The Requirement for an Application Delivery Network

By Jim Metzler, Cofounder, Webtorials Editorial/Analyst Division

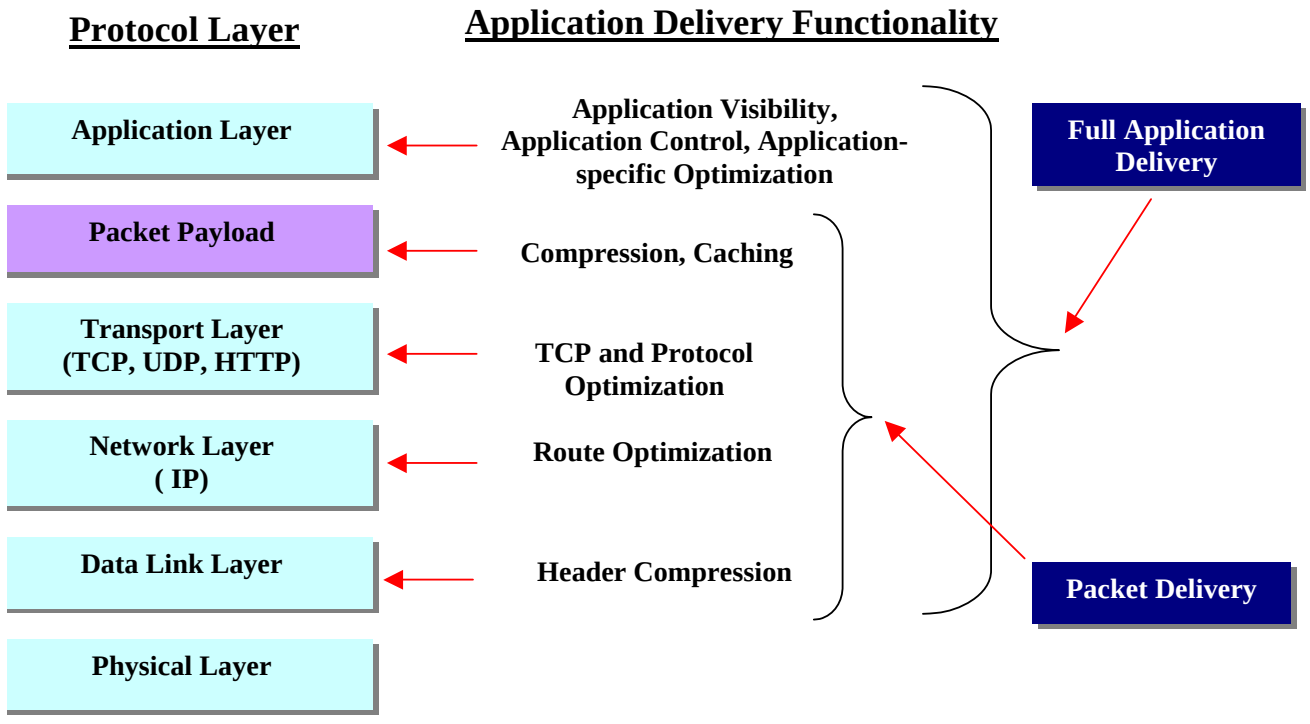
Introduction

The basic business benefits of WAN Optimization and Application Acceleration over the WAN have been well established. They include:

- Reduced WAN bandwidth expenses
- Reduced congestion on WAN ports
- Reduced OPEX and CAPEX through the facilitation of consolidation and centralization of servers, applications, and storage resources
- Improved remote employee productivity through reduced application response time

Some of these basic benefits can be gained by deploying devices that are focused on optimizations within the packet delivery network. By *packet delivery network* is meant the packet payload and the transport, network and data link layers of the Internet protocol suite, as shown in Figure 1.

