Enhanced Operations Visibility for WAAS Deployments with Cisco NAM

Contents

Introduction

Today's IT environments are built on the simple premise that business success relies on cost-effective application and service delivery. An increasingly distributed workforce has introduced new challenges in IT environments, such as remote branch management, data protection and compliance, and server installation and maintenance. IT departments are consequently realizing the need to centralize applications in the data center. However, application delivery over the WAN to remote sites brings with it the challenges of long latency, bandwidth bottleneck, and packet loss. Cisco® Wide Area Application Services (WAAS) is a comprehensive WAN optimization solution that accelerates applications over the WAN using optimization and compression technologies to provide LAN-like application performance over the WAN. Since WAAS intercepts transactions between clients and servers over the WAN, traditional performance monitoring solutions may be ineffective in such environments. Cisco® Network Analysis Module (NAM) complements WAAS by providing robust performance monitoring and operational manageability by using embedded WAAS instrumentation. Cisco NAM provides a rich set of analytics that identify response times between servers and clients and offer advanced troubleshooting functionality including threshold-based alerts and packet analysis.

Target Audience

This white paper is intended to provide an overview of the Cisco NAM's capability for ongoing performance monitoring and operational management for the Cisco WAAS solution for anyone whose job role involves monitoring, managing, planning, and responding to network performance and quality issues in WAN-optimized networks. Examples of job roles include network architects and engineers, IT architects and engineers, network operators, and performance management and optimization personnel. This white paper complements the Using NAM Reports with Cisco WAAS white paper available at http://www.cisco.com/en/US/prod/collateral/modules/ps2706/white_paper_c11-506458_ps2706_Products_White_Paper.html.

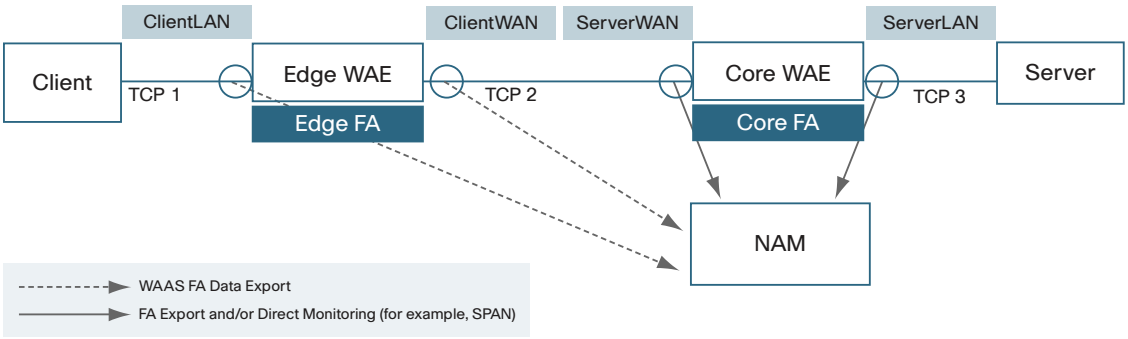
Basic knowledge of Cisco WAAS and Cisco NAM is assumed. Please find more information on Cisco WAAS at http://www.cisco.com/go/waas and on Cisco NAM at http://www.cisco.com/go/nam.

Overview

The Cisco Network Analysis Module family of products improves visibility into network performance to help manage and improve application delivery. Cisco NAM can help improve performance by identifying applications and services that would benefit from Cisco control and optimization mechanisms. Operational efficiency of networks, servers, and applications can be increased with the advanced troubleshooting and management capabilities provided by NAM. Further, performance issues can be pre-empted with threshold-based alerts for more proactive performance management.

Cisco NAM can use a number of data sources to provide performance management capabilities. For WAAS deployments, NAM uses built-in instrumentation on WAAS Acceleration Engine (WAE) devices. The WAAS instrumentation can provide information about the LAN and WAN interfaces of the WAAS products. Using the flow information from WAAS, Cisco NAM offers a rich set of performance analytics such as response time and bandwidth utilization. These performance metrics help in monitoring the impact of optimization on network resource utilization as well as end-user quality of experience. Performance analytics can be collected from various points along the server/client path, thus facilitating reporting on major segments as shown in Figure 1.

Figure 1. WAAS Flow Agent (FA) Data Collected from Various Points Along Server/Client Path



Cisco NAM complements the monitoring and troubleshooting capabilities available from the WAAS Central Manager and WAAS device command-line interface (CLI). NAM adds to the WAAS capabilities through response time analysis for TCP flows, long-term historical reports on top-N flows, as well as detailed packet analysis. Cisco NAM can help in detecting problems proactively and collecting information for troubleshooting before the problem manifests as user complaints, as well as in reactive situations for problem isolation, information gathering, and troubleshooting. Key use cases for ongoing performance monitoring and troubleshooting in a WAN optimized network using NAM's traffic analysis, intelligent application performance, packet capture, and historical reporting capabilities will be highlighted in the following sections.

