CHAPTER 6

NAM Deployment

This chapter describes usage scenarios for the Cisco Prime Network Analysis Module 5.1. Each scenario focuses on a need to be addressed or a problem to be solved. The scenario takes into account the deployment considerations discussed in Chapter 1, “Overview,” and then uses one or more of NAM’s features to meet the need or solve the problem. The goal of these use cases is to provide real-world examples that put the information provided in this User Guide to use in real-world use cases. These examples discuss best practices and approaches to effective NAM deployment.

This chapter contains the following sections:

Deployment
- Using NAMs to Monitor VoIP Quality, page 6-2
- Autodiscovery Capabilities of NAM, page 6-4
- Creating Custom Applications, page 6-5
- Utilizing Sites to Create a Geographically- or Organizationally-Familiar Deployment, page 6-5
- Integrating NAM with Third Party Reporting Tools, page 6-7
- Integrating NAM with LMS, page 6-7
- Monitoring the Nexus 1000V Switch Environment, page 6-8
- Visibility in the Branch, page 6-9
- Monitoring Cisco WAAS and Measuring Its Impact, page 6-10

Monitoring
- Real-Time Traffic Monitoring and Analysis, page 6-14
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-16
- Using NAM for Historical Trends via Interactive Report, page 6-20
- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-23
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications, page 6-23
- Using Nexus 1000V NAM VSB to Monitor Nexus 1000V Switch Environment, page 6-23
- Monitoring the Nexus 1000V Switch Environment, page 6-8

Troubleshooting
- Using NAM for Problem Isolation, page 6-26
Deployment

Using NAMs to Monitor VoIP Quality

Voice quality analysis has been significantly enhanced in Cisco NAM. The software is now capable of accurately measuring voice quality by using the industry-standard MOS algorithm. Call quality measurements are computed every 1 minute and made available through the GUI. Note that the voice-related screens on the NAM GUI are significantly different from previous releases. Changes have been made to provide useful information quickly and automatically, while allowing easy navigation to details.

Deployment: NAM deployments for voice quality analysis require that NAM be able to monitor VoIP packets from the calling phone to the called phone. The branch edge location in the network provides visibility into all calls entering and leaving the branch; similarly a campus edge location monitors calls crossing the campus boundary. Often, the distribution layer is a good location to deploy NAMs for this purpose, especially if specific phones or particular portions of the network are to be monitored. For example, a new Multiprotocol Label Switching (MPLS) link is being piloted and three buildings that are part of Company X's headquarters are part of the pilot. In order to monitor voice quality for those three buildings, a NAM could be deployed at the distribution Catalyst 6500 that serves those users.

Note

The data center is typically not an appropriate location for RTP stream analysis because calls will seldom go through the data center. However, the data center is a good location to monitor signaling messages between phones and Cisco Unified Communications Manager. NAM decodes signaling messages to track call history, caller names, phone numbers, and other relevant call details.

Use the following steps to monitor the network to make sure that call quality is good. If quality issues appear, isolate and troubleshoot the problem rapidly.

Step 1

View RTP Streams using the menu selection Analyze > Media. This chart (as shown in Figure 6-1) indicates current voice quality of all RTP streams being monitored. MOS values range from 1 to 5, where 1 is poor and 5 is excellent (see the legend in Figure 6-1 for a breakdown into categories-Poor, Fair, Good and Excellent). The figure below displays the Top N RTP Source and Destination endpoints. Notice that there are calls that are in the poor range.
Step 2  To isolate calls that had a poor MOS, scroll down to Top N RTP Streams and click on the chart to drill down into the RTP Stream Details. As shown in Figure 6-2, notice that the MOS value for the calls listed on top is 2.88, which is low. Further, looking at the other metrics provided in the same row (for example, row one), notice that jitter is 3.49 and the packet loss rate is 11 percent, resulting in the low MOS value. This information tells you that jitter is the root cause of the poor calls; instead, it is packet loss somewhere in the network.
Step 3  With the endpoints’ IP addresses, you can look at the network topology to identify where in the network the 50.5.10.38 subnet is located. For the purposes of this use case, this subnet is in Building 3 of the main campus. You know that the Building 3 distribution switch has a NAM located in it.

