Configuring the Network Analysis Module

This chapter provides information about the integration of the Cisco Network Analysis Module (NAM) in the Wide Area Application Services (WAAS) Central Manager and describes how to configure and use the NAM.

This chapter includes the following sections:

Information About NAM Integration

Cisco WAAS is enhanced with application performance-monitoring capabilities when you integrate the Cisco WAAS Central Manager with the NAM Traffic Analyzer software.

The NAM Traffic Analyzer software enables network managers to understand, manage, and improve how applications and services are delivered to end users by combining flow-based and packet-based analysis into one solution. With the NAM, you can perform traffic analysis of applications, hosts, and conversations, make performance-based measurements on application, server, and network latency, and use Quality of Service (QoS) metrics for network-based services and problem analysis using packet captures. The NAM includes an embedded, web-based Traffic Analyzer GUI that provides quick access to the configuration menus and presents easy-to-read performance monitoring and analysis on network traffic.

The architecture for WAAS Central Manager and NAM integration allows you to deploy NAM 5.1 in any form factor such as physical blade, or appliance.

Prerequisites for NAM Integration

The NAM integration has the following prerequisites:

- Cisco WAAS 4.4.1 or later Central Manager is installed and configured.
- The NAM 5.1 hardware and software are installed.
- The following configurations are performed:

  - HTTP or HTTPS is enabled.
  - An admin web user account is created.
  - A MonitorView web user account is created.
- Both the WAAS Central Manager and the client computer from which you connect to the Central Manager must be able to access the configured NAM server on the network.

For more information, see the *Cisco Catalyst 6500 Series Network Analysis Module (NAM 3) Installation and Configuration Guide*, or the *Cisco Prime Network Analysis Module (NAM) for ISR G2 SRE Installation and Configuration Guide*.

Guidelines and Limitations for NAM Integration

The NAM integration feature has the following configuration guidelines and limitations:

Supported Deployments

In WAAS v6.0.1 and later, the following types of deployments are supported:

- POC deployments
- Small and medium production networks that can be monitored by one instance of NAM (physical blade, or appliance). In this release, only one NAM instance is supported, which means that large enterprises that require more than one NAM instance to handle their network capacity must be managed separately without the WAAS-CM integration.

Limitations

- Certain browser settings can limit the functionality of the NAM integration. For example, if Internet Explorer privacy settings are set to the default, Medium, the integration does not work because of cookie restrictions. Specify the privacy settings as Low.
- When you print the NAM windows in PDF format, they do not produce the desired output.
- When duplicate data is reported by multiple WAE data sources, the NAM does not automatically remove duplicate data. Use the Data Source selector in the dashboards and charts to address this limitation.

Configuring the NAM

This section includes the following topics:

Task Flow for Configuring the NAM

This section includes the following topics:

Basic Configuration

The basic NAM configuration includes the following tasks:

- Configuring the setup (see Configuring the Basic Setup).
  - Connect to a NAM server by providing the server's IP address, protocol, and port.
  - Establish account credentials.
  - Associate a WAAS device group or WAAS Express device group with configured policies.
  - Enable Flow Agent.
- Configuring Sites—To display accurate data on charts and dashboards, every site on which WAAS is planned to be deployed must be configured on the NAM (see Configuring a Site).
  - Define sites
  - Use definition rules
  - Specify sites using subnets
- Configuring monitored servers (see Configuring a Cisco WAAS-Monitored Server).
  - Specify the servers to be monitored by the NAM using the WAAS device's flow monitoring.
  - Enabling NetFlow and flow agent data sources on the actual devices, with the NAM as the collector, to automatically create the device entries in the NAM.

Advanced Configuration

Advanced NAM configuration includes the following tasks:

- Configuring and synchronizing user-defined Classifiers and Applications with the NAM (see Synchronizing Classifiers and Applications).
- Creating and editing an auto-created WAAS data source to monitor WAAS traffic statistics (see Configuring a Data Source).
- Changing system preferences (see Setting Preferences for a NAM Module).
- Launching the NAM user interface (see Launching the NAM User Interface).