Use Case 1: NAM for Accelerating Problem Isolation

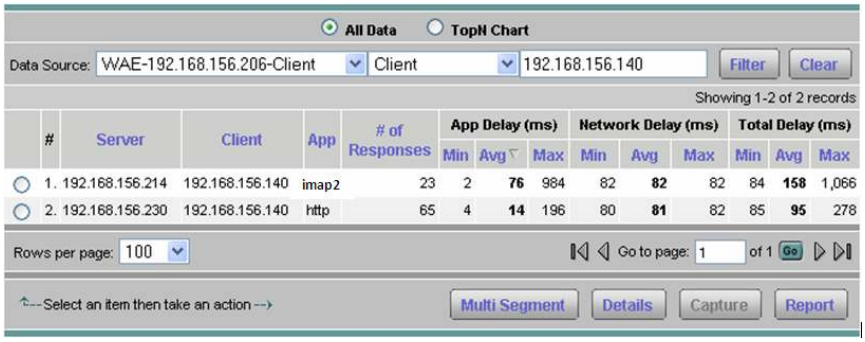
Let us consider the case where a remote user is complaining about slow response time in accessing data center resources. Having a clear problem definition will assist in pinpointing the issue quickly. The following questions can help collect information that is useful in troubleshooting an application response time issue:

1. Is this problem related to a specific application or to all the applications being used (for example, is email access the problem or are other applications affected as well)?
2. Is the problem isolated to the user, or are others in the same site experiencing the same problems?
3. Is the service unavailable, or is it slower than earlier?
4. Since when has the problem persisted?
5. What is the IP address of the client PC and the server resource involved in the problem?
6. What is the traffic mix at the remote branch?

Cisco NAM's real-time and historical traffic analysis and response time analysis capabilities can help shed more light on the information collected through the preceding questions.

Real-time response statistics from the WAE client data source filtered by the client IP address as shown in Figure 2 will provide insights into all the applications the client is accessing and the response time per application. This can be used to answer the first question: Is this problem related to a specific application or to all the applications being used? Similarly, filtering on applications will provide insights into the response time for the same application as experienced by various clients at the same site. This can be used to answer the second question: Is the problem isolated to the user, or are others in the same site experiencing the same problems?

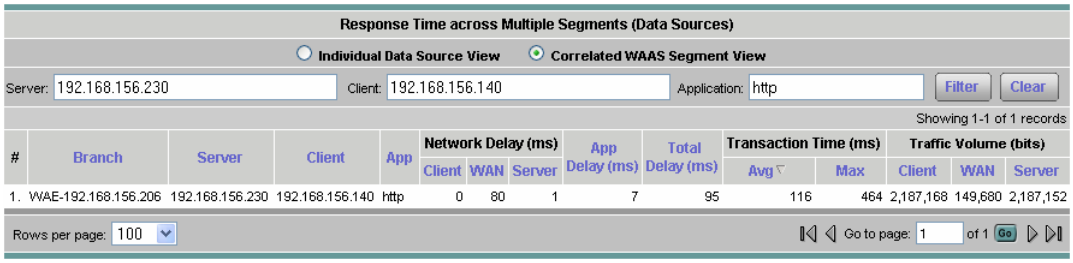
Figure 2. Real-Time Response Time Analytics from the WAE Client Data Source Filtered by Client



Monitor -> Response Time -> Server ->Client Response Time (select appropriate data source)

NAM also offers a correlated response time view from the three WAAS segments as shown in Figure 3. By filtering on the server, client, and application, NAM provides visibility into the network delay and throughput on the client LAN, WAN, and server LAN segments. The application delay, total delay, and average and maximum transaction times are also visible. This can help determine whether the issue is isolated to a particular segment or to the application server.

