Traffic and Performance Visibility for Cisco Live 2010, Barcelona

Background

Cisco® Live is Cisco's annual premier education and training event for IT, networking, and communications professionals. Cisco Live 2010, Barcelona was held at the Centre Convencions Internacional Barcelona from January 26 to January 28 with a total attendance of more than 3,000 people.

Challenge

Unlike a traditional corporate network, the Cisco Live network is built up and fully operational in a matter of days. The Cisco Live network offers many advanced services including Cisco TelePresence™, video surveillance, IPv6, and voice over IP. The network provides connectivity for the various Cisco and partner technology demonstrations, labs, streaming video of the technical sessions, and wireless access for all the attendees. With so many activities dependent on the network, the availability, reliability, and performance of the network are crucial to the success of the event. Hence, from a network operations perspective, visibility into network usage and performance are critical.

Solution

Cisco® Network Analysis Module (NAM) SVC-NAM-2 service module running version 4.1 software was installed in the core Cisco Catalyst® 6500 Series Switch to deliver granular traffic analysis, rich application performance measurements, comprehensive voice quality monitoring, and deep insightful packet captures to help monitor and troubleshoot network performance.

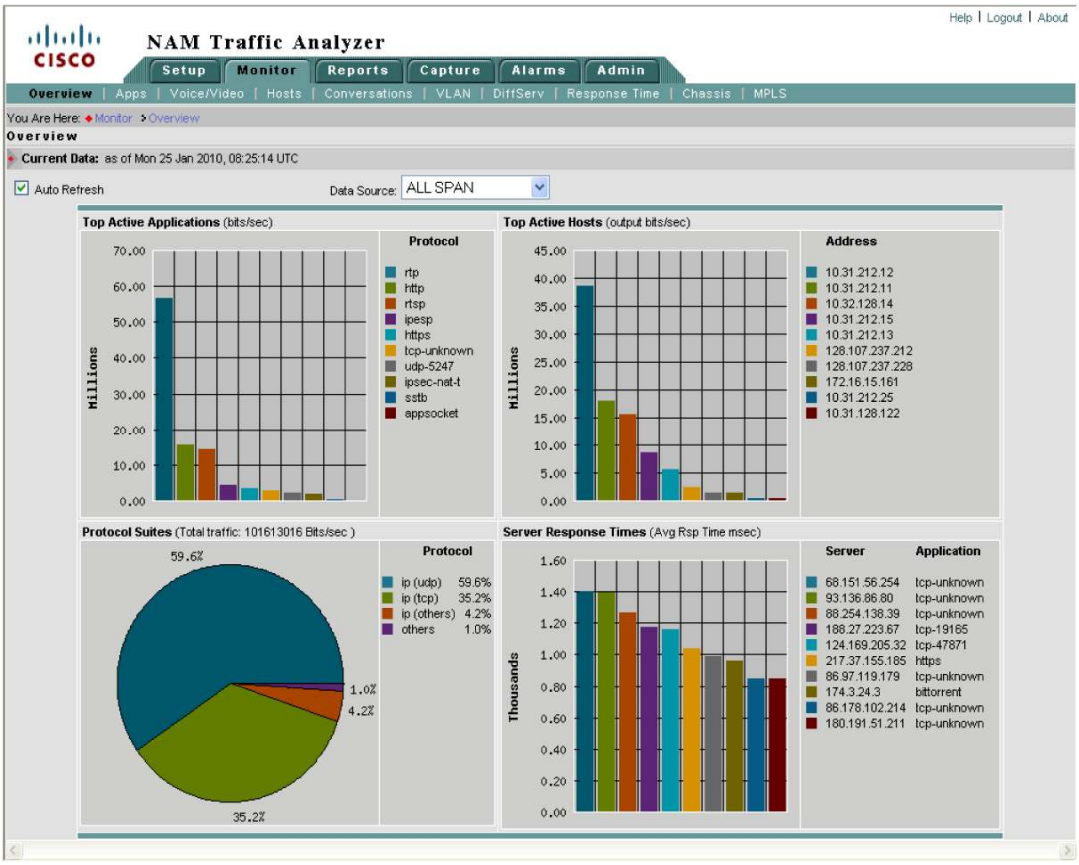
Cisco NAM Setup

The Cisco Live network had 42 VLANs configured. There were different VLANs for users, partners, demonstrations, labs, voice, wireless, management, and so on. Traffic from all 42 VLANs with a total of about 300 Mbps was set up to connect to the NAM using Switch Point Analyzer (SPAN) for analysis using the integrated data source configuration menu available in the NAM web-based graphical user interface (GUI). Various monitoring capabilities, such as core monitoring, voice and RTP steam monitoring, response time monitoring, Differentiated Services (DiffServ) monitoring, URL monitoring, and chassis parameters (switch health and port statistics) monitoring was enabled on the NAM. All this setup took less than 10 minutes and made the NAM ready to begin monitoring the network.

Traffic Analysis with Cisco NAM

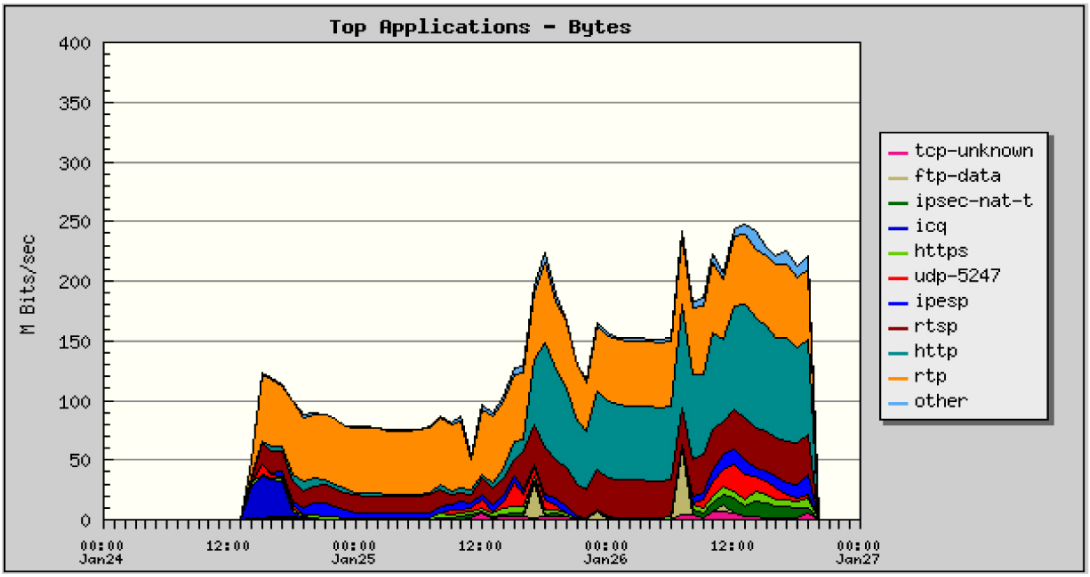
The NAM overview screen provided a real-time view into who was using the network, which applications they were using, and how much network resources were being consumed. An initial look at the NAM traffic overview screen indicated that RTP, HTTP, and RTSP traffic was consuming the most bandwidth in the network core. Additionally the most active hosts in the network were identified as belonging to the 10.31.x.x and 10.32.x.x subnets, which included the servers hosting the Cisco Live content (Figure 1).

