GUI Field Descriptions

This appendix describes critical field descriptions for the following windows. Not all fields are described as some are self-explanatory and others have tips that appear in the user interface.

Setup User Interface Windows

This section describes the field descriptions for the following dialog boxes:

- NBAR Interface Details
- Site Configuration
- Subnet Detection
- Sites Window
- Add NetFlow Interface Capacity
- Create or Edit Applications
- DSCP Group Setup Dialog Box
- Applications
- URL-Based Applications
- Response Time Configuration Window
- Media Monitor Setup Window
- URL Collection Configuration Dialog Box
- NetFlow Export Template Window

Create SPAN Session Dialog Box

Table D-1 describes the critical fields on the Create SPAN Session dialog box. Depending on NAM platform and SPAN configuration options such as SNMP, NetConf, or RISE the fields will vary in the Create SPAN Session Dialog Box.

Table D-1 Create SPAN Session Dialog Box

Field	Description
Managed Device	Managed device IP address and VDC on the managed device.
Session ID	ID of the SPAN session.
Span Session Options	• Extended: Allows for IP extended input ACLs to receive a copy of a dropped packed on a destination port even if the actual incoming packet is dropped. • Multicast Best Effort: Multicast packets are delivered to a group using **best - effort** reliability, just like IPv6 unicast packets. • Sampling: Collects NetFlow statistics for a subset of incoming (ingress) IPv4 traffic on the interface, selecting only one out of "N" sequential packets, where "N" is a configurable parameter. • MTU Truncation: Maximum bytes allowed for each replicated packet in a SPAN session • Rate Limit: Sets Committed Access Rate and Distributed Committed Access Rates for the interface's bandwidth
SPAN Type	• Switch Port • VLAN • EtherChannel • RSPAN VLAN You can have only one RSPAN VLAN source per SPAN session.

Table D-1 Create SPAN Session Dialog Box (continued)

Field	Description
SPAN Destination Interface	The NAM interface to which you want to send data.
Switch Module	Module of the switch
SPAN Traffic Direction	Direction of the SPAN traffic.
Available and Selected Sources	SPAN sources available for the selected SPAN type.

Prime NAM Data Sources Dialog Box

Table D-2 describes the critical fields on the Prime NAM Data Sources dialog box.

Table D-2 Prime NAM Data Sources

Field	Description
Device	DATA PORT if it is a local physical port or the IP address of the device that is sending NAM data.
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 exported from the router or switch or WAE device.
Activity	
Status	ACTIVE or INACTIVE.
Data Source	
Data Source Details	Physical Port or information about the data source being Enabled or Disabled.

Edit SPAN Session Dialog Box

Table D-3 describes the critical fields on the Edit SPAN Session dialog box. Depending on NAM platform and SPAN configuration options such as SNMP, NetConf, or RISE the fields will vary in the Create SPAN Session Dialog Box.

Table D-3 Edit SPAN Session Dialog Box

Field	Description
Managed Device	Managed device IP address and VDC on the managed device.
Session ID	ID of the SPAN session.

Table D-3 Edit SPAN Session Dialog Box (continued)

Field	Description
Span Session Options	• Extended: Allows for IP extended input ACLs to receive a copy of a dropped packed on a destination port even if the actual incoming packet is dropped. • Multicast Best Effort: Multicast packets are delivered to a group using **best - effort** reliability, just like IPv6 unicast packets. • Sampling: Collects NetFlow statistics for a subset of incoming (ingress) IPv4 traffic on the interface, selecting only one out of "N" sequential packets, where "N" is a configurable parameter. • MTU Truncation: Maximum bytes allowed for each replicated packet in a SPAN session • Rate Limit: Sets Committed Access Rate and Distributed Committed Access Rates for the interface's bandwidth
SPAN Type	• Switch Port • VLAN • EtherChannel • RSPAN VLAN You can have only one RSPAN VLAN source per SPAN session.
SPAN Destination Interface	The Prime NAM interface to which you want to send data.
SPAN Traffic Direction	Direction of the SPAN traffic.
Available and Selected Sources	SPAN sources available for the selected SPAN type.

SNMP Credential Options in NAM Data Sources Window

Table D-4 describes the options on the NAM Data Sources window for SNMP Credentials.

Table D-4 SNMP Credential Options in NAM Data Sources Window

Field	Description
Mode: No Auth, No Priv	SNMP will be used in a mode with no authentication and no privacy.
Mode: Auth, No Priv	SNMP will be used in a mode with authentication, but no privacy.
Mode: Auth and Priv	SNMP will be used in a mode with both authentication and privacy.
User Name	Enter a username, which will match the username configured on the device.
Auth Password	Enter the authentication password associated with the username that was configured on the device. Verify the password.
Auth Algorithm	Choose the authentication standard which is configured on the device (MD5 or SHA-1).

Table D-4 SNMP Credential Options in NAM Data Sources Window (continued)

Field	Description
Privacy Password	Enter the privacy password, which is configured on the device. Verify the password.
Privacy Algorithm	Enter the privacy algorithm, which is configured on the device (AES or DES).

Device System Information Dialog Box

Table D-5 describes the critical fields on the Device System Information dialog box.

Table D-5 Device System Information Dialog Box

Field	Description
Hardware	
Device Software Version	The current software version running on the device.
System Uptime	Total time the device has been running since the last reboot.
SNMP read from device	SNMP read test result. For the local device only.

Alarm Configuration Window

Table D-6 describes the critical fields on the Alarm Configuration Window.

Table D-6 Alarm Configuration Window

Field	Description
Name	Name given to the alarm at setup.
E-mail	**Enable** if turned on. **Disable** if turned off. Choose **Administration > System > E-Mail Setting**.
Trap	**Community:** ***xxxxx*** if configured. If not configured it is blank. Choose **Administration > System > SNMP Trap Setting**.
Trigger Capture	**Session:*xxxxx*** if configured. If no captures are configured it is blank. Choose **Capture > Packet Capture/Decode > Sessions**.
Syslog Remote	**Enable** if turned on. **Disable** if turned off. Choose **Administration > System > Syslog Setting**.
Status	**Missing Trap** means that the trap configured for that alarm action has been deleted. **OK** means the Alarm action was successfully created.

Threshold Configuration Window

Table D-7 describes the critical fields on the Threshold Configuration window.

Table D-7 Threshold Configuration

Field	Description
Type	You can configure eight types of thresholds.
Application	
Site	
Host	
Severity	High or Low (user-configured classification). These alarms are displayed on the Alarm Summary dashboard (**Monitor > Overview > Alarm Summary**). You can choose to view High, Low, or High and Low alarms.
Action	Rising action and Falling action (if configured). Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both.
Status	**OK** if configuration is complete. Otherwise, the issue displays (for example, **Missing Src Site**).
Add Metrics (button)	Adds another row.
Delete (button)	Removes that Metrics row.

Host Alarm Thresholds Window

Table D-8 describes the critical fields on the Hold Alarm Threshold window.

Table D-8 Host Alarm Thresholds

Field	Description
Name	
Site	Choose a site from the list. See Configuring Sites, page 7-47 for information on setting up a site.
Host	Choose a host from the list. You can enter the name of the host if the drop-down list does not contain the desired host.
Application	Choose an application from the list. You can enter the first few characters to narrow the selection in the drop-down list.
DSCP	Choose a DSCP value from the list. You can enter the first few characters to narrow the selection in the drop-down list.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	From the drop-down lists, choose a Rising action and a Falling action (optional). During threshold creation, by default, the falling action is the same as rising action. See Viewing Alarm Actions, page 7-33 for information on setting up alarm actions.
Host Metrics (per second)	Choose the type of metric from the list, and then enter a value for a Rising threshold and a Falling threshold.

Conversation Alarm Thresholds Window

Table D-9 describes the critical fields on the Conversation Alarm Thresholds window.

Table D-9 Conversation Alarm Thresholds

Field	Description
Name	
Application	Choose an application from the list. You can start typing the first few characters to narrow the list.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Source Site/Host	Make a selection from the drop-down lists, or leave as **Any**. See Configuring Sites, page 7-47 for information on setting up a site.
Destination Site/Host	Make a selection from the drop-down lists, or leave as **Any**. See Configuring Sites, page 7-47 for information on setting up a site.
Actions	From the lists, choose a Rising action and a Falling action (optional). See Viewing Alarm Actions, page 7-33 for information on setting up alarm actions.
Conversation Metrics (per second)	Choose from one of the six metrics, and then enter a Rising threshold and a Falling threshold.

Application Alarm Thresholds Configuration Window

Table D-10 describes the critical fields on the Application Alarm Thresholds Configuration window.

Table D-10 Application Alarm Thresholds

Field	Description
Name	
Site	Choose a site from the list. See Configuring Sites, page 7-47 for information on setting up a site.
Application	Choose an application from the list. You can start typing the first few characters to narrow the list.
DSCP	Choose a DSCP value 0-63, or Any.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	From the lists, choose a Rising action and a Falling action (optional). See Configuring Alarm Actions, page 7-31 for information on setting up alarm actions.
Application Metrics (per second)	Choose Bits or Bytes, and then enter a Rising threshold and a Falling threshold.

Response Time Alarm Threshold Configuration Window

Table D-11 describes the critical fields on the Response Time Alarm Threshold Configuration window.

Table D-11 Response Time Thresholds

Field	Description
Name	
Application	Choose an application from the list. You can start typing the first few characters to narrow the list.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview > Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Client Site/Host	Make a selection from the lists. See Configuring Sites, page 7-47 for information on setting up a site.
Server Site/Host	Make a selection from the lists, or leave as "Any." See Configuring Sites, page 7-47 for information on setting up a site.
Actions	From the lists, choose a Rising action and a Falling action (optional). See Viewing Alarm Actions, page 7-33 for information on setting up alarm actions.
Response Time Metrics	Choose a metric from the list, and then enter a Rising threshold and a Falling threshold. For the Packets and Bytes-related metrics, the entry is per second. For the time-related metrics, the unit is per microseconds (u).

DSCP Alarm Threshold Configuration Window

Table D-12 describes the critical fields on the DSCP Alarm Threshold Configuration window.

