

Overcoming the Challenges of WAN Application Delivery



WAN
 VoIP
 SME
 Internet Cloud
 VPN SaaS

OVERVIEW

Today's small-to-medium size enterprises (SME) rely heavily on their business applications being sent reliably over the Internet, outside of their local area network (LAN). Their cloud-based and SaaS applications cover such functions as inventory, accounting, customer relationship management (like Salesforce), ERP, point of sale (POS), email, voice over IP (VoIP), video conferencing, file-sharing, virtual desktop infrastructure (VDI) and other critical applications that are the livelihood of a company's operations. Quick and reliable delivery of these applications to users is a primary objective and often a major challenge for today's IT departments.

To achieve greater productivity, local employees, telecommuters, business partners and customers must all have unhindered access to critical applications. Any delay in delivering these applications, or deficiency in the availability and security of the applications, can cause user productivity to suffer and adversely affect business profitability. The best designed applications are no good if users can't reach them.

Therefore, choosing the appropriate wide area network (WAN) architecture is critical to ensure efficient use of WAN resources and infrastructure to meet today's requirements, while also ensuring the right path for tomorrow's business needs.

This white paper explores the difficulties and solutions for reliable delivery of applications over the WAN.

DIFFICULTIES ABOUND

When it comes to delivering applications over the WAN, there are many obstacles to overcome. Lack of sufficient bandwidth and latency issues result in low throughput and long delays. Slow or difficult-to-use remote access applications can also attribute to lost productivity, while insufficient security can put private data and the applications themselves at risk. Cloud-hosted applications consume significant amounts of bandwidth that organizations have not previously required. For example, an on-premises SharePoint or Office installation uses essentially no bandwidth, whereas Microsoft estimates that a cloud-based SharePoint demands about 1.6Mbps per hundred users. Extrapolate this to a number of cloud-based applications and the pressure on the WAN becomes acute.

Obstacles to efficient application delivery over the WAN

- Relying on a single ISP for network connectivity is dangerous.
- Getting enough bandwidth to support business-critical applications can be expensive.
- Getting enough bandwidth to support mission-critical applications can be hard to manage.
- Lack of planning for complete application performance over the WAN can undermine success.

WHY TRADITIONAL APPROACHES FALL SHORT

In many organizations, IT personnel find themselves bogged down addressing poorly performing WAN networks. Rather than solving the core problem with the most cost-effective and efficient solution, they often resort to adding more bandwidth, which doesn't fully solve the problem. When applications are migrated to the cloud and deployed over the WAN, the expectation is that the months of planning and trials will deliver a successful rollout. Unfortunately, problems often surface when the application is rolled out to the whole user population.

While many applications are customized to take advantage of business processes and optimize user productivity, when those applications are deployed over the WAN, the application performance often degrades, causing user productivity to suffer and adversely effecting the bottom-line. Performance issues are often classified as network problems, even if the network infrastructure is working well for other applications.

Some issues that can adversely affect applications over the WAN include:

- Poor WAN link performance
- ISP link failure
- Congestion from too much traffic going over the WAN link

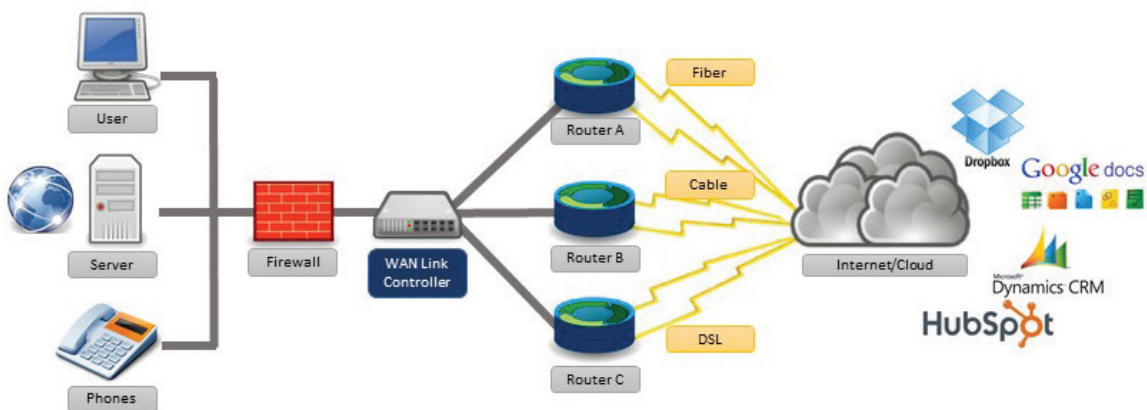
Fortunately, solutions exist that affordably address problems associated with delivery of critical applications over the WAN.