Navigate to that NAM and go to the menu selection Analyze > Managed Device > Interface. This page lists all interfaces and errors or discards on each interface. Look up the link that leaves Building 3 and connects to the core. That interface is likely the source of the packet loss. Check the interface for faults and fix as needed.

See related content Analyzing Traffic, RTP Streams, page 3-38
See related content Setting Voice Signaling Thresholds, page 2-53

Autodiscovery Capabilities of NAM

If you are an existing NAM 4.x user, you will not need to configure the SPAN sessions, and they will be autocreated on the NAM (not on the device). If you are a new NAM 5.x user, you will need to configure SPAN or NetFlow.

SPAN or NetFlow must be already configured on the device to forward traffic to NAM for auto creating the data source.

See related content Data Sources, page 2-13.
Creating Custom Applications

NAM identifies applications/protocols based on the TCP/UDP port number, so if there are applications using custom ports, the NAM can be configured to identify those applications by name instead of the port.

See related content Applications, page 2-73.

Utilizing Sites to Create a Geographically- or Organizationally-Familiar Deployment

Cisco Prime NAM 5.1 introduces the capability for users to define a site, with which you can aggregate and organize performance statistics. A site is a collection of hosts (network endpoints) partitioned into views that help you monitor traffic and troubleshoot problems. A site can be defined as a set of subnets specified by an address prefix and mask, or using other criteria such as a remote device data source (for example, remote WAE device and segment information). If you want to limit the view of your network analysis data to a specific city, a specific building, or even a specific floor of a building, you can use the sites function.

Figure 6-3 shows a centralized NAM deployment analyzing multiple data sources from different locations in the network.

For this deployment, multiple sites can be created such as SanJose-Campus, SanJose-Datacenter, NewYork-NDE-Bldg1, and NewYork-WAAS-Bldg2. The data that does not match the site configuration will be displayed in the Default site. This helps to isolate the view and information for monitoring and troubleshooting so you can drill down to the specific area of interest.

You can also include multiple types of data sources in the site definition, and you can then get an aggregated view of all network traffic.

The predefined “Unassigned Site” makes it easy to bring up a NAM without having to configure user-defined sites. Hosts that do not belong to any user-defined site will automatically belong to the Unassigned Site.
Figure 6-4 shows a list of the sites configured for this deployment.

Figure 6-4  Sites Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td>Catches All Unclassified Hosts</td>
</tr>
<tr>
<td>N1K-ERSFAN</td>
<td></td>
<td>192.168.154.0/24 ERSFAN-192.168.154.18-ID-1</td>
</tr>
<tr>
<td>New York-NDE</td>
<td></td>
<td>2.0.0.0/0 NDE-192.168.169.2-ID-0</td>
</tr>
<tr>
<td>New York-WAAS-Bkg2</td>
<td></td>
<td>WAAS client side</td>
</tr>
<tr>
<td>SanJose-Campus</td>
<td></td>
<td>192.168.0.0/16 DATA PORT 3</td>
</tr>
<tr>
<td>SanJose Datacenter</td>
<td></td>
<td>192.168.154.0/24 DATA PORT 3</td>
</tr>
<tr>
<td>VOIP-RTP</td>
<td></td>
<td>1.0.0.0/0 DATA PORT 3</td>
</tr>
<tr>
<td>VOIP-San Jose</td>
<td></td>
<td>2.0.0.0/0 DATA PORT 3</td>
</tr>
<tr>
<td>WAAS Server</td>
<td></td>
<td>WAAS-192.168.156.235-SrvrMAN</td>
</tr>
<tr>
<td>WAAS Server Passthru</td>
<td></td>
<td>WAAS Server Passthru</td>
</tr>
<tr>
<td>WAAS Client Passthru</td>
<td></td>
<td>WAAS Client Passthru</td>
</tr>
</tbody>
</table>

The interactive dashboard can be used to drill down into either San Jose or New York sites to see Top applications, hosts, VLANs, DSCP, and application response time (as seen in Figure 6-5).