Table D-12 DSCP Alarm Thresholds

Field	Description
Name	Give the DSCP Alarm Threshold a name.
Site	Choose a site from the list. See Configuring Sites, page 7-47 for information on setting up a site.
DSCP	Choose a DSCP value from the list.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	From the drop-down lists, choose a Rising action and a Falling action (optional).
DSCP Metrics (per second)	Choose one of the metric types from the list, and then enter a Rising threshold and a Falling threshold.

RTP Streams Threshold Configuration Window

Table D-13 describes the critical fields on the RTP Threshold Configuration window.

Table D-13 RTP Streams Thresholds

Field	Description
Name	
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Codec	Choose a Codec from the list.
Source Site/Host	Make a selection from the drop-down lists, or leave as "Any." See Configuring Sites, page 7-47 for information on setting up a site.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	From the drop-down lists, choose a Rising action and a Falling action (optional). See Viewing Alarm Actions, page 7-33 for information on setting up alarm actions.
RTP Stream Metrics	Choose a metric from the list: • Jitter: Variation of packet arrival time compare to expected arrival time. • Adjusted packet loss percent: Percent of packet loss which includes packets actually lost and packets that arrived beyond the expected buffering capability of the endpoint. • Actual packet loss percent: Percent of packets that Prime NAM has never seen. • MOS: Mean opinion score that is composed of both jitter and adjusted packet loss. • Concealment seconds: Number of seconds in which Prime NAM detected packets lost. • Severe concealment seconds: Number of seconds in which Prime NAM detected packets lost of more than 5%. Enter a Rising threshold and a Falling threshold.

Voice Signaling Threshold Configuration Window

Table D-14 describes the critical fields on the Voice Signaling Threshold Configuration window.

Table D-14 Voice Signaling Thresholds

Field	Description
Name	
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.

Table D-14 Voice Signaling Thresholds (continued)

Field	Description
Actions	Choose a Rising action and a Falling action from the lists (optional). See Viewing Alarm Actions, page 7-33 for information on setting up alarm actions.
Voice Signaling Metrics	Choose Jitter to enable an alarm when the software detects jitter to be more than the value set here. Check Packet Loss % to enable an alarm when the software detects Packet Loss percentage to be outside of the values you entered.

NetFlow Interface Threshold Configuration Window

Table D-15 describes the critical fields on the Network Interface Threshold Configuration window.

Table D-15 NetFlow Interface Alarm Thresholds

Field	Description
Direction	Choose Ingress or Egress.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	Choose a Rising action and a Falling action from the lists (optional). See Viewing Alarm Actions, page 7-33 for information on setting up alarm actions.
Application Metrics (per second)	Choose Bytes or Packets, and enter a Rising and Falling threshold.

Video Stream Threshold Configuration Window

Table D-16 describes the critical fields on the Video Stream Threshold Configuration window.

Table D-16 Video Stream Thresholds

Field	Description
Name	Name given to the video stream,
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview > Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Codec	Choose a Codec from the list.
Source Site/Host	Make a selection from the drop-down lists, or leave as “Any.” See Configuring Sites, page 7-47 for information on setting up a site.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.

Table D-16 Video Stream Thresholds (continued)

Field	Description
Actions	From the drop-down lists, choose a Rising action and a Falling action (optional). See Viewing Alarm Actions, page 7-33 for information on setting up alarm actions.
Video Stream Metrics	Choose a metric from the list: • I Frame Loss%: Percentage of I frame loss. • I Frame Loss Count: The loss count of I frames. • All Frame Loss%: Percentage of frame loss of all types. • All Frame Loss Count: The loss count of all types of frames. Enter a Rising threshold and a Falling threshold.

Video MDI Stream Threshold Configuration Window

Table D-17 describes the critical fields on the Video MDI Stream Threshold Configuration window.

Table D-17 Video MDI Stream Thresholds

Field	Description
Name	Name given to the video MDI Stream.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Source Site/Host	Make a selection from the drop-down lists, or leave as "Any." See Configuring Sites, page 7-47 for information on setting up a site.
Severity	Choose High or Low. These display on the Alarm Summary dashboard (**Monitor > Overview >Alarm Summary**), where you can choose to view High, Low, or High and Low alarms.
Actions	From the drop-down lists, choose a Rising action and a Falling action (optional). See Viewing Alarm Actions, page 7-33 for information on setting up alarm actions.
Video Stream Metrics	Choose a metric from the list: • Delay Factor: RFC-4445 delay factor. • Media Loss Rate: RFC-4445 media loss rate. Enter a Rising threshold and a Falling threshold.

Router System Information Window

Table D-18 describes the critical fields on the Router System Information window.

Table D-18 Router/Managed Device System Information

Field	Description
Name	
Hardware	
Managed Device Software Version	Current software version of the router.
Managed Device System Uptime	Total time the router or switch has been running.
Location	
Contact	
Managed Device	IP address of the router.
SNMP v1/v2c RW Community String	
Verify String	
Enable SNMP V3	Check the check box to enable SNMP Version 3. If SNMPv3 is not enabled, the community string is used.
Mode: No Auth, No Priv	SNMP is used in a mode with no authentication and no privacy.
Mode: Auth, No Priv	SNMP is used in a mode with authentication, but no privacy.
Mode: Auth and Priv	SNMP is used in a mode with both authentication and privacy.
User Name	Enter a username, which will match the username configured on the device.
Auth Password	Enter the authentication password associated with the username that was configured on the device. Verify the password.
Auth Algorithm	Choose the authentication standard which is configured on the device (MD5 or SHA-1).
Privacy Password	Enter the privacy password, which is configured on the device. Verify the password.
Privacy Algorithm	Enter the privacy algorithm, which is configured on the device (AES or DES).

Switch/Managed Device System Information

Table D-19 describes the critical fields on the Switch System Information window.

Table D-19 Switch Device Information

Field	Description
SNMP Test information	Displays the IP address of the NAM and the switch on which the SNMP test occurred.
Name	

Table D-19 Switch Device Information (continued)

Field	Description
Hardware	
Supervisor Software Version	
System Uptime	Total time the device has been running.
SNMP read from chassis	SNMP read test result.
SNMP write to chassis	SNMP write test result.
Mini-RMON on chassis	For Cisco IOS devices, displays the status if there are any ports with Mini-RMON configured (Available) or not (Unavailable).
NBAR on chassis	Displays if NBAR is available on the device.
VLAN Traffic Statistics on chassis	Displays if VLAN data is Available or Unavailable. **Note** Catalyst 6500 Series switches require a Supervisor 2 or MSFC2 card.
NetFlow Status	For Catalyst 6500 Series devices running Cisco IOS, if NetFlow is configured on the device, *Remote export to NAM <address> on port <number>* displays, otherwise the status displays *Configuration unavailable*.

NBAR Interfaces Window

Table D-20 describes the critical fields on the NBAR Interfaces window.

Table D-20 NBAR Interface Details

Field / Operation	Description
Enable (check box)	Check indicates that NBAR is enabled.
Interface	Depending on the IOS running on the Supervisor, port names are displayed differently. Newer versions of IOS software display a port name as Gi2/1 to represent a Gigabit port on module 2 port 1. In the Virtual Switch software (VSS), a port name might be displayed as Gi1/2/1to represent a Gigabit port on switch 1, module2, port 1.
Interface Description	Description of the interface.

Site Configuration Window

Table D-21 describes the critical fields on the Site Configuration window.

Table D-21 Site Configuration

Field	Description
Name	
Description	

Table D-21 Site Configuration (continued)

Field	Description
Disable Site (check box)	If you check this check box, the software will skip this site when classifying traffic. This is useful if the site is no longer active, but the user would still like to access historical site data in the database. Otherwise, the user should delete sites that are not needed.
Subnet	IP address subnet (IPv4/IPv6 address and mask); for example, 10.1.1.0/24. Click the blue **i** to get information about Site Rules. You can click the **Detect** button to tell the software to look for subnets in the traffic. See Configuring Sites Using Subnets, page 7-49.
Data Source	Specify the data source from where the site traffic originates. Leave this field blank if the site traffic can come from multiple data sources.

Subnet Detection Window

Table D-22 describes the critical fields on the Subnet Detection window.

Table D-22 Subnet Detection

Field	Description
Subnet Mask	Enter the subnet mask. **Note** If the bit mask is 32 or less, the software will detect an IPv4 subnet. If the bit mask is between 33 and 64, then it will detect an IPv6 subnet.
Data Source	Choose the data source in which you would like to detect subnets.
Interface	Choose the interface in which you would like to detect subnets.
Filter Subnets Within Network	Enter an IPv4 or IPv6 address
Unassigned Site (check box)	The “Unassigned” site includes any that do not match any of your site configurations. Sites are classified at the time of packet processing.

Sites Window

Table D-23 describes the critical fields on the Sites window.

Table D-23 Sites Window

Field	Description
Name	
Description	
Rule	Lists the first rule assigned to the selected site. If you see periods next to the site rule (...), then multiple rules were created for that site. To see the list of all 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.

Add NetFlow Interface Window

Table D-24 describes the critical fields on the NetFlow Interface Add window.

Table D-24 Add NetFlow Interface Capacity

Field	Description
Device	Enter the IPv4 or IPv6 address.
ifIndex	Unique identifying number associated with a physical or logical interface. Valid characters: 0-9.
ifName	Name of the interface. Valid characters are A-Z, a-z, 0-9.
ifSpeed(Mbps)	An estimate of the interface's current bandwidth in bits per second.

DSCP Group Setup Dialog Box

Table D-25 describes the critical fields on the DSCP Group Setup dialog box.

Table D-25 DSCP Group Setup Dialog Box

Field	Description	Usage Notes
Name	Name of the profile.	Enter the name of the profile you are creating. The maximum is 64 characters.
Label Format	DSCP	DSCP numbers from 0 to 63. After selecting the DSCP radio button, you can freely choose any of the 64 possible values and assign them to Groups.
	AF / EF / CS	Assured Forwarding (AF) guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, Expedited Forwarding (EF) is used for traffic that is very sensitive to delay, loss and jitter, such as voice or video traffic. Class Selector (CS) the last 3 bits of the 6-bit DSCP field, so these correspond to DSCP 0 through DSCP 7.
	Bit Field	Six bits in the IP header of a packet.