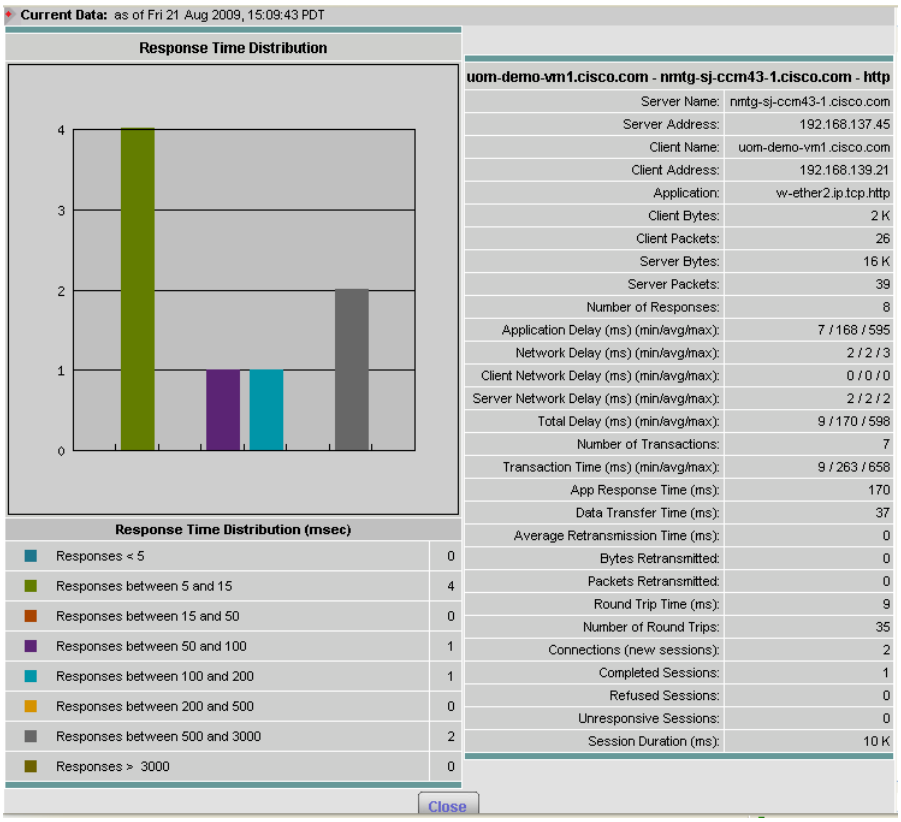
Figure 3. Correlated Response Time Across Multiple WAAS Segments



Monitor -> Response Time -> Server ->Client Response Time (select appropriate data source). Select the conversation and click the Multi-Segment button. Select the Correlated WAAS Segment View radio button in the pop-up window.

Selecting the details of a particular conversation provides details into 45 different response time metrics as shown in Figure 4. Details such as average transaction time, network delay, application delay, retransmission delay, data transfer time, and so on can be analyzed to further narrow down problem areas. For example, a high packet drop and retransmission delay can indicate congestion and other network issues.

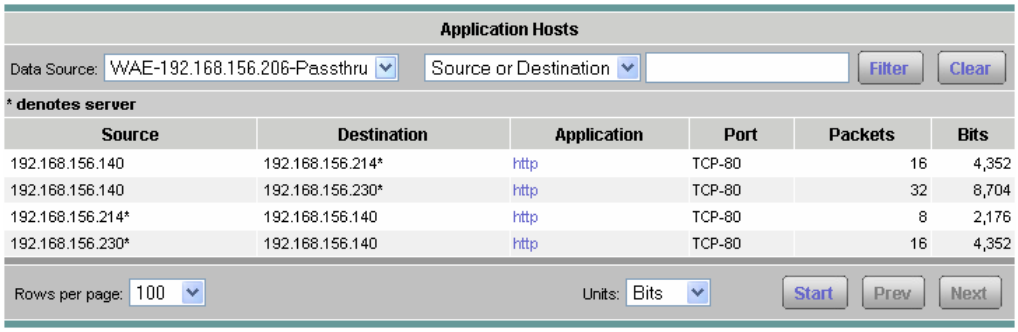
Figure 4. Detailed Response Time Analytics



Monitor -> Response Time -> Server ->Client Response Time (select appropriate data source). Select the conversation and click the Details button.

If the application is not visible in the response time screen for the WAE-optimized flows data sources, we need to find out if the application is not being optimized. This can help add more light to the third question: Is the service unavailable, or is it slower than earlier? The application layer conversations for the WAE pass-through data source for the branch WAE as shown in Figure 5 will provide this information. The WAAS Central Manager can be used to further troubleshoot and verify that the appropriate policies have been applied if unexpected pass-through traffic is seen.

Figure 5. Unoptimized Flows (Pass-Through Traffic) Visibility



Monitor -> Conversations -> Application Hosts (select WAE pass-through data source)

To gain insights into whether the application is slower than earlier and the time when the problem started, preprovisioned historical top-N reports can be viewed. With as low as 15 minutes granularity, the top-N reports can

be preprovisioned for ongoing collection of metrics when the NAM is initially set up. The collected information is stored for a period of 100 days before it is aged out.