Figure 1: Application Delivery vs. Packet



As Application Delivery technology continues to evolve, much more attention is being paid to the Application Layer. Solutions that leverage functionality that resides higher in the OSI protocol stack can dramatically improve the effectiveness of Application Delivery based on the ability of these solutions to recognize application layer signatures and to then differentiate among the various applications that share and contend for common transport resources. Differentiation among applications opens the door to significant improvements in application-specific bandwidth optimizations, security, and management.

The remainder of this brief will present a Framework for evaluating and implementing Application Delivery solutions and then will also focus on describing some of the emerging challenges facing business today. This will be following by a discussion of how Application Delivery solutions that include extensive Application Layer functionality can help IT organizations address these challenges.

The Changing Application Environment

As recently as a few years ago, the typical application environment was relatively simple. At that time, the majority of users worked in a headquarters facility and accessed applications locally. In addition, the types of applications that traversed the typical enterprise network at that time were limited in scope and were not very demanding; e.g., email, inquiry/response, bulk file transfer. In this type of simple application environment, it is generally possible to ensure acceptable application performance by implementing optimization techniques that function within the packet delivery network.

The current application environment is becoming increasingly complex. Some of the factors that are driving that complexity include:

- The majority of users now work in branch offices and access applications over a WAN.
- A growing number of real time applications such as collaboration and unified communications now transit most enterprise networks.
- The trend to consolidate data centers and also move to a single hosting[1] model results in lengthy WAN links that are likely to have increased levels of delay, jitter and packet loss.
- The number of applications on the typical enterprise network has increased dramatically and the content of these applications is increasingly likely to be rich media.
- Trends like social networking have increased the number of applications which IT organizations need to either control or eliminate.

The only way to ensure acceptable application performance in the current complex application environment is by implementing an application delivery network as described in a subsequent section of this white paper.

[1] In a single hosting environment, a given application such as SAP is hosted in only one of the enterprise's data centers.

Application Delivery Framework

The 2008 Handbook of Application Delivery presents a model for an Application Delivery Framework. This framework has proven useful as a guide for IT organizations who want to evolve their organization to where they are more effective at application delivery. This framework has also proven useful as a checklist that IT organizations can use to ensure the successful implementation of Application Delivery technology. The Framework incorporates four categories of activities: Planning, Optimization, Management, and Control.

Planning

Many planning functions are critical to the success of Application Delivery. Some of the more important steps in planning include:

- Baselining the performance of the network and of key applications.
- Developing applications with a focus on how well those applications will perform over the WAN.
- Quantifying the impact of deploying new applications.
- Predicting the benefits that can be expected from deploying various Application Delivery solutions.

Optimization

Many of the optimization techniques that are associated with Application Delivery are intended to mitigate the effects of low WAN bandwidth and high WAN latency on application performance. These optimization techniques:

- Reduce the amount of data that is sent over the WAN by implementing compression, caching and de-duplication.
- Reduce the number of WAN round trips (transport layer or application turns) that are necessary for a given transaction by implementing request prediction and spoofing.
- Mitigate the inefficiencies of applications and protocols ill-suited to the WAN environment.
- Offload computationally intensive tasks from client systems and servers.

Management

Some of the key management tasks that are associated with Application Delivery include:

- Discovering the applications running over the network and identifying how they are being used.
- Gaining end-to-end visibility into the ongoing performance of key applications.
- Identifying the component of IT that is the cause of application degradation; e.g., network, server, database or application.
- Identifying the root cause of why that component of IT was causing application degradation.

Control

Maintaining control over the application environment involves:

- Identifying and controlling the traffic traversing the WAN.
- Enforcing company policy governing applications, users, and devices that are authorized to access the network.
- Identifying, classifying, and prioritizing application traffic that is business critical and delay sensitive.
- Performing traffic management and dynamically allocating network resources.
- Identifying and eliminating any form of malicious traffic

Emerging Business Demands

There are a number of emerging business demands that are complicating the task of application delivery. These business demands include: more stringent government and industry regulations regarding privacy and data integrity, the continued trend toward globalization and workforce mobilization, and the increased emphasis on business agility as a means for maintaining competitiveness.