DSCP Group Label Formats

Table D-26 describes the DSCP Group label formats.

Table D-26 DSCP Group Label Formats

DSCP Format (DSCP 0 through DSCP 63)	AF/EF/CS Format	Bit Field Format
DSCP 0	-	000000
DSCP 8	CS1	001000

Table D-26 DSCP Group Label Formats (continued)

DSCP Format (DSCP 0 through DSCP 63)	AF/EF/CS Format	Bit Field Format
DSCP 10	AF11	001010
DSCP 12	AF12	001100
DSCP 14	AF13	001110
DSCP 16	CS2	010000
DSCP 18	AF21	010010
DSCP 20	AF22	010100
DSCP 22	AF23	010110
DSCP 24	CS3	011000
DSCP 26	AF31	011010
DSCP 28	AF32	011100
DSCP 30	AF33	011110
DSCP 32	CS4	100000
DSCP 34	AF41	100010
DSCP 36	AF42	100100
DSCP 38	AF43	100110
DSCP 40	CS5	101000
DSCP 46	EF	101110
DSCP 48	CS6	110000
DSCP 56	CS7	111000

Application Window

Table D-27 describes the critical fields on the Add Application Window.

Table D-27 Create or Edit Applications

Field	Description
Name	Unique 1 to 64 character descriptive name.
Description	
Selector	(Optional) Leave blank. An arbitrary number up to 4-digits, unique within an engine-id. It is automatically assigned if left blank. Identification number is autogenerated if left blank. Range is from 1 to 65535. This allows you to configure applications consistently across multiple NAMs, so that the same user-created application is exported with the same value. This should be used when configuring the same custom applications on multiple NAMs. The application tag for user-created applications is a combination of the engine ID and the Selector. The 32 bit is generated by using the engine ID as the highest order byte, and the Selector makes up the other 3 bytes. For standard application/protocols, the application tag is predefined.

Table D-27 Create or Edit Applications (continued)

Field	Description
Application Classification Rule	Select application type: Protocol, HTTP URL-based or Server IP Address.
Application Rule: Protocol/Port	Add the application protocol and port you want to track.
	Protocol—Lists predefined protocols. If your option is not included, you can create a custom URL-based application classification.
	Port—Enter the port number or port number range to monitor. The port is an arbitrary number you assign to handle the additional ports for the protocol family. This protocol number must be unique so it does not conflict with standard protocol/port assignments. The port number range will vary depending on the protocol type selected. You can create additional ports to enable Prime NAM to handle additional traffic for standard applications.
Application Rule: HTTP URL	Create custom URL-based applications by selecting this option. Enter at least one of the values below.
	URL Host—The host name identified in the header from which the traffic is originating.
	URL Path—The specific URL path that identifies the traffic.
Engine ID	Identifies the type of application (including ethertype, iana-14, iana-13, lic, L7, or custom).
Application Tag	System generated tag which can be used when multiple NAMs are being monitored.
Description	(Optional) Custom description to define your application. Limited to 75 characters.
Status	Active means that network traffic is being analyzed. Inactive means that the application is not being analyzed, possibly due to a duplication of effort. The Interactive Report filter may still list inactive applications if there is any historical data for the inactive application in the database, but it is not collecting new data.

Applications Window

Table D-28 describes the critical fields on the Applications Window.

Table D-28 Applications

Field	Description
Application	Unique 1 to 64 character descriptive name.
Rule	Displays application type: Protocol, HTTP URL-based or Server IP Address.

Table D-28 Applications (continued)

Field	Description
Selector	An arbitrary number up to 4-digits, unique within an engine-id. It is automatically assigned if left blank. This allows you to configure applications consistently across multiple NAMs, so that the same user-created application is exported with the same value. This should be used when configuring the same custom applications on multiple NAMs. The application tag for user-created applications is a combination of the engine ID and the selector. The 32 bit number is generated by using the engine ID as the highest order byte, and the selector makes up the other 3 bytes. For standard application/protocols, the application tag is predefined.
Engine ID	Identifies the type of application (including ethertype, iana-14, iana-13, lic, L7, or custom)
Application ID	System generated tag which can be used when multiple NAMs are being monitored.
Description	If a system-defined, contains system information about the application type. If user-defined, enter custom description to define your application. Limited to 75 characters.
Status	Active means that network traffic is being analyzed. Inactive means that the application is not being analyzed, possibly due to a duplication of effort. The Interactive Report filter may still list inactive applications, but it is not monitored by NAM and is therefore not classified or displayed on NAM dashboards.

URL-Based Applications Window

Table D-29 describes the critical fields on the URL-Based Applications window.

Table D-29 URL-Based Applications

Field	Description
Index	A unique number (1-64) of each URL-based application. You can define up to 64 URL-based applications in NAM.
Host	Matching criteria in the host portion of the URL string appears in HTTP packets. This match is a POSIX Regular Expression[1].
Path	Matching criteria in the path portion of the URL string appears in HTTP packets. This match is a POSIX Regular Expression[1].
Content-Type	Matching criteria in the Content-Type field of the HTTP packets. This match is a POSIX Regular Expression[1].
Protocol Description	Description of this URL-based application.

1. A regular expression provides a concise and flexible means for matching strings of text, such as particular characters, words, or patterns of characters. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification. The IEEE POSIX Basic Regular Expressions (BRE) standard (released alongside an alternative flavor called Extended Regular Expressions or ERE) was designed mostly for backward compatibility with the traditional (Simple Regular Expression) syntax but provided a common standard which has since been adopted as the default syntax of many Unix regular expression tools, though there is often some variation or additional features. Many such tools also provide support for ERE syntax with command line arguments. In the BRE syntax, most characters are treated as literals - they match only themselves (in other words, a matches "a").

Response Time Configuration Window

Table D-30 describes the critical fields on the Response Time Configuration Window.

Table D-30 Response Time Configuration Window

Field	Description	Usage Notes
Range 1 (µs)	Upper response time limit for the first container	Enter a number in microseconds. The default is 1 to 1,000 µs
Range 2 (µs)	Upper response time limit for the second container	Enter a number in microseconds. The default is 1,001 to 5,000 µs
Range 3 (µs)	Upper response time limit for the third container	Enter a number in microseconds. The default is 5,001 to 10,000 µs
Range 4 (µs)	Upper response time limit for the fourth container	Enter a number in microseconds. The default is 10,001 to 50,000 µs
Range 5 (µs)	Upper response time limit for the fifth container	Enter a number in microseconds. The default is 50,001 to 100,000 µs
Range 6 (µs)	Upper response time limit for the sixth container	Enter a number in microseconds. The default is 100,001 to 500,000 µs
Range 7 (µs)	Upper response time limit for the seventh container	Enter a number in microseconds. The default is 500,001 to 1,000,000 µs
Range 8 (µs)	Upper response time limit for the eighth container. This is the maximum interval that Prime NAM waits for a server response to a client request.	This range cannot be edited. Enter a number in microseconds. The default is 1,000,001 µs to infinity.

Media Monitor Setup Window

Table D-31 describes the critical fields on the Media Monitor Setup Window.

Table D-31 Media Monitor Setup Window

Field	Description
Voice Monitoring	
Enabled	Enables voice monitoring. Ensure this check box is selected if you are interested in voice monitoring.
MOS Values	

Table D-31 Media Monitor Setup Window (continued)

Field	Description
Excellent	MOS scores listed here indicate excellent quality voice transmission (where 5.0 is the highest score). The default setting considers the range between 4.34 to 5.0 as *excellent*.
Good	MOS score listed here indicate good quality voice transmission. The default setting considers the range between 4.03 to 4.33 as *good*.
Fair	MOS score listed here indicate fair quality voice transmission. The default setting considers the range between 3.6 to 4.02 as *fair*.
Poor	MOS score listed here indicate poor quality voice transmission. The default setting considers the range between 0.0 and 3.59 as *poor*. This default cannot be changed.
Video Monitoring	
Enabled	Enables video monitoring. Ensure this check box is selected if you are interested in video monitoring.
MDI Values	
Poor	MDI score listed here indicate poor quality video transmission. The default setting considers 10.000ms 0.0050pps and above as *poor*.
Fair	MDI score listed here indicate fair quality video transmission. The default setting considers the range between 5.000ms 0.0010pps and 10.000ms 0.0050pps as *fair*.
Good	MDI score listed here indicate good quality video transmission. The default setting considers the range between 1.000ms 0.0005pps and 5.000ms 0.0010pps as *good*.
Excellent	MDI scores listed here indicate excellent quality video transmission. The default setting considers the range between 0.000ms 0.0000pps and 1.000ms 0.0005pps as *excellent*. This default cannot be changed.

URL Collection Configuration Window

Table D-32 describes the critical fields on the URL Collection Configuration Window.

Table D-32 URL Collection Configuration Dialog Box

Element	Description	Usage Notes
Data Source	Identifies type of traffic incoming from the application.	Select one of the options from the drop-down box.

Table D-32 URL Collection Configuration Dialog Box (continued)

Element	Description	Usage Notes
Max Entries	Maximum number of URLS to collect.	Select one of the following options from the drop-down box: • 100 • 500 • 1000
Match only	The application URL to match.	Optional parameter to limit collection of URLs that match the regular expression of this field.

NetFlow Export Template Window

Table D-33 describes the critical fields on the NetFlow Export Template Window.

Table D-33 NetFlow Export Template Window

Field	Description
Description	A description of the NetFlow Export.
Destination IP Address	The IP address of the device to be exported to. IPv4 and IPv6 addresses are supported.
Destination Port	The port number of the device to be exported to. Valid characters: 1-9. Length: Min 1, Max 65535.
Export Record Type	The record types supported by NAM for NetFlow are: • Client Server Response Time • Application Conversation • Network Conversation • RTP Metrics
Export Interval	This will be five minutes for Client Server Response Time and one minute for the other record type.

