Using Cisco NAM Reporting with Cisco WAAS

White Paper

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Contents

1. Summary **4**
1.1 Scope 4
1.2 Target Audience 4
1.3 Supported Product Releases 4
1.4 Partner Reporting 4

2. Overview **4**
2.1 NAM Presentation of WAAS Data 4

3. WAAS deployment steps **6**
3.1 Identify Applications 7
3.2 Determining acceptable application performance 10
3.3 Find problematic sites and applications 13
3.4 Short-list candidate sites and applications 14
3.5 Install WAAS + NAM 14
3.6 Analyze impact 15
3.7 Monitor and Troubleshoot 18

4. Deployment Considerations **18**

5. Terms and Acronyms **19**

6. Related Documents **19**

7. Appendix A -- Reporting Configuration Details **19**
7.1 Configuring the Data Center NAM 19
7.2 Configuring the Cisco Branch NAM 21
7.3 Configuring WAAS -- NAM Integration 22

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's publicdomain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

User Guide for the Cisco Network Analysis Module Traffic Analyzer, 4.0

© 2009 Cisco Systems, Inc. All rights reserved.

1. Summary

1.1 Scope

This document describe the NAM 4.0 reports that can be leveraged for WAAS deployments. The following topics are not addressed in this document:

- Post-4.0 new reporting
- Partner solutions leveraging NAM reporting

1.2 Target Audience

This whitepaper is intended for the use of Cisco NAM and Cisco WAAS field. Readers are assumed to be generally familiar with NAM and WAAS functionality.

1.3 Supported Product Releases

This document describes the functionality of the following releases

- NAM 4.0/NAM 4.1
- WAAS 4.0/WAAS 4.1

1.4 Partner Reporting

It is possible to combine NAM with partner reporting solutions. In these case customers can leverage an integrated solution for the best combination of deployment flexibility, scalability, high-end reporting and troubleshooting capabilities.

This document provides NAM local reporting that could be available when partner solutions are not implemented or when a drill-down option from the partner solutions to NAM is supported.

2. Overview

The following section will serve as introduction to how NAM presents the information coming from WAAS

2.1 NAM Presentation of WAAS Data

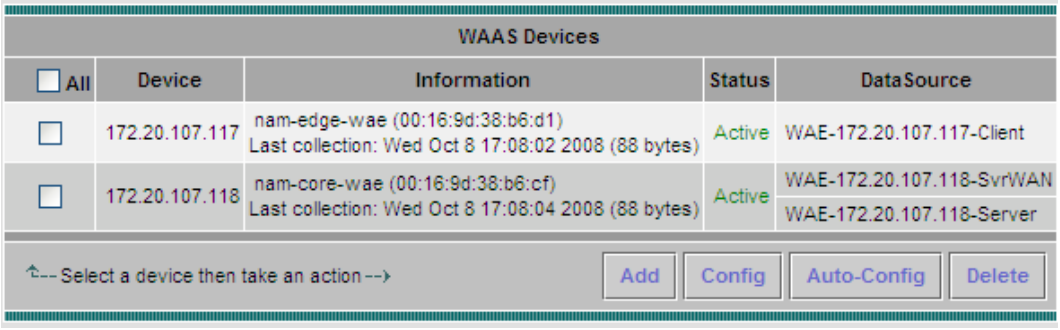
WAE Flow-Agent (aka FA) is an embedded part of WAAS software, running on WAE, which provides information about packet streams of interest traversing through both LAN and WAN interfaces of WAAS WAEs. Traffic of interest can include specific servers and type of transaction to be exported.

NAM processes the data received from FAs and derives application performance analytics and reports (branded IAP -- Intelligent Application Performance).

NAM GUI can be used to create WAAS data sources to handle WAAS FA data (see Figure 1). In addition to IAP, NAM monitors and reports on other traffic statistics derived from FA data sources including applications, hosts & conversations.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

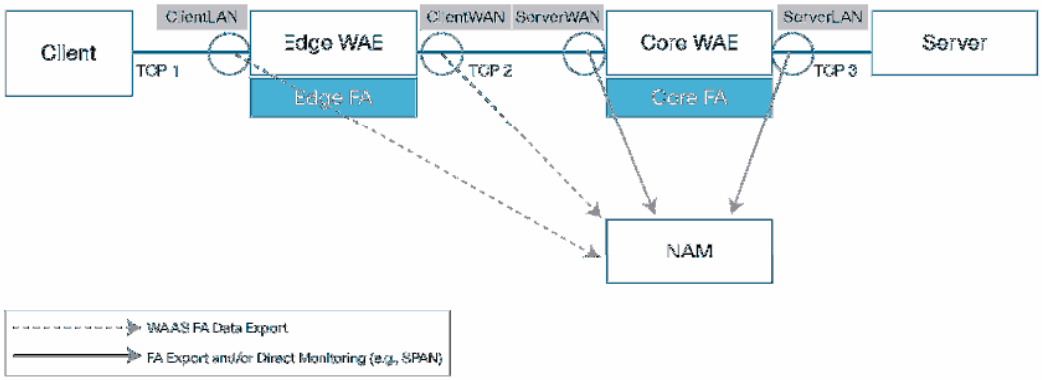
Figure 1. NAM WAAS Device configuration



NAM provides various IAP metrics by collecting data at different points of the packet path. Figure 2 shows an example of the data collection points.

Note that Figure 2 addresses the typical scenarios. For additional information about collection points from WAAS please refer to the product documentation.

Figure 2. Edge-Client to Data-Center-Server example



Understanding the different WAE data-source types

Figure 2 provides an example of available, FA-based, NAM data sources (see the text with grey background representing the data sources). Those are the data sources that are relevant when reporting on transactions between a client located in the branch to a server located in the Data Center.

The following data-sources can be configured per WAE device

- **Client LAN (aka Client):** traffic initiated by the LAN side of the WAE (initiation can be the first packet out from the client like a “SYN”)
- **Client WAN:** traffic initiated by the LAN side of the WAE as is seen on the WAN link
- **Server WAN:** traffic initiated by the WAN side of the WAE as is seen on the WAN link
- **Server LAN (aka Server):** traffic initiated from the WAN side of the WAE
- **WAAS Pass Through:** Traffic that traverses WAAS without being optimized (available in NAM 4.1)

Each FA data-source can be viewed as a specific probing point in the network.

Monitoring Client Segment

A TCP segment is defined from initiation of the TCP transaction to its termination. WAAS breaks down TCP traffic into 3 legs that are shown as TCP-1 through 3 in Figure 2. By monitoring the TCP legs between the clients and the WAAS edge device (TCP-1 segment in Figure 2), you can measure the following IAP metrics:

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

- Total Delay (TD) as experienced by the client
- Total Transaction Time as experienced by the client
- Bandwidth usage (bytes/packets) before optimization
- Number of transactions and connections.
- Network RTT broken down into two segment: client-edge and edge-server

This segment can be represented by “Client” data-source.

Monitoring WAN Segment

By monitoring the spoofed TCP legs between the edge and core WAAS devices (“TCP-2” segment in Figure 2) one can measure the bandwidth usage (bytes/packets) after optimization as well as the network round-trip time. This segment can be represented by “Client-WAN” and “Server-WAN” data-sources.

Monitoring Server Segment

By monitoring the TCP legs between the core WAAS devices and the servers (“TCP-3” segment in Figure 2), one can measure the following IAP metrics:

- Application (Server) Delay (without proxy acceleration/caching server)
- Network RTT between the core WAAS device and the servers

This segment can be represented by “Server” data-source.

For additional information about the way the metrics are defined, please refer to NAM User Guide (Monitoring Response Time section).

