unnecessary for installation or maintenance.

Policy takes two roles in the smart network, guiding both security and performance management. In the evolving hybrid service delivery environment, policies will need to be able to define performance requirements and limitations for a service, from application(s) to users, end to end. For either security or performance, policies ideally will allow the network to decide what to pass through and how to optimize it based on:

- User and application identity
- Sensitivity and compliance requirements of the data being transmitted
- User location and service source
- Time of day and even current phase of any defined business cycles (e.g. in quarter-end reporting period)
- User platform and connection method.

Thus, a truly intelligent WAN might prioritize traffic to all systems of record, internal or external, above most other traffic when the user is a company auditor and the time is within the last week of the fourth quarter. Or, it might block attempts to access the CRM, which contains sensitive data, via an unsecured mobile device, no matter whose it is.

Everyone Wants To Spend Less: The Internet-Enabled Branch

Budgets are flat or down for most IT departments; 60% of WAN budgets are flat or down. Everyone wants IT to spend less on day-to-day operations, to make more money available for the new and the strategic. The keys to reducing costs in the branch come down to reducing the capital cost of deploying networks in a branch, and the operating costs of turning branches up, running them, and decommissioning them. Cost reduction is the main driver of the rapid rise of the Internet-enabled branch.

Internet-enabled branches come in two flavors—branches with direct Internet access supplementing dedicated WAN links, and branches with Internet links only—with variations on each. (Please see Figure 2.)

Direct-to-Internet branches represent an adaptation to a world in which an increasing portion of the service portfolio—25% on average—is supplied via SaaS, and in which staff in every location will regularly utilize partner, customer, and supplier Web systems.

Offloading some or all such traffic to lower-cost branch Internet access reduces or avoids loads on high-cost WAN links (and thereby reduces WAN performance challenges, as well), reduces loads on firewalls and other security systems in the data center, frees up data center Internet bandwidth, and can even reduce overall vulnerability to distributed denial-of-service attacks against the data centers (and other incidents) by making it possible for more people to get more done without using data center services.

