Developing a Plan for Gathering Management Data

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

INTRODUCTION

In the January IT Impact Brief (The Mandate for Packet Flow Data, http://www.netscout.com/docs/itimpactbriefs/NetScout_iib_Metzler_200801_Packet_Flow.pdf) I highlighted my belief that the job of the network manager is changing. In that brief I pointed out that it was not that long ago that the job used to focus entirely on network availability. Today the role of the network manager is much broader and as a result network managers are as likely to spend their time on topics such as application performance as they are to spend their time on purely networking issues.

The expansion of the role of the network manager presents both an opportunity and a challenge. The opportunity is for the network manager to expand his or her skills, add more value to their current company and to increase their marketability both inside and outside their current organization. The challenge is to be successful in the expanded role. That challenge is made more difficult by the fact that

managing application performance is getting significantly more difficult. For example, as discussed in the last IT Impact Brief, applications that are developed using one of the emerging application architectures will be much more difficult to manage than are today's n-tier applications. This includes both Web services based applications and Web 2.0 applications. Web 2.0 applications may be a ways off for many companies, but that is not the case with Web services-based applications. For example, in a survey that we distributed in late 2007, we asked the NetScout community to indicate which business technologies are coming into vogue for 2008 versus going out of style. The technology that came out at the top of the list was Web services.

In an effort to help identify how network managers can be successful with managing application performance, the last brief described how network managers can use flow based analysis to perform tasks such as quantifying overall link utilization and identifying which network users or applications are consuming bandwidth. That brief also pointed out that in order to perform granular troubleshooting of complex IT environments, packet-level details are often necessary.

"...in a survey that we distributed in late 2007, we asked the NetScout community to indicate which business technologies are coming into vogue for 2008 versus going out of style. The technology that came out at the top of the list was Web services."

I want to use this brief to continue to identify how network managers can successfully manage application performance. With that in mind, the goal of this brief is to describe the options that IT organizations have for gathering the management data that will allow the organization to effectively and efficiently troubleshoot a wide range of issues. Those options fall into three general categories: flow collection, distributed monitoring, and continuous capture.

FLOW COLLECTION

IT organizations can typically rely on having access to management data from SNMP MIBs (Management Information Bases) on network devices such as switches and routers. SNMP data, however, does not provide the network manager with information about the applications involved, the servers the data is coming from, or the user to whom the data is being delivered. In addition, SNMP data does not provide any insight into such things as class of service, which is important for QoS management.

To get more granular information, many organizations turn to NetFlow. Within NetFlow, a flow is defined as a unidirectional sequence of packets between a given source and destination. As mentioned, flow-based analysis can be used to perform tasks such as quantifying overall link utilization and identifying which network users or applications are consuming bandwidth. In particular, flow-based analysis contains information that gives the IT organization answers to questions such as:

- Where does the traffic originate? Who's affected?
- What application is involved? Is it one of the critical applications that business managers care about?
- How much traffic has been transmitted?

Because it can provide answers to these questions, NetFlow represents a more advanced source of management data than SNMP MIBs. NetFlow has its limitations. For example, NetFlow does not provide real-time insight into the operations of the network and it only works with IP. While IP is the dominant protocol running on most networks, it is not the only protocol. In addition, while NetFlows supplies data about application usage, it lacks data about application performance. For this, even more granular data, such as is supplied by Cisco's IP Service Level Agreements (IP SLAs) is required. IP SLA, a feature of IOS, is an active traffic monitoring capability, based on synthetic traffic, that collects real-time information about response time, one-way latency, jitter, packet loss, voice quality, and other network statistics.

One common use of IP SLA is to measure performance by sending one or more packets to a Cisco router, using the timestamp information on the packet to calculate actual performance statistics. These measurements can be one-way, or, if the destination router is configured as an IP SLA responder, two-way. IP SLA operation can be scheduled for a particular time, or operated continuously over a time interval. Devices configured for IP SLA operation can trigger SNMP alerts if measurements exceed or fall below a threshold. One of the limitations of IP SLA is that it is only available for a limited number of services. Other limitations of flow collection will be discussed in the next section.

DISTRIBUTED MONITORING

As mentioned, in order to perform granular troubleshooting of complex IT environments packet-level detail is often necessary. For example, if a VoIP call were entering and exiting on different ports, this would cause the quality of the call to degrade and flow-level data would not be able to recognize this mis-configuration.

"...in order to perform granular troubleshooting of complex IT environments, packet-level detail is often necessary."

Packet-based data, such as that provided by distributed monitoring, is needed to identify this type of situation.

Probes are one of the most common devices used for distributed monitoring. By looking at the header and into the payload of the packet when necessary, probes provide the most sophisticated and complete class of management data. This data provides more detailed and granular visibility into the real-time operation of the network than is available with NetFlow. For example, probes provide application visibility and response time metrics from all aspects of the infrastructure and can provide insight into a wide range of applications, including well-known applications such as Lotus Notes, custom-developed applications, peer to peer applications, industry specific applications such as FIX, as well as complex applications such as SAP and Citrix. Probes overcome the issues that I wrote about in a previous IT Impact Brief (The Port 80 Black Hole http://www.netscout.com/docs/itimpactbriefs/NetScout_iib_Metzler_0807_Port_80_Black_Hole.pdf) by providing sophisticated URL (Uniform Resource Locator) filtering of the traffic that transits port 80.