Monitoring Pass-Through traffic

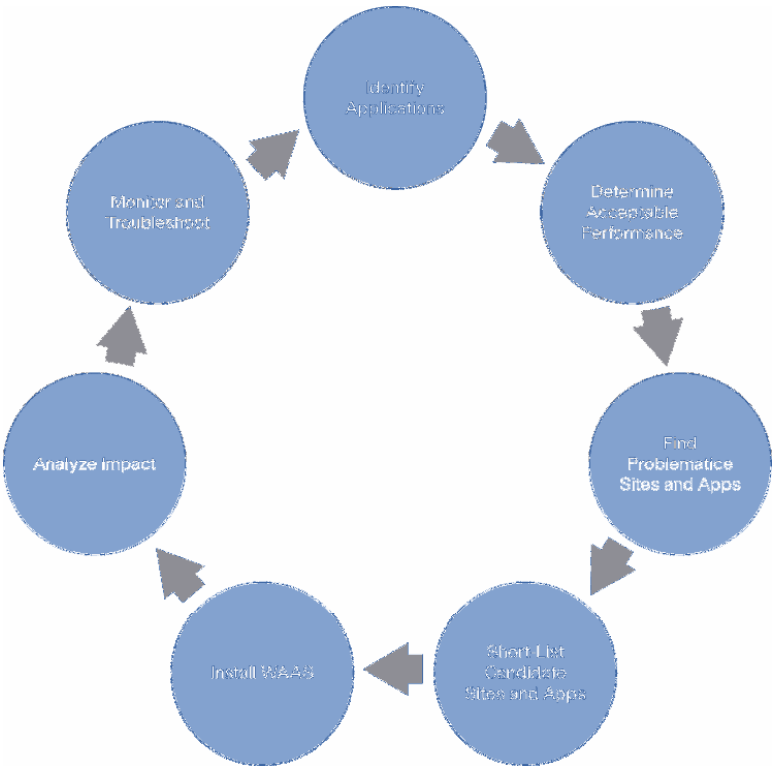
Monitoring Pass-Through traffic may help uncover policy misconfiguration, resource issues and help with before/after impact assessment

3. WAAS deployment steps

A typical WAAS deployment process consists of the following steps:

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 3. WAAS Deployment Life Cycle



1. **Identify applications:** Identify the customer business-critical applications
2. **Determine acceptable performance:** Assess and/or baseline to determine the acceptable performance
3. **Find problematic sites and applications:** Find sites, applications and time periods with unsatisfactory performance
4. **Short-list candidate sites and applications:** Short-list the ones WAAS is believed to have most impact on
5. **Install WAAS:** Install WAAS and configure the solution to enable performance analysis
6. **Analyze impact:** Perform WAAS solution impact analysis
7. **Monitor & Troubleshoot:** Keep on-going track of network performance and address performance issues

The following sections provide more information about each of the above steps.

3.1 Identify Applications

What are we trying to achieve?

In this step we are trying to find the applications that the customer should track for his business critical transactions. The applications we find can be used in the following steps for analysis and potential optimization.

How do we achieve that?

Typically, customers determine which applications are critical to their business. If the list of the important applications and servers is already known the user can skip this step.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

NAM can help identify those applications by providing application reports. These can be leveraged to assess the possible impact of WAAS since optimization ratio are application traffic dependent.

SPAN, NetFlow or any of the traditional NAM data sources can be used for the initial assessment when WAE FA traffic is not yet present.

Possible activities:

- Confirm NAM configuration (data sources, monitoring and response time collection enabled)
- Confirm WAAS configuration (FA directing traffic to NAM)
- Look at the most active applications
- Look at the most active servers
- Determine the ones that you would like to track

Useful reports

The following short-term reports can be used to provide application information:

- Most active applications & Servers (Figure 4)
- Detailed application & server breakdown (Figure 5, Figure 6, Figure 7)

The following mid-term reports (up to 100 days) can be used to provide application information:

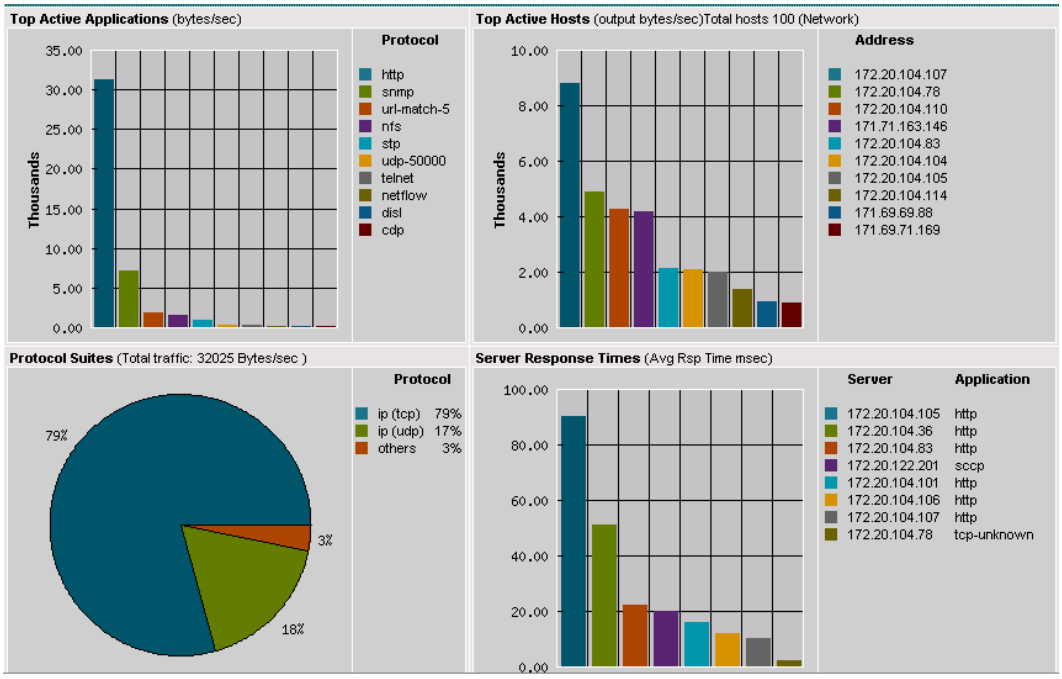
- Breakdown of top applications over time (Figure 8)

Mid-term reports can validate assumptions about the typical acceptable traffic behavior over time. Applications can be grouped together. An example can be to group under “Web” the following:

- “Browsing to XM radio services”, “Browsing to walled garden”, “HTTP generic” and “HTTPS”

Reports can show the cumulative traffic, charts and throughput per group as well as the contribution of each application in the group. Reporting views include real-time, short- and mid-term. Figure 9 illustrates the way applications can be aggregated.

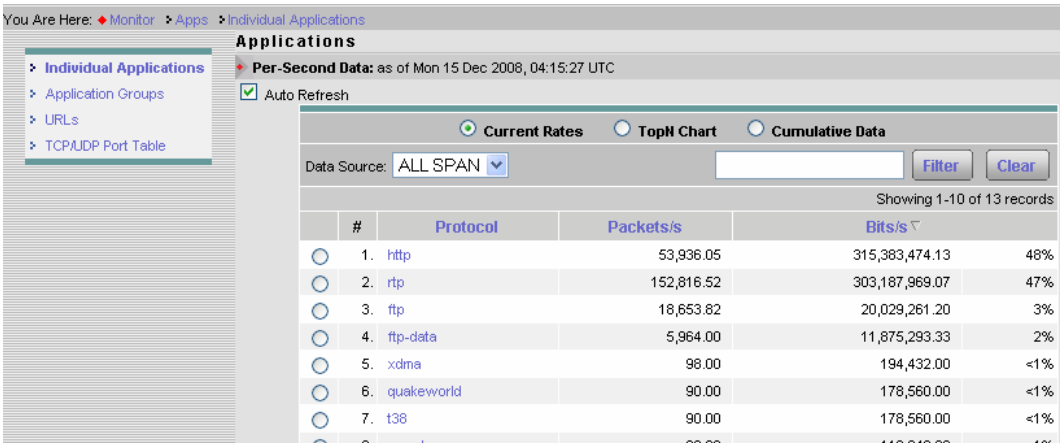
Figure 4. Overview of applications, hosts, protocols and server performance



© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

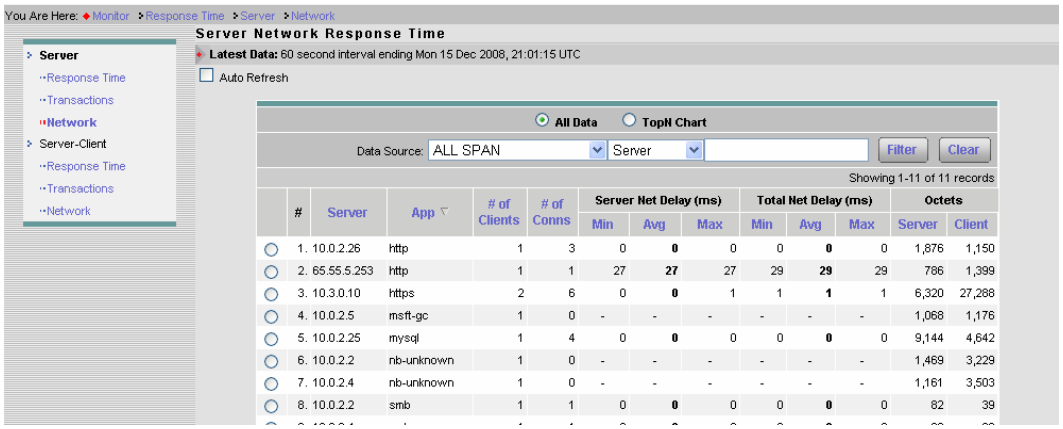
Select Monitor -> Overview.

