This chapter describes information on how to deploy NAM in your networks. It contains details on network performance management as well as usage scenarios for the Cisco Prime Network Analysis Module 5.1(3). This chapter contains the following sections:

- Network Performance Management Lifecycle, page 6-1
- Places in the Network Where NAMs Are Deployed, page 6-2
- Use Cases, page 6-7

**Network Performance Management Lifecycle**

In any network, the administrator must define *normal* and *abnormal* behavior patterns. Once this is accomplished, the goal is to maintain the network in its normal state and take any actions needed to prevent it from going into an abnormal state. When such an abnormal situation occurs, such as an outage, tools must be available to quickly isolate and fix the problem.

*Figure 6-1 The Network Performance Management Lifecycle*
Figure 6-1 depicts the Operational Network cycle that is at the center of where the network should ideally be at all times. The other two cycles indicate the process of repairing a network problem and the process of planning a change to the network. The following is a brief outline of the performance management lifecycle:

1. **Recognize and list your network performance goals**—This includes setting expected limits for response time, expected ranges for MOS values, bandwidth usage per application, and utilization on critical WAN links. The importance of these metrics is closely related to your specific network; for example, an enterprise with a large number of branches and a small main campus might focus on WAN utilization, whereas an enterprise with one main campus and one large branch with users that use collaboration tools across the two will likely focus on application performance metrics such as response time measurements.

2. **Create a baseline of current network performance metrics**—The NAM can help document a variety of these baseline metrics including applications, bandwidth per application, top conversations and hosts, QoS values used in the network, unrecognized protocols, and current server and end-to-end response time measurements. These measurements might meet or exceed your expectations in step 1. It might be worthwhile to revisit the expectations set in step 1 and check whether some refinements are necessary (for example, 80 percent utilization on the WAN link may be quite acceptable, whereas the real reason behind application delays seems to be bursts of unrecognized traffic. In this case, one might be lenient on WAN link utilization and focus more on QoS-related issues).

3. **Enforce policies using alarms, syslogs, traps, and email alerts**—NAM can provide alerts by email, traps and syslogs. These tools must be configured such that the normal functioning range of the network is demarcated. If any of the tracked metrics show values that are outside this normal range, then the NAM can be used to send alerts as appropriate. The information stored on the NAM is openly available to applications. It is recommended that any enterprisewide network management tools and monitoring applications be configured to receive alerts from NAM. The NAM is then able to act as a network sentinel and warn proactively about a host of issues and also provide access to rapid troubleshooting when problems occur.

The goal is for all important network metrics to be within the normal ranges. But knowing the normal range of the network is a constant learning process, and as the network evolves and grows, it can be a moving target. Therefore the lifecycle described above is a continuous process of fine-tuning the network and the metrics that are most important to normal behavior.

**Places in the Network Where NAMs Are Deployed**

Because NAM is available in various form factors, it allows significant flexibility in deployment. At the same time, the available NAMs must be deployed in locations that are most effective in helping you monitor, measure, and report on the network’s health. Any location that is the ingress or egress point of a logical network boundary (aggregation layer, core, campus edge, and so on) can offer valuable insights into the network activity within that partition. Therefore, such boundary locations are usually good choices for NAM deployment.

Figure 6-2 shows various possible locations at which NAMs can be deployed. The access and distribution layers, the data center, WAN edge, and branch office are all valid choices, and you should make deployment decisions based on the specific issue at hand. The following is a list of common places in the network where NAMs are deployed and the information available at each place:
Chapter 6 Understanding NAM Deployment

Places in the Network Where NAMs Are Deployed

- **Data center**—Over the past few years, data center consolidation has been a common theme across enterprises. The centralized data center becomes a critical hub of activity within the enterprise network and helps cut costs, focus IT efforts in one location, and offer a rich variety of services across the enterprise. Placing a NAM in such data centers offers excellent visibility into the most business-critical applications and transactions.

- **Server farms**—Place near server farms (web, FTP, and Domain Name System [DNS], for example), data centers, or near IP telephony devices (Cisco Unified Communications Manager), IP phones, and gateways where the Cisco NAM can monitor request-response exchanges between servers and clients and provide rich traffic analysis, including IAP.