Figure 6-5  Traffic Summary Dashboard

From each of the charts in the dashboard, you can access the context menu to further drill down to analyze data such as detailed application, host, conversation and VLAN traffic.
Figure 6-6 shows the contextual drilldowns from the Top N Applications and Top N Hosts charts.

Figure 6-6  Applications and Hosts Drilldowns

Integrating NAM with Third Party Reporting Tools

NAM 5.1 integrates with the CA NetQoS SuperAgent for the purpose of aggregating Application Response Times. NAM 5.1 also integrates with CompuWare Vantage and InfoVista 5View for Host, Conversation, RTP, and Response Time.

See the NAM 5.1 API Programmer’s Guide for configuring NAM and exporting data from the NAM (ask your Cisco representative).

Integrating NAM with LMS

The NAM GUI can be placed on the LMS (LAN Management Suite) 4.0 dashboard and accessed through the LMS GUI. See technical documentation for LMS on http://www.cisco.com.

Currently, this functionality includes:

- NAM discovery as part of the network topology that LMS builds
- NAM alarms persistent in LMS
- Ease of software updates to multiple NAMs via LMS
- Portal Integration to bring in NAM GUI inside of LMS

You can also check out supported devices for LMS to see what features of FCAPS are covered by what type of NAM:

See Figure 6-7 for a view of the NAM GUI being accessed through LMS GUI.

**Figure 6-7  NAM GUI Available In the LMS GUI**

---

**Monitoring the Nexus 1000V Switch Environment**

The Nexus 1000V switch can be monitored by other NAM platforms running the NAM 5.1 software. In this scenario, you have a NAM-2 deployed in the data center switch and a Nexus 1000V switch for the virtualized environment, and you want to monitor the virtual switch traffic.

**Step 1** Configure the Nexus 1000V Switch to direct ERSPAN or NetFlow to the NAM-2.

**Step 2** Verify that ERSPAN or NetFlow are configured on the Cisco 1000V Switch Virtual Supervisor Module (VSM) that is providing data to NAM by choosing Setup > Traffic > NAM Data Sources.

**Step 3** Create a site for this data source using Setup > Network > Sites (Figure 6-8).
Step 4  Choose Monitor > Overview > Traffic Summary (as shown in Figure 6-9) and Monitor > Overview > Response Time Summary.

Visibility in the Branch

There are three options for providing visibility in the branch:

1. A purpose-built NME-NAM-120S that works in Cisco Integrated Service Router Generation 1
2. NAM as an application, running in SM-SRE-700 or SM-SRE-900 for Cisco Integrated Service Router Generation 2 (ISR G2) deployment
3. Using Performance Agent (PA), a Cisco IOS feature available on ISR G2 that encapsulates traffic statistics as well as application response statistics. Underlying Netflow v9 can be exported to a central NAM in a Data Center (DC) or Campus. PA complements WAAS Express (another IOS feature) and when used together, delivers end-to-end visibility before and after WAN Optimization
using only one traffic source, as compared to two traffic sources NetFlow and WAAS Flow Agent from the traditional WAAS deployment in the branch. See the scenario Monitoring Cisco WAAS and Measuring Its Impact, page 6-10.

The first two options are similar and provide visibility for the local branch as well as branch to branch and the ability to capture all traffic going in and out of the branch.

Ideal deployment for these branch NAM modules would be a small number of remote sites or an empowered branch. The third option provides visibility only for the local branch and is more scalable than deploying NAM modules in multiple remote locations e.g. 100's/1000's remote sites. Based on network monitoring and troubleshooting requirements, a hybrid option can be considered such as deploying NAM modules and PA in empowered branches and PA in smaller branches. In this model, a central NAM in the DC can provide end to end visibility from DC to branch and offers the ability to capture branch to branch traffic on super branches (empowered branch).

