Cisco Network Analysis Module (NAM)

Deployment Guide

Contents

Introduction

Cisco® Network Analysis Module (NAM) is a product that provides advanced network instrumentation and allows network administrators, managers, and engineers the ability to get a variety of detailed metrics from the network. NAM offers a versatile combination of real-time traffic analysis, historical analysis, packet capture capabilities, and the ability to measure user-perceived delays across the WAN as well as analysis of voice-over-IP (VoIP) quality. Cisco's goal with NAM is to provide a uniform instrumentation layer that can collect data from a variety of sources, process the data to convert it to meaningful information, and then make it available to the user. This information is available either through an onboard web-based graphical user interface, or alternatively it can be exported to applications that are configured to collect from Cisco NAM. In addition, NAM has been tested with NetQoS SuperAgent, Compuware Vantage Analysis Server, and InfoVista 5View to solve specific network problems, both proactively and reactively.

From a deployment perspective, Cisco NAM offers value in multiple places in the network: the data center, the branch, the campus core, aggregation, and even closet locations. As a result, NAM comes in different platforms to allow for flexible deployment across the network. Currently, there are multiple variations of the NAM, software and hardware, such as the NME-NAM for the Branch Integrated Services Routers (ISRs), NAM-1/NAM-2 for the Cisco Catalyst® 6500 Series Switches, and Cisco NAM 2200 appliances. The Cisco NAM Virtual Blade provides integrated performance management capabilities for before and after analysis of the WAN optimization solution. The data source for the performance measurements are from the Cisco Wide Area Application Services (WAAS) Flow Agent. The NAM Virtual Blade is supported on the Cisco WAVE-574 and WAE-674 appliances. Please refer to http://www.cisco.com/en/US/products/ps5740/Products_Sub_Category_Home.html for further information regarding the different platforms. The newest addition, Cisco Nexus 1000V NAM Virtual Service Blade (VSB) 4.2 integrates with the Cisco Nexus 1010 appliance, extending the visibility into the virtual switching layer.

The objective of this deployment guide is to provide users with deployment options and recommendations, usage scenarios and appropriate design, and constraints. The emphasis on usage scenarios will help address NAM deployment in specific technical cases such as WAN optimization deployments using Cisco WAAS or examples specific to Cisco VoIP deployments. Examples show that deployment is fast and easy, and the NAM delivers a wide array of benefits.

Feature Overview

This section provides a brief overview of the various features that NAM 4.2 software includes. Note that NAM software has a common set of features irrespective of the hardware platform on which it is running. Some differences in behavior do exist; for example, the NAM line cards on the Cisco Catalyst 6500 Series Switches support Switch Port Analyzer (SPAN) technology, whereas the network modules on the Cisco 2800 and 3800 Series Routers do not. (SPAN is a Layer 2 feature. It is not supported on the ISR series of routers, which support only Layer 3 functionality.) But from a feature perspective, there is consistency across all platforms. Needless to say, performance and scalability will differ based on the capabilities of the hardware, and information relating to such matters will be provided wherever relevant.

Real-Time and Historical Application Monitoring

One of the main added values that NAM provides is the ability to monitor traffic in real time and provide a variety of analytics. In this category of real-time monitoring are application recognition, analysis of top conversations, hosts, protocols, differentiated services code points (DSCPs), and packet captures. More advanced processing includes intelligent application performance (IAP) analytics (response time measurements and various user-experience-

related metrics) and voice quality monitoring (which includes the ability to detect Real-Time Streaming Protocol [RTP] streams and compute the Mean Opinion Score [MOS], packet loss, and other VoIP metrics).

Intelligent Application Performance Analytics

NAM software offers many useful capabilities for network and application performance management. These features provide the ability to measure the quality of user experience using various response time measurements. These measurements are computed by monitoring and time-stamping packets sent from the user to the server providing services.

Monitoring Cisco WAAS and Measuring Its Impact

Cisco NAM has been enhanced to monitor traffic that is optimized using Cisco WAAS devices. The WAAS solution requires a pair of devices (WAN Acceleration Engines [WAEs]) that work together to optimize traffic flows. Typically, a WAE is located in the branch and another in the data center. NAM is able to monitor traffic activity on WAEs and measure the impact of traffic optimization. Such measurements allow administrators to show the benefits of implementing WAN optimization, cut unnecessary hardware upgrade costs, and monitor user experience in WAAS deployments in a granular and proactive manner. Those measurements can now be obtained from the NAM Virtual Blade that can be installed on Cisco WAVE-574 and WAE-674 appliances.

VoIP and Quality of Service Monitoring

Cisco NAM provides visibility into real-time voice quality of service (QoS), as well as historical reporting and trending of voice calls. Industry-standard MOS computations are provided through the real-time monitoring screens every minute. Alarms can be configured to trigger based on voice quality issues.

Triggered Captures, Trend Analysis, and Other Uses

The number of triggered captures has been increased - while only one capture could be triggered automatically in earlier releases, that limitation has been removed, and multiple automatic captures can be started in parallel. Note that performance considerations must be taken into account any time multiple captures are started, whether these captures are triggered or manual. Also, the protocol directory has been expanded to recognize a number of additional well-known protocols, and the menus have been improved for ease of use and configuration.

Monitoring Cisco Nexus 1000V Switch Deployment

Cisco Nexus 1000V NAM VSB is integrated with the Nexus 1010 Virtual Services Appliance to provide network and performance visibility into the Nexus 1000V switching deployment. The NAM VSB uses the embedded instrumentation, such as Encapsulated Remote SPAN (ERSPAN) and NetFlow on the Nexus 1000V switch as the data source for traffic analysis, application response time, interface statistics, and reporting. All NAM 4.x features are supported except voice over IP monitoring and packet capture. The 1000V switch can also be monitored by the other NAM hardware platforms running version 4.2.

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. Consider Figure 1. The “Operational Network” cycle that is at the center of the picture is 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:

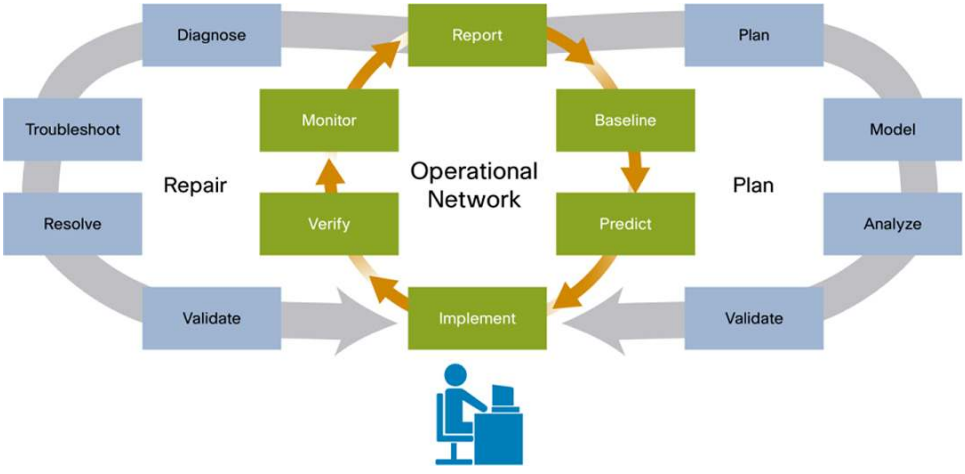
1. **Recognize and list your network performance goals:** This includes setting expected limits for response time, expected ranges for MOS values, bandwidth usage per application, and utilization on critical WAN links. The

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 other alerts:** NAM can provide alerts by email, FTP, and other traditional methods like syslogs and traps. These tools must now 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.

Again, simply stated, the goal is to remain within the normal ranges of all important network metrics. 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.

Figure 1. The Network Performance Management Lifecycle



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 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. Here is a list of common places in the network where NAMs are deployed and the information available at each place:

- **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.

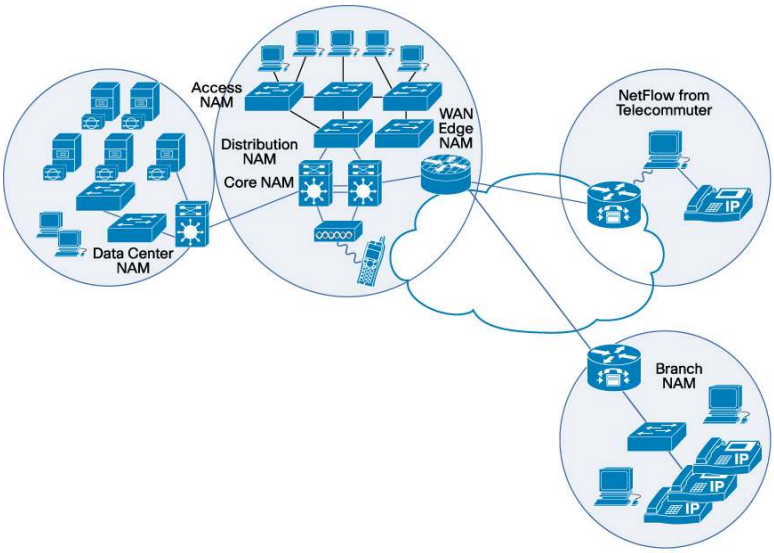
Campus and WAN edge: This location is very often a good choice - it offers visibility into traffic entering and exiting the campus. It provides a central point from which to measure voice quality of all streams leaving the campus and going across the WAN. The WAN is typically the smallest bandwidth link, 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.

Figure 2. Places in the Network in Which NAMs Can Be Deployed



Choice of Hardware and Software Platforms for a Given Place in the Network

There are multiple platforms on which NAM software is supported. 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 hardware to deploy. This section provides the necessary background and details to make such deployment decisions. See Table 1.

Table 1. Hardware Platforms

Hardware	Description	Related Details
Catalyst 6500/ Cisco 7600 blade	The NAM 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 • MEM-C6KNAM-2GB= • WS-SVC-NAM-2 • WS-SVC-NAM-1 Typical deployment locations: Data center, core, and distribution Notes: The older versions (without the -250S suffix) also support NAM 4.2. Their performance is not on par with the latest version of hardware. If required, currently owned NAM-1 and NAM-2 cards can be upgraded easily 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. Note that the memory kit only upgrades RAM and not the hard drive.
Cisco ISR Network module	The NME-NAM takes up a network module slot on a Cisco 2800, 2900, 3700, 3800, or 3900 Integrated Services Router. 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: • NME-NAM-120S • NME-NAM-80S As with the blades, the 80S version is also supported. Typical deployment locations: Campus edge, branch edge, WAN edge Notes: 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.