Table D-33 NetFlow Export Template Window (continued)

Field	Description
Version	Select v9 or IPFIX to export.
Options	The NetFlow option selection contains a set of check boxes. These allow independent selections of on or off settings for individual NetFlow options, which can be exported in addition to the NDE packets with data and templates, as follows: • Mapping of integer application ID values into application names (as strings) • Mapping of integer site ID values into site names and descriptions (as strings) If there are several NetFlow Export Descriptors defined for the same destination, then the last user's selection of option exports flags is enforced on all descriptor instances that exist for the same export.

Monitor User Interface Windows

Table D-34 and Table D-35 describe the various optional and data templates.

Table D-34 Optional Templates

ID	Length	Name
Application Template		
95	4	Application ID
96	24	Application Name
94	55	Application Description
Site Template		
42006	4	Site ID
4 42016	24	Site Name
42017	55	Site Description
Data Source Template		
42001	4	Data source ID
42018	24	Data source name
42019	55	Data source description

Table D-35 Data Templates

ID	Length	Name
Network Conversation IPv4 Template		
8	4	IPv4 source address
12	4	IPv4 destination address
42002	4	source site ID
42003	4	destination site ID
42001	4	data source ID
10	4	input SNMP if-index
14	4	output SNMP if-index
58	2	input VLAN ID
59	2	output VLAN ID
195	1	input DSCP
98	1	output DSCP
151	4	flow end seconds
1	8	byte count
2	8	packet count
Network Conversation IPv6 Template		
27	16	IPv6 source address
28	16	IPv6 destination address
42002	4	source site ID
42003	4	destination site ID
42001	4	data source ID
10	4	input SNMP if-index
14	4	output SNMP if-index
58	2	input VLAN ID
59	2	output VLAN ID
195	1	input DSCP
98	1	output DSCP
151	4	flow end seconds
1	8	byte count
2	8	packet count
Application Conversation IPv4 Templates		
8	4	IPv4 source address
12	4	IPv4 destination address
42002	4	source site ID
42003	4	destination site ID

Table D-35 Data Templates (continued)

ID	Length	Name
42001	4	data source ID
95	4	application ID
42010	4	network encapsulation ID
10	4	input SNMP if-index
14	4	output SNMP if-index
58	2	input VLAN ID
59	2	output VLAN ID
4	1	protocol
195	1	input DSCP
98	1	output DSCP
151	4	flow end seconds
1	8	byte count
2	8	packet count
Application Conversation IPv6 Templates		
8	4	IPv4 source address
12	4	IPv4 destination address
27	16	IPv6 source address
28	16	IPv6 destination address
Application Response Time IPv4 Templates		
42004	4	server site
42007	4	server IPv4 address
42005	4	client site
42008	4	client IPv4 address
95	4	app ID
42001	4	data source
58	2	VLAN ID
195	1	DSCP
151	4	duration of the flow
42010	4	net encapsulation
32792	2	server port
42020	1	waas optimization segments
42060	4	number of responses
42061	4	number of responses in bucket1
42062	4	number of responses in bucket2
42063	4	number of responses in bucket3
42064	4	number of responses in bucket4

Table D-35 Data Templates (continued)

ID	Length	Name
42065	4	number of responses in bucket5
42066	4	number of responses in bucket6
42067	4	number of responses in bucket7
42068	4	number of late responses
42071	4	sum response time
42072	4	maximum response time
42073	4	minimum response time
42074	4	sum application response time
42075	4	maximum application response time
42076	4	minimum application response time
42077	4	sum total response time
42078	4	maximum total response time
42079	4	minimum total response time
42040	4	sum number of transaction
42041	4	sum transaction time
42042	4	maximum transaction time
42043	4	minimum transaction time
42050	4	number of new connections
42054	4	sum session duration
42084	4	sum client network time
42085	4	maximum client network time
42086	4	minimum client network time
42087	4	sum server network time
42088	4	maximum server network time
42089	4	minimum server network time
42081	4	sum network delay
Application Response Time IPv6 Templates		
42004	4	server site
28	16	server IPv6 address
42005	4	client site
27	16	client IPv6 address
95	4	app ID
42001	4	data source
58	2	VLAN ID
195	1	DSCP
151	4	duration of the flow

Table D-35 Data Templates (continued)

ID	Length	Name
42010	4	net encapsulation
32792	2	server port
42020	1	waas optimization segments
42060	4	number of responses
42061	4	number of responses in bucket1
42062	4	number of responses in bucket2
42063	4	number of responses in bucket3
42064	4	number of responses in bucket4
42065	4	number of responses in bucket5
42066	4	number of responses in bucket6
42067	4	number of responses in bucket7
42068	4	number of late responses
42071	4	sum response time
42072	4	maximum response time
42073	4	minimum response time
42074	4	sum application response time
42075	4	maximum application response time
42076	4	minimum application response time
42077	4	sum total response time
42078	4	maximum total response time
42079	4	minimum total response time
42040	4	sum number of transaction
42041	4	sum transaction time
42042	4	maximum transaction time
42043	4	minimum transaction time
42050	4	number of new connections
42054	4	sum session duration
42084	4	sum client network time
42085	4	maximum client network time
42086	4	minimum client network time
42087	4	sum server network time
42088	4	maximum server network time
42089	4	minimum server network time
RTP IPv4 Templates		
8	4	source IPv4 Address
12	4	destination IPv4 Address

Table D-35 Data Templates (continued)

ID	Length	Name
42002	4	source site
42003	4	destination site
42101	4	rtp ssrc
42102	1	rtp payload type
7	2	source port
11	2	destinaiton port
195	1	DSCP
58	2	VLAN ID
151	4	flow end seconds
42001	4	data source
42010	4	net encap
42112	4	rtp duration
42113	4	average MOSx100
42115	4	worst/lowest MOSx100
37023	4	jitter x 100
37019	4	actual packet loss count
37014	4	expected packet count
RTP IPv6 Templates		
27	4	source IPv6 Address
28	4	destination IPv6 Address
42002	4	source site
42003	4	destination site
42101	4	rtp ssrc
42102	1	rtp payload type
7	2	source port
11	2	destinaiton port
195	1	DSCP
58	2	VLAN ID
151	4	flow end seconds
42001	4	data source
42010	4	net encap
42112	4	rtp duration
42113	4	average MOSx100
42115	4	worst/lowest MOSx100
37023	4	jitter x 100

Table D-35 Data Templates (continued)

ID	Length	Name
37019	4	actual packet loss count
37014	4	expected packet count

This section describes field descriptions for the following windows:

- All Alarms Table
- Applications Detail
- Application Groups Detail
- Client-Server Application Responses Window
- Client-Server Application Transactions Window
- Client-Server Network Responses Window
- DSCP Detail
- Host Detail
- Interfaces Stats Table
- Last 50 Alarms
- Server Application Responses Metrics
- Server Application Transactions Metrics
- Server Network Responses Window

All Alarms Table

Table D-36 describes the critical fields on the All Alarms table.

Table D-36 All Alarms

Field	Description
Site	This contains site or source and destination sites (source - destination) of the network traffic that generated the alarm message.
Alarm Triggered By	Details information of the network traffic that generated the alarm message. The format of the alarm triggered by string are: • Triggered by application threshold: application • Triggered by application with DSCP threshold: DSCP:codepoint - application • Triggered by host threshold: host • Triggered by host with application threshold: host - application • Triggered by host with application and DSCP: DSCP: code point - host - application • Triggered by host with DSCP: DSCP: code point - host • Triggered by conversation: source - destination • Triggered by conversation with application: source - application - destination • Triggered by response time: IAP: client - application - server. • Triggered by DSCP: DSCP: code point • Triggered by RTP stream: source - source port - codec(codec string) - SSRC(number) - destination - destination port • Triggered by voice signaling: Calling (address - number) Called (address - number) ID/References (id() - ref (calling:called)) • Triggered by NetFlow interfaces: NetFlow: Device (address) - If-Index(number) - Ingress/Egress
Threshold Variable	Parameter of the threshold that is used to evaluate alarm condition.
Threshold Value	User defined rising value of the threshold variable.
Triggered Time	Time when the alarm condition was found occurred.
Triggered Value	Parameter value when the alarm condition was raised. Note: The triggered value could be - when the viewing window does not included the alarm when it was occurring.
Clear Time	Time when the alarm condition was resolved. The alarm variable has fallen below the falling threshold value.

Applications Detail Window

Table D-37 describes the critical fields in this window.

Table D-37 Applications Detail

Field	Description
Application	Software services classified by NAM from analyze and monitor traffic.
Application Group	The application group (set of applications that can be monitored as a whole).
Bytes/sec	Traffic rate; number of bytes per second
Packets/sec	Traffic rate; number of packets per second

Application Groups Detail Window

Table D-38 describes the critical fields in this window.

Table D-38 Application Groups Detail

Field	Description
Application Group	The application group (set of applications that can be monitored as a whole).
Site	Applicable site (or Unassigned if no site)
Bytes/sec	Traffic rate; number of bytes per second
Packets/sec	Traffic rate; number of packets per second

Application Response Time (ART) Metrics

Table D-39 describes the metrics measured for response time.

