Using Cisco NAM Hardware in a WAAS Deployment

Deployment Guide

Contents

Abstract

Cisco® Wide Area Application Services (WAAS) is a powerful application acceleration and WAN optimization solution that optimizes the performance of TCP-based applications operating in a WAN environment This optimization allows IT organizations to consolidate costly branch-office servers and storage in centrally managed data centers and to deploy new applications directly from the data center while offering LAN-like application performance for any employee, regardless of location.

In a typical WAN-optimized deployment, the interception of application traffic obscures the response time, data transfer time, and other performance metrics; hence the traditional monitoring techniques fail to accurately characterize the impact of optimization.

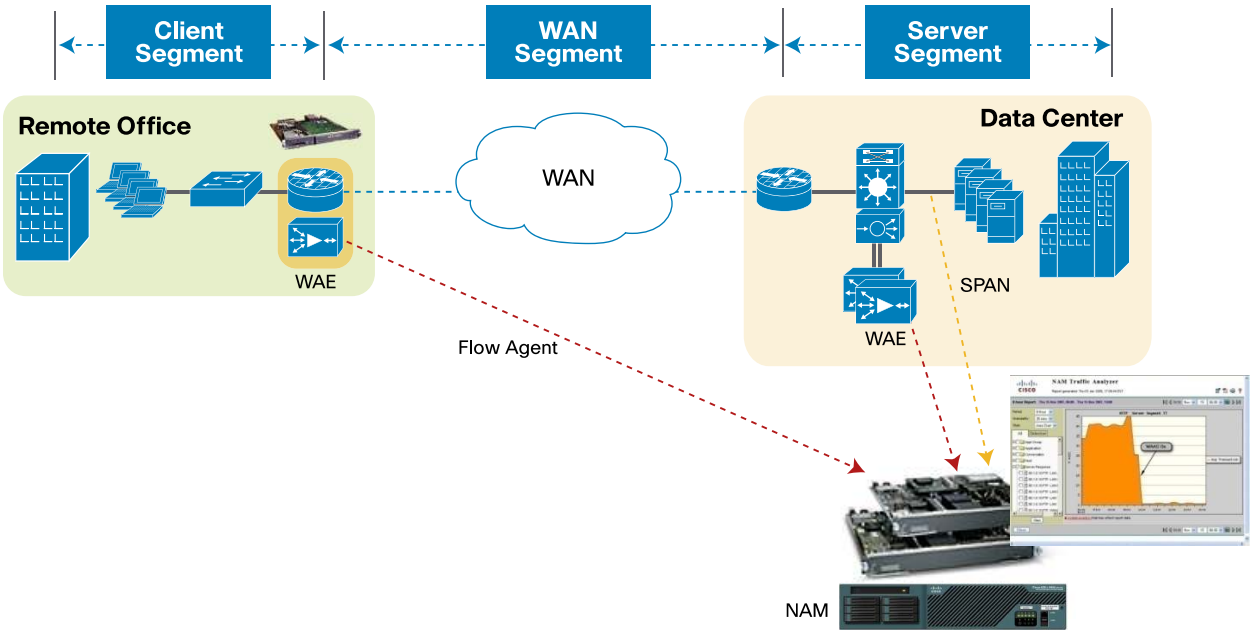
Cisco® Network Analysis Module (NAM) uses the built-in instrumentation on Wide-Area Application Engine (WAE) devices as additional data sources to gather flow data for optimized traffic and provide end-to-end application performance visibility in a Cisco WAAS environment (Figure 1). It measures and reports on application response time, transaction time, bandwidth usage, and LAN/WAN data throughput among other performance metrics. As a result, it can accurately quantify the impact of Cisco WAAS optimization.

Cisco NAM can also help to assess which applications would benefit the most from deploying WAN optimization and application acceleration services. Analyzing the response time data over a period of time, the administrator can identify the applications where the response time improvement can be significant with an increase in available bandwidth. In addition, understanding the traffic mix provides a sense of how much compression could be achieved with Cisco WAAS based on the type of applications in the mix.

Finally, Cisco NAM can be used to provide real-time visibility for ongoing optimization improvements, to monitor optimized and nonoptimized applications, and to troubleshoot any performance degradation issues.

The purpose of this document is to provide detailed steps to configure the NAM and generate useful reports to demonstrate the impact of WAAS in a proof of concept (POC) as well as in WAAS deployments.

Figure 1. Cisco NAM Provides End-to-End Application Performance Visibility in WAAS Environments



Note: The details of WAAS installation, setup, and testing are not covered in this document.

Installation and Configuration of the Data Center NAM

For WAAS monitoring, it is recommended to connect a Cisco® NAM 2200 appliance to the data center edge switch. Alternately a NAM-2-250S service module can be installed in the Catalyst® 6000 at the data center edge. The NAM Virtual Blade is covered in the link listed below. The device in which the NAM resides or to which it is connected is referred to as the managed device.

For installation instructions for the Cisco NAM 2200 appliances, please see: http://www.cisco.com/en/US/products/ps10113/prod_installation_guides_list.html.

For installation instructions for the Cisco NAM-2-250S, please see: http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.1/switch/configuration/guide/swconfig.html.

For installation instructions for the Cisco NAM Virtual Blade, please see: http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_virtual_blade/4.1/install/guide/vbinstall.html.

NAM-WAAS white papers — Using Cisco NAM 4.1 Reporting with Cisco WAAS: http://www.cisco.com/en/US/prod/collateral/modules/ps2706/white_paper_c11-506458_ps10113_Products_White_Paper.html.

Enhanced Operations Visibility for WAAS Deployments with Cisco NAM: http://www.cisco.com/en/US/prod/collateral/modules/ps2706/white_paper_c11-554563-00_ps10113_Products_White_Paper.html.

For application performance metrics, please refer to the user guide at: http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.0/user/guide/monitor.html#wp1046620.

More documents are available at http://www.cisco.com/go/nam.

Initial NAM Configuration

This section will walk you through the initial setup of the NAM using the command-line interface (CLI).

1. Log in or session to the NAM using root as the username and root as the password.
2. Enter the following commands to enable IP access:

```
ip address <IP-Address> <Subnet-Mask>
ip gateway <Gateway-IP-Address>
ip domain <Domain-name>
ip nameserver <Nameserver-IP-Address>
ip http server enable
(Enter the web username and password)

exsession on
```

3. Connect to the NAM IP address using a web browser and log in using the web username and password you have selected.
4. Go to **Setup > Preferences** and change the **Data Displayed** in value to **Bits**.

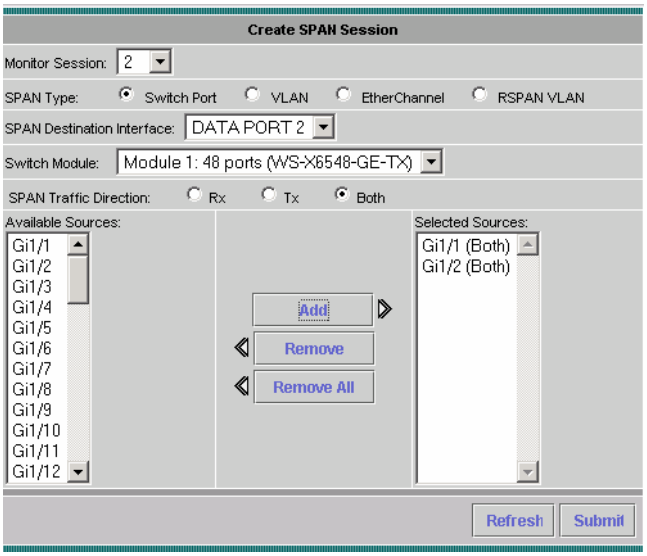
Configuring the SPAN Data Source

Select the interfaces/VLANs on the managed device that connect to the server LAN as the source for the Switched Port Analyzer (SPAN) session. The intention is to be able to see all the traffic between the data center and the branches. The SPAN destination on the NAM-2-250S can be either DATA PORT 1 or DATA PORT 2. The SPAN destination on the NAM appliance is the physical port on the managed device that is connected to the physical data port of the NAM appliance.