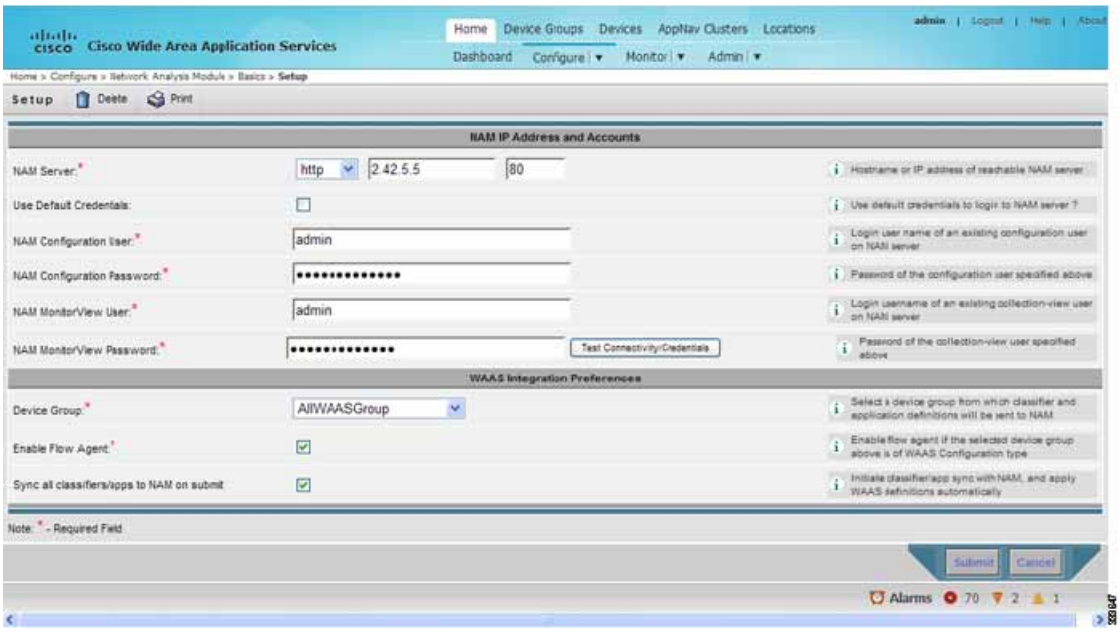
Configuring the Basic Setup

Only device group-level policy configurations are applicable for NAM.

Step 1 From the WAAS Central Manager menu, choose **Configure > Network Analysis Module > Basics > Setup**.

The Setup window appears (Figure 14-1). This window allows you to configure the NAM IP address and accounts.

Figure 14-1 Setup Window



Step 2 In the NAM Server area, provide the following information:

- Choose either **http** or **https** depending on the access that was configured during the installation of NAM.
- Enter the hostname of the NAM server.
- Enter the IP address of the NAM server.

To set up a site or sites on the NAM module, perform the following steps:

Step 3 To use the pre-configured login credentials to access the NAM server, select the **Use Default credentials** option. Proceed to Step 8.

The following preconfigured login credentials are used the Central Manager:

- Configuration user:
  - Username—admin
  - Password—admin
- MonitorView user:
  - Username—waasro
  - Password—waasrao

Note These credentials work only if you have configured the NAM with these details explicitly after installation.

Step 4 In the **NAM Configuration User** field, enter the username of an existing configuration user on the NAM server.

Step 5 In the **NAM Configuration Password** field, enter the password of the configuration user that was specified in Step 4.

Step 6 In the **NAM MonitorView User** field, enter the username of an existing collection-view user configured on the NAM server.

Step 7 In the **NAM MonitorView Password** field, enter the password of the existing collection-view user that you specified in Step 3.

Step 8 Click the **Test Connectivity/Credentials** button, to verify if the NAM server is accessible and to check if the user credentials that you specified are valid.

Step 9 The WAAS Integration Preferences area allows you to configure a WAAS device group to work with the NAM server:

a. From the **Device Group** drop-down list, choose a device group from which Cisco WAAS applications and classifier definitions are pushed to the NAM when performing a synchronization operation.

The AllWAASDevices or AllWAASExpressDevices device group is the default selection for POC deployments. For production deployments, choose a suitable device group with a subset of devices for which you require the NAM integration and APM functionality.

b. Check the **Enable Flow Agent** check box to enable sending flow agent reports from the Cisco WAAS devices in the selected device group to NAM.

This check box is disabled for the WAAS Express device group because WAAS Express does not support the flow agent or flow monitor. In this scenario, you must use a NAM Performance Agent (PA) from Cisco IOS routers to view the response-time metrics. The NAM charts that display response times in the Central Manager also automatically handle the PA from routers.

c. Check the **Sync all classifiers/apps to NAM on submit** check box to initiate a classifier and application synchronization with NAM and to apply Cisco WAAS definitions automatically.

Step 10 Click **Submit**.

Configuring a Site

A site is a collection of hosts—or network endpoints—partitioned into views that help you to monitor traffic and troubleshoot problems. These views allow you to see measurements of application performance on networks where Cisco WAAS devices are deployed and dashboards that show the traffic levels between sites and alarm levels per site. You can use other NAM features without defining any sites (the default configuration).

