IT Impact Brief JANUARY 2006 - Issue I

NETFLOW – Gaining Application Awareness

Jim Metzler
Ashton, Metzler & Associates
jim@ashtonmetzler.com

Introduction

In the last IT Impact Brief I listed a set of New Year's resolution. The first of those resolutions was "I will make my network and my network organization more applications aware."

That resolution was very much in line with the June 2005 IT Impact Brief that was entitled "It's the Application Stupid". That brief contained market research that demonstrated that a company's business managers are far more likely to see the value provided by the IT function as coming from applications than coming from the IT infrastructure. Since these are the people that either set or heavily influence the IT budget, we need to recognize how they value IT and respond accordingly.

Fulfilling the resolution of making your network and your network organization more applications aware will take methodical planning. In this regard, one issue that deserves careful attention is the source of management data that IT organizations use. As will be discussed in this brief, there are multiple sources of management data that a company can utilize. For most companies, there is not one source that makes sense in all of their locations. For example, some sources of management data are so inexpensive that it is easy to justify deploying them even in very small offices. However, these sources typically do not provide the same level of information as do some of the more sophisticated sources.

In order to develop a successful strategy for becoming more applications aware, IT organizations need to ensure that the tools that they acquire to analyze applications performance can utilize a wide range of sources for management data. The goal of this IT Impact Brief is to describe some of those sources of management data.

Applications Awareness

For the sake of this IT Impact Brief, a network organization is applications aware if it has a good understanding of the network and how the performance of the network is impacting the company's key applications. A key component of becoming applications aware is the ability to identify the applications that are running on the network. There are many factors that increase the difficulty of identifying the company's applications. One of these factors is that by default all Web-based applications use port 80. That makes it difficult to distinguish a business-critical web-based application from casual web browsing.

A second component of becoming applications aware is the ability to track and report on a wide range of relevant metrics, such as utilization, availability, and response time. It is important that the network operations group have access to these metrics on a real time basis to be able to troubleshoot problems. It is also important that the network engineering group have access to these metrics on a historical basis to be able to perform functions such as capacity planning and network design.

Source of Management Data

Standard SNMP MIB Monitoring

The most elementary management data comes from monitoring the SNMP MIBs (Simple Network Management Protocol Management Information Bases) on network devices such as routers and switches. This data source provides data link layer visibility across the entire enterprise network and captures parameters such as the number of packets sent and received, the number of packets that are discarded, as well as the overall link utilization. This data can be used for a number of functions, such as basic capacity planning; i.e., identifying where bandwidth is either under or over utilized.

NetFlow

NetFlow is a Cisco IOS software feature and also the name of a Cisco protocol for collecting IP traffic information. Within NetFlow, a network flow is defined as a unidirectional sequence of packets between a given source and destination. The branch office router outputs a flow record after it determines that the flow is finished. This record contains information such as timestamps for the flow start and finish time, the volume of traffic in the flow, and its source & destination IP addresses and source and destination port numbers.

NetFlow represents a more advanced source of management data than SNMP MIBs. For example, whereas data from standard SNMP MIB monitoring can be used to quantify overall link utilization, this class of management data can be used to identify which network users or applications are consuming the bandwidth.

Probes

The most sophisticated and complete class of management data comes from probes that are specifically designed to capture detailed application traffic information. These probes provide application visibility and response time metrics from all aspects of the infrastructure and provide insight into a wide range of applications, including well-known applications such as Lotus Notes, as well as complex applications such as SAP and Citrix. Probes overcome the issues that result from port 80 being the default port used by all Web-based applications by providing sophisticated URL (Uniform Resource Locator) filtering of the traffic that transits port 80. Probes can typically expand visibility into non-IP traffic as well, including such protocols as IPX, NetBios, SNA, DECNET and other legacy protocols that may be lurking in your network.

The management data generated by probes can be used for myriad purposes including application monitoring, network monitoring, capacity planning, troubleshooting, fault prevention, service level management, modeling, and billing.

Case Study: A Fortune 500 Bank

To put the issue of data management in a business context, this IT Impact Brief will contain a case study of a bank that is currently in the process of acquiring another bank. Once this acquisition is completed, the bank will be a member of the Fortune 500.

The bank currently operates more than 400 full-service banking offices which will expand to over 500 offices once the acquisition is completed. The bank offers a wide range of services, including commercial, installment and mortgage loans. The bank also provides trust services, insurance services, electronic and online banking services, as well as traditional checking and savings programs.

The bank's IT organization has three primary functional groupings. Those groupings are operations, engineering and architecture. The operations group provides break/fix functionality, while the engineering group evaluates and implements new products, including products to collect management data. The architecture group interfaces with the business units and defines their requirements, along with developing high-level designs. Within the bank's IT organization, it is primarily the operations and engineering groups that use management data in their day to day jobs.

The expectation of the role of the bank's networking organization has changed over the last couple of years. The networking organization is expected to have a deep understanding of the network and how the performance of that network is impacting key applications, whether those applications are based on Citrix or Web services, are custom built, or utilize some combination of these approaches. For example, many of the applications that the bank uses to generate revenues are comprised both of components that are developed internally as well as components that are purchased from a software vendor.

In spite of the expectation that the network organization will play a larger role in managing application performance, the network organization is not able to justify the cost of deploying probes at each of its 500 branch offices. For that reason, the bank makes heavy use of NetFlow in many of its branch offices, which is ideal for traffic across the MPLS WAN that is configured in a meshed design. NetFlow data, with concrete analysis on the applications in use over the WAN, is part of the basis for the bank's ongoing capacity planning decisions.

However, the bank's network organization also makes use of sophisticated probes. One of the uses that the network organization makes of these probes is to monitor some of the complex, custom-built applications that support revenue generation. The network organization has been able to identify these custom applications by using probes and filtering traffic based on factors such as port number or IP address. With probes deployed in strategic, high volume areas of the bank's data centers and headquarters locations, application degradations are quickly identified and resolved to avoid reducing quality of their users's experience over the network. This information has also allowed the network organization to focus their attention on the applications that have the most impact on the bank's revenues.

Conclusions

It is easy to say that all network organizations are under pressure to become more application aware. The difficult part is figuring out how to respond to that pressure.

I feel comfortable saying that becoming application aware will only increase in difficulty over time as new computing models, such as Web services based applications, are added into the mix of what has to be supported and managed. I also feel comfortable saying that over the next few years you will see an increasing number of tools to help you both visualize and control application behavior.

However, as we all know, the first step in any kind of IT management is gathering management data. It would be great if there were one approach to gathering management data that met all requirements. That is not the case now, and that is not going to happen anytime soon. IT organizations will always make a tradeoff between factors such as cost and sophistication. Successful IT organizations realize that these tradeoffs will always exist and build their approach to applications awareness on the assumption that they will be using a variety of sources of management data.