Hardware	Description	Related Details
Cisco NAM 2204 Appliance	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	Product types: • NAM2204-RJ45 • NAM2204-SFP Typical deployment locations: Data center, core, campus edge
Cisco NAM 2220 Appliance	The high-end appliance offers two 10 Gigabit Ethernet ports. 2 rack units	Product types: • NAM2220 The 2220 appliance is NAM's high-end hardware platform and is best suited to handle the high performance required in data center and core networks.
Cisco NAM Virtual Blade on WAAS	The NAM Virtual Blade is software residing on Cisco WAVE-574 and WAE-674 appliances	Product types: • NAM-WAAS-VB - VB on WAAS appliance • WAAS-VB-NAM-4.1 - software for WAAS 574/674
Cisco Nexus 1000V NAM Virtual Service Blade	The NAM VSB integrates with the Nexus 1010 Virtual Service Appliance to monitor Nexus 1000V switch	Product types: • N1K-C1010-NAM-4.2 • N1K-C1010-NAM-4.2= • L-N1KC1010-NAM4.2= Typical deployment location: Data center

A Note on the Cisco 2200 Series Appliances

The NAM software is available as an appliance in addition to the existing platforms. The addition of the appliance to the NAM product line provides increased flexibility and higher performance. As mentioned in Table 1, the appliance is available in two varieties. The Cisco NAM 2220 appliance offers the best performance in the NAM product line. The product contains two 10 Gigabit Ethernet ports that are ideally suited to high bandwidth data center and core environments. The Cisco NAM 2204 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.

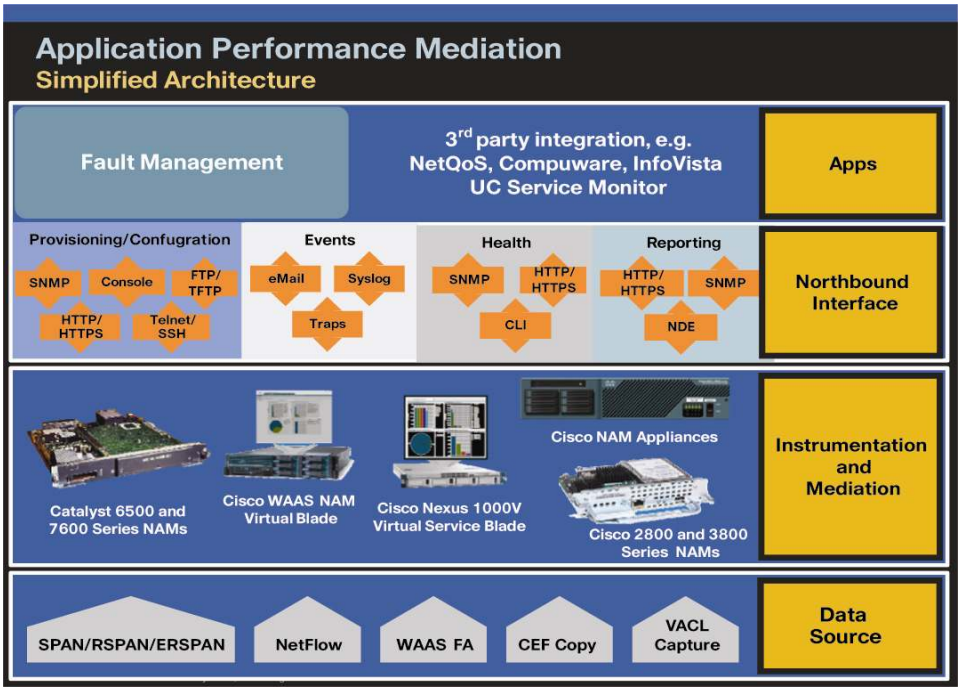
The appliance version serves as a complement to the network module versions. The network modules (or cards) reside within an ISR, Catalyst 6500 Switch, or Cisco 7600 Router and offer an integrated solution. Such integration saves rack space and power, eliminates the need for additional cabling, and efficiently 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 Switch or a Nexus 7000 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 Cisco 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 2220 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 NAM is an important consideration while planning for voice over IP quality monitoring. Other limits include 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 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.

Figure 3. Data Sources for Cisco NAM



NAM Data Sources and Export Capabilities

In the context of the NAM, a data source refers to a source of traffic whose entire stream or summaries of data from that stream are sent to the NAM for monitoring. NAM can monitor a variety of data sources and compute appropriate metrics. Figure 3 provides a snapshot of all possible sources of data and also the various export mechanisms supported by NAM. The picture shows NAM's role as a mediation layer tool - one that collects network data from a variety of sources, processes it, and then makes it available in one or more ways to northbound applications.

When you are planning and deploying NAMs in your network, it is important to have a clear understanding of how each of the data sources works, what the trade-offs are to using each of them, and which data source would be most appropriate in meeting your short- and long-term performance management goals. Table 2 provides the necessary details.

Table 2. Data Sources for Cisco NAM

Data Source	Description	Deployment Considerations	Hardware Platforms
SPAN	Different technologies are used to copy packets of interest and send them to the NAM for monitoring. SPAN and its variants, RSPAN and ERSPAN, are commonly used Cisco technologies for packet monitoring. SPAN is available in Cisco Layer 2 and Layer 3 switches. It is used to copy packets from a source port or VLAN and send a copy to a specified destination port. NAM takes advantage of this technology to listen to traffic streams on the selected ports or VLANs. RSPAN and ERSPAN are variants of SPAN. RSPAN transports packets from a remote switch (on the same Layer 2 network) to	SPAN technology allows NAM to monitor a live stream of packets. This means that NAM gets to monitor an exact copy of all packets sent in the original packet stream. Contrast this behavior to NetFlow, which does not provide access to the live stream; instead it provides a summarized update once every few minutes (at best 1 minute) about key traffic metrics. The live data stream provided by SPAN allows all of NAM's features to be used, including captures, IAP, and voice monitoring. In contrast, with NetFlow data sources, which provide only summaries and not live streams, captures, IAP, and voice monitoring are not available. NAM VSB only accepts ERSPAN and	SPAN is applicable to the Catalyst 6500, Cisco 7600, and the NAM appliance platforms. In the case of the appliance, SPAN is set up on the connected Layer 3 or Layer 2 switch and forwarded out of the port to which the appliance is connected.

Data Source	Description	Deployment Considerations	Hardware Platforms
	the destination of choice. ERSPAN transports packets from a remote IP subnet through an IP tunnel to the destination of choice. From NAM's perspective, there is no difference between these variations of SPAN. The NAM only sees packets forwarded to its internal port.	NetFlow as data sources.	
Cisco Express Forwarding copy	Cisco Express Forwarding copying is a technique used on the ISR router platform to achieve the same result that SPAN does (SPAN is not supported on the ISR platform). When enabled, Cisco Express Forwarding mechanisms on Cisco IOS® Software are used to make an extra copy of the packet, which is then forwarded to the NAM analysis port.	Cisco Express Forwarding copy, like SPAN, allows the use of all of NAM's features including captures, IAP, and voice monitoring.	Cisco Express Forwarding copy applies only to the ISR routers, Cisco 2800, 2900, 3700, 3800, and 3900.
NetFlow	NetFlow technology is supported on Cisco IOS and NX-OS Software. It provides measurements for a key set of applications including network traffic accounting, usage-based network billing, network planning, and monitoring. NetFlow technology analyzes "flows" going across the router and provides summary analyses of these flows to interested "collectors." Collectors will periodically get updates from all NetFlow-enabled routers as to the details of traffic flows over the past period. NAM serves as a NetFlow collector. Further, NAM processes NetFlow data and provides its results through its GUI.	Typical usage of NetFlow is as a complement to live traffic analysis. For example, a NAM located in the data center analyzes SPAN traffic directly, but to get visibility into traffic in remote branches with no NAMs in them, it monitors NetFlow traffic from those remote branch routers. Using this combination of data sources, NAM offers visibility into the data center and remote branches simultaneously. It is important to note that voice quality measurements, IAP, and packet captures are not available from NetFlow data exports. NetFlow data exports are merely summaries of traffic activity, whereas the aforementioned features require access to a copy of the original stream of packets.	NetFlow collection and processing is available on all NAM platforms. NetFlow performance (measured in "number of flows processed per second") varies depending on the hardware platform. The 2220 appliance offers the highest performance and is followed by the 2204 appliance and NAM-2 blades. These platforms are ideally suited to serve as centralized NetFlow collectors for exports from branch offices.
WAE Flow Agent	With Cisco NAM 4.0, the Cisco WAAS devices (WAEs) can serve as data sources to NAM. WAEs export information about optimized flows, response times, packets in/out, and so on.	A NAM blade or appliance located at the data center is the most typical example of a WAAS monitoring deployment of NAM. These devices have the performance required to handle flows from multiple WAE devices. Optionally, an NME-NAM located at a branch router would be a good location if possible. This deployment location provides the advantage of monitoring user experience before and after WAAS is enabled.	All NAM platforms are able to process data sourced from WAE devices.
VACL Capture	A VLAN access control list (VACL) can forward traffic from either a WAN interface or VLANs to a data port on the NAM. A VACL provides an alternative to using SPAN and essentially provides a way to filter traffic based on specific fields in the packet header. VACLs are useful for focused troubleshooting. Because VACLs allow refined filtering capabilities, they are useful to identify very specific packet streams, for example, packets originating from MAC address X and destined for MAC address Y.	Useful when SPAN is not supported on a WAN interface (for example, serial links). Also useful if SPAN sessions are unavailable for use by NAM. Useful when the amount of VLAN traffic exceeds Cisco NAM capacity and some prefiltering is desired, such as a 10 Gigabit Ethernet port.	Supported on the Catalyst 6500 and Cisco 7600 platforms. Requires Cisco IOS Software configuration through the command-line interface (CLI); not supported on NAM GUI.

Real-World Usage Scenarios

So far, this document has described various considerations for NAM deployment, such as data sources, location in the network, and hardware platforms. This section will bring those considerations together in typical usage scenarios. Each scenario focuses on a need to be addressed (or problem to be solved). The scenario takes into account the aforementioned deployment considerations and then uses one or more of NAM's features to meet the user's need (or solve the user's problem). The goal of these use cases is to provide real-world examples that put the

information provided in previous sections to use in real-world use cases. These examples discuss best practices and approaches to effective NAM deployment.

Scenario 1: 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.

Deployment: You manage a NAM-2 blade located in the Cisco Catalyst 6500 at the campus edge. There are no NAMs at the two branch offices.

Step 1. Open the Monitor -> Overview screen. Identify the top hosts and top applications using the available graphs (Figure 4). Take note of the top host (the top bandwidth generator).

Step 2. Click Monitor -> Conversations and select the top conversation in which the top host from the previous step is taking part. Take note of the statistics provided in this table (Figure 5).

Step 3. While keeping this conversation selected, click the Details button at the bottom of the screen. A screen pops up with details about this conversation, including applications being transported, other hosts involved in conversation with the server, and so on. Study the details provided on this screen (Figure 6).

Step 4. Close the popup window and click the Capture button at the bottom of the screen. A Java applet pops up and shows a standard three-pane capture decode window, much like any standard decoder tool (Figure 7). Click a few packets on the top screen. In the middle window, try to expand some of the fields in the header and examine the details (for example, expand the IP header and observe the values used for DSCP).