1. Click **Setup > Data Sources > SPAN > Create**

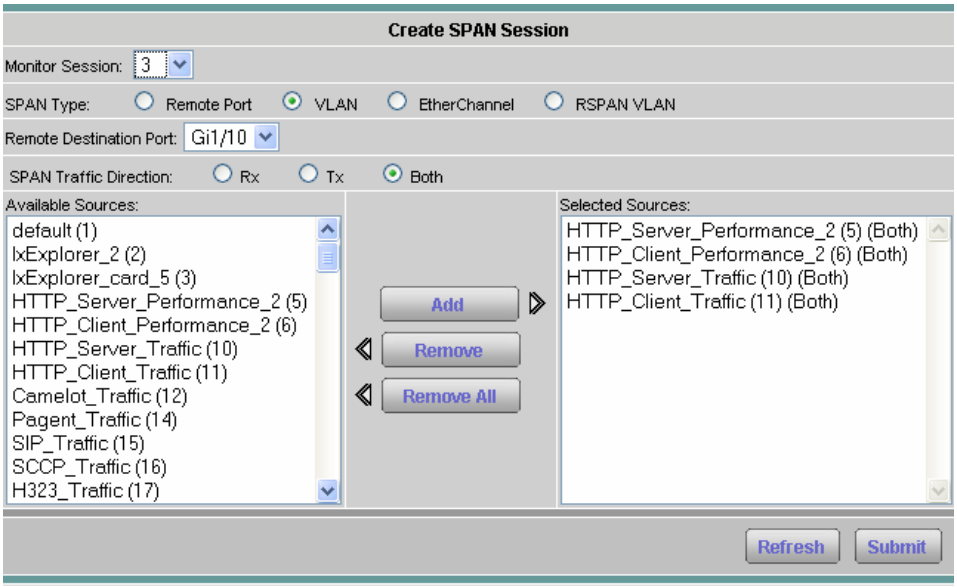
   Select the appropriate SPAN type, SPAN destination, SPAN direction, and available SPAN sources (Figures 2 and 3).

Figure 2. Creating a SPAN Session on the NAM-2-250S



Note: On the NAM appliance the SPAN destination will be the port on the managed device that is connected to the NAM appliance.

Figure 3. Creating a SPAN Session on the NAM 2200 Series Appliance



2. Click **Setup > Monitor** and make sure that **Core Monitoring** and **Response Time Monitoring** are selected for the SPAN data source (Figures 4 and 5).

Figure 4. Setting Up Core Monitoring Functions

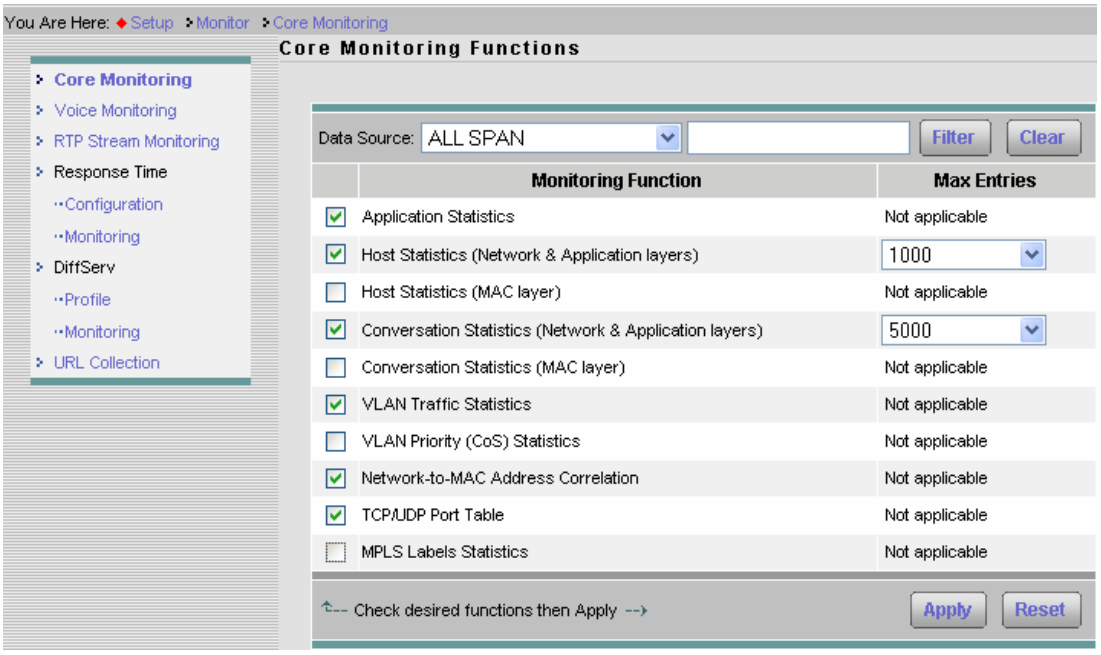
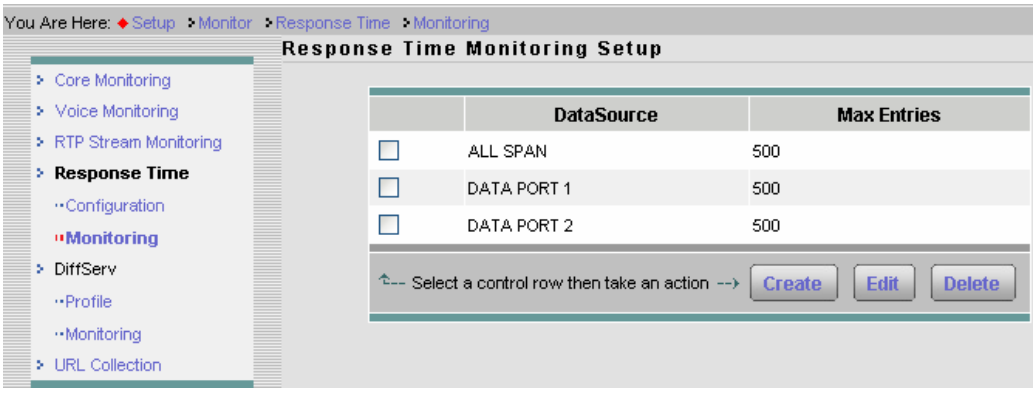


Figure 5. Setting Up Response Time Monitoring



3. You can now go to **Monitor > Overview** and other monitor screens to analyze the SPAN session's traffic to the NAM. We will cover this in greater detail later in the guide.

Configuring NetFlow Export on the Remote Branch Router (Optional)

The Cisco IOS® NetFlow records offer an aggregate view of the network traffic. When enabled on the branch router/switch, the NetFlow data source becomes available on the Cisco NAM. NetFlow provides statistics for applications, hosts, and conversions. Custom data sources can be specifically set up for some interfaces. NetFlow can be used to identify business-critical applications that are hosted in the data center and used in the branch.

Configuring NetFlow on Cisco IOS Routers

NetFlow can be configured on the branch edge router. NetFlow needs to be enabled on both the WAN and LAN interface to provide visibility into traffic flows entering and leaving the branch:

```
config t
interface <interface>
   ip route-cache flow
   exit
```

Configure the router to export NetFlow data to the NAM:

```
ip flow-export version 5
ip flow-export destination <NAM-Ip-Address> 3000
```

Note: The User Datagram Protocol (UDP) port number must be set at 3000.

Also make sure the Simple Network Management Protocol (SNMP) read-only community string is configured on the device:

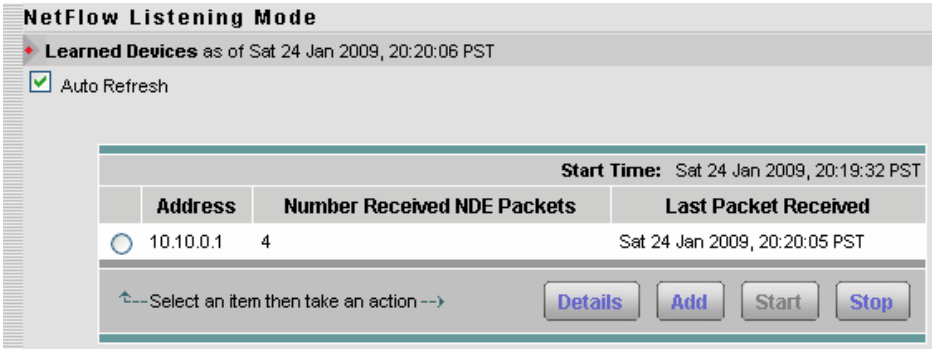
```
snmp-server community <RO-string> RO
```

Configuring the NetFlow Data Source on the NAM

Use the NAM Traffic Analyzer to enable additional NetFlow monitoring devices.