For further details on installing NAM on NME-NAM-120S or SM-SRE, see the Installation Guides on Cisco.com. For further details on configuring PA, see Chapter 2, “Setting Up The Cisco NAM”. For further details about the NAM 5.1 release, see the Cisco Prime NAM 5.1 Release Notes on www.cisco.com.

See related content Response Time Summary, page 3-5 and Analyze, Response Time, page 3-18.

Monitoring Cisco WAAS and Measuring Its Impact

Cisco Wide Area Application Services (WAAS) is a comprehensive WAN optimization solution that accelerates applications over the WAN, delivers video to the branch office, and provides local hosting of branch-office IT services. Cisco WAAS allows IT departments to centralize applications and storage in the data center while maintaining LAN-like application performance and provides locally hosted IT services while reducing the branch-office device footprint.

One of the challenges facing IT personnel who deploy WAAS is to measure and report on the benefits provided by their WAN optimization deployment. Accurate measurement provides many benefits: IT can show return on investment; IT can assess whether the improvement gained meets originally advertised expectations from the solution; and finally, IT can use WAAS ongoing for monitoring, troubleshooting, and planning information for expanding the deployment.

The NAM can monitor WAAS-optimized flows by using WAE devices or Performance Agent (PA) as data sources. Using this capability, the NAM is able to provide visibility into optimization-related metrics for the three distinct segments that are created by WAAS: the branch, the WAN, and the data center segments.

Placing a Cisco NAM 2200 series appliance or NAM-2 blade at the edge of the data center is recommended for WAAS deployments. From this location in the network, the NAM can measure local metrics using SPAN technology, and for information on the remote branch segment, it relies on flow agent exports from the remote WAE device, or PA with WAAS Express from an ISR G2 branch router. If NME-NAMs are available, deploying one at the remote branch site is very useful. This NME-NAM can provide user experience at the site before WAAS is enabled and then contrast it to user experience after WAAS is enabled. See Figure 6-10.
To deploy this solution:

**Step 1**  Using a NAM 2220 deployed at the data center, measure application response time before WAAS is enabled using **Analyze > WAN Optimization > Top Talker Detail**. As shown in **Figure 6-11**, this will display such data as utilization, concurrent connections, and average transaction time for top applications, network links, clients, and servers that are possible candidates for optimization.

**Step 2**  Create a WAAS Client Side and WAAS Server Side for the WAAS flows from the DC and Branch WAEs.
Step 3  The NAM provides an interactive dashboard to view the analyzed data. Figure 6-12 displays Client Transaction Time, Traffic Volume and Compression Ratio, Number of Concurrent Connections (Optimized vs. Passthru), and Multi-Segment Network Time (Client LAN - WAN - Server LAN). As you can see in the first graph, all non-optimized traffic is displayed as Passthru.

Figure 6-12  Application Performance Analysis -- Optimized

The screen shot above illustrates the significant improvement experienced by users in the branch when WAAS is turned on. Such reports are very useful to justify an investment in WAN optimization technologies and to show returns on those investments in terms of increase in employee productivity and improved user experience from remote sites.
Step 4

From the perspective of the NAM located in the data center, there are two sources of information for response time measurements. SPAN provides measurement at the data center and exports from the branch; WAAS flow or PA provides measurements from the branch. Using these two sources of information, the NAM at the data center can continuously monitor current response times for each branch and help IT personnel keep user experience within known bounds. When abnormal response times are detected, the NAM can be configured to send alerts to appropriate personnel with information relevant to troubleshooting the problem.

Note

The NAM 2220 in the above scenario can be substituted with the NAM Virtual Blade on the WAVE-574 and WAE-674 to obtain the same type of reports.

See related content WAN Optimization, page 3-17.
Monitoring

Real-Time Traffic Monitoring and Analysis

One of your Network Operations Center (NOC) responsibilities is to monitor the campus network and two branch offices and follow up on any abnormalities that you find in these networks.