- **Campus and WAN edge**—This location is very often a good choice—it offers visibility into traffic entering and exiting the campus. It provides a central point from which to measure voice quality of all streams leaving the campus and going across the WAN. The WAN is typically the smallest bandwidth link, and therefore, call metrics such as latency, jitter, and so on might require close monitoring for deterioration in quality. It is also an excellent location to measure WAN utilizations and health metrics of various branch routers using NetFlow. Place Cisco NAMs at the WAN edge to gather WAN statistics from the Optical Services Module (OSM) or FlexWAN interfaces or to collect NetFlow statistics on remote NetFlow-enabled routers. This can provide usage statistics for links, applications (protocol distributions), hosts, and conversations, which can be useful for trending data and capacity planning.

- **Branch office**—Place Cisco NAMs at the edge of the branch office to troubleshoot issues at remote sites. This place offers the advantage of visibility into all traffic crossing the branch boundary. Headquarters personnel can troubleshoot issues remotely through the NAM GUI.

- **Distribution layer**—The distribution layer is typically a convergence point for traffic from smaller networks; for example, three buildings of a company might feed into a distribution layer switch. Placing the Cisco NAMs at the distribution layer allows visibility into the application trends specific to that set of buildings. In troubleshooting situations, you might start working with an edge NAM and then log in to a distribution NAM to isolate and fix the problem. Also, it is a good location to capture RTP voice streams. If phone calls in one building in the campus need to be monitored for quality, the aggregation layer is a good choice, as the switch in this layer will typically “catch” all calls being made in that building.

- **Access layer**—The access layer is the layer closest to users and is not a typical location for NAMs. However, with the rapid increase in network traffic over the years, it has become somewhat common to have Cisco Catalyst 6500 Series Switches in the closet of each floor. Cisco NAMs can be very useful, especially for those access layer switches that serve critical companywide meetings or conferences and other business-critical needs. Once again, close monitoring of IP phones is a good application in this layer as well.
Choice of Hardware and Software Platforms for a Given Place in the Network

Depending on the usage scenario and the location in which the NAM will be deployed, you must make a decision on the type of NAM platform to deploy. This section provides the necessary background and details to make such deployment decisions. See Table 1 for a summary of NAM platforms. Please refer to [http://www.cisco.com/en/US/products/ps5740/Products_Sub_Category_Home.html](http://www.cisco.com/en/US/products/ps5740/Products_Sub_Category_Home.html) for further information regarding the different platforms.
Table 6-1  NAM Platforms

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Description</th>
<th>Related Details</th>
</tr>
</thead>
</table>
| Cisco NAM-1/-2 blade    | The NAM-1 and NAM-2 blade fits into any slot on a Catalyst 6500 or Cisco 7600. The NAM-2 blade has two data ports. These ports connect directly to the switching fabric and are not externally visible. Each port can support one SPAN session. Therefore, the NAM-2 blades support a total of two SPAN sessions, while the NAM-1 blades support one SPAN session. | Product types:  
  - WS-SVC-NAM-2-250S  
  - WS-SVC-NAM-1-250S  
  - WS-SVC-NAM3-6G-K9  
Typical PINs: Data center, core, and distribution  
**Note** If required, currently owned NAM-1 and NAM-2 (without -250S suffix) cards can be upgraded using a memory upgrade kit. The kit essentially provides an upgrade to the RAM on your NAM cards and offers an easy way to meet the performance needs of NAM software while allowing continued use of the existing NAM hardware investment.  
The memory kit only upgrades RAM and not the hard drive. |
| Cisco NAM-3             | The NAM-3 blade fits into any slot on a Catalyst 6500. The NAM-3 blade has two data ports. These ports connect directly to the switching fabric and are not externally visible. Each port can support one SPAN session. Therefore, the NAM-3 blades support a total of two SPAN sessions. | Product types:  
  - WS-SVC-NAM3-6G-K9  
Typical PINs: Data center, core, and distribution |
| Cisco NAM Branch module | The NAM on SM-SRE takes up a module slot on a Cisco 2900 or Cisco 3900 Integrated Services Router (ISR G2). The NME-NAM takes up a module slot on a Cisco 2800 or Cisco 3800 Integrated Services Router (ISR).  
The NME-NAM (with adapter) takes up a module slot on a Cisco 2900 or Cisco 3900 Integrated Services Router (ISR G2).  
This module has one internal and one external port. The internal interface receives traffic forwarded from router interfaces, while the external interface can be used to connect to wire taps. | Product types:  
  - SM-NAM-SW-5.1-K9 - Cisco Prime NAM Software for ISR G2 SRE – NAM on SM-SRE 700 and SM-SRE 900  
  - NME-NAM-120S  
Typical PINs: Campus edge, branch edge, WAN edge  
**Note** Because the network modules have an internal and an external port, they provide the flexibility to monitor packets from a router interface or directly tap into traffic from an external device using the external Ethernet port. |
Places in the Network Where NAMs Are Deployed