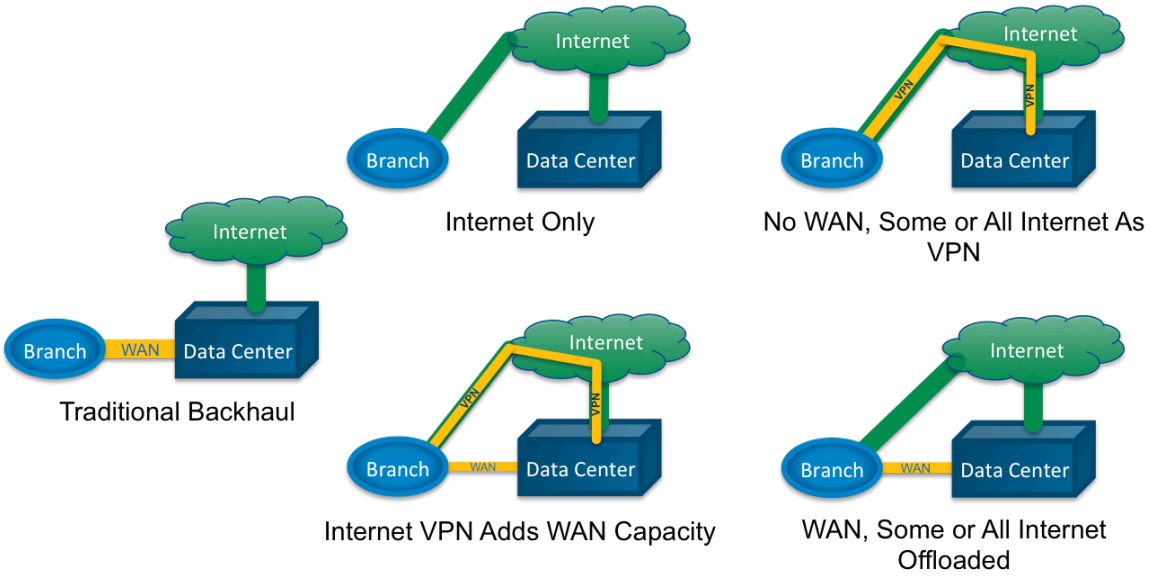

Figure 2: From Traditional WAN and Backhaul to Internet-Enabled Branches

Internet-only branches take the approach one step further, using the same cheaper bandwidth for all branch communications. Connections come in three flavors: VPN-only, split pipe, and Internet only. VPN-only connections use the whole Internet link as an encrypted pipe back to a company data center. Internet-only connections look to the data center like any other Internet site, and staff approach all systems just as they would if they were not on a company network: through public interfaces or via a device-specific VPN rather than a full-site VPN. Split-pipe installations devote some bandwidth to a site-to-site VPN and the rest to direct Internet access.

The Emerging Enterprise WAN

This set of pressures and shifts in the services landscape is driving the rise of a new WAN architecture, one reshaped by Internet VPN replacing much of the MPLS network. (Please see Figure 3.) This shift is powered first and foremost by the continued spread of high-speed, high-quality, low-cost broadband Internet. Already, technologically aggressive companies have replaced WAN with Internet for more than a third of their locations.

However, it's about more than running up traditional IPSEC VPNs over the Internet. Trends including Software Defined Networking (SDN) and Network Functions Virtualization (NFV) are shaking up the WAN just as they are the data center network.

Interest in SDN is driven by two desires: the desire to exert end-to-end control of network behavior from a central control point via changes in policies rather than node-by-node reconfiguration, and the desire to reduce the cost and complexity of the network.