If you have set up sites, you can choose a particular site to view in the Interactive Report and view data relevant to that site only. In some cases, you can select both a client site and a server site to view data that pertains to the interaction between hosts at different sites.

Note If you configure multiple data sources for the same site, the same traffic might be accounted for more than once, which results in inflated traffic statistics. For example, if you configure the NAM to receive SPAN traffic for a particular site, and it is also receiving NetFlow records for that same site, both SPAN traffic and NetFlow records are combined into the traffic statistics. In this case, if you want to see only the statistics for a particular data source, use the Interactive Report window on the left side of the Sites window to specify both the site and data source.

Note Classification of received data from data sources to sites is done only after the sites are configured. Any old data from these data sources (before the sites were configured) are counted under the default 'Unassigned' site.

The site definition is very flexible and can accommodate various scenarios. It is used not only for viewing data, but for data export and data retention as well. Typically, a site is defined by its subnets, but a site can also be defined using the following rules:

- Subnet (IP address prefix)
- Subnet from a data source
- Subnet from a given VLAN of a SPAN data source
- WAE device serving the site

We recommend that you define sites using subnets whenever possible.

Note The same rule cannot be defined in multiple sites.

Note If you are configuring a Cisco WAAS device, you must add the Cisco WAAS servers to the NAM. See Auto Creating a New WAAS Device.

To display accurate data on charts and dashboards, you must configure every site on which Cisco WAAS is to be deployed on the NAM. To get a breakdown of the traffic volume and response time for each branch and data center, configure the IP subnets for all the sites that have WAAS deployed.

This section includes the following topics:

Definition Rules

Typically, subnets alone are sufficient to define a site, for example:

```
Site Data-Center = subnet 172.20.0.0/16
```

In certain scenarios, when there are overlapping IP address spaces in the networks (for example, in private networks where hosts from different sites have the same IP addresses), you can use data sources or VLANs to differentiate the subnets, for example:

```
Site NewYork = subnet 10.11.0.0/16 from "NDE-NewYork" data source.
Site LosAngeles = subnet 10.11.0.0/16 from "NDE-LosAngeles" data source.
Site Sale-Dept = subnet 10.11.0.0/16 from VLAN 10 of "DATA PORT 1" data source.
Site Finance-Dept = subnet 10.11.0.0/16 from VLAN 12 of "DATA PORT 1" data source.
```

This section includes the following topics:

- Specifying a Site Using WAE devices (Cisco WAAS Data Sources)
- Specifying a Site Using Multiple Rules
- Resolving Ambiguity (Overlapping Site Definitions)

Specifying a Site Using WAE devices (Cisco WAAS Data Sources)

For WAAS traffic, you can define a site associated with a WAE device without specifying the site's subnets. Simply select all of the WAAS data sources coming from the WAE devices serving that site.

```
Site SanJose = WAE-SJ-Client, WAE-SJ-CltWAN, and WAE-SJ-Passthrough data sources.
```

Note We recommend that you use subnets to specify WAAS-optimized sites. Use this method only if the site's subnets cannot be determined.

Specifying a Site Using Multiple Rules

You can define a site using a combination of multiple rules, as described in Definition Rules. For example, if a site has both optimized and nonoptimized traffic, it can be defined using a combination of WAAS data sources and a subnet from a NetFlow Data Export (NDE) data source.

When you define a site using multiple data sources, ensure that those data sources do not have duplicated traffic to avoid counting the site traffic statistics twice.

Resolving Ambiguity (Overlapping Site Definitions)

Conflicting rules are not allowed in site definitions. Of the following two scenarios, the second one is not allowed:

- 1.2.3.0/24 from SPAN1 = SiteA
- 1.2.3.0/24 from SPAN1 = SiteB

Using a prefix is the preferred method. The data source and VLAN are secondary. In the following two scenarios, the first receives higher priority:

- 1.2.3.0/24 = Site D
- WAE1-Client datasrc = Site E

The longest prefix has higher priority. It has the same data source and VLAN. In the following two scenarios, the first receives higher priority:

- 1.2.3.0/24 from SPAN1 = Site A
- 1.2.0.0/16 from SPAN1 = Site C

The more refined (specific) rule has higher priority. In the following two scenarios, the first receives higher priority.

- 1.2.3.0/24 from SPAN1 = Site A
- 1.2.3.0/24 (any datasrc) = Site D

Viewing Defined Sites

To view a defined site, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Configure > Network Analysis Module > Basics > Sites**.

The Sites window appears. The defined sites are listed in a table.

