How WAN Design Needs to Change

Ashton, Metzler
& Associates

Leverage Technology & Talent
for Success

Introduction

While some organizations continue to make use of WAN services such as Frame Relay and ATM, the use of those services is quickly diminishing. As a result we are rapidly approaching a time when IT organizations will have only two WAN services to choose from: MPLS and the Internet. Given that trend, a key question facing network organizations is how to best design a branch office WAN using just those two services.

The traditional approach to answering that question has been to have T1-based access to a service provider's MPLS network at each branch office and higher speed links, possibly one or more T3 links and/or high speed Internet links, at each data center. In many cases a key characteristic of the traditional branch office WAN design has been to have a variety of hardware-based appliances in each branch office to perform a wide range of functionality including security and optimization. One downside of this approach is that provisioning and configuring these appliances is complex and time consuming. Another common characteristic of the traditional branch office WAN is backhauling Internet traffic to a data center before handing it off to the Internet. One downside of this approach is that since the Internet traffic transits the MPLS link, this adds cost and delay.

The 2015 State of the WAN Report[1] presented the results of a survey in which the survey respondents were asked to indicate the factors that were causing their organization to rethink their approach to WAN design. In descending order of importance, the top 5 factors were:

- Support real-time applications such as voice and/or video;
- Increase security;
- Improve application performance;
- Provide access to public cloud computing services;
- Reduce cost.

Over the last couple of years, a new category of WAN technologies, called Software Defined WANs (SD-WANs), has been introduced into the marketplace. These new technologies enable network organizations to rethink their approach to branch office WAN design and potentially enable network organizations to respond to the factors listed above.

In order to provide a broad unbiased analysis of how WAN design can and should change, executives at 6 networking vendors were interviewed. The interviewees were:

- Neil Abogado, Director of Product Marketing, Talari Networks;
- Lloyd Noronha, Director, Marketing Viptela;
- Apurva Mehta, co-founder and CTO, Versa Networks;
- Karl Brown, Senior Director, Product Marketing, Citrix;
- Michael Wood, VP Marketing, VeloCloud;
- Kiran Ghodgaonkar, Marketing Manager for Enterprise Networking, Cisco.

[1] http://www.webtorials.com/content/2015/06/2015-state-of-the-wan-report.html

Policy

One of the emerging components of WAN design that gets a lot of attention is the use of policy. Noronha stated that the primary challenge that network organizations currently have with policy is implementing it in a simple fashion from one place and having it be recognized by all components of the company's WAN. Ghodgaonkar said that as we continue to see more devices access the network combined with different types of users who have varying levels of security clearance, network organizations will need to implement more automation of policy. The network needs to be able to detect who the user is and automatically apply security profiles to the device. Wood said that business policy will play a significant role in the next generation of branch office WAN designs. He pointed out that a critical need for business policy in enterprise branch networks is the ongoing requirement to maintain consistent and appropriate configuration, performance and security templates. Abogado expanded on the role of policy. In his view, business policy will impact overall application priority and will dictate how functions, such as QoS, are deployed and enforced. In addition, application policy will establish which services are required from the network (e.g. load balancing) and where they are located.

Access to cloud services

As noted, one of the primary factors causing organizations to change their approach to WAN design is the requirement to provide a growing amount of access to cloud services. According to Mehta, users often have the ability to connect through multiple service providers. As a result, the branch network should be able to choose the best service provider based in part on an understanding of the network and security requirements of each application being accessed.

Abogado commented that network organizations that want to eliminate Internet backhaul in order to reduce cost and improve application performance now have the option of enabling local, direct Internet and cloud access from branch offices. According to Abogado, in order for this to work services such as security must be extended to the branch and that this results in increased infrastructure cost and branch complexity. He added that cost can be managed by implementing the relevant services using options such as a virtual appliance or a cloud-based appliance and that complexity can be managed by using orchestration tools and the controller-based services of a SD-WAN to simplify the provisioning and monitoring of this distributed environment.

Wood discussed another alternative to the current way of implementing Internet backhaul. According to Wood, with a cloud-delivered SD-WAN, enterprises can extend the end-to-end security from every branch office to private data centers, public cloud data centers and cloud service providers. He added that cloud gateways, which are part of a cloud-delivered SD-WAN, will provide full encryption, authentication, strong security, performance, quality of service and network impairment remediation from the branches to the cloud resources.

Location of functionality

In a traditional WAN, functionality such as optimization and security is typically provided either onsite or at a corporate data center. The preceding discussion highlights the fact that while those approaches are still viable, in the current environment there are other places to host network functionality including at a:

- Communications service provider’s central office;
- Cloud service provider’s facility;
- Co-location facility.