Figure 5. Application View



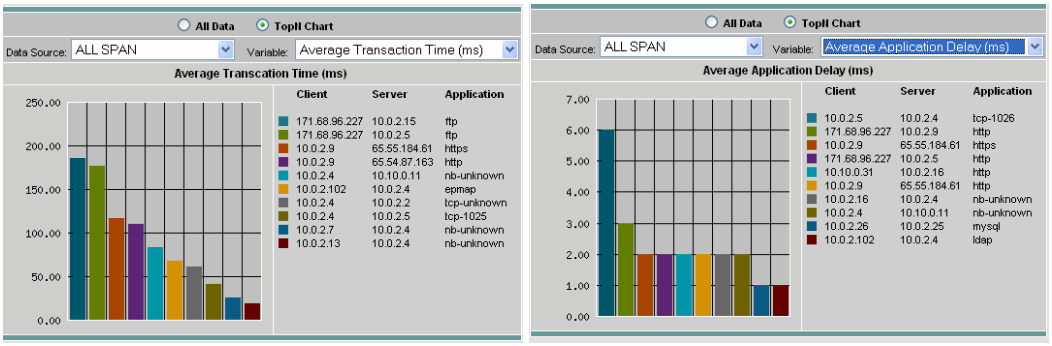
Select Monitor -> Apps.

Figure 6. Network responsiveness of servers



Select Monitor -> Response Time -> Server -> Network.

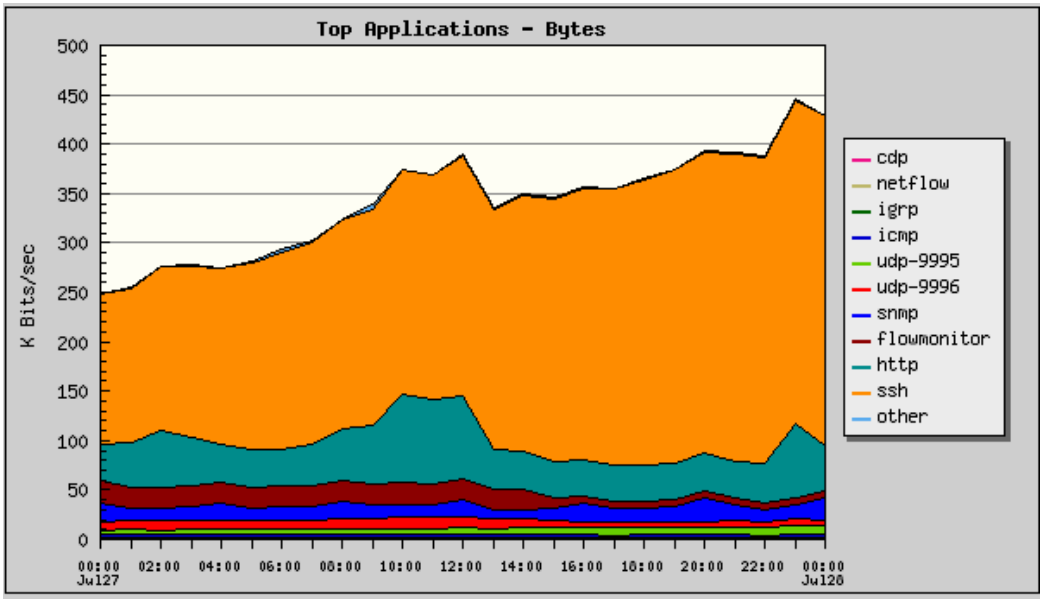
Figure 7. Top N Response Time Charts



Select Monitor -> Response Time -> Transactions -> TopN Chart.

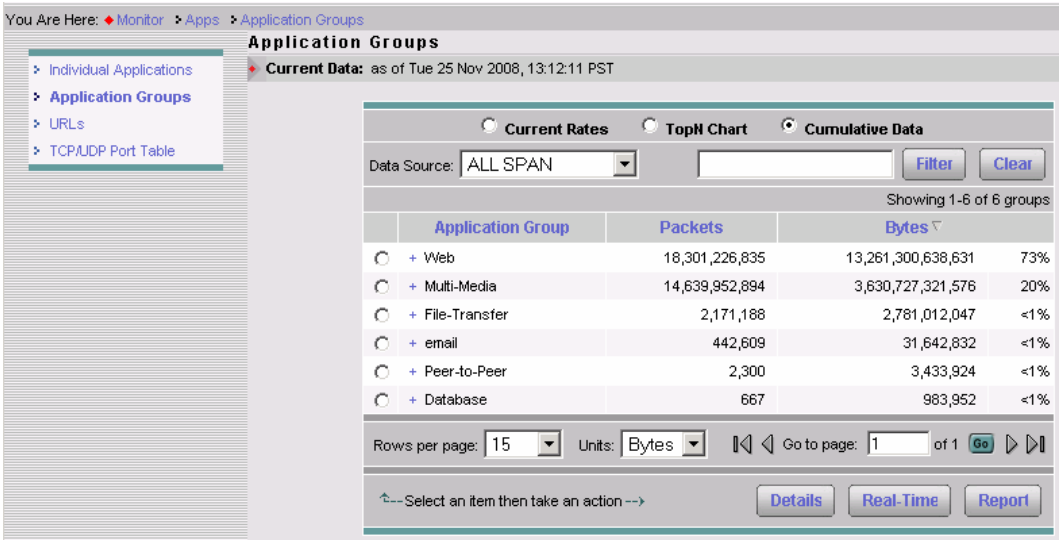
© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 8. Top N applications reports (by traffic volume)



Select Reports -> Basic Reports -> Top Applications -- Bytes.

Figure 9. Application Groups



Select Monitor -> Apps -> Application Groups -> Cumulative Data (radio button).

3.2 Determining acceptable application performance

What are we trying to achieve?

After understanding the various applications of interest, we would like to quantitatively determine the acceptable performance level for these applications.

How do we achieve that?

The user may already have a good understanding of the performance values he would like to see per application. An example can be that he determines that latency up to 200 ms for Citrix is acceptable. In this case this step can be skipped.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

NAM short-term and historical reports on application bandwidth usage and response time can help users to identify their baseline. This assumes that the users will make measurements of timeframes during which the end-users are satisfied with the level of the applications performance.

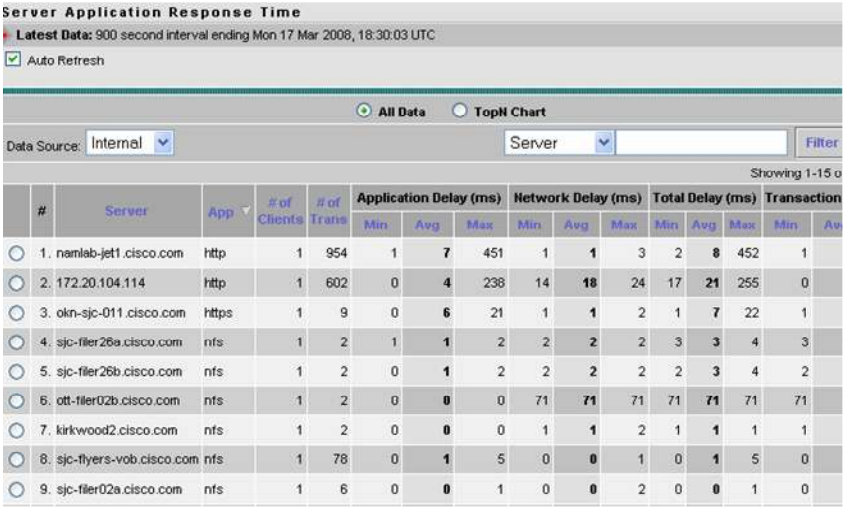
Possible activities:

- During a busy time period examine the performance values of applications of interest while users by looking at short-term response time reports
- Track specific combination of application and server or application, host and server to better understand the performance values over time

Useful reports

Figure 10 shows server transaction latency in short-term. Server view taken from SPAN data source can represent the aggregate site performance (like Data Center aggregate view assuming SPAN is taken in the Data Center, or from Pass-Through data source in case of NAM VB) when accessing a particular server and application. Using this report (and/or historical reports of the servers of interest) the performance can be determined. As an example, maximum values of response time may indicate the issues that correspond to the worse performing sites.