The following details are displayed:

- Name—Lists the name of the site.
- Description—Describes what the site includes.
- Rule—Lists the first rule that is assigned to the selected site. If you see ellipsis (...) next to the site rule, it means that multiple rules are created for that site. To see all the rules, click the **quick view** icon (after highlighting the site, click the small arrow on the right).
- Status—Shows if the site is enabled or disabled.

Defining a Site

To define a site, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Configure > Network Analysis Module > Basics > Sites**.

The Sites window appears. This window lists the sites that are set up on the NAM module.

Step 2 Click **Create**.

The Sites Configuration window displays.

Step 3 In the **Name** field, enter a name for the site.

Step 4 In the **Description** field, enter a description for the site.

Step 5 Check the **Disable Sites** check box if you want the NAM to skip this site when classifying traffic. This feature is useful if the site is no longer active, but you would still like to access historical site data in the database. Otherwise, you should delete sites that are not needed.

Step 6 In the **Subnet** field, enter the IP address subnet (IPv4 or IPv6 address and mask); for example, 10.1.1.0/24.

Step 7 Click the blue **i** to get information about the site rules.

Step 8 Click **Detect** to tell the NAM to look for subnets in the traffic. See Detecting a Subnet.

Step 9 In the **Data Source** field, specify the data source from where the site traffic is coming from.

Note Leave this field blank if the site traffic is coming from multiple data sources.

Step 10 In the VLAN field, specify the VLAN where the site traffic is coming from. This field is not valid for NDE and WAAS data sources.

Leave this field blank if the site traffic can come from multiple VLANs.

Step 11 Click **Submit**.

Note The Unassigned site (with a description of Unclassified hosts) includes sites that do not match any of your site configurations. Sites are classified at the time the packets are processed.

Detecting a Subnet

To detect a subnet, follow these steps:

Step 1 Choose **Configure > Network Analysis Module > Basics > Sites > Sites Configuration**.

Step 2 In the Sites Configuration window, click **Detect**.

The NAM looks for subnets detected within the past hour and the Subnet Configuration window is displayed. This window allows you to specify the details of the sources in which you want NAM to detect subnets.

Step 3 In the **Subnet Mask** field, enter the subnet mask.

Note If the bit mask is less than 32, the NAM detects an IPv4 subnet. If the bit mask is between 32 and 64, the NAM detects an IPv6 subnet.

Step 4 From the **Data Source** drop-down list, choose the data source in which you would like to detect subnets.

Step 5 From the **Interface** drop-down list, choose the interface in which you would like to detect subnets.

Step 6 In the **Filter Subnets within Network** field, enter an IPv4 or IPv6 address.

Step 7 Check the **Unassigned site** check box to include sites that do not match any of your site configurations. Sites are classified at the time of packet processing.

Step 8 Click **Detect**.

The NAM finds the subnets that meet the criteria that you entered.

Editing a Site

To edit sites that have been created, follow these steps:

Note The Unassigned site cannot be edited or deleted.

Step 1 Choose **Configure > Network Analysis Module > Basics > Sites**.

A list of configured sites is displayed.

Step 2 Select the site that you want to edit.

Step 3 Click **Edit**.

The Site Configuration window displays.

Step 4 Edit the required field (**Name**, **Priority**, **Data Sources**, or **Prefix/Mask**).

Step 5 Click **Submit**.

Deleting a Site

To delete sites that have been created, follow these steps:

Note The Unassigned site cannot be deleted.

Step 1 Choose **Configure > Network Analysis Module > Basics > Sites**.

A list of configured sites is displayed.

Step 2 Select the site that you want to delete.

Step 3 Click **Delete**.

Configuring a Cisco WAAS-Monitored Server

Cisco WAAS-monitored servers specify the servers from which WAAS devices export traffic flow data to the NAM monitors. To enable WAAS monitoring, you must list the servers to be monitored by the NAM using the WAAS device's flow monitoring.

Note The NAM is unable to monitor WAAS traffic until you set up Cisco WAAS-monitored servers. The NAM displays the status of Cisco WAAS devices as pending until you set up Cisco WAAS-monitored servers.

This section includes the following topics:

Adding a Cisco WAAS-Monitored Server

To add a Cisco WAAS-monitored server, follow these steps:

Step 1 Choose **Configure > Network Analysis Module > Basics > Monitored Servers**.

The WAAS Servers window appears.

Step 2 Choose **Select All** to add all the servers, or select the required servers from the list.

Step 3 Click **Add**.

Deleting a Cisco WAAS-Monitored Server

To delete a Cisco WAAS-monitored server data source, follow these steps:

Step 1 Choose **Configure > Network Analysis Module > Basics > Monitored Servers**.

The WAAS Servers window is displayed.