Brown said that enterprises don’t want to deploy multiple hardware-based devices at each branch office. He said that one option they have is to deploy a single intelligent device that can support all of the necessary functionality and which can be controlled in a centralized fashion. Alternatively, they can keep certain functions running on an intelligent device in the branch and move other functionality to the cloud. He added that independent of where the functionality is housed it’s important for network organizations to be able to centrally control how those functions are applied. The example he gave was centrally making the choice about which applications are optimized.

According to Ghodgaonkar, Cisco has found that their customers in North America like to own and maintain their own branch office equipment. Ghodgaonkar said that the size of the branch will dictate what types of services an organization will keep in the branch versus centralizing either in a data center or at a headquarters facility. For example smaller branches will lean towards centralizing network functions in a headquarters facility, while larger branches will tend to keep those functions in the branch.

Mehta’s view of where network functionality will be located is somewhat of a combination of the views of Brown and Ghodgaonkar. He believes that some organizations will keep all of the necessary functionality in the branch, others will keep it in a central site and yet others will have some functionality onsite and some offsite. Similar to Ghodgaonkar, he thinks that the size of the branch office will impact where functionality is housed. He also thinks that heavily regulated verticals, such as hospitals and banks, will tend to keep functionality in the branch while verticals such as retail that has historically been lightly staffed will lean towards centralizing that functionality.

According to Noronha, a SD-WAN controller is a strong candidate to be moved to the cloud whether it is managed there by the enterprise or by a service provider. Wood said that any function that today resides in the data center is a candidate to be virtualized and relocated to the cloud. He believes that the initial services moving to the cloud are security services such as firewall, intrusion detection and prevention, secured VPN and web security. Part of his reasoning is that security services take advantage of fast learning and nearly instantaneous updates to threat detection, mitigation and remediation which are best done with a SaaS model. In addition, all application performance monitoring and management functions will likely be relocated to the cloud due to resiliency, economies of scale and accessibility.

Network Functions Virtualization (NFV)

A topic that is closely related to the question of where WAN functionality is located is the adoption of NFV by enterprise IT organizations. According to Wood, the evolution of NFV and Virtual Network Functions (VNFs) will play a critical role in enabling network organizations to consolidate branch office resources onto a single SD-WAN Edge, using a commercially off the shelf (COTS) platform. He added that security functionality as well as network and application management functionality are good candidates to be virtualized and automated.

Ghodgaonkar agreed and added that once network organizations have virtualized the WAN, they need to look at how services can be virtualized with the goal of increasing WAN agility. He added that enterprise network organizations are already implementing a range of virtualized network services and that at the current time the highest demand is for virtualized routers, virtualized firewall and virtualized WAN optimization. Ghodgaonkar concluded by saying that by using templates to automate the deployment and configuration of network services, organizations can reduce the risk of configuration errors that can lead to exposure to security vulnerabilities.

WAN optimization

Even though *The 2015 State of the WAN Report* demonstrated that network organizations are very interested in improving application performance, some of the interviewees were not very bullish on the future role of WAN optimization. Wood said that the value of WAN optimization is diminishing in part because an increasing amount of branch office traffic is becoming uncompressible; e.g., video, UC and voice. He added that it is likely that over time that enterprises will phase out the use of WAN Optimization Controllers since a SD-WAN enables the elastic deployment of inexpensive Internet bandwidth. Mehta added that another reason why the value of WAN optimization is diminishing is because protocols such as CIFS and MAPI have evolved to where they are notably less chatty. He said that there still are circumstances in which WAN optimization is appropriate, but that what is needed is a light-weight approach that focuses on a limited set of functionality such as de-duplication, TCP and UDP optimization and optimizing access to critical cloud provided applications such as Office 365.

Security

As highlighted in *The 2015 State of the WAN Report*, increasing security is one of the primary factors driving network organizations to rethink their approach to WAN design. However, according to Ghodgaonkar, when network organizations enable direct Internet access from branch offices they are opening themselves up to greater security risks. He added that having the right security services such as content filtering, firewall, intrusion detection and prevention in the branch as well as the tools to make it easy to configure those services, will be critical for enterprises who want to reduce the security risks associated with accessing cloud-based applications.

Mehta pointed out that in the current environment that errors configuring branch office equipment can lead to security vulnerabilities. He said that while network organizations may or may not want to centralize all security functionality, they should adopt an orchestration system that can centralize the configuration of branch office functionality. He concluded by saying that to avoid errors, network organizations should have just one orchestration system to manage both security and network connectivity.

Wood stated that enterprises will be able to design better security for their branches by leveraging security functions embedded in the cloud for all traffic destined for the cloud or by leveraging VNFs on commercial off the shelf (COTS) hardware. He believes that enterprises should take a holistic approach to security design by incorporating a pervasive WAN design which delivers service insertion for cloud security services, touches cloud applications where they live (i.e., in the cloud) and monitors traffic and applications end-to-end.

