The Requirement to Re-think the Enterprise WAN

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

Introduction

The traditional approach to branch office networking is to backhaul internet traffic to one or more corporate data centers. The issues associated with backhauling Internet traffic will be discussed in the next section. Some of the other issues with the traditional branch office WAN stem from the limitations of the two dominant WAN services: MPLS and the Internet. The 2015 Application and Services Delivery Handbook identified the concerns that network organizations have with those two services. Those concerns are shown in Table 1 in descending order of importance.

<table>
<thead>
<tr>
<th>Table 1: Concerns with WAN Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Concerns with MPLS</strong></td>
</tr>
<tr>
<td>Cost</td>
</tr>
<tr>
<td>Uptime</td>
</tr>
<tr>
<td>Latency</td>
</tr>
<tr>
<td>Lead time to implement new circuits</td>
</tr>
<tr>
<td>Security</td>
</tr>
</tbody>
</table>

In addition to the concerns shown in Table 1, the next section of this white paper discusses a number of factors that are also putting pressure on network organizations to change how they design their WAN. To help network organizations avoid the negative consequences that would likely occur if they took too narrow of a view of that redesign, this white paper identifies some of the key considerations that network organizations must take into account when evolving their WAN.

Trends Driving Change in the WAN

In the traditional approach to branch office networking, organizations backhauled their Internet traffic as a way to secure this traffic. The disadvantages of that approach are that it adds to cost and it degrades performance. These disadvantages are acceptable if the amount of Internet traffic is small and if the Internet traffic isn’t business critical. However, as the amount of Internet traffic grows and/or as the traffic becomes increasingly business critical, this approach becomes unacceptable.

The 2015 State-of-the-WAN Report contained the results of a survey in which the survey respondents were asked to indicate the three factors that would likely have the most impact on their WAN over the next twelve months. The factors mentioned most frequently are shown in Table 2.
Table 2: Factors impacting WAN evolution

<table>
<thead>
<tr>
<th>Factor</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support real-time applications such as voice and video</td>
<td>37%</td>
</tr>
<tr>
<td>Increase security</td>
<td>32%</td>
</tr>
<tr>
<td>Improve application performance</td>
<td>27%</td>
</tr>
<tr>
<td>Provide access to public cloud computing based applications and services</td>
<td>26%</td>
</tr>
<tr>
<td>Reduce cost</td>
<td>24%</td>
</tr>
<tr>
<td>Support mobile users</td>
<td>24%</td>
</tr>
</tbody>
</table>

As network organizations plan for the evolution of their WAN, they must ensure that their WAN can respond to the factors shown in Table 2. As shown below, the factors listed in Table 1 are some of the biggest drivers of increased use of the Internet. This means that ensuring that a WAN can respond to these factors means planning for a significant increase in Internet traffic, and for most organization this means planning to reduce or eliminate backhauling Internet traffic.

The 2015 State-of-the-WAN Report also contained the results of a survey in which the survey respondents were asked to indicate the two applications that were driving the biggest increase in their use of MPLS and Internet services. Their responses are shown in Figure 1.

As shown in Figure 1, the three applications driving the biggest increase in the use of the Internet are public cloud computing, video and mobility. Numerous reports have documented that the use of public cloud computing, video and mobility will continue to increase for the foreseeable future. While using the Internet to access any form of public cloud computing presents security and performance challenges, those challenges are particularly difficult when accessing a SaaS-based application. The reason for that extra difficulty is that in most cases the SaaS provider won’t allow users to house any security or performance appliances on the provider’s premises.

Figure 1: Applications Driving Biggest Increase in MPLS and Internet Services
The Impact of Ineffective WAN Design

Relative to its ability to respond to the factors listed in Table 2, the traditional WAN is:

- Expensive;
- Rigid & cumbersome to deploy;
- Plagued by high latency & low bandwidth.

In an attempt to overcome the concerns highlighted in Table 1, many network organizations either already have implemented, or are looking to implement a hybrid WAN; i.e., a WAN based on having two or more disparate WAN links into branch offices. The goal of a hybrid WAN is to maximize the benefits of both MPLS and the Internet while minimizing the negatives that are associated with these services. Whether or not their WAN re-design includes implementing a hybrid WAN, network organizations are also beginning to move away from a traditional CLI-based approach of managing network elements on a box-by-box basis and are adopting the emerging approach of having all of their platforms support open APIs that tie into orchestration platforms.

There are many ways to construct a hybrid WAN. One option is to have two connections to the Internet that are provided by different ISPs and which use diverse access such as DSL, cable or 4G. Another option is to have one WAN connection be an Internet connection and the other be a connection to an MPLS service. To eliminate the disadvantages associated with backhauling Internet traffic, many hybrid WANs feature direct internet access (DIA) from branch offices. There is no doubt that implementing a hybrid WAN may provide benefits. However, there is also no doubt that no matter what type of WAN they utilize, network organizations must focus on the security and performance of that WAN.