Table D-39 Application Response Time (ART) Metrics

Metric	Description
Average Response Time	Response Time is the time between the client request and the first response packet from the server, as observed at the NAM probing point. Increases in the response time usually indicate problems with server resources, such as the CPU, Memory, Disk, or I/O due to a lack of necessary resources or a poorly written application. This and other Response Time metrics are in microseconds (µs) units.
Min Response Time	
Max Response Time	
Number of Responses	Total number of request-response pairs observed during the monitoring interval
Number of Late Responses	Total number of responses that exceed the Max Response Time
Number of Responses 1	Number of responses with a response time less than RspTime1 threshold
Number of Responses 2	Number of responses with response time less than RspTime2 and larger than RspTime1
Number of Responses 3	Number of responses with response time less than RspTime3 and larger than RspTime2
Number of Responses 4	Number of responses with response time less than RspTime4 and larger than RspTime3
Number of Responses 5	Number of responses with response time less than RspTime5 and larger than RspTime4

Table D-39 Application Response Time (ART) Metrics (continued)

Metric	Description
Number of Responses 6	Number of responses with response time less than RspTime6 and larger than RspTime5
Number of Responses 7	Number of responses with response time less than LateRsp and larger than RspTime6
Client Bits	Number of TCP payload bits sent from the client(s) during the monitoring interval
Server Bits	Number of TCP payload bits sent from the server(s) during the monitoring interval
Client Packets	Number of TCP packets sent from the client(s) during the monitoring interval
Server Packets	Number of TCP packets sent from the server(s) during the monitoring interval
Average number of concurrent connections	Average number of concurrent TCP connections during the reporting interval
Number of new connections	Number of new TCP connections made (TCP 3-way handshake) during the monitoring interval
Number of closed connections	Number of TCP connections closed during the monitoring interval
Number of unresponsive connections	Number of TCP connection requests (SYN) that are not responded during the monitoring interval
Number of refused connections	Number of TCP connection requests (SYN) that are refused during the monitoring interval
Average Connection duration	Average duration of TCP connections during the monitoring interval
Average Server Response Time	Server Response Time is the time it takes an application server (for example, a web server) to respond to a request. This is the server *think time*, which is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application and/or server resources, such as the CPU, Memory, Disk, or I/O.
Min Server Response Time	
Max Server Response Time	
Average Network Time	Network time between a client and a server. Network Time is the sum of Client Network Time and Server Network Time. NAM measures the Network Time using TCP 3-way handshakes. If there are no new TCP connections made during the monitoring interval, this metric is not reported.
Min Network Time	
Max Network Time	
Average Client Network Time	Client Network Time is the network time between a client and the NAM switch or router. In WAAS monitoring, Client Network Time from a WAE client data source represents the network RTT between the client and its edge WAE, while Client Network Time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).
Min Client Network Time	
Max Client Network Time	
Average Server Network Time	Server Network Time is the network time between a server and NAM probing point. In WAAS monitoring, Server Network Time from a server data source represents the network time between the server and its core WAE.
Min Server Network Time	
Max Server Network Time	
Average Total Response Time	Total Response Time is the total amount of time between the client request and when the client receives the first response packet from the server. Use Total Response Time with care because it is not measured directly and mixes the server response time metric with the network time metric.
Min Total Response Time	
Max Total Response Time	
Average Transaction Time	Transaction Time is the total amount of time between the client request and the final response packet from the server. Transaction times may vary depending upon client usages and application types. Transaction Time is a key indicator for monitoring client experiences and detecting application performance anomalies.
Min Transaction Time	
Max Transaction Time	

Table D-39 Application Response Time (ART) Metrics (continued)

Metric	Description
Number of Transactions	The number of transactions completed during the monitoring interval.
Average Data Transmission Time	Elapsed time from the first server-response packet to the last server-response packet, excluding retransmission time.
Average Data Time	Data Time: Average data time portion of transaction time.
Packets Retransmitted	Number of retransmitted packets detected during the monitoring interval
Bits Retransmitted	Number of retransmitted bits detected during the monitoring interval
Average Retransmission Time	Average time to retransmit lost packets per transaction
Client ACK Round Trip Time	Average network time for the client to acknowledge (ACK) a server data packet as observed at NAM probing point
Number of Client ACK Round Trips	Number of client ACK RTs observed during the monitoring interval

Client Server Application Responses Window

Table D-40 provides definitions of the critical fields of the Client-Server Application Responses window.

Table D-40 Client-Server Application Responses Window

Field	Description
Number of Responses	Total number of responses observed during the monitoring interval
Minimum Client Network Time (ms)	Minimum network time measured by analyzing TCP three-way handshake sequence.
Average Client Network Time (ms)	Average network time measured by analyzing TCP three-way handshake sequence.
Maximum Client Network Time (ms)	Maximum network time measured by analyzing TCP three-way handshake sequence.
Minimum Server Network Time (ms)	Minimum network time between a server and NAM probing point.
Average Server Network Time (ms)	Average network time between a server and NAM probing point.
Maximum Server Network Time (ms)	Maximum network time between a server and NAM probing point.
Minimum Total Response Time (ms)	The total amount of time between the client request and the final response packet from the server.
Average Total Time (ms)	Average time (ms) elapsed from the start of a client request to the completion of server response. Transaction times might vary significantly depending upon application types. Relative thresholds are useful in this situation. Transaction time is a key indicator when detecting application performance anomalies.
Maximum Total Time (ms)	The total amount of time between the client request and the final response packet from the server.

Client-Server Application Transactions Window

Table D-41 provides definitions of critical fields in the Client-Server Application Transactions window.

Table D-41 Client-Server Application Transactions Window

Field	Description
Number of Transactions	Total number of transactions observed during the monitoring interval.
Average Transaction Time (ms)	Average time elapsed from the start of a client request to the completion of server response. Transaction times might vary significantly depending upon application types. Relative thresholds are useful in this situation. Transaction time is a key indicator when detecting application performance anomalies.
Average Server Response Time (ms)	Amount of time it takes a server to send the initial response to a client request as seen by the NAM.
Average Data Transmission Time (ms)	Elapsed time from the first server-response packet to the last server-response packet, excluding retransmission time.
Average Retransmission Time (ms)	Average time to retransmit lost packets per transaction
Client ACK Round Trip Time (ms)	Average network time for the client to acknowledge (ACK) a server data packet as observed at NAM probing point

Client-Server Network Responses Window

Table D-42 describes the critical fields of the Client-Server Network Response Time window.

Table D-42 Client-Server Network Responses Window

Field	Description
Minimum Client Network Time (ms)	Minimum network time measured by analyzing TCP three-way handshake sequence.
Average Client Network Time (ms)	Average network time measured by analyzing TCP three-way handshake sequence.
Maximum Client Network Time (ms)	Maximum network time measured by analyzing TCP three-way handshake sequence.
Minimum Server Network Time (ms)	Minimum network time measured by analyzing TCP three-way handshake sequence.
Average Server Network Time (ms)	Average network time measured by analyzing TCP three-way handshake sequence.
Maximum Server Network Time (ms)	Maximum network time measured by analyzing TCP three-way handshake sequence.
Minimum Network Time (ms)	Minimum of the network time measured by analyzing TCP three-way handshake sequence. Network Time is the sum of Client Network Time and Server Network Time. NAM measures the Network Time using TCP 3-way handshakes. If there are no new TCP connections made during the monitoring interval, this metric is not reported.

Table D-42 Client-Server Network Responses Window (continued)

Field	Description
Average Network Time (ms)	Average of the network time measured by analyzing TCP three-way handshake sequence.
Maximum Network Time (ms)	Maximum of the network time measured by analyzing TCP three-way handshake sequence.

DSCP Detail Window

Table D-43 describes the critical fields in this window.

Table D-43 DSCP Detail

Field	Description
Bytes/sec	Traffic rate; number of bytes per second. In **Administration > System > Preferences**, you can choose to display NAM data in Bits or Bytes.
Packets/sec	Traffic rate; number of packets per second

Host Detail Window

Table D-44 describes the critical fields in this window.

Table D-44 Host Detail

Field	Description
In Bits/sec	Number of bits per second incoming
In Packets/sec	Number of packets per second incoming
Out Bits/sec	Number of bits per second outgoing
Out Packets/sec	Number of packets per second outgoing

Interfaces Stats Table

Table D-45. describes the critical fields in the Interfaces Stats table.

Table D-45 Interfaces Stats Table

Field	Description
Interface	Interface number.
In % Utilization	Utilization percentage of the port.
Out % Utilization	Utilization percentage of the port.
In Packets/s	Number of incoming packets collected per second.
Out Packets/s	Number of outgoing packets sent out per second.
In Bits/s	Number of bits collected per second.
Out Bits/s	Number of bits sent out per second.

Table D-45 Interfaces Stats Table (continued)

Field	Description
In Non-Unicast/s	Number of non-unicasts collected per second.
Out Non-Unicast/s	Number of non-unicasts sent out per second.
In Discards/s	Number of discards collected per second.
Out Discards/s	Number of discards sent out per second.
In Errors/s	Number of errors collected per second.
Out Errors/s	Number of errors sent out per second.

Last 50 Alarms Table

Table D-46 describes the critical fields on the Last 50 Alarms table.

Table D-46 Last 50 Alarms

Field	Description
Site	This contains site or source and destination sites (source - destination) of the network traffic that generated the alarm message.
Alarm Triggered By	Details information of the network traffic that generated the alarm message. The format of the alarm triggered by string are: • Triggered by application threshold: application • Triggered by application with DSCP threshold: DSCP:codepoint - application • Triggered by host threshold: host • Triggered by host with application threshold: host - application • Triggered by host with application and DSCP: DSCP: code point - host - application • Triggered by host with DSCP: DSCP: code point - host • Triggered by conversation: source - destination • Triggered by conversation with application: source - application - destination • Triggered by response time: IAP: client - application - server. • Triggered by DSCP: DSCP: code point • Triggered by RTP stream: source - source port - codec(codec string) - SSRC(number) - destination - destination port • Triggered by voice signaling: Calling (address - number) Called (address - number) ID/References (id() - ref (calling:called)) • Triggered by NetFlow interfaces: NetFlow: Device (address) - If-Index(number) - Ingress/Egress
Threshold Variable	Parameter of the threshold that is used to evaluate alarm condition.
Threshold Value	User defined rising value of the threshold variable.
Triggered Time	Time when the alarm condition was found occurred.

Table D-46 Last 50 Alarms (continued)

Field	Description
Triggered Value	Parameter value when the alarm condition was raised. Note: The triggered value could be - when the viewing window does not included the alarm when it was occurring.
Clear Time	Time when the alarm condition was resolved. The alarm variable has fallen below the falling threshold value.

Server Application Responses Window

Table D-47 provides definitions of the critical fields of the Server Application Responses window.

Table D-47 Server Application Responses Metrics

Field	Description
Average Client Network Time (ms)	Client Network Time is the network time between a client and the NAM switch or router. In WAAS monitoring, Client Network Time from a WAE client data source represents the network RTT between the client and its edge WAE, while Client Network Time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).
Maximum Client Network Time (ms)	
Average Server Response Time (ms)	Server Response Time is the time it takes an application server (for example, a web server) to respond to a request. This is the server *think time*, which is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application and/or server resources, such as the CPU, Memory, Disk, or I/O.
Maximum Server Response Time (ms)	
Average Total Response Time (ms)	Total Response Time is the total amount of time between the client request and when the client receives the first response packet from the server.
Maximum Total Response Time (ms)	

Server Application Transactions Window

Table D-48 provides definitions of the critical fields of the Server Application Transactions window.