Noronha said that the implementation of a SD-WAN will give network organizations something that they have always wanted – micro-segmentation. According to Noronha, when a breach occurs in a part of an enterprise network, network organizations want to be able to keep the network up and running but avoid having the breach impact other components of the network. Micro-segmentation allows them to do this.

Abogado stated that security in the branch will evolve from a model that relies on the perimeter approach to a multi-layered model that requires embedding security into all branch technologies. The philosophy behind this change is that administrators will have to make the “trust" zone an “untrust” zone since attacks can come from any vector, including inside the branch. He believes that a single layer of encryption is probably insufficient, and that IT organizations should consider encryption at both the application and network layers. Increased branch deployment of network and data segmentation are also key technologies that will support the multi-layer security model.

Abogado went on to say that the challenge with this new approach is maintaining application performance without compromising a high level of protection. An environment where no application or user flow is trusted until it is verified may drive organizations towards implementing dynamic flow policies that force unknown or unverified applications to inspection points in their network. Once these flows are verified, the SD-WAN controller can then push a more efficient trusted policy to allow for acceptable application performance.

Root cause analysis

The 2015 Application and Services Delivery Handbook identified getting better at performing rapid root cause analysis as the most important management task facing network organizations[2]. Brown agreed with the importance of getting better at performing rapid root cause analysis and added that independent of how network organization evolve their WAN design, they need insight into application delivery. He said that network organizations need to understand delay from the perspective of the application and must be able to identify how much of that delay occurred in the data center, the WAN and the branch office.

According to Wood, performing rapid root cause analysis will be much easier because a SD-WAN centralizes network visibility and monitoring functions which enables IT organizations to troubleshoot and perform root cause analysis from a central location while at the same time having network-wide, sophisticated application recognition capabilities. Abogado said that implementing a SD-WAN could add additional trouble spots to the WAN such as improperly configured tunnels or overlay routing issues. He went on to say that relative to troubleshooting a branch office WAN, that the dynamic nature of a SD-WAN link makes it difficult to establish baseline data and troubleshoot problems due to multiple, changing variables. In addition, the deployment of Internet WAN links as a part of a SD-WAN can introduce paths that traverse multiple providers and are thus difficult to monitor, control and troubleshoot. Abogado concluded by saying that one technology that will be of great help addressing these issues is an intelligent SD-WAN solution that offers simplified, automated provisioning, sophisticated reporting as well as very granular analytics that correlate application performance data from across the WAN.

[2] http://www.webtorials.com/content/2015/08/the-2015-application-and-service-delivery-handbook-2.html

Skills impact

Since the WAN is poised to undergo a dramatic transformation, there is a strong likelihood that the skills that network professionals need to have to be successful will also change. Wood said that as the WAN evolves network organizations will be modernized with advanced tools enabling them to deploy and manage branch networks as well as fostering expertise in cloud delivery architectures and application optimization practices and skill set. He added that network organizations will be freed to move up the stack to focus on revenue generating systems, solutions and applications while at the same time focusing on cost reduction initiatives.

Abogado said that it is reasonable to expect that as the WAN evolves that the demand for the traditional network skills associated with technologies such as routing and MPLS implemented via a CLI-driven provisioning and monitoring system will plateau and start to decline. He added that in contrast to the decline in the demand for these traditional skills there will be an increased demand for a skill set that enables the merging of applications, security, and networks into a virtualized or cloud infrastructure that is provisioned via orchestration tool(s). Abogado recommended that network professionals develop skills that allow them to understand an application's architecture and requirements. He added that these skills will enable network professionals to take an application’s requirements and build a policy compliant orchestration blueprint that accommodates security, QoS, optimization services and network resource allocation. That blueprint can then be leveraged by an orchestration tool, in conjunction with an underlying controller-based infrastructure, to deploy the application with the appropriate access and services across the WAN.

Call to action

There is no doubt that the introduction of SD-WAN technologies has started what will be a multi-year evolution of the WAN. At a high level, many aspects of what the next generation branch office WAN will look like, such as the increased use of policy, are very clear. However, the details of the next generation branch office WAN are far less clear and likely will vary somewhat by enterprise.

Sitting on the sidelines waiting for all of the issues to be resolved is not an effective strategy for most network organizations and that passive approach does not advance the career of network professionals. *The 2015 Guide to WAN Architecture and Design*[3] contains the outline of a project plan that network organizations can use to evolve its WAN. It includes topics such as how to choose vendors, how to manage existing contracts with communications services providers and how to build a business case.

[3] http://www.webtorials.com/content/2015/06/2015-guide-to-wan-architecture-and-design.html