Figure 10. Application Response Time



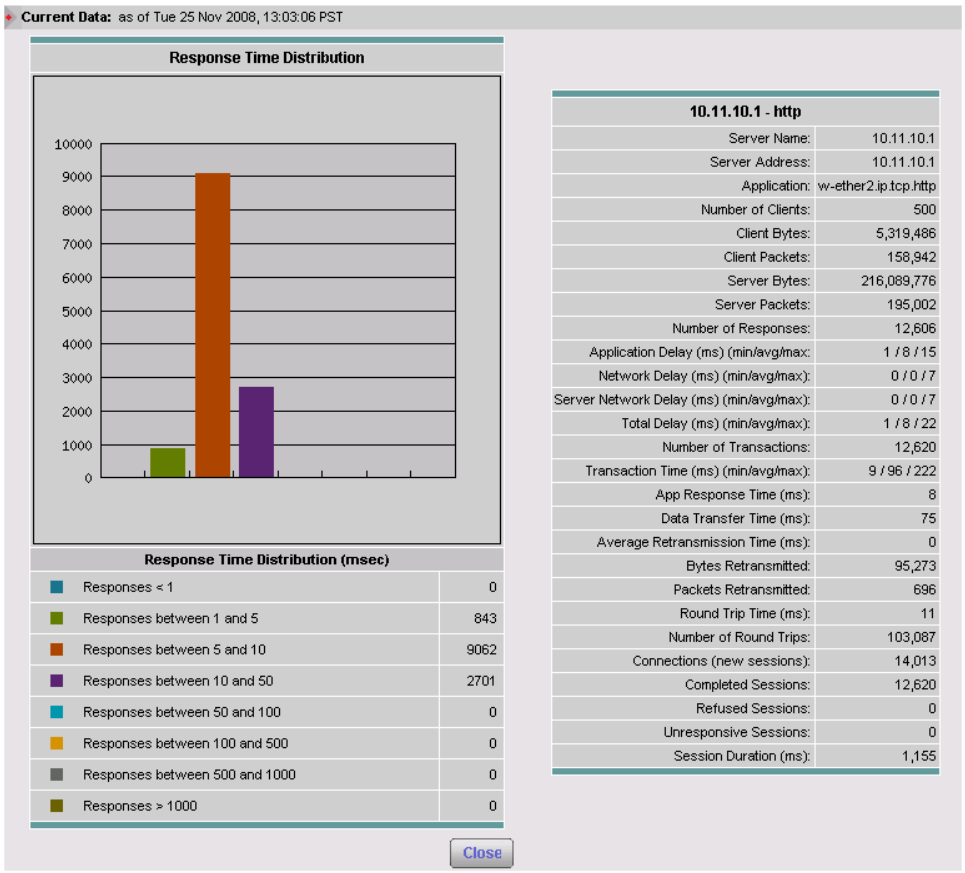
	#	Server	App	# of Clients	# of Trans	Application Delay (ms)			Network Delay (ms)			Total Delay (ms)			Transaction	
						Min	Avg	Max	Min	Avg	Max	Min	Avg	Max	Min	Av
○	1.	namlab-jet1.cisco.com	http	1	954	1	7	451	1	1	3	2	8	452	1	
○	2.	172.20.104.114	http	1	602	0	4	238	14	18	24	17	21	255	0	
○	3.	okn-sjc-011.cisco.com	https	1	9	0	6	21	1	1	2	1	7	22	1	
○	4.	sjc-filer26a.cisco.com	nfs	1	2	1	1	2	2	2	2	3	3	4	3	
○	5.	sjc-filer26b.cisco.com	nfs	1	2	0	1	2	2	2	2	2	3	4	2	
○	6.	ott-filer02b.cisco.com	nfs	1	2	0	0	0	71	71	71	71	71	71	71	
○	7.	kirkwood2.cisco.com	nfs	1	2	0	0	0	1	1	2	1	1	1	1	
○	8.	sjc-flyers-vob.cisco.com	nfs	1	78	0	1	5	0	0	1	0	1	5	0	
○	9.	sjc-filer02a.cisco.com	nfs	1	6	0	0	1	0	0	2	0	0	1	0	

Select Monitor -> Response Time -> Server Response Time.

The response time distribution is be shown in Figure 11. User experience data can be obtained from reports like Client/Server response time (Figure 12). As an example, if Network Delay has the largest values by far, it could suggest a network configuration issue, as opposed to a server capacity issue.

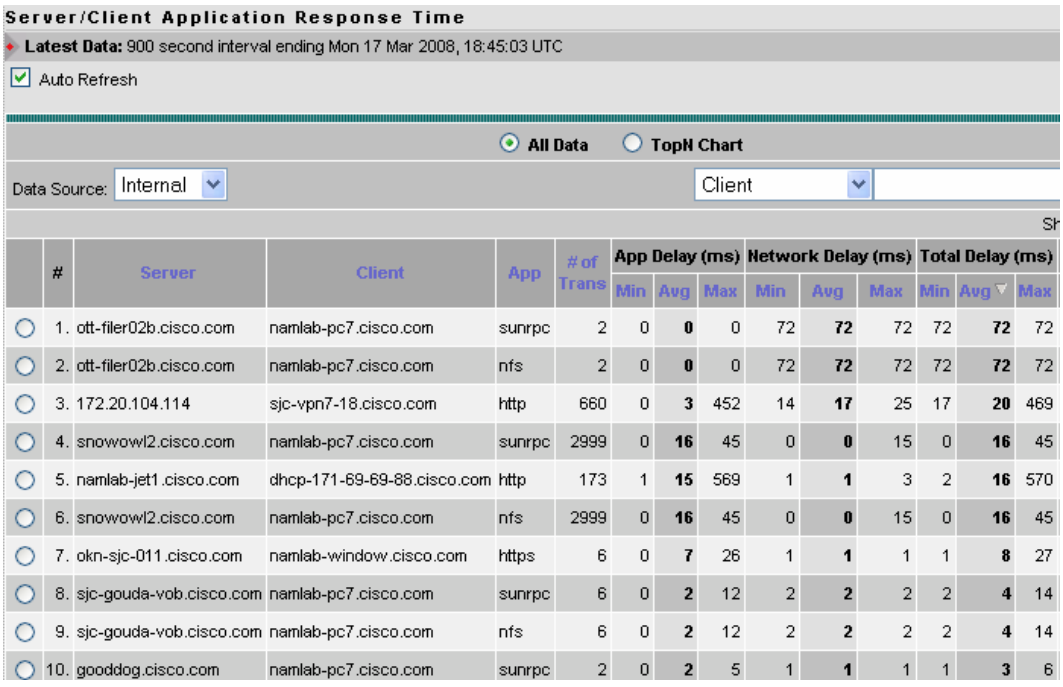
© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 11. Server details



Select a particular Server in the Monitor -> Response Time screen and click the Details button.

Figure 12. Client-Server Response Time



	#	Server	Client	App	# of Trans	App Delay (ms) Min	App Delay (ms) Avg	App Delay (ms) Max	Network Delay (ms) Min	Network Delay (ms) Avg	Network Delay (ms) Max	Total Delay (ms) Min	Total Delay (ms) Avg	Total Delay (ms) Max
○	1.	ott-filer02b.cisco.com	namlab-pc7.cisco.com	sunrpc	2	0	**0**	0	72	**72**	72	72	**72**	72
○	2.	ott-filer02b.cisco.com	namlab-pc7.cisco.com	nfs	2	0	**0**	0	72	**72**	72	72	**72**	72
○	3.	172.20.104.114	sjc-vpn7-18.cisco.com	http	660	0	**3**	452	14	**17**	25	17	**20**	469
○	4.	snowowl2.cisco.com	namlab-pc7.cisco.com	sunrpc	2999	0	**16**	45	0	**0**	15	0	**16**	45
○	5.	namlab-jet1.cisco.com	dhcp-171-69-69-88.cisco.com	http	173	1	**15**	569	1	**1**	3	2	**16**	570
○	6.	snowowl2.cisco.com	namlab-pc7.cisco.com	nfs	2999	0	**16**	45	0	**0**	15	0	**16**	45
○	7.	okn-sjc-011.cisco.com	namlab-window.cisco.com	https	6	0	**7**	26	1	**1**	1	1	**8**	27
○	8.	sjc-gouda-vob.cisco.com	namlab-pc7.cisco.com	sunrpc	6	0	**2**	12	2	**2**	2	2	**4**	14
○	9.	sjc-gouda-vob.cisco.com	namlab-pc7.cisco.com	nfs	6	0	**2**	12	2	**2**	2	2	**4**	14
○	10.	gooddog.cisco.com	namlab-pc7.cisco.com	sunrpc	2	0	**2**	5	1	**1**	1	1	**3**	6

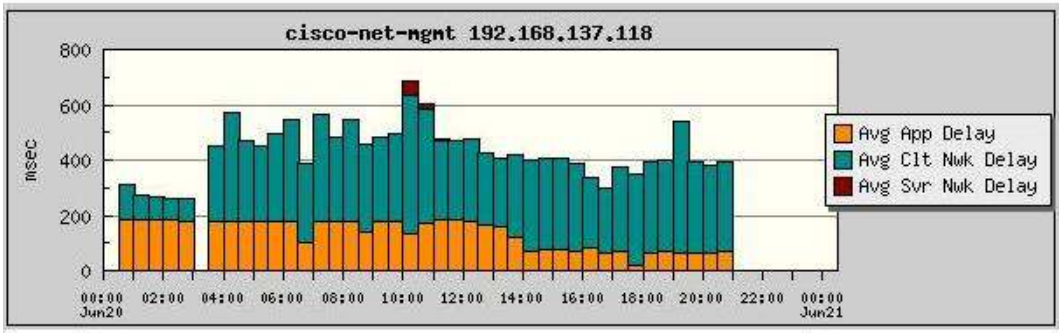
© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Select Monitor -> Response Time -> Server -- Client Response Time.