Figure 1. NAM Traffic Overview



Apart from looking at the traffic mix and top talkers in real time, predefined top-N historical reports revealed the network usage pattern though the course of the event. A peak usage of about 250 Mbps was observed (Figure 2).

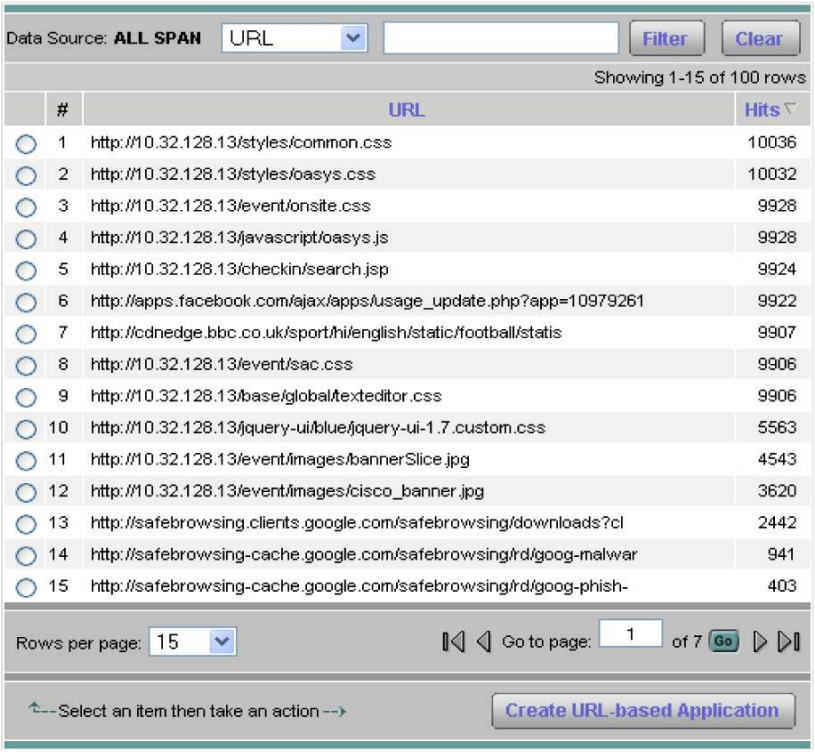
Figure 2. Top-N Applications Over Time



URL Monitoring

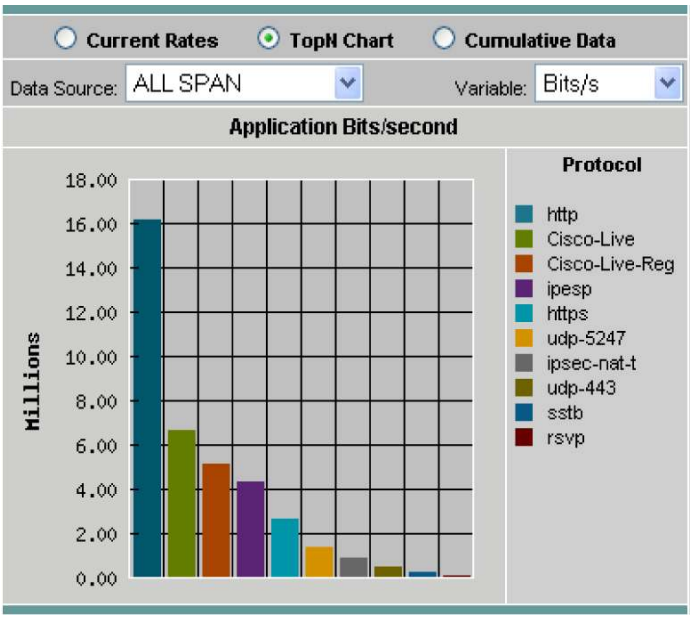
To get a deeper look at the HTTP traffic, Monitor > Apps > URLs was selected and the URLs were sorted by maximum hits. As expected the Cisco Live content and registration servers had the most hits due to people checking into the event as well as searching for sessions and viewing online content (Figure 3). To track this usage more accurately, URL-based applications were created for Cisco Live and Cisco Live Registration URLs (Figure 4). Additionally, as observed, the next most popular websites were Facebook and BBC for football scores. A URL-based application was created for Facebook as well to track bandwidth utilization.

Figure 3. Cisco NAM URL Monitoring



#	URL	Hits
1	http://10.32.128.13/styles/common.css	10036
2	http://10.32.128.13/styles/oasys.css	10032
3	http://10.32.128.13/event/onsite.css	9928
4	http://10.32.128.13/javascript/oasys.js	9928
5	http://10.32.128.13/checkin/search.jsp	9924
6	http://apps.facebook.com/ajax/apps/usage_update.php?app=10979261	9922
7	http://cdnedge.bbc.co.uk/sport/hi/english/static/football/statis	9907
8	http://10.32.128.13/event/sac.css	9906
9	http://10.32.128.13/base/global/texteditor.css	9906
10	http://10.32.128.13/jquery-ui/blue/jquery-ui-1.7.custom.css	5563
11	http://10.32.128.13/event/images/bannerSlice.jpg	4543
12	http://10.32.128.13/event/images/cisco_banner.jpg	3620
13	http://safebrowsing.clients.google.com/safebrowsing/downloads?cl	2442
14	http://safebrowsing-cache.google.com/safebrowsing/rd/goog-malwar	941
15	http://safebrowsing-cache.google.com/safebrowsing/rd/goog-phish-	403

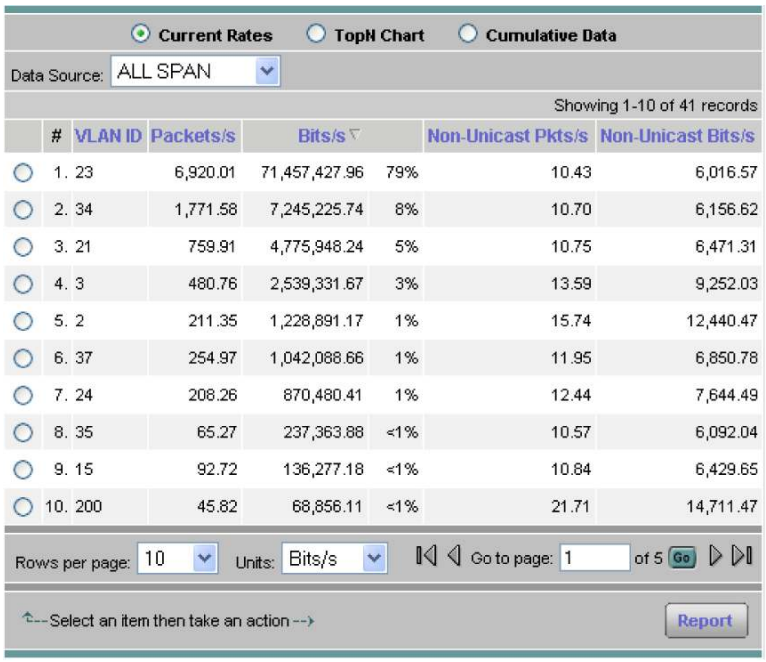
Figure 4. Cisco NAM URL-Based Applications