Security and Regulatory Compliance

Companies of virtually all sizes and industries are under increasing pressure to demonstrate compliance with corporate policy as well as government regulations and industry standards to ensure privacy and data integrity. As a result, regulatory compliance has been one of the primary drivers for the consolidation of IT resources into centralized data centers. While centralization makes data easier to manage, it forces IT departments to provide enhanced, self-documenting security measures to ensure data privacy/integrity and to control user access to central resources via both the private WAN and the Internet.

Business Globalization and Workforce Mobilization

The continuing trend to globalization drives many requirements, including the requirement to:

- Interconnect facilities such as branch offices, manufacturing sites, distribution centers, customer service sites and R&D installations around the world.
- Support the outsourcing of key functions, such as manufacturing, distribution and call centers.
- Interconnect the company with a wide range of business partners.

Globalization also tends to broaden the range of applications delivered over the network to include more Internet-based Web applications as well as software-as-a-service (SaaS) applications and unified voice/video/data communications. As a result, globalization adds significantly to the challenges of securing the network and assuring regulatory compliance.

In addition, because of the decentralization and mobility of the modern workforce, the IT organization must enable employees to successfully access applications from anywhere, including branch offices, home offices, hotels, coffee shops, etc. The phrase *successfully access applications* means that the access must be secure, cost effective and exhibit acceptable performance. Unfortunately, worker mobility and the associated mobile computing devices exacerbate security risks from viruses and other malware that can be propagated into the enterprise network. Therefore, the mandate to support mobility results in

the requirement for more robust security measures, including virus/malware detection and traffic screening to thwart intrusions that masquerade as legitimate enterprise application flows.

Business Agility

The requirement for increased business agility is motivating IT organizations to adopt new application architectures including Services Oriented Architecture (SOA), SaaS/Cloud Computing, and Web 2.0/mashups. Because most of these architectures are based on Web technologies, IT organizations are challenged to find ways to identify which Web applications are business critical in order to provide preferential treatment for these applications over the more mundane or recreational applications that are also Web-based. Maximizing the business-effectiveness of the network may also make it necessary to limit or possibly eliminate the usage of certain recreational applications and Web sites.

The Application Delivery Network

As shown in Figure 1, packet delivery and the corresponding optimization techniques correspond to functionality focused on the packet payload and the lower four layers of the Internet protocol suite. The packet delivery network is quite effective in terms of providing the basic benefits of WAN Optimization as described in the introduction. However, just focusing at the packet layer is limited. In particular, the packet delivery network has limited knowledge of users and content and can not identify malicious traffic. In addition, the packet delivery network cannot leverage the application headers that contain a wealth of valuable information that can be leveraged to control the performance and security of applications in order to meet the evolving business challenges.

Application Delivery Network (ADN) is an emerging industry phrase that refers to implementing application delivery technologies that reside above layer 4 in the OSI stack. For example, the ADN employs deep packet inspection (DPI) to parse application headers and content and uses this information to further optimize performance monitoring, application acceleration, the management of application security and WAN access, and control of how application utilize WAN resources. Therefore, in the context of the Application Delivery Framework, the ADN provides enhanced functionality in all three areas of implementation: Optimization, Management, and Control.

Optimization

DPI enables application delivery solutions to recognize applications based on signatures in the application headers. Application recognition enables application-specific optimization techniques that can significantly minimize bandwidth consumption and mitigate the effects of WAN latency. DPI also makes it possible to distinguish between business critical Web-based applications (e.g., webified enterprise applications, as well as specific SOA and Web 2.0 applications) and other traffic that relies on HTTP. In addition, DPI makes it possible to sub-classify the network flows generated by complex enterprise applications, such as SAP and Oracle, allowing the critical operations and transactions to be afforded the highest priority access to WAN bandwidth.

Management

ADN functionality as described above also provides the visibility that allows the performance of each application and of each application user to be monitored in a highly granular fashion. This functionality provides IT organizations with the capability to identify performance issues before they impact end users.