Step 2 Choose the monitored WAAS server to delete, and click **Delete**.

A confirmation dialog box asks you if you want to delete the selected Cisco WAAS-monitored server.

Step 3 Click **OK** to delete the Cisco WAAS-monitored server.

Synchronizing Classifiers and Applications

You can synchronize the WAAS classifier and application definitions with the application and application groups in the NAM. A classifier and an application in WAAS are equivalent to an application and application group respectively in the NAM. WAAS applications and classifier definitions from the device group specified during the setup configuration are matched with those in the NAM server that WAAS is connected to. WAAS classifiers can contain source and destination IP addresses while the NAM recognizes an application on the basis of port numbers. Hence, only the WAAS classifiers that contain port numbers are synchronized.

To view the results of the synchronization, follow these steps:

Step 1 Choose **Configure > Network Analysis Module > Advanced > Classifier/App Sync**.

The **Classifier/App Sync Preferences** window appears.

The Classifier/AppSync Preferences results are displayed under the following categories:

- Conflicting classifiers/applications—You can choose one or all the WAAS classifiers and applications for synchronization with the NAM. By default, all the classifier and applications are selected.
- NAM-only applications/application groups—Applications and application groups in the NAM are displayed. If required, you can manually add the NAM-only applications and application group definitions in WAAS at the device-group or device levels.

Step 2 To view the differences in classifier definitions in WAAS and the NAM, click on the arrow next to **Classifier Definition Differences**.

Step 3 Choose the WAAS classifiers that you want to synchronize with the NAM applications and provide the required information to define the filter criteria.

Step 4 Click **Go**.

The differences in the definitions are displayed.

Step 5 To view applications and application groups in the NAM, click on the arrow next to **NAM-Only Applications**. Information about the applications and application groups is displayed. If required, you can manually add these definitions in WAAS at the device-group or device levels.

Step 6 To refresh the Classifier/App Sync page, click **Refresh**.

Step 7 Click **Submit** to start the synchronization process.

Configuring a Data Source

Data sources are the source of traffic for the NAM Traffic Analyzer. Some examples of this are physical data ports of the NAM, where you get SPAN (Switched Port Analyzer) data, a specific router or switch that sends NetFlow to the NAM, or a WAAS device segment that sends data to the NAM or ERSPAN (Encapsulated Remote Switched Port Analyzer) and that goes to the NAM's management port.

A new feature in NAM 5.0 is the auto discovery of data sources, using which you can click **Auto Create** so that the NAM can automatically discover the data sources. You can see details such as the IP addresses of devices that send packets to the NAM and the time at which the last NDE packet was received (in NAM 4.x, this feature was called Listening Mode).

Note If you have configured sites, you can assign data sources to that particular site. If you do assign data sources to a site, and you also configure the data sources, the two could overlap because sites can also be a primary view into data sources. If there is a mismatch between the two, you will not see any data.

Note We recommend that you configure a site using subnets instead of selecting a data source.

The following areas contain specific information about the types of data sources:

- SPAN
- ERSPAN
- VACL
- NetFlow
- WAAS

The NAM Data Sources window lists the data sources that are configured for that NAM module, and contains the following fields:

- Device—DATA PORT if it is a local physical port or the IP address of the learned device.
- Type—The source of traffic for the NAM.
  - DATA PORT if it is a local physical port.
  - WAAS, ERSPAN, or NETFLOW if a data stream is exported from the router, switch, or WAE device.
- Activity—Most recent activity.
- Status—ACTIVE or INACTIVE.
- Data Source—Name given to the data source.
- Data Source Details—Physical Port, or information about the data source being enabled or disabled.

This section includes the following topics:

Adding a Data Source for a New WAAS Device

The NAM uses WAAS data sources to monitor traffic that is collected from different WAAS segments: Client, Client WAN, Server WAN, Server, and Passthrough. Each WAAS segment is represented by a data source. You can set up the NAM to monitor and report other traffic statistics of the WAAS data sources, such as application, host, and conversation information in addition to the monitored Response Time metrics.

Adding a WAAS device is not usually necessary because export-enabled WAAS devices are detected and added automatically.

To manually add a WAAS device to the list of devices monitored by the NAM:

Step 1 Choose **Configure** > **Network Analysis Module** > **Advanced** > **Data Sources**.

Step 2 Click **Create**.

The NAM Data Source Configuration dialog box is displayed.

Step 3 Choose **WAAS** from the **Types** drop-down list.

Step 4 In the **IP** field, enter the device IP address.

Step 5 Check the check boxes pertaining to the appropriate WAAS segments.