VLAN Monitoring

To gain visibility into traffic volume per VLAN, Monitor > VLAN was selected and the VLANs were sorted by bits/s. VLANs 23 and 34 were the most heavily used VLANs (Figure 5). VLAN 34 was the Cisco Live registration VLAN and VLAN 23 was a demonstration VLAN. To understand the traffic mix for VLAN 23, it was added as a separate data source. The traffic mix revealed that most of the traffic in VLAN 23 was RTP (Figure 6). Looking at the details, the hosts originating the RTP traffic were identified as the video servers streaming in high definition (HD) mode. Thresholds were set in the NAM to alert the network operations center for the event when RTP traffic consumed more than 100 Mbps bandwidth, in which case the operators could request the demonstrations to reduce streaming resolution. Syslog alerts and Simple Network Management Protocol (SNMP) traps were set up to be generated to notify CiscoWorks LAN Management Solution (LMS), which was acting as the centralized fault management system in the event of threshold violation (Figure 7).

Figure 5. VLAN Monitoring

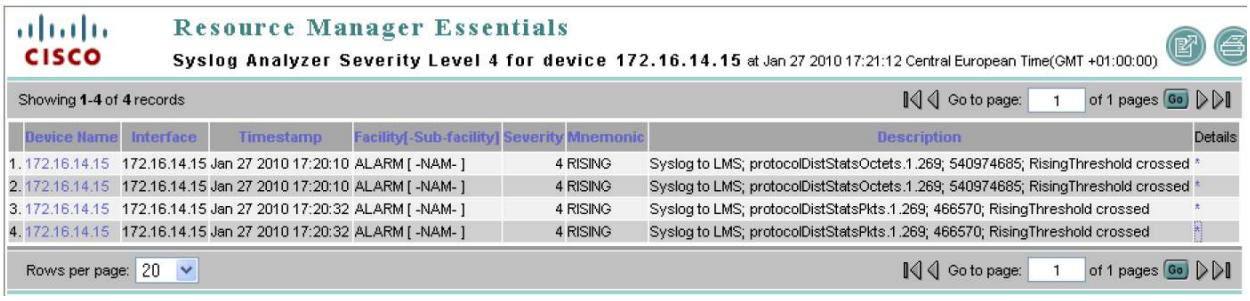


#	VLAN ID	Packets/s	Bits/s		Non-Unicast Pkts/s	Non-Unicast Bits/s
1.	23	6,920.01	71,457,427.96	79%	10.43	6,016.57
2.	34	1,771.58	7,245,225.74	8%	10.70	6,156.62
3.	21	759.91	4,775,948.24	5%	10.75	6,471.31
4.	3	480.76	2,539,331.67	3%	13.59	9,252.03
5.	2	211.35	1,228,891.17	1%	15.74	12,440.47
6.	37	254.97	1,042,088.66	1%	11.95	6,850.78
7.	24	208.26	870,480.41	1%	12.44	7,644.49
8.	35	65.27	237,363.88	<1%	10.57	6,092.04
9.	15	92.72	136,277.18	<1%	10.84	6,429.65
10.	200	45.82	68,856.11	<1%	21.71	14,711.47

Figure 6. Traffic Analysis per VLAN

#	Protocol	Packets/s	Bits/s	
1.	rtp	4,970.77	56,824,065.07	80%
2.	rtsp	1,867.48	13,865,085.75	20%
3.	sstb	10.42	6,003.20	<1%
4.	http	1.27	1,690.31	<1%
5.	arp	0.74	402.96	<1%
6.	ntp	0.06	46.46	<1%

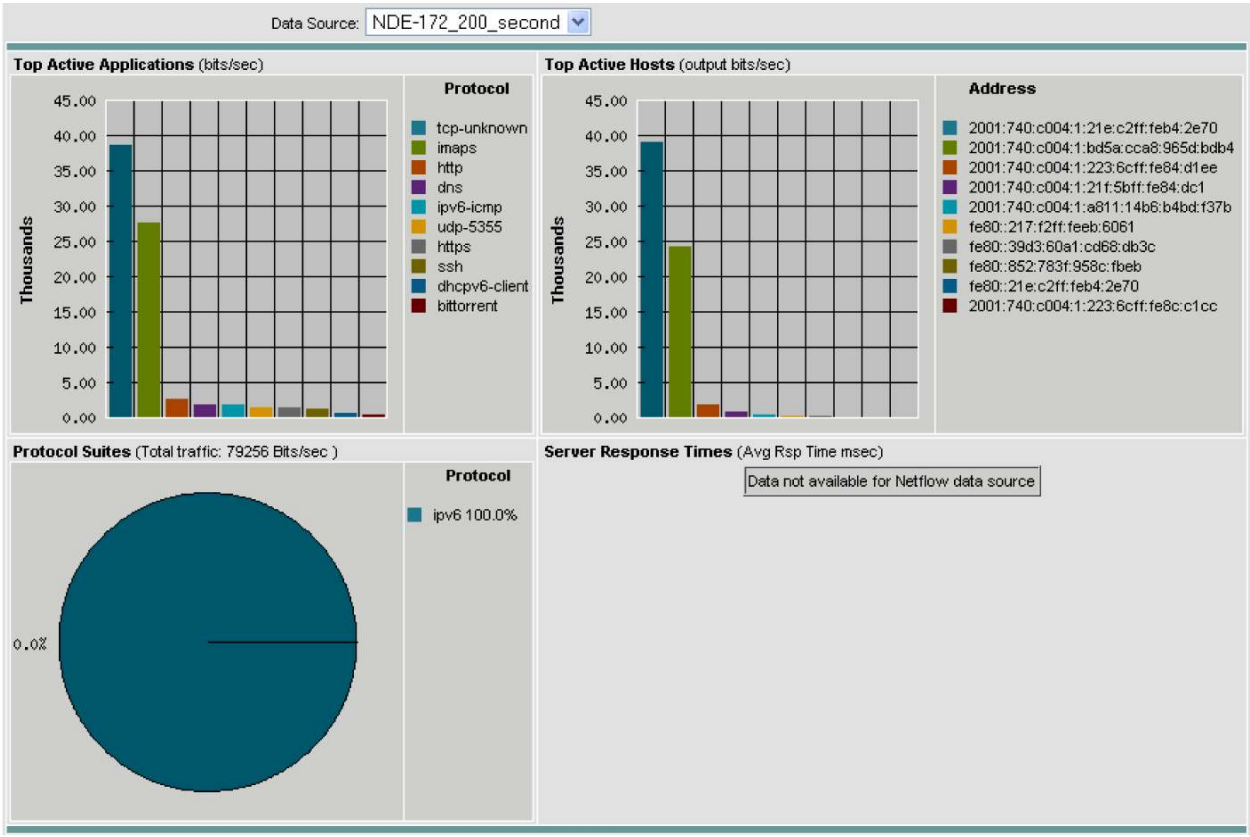
Figure 7. NAM Alert Integration with CiscoWorks LMS