The following steps lead you through managing a NAM-2 blade located in the Cisco Catalyst 6500 Series Switch at the campus edge. There is local SPAN and remote NDE traffic being monitored by this NAM. You have defined sites based on those data sources.

---

Step 1  On the Traffic Summary dashboard (Monitor > Overview > Traffic Summary), use the Interactive Report and the Filter button on the left side of the screen to narrow the data on the dashboard to a particular site. Then, you will be able to view the Top Applications, Hosts, VLANs, and DSCP for that site. Take note of the Top Host, or in other words, top bandwidth generator (see Figure 6-14).

![Figure 6-14 Top Applications and Hosts](image)

---

Step 2  Click on the Top Applications graph to drill down to see all the hosts using the GRE application. Notice that this application traffic is being generated by three hosts (see Figure 6-15).

![Figure 6-15 Top N Hosts In and Out](image)
Step 3  Go back to Traffic Summary > Top N Hosts In and Out and click on the host (in the example shown in Figure 6-15, “192.168.152.10”).

Step 4  Select Analyze > Traffic > Host to see how long this host and application have been generating this traffic. The Time Range can be changed using the Interactive Report and the Filter button on the left; a shorter or longer period of time may be needed to understand the pattern and trend.

Step 5  Based on those patterns, thresholds can be configured to alert via e-mail, trap, and syslog. The alert can be used to start a packet capture as well. On the context menu (found by left-clicking on the colored bar), there is an option to initiate a packet capture if desired (see Figure 6-17).
Figure 6-17 One-click Packet Capture

Although the NAM was deployed at the campus edge, other possible locations that offer similar information include the core, distribution (NAM-2 or appliance), and branch office (NME-NAM). This use case illustrates some of the benefits of real-time analysis. You were able to study applications and conversations in real time and were able to take a capture of a particular stream that was of interest. See Application Response Time, page 3-22. See Alarm Actions, page 2-44. See Thresholds, page 2-46.

Using NAM to Monitor QoS/DiffServ (DSCP)

Differentiated Services (DiffServ) provides insight into how traffic is being classified by QoS and detects incorrectly marked or unauthorized traffic. The NAM identifies the application/protocol based on the type of service (ToS) bits setting. The administrator can configure DSCP Groups or use the ones provided (as shown in Figure 6-18). The voice template can be used to monitor whether voice traffic is marked properly. Figure 6-20 displays the DiffServ application statistics for all DSCP value. Looking at this, you will notice that RTP and Session Initiation Protocol (SIP) are listed, which indicates that they are not being correctly marked throughout its path.

In the following scenario, IT has deployed QoS to prioritize VoIP traffic to improve voice quality across the network. The NAMs are deployed in the data center and branches and utilized to monitor the DSCP to validate QoS policies.