Table D-48 Server Application Transactions Metrics

Field	Description
Average Transaction Time (ms)	Average time (ms) elapsed from the start of a client request to the completion of server response. Transaction times might vary significantly depending upon application types. Relative thresholds are useful in this situation. Transaction time is a key indicator when detecting application performance anomalies.
Average Server Response Time (ms)	Amount of time it takes a server to send the initial response to a client request as seen by the NAM.
Average Data Transfer Time (ms)	Average elapsed time from the first server-response packet to the last server-response packet, excluding retransmission time. Data transfer time is always measured in the server-to-client direction and can be used to detect problems for a particular type of transaction of an application.
Average Retransmission Time (ms)	Average time to retransmit lost packets, per transaction.
Client ACK Round Trip Time (ms)	Average round trip time for the client to acknowledge (ACK) a server TCP packet.

Server Network Responses Window

Table D-49 provides definitions of the critical fields of the Server Network Response Times window.

Table D-49 Server Network Responses Window

Field	Description
Average Server Network Time (ms)	Average of the Server Network Time (network time between a server and NAM probing point).
Maximum Server Network Time (ms)	Maximum of the Server Network Time (network time between a server and NAM probing point).
Average Network Time	Average of the network time between client and server. Network Time is the sum of Client Network Time and Server Network Time. NAM measures the Network Time using TCP 3-way handshakes. If there are no new TCP connections made during the monitoring interval, this metric is not reported.
Maximum Network Time	Maximum of the network time between client and server.
Server Bytes	Number of TCP payload bytes sent from the server(s) during the monitoring interval.
Client Bytes	Number of TCP payload bytes sent from the client(s) during the monitoring interval.

Calls Table

Table D-50 provides definitions of the critical fields of the Calls Table.

Table D-50 Calls Table

Field	Description
Calling Number	Calling number as it appears in the signaling protocol.
Called Number	Called number as it appears in the signaling protocol.
Calling Host Address	RTP receiving address of the calling party detected by the NAM from inspecting the call signaling protocol.
Calling Port	RTP receiving port of the calling party detected by NAM from inspecting call signaling protocol.
Calling Alias	Calling party name detected by NAM from inspecting call signaling protocol.
Called Host Address	IP address of the phone receiving the call.
Called Port	Port of the phone receiving the call.
Called Alias	Alias name, MGCP endpoint ID, or SIP URI of the called party phone.
Calling Reported Jitter (ms)	Jitter value reported by calling party at the end of the call.
Calling Reported Packet Loss (%)	Percentage of packet loss reported by calling party at the end of the call.
Start Time	Time when the call was detected to start.
End Time	Time when the call was detected to end.
Duration	Duration of the call. **Note** When the call signaling's call tear down sequence is not detected by the NAM, the NAM will assume: - the call ended after 3 hours in low call volume per interval - the call ended after 1 hour in high call volume per interval (high call volume is defined as call table filled up during the interval.)
Called Reported Jitter (ms)	Jitter value reported by called party at the end of the call.
Called Reported Pkt Loss (%)	Percentage of packet loss reported by called party at the end of the call.

RTP Stream for Selected Call Report Statistics

Table D-51 provides definitions of the critical fields of the RTP stream statistics of a selected call calculated by the NAM.

Table D-51 RTP Streams for the Selected Call Table

Field	Purpose
Source Address	IP Address of the originator of the RTP stream
Source Port	UDP port of the originator of the RTP stream
Destination Address	IP address of the receiver of the RTP stream

Table D-51 RTP Streams for the Selected Call Table (continued)

Field	Purpose
Destination Port	UDP port of the receiver of the RTP stream
Codec	Encoding decoding format/algorithm of the RTP stream
SSRC	Synchronization source number as it appear in the RTP header
Duration Weighted MOS	NAM calculated score that takes into account of the duration of the stream
Duration Weighted Jitter	Jitter that takes into account of the duration of the RTP stream among all per-interval reports
Overall Adjusted Packet Loss	Percentile of adjust packets lost against total packets of all per-interval RTP reports.

Video Signaling Channel

Table D-52 provides definitions of the critical fields of the video signaling channel.

Table D-52 Video Signaling Channel

Field	Description
Video Source IP/Port	Video stream sending IP address/L4 port of the signaling session detected by the NAM from the media signaling protocol.
Video Destination IP/Port	Video stream receiving IP address/L4 port of the signaling session detected by the NAM from the media signaling protocol.
Signaling Protocol	Signaling protocol.
Codec	Encoding decoding format/algorithm of the video stream.
Payload Type	RTP payload type in video stream detected by NAM from inspecting call signaling protocol.
Media Transport Protocol	Transport protocol of video stream detected by NAM from inspecting call signaling protocol.
Source Alias	Video source host name or calling party name detected by NAM from inspecting call signaling protocol.
Destination Alias	Video destination host name or calling party name detected by NAM from inspecting call signaling protocol.
SSRC	Synchronization source number in the RTP header from inspecting call signaling protocol.
Start Time	Time when the video channel was setup and detected by the NAM.
End Time	Time when the video channel was ended and detected by the NAM.
Duration	Video stream duration.
Signaling Server IP/Port	IP Address/L4 port of signaling server.
Signaling Client IP/Port	IP Address/L4 port of signaling client.
Signaling Session VLAN	VLAN of signaling session packets.
Signaling Transport Protocol	Transport layer protocol of signaling session.

Video Stream Conversations

Table D-53 provides definitions of the critical fields of the Video Stream Conversations.

Table D-53 Video Stream Conversations

Field	Description
Source Address/Port	IP Address/L4 port of the originator of video stream.
Destination Address/Port	IP Address/L4 port of the receiver of video stream.
SSRC	Synchronization source number as it appears in the RTP header of the video stream.
Program ID: Sortable	Program ID for MPEG2-TS video traffic.
Codec	Encoding decoding format/algorithm of the video stream.
Protocol	Codec protocol, it could be H264, MPEG2-TS or the others supported by NAM.
Avg I Frame Loss Rate (%)	I-Frame loss rate in average of this period in percentage.
Avg All Frame Loss Rate (%)	Frame loss rate in average of this period in percentage.
Avg DF(ms)	Delay Factor average of this period in unit of ms.
Avg MLR (packet(s))	Media Loss Rate in average of this period, it is the percentage rate of packets loss.

Media Signaling Sessions

Table D-54 provides definitions of the critical fields of the media signaling sessions.

Table D-54 Media Signaling Sessions

Field	Description
Called or Server IP/Port	IP Address/L4 port of video server or video sender of calling party.
Calling or Client IP/Port	IP Address/L4 port of video client or video receiver of calling party.
Called or Server alias	Calling party name detected by NAM from inspecting call signaling protocol or video server alias. It could be MGCP endpoint ID, or SIP URI of the called party phone and so on.
Calling or Client Alias	Called party name detected by NAM from inspecting call signaling protocol or video client alias. It could be MGCP endpoint ID, or SIP URI of the called party phone etc.
Protocol	Signaling protocol of this media session.
Start Time	Time when the signaling session was detected to start.
End Time	Time when the signaling session was detected to end.
Duration	Duration of this signaling session.
Calling Number	Calling number as it appears in the signaling protocol, if it is a VoIP call.
Called Number	Called number as it appears in the signaling protocol, if it is a VoIP call.

RTP Stream for Selected Media Signaling Session

Table D-55 provides definitions of the critical fields of the RTP stream statistics of a selected media signaling session.

Table D-55 RTP Streams for the Selected Media Signaling Session

Field	Purpose
Source Address/Port	IP address or UDP port of the originator of the RTP stream.
Destination Address/Port	IP address or UDP port of the receiver of the RTP stream.
Codec	Encoding decoding format/algorithm of the RTP stream.
SSRC	Synchronization source number as it appears in the RTP header.
Duration Weighted MOS	NAM calculated score that takes into account of the duration of the stream.

RTP Conversations Table

Table D-56 provides definitions of the critical fields of the RTP Conversations Table.

Table D-56 RTP Conversations Table

Field	Purpose
Start Time	Time when the RTP stream was discovered by the NAM
Source Address	IP Address of the originator of the RTP stream
Source Port	UDP port of the originator of the RTP stream
Destination Address	IP address of the receiver of the RTP stream
Destination Port	UDP port of the receiver of the RTP stream
Codec	Encoding decoding format/algorithm of the RTP stream
SSRC	Synchronization source number as it appear in the RTP header
Duration Weighted MOS	NAM calculated score that takes into account of the duration of the stream

Capture User Interface Windows

This section includes the following topics:

Capture Analysis Window

Table D-57 describes the Capture Analysis window fields.

Table D-57 Capture Analysis Window Fields

Field	Description
Capture Overview	Provides a summary of the displayed capture including number of packets captured, bytes captured, average packet size, capture start time, duration of capture, and data transfer rate (both bytes and bits per second)
Traffic over Time	Displays a graphic image of network traffic (KB/second)
Protocol Statistics	Displays packets and bytes transferred for each protocol
Hosts Statistics	Displays packets and bytes transferred for each host address

Capture Session Fields

Table D-58 describes the critical fields on the **Capture > Packet Capture/Decode > Sessions** page.