IPv6 NetFlow Monitoring

Although the core of the network at Cisco Live Barcelona ran IPv4, part of the network used IPv6 for demonstrating specific functionality. Remote NetFlow monitoring capability of the NAM was utilized to gain insights into the IPv6 traffic. The remote router was configured to export NetFlow version 9 data to the NAM, so that the NAM could monitor the IPv6 traffic flow (Figure 8).

Figure 8. NAM Monitoring IPv6 NetFlow Version 9 Traffic Records



Application Response Time Monitoring

Cisco NAM can look at TCP client/server messages and determine more than 40 transaction-based statistics, such as application server delay, network delay, transaction time, retransmission delay, and so on, that provide valuable information for monitoring the performance of TCP-based applications. Through traffic analysis, HTTP had been identified as the most heavily used Transmission Control Protocol. Through URL monitoring, the Cisco Live content hosting servers were identified as receiving the highest hits. A look at Monitor > Response Time, sorted by number of clients, further verified this information (Figure 9).

Figure 9. Server Response Time Monitoring

All Data | TopN Chart

Data Source: ALL SPAN | Server | Filter | Clear

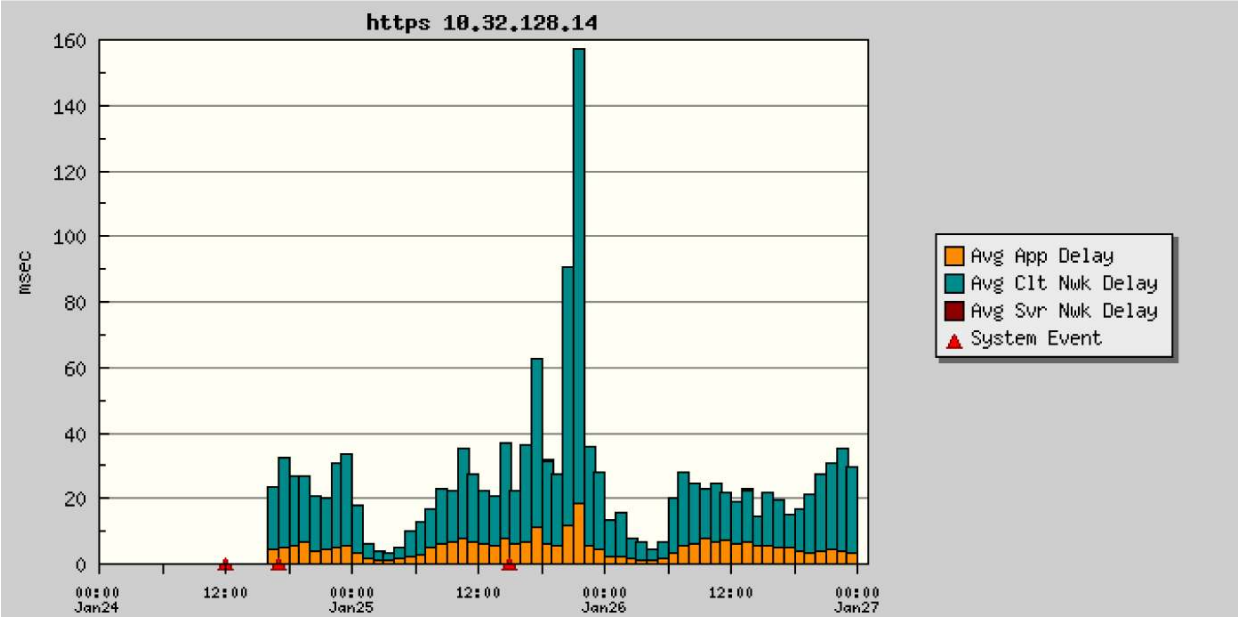
Showing 1-10 of 189 records

#	Server	App	# of Clients	# of Responses	Application Delay (ms)			Network Delay (ms)			Total Delay (ms)		
					Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
1.	10.32.128.14	https	38	1,993	0	**5**	1,380	0	**11**	899	11	**16**	2,279
2.	10.31.180.99	sccp	25	51	0	**0**	1	-	-	-	-	-	-
3.	10.32.128.14	http	24	128	0	**18**	119	0	**21**	198	21	**39**	317
4.	10.32.128.13	http	16	304	0	**2**	44	0	**0**	4	0	**2**	48
5.	68.142.138.15	https	3	11	170	**175**	177	-	-	-	-	-	-
6.	10.31.128.124	nb-unknown	2	13	0	**0**	0	0	**0**	1	0	**0**	1
7.	10.31.132.101	nb-unknown	2	22	0	**0**	1	1	**1**	1	1	**1**	2
8.	10.31.132.109	nb-unknown	2	22	0	**0**	1	0	**0**	1	0	**0**	2
9.	74.125.79.100	http	2	2	0	**3**	6	59	**69**	79	69	**72**	85
10.	80.92.66.130	http	2	3	0	**0**	1	48	**49**	49	49	**49**	50