1. From **Setup > Data Sources > NetFlow > Listening Mode**, click **Start** (Figure 6).

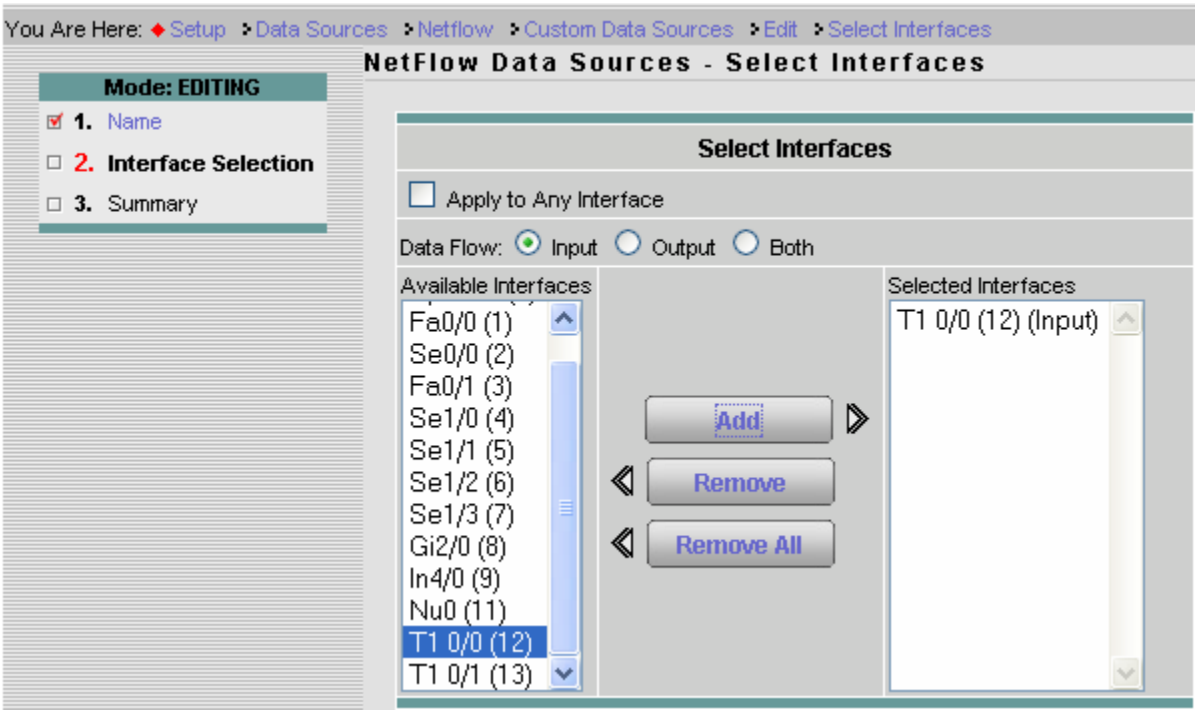
Figure 6. NetFlow Listening Mode



This allows the Cisco NAM to listen to any NetFlow packets being sent to it.

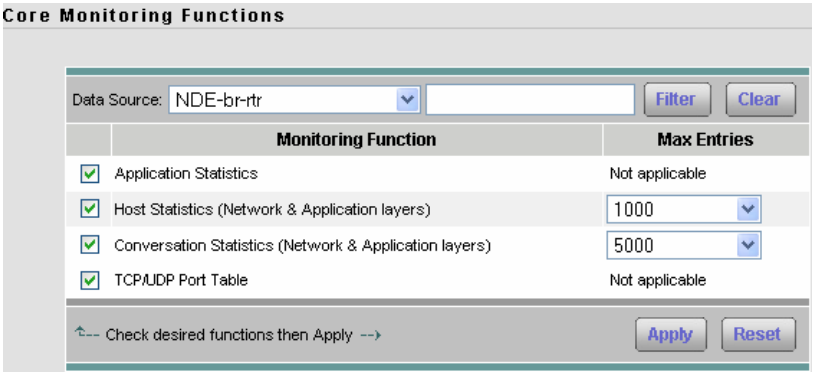
2. When you see the IP address or addresses, select and add the device or devices, and provide the SNMP read community string. Checking the **Create Data Source** check box will create a NetFlow data source for that device with an aggregate of flows received from all NetFlow-enabled interfaces.
3. Test for connectivity and the SNMP community string from **Setup > Data Sources > NetFlow > Devices**, then click Test.
4. To add a custom data source with just selected interfaces, select **Setup > Data Sources > NetFlow > Custom Data Sources**. Select a NetFlow device, provide a name, and click **Next**. Add the WAN interface to monitor in this data source (Figure 7), click Next, review the settings, and click **Finish**.

Figure 7. Selecting the WAN Interface for NetFlow Monitoring



5. Next, go to **Setup > Monitor > Core Monitoring** and select the desired data sources with a prefix NDE as the NetFlow data source and enable the collections (Figure 8).

Figure 8. Enable Collections on the Desired Data Sources with a Prefix NDE

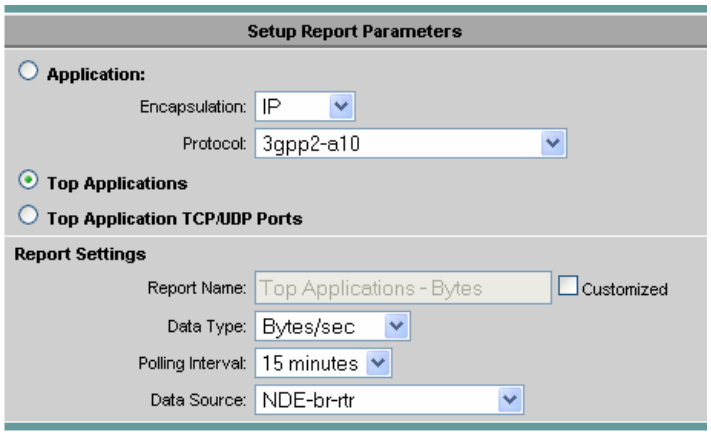


Configuring NetFlow Reports on the NAM

Creating a top applications and top hosts report for the NetFlow data source will provide trending and visibility into the top applications and top talkers for a particular branch over a period of time.

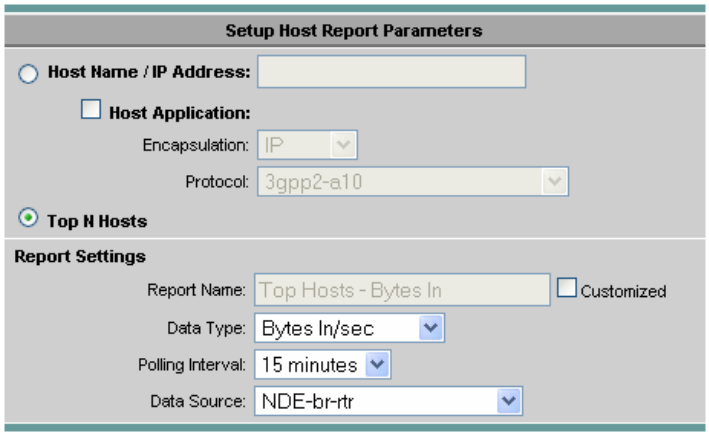
1. Click **Reports > Basic Reports > Create**.
2. Select **Applications** and click **Next**.
3. Select **Top Applications** and the NetFlow data source and click **Finish** (Figure 9).

Figure 9. Setting Up the Top Applications Report



4. Select **Create** again.
5. Select **Hosts** and click **Next**.
6. Select **Top N Hosts** and the NetFlow data source and click **Finish** (Figure 10).

Figure 10. Setting Up the Top N Hosts Report

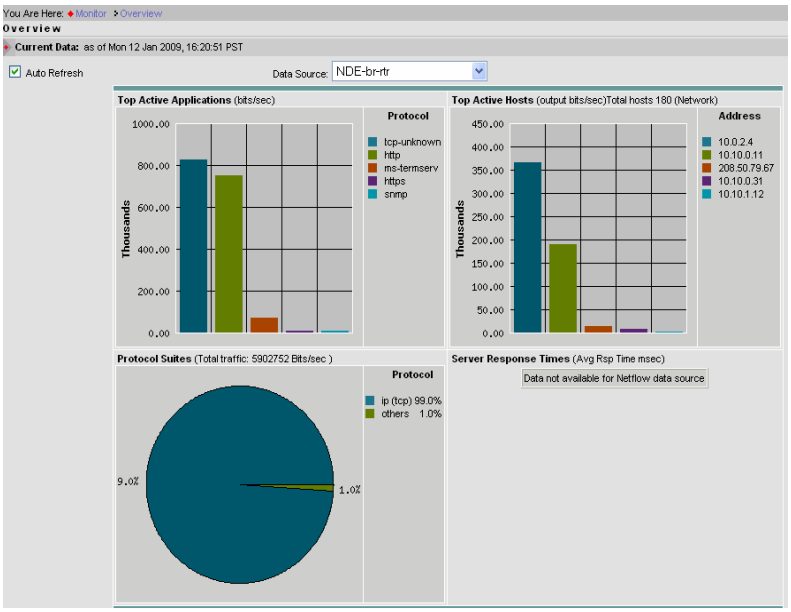


Using SPAN and NetFlow to Identify Business-Critical Applications

Information from the SPAN data source from the data center switch can be used to identify aggregate traffic statistics, such as top applications and top talkers, for all the branches being served by the data center. NetFlow data from the branch router can be used to identify top applications, top talkers, and the amount of network resources being utilized by a particular branch. Information from both sources can be used to identify application optimization opportunities, as well as to select sites to target for the WAAS pilot. The illustrations below use the NetFlow data source. However, the same real-time monitoring screens are also available for the ALL SPAN data source.