You can configure the WAAS data sources to monitor the following WAAS segments:

- Client—Configures the WAE device to export the original (LAN side) TCP flows that originated from its clients to the NAM for monitoring.
- Client WAN—Configures the WAE device to export the optimized (WAN side) TCP flows that originated from its clients to the NAM for monitoring.
- Server WAN—Configures the WAE device to export the optimized (WAN side) TCP flows from its servers to the NAM for monitoring.
- Server—Configures the WAE device to export the original (LAN side) TCP flows from its servers to the NAM for monitoring.
- Passthrough—This setting configures the WAE device to export the TCP flows that are passed through unoptimized.

Step 6 Click **Submit** to add the new WAAS custom data source.

Auto Creating a New WAAS Device

If you have numerous WAE devices, you can set up the NAM to configure newly discovered WAE devices using a predefined configuration template using the NAM Auto Config option.

Note If most of your WAE devices are edge WAE devices, you might want to set the **auto config** option as an edge device, and manually configure the data center WAE, for example, choose the **Client** segment for monitoring.

To auto create a new WAAS device, follow these steps:

Step 1 Choose **Configure** > **Network Analysis Module** > **Advanced** > **Data Sources**.

Step 2 The Data Sources window is displayed.

Step 3 Click **Auto Create**.

The NAM Data Source Configuration dialog box appears.

Step 4 Check the **WAAS** check box.

Step 5 Check the check boxes pertaining to the required segments. See Adding a Data Source for a New WAAS Device, for more information.

Step 6 Click **Submit** to add the new WAAS custom data source.

Editing a WAAS Data Source

To edit a WAAS device's custom data source, follow these steps:

Step 1 Choose **Configure** > **Network Analysis Module** > **Advanced** > **Data Sources**.

The Data Sources window is displayed.

Step 2 Select the WAAS device that you want to modify, and click **Edit**. The NAM Data Source Configuration dialog box is displayed.

Step 3 Modify the segments as required.

Step 4 Click the **Edit** button to edit the WAAS custom data source.

Deleting a WAAS Data Source

To delete a WAAS custom data source, follow these steps:

Step 1 Choose **Configure** > **Network Analysis Module** > **Advanced** > **Data Sources**.

The data sources window is displayed.

Step 2 Select the WAAS custom data source that you want to delete, and click **Delete**.

A confirmation dialog box asks you to confirm that you want to delete the selected WAAS monitored server.

Step 3 Click **OK** if you want to proceed with a deletion of the WAAS custom data source.

Setting Preferences for a NAM Module

You can configure characteristics such as NAM display, audit trail, and file format preferences for a NAM module.

Step 1 Choose **Configure** > **Network Analysis Module** > **Advanced** > **Preferences**.

The Preferences window is displayed.

Step 2 Specify the following preferences:

- **Refresh Interval** (60-3600 sec)—Amount of time between the refresh of information on dashboards.
- **Top N Entries** (1-10)—Number of colored bars on the Top N charts.
- **Perform IP Host Name Resolution**—Wherever an IP address appears, it gets translated to a hostname via a DNS lookup.
- **Data Displayed In**—Data displayed in Bytes or Bits.
- **International Notation**—Choose the way you would like the numbers to appear.
- **Audit Trail**—The Audit Trail option displays a listing of recent critical activities that have been recorded in an internal syslog log file. Syslog messages can also be sent to an external log.

Step 3 Click **Submit** to save your configurations.

Launching the NAM User Interface

You can launch the NAM user interface to perform advanced configuration and monitoring tasks.

To launch the NAM user interface:

Choose **Configure > Network Analysis Module > Advanced > Launch NAM GUI**.

A new window or a tab (depending on your browser settings) opens, displaying a NAM session that uses the existing login credentials.

Monitoring and Analyzing Traffic

The monitoring and analyzing traffic feature provides intuitive workflows and interactive reporting capabilities.

The monitoring and analyzing dashboards allow you to view network traffic, application performance, site performance, and alarms at a glance.

This section provides information about monitoring your network traffic and analyzing the information presented, and contains the following topics:

Navigation

This section includes the following topics:

Interactive Report

On most monitoring dashboards, you can use the Interactive Report on the left column to redefine the parameters of the information displayed in the dashboards. Click the **Filter** button to change the parameters of the information that appears in the charts.

You can choose from various parameters, such as the time interval for the data being displayed.

Note An asterisk represents required fields.