Figure 4. Top Hosts and Applications

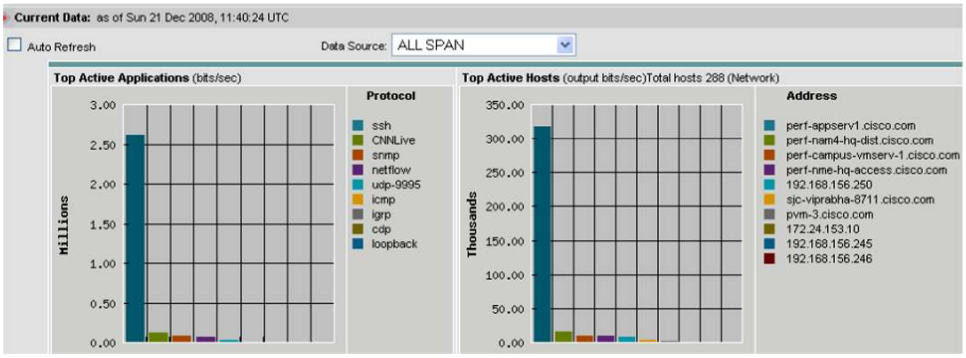
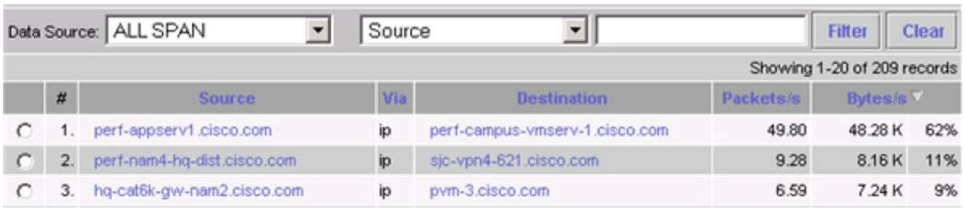


Figure 5. Statistics on the Top Conversations



	#	Source	Via	Destination	Packets/s	Bytes/s	
○	1.	perf-appserv1.cisco.com	ip	perf-campus-vmserv-1.cisco.com	49.80	48.28 K	62%
○	2.	perf-nam4-hq-dist.cisco.com	ip	sjc-vpn4-621.cisco.com	9.28	8.16 K	11%
○	3.	hq-cat6k-gw-nam2.cisco.com	ip	pvm-3.cisco.com	6.59	7.24 K	9%

Figure 6. Details in the Top Conversation

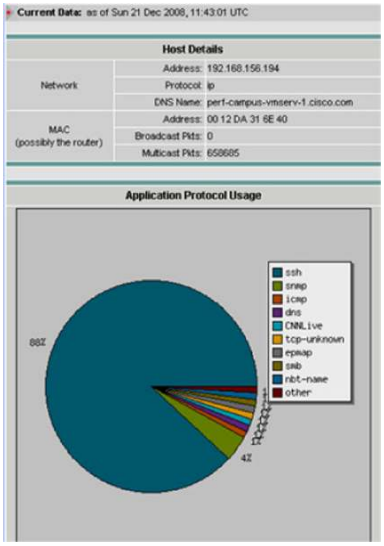
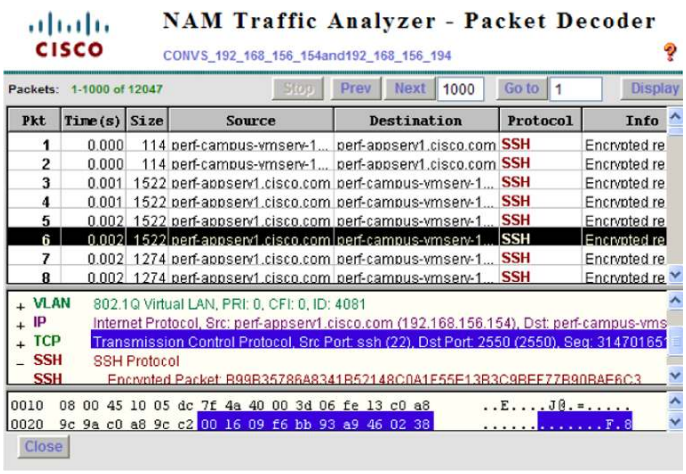


Figure 7. The Three-Pane Capture Decode Window



Alternate Deployments: 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.

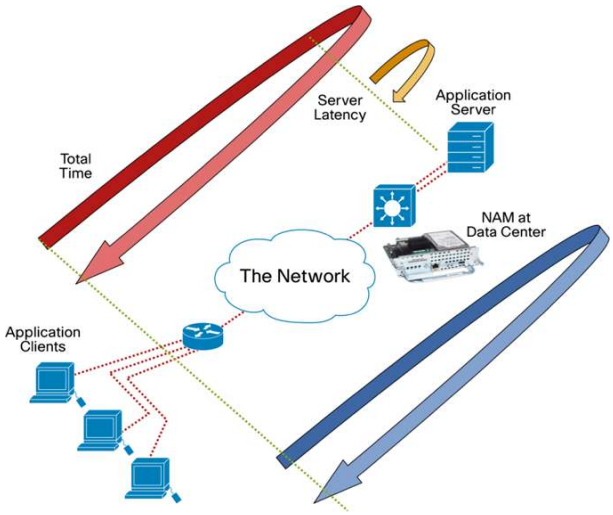
Scenario 2: Troubleshooting User-Experience Problems Using IAP Analysis

Providing a high-quality network experience to users located in branch locations that are geographically dispersed from data centers is one of the tougher challenges facing IT today. The trend toward data center consolidation has provided significant savings in resources and made data centers more robust and reliable. At the same time, this trend has pushed most enterprise users further away from the data center (typically, large, consolidated data centers are located in a few locations across the country and serve tens of thousands of users spread across offices in the country and the rest of the world). As a result, transaction-intensive (chatty) applications that were designed to communicate across a LAN are now forced to work across the WAN, resulting in poor performance. In short, while data center consolidation offers a host of benefits, it also raises issues around the experience of individual users. It is therefore critical for IT to measure user experience as perceived by users in each office and proactively manage network performance so that employee productivity remains unaffected irrespective of location.

The IT engineer detects that the response time in the Atlanta branch has dipped below normal levels. The payroll application server seems to be responding slowly to user requests and is timing out frequently (as per user complaints).

Deployment: NAMs are deployed at the data center (NAM-2 blade or 2220 appliance), and NME-NAMs are deployed at key branch locations. IAP technology allows NAM to break down the total response time into its component pieces: the application server portion of the delay (see the orange U-turned arrow in Figure 8) and the network portion of the delay (see the blue U-turned arrow in Figure 8).

Figure 8. NAM Breaks Down the Total Response Time into Its Components

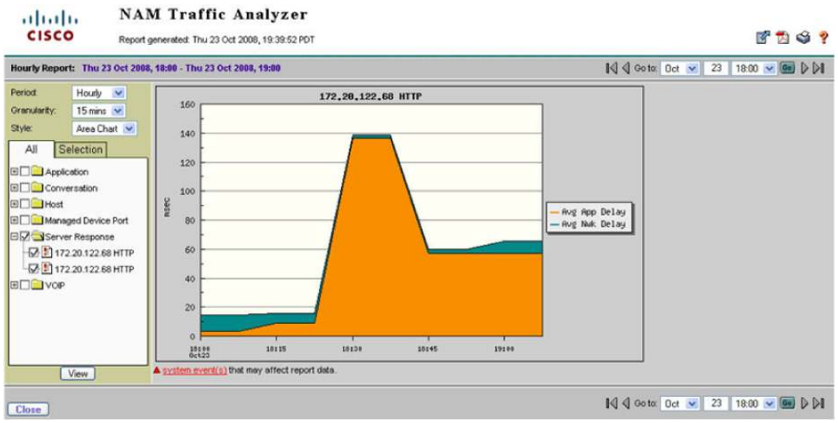


Step 1. Enable IAP monitoring. Use the live screen to monitor response times for two or three periods (a period is typically 5 minutes and is user configurable).

Step 2. A historical report that charts network and application response time provides information on latency on the network and compares it to latency in the data center (Figure 9). From 10 a.m. to about 10:25 a.m., both application and network delay are low (less than 10 msec). Between 10:20 and 10:25, there is a sudden spike in the total delay. Clearly, the graph indicates that the total time (which used to be around 12 msec) has now shot up to about 140 msec. Importantly, the graph points out that the increase has occurred due to a spike in application delay, not a network delay.

Step 3. Now that the engineer knows that the network is working as expected, he or she spends the rest of the time troubleshooting the source of the problem in the data center. Therefore, redundant efforts from multiple teams are cut out, and IT starts to focus all its efforts on the problem area from the start.

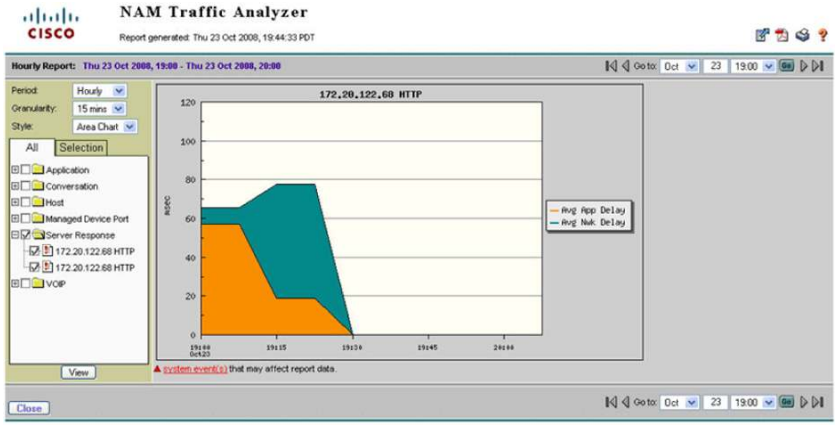
Figure 9. Comparison of Latency on the Network with Latency in the Data Center



Step 4. The other possibility is that the network delay spikes up. See Figure 10, in which the application delay decreases but the network delay actually increases. In this case, the engineer will focus all the effort on the network side. The NAM provides various tools to continue troubleshooting the network.

Note: These graphs have been created under lab conditions using traffic generation tests. Do not use these values as benchmarks for real-world numbers. This is also the reason the graph ends (in the real-world, historical reporting would typically trend the network continuously).

Figure 10. Application Delay Deceases but Network Delay Actually Increases



The IAP toolkit is powerful, offering more than 40 metrics relating to user experience. Becoming familiar with the metrics that are important to your network will provide significant benefits in helping manage your network performance.

Alternate Deployments: IAP functionality can be useful at any place in the network where there is a need to measure response-time-related metrics. Although NAM is deployed at the data center in this scenario, you can get similar benefits in any other location. The only thing to keep in mind with IAP metrics is that NAM must be able to monitor the interactions between the client and the server; that is, the data source must be set up in such a way that NAM has access to the packet stream of interest.