However, while identifying performance issues before they impact end users is highly desirous, that capability alone is not sufficient to ensure acceptable application performance. In particular, the ADN must also be able to control the applications that are contributing to the performance issues.

Control

The control component of application delivery focuses on performance and security.
In particular, ADN functionality allows the IT organization to implement highly granular policies governing QoS and bandwidth allocation and to enforce policies governing authorized user access to specific applications. ADN DPI technology that can scan application headers and the packet payloads for application signatures provides another layer of security to the network. DPI can also be used to scan for viruses and other malware that may be contained in Web content or may be attempting to piggyback over enterprise application flows. By maintaining logs of user access to applications and by logging the results of security scans, the ADN provides another source of audit information that be used to document compliance with various privacy/integrity regulations, such as HIPAA and PCI.

As previously noted, companies of virtually all sizes and industries are under increasing pressure to demonstrate compliance with government regulations and industry standards to ensure privacy and data integrity. In addition to that pressure, in difficult economic times the occurrence of cyber hacking increases dramatically. For example, a number of recent articles have commented on the great increase in the amount of malware[2] [3]. As a result, an effective ADN must support security functionality beyond what was described in the preceding paragraph. An example of the requisite additional security functionality is the ability to protect naïve users from clicking on what they believe is a legitimate URL only to introduce some form of malware into the company's IT environment. Providing this protection is complex in part because so many users access Internet based content remotely and hence are not protected by a powerful enterprise firewall. To respond to these challenges, an effective ADN must be able to use a cloud computing approach to check for and evaluate the validity of a URL before establishing a connection to the site.

Another example of the requisite additional security functionality is that an effective ADN must support content filtering to prevent data leaks[4]. An effective ADN must also support intrusion detection and intrusion protection functionality. An intrusion detection system (IDS) passively watches packets transiting the network and sets off an alarm if it finds anything suspicious. A typical intrusion protection system (IPS) has all of the features of an IDS, and in addition it can stop malicious traffic from entering the network.

[2] IM Malware Attacks Increase, http://www.scmagazineus.com/IM-malware-attacks-increase-report/article/109663/
[3] New report predicts massive increase in malware and phishing in 2009, http://www.chutneytech.com/new-report-predicts-massive-increase-in-malware-and-phishing-in-2009/
[4] Improve Data Protection Processes with Content Discovery, Monitoring and Filtering, http://adventuresinsecurity.com/Papers/CMF.pdf

Summary

As recently as a couple of years ago, few IT organizations paid significant attention to application delivery. Now that is a top of mind issue for most IT organizations. When IT organizations first began to pay attention to improving application delivery they focused on the packet delivery network and simply accelerating a few specific applications across the application layer. While that is a reasonable starting point, focusing just on the packet delivery network or singling out a handful of application does not provide the insight into applications that is necessary to enable IT organizations to manage, optimize and control application performance.

Ensuring acceptable application delivery was never an easy task. The task is made more difficult in part by the ongoing emergence of new business requirements such as the ones discussed in this brief. The task is also made more difficult by the fact that the application environment is becoming increasing complex. In order to respond to these challenges and continue to ensure acceptable application delivery, IT organizations must implement an ADN that focuses on the higher level of the OSI protocol stack. The ADN must have the capability, and the IT organization must have established the policies, to cope with the vast and growing variety of applications that traverse the typical enterprise network. For example, as part of supporting business agility, an ADN must be able to identify and control applications such as bulk file transfer to keep those applications from interfering with the performance of applications such as SAP or VoIP. The ADN must be able to recognize You Tube traffic and control or eliminate that traffic as appropriate given the IT organization's policies for the acceptable usage of IT resources. In addition, to support both security and compliance requirements as well as to enable globalization and workforce mobilization, the ADN must also be able to identify malicious traffic and eliminate it.

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.

Webtorials Briefs
Vol 3, Number 1

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com