The report in Figure 6 can display the top 50 conversations for any 15-minute interval in the past 100 days. By viewing the report for NetFlow, WAE-optimized flows, or pass-through flow records from a remote branch, visibility into traffic flowing to a particular branch can be achieved. This can help answer the fourth question: Since when has the problem persisted? In case the access became unavailable, these historical reports can provide insights into when the flows disappeared.

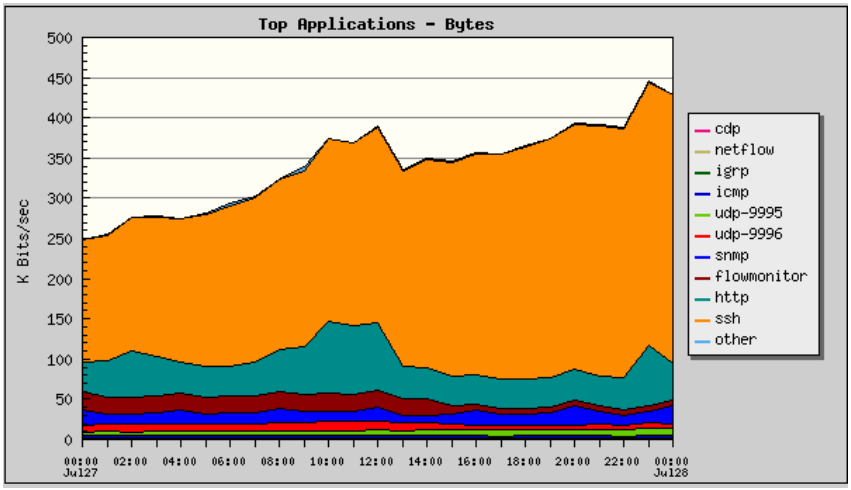
Figure 6. Historical Top-N Application-Level Conversations Report

Time	Top Conversations (AL) - Bytes	bits/sec
19:00 - 19:15	192.168.156.154* - 192.168.156.194 - tcp (tcp 22) 192.168.156.154* - 192.168.156.194 - ssh (tcp 22) 192.168.156.194 - 192.168.156.154* - tcp (tcp 22) 192.168.156.194 - 192.168.156.154* - ssh (tcp 22) 192.168.156.214* - 192.168.156.140 - tcp (tcp 80) 192.168.156.214* - 192.168.156.140 - http (tcp 80) 192.168.156.214 - 192.168.156.156* - udp (udp 9995) 192.168.156.214 - 192.168.156.156* - udp-9995 (udp 9995) 192.168.156.234 - 192.168.156.156* - udp (udp 9996) 192.168.156.234 - 192.168.156.156* - udp-9996 (udp 9996)	1,020,065.17 1,020,065.17 35,459.56 35,459.56 32,087.86 32,087.86 20,933.97 20,858.15 16,291.24 16,291.24
19:15 - 19:30	192.168.156.154* - 192.168.156.194 - tcp (tcp 22) 192.168.156.154* - 192.168.156.194 - ssh (tcp 22) 192.168.156.214* - 192.168.156.140 - tcp (tcp 80) 192.168.156.214* - 192.168.156.140 - http (tcp 80) 192.168.156.194 - 192.168.156.154* - ssh (tcp 22) 192.168.156.194 - 192.168.156.154* - tcp (tcp 22) 192.168.156.214 - 192.168.156.156* - udp (udp 9995) 192.168.156.214 - 192.168.156.156* - udp-9995 (udp 9995) 192.168.156.234 - 192.168.156.156* - udp (udp 9996) 192.168.156.234 - 192.168.156.156* - udp-9996 (udp 9996)	987,943.68 987,943.68 34,381.33 34,381.33 34,328.00 34,328.00 20,937.44 20,861.62 16,407.08 16,398.24

Reports -> Basic Reports -> Select the report and fine-tune the viewing granularity (the report must be preprovisioned)

The top applications report in Figure 7 can also be used to check whether particular critical application traffic reduced significantly or stopped after a particular time. This can also be used to answer the sixth question: What is the traffic mix at the remote branch?

Figure 7. Historical Top-N Applications Report



Reports -> Basic Reports -> Select the report and fine-tune the viewing selections (the report must be preprovisioned)

The top-N response time report in Figure 8 can show whether there was a significant increase in response time for applications during any 15-minute interval in the past 100 days. Further, creating reports for network delay and application delay will provide insights into whether the network or the application is the cause of the delay.