IT TAKES MORE THAN JUST A DUAL WAN ROUTER

Solving the WAN application delivery challenge requires intelligent WAN link controllers, which differ significantly from dual WAN routers. A dual WAN router uses simple policies to “route outbound-only traffic” over one of two lines. There is no intelligence in the technique and no method to avoid or minimize congestion. In fact, the rigid nature of the dual WAN router’s technique frequently adds to congestion problems and does nothing in terms of WAN and ISP link load balancing.

Moreover, dual WAN routers are incapable of failover for inbound traffic, leaving inbound services susceptible to outages. This can cause lost revenue associated with downed e-commerce sites, or lost productivity from remote offices with users losing access across VPNs.

A more cost-efficient and flexible solution uses WAN link controllers that provide ISP multi-homing and intelligent load balancing and failover. This solution utilize micro-appliances that are located between firewalls and WAN gateway devices, and use a simplified and more up-to-date architecture often based on Network Address Translation (NAT) and Domain Names Service (DNS).



SOLVING THE WAN APPLICATION DELIVERY CHALLENGE

INTELLIGENT LOAD BALANCING, FAILOVER AND SECURITY

The most cost-effective and flexible solutions for addressing WAN application delivery challenges are WAN optimization solutions that bring together cost-saving bandwidth, flexible link aggregation, network security and automatic WAN link and site failover required for small-to-medium size enterprises that deploy critical applications over WAN or ISP networks. Today’s advanced WAN optimization products bring together the capabilities required for ensuring network availability for applications. These products should include three key capabilities:

1. Inbound and Outbound Load Balancing — Ensures that bandwidth is always available to all applications and users
2. Inbound and Outbound Failover — Ensures network reliability and site uptime
3. Security — Ensures applications are protected from network attacks

ISP and WAN Link Aggregation — provides the flexibility needed to cost- effectively bring multiple links together

OUTBOUND LOAD BALANCING - An optimal WAN solution provides outbound bandwidth load balancing and failover. The user defines weights (bandwidth capacity) based on the bandwidth of each WAN link. When a session or call is generated from the LAN, the appliance computes which link has the most available bandwidth and routes traffic from that session or call over that particular WAN link. The device typically allows the selection of two link load balancing algorithms:

- Symmetrical round robin - routes sessions to all links in a round robin manner.
- Intelligent (weighted) load balancing - computes a ratio between the weight (bandwidth capacity) of the different WAN links, and then routes sessions and calls accordingly. That is, the faster the link, the more sessions or calls that will be sent over that link, in order to make the most efficient use of all the bandwidth available. Additionally, an intelligent link load balancing solution will examine the amount of real-time traffic on each link, compared to the amount of available bandwidth resources left, and choose the best path for the next session or call's most optimal route for performance.

INBOUND LOAD BALANCING - This is accomplished by the WAN micro-appliance acting as the authoritative DNS server for the domain. The appliance advertises all available WAN links to the DNS caching servers which in turn resolve the domain names to queries in a round robin format. In this manner, all externally initiated sessions are load balanced over all available links. Since the appliance is resident at the domain site and is able to directly monitor the link status, failed links are removed from the DNS tables immediately upon failure. By setting the host name record Time-to-Live (TTL) to a short period (i.e. 30 seconds), the DNS caching servers will flush their address tables and will update them from the appliance regularly, and thus be informed when a link fails.