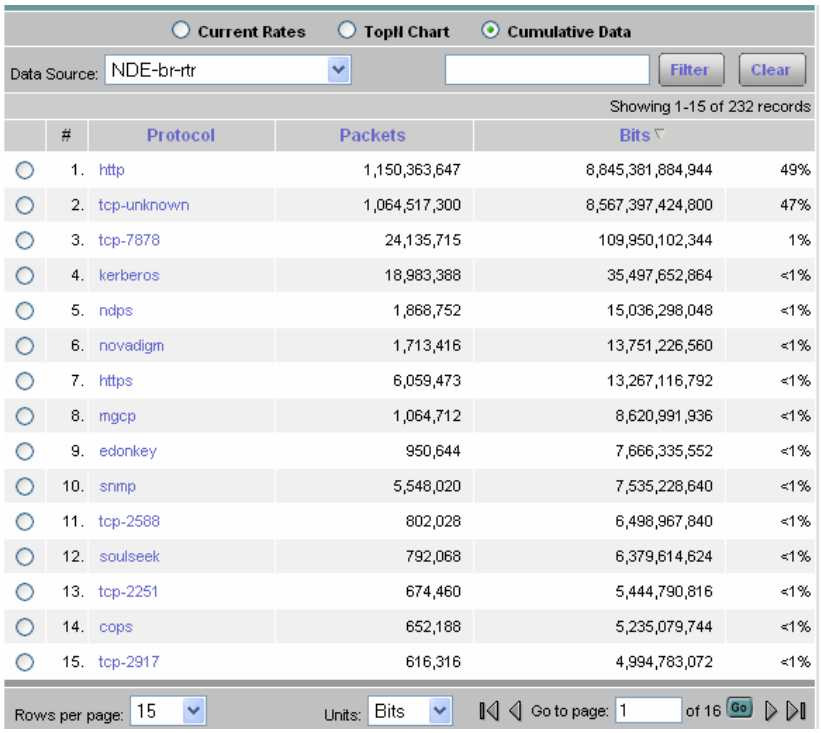
1. Select **Monitor > Overview** and select the NetFlow (NDE) data source. This will provide a real-time view into the top active applications and top active hosts (Figure 11).

Figure 11. The Overview Provides a Real-Time View of the Top Active Applications and Top Active Hosts



2. Select **Monitor > Apps** and select the NetFlow (NDE) data source. This will provide visibility into the top applications and the current rates. Selecting the **Cumulative Data** radio button will show the top applications and the cumulative data for those applications and the percentage of network traffic made up by each application (Figure 12).

Figure 12. Cumulative Data for the Top Applications



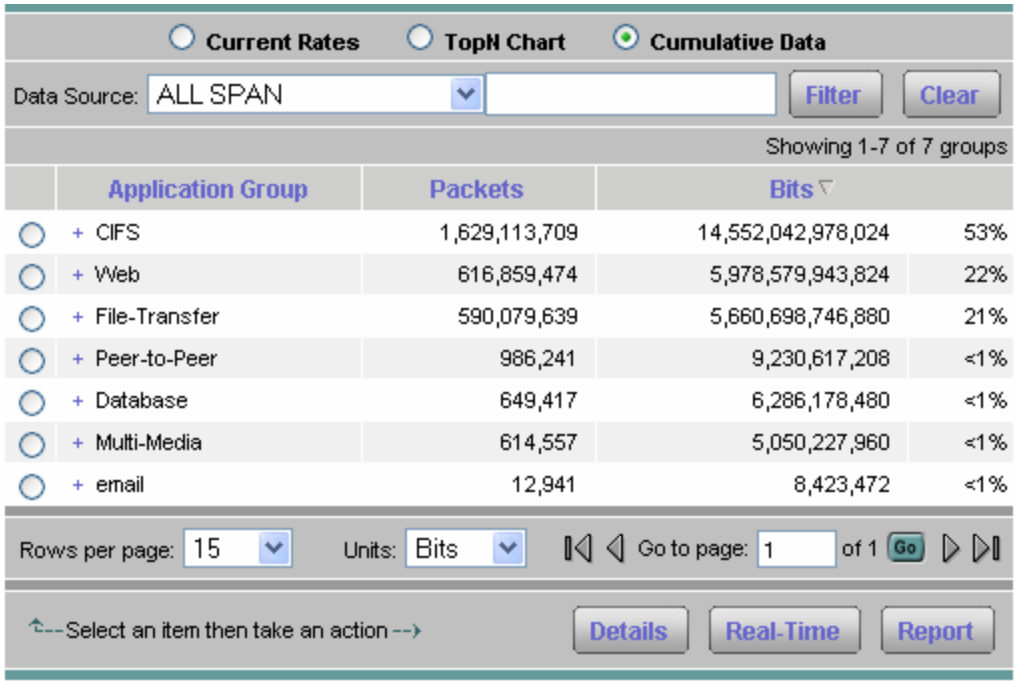
3. Select **Monitor > Hosts** and select the NetFlow (NDE) data source. This will provide visibility into the top hosts and the current rates. Selecting the **Cumulative Data** radio button will show the top hosts and the cumulative data for those hosts and the percentage of network traffic used by each host (Figure 13).

Figure 13. Cumulative Data for the Top Hosts

#	Address	Via	In Packets	Out Packets	In Bits	Out Bits		Non-Unicast
1.	10.0.2.4	ip	3,298,604,830	3,922,159,905	19,252,648,764,736	35,311,306,669,648	65%	0
2.	10.10.0.11	ip	3,927,091,503	3,185,012,546	35,316,136,652,752	18,098,872,369,368	33%	0
3.	171.68.96.135	ip	0	118,820,164	0	1,166,936,164,480	2%	0
4.	10.1.1.10	ip	13,278,558	10,836,051	5,968,703,184	103,819,188,648	<1%	0
5.	10.10.1.12	ip	13,039,304	17,744,888	106,798,325,280	12,818,861,056	<1%	0
6.	10.10.1.20	ip	948,214	2,553,156	1,963,049,712	5,482,904,800	<1%	0
7.	10.10.1.10	ip	799,416	2,075,748	1,396,080,664	4,495,640,640	<1%	0
8.	10.1.0.10	ip	4,621,086	1,750,757	10,003,476,800	3,474,314,616	<1%	0
9.	10.0.2.2	ip	3,959,744	3,885,941	8,656,862,912	3,310,676,640	<1%	0
10.	10.10.0.31	ip	2,568,480	3,829,159	4,330,313,888	2,704,742,216	<1%	0
11.	10.0.0.10	ip	3,702,680	1,847,988	4,875,468,592	2,660,946,352	<1%	0
12.	10.0.2.16	ip	2,720,540	2,005,604	1,670,936,320	2,062,209,696	<1%	0
13.	10.0.2.5	ip	1,937,084	1,888,919	4,934,451,456	1,865,050,880	<1%	0
14.	12.190.48.115	ip	53,952	102,888	19,229,600	1,207,439,360	<1%	0
15.	10.10.0.20	ip	930,206	1,036,020	786,007,360	1,077,314,432	<1%	0

4. Select **Monitor > Apps > Application Group** and select the **Cumulative Data** radio button (Figure 14).

Figure 14. Cumulative Data for Application Groups

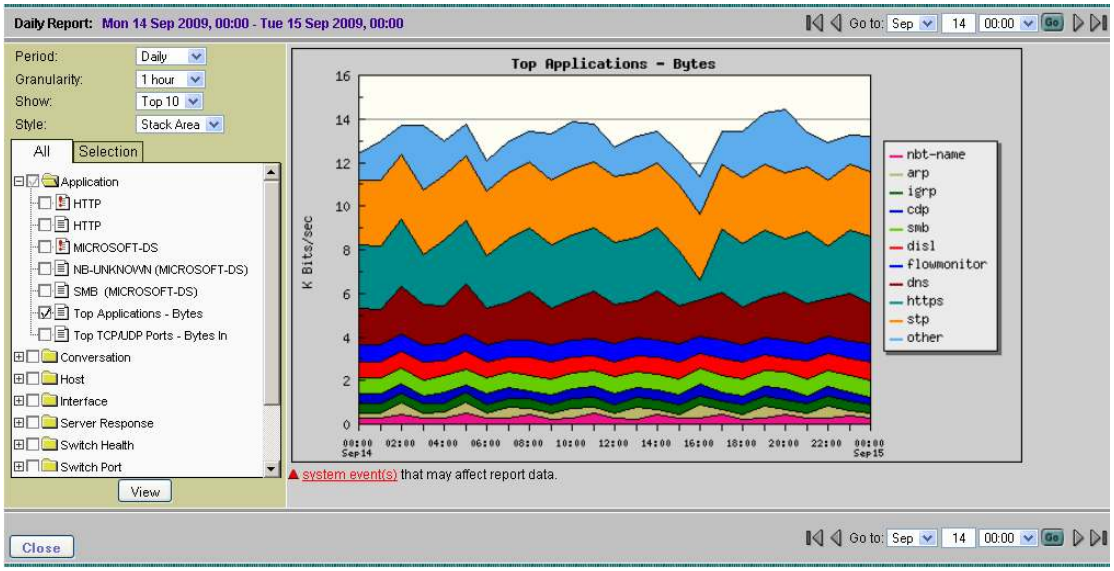


Application Group	Packets	Bits	
+ CIFS	1,629,113,709	14,552,042,978,024	53%
+ Web	616,859,474	5,978,579,943,824	22%
+ File-Transfer	590,079,639	5,660,698,746,880	21%
+ Peer-to-Peer	986,241	9,230,617,208	<1%
+ Database	649,417	6,286,178,480	<1%
+ Multi-Media	614,557	5,050,227,960	<1%
+ email	12,941	8,423,472	<1%

This shows how applications can be grouped. In this case we see that the CIFS, Web, and File-Transfer application groups consume the most bandwidth. These are also conducive to optimization, and hence WAAS can provide substantial improvements in this network.

