

Troubleshooting with Network Analysis Module

Introduction

The Cisco® Network Analysis Module (NAM) provides visibility into how the network is performing and how users experience the applications and services delivered over the network.

NAM delivers granular traffic analysis, rich application performance measurements, comprehensive voice quality monitoring, and deep insightful packet captures to help improve network performance.

Cisco NAM is available in an integrated services module and virtual blade and appliance form factors to address diverse monitoring needs throughout the Cisco network: the data center, the branch, the campus core, aggregation, and even closet locations. All form factors support the latest software version 4.2.

Cisco NAM leverages the instrumentation in Cisco IOS® Software such as Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), Encapsulated Remote SPAN (ERSPAN), NetFlow Data Export (NDE), Remote Monitoring (RMON), and network-based application recognition as the data source.

The following sections will cover proactive alert configurations and troubleshooting steps for application performance; host, conversation, and interface utilization; Differentiated Services (DiffServ); and voice issues.

Alerting and Troubleshooting with NAM

With Cisco NAM deployed in different places in the network collecting and analyzing the network traffic, it becomes a very valuable tool for alerting and troubleshooting issues. NAM can be configured with thresholds to trigger alerts and capture packets when the thresholds are exceeded.

Intelligent Application Performance

Intelligent application performance (IAP) monitoring is a key feature that NAM provides: an ability to measure the response time of transactions between the client and server.

The IAP toolkit is powerful, providing 45 metrics into application response times and network latency. Becoming familiar with the metrics that are important to your network will provide significant benefits in helping manage your network performance. The metrics can be found in Table 4-40 in the NAM user guide at http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.1/user/guide/monitor.html#wp1046620.

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.

IAP technology allows NAM to break down the total response time into its component pieces: the application server portion of the delay and the network portion of the delay. IAP analysis will identify the delays users are experiencing accessing the applications on the server.

Scenario: A NAM is deployed at the data center (NAM-2 blade or 2200 appliance) closest to the servers. The administrator needs to trend over time the HTTP response time from the **servers'** perspective. Based on those trends, administrators can configure alarm alerts and thresholds and capture and troubleshoot a response time issue when an alert is received. The Server Average Response Time variable will be used for this scenario. However, thresholds based on other variables can be configured for your environment.

Use Case: Detecting Abnormal Response Times and Troubleshooting Using NAM

Once the network is in a steady state (for example, network metrics such as response time, bandwidth utilization, and so on are all within acceptable limits), NAM can monitor for deviation from the norm. If such a deviation occurs, the system raises an alarm, packet capture is executed, and subsequent actions can be taken, for example, viewing the application response time table to identify the application and hosts having issues.

Configuration

Set up thresholds on the NAM, which when exceeded will generate an alarm. Set up relevant actions to be performed under threshold conditions (for example, send email, traps, or logs). Packet capture can also be initiated by the alarm.

Refer to the NAM 4.2 user guide for detailed instructions for configuring thresholds and alarms at http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.2/user/guide/nam42 Ug.html.

Abnormal Behavior Seen in Data Center Server Farm

Use response time measurements to identify which server displays abnormal response times.

If Server Y is identified, monitor response times between Y and each host that sends traffic to Y.

If response times are high uniformly for all hosts, it could be a server issue. If response times are high for one particular subnet or host, use other NAM monitoring features to identify the root cause. This can be done by looking at managed device interface/port utilization - see if there are any spikes; top hosts - which host is utilizing the bandwidth; and top conversations - which server client pairs are causing issues. See Figure 1.

Figure 1. Server Application Response Time

Server Application Responses
 Latest Data: 300 second interval ending Mon 19 Jul 2010, 14:50:35 PDT
☒ Auto Refresh