Scenario 3: Monitoring Cisco WAAS and Measuring Its Impact

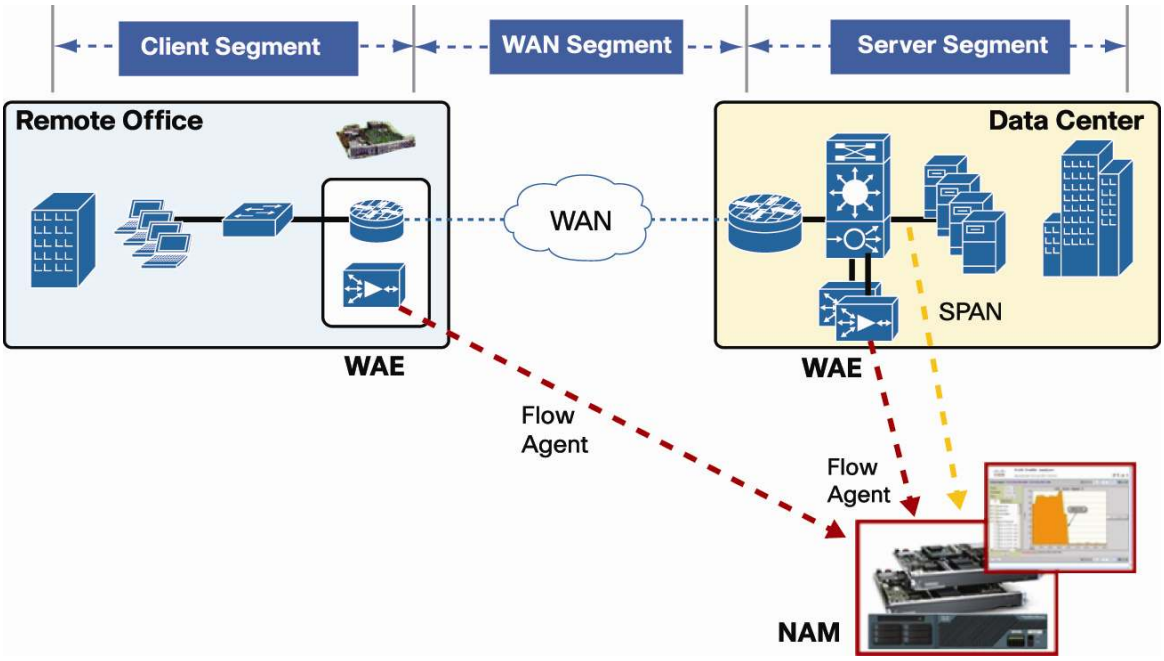
Cisco Wide Area Application Services is a comprehensive WAN optimization solution that accelerates applications over the WAN, delivers video to the branch office, and provides local hosting of branch-office IT services. Cisco WAAS allows IT departments to centralize applications and storage in the data 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 to provide troubleshooting as well as planning information for expanding the deployment.

NAM 4.0 adds the ability to monitor WAAS-optimized flows by using WAE devices as data sources. Using this capability, 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.

Deployment: Placing a Cisco NAM 2220 appliance at the edge of the data center is the best choice for WAAS deployments. From this location in the network, 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. 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.

Figure 11. Cisco NAM's Ability to Analyze from Multiple Data Sources

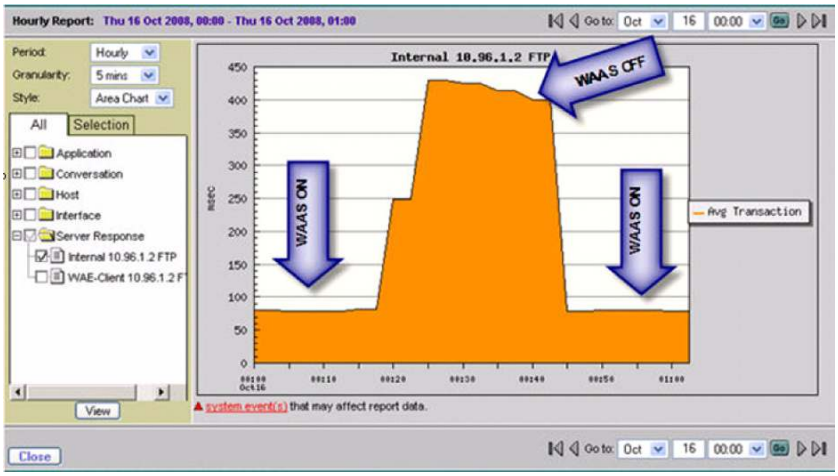


Step 1. Using a NAM 2220 deployed at the data center, measure application response time before WAAS is enabled using a historical report.

Step 2. Enable WAAS; continue measuring application response (same report as in step 1, no further action required in this step).

Step 3. Observe changes in the historical report over time. Refresh the report viewer to get the latest measured data. See Figure 12. The picture shows a scenario where WAAS is initially on, then it is disabled, and finally, it is enabled again. Notice that when WAAS is on, application response time for FTP transfers between the data center and the branch is about 80 milliseconds. When WAAS is disabled, application response time spikes to ~430 milliseconds. And finally, when WAAS is enabled again, it returns to the original 80-millisecond range. This picture 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.

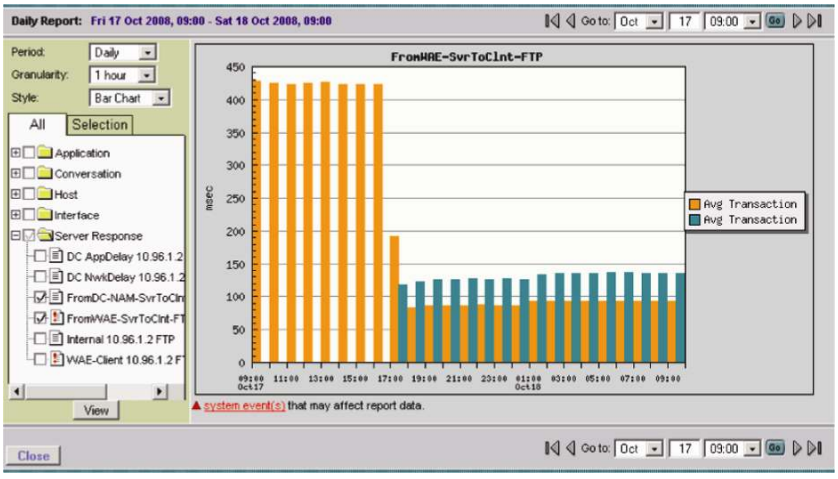
Figure 12. A Scenario with WAAS Initially On, Then Turned Off, Then Turned On Again



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; WAE 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, NAM can be configured to send alerts to appropriate personnel with information relevant to troubleshooting the problem.

Figure 13 shows the initial response time before WAAS was enabled, measured at the data center using SPAN (orange bars). After WAAS was enabled, response time reduced as expected. Also, the WAE device started to export information about the optimized flows (green bars). (You see that the green bars are on average a few milliseconds more than the orange bars. This is the additional time that it takes for packets to traverse the WAN.)

Figure 13. Response Time Before and After WAAS Was Enabled



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.

Scenario 4: 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.

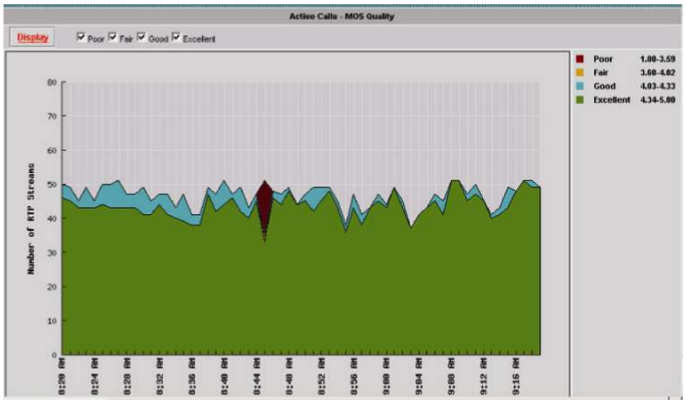
Deployment: NAM deployments for voice quality analysis require that NAM be able to monitor VoIP packets from the calling phone to the called phone. The branch edge location in the network provides visibility into all calls entering and leaving the branch; similarly a campus edge location monitors calls 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 Case: Monitor the network to make sure that call quality is good. If quality issues appear, isolate and troubleshoot the problem rapidly.

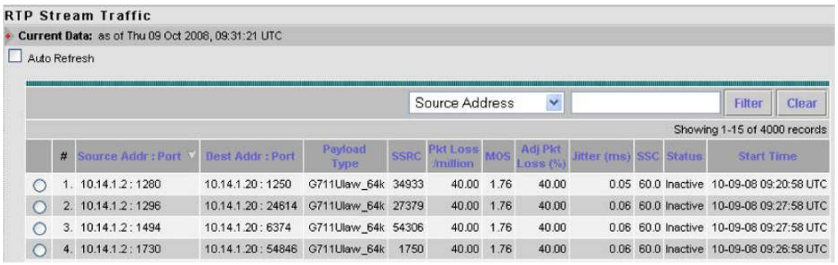
Step 1. Under the Monitor -> Voice/Video menu, click Active Calls -> MOS Quality Chart. This chart (see Figure 14) indicates current voice quality of all RTP streams being monitored. MOS values range from 1 to 5 where 1 is poor and 5 is excellent (see the legend in Figure 14 for a breakdown into categories - excellent, good, and so on - within this range). Notice that there are calls that are in the poor range.

Figure 14. Current Voice Quality for All RTP Streams Being Monitored



Step 2. To isolate calls that had a poor MOS, navigate to the Active Calls Table and sort by the MOS value. In Figure 15, notice that the MOS value for the calls listed on top is 1.76, which is very low. Further, looking at the other metrics provided in the same row (take row 1 for example), notice that jitter is.05 (which is a good value) but the adjusted packet loss rate is 40 percent (an unusually high value, which can lead to poor call quality). This information tells you that jitter is not the root cause of the poor calls; instead it is packet loss somewhere in the network.

Figure 15. The Active Calls Table Sorted by MOS



#	Source Addr : Port	Dest Addr : Port	Payload Type	SSRC	Pkt Loss /million	MOS	Adj Pkt Loss (%)	Jitter (ms)	SSC	Status	Start Time
1.	10.14.1.2 : 1280	10.14.1.20 : 1250	G711Ulaw_64k	34933	40.00	1.76	40.00	0.05	60.0	Inactive	10-09-08 09:20:58 UTC
2.	10.14.1.2 : 1296	10.14.1.20 : 24614	G711Ulaw_64k	27379	40.00	1.76	40.00	0.06	60.0	Inactive	10-09-08 09:27:58 UTC
3.	10.14.1.2 : 1494	10.14.1.20 : 6374	G711Ulaw_64k	54306	40.00	1.76	40.00	0.06	60.0	Inactive	10-09-08 09:27:58 UTC
4.	10.14.1.2 : 1730	10.14.1.20 : 54846	G711Ulaw_64k	1750	40.00	1.76	40.00	0.06	60.0	Inactive	10-09-08 09:26:58 UTC

Step 3. The next step is to identify where packets are being lost. Using the IP addresses provided in the active calls table (for the source IP address), it is clear that all calls originate from 10.14.1.2 but with different source port numbers. This is typical of a conference call where multiple callers have dialed into a conferencing system. Now look up your network topology to identify where in the network the 10.14.1.0 subnet is located. For the purposes of this use case, say this subnet is in Building 3 of the main campus.

Step 4. You know that the Building 3 distribution switch has a NAM located in it. Navigate to that NAM and look up Monitor -> Chassis Parameters -> Interface Statistics. 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.

Scenario 5: Using NAM for Historical Reporting and Trends

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

- Every real-time metric that is provided by NAM can be tracked historically. But it is important to note that while real-time analysis is enabled when a service is turned on, historical reports are not automatically enabled at the same time (see the following note for an exception to this). In order to track metrics historically, you must manually create a report using the NAM GUI. This involves using the Reports menu on the NAM GUI and selecting the data source to be used, the granularity of the report, and the specific metrics that need to be measured.

Note: Some basic reports are in fact enabled automatically on the NAM. Examples include the Top Applications and Top Hosts reports. Click Reports -> Basic Reports to see what reports are created automatically.