5. Select **Report > Basic Reports** and select the **Top Applications** report for the NDE data source (Figure 15). This will provide visibility into trending of the top applications' rates over time. The same can be done to view the top host rates over time by selecting the Top Hosts report.

Figure 15. Trending of the Top Applications' Rates Over Time



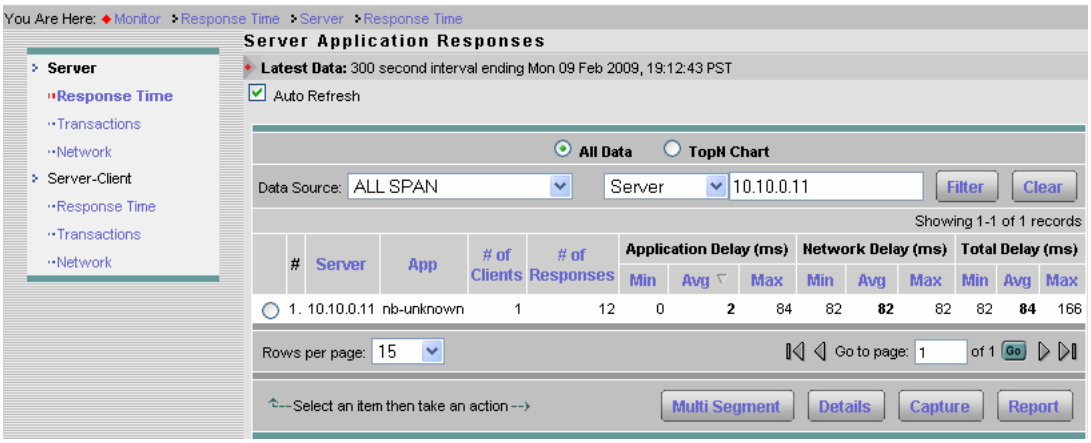
Creating a Baseline of Application Performance

After understanding the various applications of interest, we would like to quantitatively determine the acceptable performance level for these applications. The NAM short-term and historical reports on application bandwidth usage and response time can help users in creating a baseline. The measurements can be made in busy time periods when users are experiencing poor performance as well as when the performance is acceptable to derive a baseline.

Real-Time Reports for Evaluating Application Performance

1. Click **Monitor > Response Time > Server Response Time**. You can now filter on the specific server for which you are looking to baseline the application performance. This will provide the aggregate view for a particular server and application as observed from the SPAN traffic on the data center switch (Figure 16).

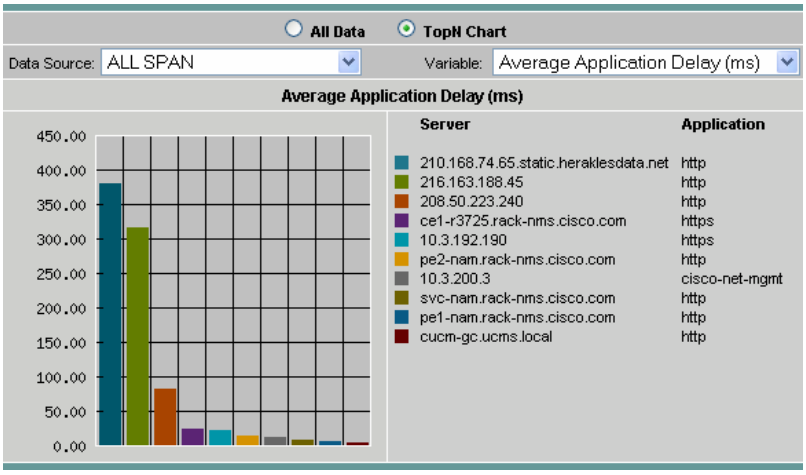
Figure 16. Server Response Time



In this case we notice that the network delay (which includes the WAN delay in this case) is contributing significantly to the response time. So this application might benefit from caching, compression, and other techniques that would reduce the number of round trips on the WAN. On the other hand, if the application delay is huge, then some application fine-tuning might provide further benefits in addition to the server offloading that some of the WAN optimization techniques might offer.

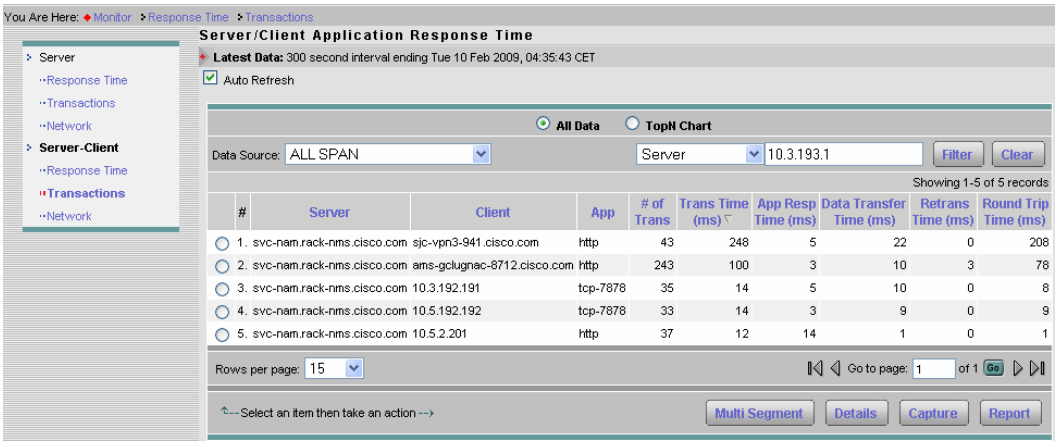
2. Select the **Top N** radio button and select **Average Application Delay** from the drop-down list. This will provide insights into which servers are most heavily loaded and have the maximum average latency (Figure 17).

Figure 17. Average Application Delay Shows Which Servers Are Most Heavily Loaded



3. Now select **Monitor > Response Time > Server-Client Transactions**. You can again filter on the Server IP address. This will help us identify which sites are experiencing poor performance and where WAN optimization would yield the maximum benefits (Figure 18).

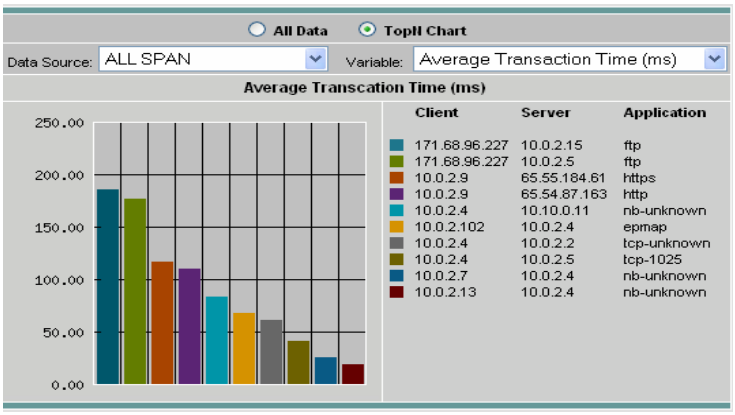
Figure 18. The Server/Client Application Response Time



What we see in Figure 18 is that the first client in the list is experiencing far poorer performance based on the transaction time (average), which is 248 ms averaged over 43 transactions. The average application response time is just 5 ms, so that is not a contributor to the problem. The round-trip time (which is the acknowledgement delay time and is a good indicator of the delay introduced by the WAN when the NAM is in the data center), shows that the WAN is contributing significantly to the poor performance.