☒ All Data ☐ TopN Chart

Data Source: DATA PORT 2 Server: Filter

Showing 1-15 of 36 records

#	Server	App	# of Clients	# of Responses	Application Delay (ms)			Network Delay (ms)			Total Delay (ms)		
					Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
<input type="radio"/>	1. 128.107.241.169	http	1	1	502	502	502	1	4	14	506	506	516
<input type="radio"/>	2. 192.168.137.82	http	1	8	2	161	355	0	0	0	2	161	355
<input type="radio"/>	3. 192.168.137.25	laplink-pcsync-secure	1	14	0	114	619	0	0	1	114	620	
<input type="radio"/>	4. 192.168.137.4	https	1	3	1	87	259	0	0	0	1	87	259
<input type="radio"/>	5. 192.168.140.21	laplink-pcsync-secure	1	29	0	71	285	0	0	1	0	71	286
<input type="radio"/>	6. 171.70.146.23	http	1	1	61	61	61	1	1	1	62	62	62
<input type="radio"/>	7. 171.70.145.48	http	1	1	53	53	53	1	1	1	54	54	54
<input type="radio"/>	8. 192.168.154.21	https	1	78	1	38	120	-	-	-	-	-	-
<input type="radio"/>	9. 172.25.109.73	laplink-pcsync-secure	1	73	0	34	333	0	2	8	2	36	341
<input type="radio"/>	10. 192.168.76.114	laplink-pcsync-secure	1	29	0	34	130	0	1	1	1	35	131
<input type="radio"/>	11. 192.168.140.136	https	1	3	0	29	63	0	0	0	0	29	63
<input type="radio"/>	12. 192.168.140.19	https	1	8	1	20	152	0	0	0	1	20	152
<input type="radio"/>	13. 192.168.137.25	https	1	22	0	9	61	0	3	28	3	12	89
<input type="radio"/>	14. 192.168.140.83	http	1	13	0	7	77	0	0	0	0	7	77
<input type="radio"/>	15. 192.168.140.138	http	2	6	0	5	25	0	0	0	0	5	25

Hosts, Conversations, and Interfaces

Host, conversation, and interface monitoring provides bandwidth consumption for those items. The bandwidth consumption can help identify bottlenecks before the users complain about network performance and availability. Using the same scenario stated above and following similar steps, the administrator can view the host, conversation, and interface statistics tables to identify high-bandwidth consumers such as servers in the data center and which clients are accessing those servers. Once those are known, reports can be configured to trend the bandwidth consumption for a period of time. Based on the trends for the top talkers, thresholds can be configured to trigger alerts and packet captures. Packet capture is not available for triggers from interface bandwidth threshold violations.

Use Case: Top N Applications, Hosts, and Conversations and Traffic Trends

Once the network is in a steady state (for example, network metrics such as top talkers, bandwidth utilization, and so on are all within acceptable limits), NAM can monitor for deviation from the norm. If such a deviation occurs, the system raises an alarm, a trap or syslog is sent, and packet capture is started.

Configuration

Set up thresholds on the NAM, which when exceeded will generate an alarm. Set up relevant actions such as send email, traps, or logs and start packet capture to decode during troubleshooting to identify the cause of the alarm.

Abnormal Behavior Seen in Application/Host/Conversation Traffic

Use core monitoring traffic analysis measurements and reports for applications, hosts, and conversations to identify potential issues, for example, hosts or conversations hoarding bandwidth, an unknown host being listed, unknown applications, and so on. View the monitoring screens and reports to find when the abnormal behavior occurred.

Figures 2, 3, and 4 show the monitoring screens for hosts, conversations, and interface statistics, respectively.

Figure 2. Network Hosts

Network Hosts
 Per-Second Data: as of Fri 19 Feb 2010, 13:12:56 PST
☒ Auto Refresh

Current Rates | TopN Chart | Cumulative Data

Data Source: ALL SPAN | Address: | Filter | Clear

Showing 1-15 of 389 records

#	Address	Via	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	Non-Unicast/s
1	192.168.137.73	ip	159.73	159.97	11,820.27	33,245.87	34%
2	192.168.156.146	ip	159.97	159.73	33,245.87	11,820.27	12%
3	192.168.140.21	ip	5.13	11.13	679.92	9,149.30	9%
4	192.168.159.36	ip	7.95	11.25	1,528.22	6,650.22	6%
5	171.70.145.46	ip	0.02	3.87	1.07	5,337.78	5%
6	192.168.139.21	ip	39.33	32.85	22,440.57	5,071.08	5%
7	192.168.137.25	ip	5.60	6.20	734.23	4,457.13	4%
8	192.168.139.56	ip	12.95	15.35	3,985.92	3,942.00	4%
9	171.70.145.48	ip	0.00	3.08	0.00	3,645.35	3%
10	192.168.140.19	ip	20.22	14.13	2,532.97	3,217.23	3%
11	192.168.140.83	ip	15.63	18.20	2,580.57	2,817.60	2%
12	192.168.137.118	ip	4.75	7.77	1,522.12	2,817.00	2%
13	192.168.139.11	ip	14.72	13.23	2,329.83	2,008.83	2%
14	192.168.137.102	ip	8.87	8.73	1,536.82	1,549.80	1%
15	192.168.137.46	ip	3.00	3.00	361.23	1,547.07	1%