- Once a historical report is created, data collection starts, and data points are created every period. For example, you create a "conversation report" on the conversation that was analyzed in Scenario 1. You set the granularity to be 5 minutes - this means NAM will compute average statistics every 5 minutes and store a data point in the hard drive. It will continue to do so for 100 days. At this point, any new data points will continue to be collected, but the oldest data points will be dropped, one at a time. Think of it as a moving time window of 100 days.
- The report viewer on NAM offers good flexibility. It is possible to open a report at daily granularity in a bar chart format and then change to hourly granularity in an area chart format. Also, you can open one report and then compare or contrast the output to another NAM report dynamically. (If you have a NAM that is currently operational, try the following: On the report tree situated in the left pane of the report viewer, click two checkboxes and then click the View button. You will see that both reports are pulled up and shown in the same window.)

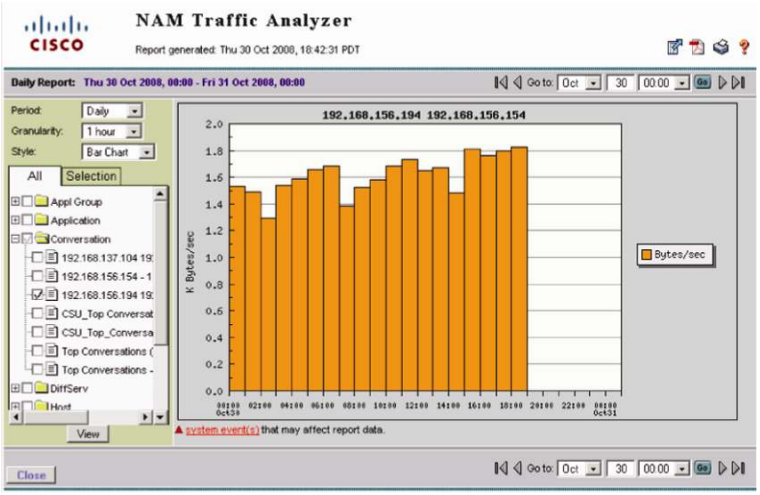
The IT engineer needs to predict the capacity needed for a new branch buildout due in 6 months by studying the usage of an existing branch office of a similar size.

Deployment: NME-NAM located in the branch router (ISR) of the existing branch.

Step 1. The engineer starts capturing traffic rates between the branch and the data center. The engineer lets historical monitoring reports run for a month.

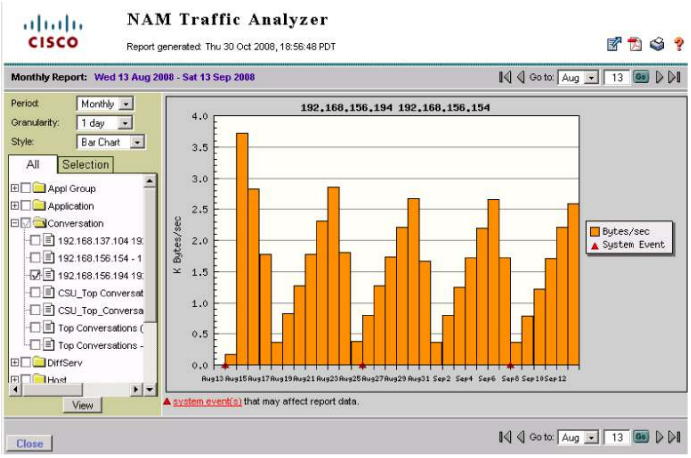
Step 2. The engineer opens a conversation report from today and finds a stream that has a mildly increasing trend but is unable to confirm the rate at which it is increasing (Figure 16).

Figure 16. A Stream with a Mildly Increasing Trend



Step 3. The engineer changes the reporting period dynamically on the Report Viewer to study the trend with a granularity of 1 month. The engineer finds that the pattern does show periodic increases, but it always hits a ceiling between 2.5 KBps and 3.5 KBps (Figure 17). The engineer is 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 17. The Trend Shown with a Granularity of 1 Month



Studying historical trends is a valuable exercise in planning and baselining a network. You are encouraged to start a number of reports using metrics and data sources that are most relevant. These reports should provide handy information in a variety of day-to-day decisions.

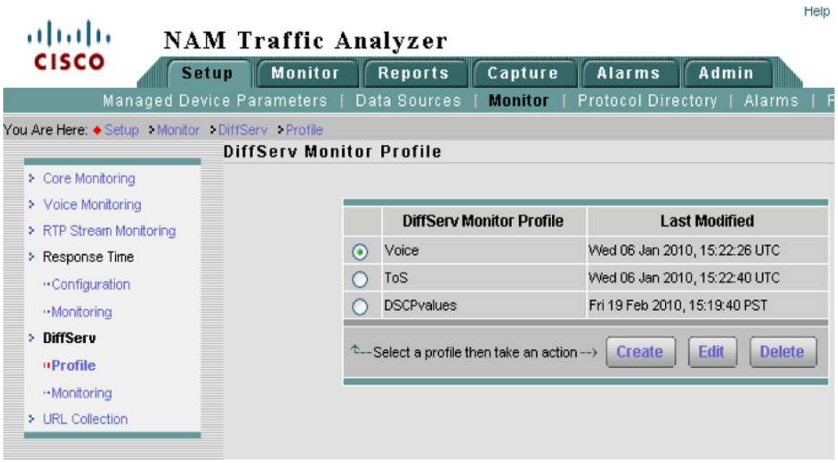
Scenario 6: Using NAM to Monitor QoS/DiffServ

Differentiated Services (DiffServ) provides insight into how the traffic is being classified by QoS and detects incorrectly marked or unauthorized traffic. NAM identifies the application/protocol based on the type of service (ToS) bits setting. The administrator must configure DiffServ profiles based on templates provided or create one (Figure 18). The voice template can be used to monitor whether voice traffic is marked properly. Figure 19 displays the DiffServ application statistics for DSCP value 0. Looking at this you'll notice that RTP and Skinny Client Control Protocol (SCCP) are listed, which indicates that they are not being correctly marked throughout its path.

Deployment: 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.

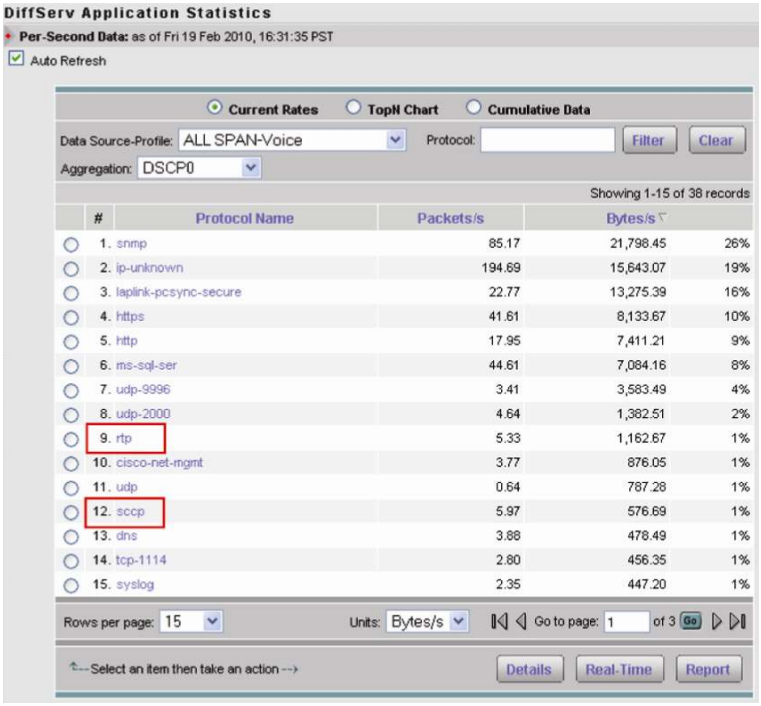
Step 1. Access the NAM and create a DiffServ profile for voice in Setup -> Monitor -> DiffServ Profile. Select the desired DSCP value such as 46 for RTP and 24 for SCCP signaling.

Figure 18. Creating DiffServ Monitor Profile



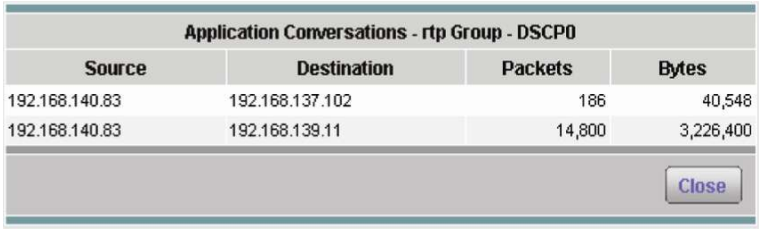
Step 2. Access the DiffServ monitoring screen to display the protocols detected on each of the DSCP values. Notice that rtp and sccp are highlighted in Figure 19. The protocols are listed for DSCP 0, which is incorrect since the standard classification for voice traffic is DSCP 46 and for signaling is DSCP 24. This informs the administrator that some of the voice traffic is misclassified on the network. The administrator can also view the branch NAMs to investigate whether voice traffic is being misclassified.

Figure 19. DiffServ Application Statistics



Step 3. Clicking rtp or sccp displays the clients using those protocols and helps in troubleshooting why RTP or SCCP traffic from these clients is not marked correctly. it is time to review the QoS policy implemented on the routers and switches between the clients. Figures 20 and 21 display the IP addresses of the phones and Cisco Unified Communications Manager or the gateway.

Figure 20. Application Conversations for RTP

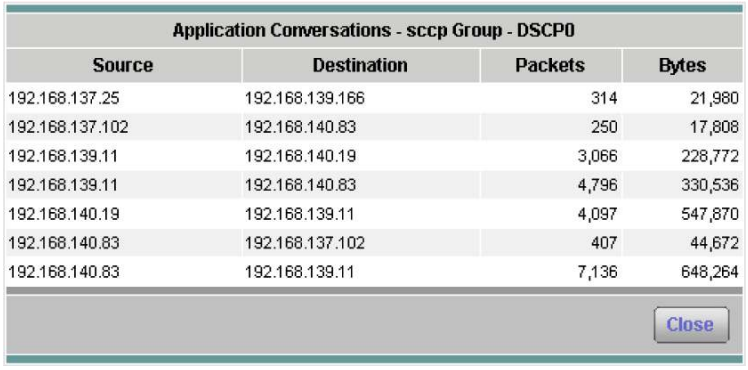


Application Conversations - rtp Group - DSCP0

Source	Destination	Packets	Bytes
192.168.140.83	192.168.137.102	186	40,548
192.168.140.83	192.168.139.11	14,800	3,226,400

Close

Figure 21. Application Conversations for SCCP



Application Conversations - sccp Group - DSCP0

Source	Destination	Packets	Bytes
192.168.137.25	192.168.139.166	314	21,980
192.168.137.102	192.168.140.83	250	17,808
192.168.139.11	192.168.140.19	3,066	228,772
192.168.139.11	192.168.140.83	4,796	330,536
192.168.140.19	192.168.139.11	4,097	547,870
192.168.140.83	192.168.137.102	407	44,672
192.168.140.83	192.168.139.11	7,136	648,264