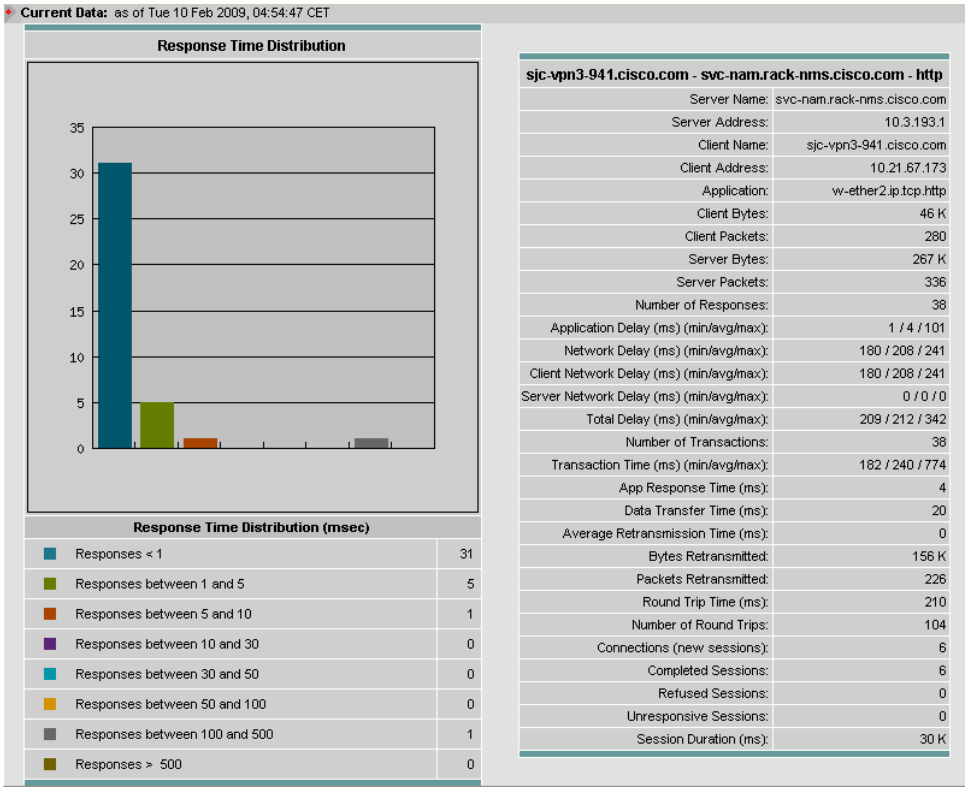
4. Select the **Top N** radio button and select **Average Transaction Time** from the drop-down list to view the chart that can provide insights into which site (client) is experiencing poor transaction time for which application (Figure 19).

Figure 19. The Average Transaction Time Report



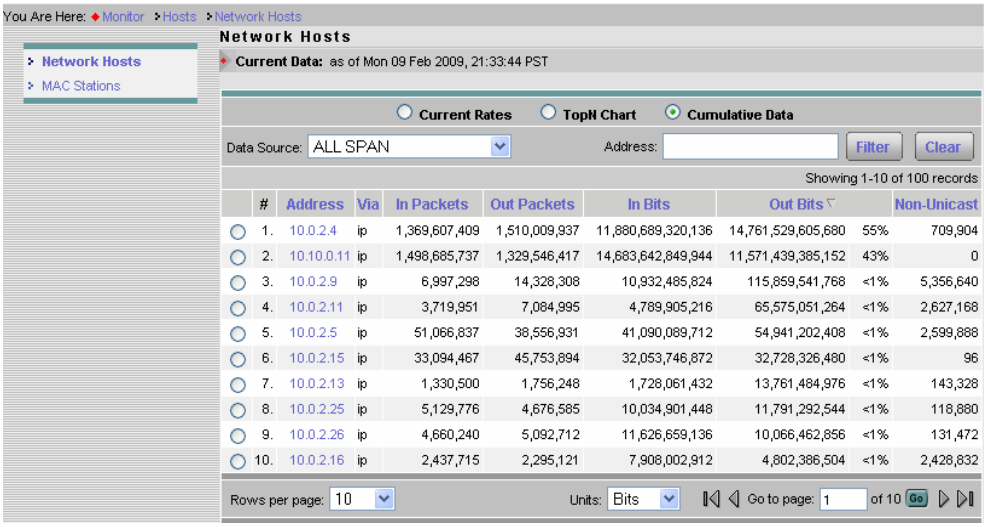
5. Click the **All Data** radio button and select the server, client, and application you want to baseline and click **Details**. This provides about 45 different metrics related to the server and a test client at a target branch related to the chosen application (Figure 20). Average transaction time is a good indication of the end-user experience and should be recorded.

Figure 20. Metrics Related to the Selected Server, Client Pair



6. We can also determine the bandwidth usage per host by selecting **Monitor > Hosts** and selecting the **Cumulative Data** radio button (Figure 21).

Figure 21. Bandwidth Usage per Host

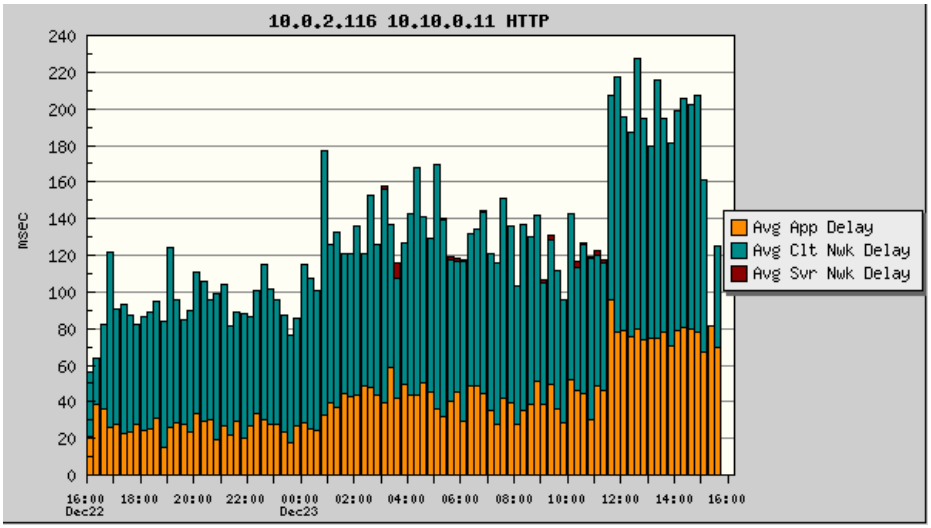


Note: The host view can provide traffic volume values that are larger than those reported by the WAE. As an example, if the server serves UDP and TCP traffic, and only TCP is being monitored by WAEs, the host report would include also the UDP traffic. Selecting a host and clicking **Details** will show the application distribution for that host.

Historical Reports for Evaluating Application Performance

1. Go to **Monitor > Response Time > Server-Client Response Time**. Select the server, client, and application you want to baseline and click Report. This starts a historical report for the average application delay, average client network delay, and average server network delay. Let the report run for a period of 24 hours, so we can understand the performance trend over the course of a day.
2. Select **Reports > Basic Reports**. Select the **Avg App Delay**, **Avg Clt Nwk Delay**, and **Avg Svr Nwk Delay** reports and click **View**. Set the style to **Stack Bar** (Figure 22).

Figure 22. Report of Average Delay for Application, Client Side Network, and Server Side Network



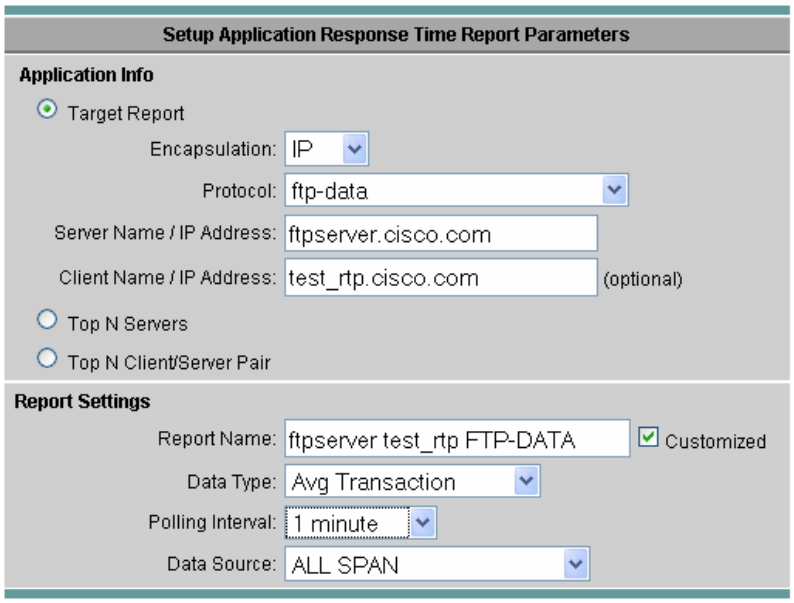
The graph in Figure 22 can provide insights into periods of the day when application performance drops and whether the drop is due to the server load or to network congestion. It can help determine whether latency issues are transient and the time periods when the biggest gains from optimization might be seen.