Rows per page: 10 | Go to page: 1 of 19 Go

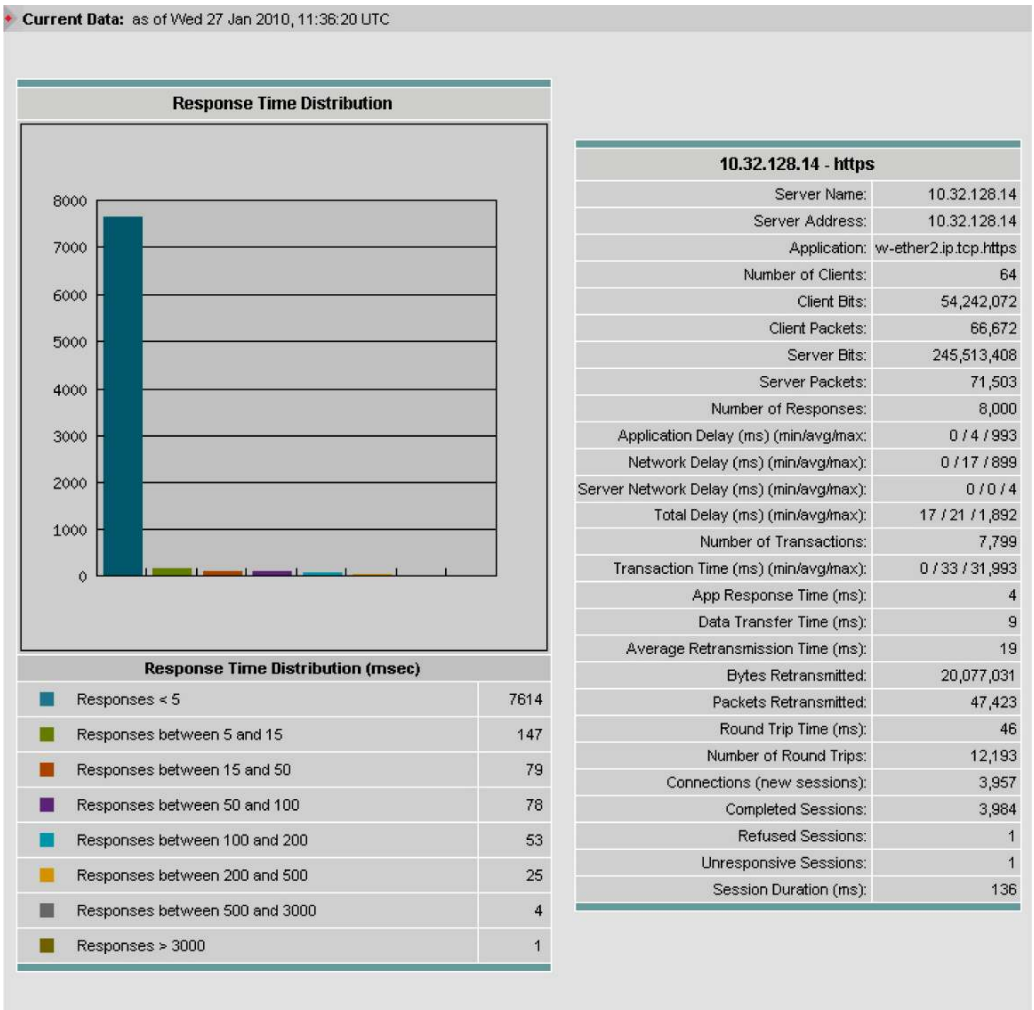
Since the server 10.32.128.14 had the most number of clients, it required more careful monitoring to observe response time trends and catch any performance issues before they started affecting user experience. Historical trending reports for average application delay, average client network delay, and average server network delay were created (Figure 10).

Figure 10. Server Response Time Trending Report



As noted, toward the end of January 25 a network issue affected the response time of the server significantly. The response time, which was averaging around 30 msec, shot up to 160 msec. The time of this corresponded to a power outage on location. A detailed look at the various transaction-based statistics for this server indicated a significant packet drop in the network based on the bytes retransmitted metric (Figure 11).

Figure 11. Detailed Server Response Time Metrics



Response Time Distribution (msec)	
Responses < 5	7614
Responses between 5 and 15	147
Responses between 15 and 50	79
Responses between 50 and 100	78
Responses between 100 and 200	53
Responses between 200 and 500	25
Responses between 500 and 3000	4
Responses > 3000	1

10.32.128.14 - https	
Server Name:	10.32.128.14
Server Address:	10.32.128.14
Application:	w-ether2.ip.tcp.https
Number of Clients:	64
Client Bits:	54,242,072
Client Packets:	66,672
Server Bits:	245,513,408
Server Packets:	71,503
Number of Responses:	8,000
Application Delay (ms) (min/avg/max:	0 / 4 / 993
Network Delay (ms) (min/avg/max):	0 / 17 / 899
Server Network Delay (ms) (min/avg/max):	0 / 0 / 4
Total Delay (ms) (min/avg/max):	17 / 21 / 1,892
Number of Transactions:	7,799
Transaction Time (ms) (min/avg/max):	0 / 33 / 31,993
App Response Time (ms):	4
Data Transfer Time (ms):	9
Average Retransmission Time (ms):	19
Bytes Retransmitted:	20,077,031
Packets Retransmitted:	47,423
Round Trip Time (ms):	46
Number of Round Trips:	12,193
Connections (new sessions):	3,957
Completed Sessions:	3,984
Refused Sessions:	1
Unresponsive Sessions:	1
Session Duration (ms):	136

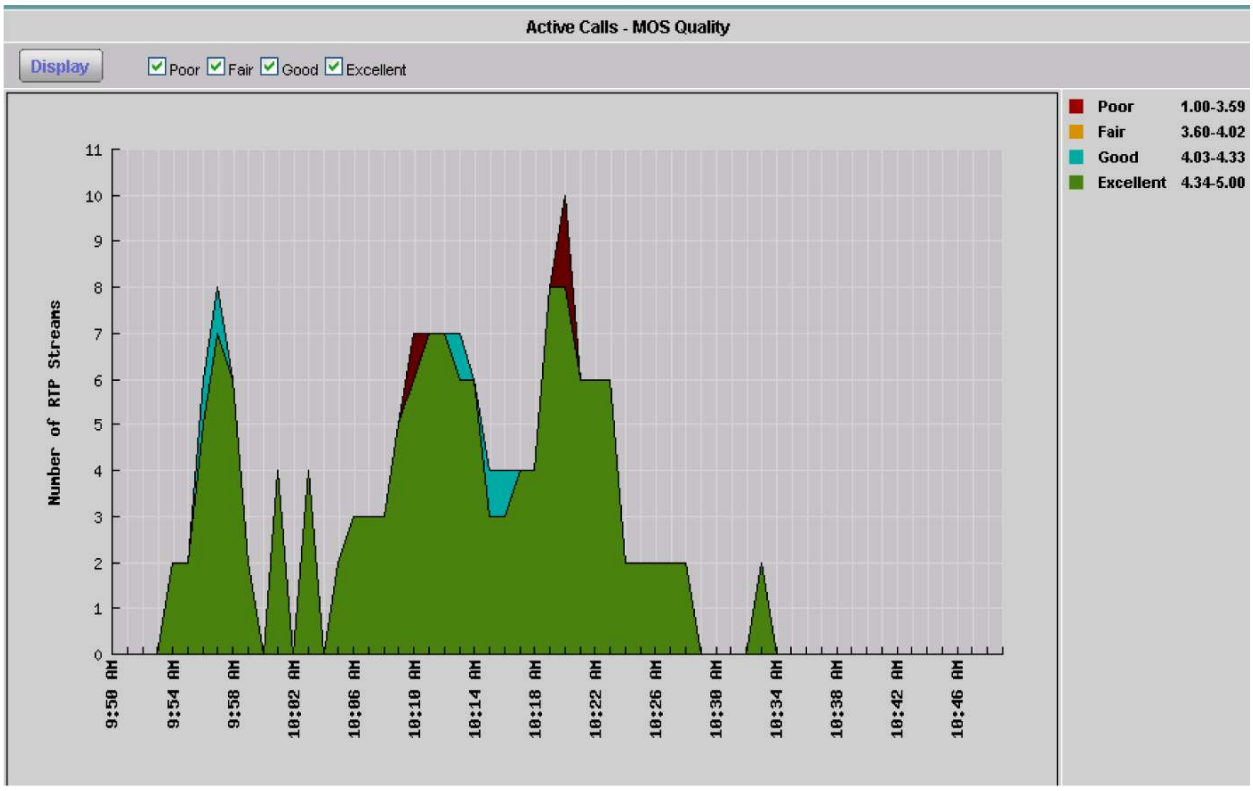
In order to more proactively monitor the server response time, thresholds were set and alerts sent to CiscoWorks LMS.