Table D-58 Capture Session Fields

Operation	Description
Start Time	Time the capture was last started. You can stop and restart the capture as many times as necessary.
Size (MB) (Capture to Memory) **Size (MB) x No. files (Capture to Files)**	Size of the session **Note** *Capture to files* indicates the capture is being stored in one or more files and is a link to those files. The capture file size is limited to 500 MB on Nexus 1000V and vNAM. On all other NAM platforms, the capture file size limit is 2,000 MB.
State	The current status of the capture: • Running—Packet capture is in progress • Stopped—Packet capture is stopped. Captured packets remain in buffer, but no new packets are captured • Full—The memory or file is full, and no new packets will be captured.
Location	The location of the capture (Memory, Local Disk, and external storage).
Capture Operation Buttons	
Create	Create a new capture session. See Configuring Capture Sessions, page 4-6.
Edit	Edit the settings of the selected capture.
Delete	Delete a selected session. Not available if capture session is running.
Start	Start capturing to a selected session. The number in the Packets column for that session will start to increase.
Stop	Stop capturing to the selected session (no packets will go through). Capture data remains in the capture memory buffer, but no new data is stored. Click Start to resume the capture.
Clear	Clear captured data from memory.

Table D-58 Capture Session Fields (continued)

Operation	Description
Decode	Display details of the capture session.
Save to File	Save a session to a file on the NAM hard disk. See Working with Capture Files, page 4-21.

Capture Setting Fields

Table D-59 describes the Capture Settings fields.

Table D-59 Capture Settings Fields

Field	Description	Usage Notes
Packet Slice Size (bytes)	The slice size in bytes; used to limit the size of the captured packets.	Enter a value between 64 and 9000. Enter zero (0) to not perform slicing. If you have a small session but want to capture as many packets as possible, use a small slice size. If the packet size is larger than the specified slice size, the packet is *sliced* before it is saved in the capture session. For example, if the packet is 1000 bytes and slice size is 200 bytes, only the first 200 bytes of the packet is stored in the capture session.
Capture Source	Data-Ports or ERSPAN	Choose the capture source (check one or more check boxes): • Data-ports: This accepts SPAN, RSPAN, and VACL capture. On NAM-NX1, you can select only one data-port at a time. • ERSPAN: Locally terminated is recommended. **Note** On some platforms, you may be limited to selecting only one of the dataports at a time. Most platforms allow you to select both dataports at once.
Storage Type: Memory	Check to store captures in memory	Enter values for **Memory Size** for this capture. Enter a number from 1 up to your platform maximum. If system memory is low, the actual session size allocated might be less than the number specified here. Check (if desired) **Wrap when Full** to enable continuous capture (when the session is full, older packet data is removed to make room for new incoming packets). If you do not check **Wrap when Full**, the capture will end when the amount of data reaches size of session.

Table D-59 Capture Settings Fields (continued)

Field	Description	Usage Notes
Storage Type: File(s)	File Size (MB)	Enter a value for **File Size** (file size can be from 1 MB to 500/2000 MB depending on your platform). If disk space is not available, you are not able to start new capture-to-disk sessions.
	Number of Files	Enter a value for Number Of Files to use for capture. The maximum is determined on the size of the file, numbers of files stored, and the amount of disk space available at the location where these files are stored.
	Rotate Files	Use this feature if you plan to capture sets of small files that allow you to perform instantaneous downloads, decodes, and analysis. Rotating files allows you to automatically maintain your storage space. Check the Rotate Files check box to rotate files. Available only for remote storage or NAM appliances. For information about configuring remote storage, see About Capturing to Data Storage, page 4-25. If you choose the **Rotate Files** option, when you reach the highest number file, the earliest file is overwritten. For example, if you specify **No. Files** to 10, file **CaptureA_1** is overwritten after the NAM writes capture data to file **CaptureA_10**. To determine the most recent capture, check each file's time stamp.
	File Location	If file data storage is available, choose one of the storage targets in the drop-down list. The drop-down list displays only those targets in the Ready state. Local disk is the default, or choose a previously configured remote storage location if available. Each option shows the amount of disk space available for capture packet storage. Maximum capture session size for capture to disk is determined by the available space on the capture target. You can manage these locations from the **Capture > Data Storage** page (see Utilizing Capture Data Storage, page 4-24).

Custom Decode Filter Dialog Box

Table D-60 describes the critical fields on the custom decide filter window.

Table D-60 Custom Decode Filter Dialog Box

Field	Description	Usage Notes
Protocol	The protocol to match with the packet.	Choose a protocol from the list. (Select **All** to match all packets regardless of protocol.)
Address (MAC or IP)	Indicates whether to filter by MAC or IP address.	Choose MAC to filter using the source/destination MAC address of the packets. Choose IP to filter using the source/destination addresses of the packets.
Both Directions	Indicates whether the filter is applied to traffic in both directions.	If the source is host A and the destination is host B, enabling both directions filters packets from A to B and B to A. If the source is host A and the destination is not specified, enabling both directions filters packets both to and from host A.
Offset	The offset (in bytes) from the Base where packet data-matching begins.	Enter a decimal number.
Base	The base from which the offset is calculated. If you select absolute, the offset is calculated from the absolute beginning of the packet (for example, the beginning of the Ethernet frame). If you select protocol, the offset is calculated from the beginning of the protocol portion of the packet. If the packet does not contain the protocol, the packet fails this match.	Choose **absolute** or a protocol.

Table D-60 Custom Decode Filter Dialog Box (continued)

Field	Description	Usage Notes
Data Pattern	The data to be matched with the packet.	Enter *hh hh hh ...*, where *hh* are hexadecimal numbers from 0-9 or a-f. Leave blank if not applicable.
Filter Expression	An advanced feature to set up complex filter conditions. The simplest filter allows you to check for the existence of a protocol or field. For example, to see all packets that contain the IPX protocol, you can use the simple filter expression **ipx**.	See Tips for Creating Custom Decode Filter Expressions, page 4-35.

Custom Decode Subexpressions Fields

Table D-61 describes the custom decode fields and provides filter and format details.

Table D-61 Custom Decode Field Subexpressions

Field	Filter By	Format
eth.addr eth.src eth.dst	MAC address	*hh:hh:hh:hh:hh:hh*, where h is a hexadecimal number from 0 to 9 or a to f.
ip.addr ip.src ip.dst	IP address	*n.n.n.n or n.n.n.n/s*, where n is a number from 0 to 255 and s is a 0-32 hostname that does not contain a hyphen.
tcp.port tcp.srcport tcp.dstport	TCP port number	A decimal number from 0 to 65535.
udp.port udp.srcport udp.dstport	UDP port number	A decimal number from 0 to 65535.
protocol	Protocol	Click the Protocol list in the Custom Decode Filter dialog box to see the list of protocols on which you can filter.
protocol [*offset*:*length*]	Protocol data pattern	*hh:hh:hh:hh...*, where hh is a hexadecimal number fro 0 to 9 or a to f. *offset* and *length* are decimal numbers. *offset* starts at 0 and is relative to the beginning of the *protocol* portion of the packet.
frame.pkt_len	Packet length	A decimal number that represents the packet length, not the truncated capture packet length.

Error Scan Window

Table D-62 describes the Error Scan window fields.

Table D-62 Error Scan Window Descriptions

Field	Description
Severity	**Warn**: Warning; for example, an application returned an unusual error code **Error**: A serious problem, such as malformed packets
Group	**Checksum**: A checksum was invalid **Sequence**: Protocol sequence is problematic **Response Code**: Problem with the application response code **Request Code**: An application request **Undecoded**: Dissector incomplete or data can't be decoded **Reassemble**: Problems while reassembling **Malformed**: Malformed packet or dissector has a bug; dissection of this packet aborted

Hardware Filter Dialog Box

Table D-63 describes the Create Hardware Filter dialog box.

Table D-63 Create Hardware Filter Dialog

Attribute	Options	Range
Data Ports	Both Ports, Data Port 1, Data Port 2	—
Frame Length	Equal To, Not Equal To, Greater Than, Less Than	Min. 64, Max 65535
VLAN IDs	Equal To, Not Equal To, Greater Than, Less Than	Min. 1, Max 4095
MPLS Label	Equal To, Not Equal To	Min. 0, Max 1048575
Source Address / Mask	Equal To, Not Equal To	IPv4 address
Destination Address / Mask	Equal To, Not Equal To	IPv4 address
L4 Protocol	Equal To, Not Equal To ICMP, IGMP, IP in IP, GRE, L2Tp, TCP, UDP, Integer	With Custom, you can enter a custom value that is not in the list of common protocols. Enter min. 1, max 255.
L4 Source Port	Equal To, Not Equal To	Min. 1, Max 65535
L4 Destination Port	Equal To, Not Equal To	Min. 1, Max 65535
Pattern Match	Filters packets based on 4-byte hexadecimal patterns anywhere in the first 256 bytes. Equal To, Not Equal To	

NAM Packet Analyzer Decode Window

Table D-64 describes the critical fields on the NAM Packet Analyzer window.

Table D-64 Packet Browser

Field	Description
No.	Packet numbers, listed numerically in capture sequence. If the decode (display) filter is active, the packet numbers might not be consecutive.
Time	Time the packet was captured relative to the first packet displayed (not the first packet in the session). To see the absolute time, see the Detail window.
Source	Packet source, which might be displayed as hostname, IP, IPX, or MAC address. To turn hostname resolution on and off for IP addresses, choose the Setup tab and change this setting under Preferences.
Destination	Packet destination, which might be displayed as hostname, IP, IPX, or MAC address.
Protocol	Top-level protocol of the packet.
Length	Size of the packet, in bytes.
Info	Brief text information about the packet contents.

Software Filter Dialog Box

Table D-65 describes key Software Filter dialog box fields.

Table D-65 Software Filter Dialog Box

Field	Description	Usage Notes
Name	Name of the software filter.	Enter the name of the software filter.
Source Address / Mask	Source address of the packets.	• For IP, IPIP4, GRE.IP, or GTP.IPv4 addresses, enter a valid IPv4 address in dotted-quad format *n.n.n.n,* where *n* is 0 to 255. The default (if blank) is 255.255.255.255. • For IPv6 or GTP.IPv6 addresses, enter a valid IPv6 address in any allowed IPv6 address format. For example: – 1080::8:800:200C:417A – ::FFF:129.144.52.38 **Note** See RFC 5952 for valid text representations. For MAC address, enter *hh hh hh hh hh hh,* where *hh* is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff.
	The mask applied to the source address.	• If a bit in the Source Mask is set to 1, the corresponding bit in the address is relevant. • If a bit in the Source Mask is set to 0, the corresponding bit in the address is ignored.