Close

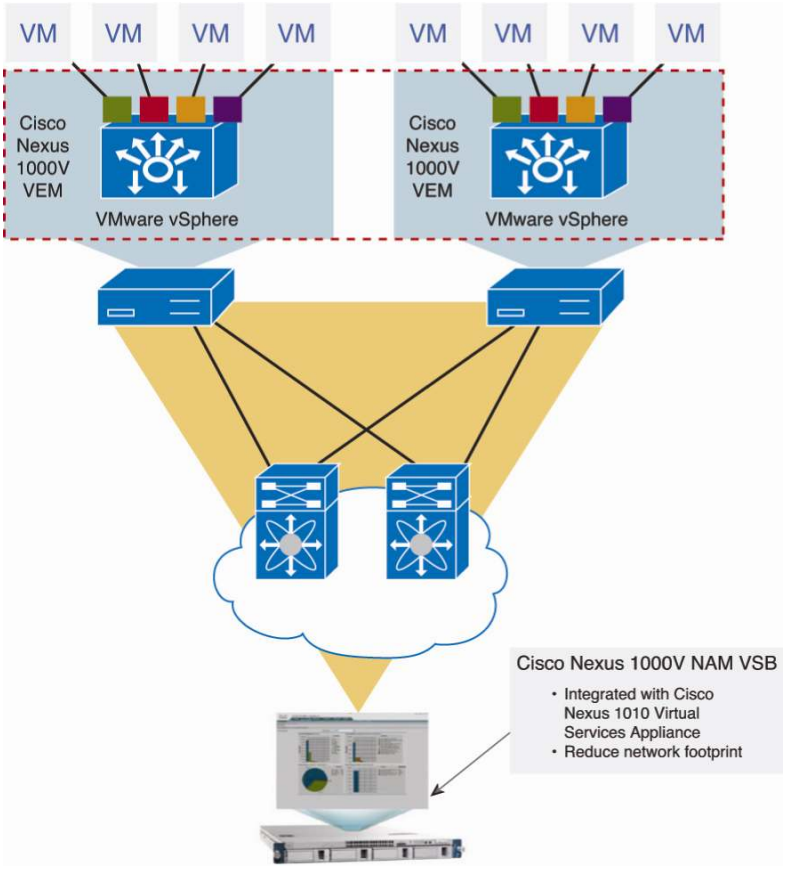
Scenario 7: Using Nexus 1000V NAM VSB to Monitor Nexus 1000V Switch Environment

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 22.

Deployment: 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, NAM upgraded to version 4.2 can be utilized to monitor the switches through ERSPAN or NetFlow data sources to the NAM. The 1000V switch and NAM should be directly connected to the same physical switch.

Figure 22. Cisco Nexus 1000V NAM Virtual Service Blade Deployment



Step 1. Install and configure NAM VSB on the Nexus 1010 Virtual Services Appliance. Refer to the Appendix, “Installing and Using Cisco NAM.”

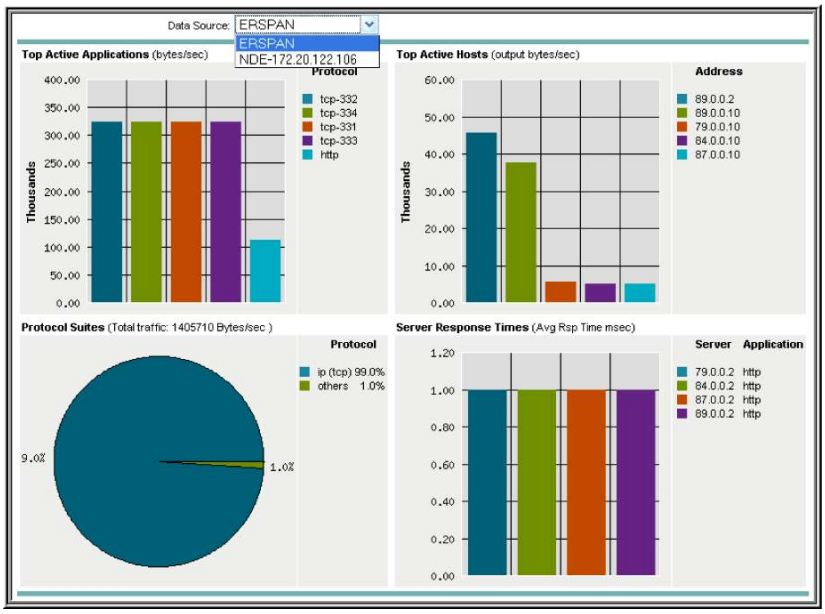
Step 2. Verify that ERSPAN or NetFlow are configured on the 1000V switch Virtual Supervisor Module (VSM) providing data to NAM.

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 23 shows the Overview page, displaying top N information, for example, applications, hosts, protocol, and server response time. Navigation is provided to view and display details for each of the categories listed.

Step 5. Configure reports for trending on the application response time, hosts and conversation traffic patterns.

Figure 23. NAM Monitor Overview



Step 6. The physical and virtual interfaces table provides VM-to-VM traffic utilization (Figure 24). Because one virtual interface connects to one VM, the data displays which VMs are utilizing the switch resources. The administrator then can view the hosts and conversations tables to identify the culprit utilizing the resources.

Figure 24. NAM Monitor Managed Device Interfaces

#	Interface	In % Utilization	Out % Utilization	In Packets/s	Out Packets/s	In Bytes/s		Out Bytes/s	In Non-Unicast/s	Out Non-Unicast/s	In Discards/s	Out Discards/s	In Errors/s	Out Errors/s
1.	Ethernet6/2	1.42	1.50	3,930.63	4,850.26	1,778,666.67	17%	1,873,078.83	7.76	0.02	0.00	0.00	0.00	0.00
2.	Ethernet3/2	13.91	6.46	3,425.44	3,517.51	1,738,865.34	16%	806,911.05	7.74	0.03	0.00	0.00	0.00	0.00
3.	Ethernet5/2	1.38	0.65	3,415.40	3,524.87	1,729,891.73	16%	814,646.88	7.77	0.02	0.00	0.00	0.00	0.00
4.	Ethernet4/2	1.38	0.64	3,406.37	3,499.42	1,729,144.48	16%	805,829.48	7.75	0.02	0.00	0.00	0.00	0.00
5.	Vethernet9	0.00	0.00	451.76	3,683.40	1,024,070.58	10%	1,611,333.46	0.00	0.01	0.00	0.00	0.00	0.00
6.	Vethernet2	0.00	0.00	4,113.12	59.51	660,844.05	6%	85,633.24	0.00	7.70	0.00	0.00	0.00	0.00
7.	Vethernet3	0.00	0.00	3,260.58	93.96	537,747.67	5%	134,824.35	0.00	7.70	0.00	0.00	0.00	0.00
8.	Vethernet4	0.00	0.00	3,245.21	95.60	535,710.03	5%	137,077.28	0.01	7.70	0.00	0.00	0.00	0.00
9.	Vethernet1	0.00	0.00	3,243.39	67.94	535,479.84	5%	97,686.51	0.00	7.70	0.00	0.00	0.00	0.00
10.	Vethernet6	0.00	0.00	51.39	3,209.14	108,873.69	1%	1,580,929.43	0.01	0.01	0.00	0.00	0.00	0.00
11.	Vethernet8	0.00	0.00	43.26	3,182.70	102,394.66	1%	1,571,921.46	0.01	0.01	0.00	0.00	0.00	0.00
12.	Vethernet7	0.00	0.00	44.13	3,201.02	102,391.13	1%	1,580,339.59	0.01	0.01	0.00	0.00	0.00	0.00
13.	mgmt0	0.00	0.00	12.18	412.39	1,897.24	<1%	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Note: NAM VSB provides the same complement of features as version 4.1 except that it supports only ERSPAN and NetFlow data sources and performs no voice monitoring and packet capture.

Addressing Some Common NAM Deployment Questions and Concerns

New users of the NAM sometimes wonder if there are potential negative side effects to using a NAM and especially to inserting a NAM into a business-critical switch or router. Some of the more common questions and concerns are addressed below.

Q. Will using SPAN or Cisco Express Forwarding copy have an impact on the original traffic stream?

A. A. No, there is no impact to the original traffic stream. SPAN technology heavily uses hardware and therefore has minimal impact on the CPU utilization of the router. Also, SPAN replicates and then directs traffic to the SPAN destination. It does not in any way hinder the original stream, which continues along its path without bearing any impact of SPAN being enabled.

Cisco Express Forwarding copy behaves similarly, with the only difference being that software processes are used in the process of copying and directing traffic to the secondary destination. Consequently, you might possibly see a slight increase in CPU utilization on the router as a result of packet replication (whereas on the Catalyst 6500, the CPU impact of SPAN is negligible and does not have a tangible impact on CPU utilization). This increase in CPU utilization on the router is not harmful in any way; however, users must take note of this during deployment and make sure that routers are not overloaded when turning on this feature.

Q. Can I hot-swap NAM cards?

A. On a Catalyst 6500 or Cisco 7600, all cards are hot-swappable, and so are the NAMs. Therefore, you can insert or remove a NAM when the switch is in operation. It is always good practice to perform a “shutdown” operation on the NAM before removing a card that is in operation.
On an ISR router, NAMs are hot-swappable only on the Cisco 3845 and the 3900 Series. NAMs are not hot-swappable on any other router within this platform, including the Cisco 3825 and the Cisco 2800 Series. Also, when performing a hot swap on the 3845, make sure that all interfaces are shut down and that the NAM is not receiving any traffic.

Q. What will happen to my router or switch if my NAM suffers a crash or a hardware fault?

A. A crash on the NAM will not affect any operations on the router or switch. As you can see from previous answers in this section, NAM is a very independent module with its own hardware, operating system, and software. As a result, if a crash occurs on the NAM, it does not affect the switch or router in any way. NAM functionality will be affected, obviously, but routing and switching operations will continue unaffected. As a corollary, upgrading NAM software can be done on a live production router.
Hardware faults, similarly, do not affect the switch or router. The NAM itself will be affected and will shut itself down in the event of a hardware fault or reboot the operating system in the event of a software crash (a crash file will also be created). But the impact is local to the NAM and has no effect on the system as a whole.

Q. How can the Cisco NAM solution be made more secure?

A. Take the following steps to increase security for the Cisco NAM solution:

- Enable Secure Sockets Layer (SSL) on the Cisco NAM for secure, encrypted HTTP sessions.
- Enable Secure Shell (SSH) Protocol for secure Telnet to the Cisco NAM.
- Enable TACACS+ for authentication and authorization. The Cisco NAMs also provide support for multiple TACACS+ servers.

Q. Can the other NAM platforms monitor the Nexus 1000V switch?

A. Yes, the other NAM platforms running version 4.2 will provide insight into the 1000V switch environment through ERSPAN and NetFlow data sources. It is recommended that NAM and the 1000V switch be directly connected to same physical switch.

Cisco NAM Integrations with Monitoring and Reporting Applications

While the NAM provides its own GUI, it is often useful to combine the information provided by the NAMs in your network and centralize it within one tool. Centralization of networkwide information allows easier visibility across the network and more proactive reporting and analysis. Table 3 describes how NAM integrates with Cisco and third-party applications.