Step 1 Choose Setup > Media > DSCP Groups to display the default groups.
### Figure 6-18  Default DSCP Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>DSCP Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF_EF</td>
<td>DSCP 10, DSCP 12, DSCP 14, DSCP 18, DSCP 20, DSCP 22, DSCP 26, DSCP 28, DSCP 30, DSCP 34, DSCP 36, DSCP 38, DSCP 48</td>
</tr>
<tr>
<td>CiscoVoice</td>
<td>DSCP 25, DSCP 46</td>
</tr>
<tr>
<td>TeS0</td>
<td>DSCP 0, DSCP 1, DSCP 2, DSCP 3, DSCP 4, DSCP 5, DSCP 6, DSCP 7</td>
</tr>
<tr>
<td>TeS1</td>
<td>DSCP 8, DSCP 9, DSCP 10, DSCP 11, DSCP 12, DSCP 13, DSCP 14, DSCP 15</td>
</tr>
<tr>
<td>TeS2</td>
<td>DSCP 18, DSCP 17, DSCP 19, DSCP 20, DSCP 21, DSCP 22, DSCP 23</td>
</tr>
<tr>
<td>TeS3</td>
<td>DSCP 24, DSCP 25, DSCP 26, DSCP 27, DSCP 29, DSCP 28, DSCP 30, DSCP 31</td>
</tr>
<tr>
<td>TeS4</td>
<td>DSCP 32, DSCP 33, DSCP 34, DSCP 35, DSCP 36, DSCP 37, DSCP 38, DSCP 39</td>
</tr>
<tr>
<td>TeS5</td>
<td>DSCP 40, DSCP 41, DSCP 42, DSCP 43, DSCP 44, DSCP 45, DSCP 46, DSCP 47</td>
</tr>
<tr>
<td>TeS6</td>
<td>DSCP 48, DSCP 49, DSCP 50, DSCP 51, DSCP 52, DSCP 53, DSCP 54, DSCP 55</td>
</tr>
<tr>
<td></td>
<td>DSCP 56, DSCP 57, DSCP 58, DSCP 59, DSCP 60, DSCP 61, DSCP 62</td>
</tr>
</tbody>
</table>
Step 2  Choose Analyze > Traffic > DSCP to find any misclassified traffic. In Figure 6-19, the RTP protocol is displayed for ToS0 classification.

Figure 6-19  DSCP Group - ToS0

Step 3  Click on the All DSCP button to view all DSCP and applications.
Step 4 In Figure 6-20, RTP and SIP are highlighted. The protocols are listed for DSCP 0, which is incorrect since the standard classification for voice traffic is DSCP 46 and 24. This means that some of the voice traffic is misclassified on the network. You can also view the branch NAMs to investigate whether voice traffic is being misclassified.

Figure 6-20 All DSCP Table

<table>
<thead>
<tr>
<th>DSCP</th>
<th>Application</th>
<th>Bits/sec</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>sip</td>
<td>71,273,098</td>
<td>429,705,213</td>
</tr>
<tr>
<td>16</td>
<td>ftp</td>
<td>69,706,551</td>
<td>136,175,301</td>
</tr>
<tr>
<td>9</td>
<td>ftp-data</td>
<td>2,073,134</td>
<td>6,624,376</td>
</tr>
<tr>
<td>0</td>
<td>ftp-data</td>
<td>1,645,728</td>
<td>5,246,116</td>
</tr>
<tr>
<td>9</td>
<td>ftp</td>
<td>1,078,236</td>
<td>22,021,998</td>
</tr>
<tr>
<td>0</td>
<td>http</td>
<td>7,09,084</td>
<td>2,733,247</td>
</tr>
<tr>
<td>0</td>
<td>ftp</td>
<td>792,676</td>
<td>11,866,266</td>
</tr>
<tr>
<td>0</td>
<td>pre</td>
<td>674,399</td>
<td>1,402,790</td>
</tr>
<tr>
<td>0</td>
<td>fowmonitor</td>
<td>111,941</td>
<td>205,702</td>
</tr>
<tr>
<td>0</td>
<td>sip</td>
<td>24,576</td>
<td>118,138</td>
</tr>
<tr>
<td>0</td>
<td>unknown</td>
<td>22,462</td>
<td>253,669</td>
</tr>
<tr>
<td>0</td>
<td>snmp</td>
<td>3,904</td>
<td>101,861</td>
</tr>
<tr>
<td>0</td>
<td>h323host:all</td>
<td>8,265</td>
<td>150,703</td>
</tr>
<tr>
<td>0</td>
<td>ttlb</td>
<td>6,096</td>
<td>152,559</td>
</tr>
<tr>
<td>0</td>
<td>wc:ip</td>
<td>4,925</td>
<td>30,364</td>
</tr>
<tr>
<td>0</td>
<td>irrep</td>
<td>995</td>
<td>17,089</td>
</tr>
<tr>
<td>0</td>
<td>arp</td>
<td>550</td>
<td>14,557</td>
</tr>
<tr>
<td>0</td>
<td>bootps</td>
<td>498</td>
<td>1,616</td>
</tr>
<tr>
<td>46</td>
<td>eigrp</td>
<td>446</td>
<td>12,446</td>
</tr>
<tr>
<td>0</td>
<td>dns</td>
<td>373</td>
<td>10,169</td>
</tr>
<tr>
<td>0</td>
<td>naffinw</td>
<td>361</td>
<td>3,978</td>
</tr>
</tbody>
</table>
Step 5 Left-click on the RTP graph and select **Application Traffic by Host** to display the clients using those protocols. This helps to troubleshoot why RTP or SIP traffic from these clients is not marked correctly. As shown in **Figure 6-21**, the NAM displays the IP addresses of the phones using those protocols. This helps you review the QoS policy implemented on the routers and switches between the clients.