Figure 8. Historical Top-N Average Transaction Time Report

Time	Top Client/Server - Avg Transaction	avg transaction
22:00 - 22:15	192.168.156.214-192.168.156.140-4 1000001 800 6 50 0 1 0 0 192.168.156.230-192.168.156.140-4 1000001 800 6 50 0 1 0 0	165.00 113.00
22:15 - 22:30	192.168.156.214-192.168.156.140-4 1000001 800 6 50 0 1 0 0 192.168.156.230-192.168.156.140-4 1000001 800 6 50 0 1 0 0	165.00 123.00
22:30 - 22:45	192.168.156.214-192.168.156.140-4 1000001 800 6 50 0 1 0 0 192.168.156.230-192.168.156.140-4 1000001 800 6 50 0 1 0 0	166.00 131.00
22:45 - 23:00	192.168.156.214-192.168.156.140-4 1000001 800 6 50 0 1 0 0 192.168.156.230-192.168.156.140-4 1000001 800 6 50 0 1 0 0	174.00 121.00

Reports -> Basic Reports -> Select the report and fine-tune the viewing granularity (the report must be preprovisioned)

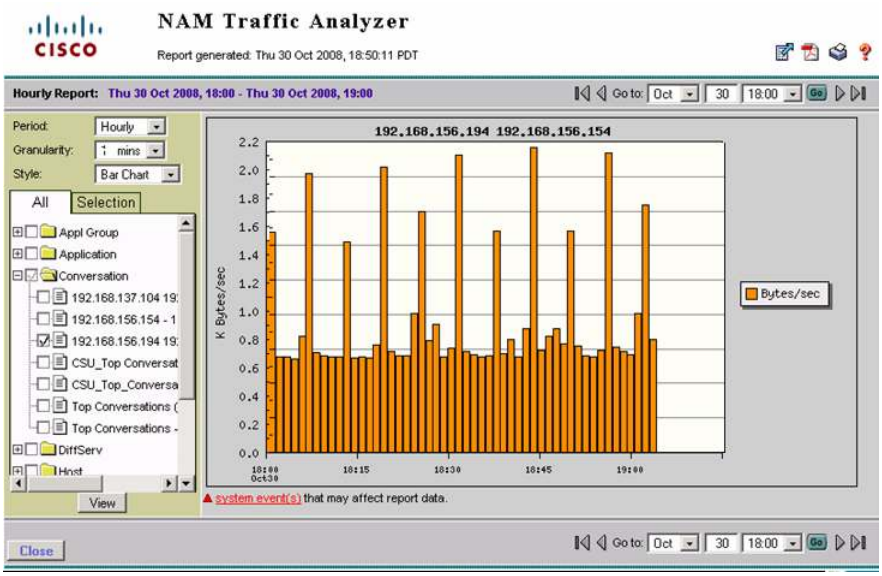
As seen in the preceding examples, real-time statistics and historical reports can help in narrowing down the problem areas and isolating the problem in conjunction with information available through the WAAS Central Manager.

Use Case 2: NAM for Reactive Troubleshooting of Cisco WAAS

Once a problem has been isolated to a particular user or branch or application, we may want to monitor that particular entity in greater detail and granularity to further isolate the root cause of the problem. NAM offers the ability to provision detailed trending reports on specific metrics with a granularity of one minute. These reports can also be merged to get relative trending information, which can be valuable in troubleshooting.

In Figure 9, the rate of traffic for a particular conversation is analyzed with one-minute granularity. This can help identify unusual patterns in traffic flow and pinpoint the time period when a connection was dropped, for example. This can be correlated later with other network or application server events.

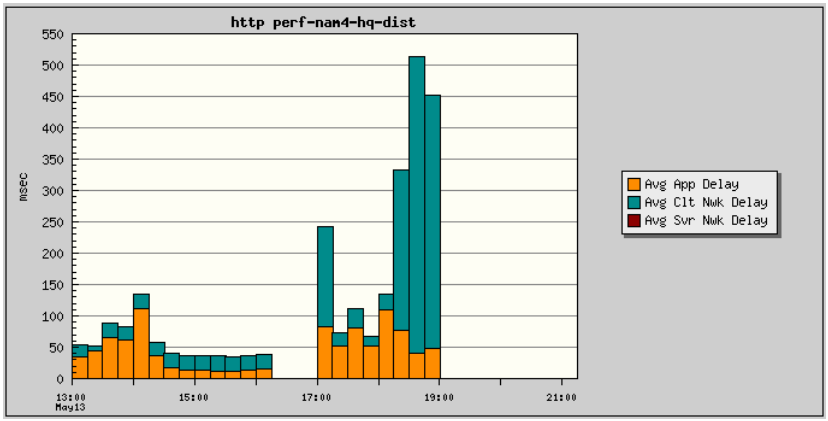
Figure 9. Granular Historical Conversation Traffic Rate Report



Reports -> Basic Reports -> Select the report (the report must be provisioned for troubleshooting)

In Figure 10, the average application delay, average client network delay, and average server network delay reports have been combined for the same conversation as seen from a particular data source. This provides valuable insights; for example, in this case, the client network delay, which used to be around 25 millisecond, began to rise to almost 400 millisecond before the connection died down. This might point to some severe congestion or hardware failure downstream from the NAM. Similarly, correlating multiple metrics for the same conversation provides valuable insights.