The reporting-time interval selection changes depending upon the dashboard that you are viewing, and the NAM platform that you are using:

- The NAM appliance supports the following short term intervals: Last 5 minutes, last 15 minutes, last 1 hour, last 4 hours, and last 8 hours.
- The Branch Routers (NME-NAM) support the following short term intervals: Last 5 minutes, last 15 minutes, and last 1 hour.
- The other platforms support the following short term intervals: Last 5 minutes, last 15 minutes, last 1 hour, and last 4 hours.
- The Long Term interval selections (Last 1 day, 1 week, and 1 month) are disabled from the following dashboards: RTP Streams, Voice Call Statistics, Calls Tables, RTP Conversations, Host Conversations, Conversations, and Response Time Details Views.
- A maximum interval for up to 1 hour is supported for the following dashboards: RTP Streams, Voice Call Statistics, Calls Tables, RTP Conversations, Host Conversations, Conversations, Response Time Details Views.

Note The From and To fields are enabled only when the Time Range is set to Custom.

Saving Filter Parameters

After clicking the Filter button in the Interactive Report and selecting the desired parameters, you can then save these selections with the purpose of viewing that same data at a future time.

To save filter parameters, follow these steps:

Step 1 At the Interactive Report on the monitoring dashboard, enter a name in the **Filter Name** field.

A filter is saved only if a filter name is entered. Only saved filters are persisted across multiple login sessions.

Step 2 Click **Submit**.

The filter is now saved and displayed underneath the Interactive Report. You can save up to five filters.

Setting up a Scheduled Export

You can create a Scheduled Export to have the dashboards extracted regularly and sent to you in CSV or HTML format.

You can set up scheduled jobs that will generate a daily report at a specified time, in the specified interval, and then e-mail it to a specified e-mail address. You can also obtain a report on the spot by clicking **Preview**, rather than wait for the scheduled time. This report can also be sent after you preview it.

To set up a Scheduled Export, follow these steps:

Step 1 On most windows under **Network Analysis**, the Interactive Report is available on the left side of the screen. Click the **Export** button in the **Interactive Report** area.

The **Create Scheduled Report** window is displayed.

Step 2 From the **Export Type** drop-down list, choose **Daily** or **Weekly**.

Step 3 From the **Export Time** drop-down list (when you would like the report delivered to you), choose **Day** and **Hour**.

Step 4 Choose the **Report Time** (if Daily) or the **Data Time Range** (if Weekly). This is the time interval you want measured.

The Report Time for a daily report is restricted to the current 24 hours.

The Report Time for a weekly report is always from 5:00 p.m to 5:00 p.m. (17:00 to 17:00), for however many days chosen.

For example, if you choose Export Type Weekly, Data Time Range Last 2 Days, and Export Time: Day Wednesday and Hour 13:00, the report will show data from Sunday at 17:00 to Tuesday at 17:00.

If you choose Export Time: Day Wednesday and Hour 18:00, the report will show data from Monday at 17:00 to Wednesday at 17:00.

Step 5 Enter the e-mail address to which you would like the report delivered.

Step 6 Choose the delivery option (HTML or CSV).

Step 7 Enter the report description, that will appear at the end of the filename of the report delivered to you.

Step 8 Depending on the task you want to perform, perform one or more of the following tasks:

- Click **Reset** to clear the values in the dialog box.
- Click **Preview** to preview the report.
- Click **Submit** to submit the request for the scheduled job.
- Click **Cancel** to close the dialog box and return to the previous screen.

Top Talkers Dashboard

This section includes the following topics:

Top Talkers Traffic Summary Dashboard

The Top Talkers Traffic Summary dashboard allows you to view the Top N Applications, Top N Application Groups, Top N Hosts (In and Out), IP Distribution by Bytes, Top N DSCP, and Top N VLAN that is being monitored on your network. It provides auto monitoring of traffic from all WAAS devices. You can view the Traffic Summary Dashboard by choosing **Monitor > Network Analysis Module > Overview.**

You can use the Interactive Report on the left to filter the information for a particular site, data source, VLAN, or reporting time interval. You can specify just one type of criteria and leave the others blank, or specify all of them. You can also choose to view the rate or cumulative data from the Interactive Report.

When you log in to the NAM for the first time, the default view is the Traffic Summary dashboard, and the top data source is selected by default.

The charts shown on this dashboard are as follows:

- Top N Applications

  The Top N Applications Chart enables you to view the traffic rate (bytes per second or bits per second) or traffic volume (bytes or bits), depending on the Interactive Report filter selection (data rate or cumulative, respectively). When you place your cursor over the colored bar, you will see the number of bytes per second collected or the total bytes over the last time interval.

- Top N Application Groups

  This chart shows a detailed analysis of the Top N application groups and the traffic rate or volume for this interval. In the Interactive Report, you can select either rate or cumulative, where rate indicates the bytes per second, and cumulative indicates the total number of bytes.