Voice Quality Monitoring

Cisco NAM provides visibility into the quality of voice calls based on voice signaling protocols as well as RTP stream monitoring. The metrics are calculated every 3 seconds and averaged over a minute for reporting. The metrics include Mean Opinion Score (MOS), packet loss, jitter, seconds of severe concealment, and so on. These metrics are also exported to Cisco Unified Service Monitor for integration into the Cisco Unified Communications Management Suite.

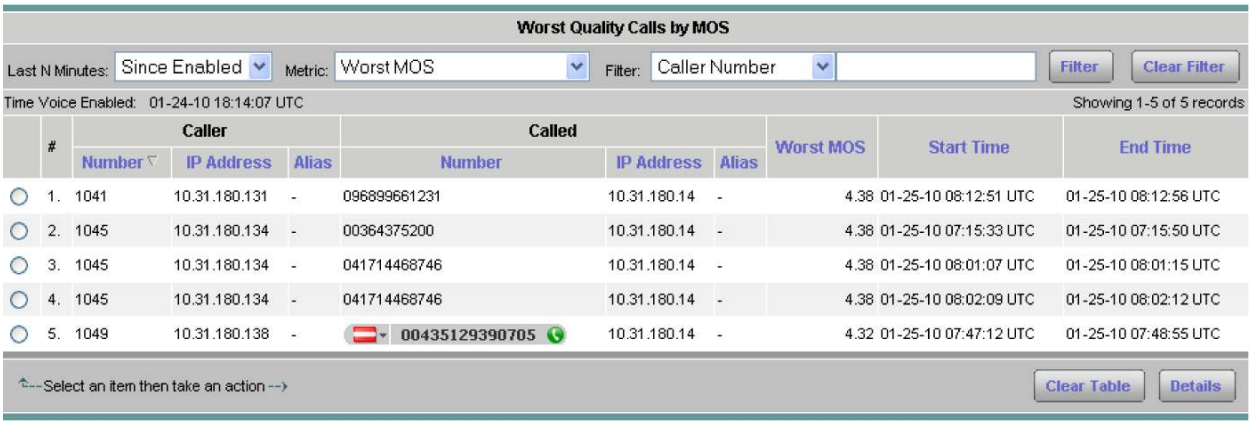
At Cisco Live Barcelona, a number of IP phones were set up in the lobby to help attendees to stay connected. The Cisco NAM was monitoring the voice VLANs and provided real-time visibility into the quality of voice calls (Figure 12).

Figure 12. Voice Quality Monitoring for Active Voice over IP Calls



The NAM also enables a more detailed look at the worst phone calls, the various metrics, as well as start and end times of calls, to help troubleshoot voice quality issues (Figure 13). Note also visibility into Skype calls.

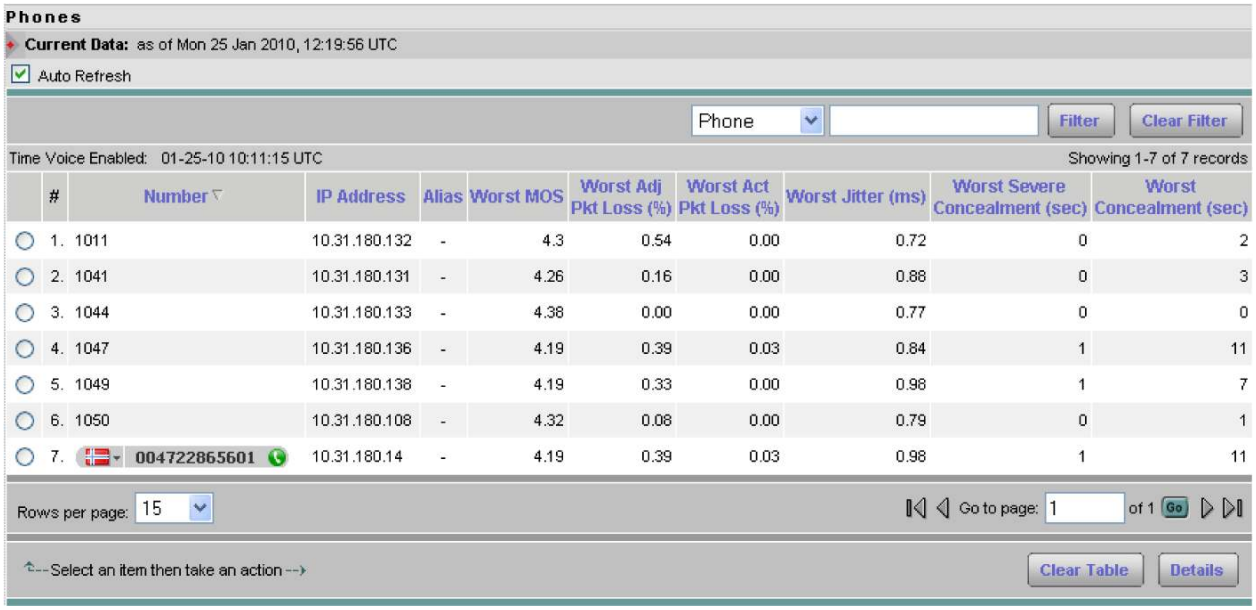
Figure 13. Worst N Phone Calls



#	Caller			Called			Worst MOS	Start Time	End Time
	Number	IP Address	Alias	Number	IP Address	Alias			
1.	1041	10.31.180.131	-	096899661231	10.31.180.14	-	4.38	01-25-10 08:12:51 UTC	01-25-10 08:12:56 UTC
2.	1045	10.31.180.134	-	00364375200	10.31.180.14	-	4.38	01-25-10 07:15:33 UTC	01-25-10 07:15:50 UTC
3.	1045	10.31.180.134	-	041714468746	10.31.180.14	-	4.38	01-25-10 08:01:07 UTC	01-25-10 08:01:15 UTC
4.	1045	10.31.180.134	-	041714468746	10.31.180.14	-	4.38	01-25-10 08:02:09 UTC	01-25-10 08:02:12 UTC
5.	1049	10.31.180.138	-	00435129390705	10.31.180.14	-	4.32	01-25-10 07:47:12 UTC	01-25-10 07:48:55 UTC

The Cisco NAM phones report keeps track of the phones in the network and provides visibility into the last N phone calls made from each phone to provide insight into issues with specific equipment (Figure 14).