Probes can be deployed either in the LAN or the WAN. The typical LAN probe attaches to the network either by a passive tap or a switch mirror port whereas the typical WAN probe attaches via a passive tap. One of the advantages of using a probe vs. using flow collection is that when probes are used, the IT organization has dedicated monitoring devices focused on that particular task. However, when flow collection is used, the routers and switches have to ration their memory and processing resources between providing flow-level data and transferring the production traffic towards its' destination.

"Probes are one of the most common devices used for distributed monitoring. By looking at the header and into the payload of the packet when necessary, probes provide the most sophisticated and complete class of management data."

Another advantage of using a probe is that probes enable a richer set of reporting functionality than is usually associated with flow collection. For example, the management data generated by probes can be used to generate real-time alarms. This management data can also be exported to other devices for report generation and analysis and used for myriad purposes including application monitoring, network monitoring, capacity planning, troubleshooting, fault prevention, service level management, modeling, and billing.

One of the characteristics of distributed monitoring devices is that they have relatively little storage. As a result, distributed monitoring devices do not capture and store all of the packet data. Instead, they typically only store packet data once a threshold has been reached or the system user launches a data capture manually. Another characteristic is that they often support enhanced functionality that is application specific. For example, a distributed monitoring device might support the capability to monitor VoIP traffic based on a combination of having access to packet level detail combined with a thorough understanding of the requirements of VoIP traffic. This capability is enhanced by the fact that probes also have the ability to monitor converged links with the ability to track data for voice, video (including Telepresence) and data from a single point.

CONTINUOUS CAPTURE

Some continuous capture tools provide simple ongoing packet recording with terabytes of storage, but little analysis capability. However, the more sophisticated solutions combine continuous capture with the distributed monitoring functionality that was described in the previous section. As such, these solutions can store large amounts of data for extended periods of time and that data can be used for tasks such as post-event data mining and network forensics. As such, of the three classes of monitoring options, continuous capture with distributed monitoring capability is the most powerful.

The major advantage of utilizing continuous capture solutions with integrated distributed monitoring capability relates to intermittent troubles. If an IT organization was using a distributed monitoring

solution and there was some form of intermittent problem, the IT organization would typically not have stored enough packet data to identify the cause of the problem. As a result, the IT organization would have to wait until the problem re-occurred. If, however, the IT organization was using a continuous capture solution, the packet data would have been stored and would enable the IT organization to trouble shoot the problem. Because it enables the IT organization to start to troubleshoot the problem immediately, a continuous capture solution tends to lower the MTTR associated with a trouble.

SUMMARY

Managing application performance is a key issue for the NetScout community. Unfortunately, a number of factors are coalescing to make this task notably more difficult. Given this increasing difficulty, network managers will not be able to successfully manage application performance without a detailed plan, and that plan must include how the organization will gather management data.

This brief describes three approaches for gathering management data: flow collection, distributed monitoring and continuous capture. The order in which those approaches were described reflects the level of detail the management data delivered provides in terms of relative sophistication - with continuous capture being the most sophisticated and flow collection the least sophisticated.

As is usually the case with most technical designs, designing a plan to gather management data is a combination of designing the best technological solution for the money. For example, it would be simple to blithely recommend that network managers deploy a continuous capture solution everywhere based on the fact that a continuous capture solution will provide the most functionality to help network managers troubleshoot troubles. However, deploying a continuous capture solution everywhere will also be the most expensive solution. As such, a balance must be struck. For example, consider a hypothetical company that has backbone network that connects its four headquarters facilities, and has twenty major branch offices as well as a number of smaller branch offices. In this case, a reasonable design might be to deploy a continuous capture solution in the four backbone sites, a distributed monitoring solution in the twenty major branch offices and a flow collection solution in the smaller branch offices.

Coming up with a design for capturing management data is only half of the challenge. The other half of the challenge is getting approval and funding for the design. We addressed that challenge in a recent IT Impact Brief (Demonstrating the Value of Performance Management http://www.netscout.com/redirect_pdf/itimpact_0907.asp). As that brief demonstrated, getting approval to implement performance management technologies is a complex, demanding task.

The next IT Impact Brief will continue the discussion of how network managers can successfully manage application performance. That brief will focus on the deployment of more effective processes in general, and the use of ITIL in particular.

NetScout Systems, through its Sniffer and nGenius® solutions, offers large organizations cohesive views into application services delivered over today's complex, global networks, helping IT professionals optimize network and application performance and prevent misuse of critical enterprise resources. Based on granular, packet-flow performance information gathered across the enterprise, NetScout delivers key performance management functions, including application and network monitoring, capacity planning, troubleshooting, and user experience assurance, in a single integrated solution. For more information visit www.netscout.com.