Border Gateway Protocol (BGP) has long been used for multi-homing by some large enterprises, but the cost and complexity of BGP makes it impractical for most small and midsized businesses. The alternate approach using NAT and authoritative DNS to overcome these restrictions provides more manageable and less expensive outbound and inbound link load balancing and failover.

ISP and WAN Link Load Balancing — Ensures that bandwidth is always available to all applications and users

HIGH AVAILABILITY - Since all outbound and inbound traffic must pass through the micro-appliance, should it fail, the entire site will be inaccessible. To address this, some vendors support redundant configurations. Usually, a standby (or redundant) configuration is supported, sometimes referred to as High-Availability or HA. It is advisable to utilize High Availability, as it would be risky to deploy multiple WAN links for redundancy and scalability, only to lose the entire site due to the micro-appliance hardware failure. Should one of the micro-appliances go down, the other device takes over automatically and an alert is sent to the administrator. Traffic flow resumes over the second device. For more information about device failover, see the Ecessa white paper “Everything You Need to Know About Network Failover.”

PERFORMANCE - Performance of applications over the WAN directly affects response time. This includes not only total average transaction time, but assures that users located at performance-challenged sites (such as branch offices) still receive the acceptable level of performance.

Performance is an important criterion for any piece of networking equipment, but it is critical for WAN devices, because datacenters are central points of aggregation. As such, the micro-appliance should support extremely high volumes of traffic transmitted to and from sites.

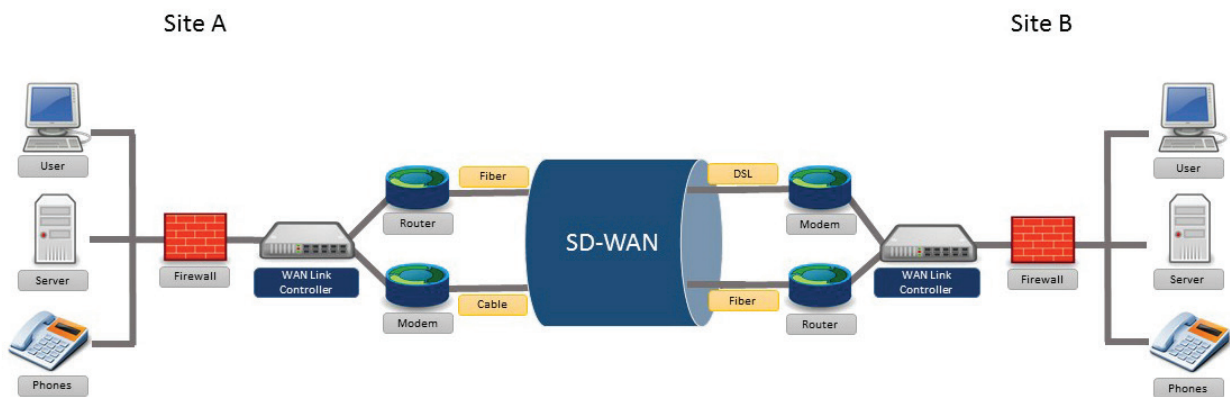
A simple definition of performance is how many bits-per-second the device can support. While this is extremely important, in the case of a micro-appliance, other key measures of performance include how many WAN links, how fast the failover occurs from one link to another, number of supported concurrent sessions, number of domain names, and number of hostnames within each domain.

TRAFFIC SHAPING AND APPLICATION PRIORITIZATION - Traffic shaping includes the ability to prioritize network traffic to ensure that adequate bandwidth is always available to specific bandwidth-intensive applications, especially during periods of congestion. Rules determine bandwidth minimums and maximums for specific types of traffic and use load balancing and automatic failover to direct this traffic to links with sufficient bandwidth. WAN devices should provide traffic shaping and application prioritization support for traffic based on defined rules.