Figure 14. Phones Report



Phones

Current Data: as of Mon 25 Jan 2010, 12:19:56 UTC

Auto Refresh

Phone | Filter | Clear Filter

Time Voice Enabled: 01-25-10 10:11:15 UTC — Showing 1-7 of 7 records

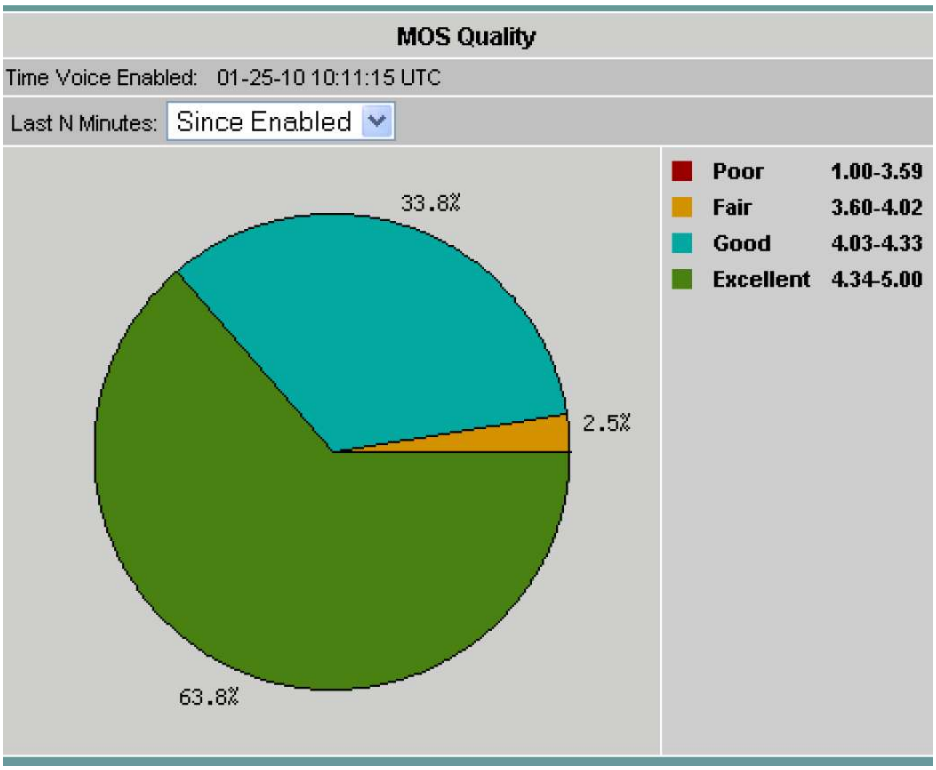
#	Number	IP Address	Alias	Worst MOS	Worst Adj Pkt Loss (%)	Worst Act Pkt Loss (%)	Worst Jitter (ms)	Worst Severe Concealment (sec)	Worst Concealment (sec)
1.	1011	10.31.180.132	-	4.3	0.54	0.00	0.72	0	2
2.	1041	10.31.180.131	-	4.26	0.16	0.00	0.88	0	3
3.	1044	10.31.180.133	-	4.38	0.00	0.00	0.77	0	0
4.	1047	10.31.180.136	-	4.19	0.39	0.03	0.84	1	11
5.	1049	10.31.180.138	-	4.19	0.33	0.00	0.98	1	7
6.	1050	10.31.180.108	-	4.32	0.08	0.00	0.79	0	1
7.	004722865601	10.31.180.14	-	4.19	0.39	0.03	0.98	1	11

Rows per page: 15 — Go to page: 1 of 1 Go

Select an item then take an action --> — Clear Table | Details

The call quality distribution report provides visibility into the overall call quality in the network. As seen in Figure 15, about 64 percent of the calls were of excellent quality, 34 percent of good quality.

Figure 15. Call Quality Distribution Report



Voice quality alerting was provided by Cisco Unified Operations Manager based on the data feed from the NAM (Figure 16). To further troubleshoot RTP stream issues, navigation back into the NAM from Cisco Unified Operations Manager was set up (Figure 17).

Figure 16. Call Quality Alert in Cisco Unified Operations Manager

Event ID: 00000TN

Property	Value
Destination	213.156.74.10
Destination IP Address	213.156.74.10
Destination Type	Endpoint
Destination Model	N/A
Switch For Destination	N/A
Destination Port	N/A
SourceEndPoint	217.124.198.85
Source IP Address	217.124.198.85
Source Type	Endpoint
Source Model	N/A
Switch For Source	N/A
Source Port	N/A
Detection Algorithm	NAM based voice quality
MOS	1.0
Critical MOS Threshold	3.5
Cause	Packet Loss
Codec	GSM Full Rate
Jitter	134 ms
Packet loss	15 Packets
NAM IP	172.16.14.15
Number of suppressed traps	0
Suppression start time	Mon 25-Jan-2010 10:50:59 CET
Suppression end time	Mon 25-Jan-2010 10:51:00 CET
NAM Call Details	http://172.16.14.15/monitor/stream/omStreams.php?srcIp=217.124.198.85&srcPort=54706&dstIp=213.156.74.10&dstPort=18814&ssrc=687874888&ts=1264
NAM Source	http://172.16.14.15:80

Clear Cl

Figure 17. RTP Stream Monitoring for Voice and Video Streams

RTP Stream Traffic

Current Data: as of Mon 25 Jan 2010, 13:13:34 UTC

Auto Refresh

Source Address Filter Clear

Showing 1-15 of 162 records

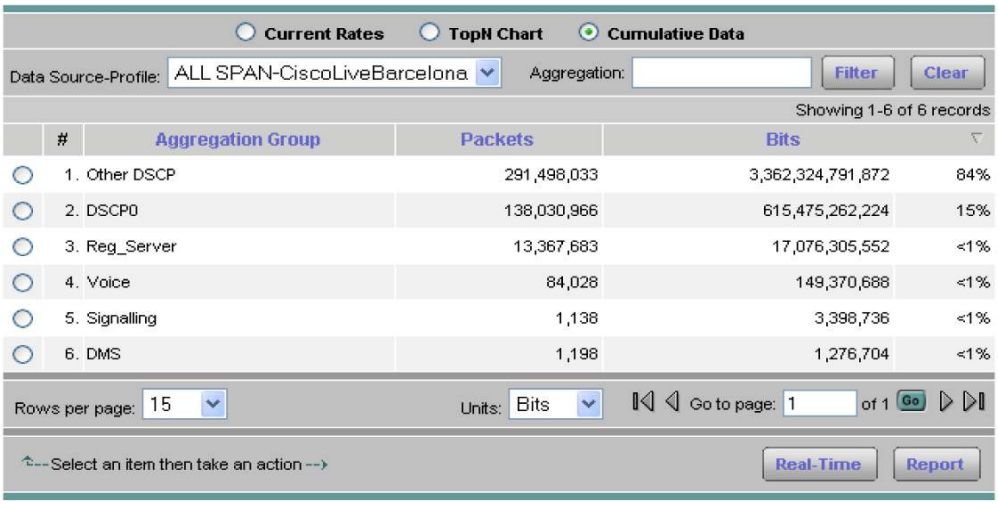
	#	Source Addr : Port	Dest Addr : Port	Payload Type	SSRC	Act Pkt Loss /million	Worst MOS	Adj Pkt Loss (%)	Jitter (ms)	Total SSC	Status	Start Time
○	1.	10.31.212.11 : 3028	10.31.212.25 : 16400	Unknown	1127060992	0	-	2.11	0.95	0	Active	01-25-10 10:55:43 UTC
○	2.	10.31.212.11 : 4028	10.31.212.25 : 16404	Unknown	846614247	0	-	0.00	0.00	0	Active	01-25-10 10:55:53 UTC
○	3.	10.31.212.12 : 3028	10.31.212.25 : 16406	Unknown	29001448	0	-	0.86	0.46	0	Active	01-25-10 10:55:21 UTC
○	4.	10.31.212.12 : 4028	10.31.212.25 : 16402	Unknown	63451962	38,326	-	3.83	0.00	0	Active	01-25-10 10:55:25 UTC
○	5.	10.31.180.101 : 16580	10.31.180.14 : 18950	G711Ulaw_64k	2952536897	0	4.28	0.31	0.06	0	Inactive	01-25-10 10:15:03 UTC