Table 3. Tools That Can Be Integrated with Cisco NAM

Integration with	Details	Uses
NetQoS SuperAgent	With Cisco NAM 4.0, NAM and NetQoS SuperAgent 8.1 offer an integrated workflow. NAM essentially plays the role of NetQoS aggregator. NAM collects IAP metrics and forwards the information to the SuperAgent Master Console. Another extension of the same feature is from the perspective of Cisco WAAS. NetQoS SuperAgent, once again, serves as the central dashboard for WAAS monitoring and analysis. Cisco NAM 4.0 provides mediation and processing for optimized flow information sent from WAE data sources.	Centralized IAP management using NAMs as mediation layer
CiscoWorks LAN Management Solution (LMS)	LMS is a network configuration and change management solution offered as part of the CiscoWorks line of products. Users who own LMS can use built-in capabilities to upgrade NAM software (SWIM module within LMS). Also, when syslog and trap collection is turned on in LMS, it can serve as a collector and aggregator of alerts and information from NAMs.	NAM software upgrades Syslog/trap collection
Compuware Vantage Analysis Server (VAS)	Cisco NAM and VAS 11.1 provide an integrated offering to deliver end-to-end application performance management and network visibility. Vantage uses application response time data (IAP) from multiple Cisco NAMs and delivers enterprisewide reporting (supports WAAS deployments). Vantage also provides real-time reports and alerts, plus baseline analysis and trending.	Centralized application management using NAM as the mediation layer
Other third-party solutions	NAM is an open device. Any tool that has the ability to interface with the NAM through Simple Network Management Protocol (SNMP) and comma-separated value (CSV) interfaces will be able to use the NAM as a data source.	Data collected from NAM modules can be used as input into any currently used network management applications. Syslogs and traps can be exported to general-purpose network management solutions. Performance data can be exported to applications that collect network and application performance metrics from the network. Centralized network management tools that can poll Remote Monitoring (RMON) MIBs on NAM (as well as syslogs and traps exported by NAM) and provide a single dashboard through which to monitor the network.

References

Cisco Network Analysis Module Series product page: http://www.cisco.com/go/nam.

Cisco Network Analysis Module Technical Documentation: http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html.

Cisco Nexus 1000V Technical Documentation: http://www.cisco.com/go/1000vdocs.

Configuring Local SPAN, Remote SPAN, and Encapsulated RSPAN:

- Catalyst 6500: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/span.html .
- Catalyst 4500: http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/53SG/configuration/span.html.
- Nexus 7000: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/system_management/configuration/guide/sm_14span.html

Cisco IOS NetFlow: http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html.

Product Installation, Configuration, and Upgrade Guides: http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html.

User Guides: http://www.cisco.com/en/US/products/sw/cscowork/ps5401/products_user_guide_list.html.

Appendix

Installing and Using Cisco NAM

Installation and Configuration

The initial steps before launching the Cisco NAM web GUI are as follows:

Step 1. Install the NAM hardware.

Step 2. Log in to the NAM CLI to set up the initial configuration.

Step 3. Upgrade the software to the desired version.

Step 4. Configure the data sources through the GUI (or CLI in the case of the NME-NAM).

Step 5. Enable the desired monitoring capabilities.

Installation and Configuration of Catalyst 6500 and 7600 Service Module

This section covers the basic instructions for installing and configuring a NAM Catalyst 6500 and 7600 Service Module. Please refer to the Quick Start Guide (see “References”) for more detailed discussion.

Step 1. Insert the Cisco NAM into any available slot (except the slot reserved for supervisor modules) in your Cisco Catalyst 6500 or Cisco 7600 chassis. For further information on physically installing the Cisco NAM in a Cisco Catalyst 6500 or Cisco 7600 chassis, see “References.”

Step 2. Select a management VLAN for the NAM:

```
conf t
analysis module slot_number management-port access-vlan vlan_number
end
```

Step 3. Open a session into the NAM:

```
Cisco IOS Software:
session slot <module-number> processor 1
Catalyst OS:
session <module-number>
```

Step 4. Log in to the NAM using the username root. The default password is root. Please change the password once logged in using the command:

```
password root
```

Step 5. Enable the NAM network parameters:

```
ip address <ip-address> <subnet-mask>
ip gateway <default-gateway>
ip domain <domain-name>
ip host <name>
ip nameserver <ip-address>
```

Step 6. Enable the NAM Traffic Analyzer GUI:

```
ip http server enable
```

Enter a web username and password.

Step 7. You can now type the NAM IP address in a browser to access the NAM Traffic Analyzer GUI.

Installation and Configuration of the NAM Branch Router Network Module

This section covers the basic instructions for installing and configuring a NAM ISR network module. Only the scenario of using the internal NAM interface for management is covered.

Step 1. Configure the router side network parameters:

```
conf t
interface integrated-service-engine <slot>/0
ip address <router-side-ip-address> <subnet-mask>
   or
ip unnumbered <interface>
service-module ip address <module-side-ip-address> <subnet-mask>
service-module default-gateway <gateway-ip-address>
exit
If using the unnumbered interface, configure a default route for the NAM IP address:
ip route <module-side-ip-address> 255.255.255.255 integrated-service-engine <slot>/0
copy running-config startup-config
```

Step 2. Now we are ready to open a session to the NAM.

```
Opening a session:
service-module integrated-service-engine <slot>/0 session clear
service-module integrated-service-engine <slot>/0 session
Closing the session:
Control-Shift-6 x
disconnect
```

Step 3. Log in to the NAM using the username root. The default password is root. Change the password once logged in using the command:

password root

Step 4. Configure the NAM for network connectivity:

ip interface [internal | external]

ip address <module-side-ip-address> <subnet-mask>

ip gateway <gateway-ip-address>

ip domain <domain-name>

ip host <name>

ip nameserver <ip-address>

Step 5. Enable the NAM Traffic Analyzer GUI:

```
ip http server enable
```

Enter a web username and password.

Step 6. You can now type the NAM IP address in a browser to access the NAM Traffic Analyzer GUI.

Installation and Configuration of the Cisco NAM Appliance

This section covers the basic instructions for installing and configuring a NAM appliance. For further details, follow links provided in the “References” section.

Step 1. Connect to the console of the appliance and log in using the username root. The default password is root. Change the password once logged in using the command:

```
password root
```

Step 2. Configure the NAM for network connectivity:

```
ip address <ip-address> <subnet-mask>
ip gateway <ip-address>
ip domain <domain-name>
ip host <name>
ip nameserver <ip-address>
```

Step 3. Enable Telnet or SSH for direct access to the appliance:

```
exsession on (Telnet)
   OR
```

exsession on ssh (SSH)

Step 4. Enable the NAM Traffic Analyzer GUI:

```
ip http server enable
```

Enter a web username and password.

Step 5. You can now type the NAM IP address in a browser to access the NAM Traffic Analyzer GUI.

Installation and Configuration of the Cisco NAM VSB

This section covers the basic instructions for installing and configuring a NAM VSB. For further details, follow links provided in the “References” section.

Step 1. Log in to the Nexus 1010 and enter virtual blade configuration mode:

```
vsm-nam1# conf t
vsm-nam1(config)# dir bootflash:/repository
  ...
  153135104     Jan 20 09:37:17 2010  nam-app-x86_64.4-2-0-13.iso
  ...
```

Step 2. Enter the NAM configuration information:

```
vsm-nam1(config)# virtual-service-blade NAM
vsm-nam1(config-vb-config)# virtual-service-blade-type new
nam-app-x86_64.4-2-0-20091207.iso
vsm-nam1(config-vb-config)# interface data vlan 3
vsm-nam1(config-vb-config)# enable
Enter Management IP address:  10.10.10.11
Enter Management subnet mask length:  25
IPv4  address of the default gateway:  10.10.10.1
Enter Switchname:  nam-vsm1
Setting Web user/passwd will enable port 80. Press Enter:
Web User name:  [admin]
Web User password:  admin
```

Step 3. You can now type the NAM IP address in a browser to access the NAM Traffic Analyzer GUI.

Upgrading Software on the Catalyst 6500 and 7600 Service Module

This section covers the basic instructions for upgrading the application image on the NAM running on a Catalyst 6500 and 7600 running Cisco IOS Software. For further details, follow links provided in the “References” section.

Step 1. Boot the NAM into maintenance mode:

```
hw-module module <slot> reset cf:1
```

Step 2. Open a session into the NAM and log in:

```
session slot <slot> processor 1
```

Log in using root as the username and cisco as the password.

Step 3. Upgrade the NAM application image:

```
upgrade <ftp-url>
```

Follow the prompts during installation, and log out after it is done.

Step 4. Reset the NAM to reboot the newly installed image:

```
hw-module module <slot> reset
```

Upgrading Software on the NAM Branch Router Network Module

This section covers the basic instructions for upgrading the application image on the NAM on an ISR router. For further details, follow links provided in the “References” section.

Reload the NAM:

```
service-module integrated-service-engine <slot>/0 reload
```

Step 1. Session into the NAM:

```
service-module integrated-service-engine <slot>/0 session
```

While the service module reboots, it displays the following prompt:

Enter *** to change boot configuration:

Step 2. Enter ***

Step 3. At the bootloader prompt, boot the helper image:

```
boot compactflash
```

Step 4. At the helper menu, select 1 to install the new application image.

Step 5. Select r after the installation to reboot the new application image.

Configuring Data Sources on the NAM

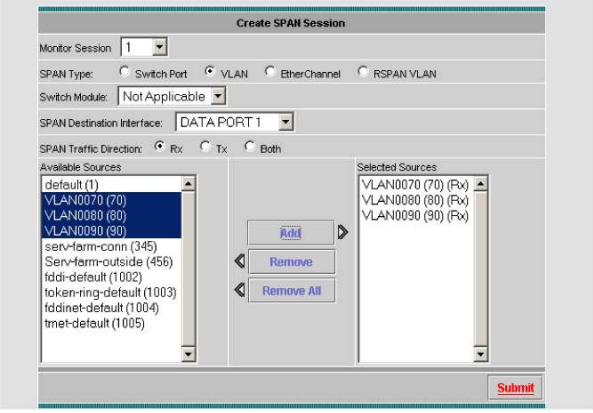
For details on SPAN and RSPAN configurations, please refer to “Configuring Local SPAN, Remote SPAN, and Encapsulated RSPAN” in the “References” section.

RSPAN copies packets to a remote destination port across one or more intermediary Layer 2 switches. Because RSPAN puts the monitoring traffic on the network, you should determine bandwidth or design restrictions involving RSPANs.

The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated to that RSPAN session in all participating switches. The SPAN traffic from the source or sources is switched to the RSPAN VLAN and then forwarded to destination ports configured in the RSPAN VLAN.

RSPAN requires configuring the source switch manually as shown in the following example. Once RSPAN is configured with the destination switch where the Cisco NAM resides, you should then use the NAM Traffic Analyzer to create the session to monitor RSPAN. Figure 25 illustrates the configuration on the destination NAM card.

Figure 25. Creating a SPAN Session from NAM Traffic Analyzer



Using VACL as a Data Source Within NAM

Why would one use or not use VACLs compared to SPAN and NetFlow?