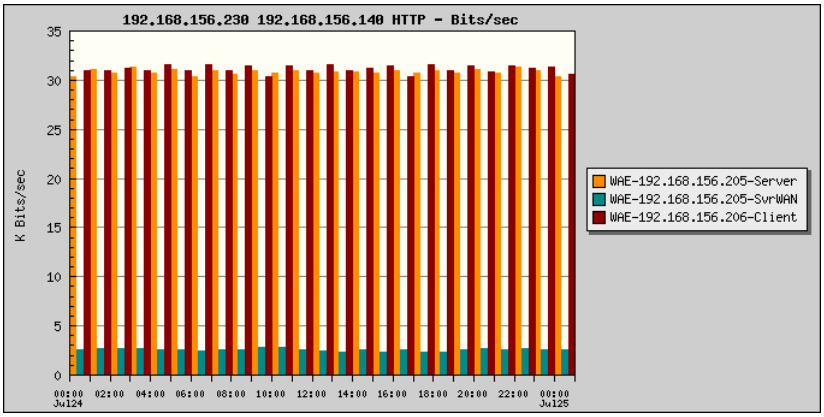
Figure 10. Combined Historical Report for Avg. App. Delay, Avg. Clt. Nwk. Delay, and Avg. Svr. Nwk. Delay



Reports -> Basic Reports -> Select relevant reports -> View (the report must be provisioned for troubleshooting)

Figure 11 shows the throughput in the three WAAS segments for a particular conversation. This provides valuable insights into ongoing improvements observed due to Data Redundancy Elimination (DRE) and compression. If the throughput on the WAN suddenly increases while the throughput on the LAN segments remains unchanged, the WAAS optimization policies can be examined to check for any changes or misconfigurations.

Figure 11. Combined Historical Report for Conversation Traffic Rate for WAE Client, WAE WAN, and WAE Server Data Sources



Reports -> Basic Reports -> Select relevant reports -> View (the report must be provisioned for troubleshooting)

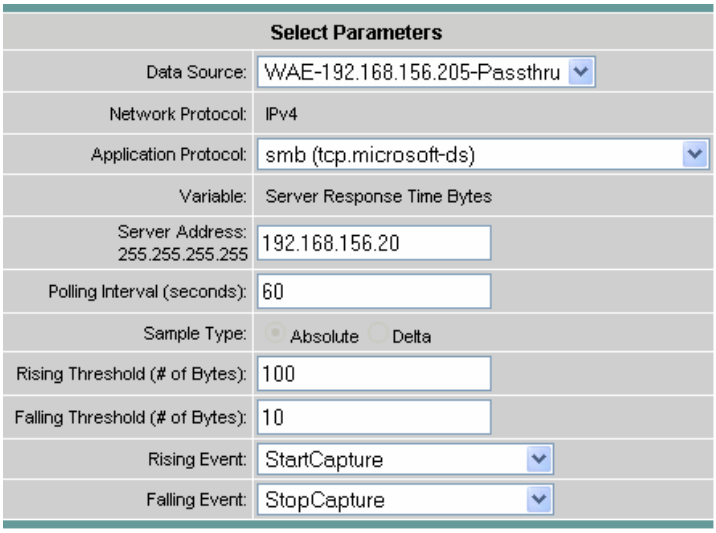
As shown in the preceding examples, reports with one-minute granularity for various metrics for specific clients, servers, and applications can be created and combined to aid in troubleshooting. Further, the real-time response time statistics can also be observed during troubleshooting for added insights.

Use Case 3: Detect Problems Proactively Before Users Complain

As we have seen in earlier use cases, NAM offers a rich set of real-time traffic and response time analytics. We have also seen how historical reports can provide insights into the trending of these metrics over a period of 100 days. The NAM also provides for proactive performance monitoring, by setting up thresholds for the key performance indicators for business-critical applications. Alarms can be raised when these thresholds are exceeded and various actions can be taken such as sending email, syslog messages, and Simple Network Management Protocol (SNMP) traps. Further, packet capture can be triggered when a threshold is exceeded, making it possible to conduct a more detailed analysis of the traffic when the problem occurs.