Security

In 2014 a highly publicized security attack on a US retailer highlighted both the growing sophistication of security attacks as well as the fact that in addition to being an IT challenge, protecting against security attacks is also a business challenge. In that attack, thieves stole massive amounts of credit and debit card information and they also stole the names, addresses and phone numbers of millions of the retailer’s customers. As a result of the security breach, the company’s profits dropped by almost 50%. As sometimes happens when there is a breach of this magnitude, the company fired their CIO. However, because of the impact on profits, the company also fired their CEO.

According to the IBM X-Force Threat Intelligence Quarterly 1Q 2015, the attack on that retailer was part of a significant increase in security attacks that occurred in 2014. According to that report, in 2014 there were a billion leaked records (i.e., emails, credit card numbers, passwords and other personally identifiable information) which was an increase of 25% over the 800 million records that were leaked in 2013. The IBM report also stated that in 2014 mobile devices were shown to present some unique security vulnerabilities that enable attackers to perform man-in-the-middle attacks against some mobile applications. The report also highlighted the fact that there are more than a billion unique websites on the Internet and that a large percentage of these sites are dependent on the same operating systems, open-source libraries and content management system (CMS) software. According to the report, in 2014, several of the most popular CMS platforms had major vulnerabilities in both the core platform and widely used plug-ins.

The IBM X-Force Threat Intelligence Quarterly 1Q 2015 also presented survey data that indicated that the two most common forms of security attack are malware and DDoS. Part of the challenge with combatting malware attacks is that malware authors continue to develop new, sophisticated ways to
infect systems, sometimes as part of a multi-stage attack. Perhaps more concerning than the frequency of DDoS attacks that is documented in the IBM report is the growing intensity of those attacks.

As mentioned, many network organizations either already have implemented DIA or are looking at it. Implementing DIA without having an effective layer of security opens these organizations to the types of security breaches discussed above. While it is possible to attempt to implement a secure approach to DIA by keeping security appliances such as firewalls and secure Web gateways in each branch, this approach is both capital intensive and requires significant support. It is also highly likely that this approach will not be able to effectively respond to a DDoS attack of the magnitude discussed above. In addition, implementing security functionality in branch offices won’t provide protection for mobile workers.

Performance

Due to a number of factors, the Internet experiences much higher levels of latency and packet loss that do enterprise WAN services such as MPLS. Those factors include:

- The Internet is a network of networks and there isn’t a person or a body that is responsible for the end-to-end design or performance;
- Due to the Internet business model that there is often congestion at peering points;
- Routing through the Internet is based on economic considerations not performance.

The Internet’s high levels of latency and packet loss are demonstrated in Figure 2 and Figure 3. Those figures were generated on October 27, 2015 using Keynote.

Figure 2: Internet Latency

Source: Keynote Internet Health Report

![Figure 2: Internet Latency](image-url)
The higher levels of latency and packet loss that are associated with the Internet typically lead to degraded application performance. *The 2014 State of the WAN Report* contained the results of a survey in which the respondents were asked to indicate what happens if one or more of their company’s business critical applications doesn’t perform well. The three most common responses were that the CIO gets pressure from their boss or from the related business unit manager; that it tarnishes the reputation of the IT department; and that it causes the company to lose revenue.

One of the reasons why increased latency results in poor application performance is due to chatty protocols and applications which require hundreds of round trips to complete a transaction. For the sake of example, assume that a business transaction requires 200 round trips. If that transaction takes place over a LAN with 1 ms of round trip delay, the chatty nature of the transaction adds a mere one fifth of a second to the overall delay. In virtually all instances, that amount of added delay is negligible. However, if that transaction ran over a WAN with 50 ms round trip delay, the chatty nature of the transaction would add 10 seconds of delay which would likely cause users to complain bitterly.

As demonstrated in an article entitled *More Bandwidth Doesn’t Matter (much)*, due to the way that HTTP uses short, bursty connections, WAN latency also has a significant impact on the amount of time it takes to download a Web page. The authors of that article ran tests that demonstrated the impact that latency has on Web-page download times. The result of those tests, which assumed zero packet loss, a round-trip-time (RTT) of 60 ms and which were based on a simulation of 25 of the web’s most popular web pages, is shown in Figure 4.
As shown in Figure 4, network latency has a dramatic impact on the page load time.

The impact of packet loss was documented in a paper by Mathis, et.al.\(^1\). That paper contains a formula that provides insight into the maximum TCP throughput on a single session when there is packet loss. That formula, which is independent of the bandwidth of the WAN link, is:

\[
\text{Throughput} \leq (\text{MSS}/\text{RTT}) \times (1 / \sqrt{\text{p}})
\]

Where MSS is the maximum segment size and p is the packet loss rate. The preceding equation shows that throughput decreases as either the round trip time or packet loss increases. To exemplify this, assume that MSS is 1,420 bytes. The following table exemplifies how the maximum throughput decreases for varying value of RTT and p.