**Figure 6-21  RTP Host Table**

---

See DSCP Groups, page 2-70.

**Using NAM for Historical Trends via Interactive Report**

Historical trending is an important component of network performance management. While real-time analysis provides information about events, historical trending provides visibility into event sequences. Such sequences offer valuable information about various aspects of the network such as changes in network traffic behavior, anomalies and unusual activities, and network usage in peak times versus low times. It is also helpful in planning future network upgrades, application rollouts, and hardware buildouts. Here are some things to take note of regarding NAM’s historical trending capabilities:

- Use the Interactive Report > **Filter** button (located on the left side of the NAM window) to look at short term and long term trends by changing the Time Range. The interactive reports can be exported or the filter setting saved for quick view in the future. The exported data can be sent via e-mail in CSV or HTML format. See **Figure 6-22**.
Figure 6-22 Interactive Report

Figure 6-16 displays host traffic for the last day, and using the middle graph you can zoom down to the time range of 10:00 - 16:00 to view what other application this host is using.

Figure 6-23 Host Traffic for Last 1 Day

In the following deployment scenario, you will predict the capacity needed for a new branch build out due in six months by studying the usage of an existing branch office of a similar size. To deploy an NME-NAM located in the branch router (ISR) of the existing branch:

**Step 1** Start capturing traffic rates between the branch and the data center. View the traffic for the last month from Interactive Report > Filter > Time Range > Custom (enter a date covering a month).
**Step 2**  
Open a conversation report from today and find a stream that has a mildly increasing trend but is unable to confirm the rate at which it is increasing (see Figure 6-24).

![Figure 6-24 A Stream with a Mildly Increasing Trend](image)

**Step 3**  
Change the Time Range dynamically in the Interactive Report to study the trend with a granularity of one month. You may find that the pattern does show periodic increases, but it always hits a ceiling between 4.5 KBps and 5.0 KBps (see Figure 6-25). You are then able to conclude that the ISP link needed at the new site would be similar, and so a standard T1 line would be more than sufficient for the needs of the new remote office.

![Figure 6-25 The Trend Shown with a Granularity of 1 month](image)

Studying historical trends is a valuable exercise in planning and baselining a network. Monitor and trend on business critical applications and servers. These trends should provide handy information in a variety of day-to-day decisions.
Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications

Application Performance Response Time Analysis provides up to 45 metrics. You can configure thresholds based on many of these metrics, and receive an alert when the thresholds are passed. Thresholds should be set for critical applications or servers using Average Server Response Time, or Average Transaction Time, or Average Network Time and Average Server Network Time. These thresholds will help identify where the problem lies in the application performance, and show whether the problem is a server or network issue. Depending on the alarm, you can access the NAM to see the applications and clients accessing the server, or to check the devices in the traffic path monitoring device and interface utilization.

See Application Response Time, page 3-22.
See Thresholds, page 2-46.

Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications

The NAM monitors RTP streams: When a phone call ends, the endpoints calculate the information and send it to the Call Manager. If a NAM is along that path, it will intercept it.

The NAM monitors and analyzes RTP streams and voice calls statistics from the endpoint. The voice calls statistics from the endpoint is used in conjunction with the RTP stream to correlate the phone number with the IP address of the endpoint. Alerting is based on analysis of the RTP streams for MOS, Jitter, and Packet Loss.