Configuring Response Time Reports for Impact Analysis

Set up a historical report for the average transaction time.

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 **Avg Transaction** as the **Data Type** and select **ALL SPAN** as the **Data Source** (where this traffic is seen), and set the appropriate **Polling Interval**. This can be as low as 1 minute. See Figure 23.

Figure 23. Setting Up the Application Response Time Report



This report will be useful for creating a WAAS before and after report.

Configuring Conversation Throughput Reports for Impact Analysis

The conversation throughput report can show the reduction in the bandwidth utilized after optimization.

1. Click **Reports > Basic Reports**.
2. Click **Create** and select **Conversations**.
3. Enter the host names for the IP server and the IP client and, if needed, the application information.
4. Select **Bit/Sec** as the **Data Type**, set the appropriate polling interval (as low as 1 minute), and select **SPAN** as the **Data Source**.
5. From **Reports > Basic Reports**, you can check multiple reports and then select **View** to provide a composite report.

This report will be useful to create a WAAS before and after report.

Configuring NAM-WAAS Integration

This section discusses how to enable WAAS to send flow information to the NAM and how to generate before and after reports to demonstrate the impact of WAAS.

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.

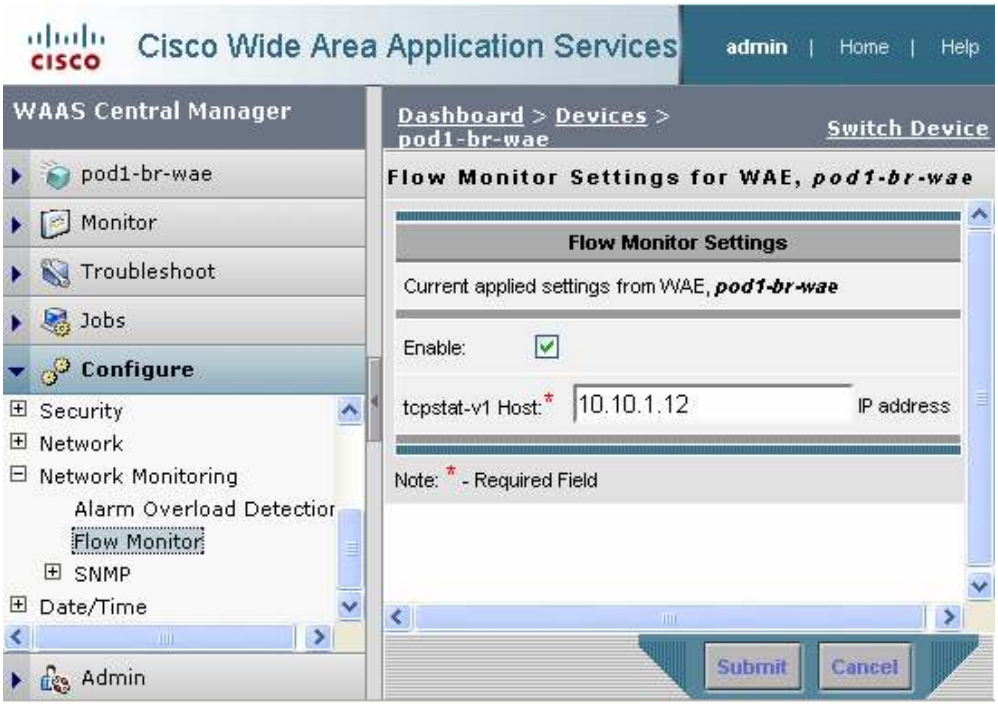
To configure the WAAS device to export the flow record data, use the WAAS CLI **flow monitor** command as follows:

```
config t
no flow monitor tcpstat-v1 enable
flow monitor tcpstat-v1 host  <NAM-IP-ADDRESS>
flow monitor tcpstat-v1 enable
end
```

Alternately, you can use the WAAS Central Manager graphical user interface (GUI):

From **Configure > Network Monitoring > Flow Monitor**, enter the NAM IP address and enable flow monitoring (Figure 24).

Figure 24. Enabling Flow Monitoring with the WAAS GUI

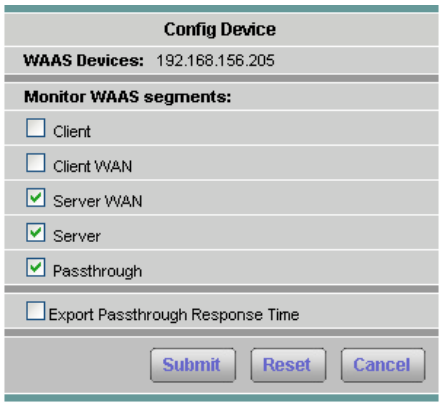


After you enable flow export to the NAM using WAAS CLI commands or the WAAS GUI as above, WAAS devices will be detected and automatically added to the NAM's WAAS device list.

Configuring the WAAS Data Source in NAM

1. Log in to the NAM GUI.
2. Click **Setup > Data Sources**.
3. From the contents menu, choose **WAAS -- Devices**.
4. Choose the WAAS device you want to modify, then click **Config** (Figure 24).

Figure 25. Configuring a WAAS Data Sources



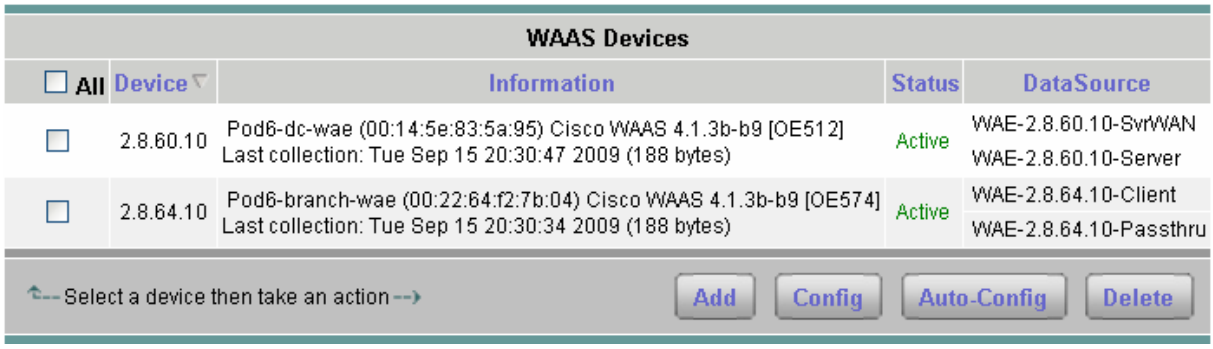
5. You can configure WAAS to monitor the following WAAS segments or WAAS data sources (data collection points):
   - **Client:** This setting configures the WAE device to export the original (LAN side) TCP flows from/to the clients to NAM for monitoring. Set this on the branch side WAE.
   - **Client WAN:** This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to NAM for monitoring. Set this on the branch side WAE if the NAM is located close to the branch.
   - **Server WAN:** This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to NAM for monitoring. Set this on the Core WAE if the NAM is close to the data center.
   - **Server:** This setting configures the WAE device to export the original (LAN side) TCP flows from/to the servers to NAM for monitoring. Set this on the core WAE.
   - **Passthrough:** Set this on the branch side or core WAE if you wish to gain visibility into passthrough flows.
6. With NAM in the data center (NAM-2 or the NAM 2200 appliance), configure the following (see figure 26):

   Branch WAE data source: Client, Passthrough

   Core WAE data source: Server, ServerWAN

Note: SPAN data sources might take the place of the server data source. For example, if you already configured SPAN to monitor the server LAN traffic, it is not necessary to enable the server data source on the WAE device.

Figure 26. WAAS Data Sources



7. Click **Setup > Monitor** and make sure that **Core Monitoring** and **Response Time Monitoring** are selected for the WAE data source.

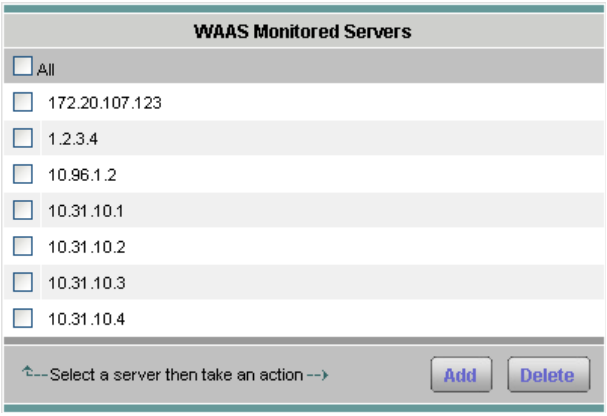
Note: The status will remain Pending until the monitored servers are configured (as described in the next section) and the NAM starts receiving the flows from the WAE.