In Figure 12, we are setting up an alarm threshold to trigger packet capture when the pass-through traffic for the SMB application increases at a particular branch. This will help us identify cases when there is an issue with WAN optimization policies applied on the WAAS device.

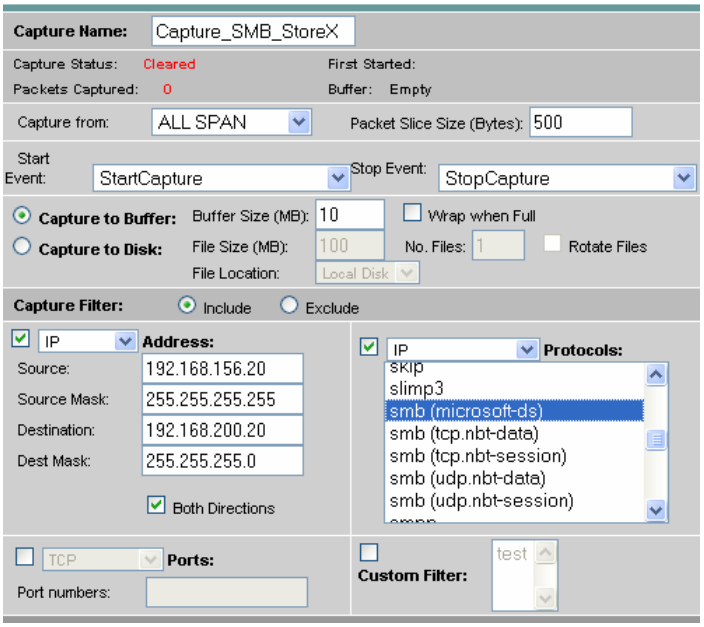
Figure 12. Alarm Threshold Setup



Setup -> Alarms -> Alarm Thresholds -> Create -> Server Response Time Bytes

In Figure 13, we configure the packet capture session from the Switched Port Analyzer (SPAN) data source in the data center to capture all SMB traffic going to the particular branch for which the alarm threshold was created. Setting up the capture session when the alarm threshold is set up will facilitate proactive troubleshooting when the issue surfaces. Capture filters are utilized to filter packets for the particular server, application, and branch subnet.

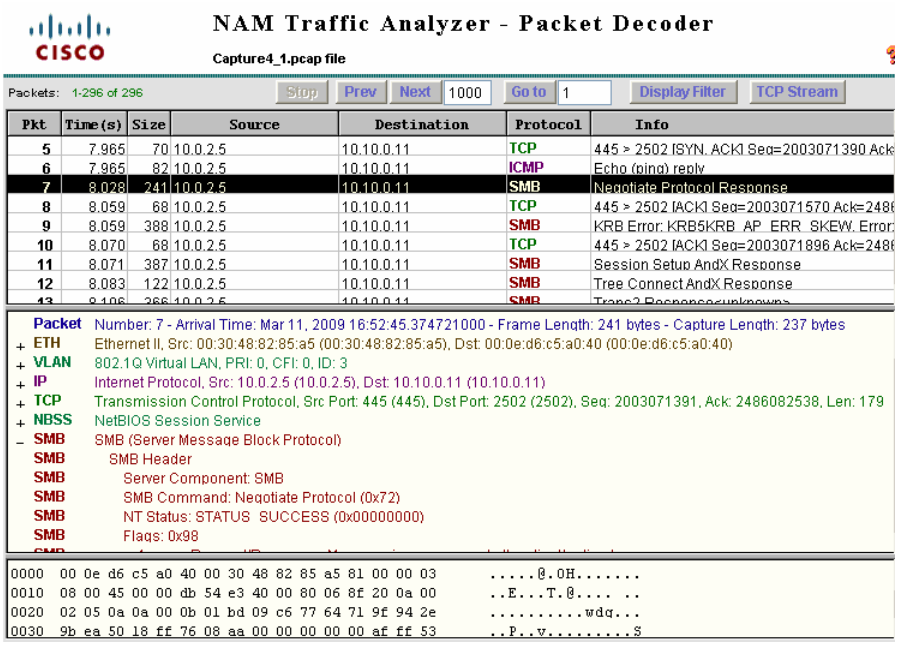
Figure 13. Triggered Packet Capture Setup



Capture -> Buffers -> New Capture

The captured packets can be decoded and analyzed on the NAM itself for more efficient problem isolation as shown in Figure 14.