ISP and WAN Link Failover — Ensures network reliability and site uptime

DISASTER RECOVERY/SITE FAILOVER - Many businesses need to redirect Internet traffic to a disaster recovery site should a catastrophe disrupt a main site. WAN optimization solutions have, in effect, reduced the cost to ensure that site failover and fallback occur automatically, and reliably, making this functionality practical and affordable even for the smallest businesses.

SD-WAN AND WAN VIRTUALIZATION - Some of today's most advanced WAN device offerings integrate software-defined WAN features to bond multiple network links into a single high-bandwidth channel to ensure high-availability for applications. If one link goes down or degrades in performance, traffic is automatically directed to the best working links without interruption.



WAN Virtualization is a form of load balancing which allows for stateful failover of traffic to the best performing links to ensure critical applications avoid problems that occur when they are stopped on one link and restarted over another link. Using different SD-WAN traffic routing options, network administrators can ensure that critical applications avoid failures and are never adversely affected, even during carrier or ISP disruptions and outages.

SECURITY - Advanced WAN offerings include built-in firewalling and security features to provide added security and lower the cost of support, maintenance and overall infrastructure complexity through device consolidation. This is a desirable feature for many small businesses.

SUMMARY

When it comes to delivering applications over the WAN, there are many obstacles to overcome. Lack of sufficient bandwidth for cloud-based applications and latency issues will result in low throughput and long delays. Getting enough bandwidth to support business-critical applications can be expensive and difficult to manage. Insufficient security can put private data and the applications themselves at risk. Lack of planning for complete application performance over the WAN can undermine success.

Dual WAN routers are insufficient to meet the needs of organizations that rely on WAN/Internet connectivity and cloud-based resources. BGP is not an affordable or practical solution for SMEs. Cost-efficient and flexible solutions exist using WAN link controllers that provide ISP multi-homing and intelligent load balancing and failover. Advanced SD-WAN solutions provide additional WAN management features, including stateful failover to ensure that critical applications avoid failures and are never adversely affected, even during carrier or ISP disruptions and outages.

KEY NETWORK CONSIDERATIONS

To optimize network and application performance, make sure your WAN architecture includes:

1. Inbound and Outbound Load Balancing — Ensures that bandwidth is always available to all applications and users
2. Inbound and Outbound Failover — Ensures network reliability and site uptime
3. Security — Ensures applications are protected from network attacks

ECESSA WAN SOLUTIONS

Ecessa's intelligent WAN link controllers and SD-WAN solutions improve network performance, while delivering high-availability and reliable connectivity for multiple and diverse ISP and WAN links. Ecessa is the ideal solution for any SME seeking to cost-effectively improve performance and uptime for applications going over the WAN or Internet. Ecessa integrates multiple technologies to deliver highly efficient link aggregation, load balancing and failover for greater reliability and improved performance, while reducing ongoing operational expenses through the consolidation of multiple WAN capabilities within a single micro-appliance. This is an affordable solution for reducing the number of WAN traffic management devices and allows SMEs to take advantage of cost-efficient bandwidth to meet application delivery needs. Ecessa solutions deliver...

- Faster and less expensive deployment and administration of multiple ISP and WAN links, automatically directing traffic to the more cost-efficient and best performing WAN links
- Reduction of expensive WAN links, dramatic performance gains through efficient management of WAN link availability, and reduced WAN deployment costs
- Higher productivity for users, featuring automatic WAN and ISP link load balancing and failover, multiple site failover, and traffic shaping and application prioritization to speed the delivery of critical applications

Visit www.ecessa.com for more white papers.



13755 1st Avenue North, Plymouth, MN 55441 | www.ecessa.com
toll free: 1.800.669.6242 | 763.694.9949