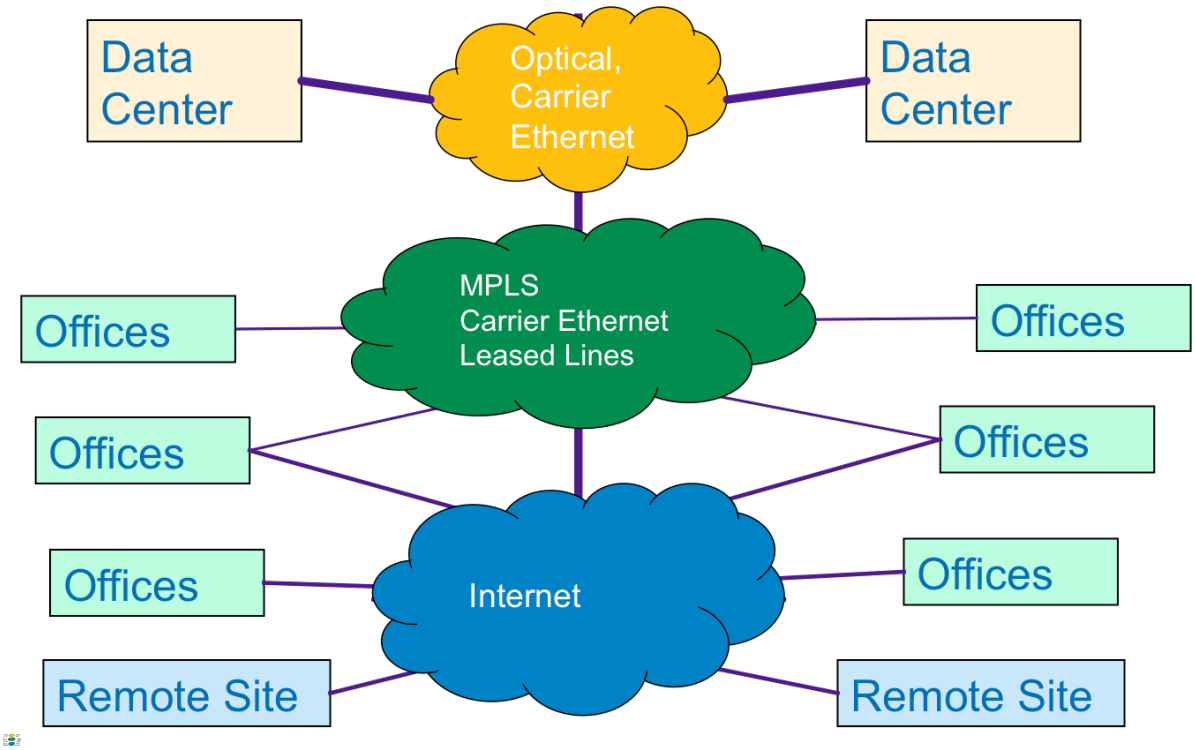

Figure 3: The New 3-Tier WAN

By separating the control plane of the network (where decisions are made about how to handle traffic) from the data plane (which implements those decisions), SDN in theory makes it possible for network applications to implement both performance and security policies on any network port, physical or virtual, data center or branch. Moreover, SDN promises to do so in a very dynamic way, eliminating the latency between policy changes and policy implementation. SDN also allows easy overlay of virtual networks on physical ones, in the same way server virtualization let multiple virtual servers share a single physical host.

Interest in NFV is similarly driven by desire to reduce costs, this time by replacing specialized hardware with virtual machines running on commodity hardware. Nearly all organizations already do this to some extent in their use of virtual switches inside VMware, HyperV, KVM, or Xen environments. The approach is spreading to the WAN in the form of virtualized WAN appliances to replace "the stack" in each closet, driving down the capital expense of a new branch, as well as easing upgrades and additions to that stack operationally.

And, of course, the shift to service-consumption (the "as a Service" model) is having profound impact not just in terms of rising demand for Internet bandwidth but also for how a WAN can be provisioned.

Combining SDN/NFV, inexpensive and easy to deploy broadband Internet, and the rise of cloud services, we see three major trends shaping the next generation of WAN: Software Defined WAN (SDWAN), Network as a Service (NaaS), and WAN Cloud Exchanges (WAN-CXes).

SDWAN

Software Defined WANs seek to bring the world of SDN to the edge of the network with the same goals as SDN generally: decreased capital expense, by shrinking the "branch stack" and shifting to generic hardware; decreased operating expense, through simpler management and promoting use of broadband Internet connectivity; and increased agility and flexibility. SDWAN also aims to make the WAN more service-centric, with both monitoring and management of traffic focusing on delivery of applications.

Virtual WAN (vWAN) technologies constitute a key subset of SDWAN, indeed were the first aspect of SDWAN to emerge, before SDN was even a common concept. A somewhat older and more limited idea than SDWAN, vWAN focuses on on-premises solutions that aggregate branch connectivity transparently, so users and applications get the equivalent of a single large link from the aggregation of several smaller ones. This has become ever more attractive as consumer broadband has improved, and 4G LTE and Carrier Ethernet have become common. Aggregation allows an organization to supplement or replace high-cost-per-bit MPLS links with broadband, Carrier Ethernet, and other diverse link options.

SDWAN solutions can expand on the vWAN idea of making a single WAN out of disparate connectivity in several ways. They expand on the idea of virtualization, typically allowing many separate, segregated WANs to be defined and overlaid on the available connectivity. The WAN overlays may provide network services to a specific application or set of applications, or set of locations, or set of users.

SDWAN solutions may secure vWAN traffic not only by encrypting transmission across shared networks, but also by providing layers of additional security functionality such as firewalling, or creation of “service chains” that selectively direct traffic for specific locations, applications, or users through security appliances.

They may also support a control plane/data plane separation and use of OpenFlow, VXLAN, NVGRE, or other SDN protocols to control the hardware. They also may expose APIs for other tools to use in managing them and thus support a seamless integration of the WAN into an end-to-end policy-driven management framework. SDWANs may involve both physical and virtual appliances, and in high-scale environments may entail an NFV deployment, as well.