Table 6-1  NAM Platforms

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Description</th>
<th>Related Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NAM 2304/2204 Appliance</td>
<td>The midrange appliance has four 1 Gigabit Ethernet ports, available either as copper or optical interfaces. Appliances offer the flexibility to deploy NAMs with any Cisco device irrespective of platform. 1 rack unit.</td>
<td>Product types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NAM2304-RJ45 - Cisco NAM 2304 Appliance, four 1 GB Ethernet, RJ-45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NAM2304-SFP - Cisco NAM 2304 Appliance, four 1 GB Ethernet, SFP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Typical PINs: Data center, core, campus edge</td>
</tr>
<tr>
<td>Cisco NAM 2320/2220 Appliance</td>
<td>The NAM high-end appliances offer two 10 Gigabit Ethernet ports. 2 rack unit.</td>
<td>Product type—NAM2320 – Cisco NAM 2320 Appliance, two 10 GB Ethernet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The 2320 appliance is NAM’s high-end hardware platform and is best suited to handle the high performance required in data center and core networks.</td>
</tr>
<tr>
<td>Cisco PRIME NAM Virtual Blade on WAAS</td>
<td>The NAM Virtual Blade is software residing on a Cisco WAVE-574 and WAE-674 appliances</td>
<td>Product types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NAM-WAAS-VB – VB on WAAS appliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• WAA5-VB-NAM5.1-K9 – software for WAAS 574/674</td>
</tr>
<tr>
<td>Cisco PRIME NAM Virtual Service Blade on Nexus 1010</td>
<td>NAM Virtual Service Blade is a software that resides in Nexus 1010 providing visibility into Nexus 1000V switch.</td>
<td>Product type—N1K-C1010NAM51-K9 - Cisco Prime NAM Software 5.1 for Nexus 1010</td>
</tr>
</tbody>
</table>

A Note on the Cisco NAM Appliances

In addition to the existing platforms on which the NAM can be installed, the NAM software is also available as an appliance. The addition of the appliance to the NAM product line provides increased flexibility and higher performance. The appliances are available in two varieties. The Cisco NAM 2x20 Appliance offers the best performance in the NAM product line. The product contains two 10-Gigabit Ethernet ports that are ideally suited to the high-bandwidth data center and core environments. The Cisco NAM 2x04 Appliance contains four 1-Gigabit Ethernet ports, available both in copper and fiber, and allows flexible deployment in a variety of locations across the network.

The NAM appliance serves as a complement to the network module implementations of the NAM. The network modules (or cards) reside within an ISR, Catalyst 6500 Series Switch, or Cisco 7600 Series Router, and offer an integrated solution. Such integration saves rack space and power, eliminates the need for additional cabling, and efficiently monitors device traffic with no network overhead. Still, there are situations where an appliance is preferred. For example, you may wish to monitor a Catalyst 4500 Series Switch or a Nexus 7000 Series Switch that does not support NAM network modules. Or, you may wish to connect the NAM to multiple switches in parallel as you build a new segment in the network. This can be achieved easily with the NAM 2204 Appliance, which has four ports that can each be connected to different devices. Or, you may want to monitor traffic from a couple of core routers that feed into the data center, and therefore require 10-Gigabit Ethernet ports. The Cisco 2320 Appliance might be ideally suited for this scenario. The addition of the appliances to the NAM product line provides users with additional flexibility in deploying the appropriate NAM hardware depending on the location in the network.
Enhanced performance also provides other deployment benefits. For example, the number of voice streams supported by the NAM is an important consideration while planning for voice over IP quality monitoring. Other limits include the number of NetFlow records processed per second, buffer sizes available for packet capture, number of WAE devices that send WAN optimization data to NAM, and in general, monitoring performance under load.