Figure 13 provides the historical view of the delay in order to assess whether the latency values are transient. This chart can be used to determine what elements contribute to the total delay client experiences. Is there network congestion? Is the server overloaded? It can also help determine the time pattern when the performance issues strike. This information may be used to determine the best time for optimization improvement.

An additional angle of the server traffic load can be obtained from the specific Host view (Figure 14). Note that the host view can provide traffic volume values that are larger than the one reported by the WAE FAs. As an example, if the server serves UDP and TCP traffic, and only TCP is being monitored by WAEs, the host report would include also the UDP portion. The report can be used to identify the servers that generate most traffic. The “real-time” drill-down option can show the host throughput. It could be noted for the server of interest, as a baseline to compare with WAAS optimized throughput.

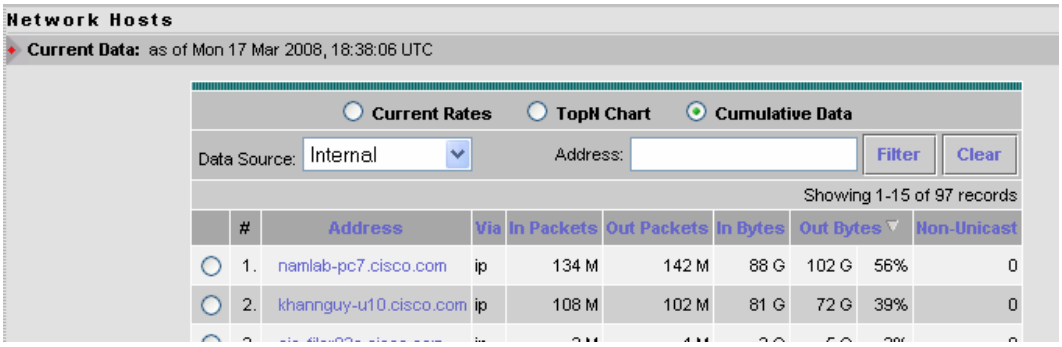
Figure 13. Application Response Time -- Historical Trend



Select Reports -> Basic Reports. Select the Avg App Delay, Avg Clt Nwk Delay and Avg Svr Nwk Delay reports for a server & application and click View. Set Style to Stack Bar.

Note: See Appendix for instructions on setting up reports.

Figure 14. Bandwidth Usage (per host/server)



Select Monitor -> Hosts -> Cumulative Data (radio button).

3.3 Find problematic sites and applications

What are we trying to achieve?

Once customers establish the acceptable application performance values, they can identify sites and locations that do not comply.

How do we achieve that?

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

NAM can provide per-client and per-server reports to help identify problematic sites and applications. Problematic sites and application information can be also obtained from sources like end-user complaints, known infrastructure limitations and dedicated tests.

Possible activities:

- View worst performing client/server pairs for non-complying applications, determine the client site, application and server
- Use mid-term reports of client/server of interest to further confirm that the problem is capacity

Useful reports

Worst client-server performing transaction report can be used to determine the typical branch site that experiences issues, based on the client network address (Figure 12). Filtering can be performed on clients to confirm that a particular client would have performance issue with various servers -- indicating a potential site issue.

If the customer has NAM located in the Branch, he can get insight into the aggregate performance of a particular application /server (example is shown in Figure 10).

3.4 Short-list candidate sites and applications

What are we trying to achieve?

Decide on the sites for WAAS optimization.

How do we achieve that?

The most sites that have application performance level that do not comply with the objectives are naturally WAAS deployment candidates.

Selection of the candidates for WAAS could include the following:

- assessment of the previous steps
- assessment of how much the issues can be addressed by addition of more bandwidth
- operational factors like for PoC/Pilot -- selection of an accessible site

3.5 Install WAAS + NAM

What are we trying to achieve?

Have WAAS and NAM reporting components properly configured

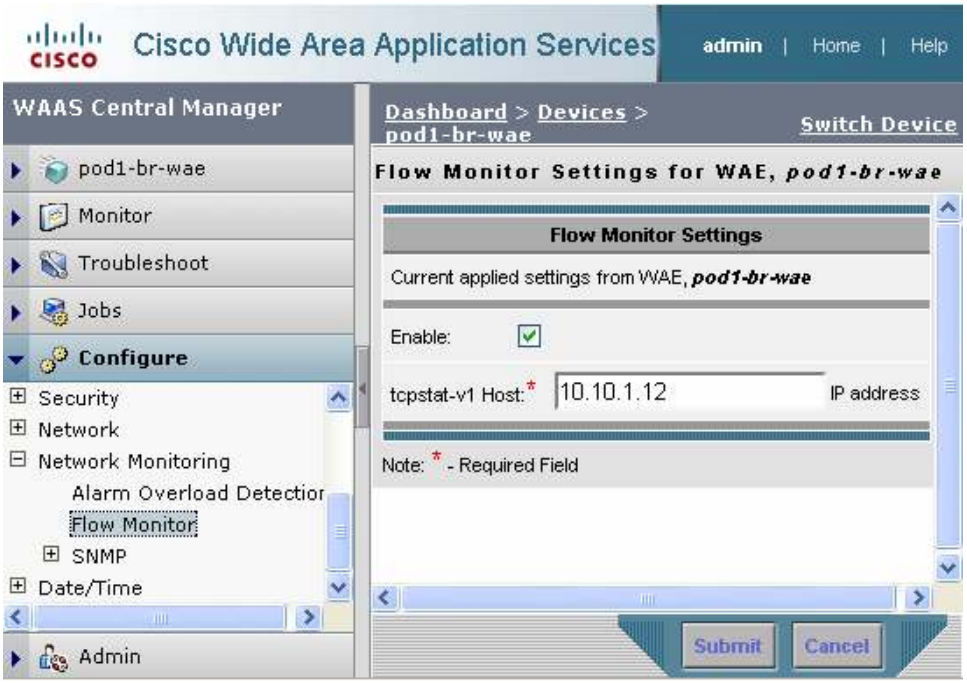
How do we achieve that?

WAAS deployment includes the following reporting components:

- Configuration of WAE FA to send the traffic reports to NAM (typically done using WAAS CM).

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 15. WAAS Central Manager configuration of FA destination



- Configuration of WAE collection in NAM as well as reporting for the clients of interest.
- Identification of test clients for critical applications that are part of the branch (an example can be a SAP test client to be closely monitored).

For configuration details please refer to Appendix A -- Reporting Configuration Details.

3.6 Analyze impact

What are we trying to achieve?

Show the impact of optimization performed by WAAS. Impact visibility has a special value for POCs and Pilots where it can tie to an ROI model to help drive a sale.

How do we achieve that?

- Several aspects of the WAAS deployment impacts can be shown
- Improvement of user-experience

The impact of WAAS on the application performance as experienced by the user can be shown by comparing the user experience before the optimization and the user experience after the optimization. The user experience before the optimization can be obtained by Data Center reports, using SPAN or Pass-Through data sources. The user experience after the optimization can be determined by reporting on traffic coming from the Edge WAE “Client” data source

Improvement of productivity

The benefit of increased branch application traffic, as result of WAN optimization, can be shown by comparison of utilization and traffic before and after activation of optimization. Availability of the reports will depend on the option of NAM to gain access to the device of interest (as a managed device) and on the ability of the device to see both the optimized and the non-optimized traffic from the site of interest. NAM allows management of one chassis at a time (router or switch) for short-term and historical port reporting. The chassis selection is fixed for NAM, NAM2, NM and NME. For the appliance the user can select which chassis to manage.