<table>
<thead>
<tr>
<th>Round Trip Time</th>
<th>Packet Loss</th>
<th>Maximum Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 ms</td>
<td>0.1%</td>
<td>7.18 Mbps</td>
</tr>
<tr>
<td>50 ms</td>
<td>1%</td>
<td>2.27 Mbps</td>
</tr>
<tr>
<td>100 ms</td>
<td>0.1%</td>
<td>3.59 Mbps</td>
</tr>
<tr>
<td>100 ms</td>
<td>1%</td>
<td>1.14 Mbps</td>
</tr>
<tr>
<td>200 ms</td>
<td>0.1%</td>
<td>1.80 Mbps</td>
</tr>
<tr>
<td>200 ms</td>
<td>1%</td>
<td>0.57 Mbps</td>
</tr>
</tbody>
</table>

The data in Table 3 shows that if the packet loss increases from 0.1% to 1%, the maximum throughput decreases by 68%. That data also shows that as the round trip time increases from 50 ms to 200 ms, the maximum throughput decreases by 75%.

\(^1\) The macroscopic behavior of the TCP congestion avoidance algorithm by Mathis, Semke, Mahdavi & Ott in Computer Communication Review, 27(3), July 1997
Summary and Key Considerations for WAN Design

There are a number of trends that are pressuring network organizations to change their approach to how they design their WAN. In addition to the perpetual requirement to reduce cost, these factors include:

1. Supporting real time applications such as voice and video;
2. Increasing security;
3. Improving application performance;
4. Providing access to public cloud based applications and services;
5. Supporting mobile users.

As part of their response to these trends, network organizations are exploring a range of WAN design alternatives, including implementing a hybrid WAN. While bullets #2 and #3 explicitly highlight the requirement to focus WAN design on security and performance, that requirement is also implicit in the other three bullets. For example, as companies make more use of public cloud based applications and services, the combination of security and performance are critical considerations. Unfortunately, in some instances network organizations are choosing solutions that provide better performance or enhanced security instead of choosing solutions that provide both better performance and enhanced security.

As discussed in this white paper, the reasons why security and performance are critical considerations are quite simple and quite compelling. On an ever increasing basis, security attacks are getting more sophisticated and more intense and these attacks are causing companies to lose revenue and market valuation. They are also causing senior executive to lose their jobs. In a similar vein, network organizations are under intense pressure to show business relevance. One sure way to not show relevance is to cause the business to lose revenue, which commonly happens when the performance of a business critical application degrades.

Because of the security vulnerabilities and performance issues that are associated with the Internet, it is important that as network organizations re-design their WAN that they pay particular attention to what they can do to improve both the security and performance of the Internet. For example, given the concerns that were shown in Table 1, network organizations must ensure that Internet transport is reliable and secure and that it is optimized to minimize both latency and the impact of packet loss. Ideally, the Internet transport will have the same type of SLA that is commonly available with enterprise WAN services such as MPLS.

There is a range of functionality that can be leveraged to improve the performance of Internet transport. That includes:

- **Route optimization:** Choose the optimum path through the Internet
- **Caching:** One option is to have a proxy server cache frequently accessed objects from Web pages that are hosted remotely over the WAN
- **De-duplication:** Only send the changes that have been made to a file since the last time the file was sent
- **Forward error correction:** Have each packet carry additional information that negates the need to re-transmit lost packets
QoS: Prioritize traffic based on its business criticality

As part of improving the security of the Internet, network organizations need to consider either replacing or supplementing their on-premise security devices with a highly-distributed, cloud-based security functionality. That functionality includes:

Next generation firewalls: Protects against the current generation of intense DDoS attacks that can overwhelm the capacity of premise-based appliances

Secure Web gateways: Filters unwanted software/malware from branch office and mobile user-initiated Internet traffic and enforces corporate and regulatory policy compliance

As mentioned, as companies evolve their WAN, it is highly desirous to have the WAN provide an SLA, whether the traffic is carried over MPLS or over the Internet. Monitoring and managing an SLA is difficult. It is particularly difficult when accessing SaaS-based applications because as mentioned, SaaS provider typically won’t allow their customers to house any functionality on the provider’s premises. Hence, similar to the situation with security, network organizations need to consider either replacing or supplementing their on-premise management functionality with cloud-based management functionality. However, in part to avoid the siloed approach to management that results from using proprietary tools and in part to be able to tie into orchestration platforms, these cloud-based tools must support open APIs.
About the Sponsor:

Akamai is the global leader in Content Delivery Network (CDN) services, making the internet fast, reliable and secure for its customers. The company’s advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere.

About the Webtorials® Editorial/Analyst Division

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

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.