The appliances are not integrated into the Cisco infrastructure, but they do support some of the features that the integrated NAM modules bring. On the integrated Catalyst 6500 NAM cards, you may have used the ability to poll MIBs on the supervisor and collect statistics on important aspects such as switch CPU health, interface traffic, utilization, and so on. The appliance defines the concept of a “managed device” that achieves the same result for the device being monitored. You will need to choose one of the Cisco devices (supported platforms include Catalyst 6500, Cisco 7600, and Catalyst 4500 Series devices) being monitored by the appliance as your managed device. The NAM appliance will be able to poll MIBs on this managed device and obtain relevant performance troubleshooting information just like the NAM cards. Also available is the ability to configure SPAN sessions on the managed device through the NAM GUI on the appliance. Credentials to access the managed device need to be configured in order for these capabilities to be enabled.

To view which release versions run on the supported NAM appliances, see the NAM Compatibility Matrix.

Use Cases

The following use cases focus on a specific need to be addressed or a problem to be solved. Each 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. These examples discuss best practices and approaches to effective NAM deployment and are grouped into the following categories:

- Data Center
- Campus
- Branch
- General Usage Scenarios
- NAM Integrations with Monitoring and Reporting Applications

Data Center

- Monitoring the Nexus 1000V Switch Environment, page 6-29
- Real-Time Traffic Monitoring and Analysis, page 6-20
- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-29
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications, page 6-29
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-22
- Monitoring Cisco WAAS and Measuring Its Impact, page 6-16
Deployment Examples

Campus

- Real-Time Traffic Monitoring and Analysis, page 6-20
- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-29
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications, page 6-29
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-22
- Using NAMs to Monitor VoIP Quality, page 6-9

Branch

- Visibility in the Branch, page 6-15
- Real-Time Traffic Monitoring and Analysis, page 6-20
- Using NAM to Evaluate Application-Level Performance Monitoring for TCP-Interactive Applications, page 6-29
- Using NAM to Evaluate Application-Level Performance Monitoring for UDP Realtime Applications, page 6-29
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-22
- Monitoring Cisco WAAS and Measuring Its Impact, page 6-16
- Using NAMs to Monitor VoIP Quality, page 6-9

General Usage Scenarios

These use cases are applicable to any part of the network:

- Utilizing Sites to Create a Geographically- or Organizationally-Familiar Deployment, page 6-12
- Using NAM for Historical Trends via Interactive Report, page 6-26
- Using NAM for Problem Isolation, page 6-33
- Creating Custom Applications, page 6-12
- Autodiscovery Capabilities of NAM, page 6-11
- Using NAM for SmartGrid Visibility, page 6-33

NAM Integrations with Monitoring and Reporting Applications

- Integrating NAM with LMS, page 6-14
- Integrating NAM with Third Party Reporting Tools, page 6-14

Deployment Examples

- Using NAMs to Monitor VoIP Quality, page 6-9
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 6-3) 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 6-3 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 6-4, 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.


**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 autocrated 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 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 Applications, page 2-74.

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

Cisco Prime NAM has 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 6-5 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 6-6 shows a list of the sites configured for this deployment.

![Sites Table](image)

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 6-7).

![Traffic Summary Dashboard](image)

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 6-8 shows the contextual drilldowns from the Top N Applications and Top N Hosts charts.

**Figure 6-8  Applications and Hosts Drilldowns**

See Sites, page 2-65.

See Site Definition Rules, page 2-66.

**Integrating NAM with Third Party Reporting Tools**

Prime NAM 5.1(3) integrates with the CA NetQoS SuperAgent for the purpose of aggregating Application Response Times. Prime NAM 5.1(3) 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).

See Response Time Summary.

**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](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 6-9 for a view of the NAM GUI being accessed through LMS GUI.

Figure 6-9  NAM GUI Available In the LMS GUI

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-7xx or SM-SRE-9xx 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 6-16.
Deployment Examples

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(3) release, see the Cisco Prime NAM 5.1(3) Release Notes on www.cisco.com.