SDWANs can optimize traffic in many ways: they can load balance across their aggregated communications channels, and can selectively route flows or packets based on link performance at the moment. They can also do traditional traffic shaping via differentiated handling of flows for specific services, destinations, or users.

Key emerging SDWAN vendors are CloudGenix, Elfiq Networks, Mushroom Networks, Saisei , Talari, VeloCloud, and Viptela. UC platform vendor Sonus has entered the space, as have traditional WAN and optimization vendors including Allot, Cisco, Ipanema, Riverbed, and Silver Peak.

Network as a Service

NaaS vendors deliver WAN services virtually over the Internet on a pay-per-use or subscription basis. The client enterprise sets up connectivity to a provider's point of presence, either as an encrypted tunnel over the Internet or via direct link (typically metro Ethernet); the provider uses their own backbone to transport client traffic among sites or to the Internet. The provider layers on Application Delivery Optimization (ADO) and security services, either solely in their own infrastructure or via a combination of that infrastructure plus a customer-premises appliance (physical or virtual). NaaS solutions aim both to displace traditional MPLS connectivity and to make branch networking more nimble by making it possible to turn up a new branch site's connectivity very quickly and easily.

Emerging NaaS providers include Aryaka, BatBlue, and Velocloud. More traditional Virtual Network Operators (VNOs) and Content Distribution Networks (CDNs) are also entering the space, including Akamai, Masergy, and NTT's Virtela. CloudFlare is a fascinating adjacent service provider, not exactly NaaS for branch connectivity but certainly NaaS-like for enterprise application access.

WAN- Cloud Exchange (WAN-CX)

WAN-CX solutions provide for the easy interconnection of the enterprise WAN (however provisioned) to a Cloud Service Provider (CSP) network, in order to provide access to a public cloud solution that bypasses the Internet. The goals of WAN-CX services are to provide more secure connections to and more consistent performance from public cloud solutions, reducing both business and operational risk. WAN-CX providers can be traditional carriers or NaaS providers, who make the connection directly; or connectivity exchanges operating inside carrier hotels and big colocation/hosting facilities, that serve as a third-party junction point between the WAN and the CSP.

The rise of WAN-CX is somewhat at odds with the Internet-only branch model, but the two are not mutually exclusive. WAN-CX can combine with NaaS, for example, when the NaaS provider's network touches the CSPs. WAN-CX can also combine with split-route branches; when a CSP is connected to the WAN, some or all traffic for that CSP can be rerouted off the public Internet to flow through the WAN instead. And, of course, if much of the traffic is inter-application rather than user facing, the WAN-CX might serve only data centers.

Key WAN-CX providers are AT&T, Equinix, Level 3, TelX, and Verizon. NaaS providers including Aryaka and VeloCloud, although they do not directly interconnect with CSP networks, often have points of presence in the same colocation facilities, and so their customers' traffic flows have only intra-DC hops to reach the CSP.

Conclusions and Recommendations

Changed business expectations and needs drive the shift to the new 3-tier model for the WAN and the gradual retreat from MPLS. The rise of the new WAN both drives and is driven by the emergence of SDWAN solutions, and NaaS and WAN-CX services. In combination, these changes and solutions provide the enterprise with a way to reshape their WANs in ways that make them more agile, more flexible, and better able to meet the current and future needs of the business at lower cost and with greater resilience.

Any enterprise that has a WAN and that struggles with managing it, upgrading it, expanding it, or speeding it up should be actively evaluating these alternative approaches to provisioning and managing their WANs. They should be looking for solutions that give them the right balance of control and agility, simplicity and scalability, flexibility and affordability. First and foremost, they should be looking for a WAN that suits the businesses they are and want to become, not one that looks familiar or that "was good enough for the last 10 years and should be good enough now." Good enough is not good enough any more.