Table D-65 Software Filter Dialog Box (continued)

Field	Description	Usage Notes
Destination Address / Mask	Destination address of the packets.	• For IP, IPIP4, GRE.IP, or GTP.IPv4 addresses, enter a valid IPv4 address in dotted-quad format *n.n.n.n,* where *n* is 0 to 255. The default (if blank) is 255.255.255.255. • For IPv6 or GTP.IPv6 addresses, enter a valid IPv6 address in any allowed IPv6 address format. For example: – 1080::8:800:200C:417A **Note** See RFC 5952 for valid text representations. For MAC address, enter *hh hh hh hh hh hh,* where *hh* is a hexadecimal number from 0 to 9 or a to f. The default is ff ff ff ff ff ff.
	The mask applied to the destination address.	• If a bit in the Dest. Mask is set to 1, the corresponding bit in the address is relevant. • If a bit in the Dest. Mask is set to 0, the corresponding bit in the address is ignored.
Network Encapsulation	The protocol to match with the packet.	
Both Directions (check box)	This check box indicates whether the filter is applied to traffic in both directions.	If the source is host A and the destination is host B, enabling both directions filters packets from A to B and B to A. If the source is host A and the destination is not specified, enabling both directions filters packets both to and from host A. The “both directions” check box also affects the ports and not only the addresses (the same logic applies).
VLAN Identifier(s)	The 12-bit field specifying the VLAN to which the packet belongs.	Choose a VLAN Range or enter an individual VLAN IDs. Prime NAM filters the first VLAN only. If you include a range, note this limitation. The VLAN ID can range from 1-4095.

Table D-65 Software Filter Dialog Box (continued)

Field	Description	Usage Notes
TCP Flag Bits	• URG – Indicates that the urgent pointer field is significant. • ACK – Indicates that the acknowledgment field is significant. • PSH – Indicates Push function. • RST – Indicates to reset the connection (You can see this on rejected connections). • SYN – Indicates that it synchronizes sequence numbers (You can see this on new connections). • FIN – Indicates that there is no more data from sender (You can see this after a connection is closed).	This is for TCP packets only. The six flags can be selected individually or combined with other flag(s) using AND/OR logic. Only packets that have those selected flags set will be captured.
Application[1]	Select the **Application** drop list to filter by application.	Select one protocol to capture from the Application drop-down list.
Source Port(s)	Select the **Port** radio button to filter by port.	Enter one or more ports separated by commas.
Destination Port(s)		Enter one or more ports separated by commas.
IP Protocol		Choose TCP, UDP, or SCTP. No selection (default) means that any will be allowed.

1. The application filter can be used to filter on the highest layer of the protocol parsing; that is usually a layer 4 protocol (based on port). If you want to filter on the transport protocol (for example, UDP or TCP), you will need to use the "IP Protocol" selector. Selecting, for example, TCP in the "IP Protocol" selector will filter on all packets using TCP.

Administration User Interface Windows

This section includes the following sections:

System Overview

9

Table D-66 System Overview

Field	Description
Inputs Tab	
Cumulative Input Statistics	Health and usage information on all the traffic received by the NAM. It shows the number of packets received (Rx Packets), number of packets lost or dropped (Rx Packets Lost), and number of bytes received (Rx Bytes). The Cumulative column shows cumulative counts since the start of the NAM, and the Rate column one shows the same counters for the last ten seconds.
Input Traffic	Usage information in bytes and packets based on the input you select. You can toggle between a chart or table format. Data is updated every 30 seconds and contains data from the past hour. The table time interval cannot be changed. The input table rate is calculated every 10 seconds. A table legend provides data for standard statistics provided by the software for data collected over a period of time. To reset the traffic counters, click on **Reset Traffic** at the bottom of Input Traffic chart.
Resources Tab	
Date	Current date and time synchronized with the switch, router, or NTP server.
IPv4 Address **IPv6 Address**	Based on your configuration, IPv4 address and/or IPv6 address displays.
System Uptime	Length of time the host has been running uninterrupted.
Disk Usage	Config, data, and root partitions with their total and free space. Also shows the amount of disk space used by the performance data base files (DB) and the packet capture to disk (capture files). Use this information to ensure you have enough disk space and perform the needed maintenance as necessary.
Utilization	Percentage of memory resources being consumed by the NAM as well as the total memory available.
CPU Usage	Percentage of CPU resources being consumed by the NAM. Each individual CPU in a multi-CPU platform is listed separately.

SNMP Agent

Table D-67 System SNMP Agent Dialog Box

Field	Description
Location	(Optional) The physical location of the switch or router in which the NAM is installed.
Community String	Add permission and community string information.

E-Mail Setting

Table D-68 Mail Configuration Options

Field	Description
Enable Mail	Enables e-mail of reports and notification of alarms
External Mail Server	IP address or hostnameof external mail server
Send Test Mail to	Optional. List e-mail addresses for up to three e-mail recipients.Use this as a verification of your mail setup.
Mail Alarm to	This recipient will receive alarm notifications and scheduled exports. Enter multiple addresses using space or comma delimiters.
Advanced Settings	Enables you to designate an e-mail access server port, as well as select a encryption protocol.
Mail Server Port	Optional. Designate an e-mail port for the NAM.If your mail server is configured with a non-default server port number, use this field to ensure it works with Prime NAM.
Mail Server Encryption	Optional. Select Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption for e-mail messaging. Use these encryption protocols to authenticate servers and clients and encrypt messages between you and Prime NAM.

Preferences

Table D-69 describes the critical fields of the Preferences window.

Table D-69 System View and Logging Preferences

Field	Description
Idle Timeout (1-1440 min)	An idle timeout is supported to prevent unauthorized access to the NAM GUI or CLI. Default value is 30 minutes.
Refresh Interval (60-3600 sec)	Amount of time between refresh of information on dashboards. Default is 300.
Top N Entries (1-10)	Number of entries on the Top N charts. Default is 5. To view up to 100 entries, use the Table view versus the chart view.

Table D-69 System View and Logging Preferences (continued)

Field	Description
Perform IP Host Name Resolution	Display hostnames instead of IP Addresses. This option performs translation using DNS lookup. Ensure you set your DNS nameserver parameters. See Setting Network Parameters, page 5-3.
Traffic Display Unit	Data displayed in graph and tables; Bits (default) or Bytes.
Response Time Display Unit	Default is automatic. Options include: microseconds, milliseconds, and seconds.
International Notation	Display options for numbering. May affect report accuracy; see the Cisco Bug Search tool for details.
Audit Trail	Display a listing of recent events that have been recorded. This includes CLI and GUI configuration events. To view, choose **Administration > Diagnostics > Audit Trail**.
IP TOS Flow Key	Include type of service (TOS) data in the NAM network flow. Select only if you are measuring Differentiated Services Code Point (DSCP) for monitored traffic. If you require ART and other flow-based analysis and expect that the TOS information in your network may change in an on-going flow, do not select TOS information to be part of flow configuration. **Note** If TOS byte changes in an on-going flow this results in a new flow being created. If this option is not selected, the entire flow transaction is treated as one flow regardless of a TOS change in this flow. If your network configuration allows the IP TOS value to change dynamically during the life of a flow, and you enable the IP TOS Flow Key option, then the ART and application classification features may not work accurately. These features are based on the state of each flow, and rely on seeing all the packets for a flow grouped together. However, if the IP TOS value changes during a flow, then that flow will be broken into two or more flows when the IP TOS is used as a key. Disabling the IP TOS Flow Key option will correct these issues. However, in this case your DSCP statistics becomes inaccurate because only the first IP TOS value will be recorded for each monitored flow. See Using NAM to Monitor QoS/DiffServ (DSCP).

New User Dialog Box

Table D-70 describes the critical fields in the New User dialog box.

Table D-70 New User Dialog Box

Field	Description	Usage Notes
Password **Verify Password**	The account password	Enter a password that adheres to your site security policies.
Privileges	Privileges associated with this account	Select each privilege to grant to the user.

User Privileges

Table D-71 describes the critical fields in the User Privileges window.

Table D-71 User Privileges

Privilege	Access Level
Report	Enables a user to schedule and view the saved reports through the web interface, as well as access the saved reports through file sharing. See Sharing Files, page 7-41 for details.
AccountMgmt	Enables a user to create, delete, and edit user accounts.
SystemConfig	Enables a user to edit basic NAM system parameters such as IP address, gateway, HTTP port, and so on.
Capture	Enables a user to perform packet captures, manage capture sessions, use the NAM packet analyzer to decode packet data and access capture files through file sharing.
AlarmConfig	Enables a user to create, delete, and edit alarms on the switch/router and NAM.
MonitorConfig	Enables a user to create, delete, and edit the following: • Collections and reports • Protocol directory entries • Protocol groups • URL-based applications
MonitorView	Enables a user to view monitoring data and reports (granted to all users).

TACACs+ Authentication and Authorization

Table D-72 TACACS+ Authentication and Authorization Dialog Box

Field	Usage Notes
Enable TACACS+ Authentication and Authorization	Determines whether TACACS+ authentication and authorization is enabled. • To enable, check the check box. • To disable, uncheck the check box.
Primary TACACS+ Server	Enter the IP address of the primary server.

Table D-72 TACACS+ Authentication and Authorization Dialog Box (continued)

Backup TACACS+ Server	Enter the IP address of the backup server (optional). **Note** If the primary server does not respond after 30 seconds, the backup server will be contacted.
Secret Key	Enter the TACACS+ secret key.
Verify Secret Key	Reenter the TACACS+ secret key.

Current User Sessions

Table D-73 describes the critical fields in the Current User Sessions window.

Table D-73 Current User Sessions

Field	Description
From	The name of the machine the user logged in from.
Last Activity	The time stamp of the last user activity.

Report Descriptions

Table D-74 lists the MIB objects supported by the NAM.

Table D-74 NAM RMON Support

Description	Source
MIB-II: All groups except Exterior Gateway Protocol (EGP) and transmission.	RFC 1213
RMON-MIB: Alarm and Event groups only	RFC 2819
RMON2: trapDestTable only	RFC 2021
CDP-MIB: Cisco Discovery Protocol	
EntityMIB	RFC 2737