See Analyzing Traffic, RTP Streams, page 3-38.
See Table 2-40, Voice Monitor Setup Window.

Using Nexus 1000V NAM VSB to Monitor Nexus 1000V Switch Environment

As networks and applications move into the virtualization environment, the challenge for administrators is finding tools to gain insight into that environment. The NAM VSB provides that function by integrating with the Cisco Nexus 1010 virtualization appliance. Using the NAM VSB, the administrator gains operational visibility into the virtual switching layer and is able to see virtual machine (VM) to VM statistics. See Figure 6-26.

In this scenario, applications are being deployed in the virtualized environment and the Nexus 1000V switch is providing the network connectivity. The NAM VSB installed on the Nexus 1010 Virtual Services Appliance will be used to monitor the environment.

Note
If Nexus 1000V switches and NAMs are already deployed in the network, ERSPAN or NetFlow data source can be directed any one of those NAMs. The 1000V switch and NAM should be directly connected to the same physical switch.
To monitor the Nexus 1000V environment:

**Step 1** Install and configure NAM VSB on the Nexus 1010 Virtual Services Appliance. See the Installation and Configuration Guides for the NAM on Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html

**Step 2** Verify that ERSPAN or NetFlow are configured on the Cisco 1000V Wwitch Virtual Supervisor Module (VSM) that is providing data to NAM.

**Step 3** Configure the ERSPAN or NetFlow data source on the NAM VSB.

**Step 4** Enable all applicable monitoring parameters in NAM for ERSPAN and NetFlow. Figure 6-27 shows the Traffic Summary window, which displays Top N information such as applications, hosts, protocol, and server response time. Navigation is provided to view and display details for each of the categories listed.

**Step 5** Using the Interactive Report on the left side of the window, configure reports for trending on the application response time, hosts, and conversation traffic patterns.
Step 6  The physical and virtual interfaces table provides VM-to-VM traffic utilization (Figure 6-28). Because one virtual interface connects to one VM, the data shows which VMs are utilizing the switch resources. The administrator then can view the hosts and conversations tables to identify the culprit utilizing the resources.

Note  NAM VSB provides the same complement of features except that it supports only ERSPAN and NetFlow data sources and performs no voice monitoring and packet capture.
Troubleshooting

Troubleshooting

Using NAM for Problem Isolation

The alarm details (found in the Cisco Prime Network Analysis Module 5.1 under Monitor > Overview > Alarm Summary) provides information you can use to drill-down on the threshold that was violated. You may also receive this alarm in e-mail (Setup > Alarms > E-mail). An example of the alarm is:

2010 SEPT 28 9:17:0:Application:Exceeded rising value(1000);packets;60653;Site(San Jose), Application(http)

After receiving this alarm, you can access the NAM GUI to view the application in site San Jose to determine why there was a spike. Click on Analyze > Traffic > Application; in the Interactive Report window on the left, change Site to “San Jose,” Application to “HTTP,” and Time Range to the range when the alert was received. This will display all the hosts using this protocol. You can see the Top hosts and verify there are no unauthorized hosts accessing this application. You can also access Analyze > Traffic > Host to view which conversations are chatty, and therefore causing the increase traffic for this application.

If the alarm is for an Application Response Time issue, you can access Monitor > Response Time Summary or Analyze > Response Time > Application to drill-down on what hosts are accessing the application. Identify the application server and view what other applications are hosted and all the clients accessing that server.

See Monitor: Response Time Summary, page 3-5.
See Analyze: Response Time, page 3-18.

Using NAM for SmartGrid Visibility

The NAM will not recognize the IEC 60870 protocol out of the box (this is one of the main protocols used by power distribution companies). You will have to add a custom protocol, because it is a specific port you will be using. When you choose Setup > Classification > Application Configuration, you will see all hosts using that application. It will be identified as a Telnet application.