See related content Response Time Summary and Analyze, Response Time.

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 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 2x20 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.
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.

The NAM 2x20 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.

**Monitoring**

- Real-Time Traffic Monitoring and Analysis, page 6-20
- Using NAM to Monitor QoS/DiffServ (DSCP), page 6-22
- Using NAM for Historical Trends via Interactive Report, page 6-26
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).

**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).
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).
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 2-47.

**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 46</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 16, DSCP 17, DSCP 18, 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 28, DSCP 29, 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>
</tbody>
</table>

- **TeS0** and **TeS1** are highlighted in green, indicating they are active DSCP groups.
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*

![DSCP Group - ToS0](image)

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](image)

<table>
<thead>
<tr>
<th>DSCP</th>
<th>Application</th>
<th>Bits/sec</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>RTP</td>
<td>71,273,098</td>
<td>439,105,213</td>
</tr>
<tr>
<td>16</td>
<td>http</td>
<td>69,709,851</td>
<td>136,175,301</td>
</tr>
<tr>
<td>9</td>
<td>ftp-data</td>
<td>2,072,134</td>
<td>6,924,376</td>
</tr>
<tr>
<td>0</td>
<td>ftp-data</td>
<td>1,845,728</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>769,064</td>
<td>2,733,247</td>
</tr>
<tr>
<td>0</td>
<td>sip</td>
<td>792,676</td>
<td>11,866,266</td>
</tr>
<tr>
<td>0</td>
<td>pre</td>
<td>674,319</td>
<td>1,491,790</td>
</tr>
<tr>
<td>0</td>
<td>flowmonitor</td>
<td>111,941</td>
<td>205,382</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>363,669</td>
</tr>
<tr>
<td>0</td>
<td>snmp</td>
<td>9,904</td>
<td>101,861</td>
</tr>
<tr>
<td>0</td>
<td>h323host:all</td>
<td>8,265</td>
<td>158,703</td>
</tr>
<tr>
<td>0</td>
<td>stb</td>
<td>6,096</td>
<td>152,599</td>
</tr>
<tr>
<td>0</td>
<td>wcp</td>
<td>4,025</td>
<td>30,364</td>
</tr>
<tr>
<td>0</td>
<td>icmp</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>rafflow</td>
<td>361</td>
<td>7,078</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.
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 6-23  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

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.x 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

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 2-47.

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 Table 2-40, Voice Monitor Setup Window.

Monitoring the Nexus 1000V Switch Environment

As networks and applications move into the virtualization environment, the challenge for you is to find 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, you can gain operational visibility into the virtual switching layer and is able to see virtual machine (VM) to VM statistics. See Figure 6-26.

The Nexus 1000V switch can also be monitored by other NAM platforms running the NAM 5.1 software. In this scenario, there are two options:

- You are deploying applications 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 is used to monitor the environment.
- 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.
If Nexus 1000V switches and NAMs are already deployed in the network, ERSPAN or NetFlow data source can be directed by any one of those NAMs. You should directly connect the 1000V switch and NAM to the same physical switch.

To monitor the Nexus 1000V environment:

**Step 1** Install and configure either the NAM VSB on the Nexus 1010 Virtual Services Appliance or the Nexus switch to the NAM-2. 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](http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html)

**Step 2** For the NAM VSB:

1. Verify that ERSPAN or NetFlow are configured on the Cisco 1000V Switch Virtual Supervisor Module (VSM) that is providing data to NAM.
2. Configure the ERSPAN or NetFlow data source, depending on your NAM:
3. 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.
4. 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.
5. 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. You can then 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.

Step 3

For other NAM platforms running version 5.1 (NAM-2):

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

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.

3. Create a site for this data source using Setup > Network > Sites (Figure 6-29).
4. Choose Monitor > Overview > Traffic Summary (as shown in Figure 6-30) and Monitor > Overview > Response Time Summary.

Troubleshooting

- Using NAM for Problem Isolation, page 6-33
- Using NAM for SmartGrid Visibility, page 6-33
- Real-Time Traffic Monitoring and Analysis, page 6-20
Using NAM for Problem Isolation

The alarm details (found in the Cisco Prime Network Analysis Module 5.1(3) 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.