- With SPAN, it is easy to create the sessions with full monitoring capability using the NAM Traffic Analyzer.
- VACLs allow SPAN-like capability to WAN interfaces or when SPAN sessions are limited and run out. They allow prefiltering of interesting traffic, specified subnets, or simply when traffic is too large. In addition, VACLs can be implemented to direct traffic to multiple Cisco NAMs.
- NetFlow provides comprehensive statistics and doesn't rely on SPAN or VACLs. It is also useful in collecting data from the Cisco Catalyst 6500 Series Multilayer Switch Feature Card or remote devices such as routers.

Table 2 provides a summary of possible data sources for the Cisco NAM, including benefits and limitations.

VACLs provide an alternative to using SPAN for similar purposes. The NAM Traffic Analyzer will use VACLs to capture or "filter" selected VLANs or (on Cisco IOS Software) WAN traffic to the NAM port or ports.

Note: In Cisco IOS Software Release 12.1(13)E or later, VACLs can also be applied to WAN interfaces. VACLs attached to WAN interfaces support only standard and extended Cisco IOS IP ACLs (not Internetwork Packet Exchange [IPX] protocol or MAC). VACLs can only be applied to packet-over-SONET (POS), ATM, and serial WAN interfaces. The VACL data analysis capability is not supported for the Cisco first-generation NAM.

The following examples illustrate the steps required to configure a VACL for a switch running native Cisco IOS Software Release 12.1(13)E1 or later.

Configuring VACL on a WAN Interface

```
Cat6509#conf t
Enter configuration commands, one per line. End with CNTL/Z.
6509(config)#access-list 100 permit ip any any
6509(config)#vlan access-map wan 100
6509(config-access-map)#match ip address 100
6509(config-access-map)#action forward capture
6509(config-access-map)#exit
6509(config)#vlan filter wan interface ATM6/0/0.1
6509(config)#analysis module 3 data-port 1 capture allowed-vlan 1-4094
6509(config)#analysis module 3 data-port 1 capture
6509(config)#exit
```

Configuring VACL on a VLAN Monitoring a LAN

For VLAN traffic monitoring on the LAN, the traffic can be forwarded to the NAM by using the SPAN feature on the switch. However, in some rare circumstances, if the traffic spanned exceeds the NAM's monitoring capability, it may be desirable to prefilter the LAN traffic before it is forwarded to the NAM. This can be achieved by using the VACL as illustrated below.

For LAN VACL on Cisco Catalyst OS 7.5 and later, the following example demonstrates how to configure VACL for LAN-VLAN interfaces. In this example, all traffic directed to the server 172.20.122.226 on VLAN 1 is captured and forwarded to the NAM located at slot 3.

```
Cat6509(config)#access-list 100 permit ip any any
Cat6509(config)#access-list 110 permit ip any host 172.20.122.226
Cat6509(config)#vlan access-map lan 100
Cat6509(config-access-map)#match ip address 110
Cat6509(config-access-map)#action forward capture
Cat6509(config-access-map)#exit
Cat6509(config)#vlan access-map lan 200
Cat6509(config-access-map)#match ip address 100
Cat6509(config-access-map)#action forward
Cat6509(config-access-map)#exit
Cat6509(config)#vlan filter lan vlan-list 1
Cat6509(config)#analysis module 3 data-port 1 capture allowed-vlan 1
Cat6509(config)#analysis module 3 data-port 1 capture
Cat6509(config)#exit
```

NetFlow from the Local Switch as Data Source

NetFlow Data Export records offer an aggregate view of the network. When enabled on the local/remote switch, the NetFlow data source becomes available on the NAM without the need to create any SPAN sessions. All traffic that is Layer 3-switched on the Cisco Catalyst 6500 Series Policy Feature Card and all traffic that is NetFlow-switched on the Cisco Catalyst 6500 Series Multilayer Switch Feature Card are available as NDE for monitoring. With NetFlow available as a data source, the NAM can provide information such as hosts and conversations, applications, and so on directly from the Cisco NAM's application or other third-party tools.

NDE records offer broader traffic monitoring capacity, because this data source is available (once enabled from the switch) without creating any SPAN sessions to the NAM. NetFlow data can also be obtained from remote switches/routers. The Cisco NAM can get detailed information on the packets through the NDE records without having to examine each packet, and hence more traffic can be analyzed. However, NetFlow only gives statistics for applications, hosts, and conversations. Detailed monitoring for voice, VLAN, IAP, DiffServ, and packet captures and decodes are not available with NetFlow.

The Cisco NAM-1/NAM-2 supports monitoring with both SPAN and NetFlow using independent backplane interfaces. These two data sources complement each other to provide a very powerful and comprehensive monitoring solution. Use NetFlow to monitor the traffic at an aggregate level to obtain application, host, and conversation statistics. For detailed examination, use SPAN to send the traffic of interest to the NAM.

Note: Cisco NAM-1/NAM-2 supports NetFlow versions 1, 5, 6, 7, 8, 9, and v8 aggregation caches.

Configuring NetFlow from the Catalyst 6500 Card

To configure NetFlow from the Cisco Catalyst 6500 Series Multilayer Switch Feature Card, follow these steps in configuration mode (Cisco IOS Software):

Step 1. Select an interface for turning on routed flow cache.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

Step 2. Select the NetFlow version.

```
Router(config)# ip flow-export version version-number
```

Step 3. Enable the routed flows cache on an interface.

```
Router(config-if)# interface interface-specific
Router(config-if)# ip address address mask
Router(config-if)# ip route-cache flow
```

Step 4. Export the NetFlow packets to the NAM User Datagram Protocol (UDP) port 3000.

```
Router(config)# ip flow-export destination NAM-Address 3000
```

Step 5. Verify the NetFlow flows.

```
Router# show ip cache flow
Router# show ip flow export
```

To configure NetFlow from the Cisco Catalyst 6500 Series Policy Feature Card (multilayer switching cache), follow these steps in configuration mode:

Step 1. Enter configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

Step 2. Select the version of NetFlow.

```
Router(config)# mls nde sender version version-number
```

Note: Cisco NAM-1/NAM-2 supports NetFlow versions 1, 5, 6, 7, 8, and v8 aggregation caches.

Step 3. Select the NetFlow flow mask.

```
Router(config)# mls flow ip [interface-full | full]
```

Note: Flow mask “full” is required to include additional details of collection data.

Step 4. Enable NetFlow export.

```
Router(config)# mls nde sender
```

Step 5. Export NetFlow packets to the NAM UDP port 3000.

```
Router(config)# ip flow-export destination NAM-Address 3000
```

NetFlow from a Remote Device as a Data Source

In addition to providing comprehensive LAN traffic analysis, the Cisco NAM can also provide detailed traffic analysis for WAN interfaces by enabling NDE on those devices. The following are configuration examples for enabling NetFlow on Cisco IOS routers.

Note: Cisco recommends that the remote NetFlow devices be within near network proximity of the Cisco NAMs. Additionally, limit NetFlow traffic across the WAN.

NetFlow Configurations for Cisco IOS Software

To configure NetFlow for Cisco IOS Software, follow these steps:

Step 1. Configure NetFlow.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# interface type slot/port
```

Step 2. Enable NetFlow for the interface.

```
Router(config)# ip route-cache flow
```

Step 3. Export the routed flow cache entries to the NAM UDP port 3000.

```
Router(config)# ip flow-export destination NAM-address 3000
```

Note: The UDP port number must be set at 3000.

When you configure a Cisco NAM as a NetFlow collector, you should use the IP address of the Cisco NAM (set up by sessioning into the NAM).

This example shows how to set up a basic NetFlow configuration:

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# interface vlan 2
Router(config)# ip route-cache flow
Router(config)# ip flow-export destination 172.20.104.74 3000
Router(config)# exit
```

Enabling NetFlow Data Sources Through the Cisco NAM GUI

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

Step 1. From Setup > Data Sources > NetFlow > Listening Mode, click Start.

This allows the Cisco NAM to listen to any NetFlow packets being sent to it (see Figure 26).

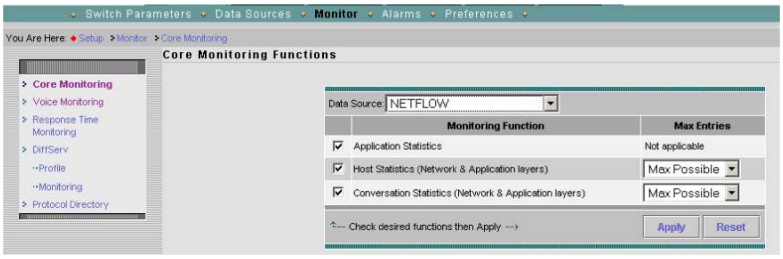
Step 2. When you see the IP address or addresses, select and add the device or devices, and provide the SNMP read community string.

Step 3. Test for connectivity and the SNMP community string from Setup > Data Sources > NetFlow Devices, then click Test.

Figure 26. Adding NetFlow-Enabled Monitoring Devices

Step 4. Next, go to Setup > Monitor > Core Monitoring and select the desired devices with a prefix NDE as the NetFlow data source and enable the collections (see Figure 27).

Figure 27. Enabling NetFlow Data Collection Using the Cisco NAM GUI



Backup

DiffServ: This screen breaks down monitored traffic by the value of the DSCP field in the header. The table provided allows you to determine what proportion of the traffic uses DSCP0, what proportion uses DSCP1, and so on. When applications with differing QoS needs share the network, it is imperative to provide superior resources to business-critical applications that have special bandwidth and latency requirements. These screens help drive your analysis. Note that this screen has alternate views. For example, you can configure DSCP4 to be voice traffic; all future traffic on DSCP4 will be profiled as voice traffic, enabling you to trend voice traffic in your network.

URL Monitoring: NAM's URL monitoring feature helps calculate the number of hits received by a particular URL (a specific file). If multiple URLs are located behind one IP address, it is useful to know if one URL was hit much more than the other. A good example is that of a movie theater that wishes to determine which of its movies was receiving the most interest from its weekend audience (based on number of hits).

TCP/UDP port table: In addition to the ability to break down traffic usage by protocol, NAM also provides traffic usage per protocol per Layer 4 port. This view is very useful to analyze popular protocols such as FTP, HTTP, and so on. Also, if you are concerned about excessive usage of recreational traffic, such as bittorrent, it is easy to determine current usage levels of this protocol. Note that NAM provides the ability to add home-grown protocols (or any protocol that is not already listed) in the protocol directory.

Switching data sources using the drop-down menu: Notice that all real-time screens have a drop-down menu that allows you to switch from a SPAN data source to a NetFlow data source. With NAM 4.0, the software supports WAAS data sources as well. It is often useful to compare the output of one data source with that of another. Familiarize yourself with the different sources of data and the information that you can glean from each. Notice that data sources that provide full packet streams (for example, SPAN) are the ones that provide capture capabilities, response time measurements, and voice quality analysis. In contrast, a NetFlow data source cannot provide these metrics, and only provides more basic information about host statistics, conversation statistics, and so on.

Viewing options, including current rates, cumulative rates, and Top N charts: Many screens on the NAM GUI provide these options. The "Current rates" option, which is set by default, provides live information. The "Cumulative rates" option provides information that has accumulated since the NAM booted up. The top N chart provides a pictorial view of the data, whereas the tabular format provides more quantitative details. Note that you can directly start a historical report from any of the live monitoring screens. Simply click a host or application or conversation of interest, and then click the Report button at the bottom of the screen.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-505273-02 09/10