Rows per page: 15 | Units: Bytes/s | Go to page: 1 of 26

Select an item then take an action --> | Details | Capture | Real-Time | Report

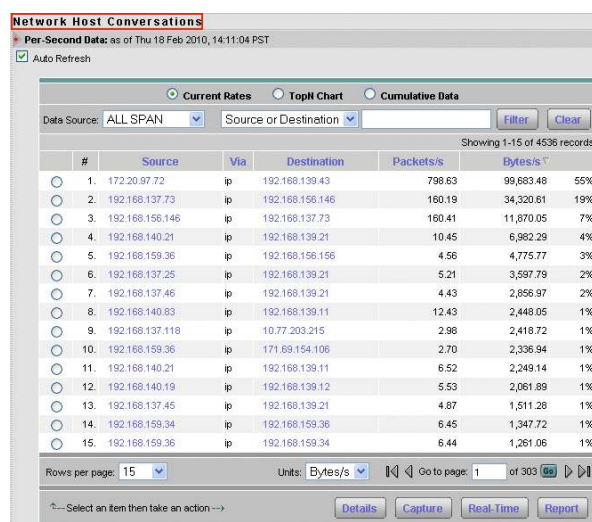
Figure 3. Network Host Conversations

Figure 3 displays the host-conversation pairs. Clicking the IP address will display the host details with to and from protocol information.

Use Case: Managed Device - Interface Utilization

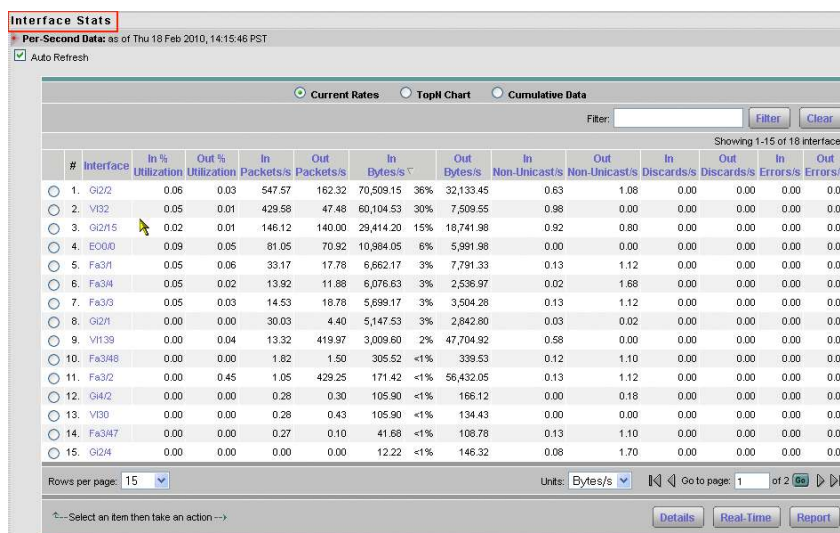
Once the network is in a steady state (for example, interface utilization is all within acceptable limits), NAM can monitor for deviation from the norm. If such a deviation occurs, the system raises an alarm, and subsequent action is taken.

Configuration

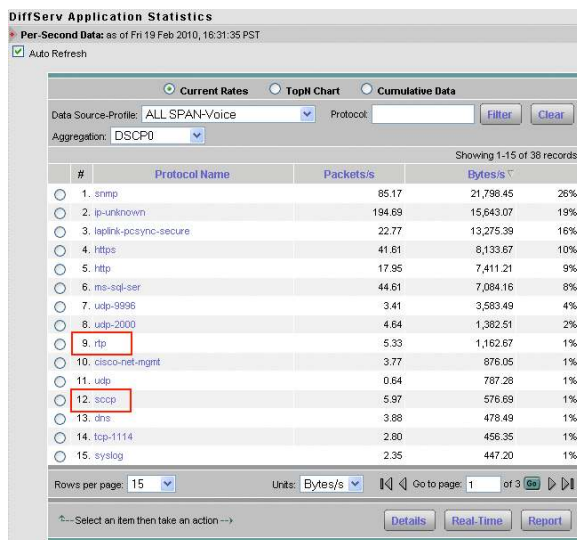
Set up thresholds on the NAM, which when exceeded will generate an alarm. Set up relevant actions such as send email, traps, or logs and start packet capture to decode during troubleshooting to identify the cause of the alarm.