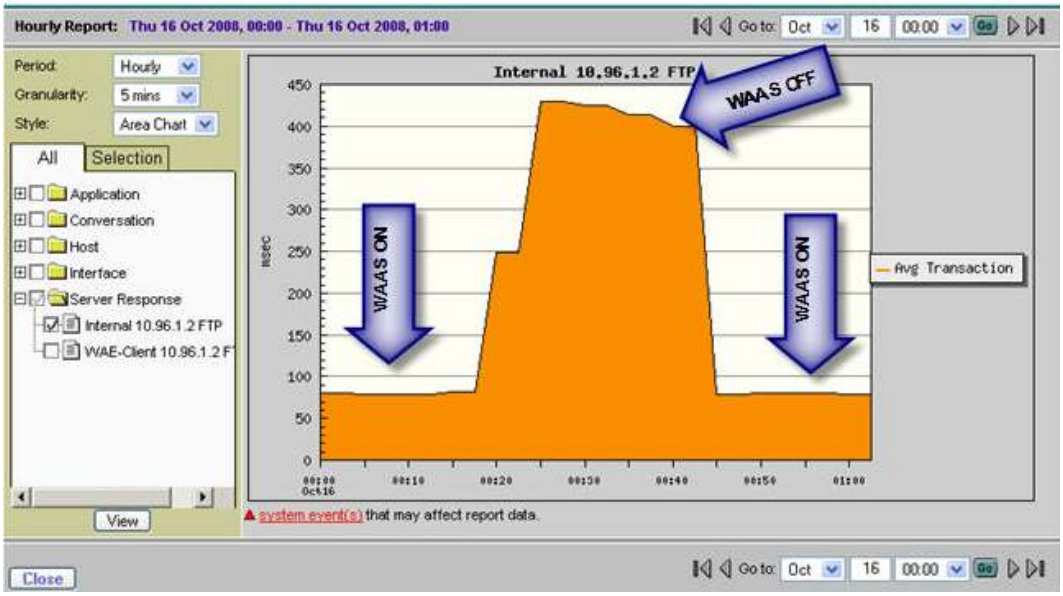
© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Useful reports

The following reports can be leveraged:

- **Comparison of test client experience** -- based on mid-term before/after reports like Figure 17 or, short-term snapshot like the one described in Figure 11
- **Comparison of server-side improvements** (reports on similar to Figure 16 but from the Data Center server perspective)
- **In case of NAM in the branch**, comparison can be of the site application/server experience to show the overall site improvement using reports like Figure 13 for the pre-WAAS as well as the post-WAAS performance
- **Comparison of LAN/WAN traffic**: branch short-term and mid-term interface statistics, when available, can show branch and WAN traffic impact (Figure 18). If the WAN is congested, after optimization activation, traffic is expected to go up on the LAN and remain at a similar level in the WAN. Uncongested WAN traffic may shrink.

Figure 16. Average transaction time -- Branch view of WAAS impact

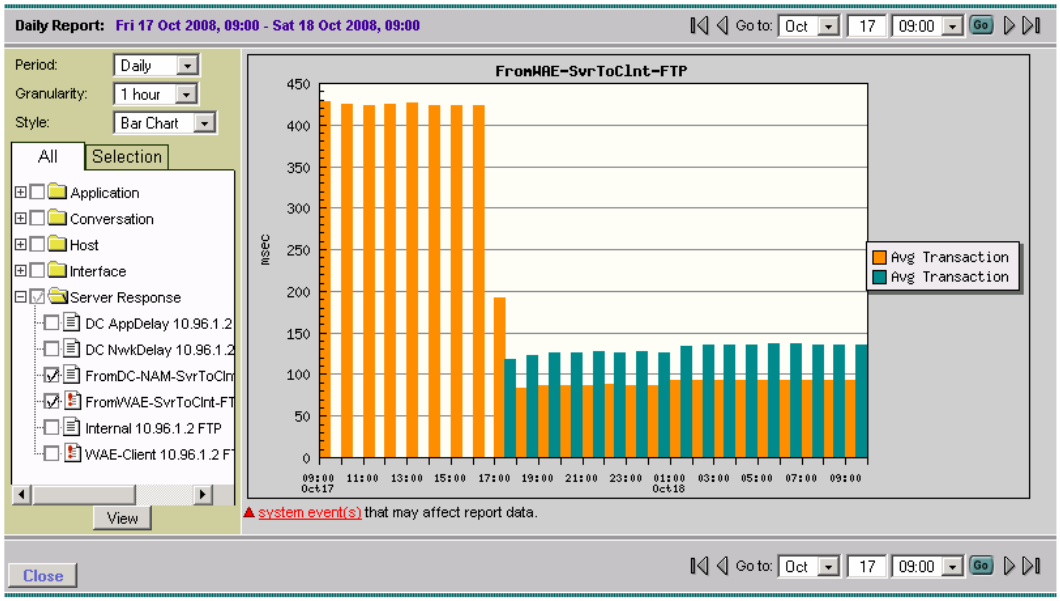


Select Reports -> Basic Reports. Select the Avg Transaction report for a server, application and click View. Set Style to Area Chart.

Note: See Appendix for instructions on setting up reports.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 17. Average transaction time -- Data Center view of WAAS impact

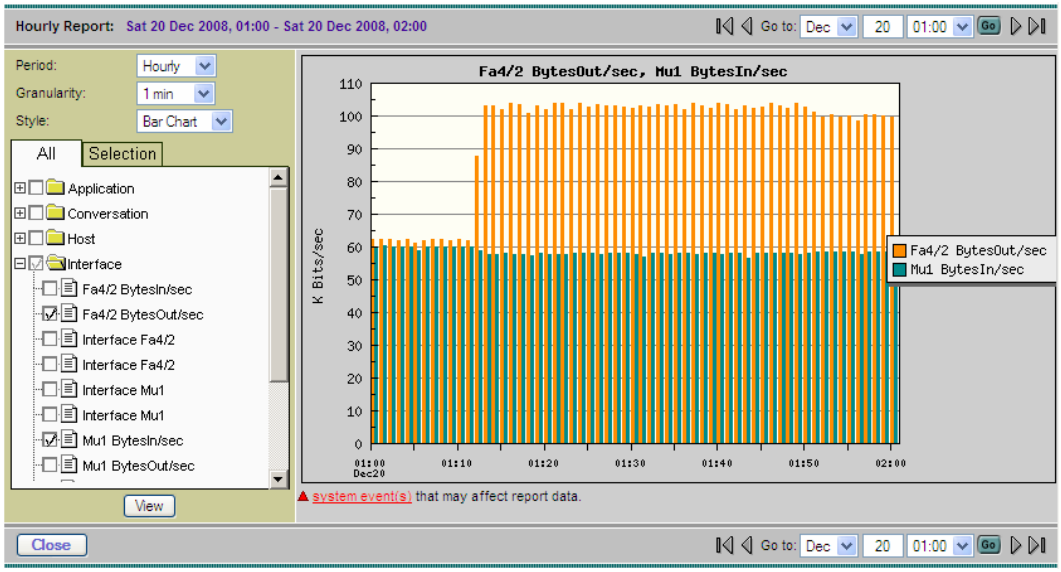


The orange part represents packet measurements from the data center (SPAN or CEF). The green part shows FA measurements from the branch. The orange peak shows the average transaction time when WAAS is turned off. The Branch user experience improvement is between the orange values of ~430ms ("before") and the green values of ~120ms ("after"). The orange is lower after optimization was turned on due to the server-side WAE acting as a proxy and terminating fast the transactions on the server side.

Select Reports -> Basic Reports. Select the Avg Transaction report for the same server, client, application from the SPAN data source and from the WAE data source and click View. Set Style to Bar Chart.

Note: See Appendix for instructions on setting up reports.

Figure 18. Historical reporting of LAN and WAN traffic before and after WAAS optimization activation



© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The graph below shows the changes to a ~60Kbps limited WAN link. Fa4/2 represents the outgoing branch traffic. Traffic increased about 60% in the LAN and was slightly reduced in the WAN after optimization was turned on. Port information is taken from if Table polling of the branch router after configuration of the managed chassis in NAM.

Click Reports -> Basic Reports. Select the LAN bytes out and WAN bytes in reports for the branch Router/Switch.

Note: See Appendix for instructions on setting up reports.

3.7 Monitor and Troubleshoot

What are we trying to achieve?

Support for end-to-end monitoring and troubleshooting when WAAS is deployed

How do we achieve that?

Once WAAS solution is deployed, users can leverage the additional points of probing provided by WAE FAs to complement the picture they can get from direct packet examination (like SPAN) and NetFlow. NAM functions like Monitoring, Reporting, Threshold setting and packet capture/decode can help monitor the deployment health and troubleshoot issues.