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. Figure 12 and Figure 13 can be used to help identify these business-critical applications and the servers that host them.

1. Click **Setup > Data Sources**.
2. From the contents menu, choose **WAAS > Monitored Servers** (Figure 27).
3. Click **Add** and enter the test server IP address in the Server Address field.

Figure 27. Adding a WAAS Monitored Server Address



Configuring Response Time Reports for WAAS 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 from the branch WAE. This report will provide visibility on response time improvement as experienced by the branch when combined with the transaction time report from the SPAN data source.

1. Click **Reports > Basic Reports**.
2. Click **Create** and select **Response Time**.
3. Enter the application information for the application and the server.
4. Select **Avg. Transaction** as the **Data Type** and select **WAE-<BranchWAE-IP>-Client** as the **Data Source**. The **Polling Interval** can be set as low as 1 minute.
5. From **Reports > Basic Reports**, check multiple reports and then select **View** to provide a composite report.

Configuring Conversation Throughput Reports for WAAS Impact Analysis

The conversation throughput report can show the reduction in the bandwidth utilized after optimization.

1. Click **Reports > Basic Reports**.
2. Click **Create** and select **Conversations**.
3. Enter the host names for the IP server and the IP client and if needed the application information.

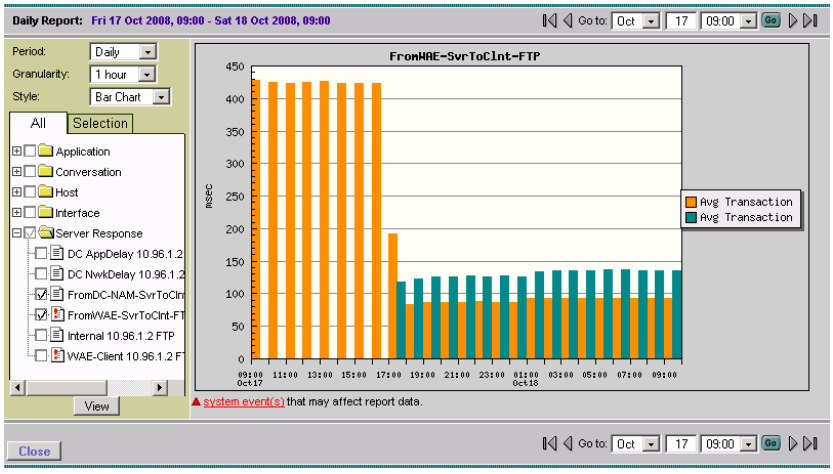
4. Select **Bits/Sec** as the **Data Type**, set the appropriate polling interval (which could be as low as 1 minute), and select **WAE-<CoreWAE-IP>-ServerWAN** as the **Data Source**.
5. Now repeat the above steps and select WAE-<BranchWAE-IP>-Client as the Data Source.
6. From **Reports > Basic Reports**, you can check multiple reports and then select **View** to provide a composite report.

Generating WAAS Before and After Reports

This section will discuss how to generate WAAS before and after reports.

1. Click **Reports > Basic Reports** and select the **Avg Transaction** report for the same server, client, and application from the SPAN data source in the data center (Orange) created in the "Configuring Response Time Reports for Impact Analysis" section and from the WAE client data source from the branch (Blue) created in the "Configuring Response Time Reports for WAAS Impact Analysis" section and click **View**. Set the style to **Bar Chart**. This will bring up the composite report indicating the average transaction time reduction, which is an indication of the end-user experience improvement (Figure 28).

Figure 28. A Composite Report Showing Average Transaction Time Reduction



Note: The average transaction time before WAAS was ~430 ms. After WAAS is enabled, the WAE client data source starts up and the average transaction time has dropped to ~120 ms.

2. Select **Reports > Basic Reports** and select the **Conversation - Bytes** report created in the "Configuring Response Time Reports for Impact Analysis" and "Configuring Conversion Throughput Reports for WAAS Impact Analysis" sections. You can also select the **Avg Transaction** reports created for SPAN and WAE client data sources for the same server-client pair. Click **View**. Chose the **Bar Chart** style (Figure 29).

Figure 29. Transaction Reports for SPAN and WAE Client Data Sources

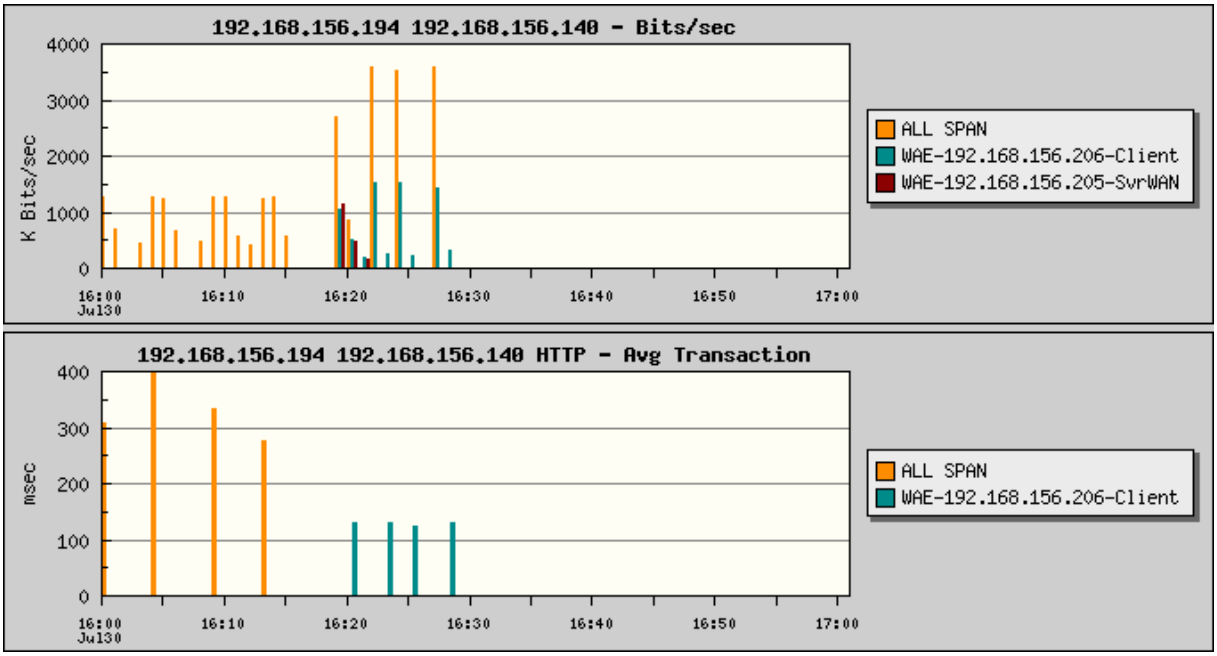


Figure 29 is the report for a test conducted with transferring a 12 MB file from the data center to a branch. Note that before WAAS was enabled the traffic rate was limited by the WAN bandwidth as seen from SPAN. The file also took longer to transfer from server to client. After WAAS is enabled, we observe the new WAE data sources. We also see the file transfer across the WAN in maroon. However, after the first time, caching kicks in and file transfer across the WAN is eliminated. We observe the core WAE requesting the file from the server and verifying the cache and then the branch WAE sending the file across to the client. In the bottom half of the report, we see the transaction time reduction from an average of 300 ms to 120 ms after WAAS is enabled.

3. Click **Monitor > Response Time**. Under **Server-Client**, select the conversation and click **Multi Segment**. This report will show the network delay introduced by the three segments; you can check the data redundancy elimination (DRE) effects by looking at the traffic volume values (Figure 30).

Figure 30. Response Time Across Multiple Segments

Response Time across Multiple Segments (Data Sources)

Individual Data Source View Correlated WAAS Segment View

Server: 192.168.156.230 Client: 192.168.156.140 Application: http Filter Clear

Showing 1-1 of 1 records

#	Branch	Server	Client	App	Network Delay (ms)			App Delay (ms)	Total Delay (ms)	Transaction Time (ms)		Traffic Volume (bits)		
					Client	WAN	Server			Avg	Max	Client	WAN	Server
1.	WAE-192.168.156.206	192.168.156.230	192.168.156.140	http	0	80	1	7	95	116	464	2,187,168	149,680	2,187,152

Rows per page: 100 Go to page: 1 of 1 Go

Summary

As we have seen in this document, the NAM is able to collect and analyze information from various data sources, such as, SPAN, NetFlow, and the embedded instrumentation on WAE to provide insights into various stages of WAAS POC and deployment. The NAM's real-time monitoring, historical reporting, and application performance analytics can be used to gain visibility into optimization opportunities and for baselining application performance, understanding the impact of WAN optimization, and ongoing troubleshooting.

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 C07-584729-00 02/10