Abnormal Behavior Seen in Interface Traffic

Use managed device interface utilization measurements and reports to identify potential application performance issues, for example, high utilization on the interfaces. View the monitoring screens and reports to find when the abnormal behavior occurred. See Figure 4.

Figure 4. Interface Statistics**Differentiated Services Code Point**

DiffServ provides insight into how the traffic is being classified by quality of service (QoS) and detects incorrectly marked or unauthorized traffic. NAM identifies the application or protocol based on the type of service (ToS) bits setting. The administrator must configure DiffServ profiles based on templates provided or create one. The voice template can be used to monitor whether voice traffic is marked properly. Figure 5 displays the DiffServ application statistics for DSCP value 0. Looking at this you'll notice Real-Time Transport Protocol (RTP) and Skinny Client Control Protocol (SCCP) in the list, which indicates that they are not being correctly marked throughout their path.

Figure 5. DiffServ Application Statistics

Clicking rtp or scdp will display the clients using those protocols and help in troubleshooting why RTP or SCCP traffic from these clients is not marked correctly (Figure 6). Review the QoS policy implemented on the routers and or switches between the clients.

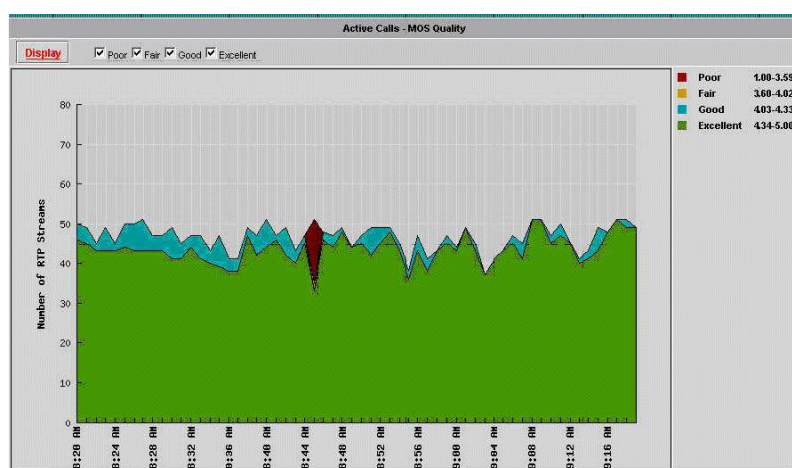
Figure 6. Application Conversations

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

Voice Quality

Use Case: Troubleshooting Voice Quality Degradation

Consider a situation in which the network administrator learns about problems with voice-over-IP (VoIP) quality by monitoring the NAM GUI. What steps could the administrator follow to isolate the problem's root cause?

Figure 7. Active Calls - MOS Quality

As illustrated in Figure 7, NAM classifies the voice calls by quality into poor, fair, good, and excellent categories. This rating is based on Mean Opinion Scores (MOSs) and can be configured by the user to suit the network's sensitivity levels. NAM uses preset default values for the MOS ranges. The chart indicates that there were a few calls with poor quality a few minutes ago.

Figure 8. RTP Streams Traffic

RTP Stream Traffic										
Current Data: as of Thu 09 Oct 2008, 09:31:21 UTC										
<input type="checkbox"/> Auto Refresh										
Source Address										
#	Source Addr : Port	Dest Addr : Port	Payload Type	SSRC	Pkt Loss (million)	MOS	Avd Pkt Loss (%)	Jitter (ms)	SSC	
1	10.14.1.2 : 1280	10.14.1.20 : 1250	G711Ulaw_64k	34933	40.00	1.76	40.00	0.05	60.0	
2	10.14.1.2 : 1296	10.14.1.20 : 24614	G711Ulaw_64k	27379	40.00	1.76	40.00	0.06	60.0	
3	10.14.1.2 : 1494	10.14.1.20 : 6374	G711Ulaw_64k	54306	40.00	1.76	40.00	0.06	60.0	
4	10.14.1.2 : 1730	10.14.1.20 : 54846	G711Ulaw_64k	1750	40.00	1.76	40.00	0.06	60.0	