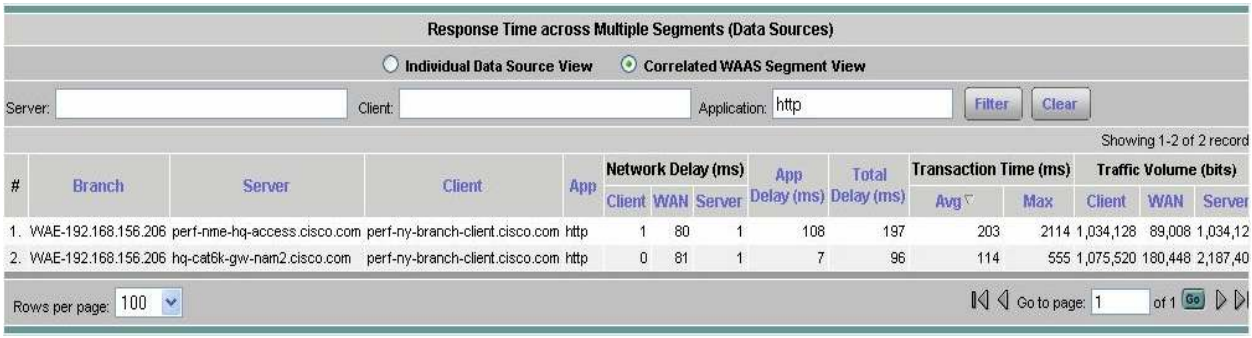
Multi data-source report was added to ease troubleshooting across different probing point. This report (Figure 19) can show the response time experience from multiple data sources to help assess the problem source. As an example, if various probing points show a larger delay toward the WAN (say the Edge-Client shows a larger Server-Network-Delay and the DC-Server shows the opposite), it may suggest a network issue in the WAN.

Useful reports

The following reports can be leveraged:

- Short-term and mid-term reports discussed in the previous sections
- Multi data-source report (Figure 17)

Figure 19. Cross data-source report



Select Monitor -> Response Time -> Multi Segment.

4. Deployment Considerations

This document assumes the following:

- WAAS is deployed in a hub and spoke model
- NAM is located in the Data-Center side of the WAAS deployment. Support for cases where NAM is located in the branch will be noted explicitly. NAM deployment can be a Virtual Blade on Core WAE or a dedicated hardware (blade or appliance).

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The benefit of using NAM in the Data-Center is for both centralized view as well as scale when collecting traffic from the Core WAE.

5. Terms and Acronyms

Acronyms	Definition
NAM	Network Analysis Module
WAAS	Wide Area Application Services
WAE	Wide Area Application Engine
FA	FlowAgent -- reporting agent residing on WAE
IAP	Inteligent Application Performance -- next generation of ART
Short-term (reporting)	In context of reporting “short-term” means here report of data for the current time interval (which can be lowered to 30 seconds. These reports are under “Monitor” in NAM GUI.
Mid-term (reporting)	Reports held up to 100 days in NAM

6. Related Documents

NAM documentation can be found in the following locations:

- Cisco Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html.
- Cisco Branch Routers Series Network Analysis Module: http://www.cisco.com/en/US/products/ps7176/index.html.

7. Appendix A -- Reporting Configuration Details

7.1 Configuring the Data Center NAM

NAM-2 Catalyst 6000 and 7600 Blade or Cisco NAM 2220 and NAM 2204 appliance is typically deployed in the Data Center to provide application performance visibility and traffic analysis. The Data Center NAM will be able to provide aggregate response time statistics for a particular server-application pair, as well as the response time statistics for a particular server-client-application tuple, where the client can be test client located in a remote branch.

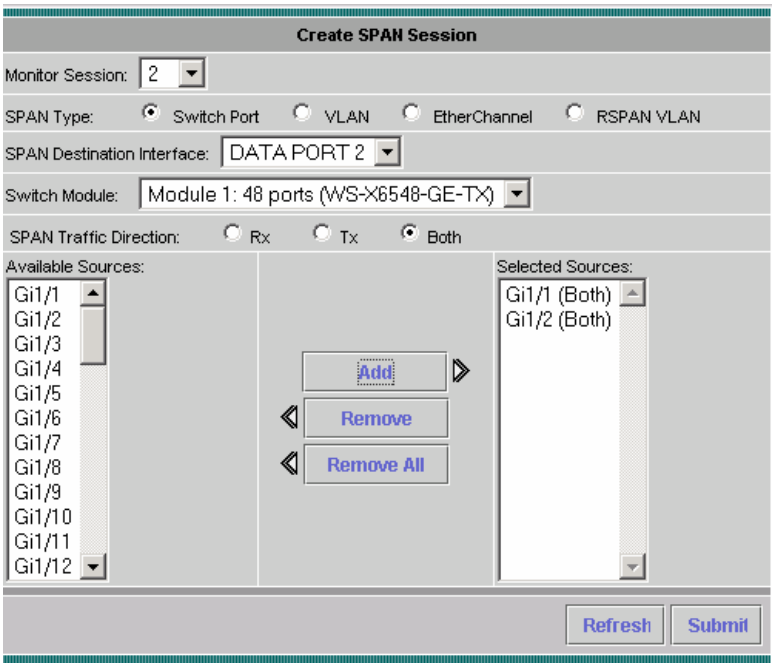
Configuring SPAN Data Source on NAM Blade and Appliance

Click Setup -> Data Sources -> SPAN -> Create.

Select the appropriate SPAN Type, SPAN Destination (On the NAM Appliance this will be the Port on the Managed Device that is connected to the NAM Apppliance), SPAN Direction and Available SPAN Sources.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 20. Creation of SPAN session



Click Setup -> Monitor and ensure that Core Monitoring and Response Time Monitoring are enabled for the SPAN Data Source.

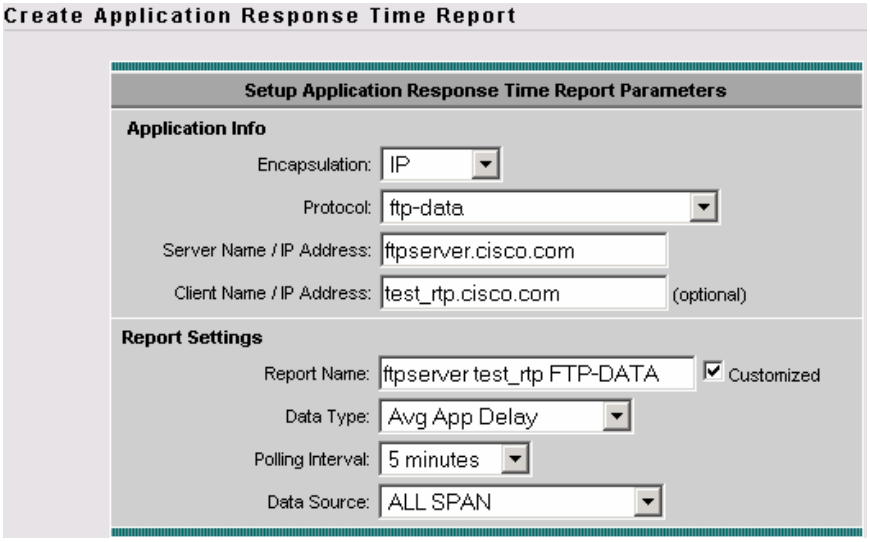
Useful Historical Reports on the Data Center NAM

Response Time Reports between a Server hosting the application to be optimized and a Test Client at a remote Branch provide the useful insights into the impact of a WAAS deployment as observed from the Data Center.

1. Identify the application, server in the data center and test client in the branch for which you wish to monitor response time to view historic trends.
2. Click Reports -> Basic Reports.
3. Click Create and Select Response Time.
4. Enter the Application information for the optimized application as well as the server and test client (in the branch).
5. Select Data Type as Avg App Delay and Data Source: as the SPAN data source (where this traffic is seen) and set the appropriate Polling Interval. This can be as low as 1 minute.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 21. Application performance report setting – server and client



6. Repeat the above steps for Data Type Avg Clt Nwk Delay, Avg Svr Nwk Delay and Avg Transaction.
7. From Reports -> Basic Reports, multiple reports can be checked and then selecting View provides a composite report. Figure 15 is a composite report of Avg App Delay, Avg Clt Nwk Delay, Avg Svr Nwk Delay for a particular Server, Client and Application as observed from the Data Center.

7.2 Configuring the Cisco Branch NAM

NME-NAM ISR Service Module or NAM2220/NAM2204 appliance is typically deployed in the Branch edge to provide application performance visibility and traffic analysis for the Branch. The Branch NAM will be able to provide response time data as experienced by the clients in that particular branch/site.

Configuring Internal Data Source on the NME-NAM

Cisco Express Forwarding (CEF) can be used to sends an extra copy of each IP packet that is received from or sent out on an interface to the NAM through the Integrated-Service-Engine interface on the ISR router and the internal NAM interface.

To configure the Data Sources, execute these commands on the Router:

```
Router#config t
Router(config)#ip cef
Router(config)#interface type slot/port or interface type slot/wic-slot/port
Router(config-if)#analysis-module monitoring
```

Repeat the above two steps for each interface that you want the NAM to monitor.