Figure 14. Packet Capture Decode



Capture -> Buffers -> Select a buffer -> Decode

By combining the rich traffic and response time analytics provided by Cisco NAM with advanced threshold-based packet capture and decode, IT departments can take a proactive approach toward detecting performance issues before they affect end-user experience.

Use Case 4: NAM Helps Fine-Tune WAAS Optimization Policies

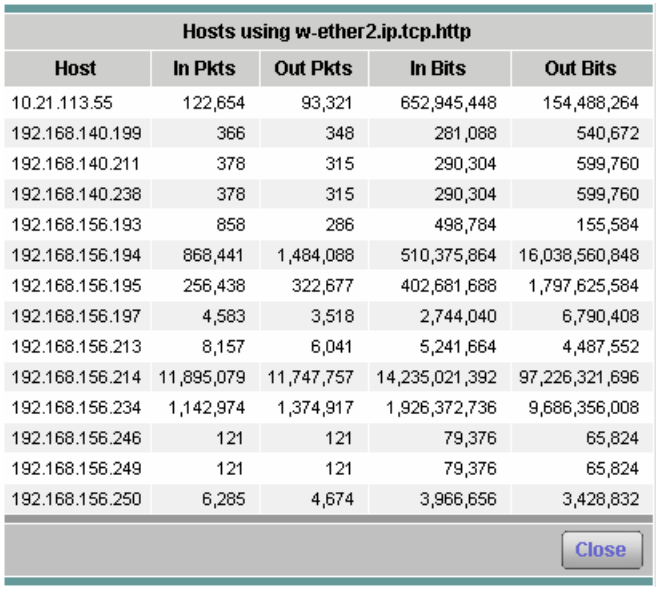
Once WAAS is deployed, NAM can monitor critical servers in the network to provide visibility into connections to those servers, such as whether the connections are optimized or pass-through. Further, NAM can also monitor NetFlow data from a remote branch router to view the traffic flow to that particular branch.

WAAS has default classifiers. For certain customized applications on certain servers, specific policies may be applied. There may be cases where the same customized application may also be hosted on other servers that are not getting classified appropriately and hence not getting optimized. A combination of NAM's NetFlow reporting and WAAS monitoring can help identify such situations. This information can be used to fine-tune the application classifiers and the policies applied.

The top talkers by protocol and port number shown in Figure 6 can be used to cross-check with the WAAS Central Manager. If certain applications and hosts are not included in the default WAAS policy, classifiers can be added for these.

Additionally, in Figure 15, we are reviewing all the hosts using a particular application as reported by NetFlow. The hosts that list a greater out bits value compared to in bits would indicate the servers. These servers can be added as monitored servers for WAAS monitoring in the NAM (Setup -> Data Sources -> WAAS -> Monitored Servers).

Figure 15. Hosts Using a Particular Application



Hosts using w-ether2.ip.tcp.http

Host	In Pkts	Out Pkts	In Bits	Out Bits
10.21.113.55	122,654	93,321	652,945,448	154,488,264
192.168.140.199	366	348	281,088	540,672
192.168.140.211	378	315	290,304	599,760
192.168.140.238	378	315	290,304	599,760
192.168.156.193	858	286	498,784	155,584
192.168.156.194	868,441	1,484,088	510,375,864	16,038,560,848
192.168.156.195	256,438	322,677	402,681,688	1,797,625,584
192.168.156.197	4,583	3,518	2,744,040	6,790,408
192.168.156.213	8,157	6,041	5,241,664	4,487,552
192.168.156.214	11,895,079	11,747,757	14,235,021,392	97,226,321,696
192.168.156.234	1,142,974	1,374,917	1,926,372,736	9,686,356,008
192.168.156.246	121	121	79,376	65,824
192.168.156.249	121	121	79,376	65,824
192.168.156.250	6,285	4,674	3,966,656	3,428,832

Close

Monitor -> Apps -> (Select application) -> Details

We can now look at the pass-through flows and check whether the application appears under pass-through and the hosts that are not getting optimized. This information can then be used to update the classifiers in WAAS.

Summary

Cisco NAM offers operational management for the Cisco WAAS solution by using embedded instrumentation on the WAAS devices. In addition to analyzing the flow information received from the WAAS devices, Cisco NAM uses other data sources such as SPAN and NetFlow to provide more detailed traffic analysis and troubleshooting capabilities. Cisco NAM facilitates ongoing management by IT departments of their WAN-optimized networks by providing a rich set of analytics for real-time monitoring, historical trending, and threshold-based proactive troubleshooting. The operational management capabilities in the NAM complement those in the WAAS Central Manager to provide a rich set of tools and in-depth visibility for ongoing management of the WAAS deployment.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-554563-00 10/09