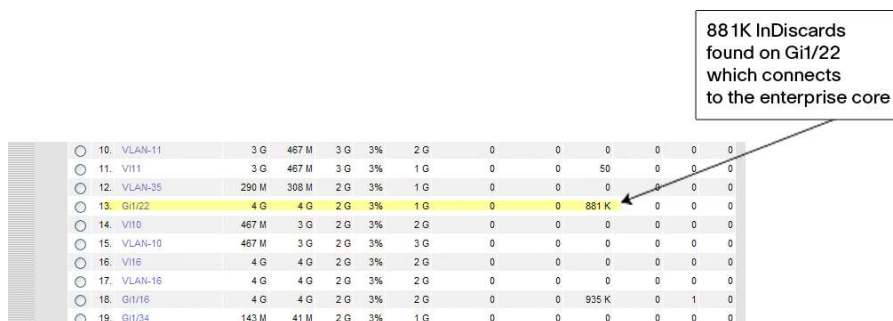
In response to this problem, the next step in troubleshooting is to navigate to obtain more detail about poor calls. Figure 8 shows the individual RTP streams and the MOS values associated with them. As indicated in the highlighted portion of the table in Figure 8, the MOS of the first several calls is very low (1.76) as per the ranges defined in the foregoing chart.

There are other interesting clues that can be gleaned from Figure 8. Note that the Packet Loss column indicates that VoIP streams are experiencing packet loss.

The next step is to get clues as to where packets are being dropped. The source address of the RTP stream should be examined. All calls have the source IP address 10.14.1.2 but with different port numbers. This is typical of a

conferencing system that uses different port numbers for different streams. By looking up the network topology diagram, we learn that 10.14.1.2 is located in Building 3 of the main campus of the company. The topology also indicates that there is a NAM at the edge router for Building 3. We log in to that NAM looking for clues on where packets might be getting dropped.

Figure 9. Interface Statistics



10.	VLAN-11	3 G	467 M	3 G	3%	2 G	0	0	0	0	0	0	0	0	0	0
11.	VII1	3 G	467 M	3 G	3%	1 G	0	0	50	0	0	0	0	0	0	0
12.	VLAN-35	290 M	308 M	2 G	3%	1 G	0	0	0	0	0	0	0	0	0	0
13.	Gi1/22	4 G	4 G	2 G	3%	1 G	0	0	0	881 K	0	0	0	0	0	0
14.	VII10	467 M	3 G	2 G	3%	2 G	0	0	0	0	0	0	0	0	0	0
15.	VLAN-10	467 M	3 G	2 G	3%	3 G	0	0	0	0	0	0	0	0	0	0
16.	VII16	4 G	4 G	2 G	3%	2 G	0	0	0	0	0	0	0	0	0	0
17.	VLAN-16	4 G	4 G	2 G	3%	2 G	0	0	0	0	0	0	0	0	0	0
18.	Gi1/16	4 G	4 G	2 G	3%	2 G	0	0	935 K	0	1	0	0	0	0	0
19.	Gi1/24	143 M	41 M	2 G	3%	1 G	0	0	0	0	0	0	0	0	0	0

By navigating to the Interface statistics screen that provides details about packet-related statistics (Figure 9), we find that Gi1/22, the interface that connects to the core of the campus network, is experiencing serious packet loss.

As this interface serves all traffic going from and to Building 3 and the rest of the campus, including voice traffic, this is most likely the root cause for packet drops on the RTP stream. The problem in this case was found to be a hardware defect on the line card that affected the interface. Replacing the card fixed the issue.

This troubleshooting workflow highlights some of the VoIP quality monitoring capabilities and also shows how VoIP features can be used in combination with other traffic monitoring features on the NAM. In this particular case, we used interface statistics monitoring in the NAM in Building 3 to isolate the root cause of the problem.

Summary

This document provides use cases for configuring alarm alerts and thresholds and for troubleshooting the alarm once received. The alarm is generated when the baseline threshold configured is exceeded. The alert can be configured for notification by email, log, trap, or all three. The scenarios covered application performance, hosts, conversations, interface utilization, DiffServ, and voice.

NAM is able to collect and analyze information from various data sources, such as, SPAN (including RSPAN and ERSPAN), NetFlow, and the embedded instrumentation on WAN Acceleration Engine (WAE) to provide insights into the different stages in the network. The NAM's real-time monitoring, historical reporting, and application performance analytics can be used to gain visibility into optimization opportunities, baselining application performance, understanding the impact of WAN optimization, and ongoing troubleshooting across the network.



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)