- Top N Hosts (In and Out)

  This chart displays the traffic rate (bytes per second or bits per second) or traffic volume (bytes or bits).

- IP Distribution by Bytes

  This chart shows the percentages of bytes that are distributed to IP protocols, for example, IPv4 TCP.

- Top N DSCP

  This chart shows statistics for the top Differentiated Services Code Point (DSCP) aggregation groups.

- Top N VLAN

  This chart shows the Top N VLAN statistics. In this chart, you might see VLAN 0, which is for traffic that does not have any VLAN tags.

To see a chart in table format, use the View as Chart or View as Grid toggle button at the bottom right corner of the chart. Alternatively, you can also click **Show as Image** to view the image and save it as a PNG file.

When viewing the data as a Grid, the numbers are formatted according to what you have configured in the Preferences window (**Configure** > **Network Analysis Module** > **Advanced** > **Preferences**). In the Preferences window, you can also configure the number of Top N entries you would like to display.

Top Talkers Details

While you are in the process of deploying WAAS devices, you can get data to assist in the WAAS planning and configuration. For information about setting up WAN traffic, see Adding a Data Source for a New WAAS Device.

The Top Talkers Detail window (**Monitor > Network Analysis Module > Top Talkers Details)**, assists you in the predeployment process. Use the Interactive Report window to select the traffic you want to analyze for optimization. The Interactive Report window displays the Top Applications, Top Network Links, Top Clients, and Top Servers.

Throughput Dashboards

This section includes the following topics:

Network Dashboard

The Network dashboard enables you to view LAN versus WAN throughput for WAAS users both in the incoming and outgoing directions. To view these reports, configure interface groups that comprise WAN and LAN interfaces. The displayed information represents the total data collected since the collection was created, or since the NAM was restarted. To view the Network dashboard, choose **Monitor > Network Analysis Module > Throughput > Network**.

Choose an interface group view from the Interface Selector on the left side of the window to see traffic in the charts. Click the arrow icon to the left of the NDE data source name to display all interfaces groups, and then select an interface group view. If the charts show no data, and you see the message “Interface needs to be selected,” you have not yet chosen an interface group view.

Once chose the interface group view, you see the following charts populated:

- Interface Traffic (Ingress % Utilization and Egress % Utilization)
- Top N Applications—Ingress
- Top N Applications—Egress
- Top N Hosts—Ingress
- Top N Hosts—Egress
- Top N DSCP Aggr—Ingress
- Top N DSCP Aggr—Egress

You can enter the interface speed manually through the Interface capacity table, or the speed can be auto configured if the SNMP settings for the NDE device are entered in the data source table.

Top Applications Dashboard

In the Top Applications dashboard, you can view the top applications by traffic rate over a selected time period and for the specified site or data source or both.

Applications Over Time shows you all of the applications that have been running for a specific time period. The color-coded legend shows you what the applications are running.

If you place your cursor over any of the data points, you get more details about the exact value for each of the applications that are running.

Application Dashboard

- In the Application window (**Monitor > Network Analysis Module > Throughput > Application**), you can see the traffic level for a given application over a selected period of time. It is available under the . This window shows you the following:
- A graph of application traffic over time.
- Top hosts that transmit and receive traffic on that application for a selected time period.
- Application Configuration that shows the criteria by which the NAM classifies packets as that application. This criteria is typically a list of TCP or UDP ports or both that identify the application.

Note Note that some applications are identified by heuristic or other state-based algorithms.

Performance Analysis Dashboards

This section includes the following topics:

Application Dashboard

The Application dashboard provides the transaction time performance for an application as well as the original and optimized traffic volume reported by the flow agent. Information about how the transaction time is broken up across client, WAN, and server segments is also provided. For example, if the transaction time is dominated by the server segment time (due to a slow server), WAAS may not be able to improve the performance as much as when it is dominated by WAN network time. To view the Application performance analysis dashboard, choose **Monitor > Network Analysis Module > Performance Analysis > Application**.

The charts that are available on this dashboard are as follows:

- Transaction Time (Client Experience)
- Traffic Volume and Compression Ratio
- Average Concurrent Connections (Optimized vs. Passthru)
- Multi-Segment Network Time (Client LAN - WAN - Server LAN)

Conversation Multiple Segments Dashboard

The Conversation Multiple Segments dashboard correlates data from different data sources, and allows you to view and compare response time metrics from multiple WAAS segments (data sources). To view the Conversation Multiple Segments dashboard, choose **Monitor > Network Analysis Module > Performance Analysis > Conversation Multisegments**.

The Response Time Across Multiple Segments window shows the response time metrics of the selected server or client-server pair from applicable data sources.