Click Setup -> Monitor on the NAM GUI and ensure that Core Monitoring and Response Time Monitoring are enabled for the Internal Data Source.

Useful Historical Reports on the Branch NAM

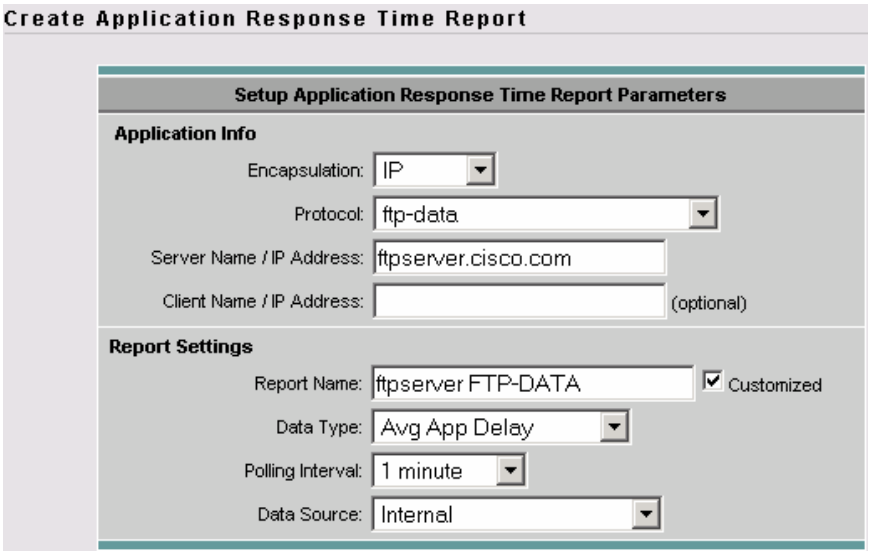
Response Time Reports for a Server hosting the application to be optimized provides useful insights into the impact of a WAAS deployment as observed from the Branch. This provides an aggregate Branch/site level view into response time improvement.

1. Identify the application, server in the data center for which you wish to monitor response time to view historic trends.
2. Click Reports -> Basic Reports.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

3. Click Create and Select Response Time.
4. Enter the Application information for the optimized application and the Server.
5. Select Data Type as Avg App Delay and Data Source: as the Internal data source (where this traffic is seen) and set the appropriate Polling Interval. This can be as low as 1 minute.

Figure 22. Application performance report setting – server only



6. Repeat the above steps for Data Type Avg Clt Nwk Delay, Avg Svr Nwk Delay and Avg Transaction.
7. From Reports -> Basic Reports, multiple reports can be checked and then selecting View provides a composite report. Figure 11 is a composite report of Avg App Delay, Avg Clt Nwk Delay, Avg Svr Nwk Delay for a particular Server and Application as observed from the Branch NAM.
8. Figure 12 is the Avg Transaction report for a particular Server and Application as observed from the Branch NAM.

7.3 Configuring WAAS -- NAM Integration

Configuring WAAS to send Flow information to NAM

Before you can monitor WAAS traffic, you must first configure the WAAS device to export WAAS flow record data to the NAM using the WAAS command-line interface (CLI) flow monitor command like the following:

```
Core-WAE#config t
Core-WAE(config)#no flow monitor tcpstat-v1 enable
Core-WAE(config)#flow monitor tcpstat-v1 host  <NAM-IP-ADDRESS>
Core-WAE(config)#flow monitor tcpstat-v1 enable
Core-WAE(config)#end
Core-WAE#
```

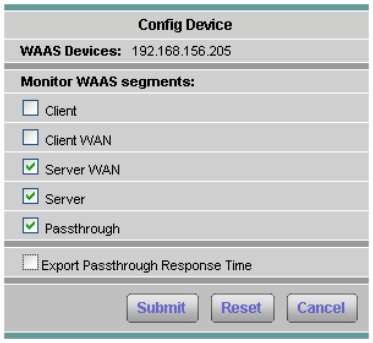
After you enable flow export to the NAM using WAAS CLI commands like those above, WAAS devices will be detected and automatically added to the NAM's WAAS device list. Alternatively, you could configure the flow monitor using the CM (see Figure 15).

Configuring WAAS Data Source in NAM

1. Click Setup -> Data Sources
2. From the contents menu, choose WAAS -- Devices.
3. Choose the WAAS device you want to modify, then click Config.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 23. Selection of WAAS source segments



4. You can configure the WAAS data sources to monitor the following WAAS segments as shown in Figure 2, WAAS Data Sources (Data Collection Points):
   - **Client:** This setting configures the WAE device to export the original (LAN side) TCP flows originated from its clients to NAM for monitoring.
   - **Client WAN:** This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to NAM for monitoring.
   - **Server WAN:** This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to NAM for monitoring.
   - **Server:** This setting configures the WAE device to export the original (LAN side) TCP flows from.
   - **Pass-Through:** This setting configures the WAE device to export the flows that traverses WAAS without being optimized (available in NAM 4.1)
5. Let us consider two deployment scenarios with Servers in the Data Center(Core) and Clients in the Branch(Edge):
   - NAM in the Data Center (NAM-2 or NAM2200 appliance)

     Edge WAE Data Source: Client

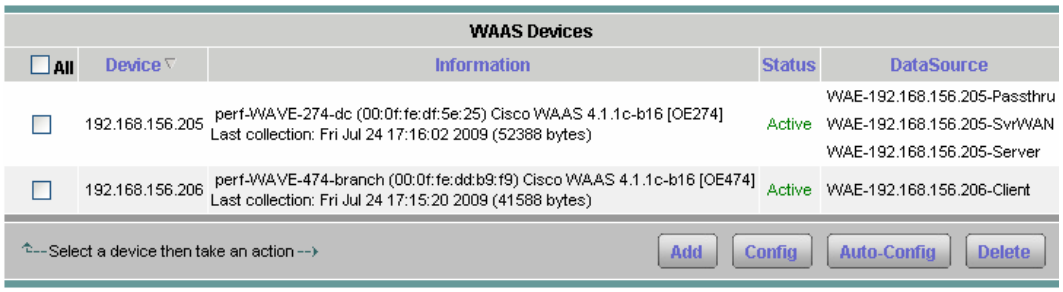
     Core WAE Data Source: Server, ServerWAN, Pass-Through (available in 4.1)

     PS: SPAN data sources might take the place of the Server data source. For example, if you already configure SPAN to monitor the server LAN traffic, it's not necessary to enable the Server data source on the WAE device.The Pass-Through data source will take the place of SPAN in the VB environment and can be used to provide baseline statistics before optimization is enabled.
   - NAM in the Branch (NME-NAM or NAM2200 appliance)

     Edge WAE Data Source: Client, ClientWAN

     Core WAE Data Source: Server, Pass-Through

Figure 24. WAAS devices status



6. Click Setup -> Monitor and ensure that Core Monitoring and Response Time Monitoring are enabled for the

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

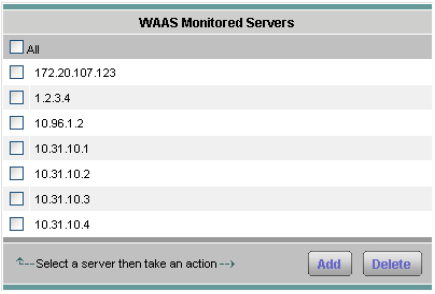
WAE Data Source.

Configuring WAAS Monitored Servers in NAM

WAAS needs to know which flows it must export to NAM. Entering Server IP addresses in the WAAS Monitored Servers will enable WAAS to export flows related to those servers to the NAM, so NAM can monitor the response time for the given servers.

1. Click Setup -> Data Sources.
2. From the contents menu, choose WAAS -> Monitored Servers.
3. Click Add and enter the server IP address in the Server Address field.

Figure 25. WAAS monitored servers



Configuring Response Time Reports for Impact Analysis

The reports function allows you to store and retrieve up to 100 days of historical data about the network traffic monitored by the NAM. Response Time reports in NAM can provide visibility into the impact of WAAS. Create a response time report for the average transaction time as experienced by the client, based on the Client WAE Data Source. This report can be created on the Data Center NAM to gain visibility on response time improvement as experienced by a particular client in the branch.

Response Time Report on the Data Center NAM

1. Click Reports -> Basic Reports.
2. Click Create and Select Response Time.
3. Enter the Application information for the optimized application as well as the server and test client (in the branch).
4. Select Data Type as Avg. Transaction and Data Source: as the Client WAE data source.
5. From Reports -> Basic Reports, multiple reports can be checked and then selecting View provides a composite report. Figure 13 is a composite report of Avg Transaction for a particular Server and Application from the local SPAN Data Source and from the remote WAE Data Source.

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Printed in USA C11-506458-01 08/09

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.