DiffServ Monitoring

Cisco NAM can examine the DiffServ and type of service (TOS) bits within IP packets and classify the packets based on DiffServ profiles. Each category can be examined for traffic volume and applications and hosts sending traffic with specific markings, which helps in verifying quality of service (QoS) planning assumptions.

At Cisco Live Barcelona, a DiffServ profile was created for voice RTP and voice signaling as well as for the Cisco Live registration server (Figure 18). However, as seen, most of the traffic was best effort in this network, which worked fine due to abundant bandwidth availability.

Figure 18. DiffServ Profile

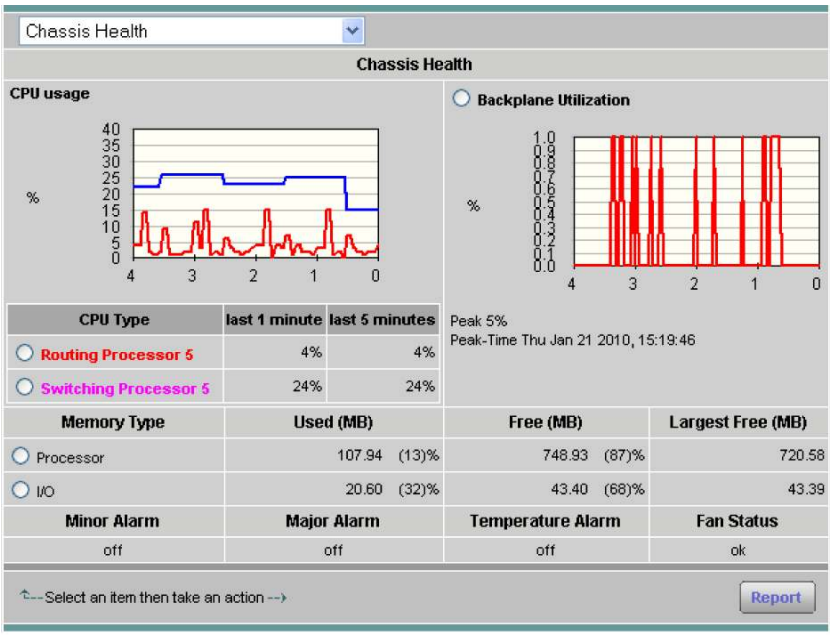


#	Aggregation Group	Packets	Bits	
1.	Other DSCP	291,498,033	3,362,324,791,872	84%
2.	DSCP0	138,030,966	615,475,262,224	15%
3.	Reg_Server	13,367,683	17,076,305,552	<1%
4.	Voice	84,028	149,370,688	<1%
5.	Signalling	1,138	3,398,736	<1%
6.	DMS	1,198	1,276,704	<1%

Switch Monitoring

At Cisco Live Barcelona, since the NAM was placed in the core Catalyst 6500 Series Switch, the NAM was able to provide visibility into the health of the switch including CPU and memory utilization (Figure 19), as well as port and error statistics.

Figure 19. Switch Health Monitoring



CPU Type	last 1 minute	last 5 minutes
Routing Processor 5	4%	4%
Switching Processor 5	24%	24%

Memory Type	Used (MB)	Free (MB)	Largest Free (MB)
Processor	107.94 (13)%	748.93 (87)%	720.58
I/O	20.60 (32)%	43.40 (68)%	43.39

Minor Alarm	Major Alarm	Temperature Alarm	Fan Status
off	off	off	ok

Managing the Cisco NAM with CiscoWorks LMS

CiscoWorks LMS was set up to manage all the devices at Cisco Live Barcelona, including the Cisco NAM. CiscoWorks LMS managed the inventory and configuration of the NAM, consolidated the syslogs and alerts received from the NAM (Figure 20), and provided visibility into the NAM through the centralized portal (Figure 21) by using NAM's web publishing feature.

Figure 20. CiscoWorks LMS Managing Cisco NAM

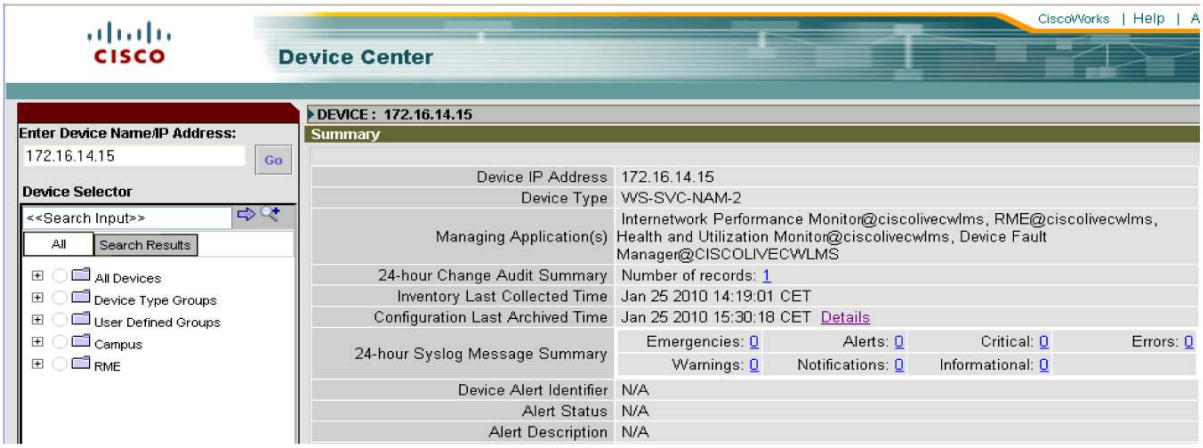
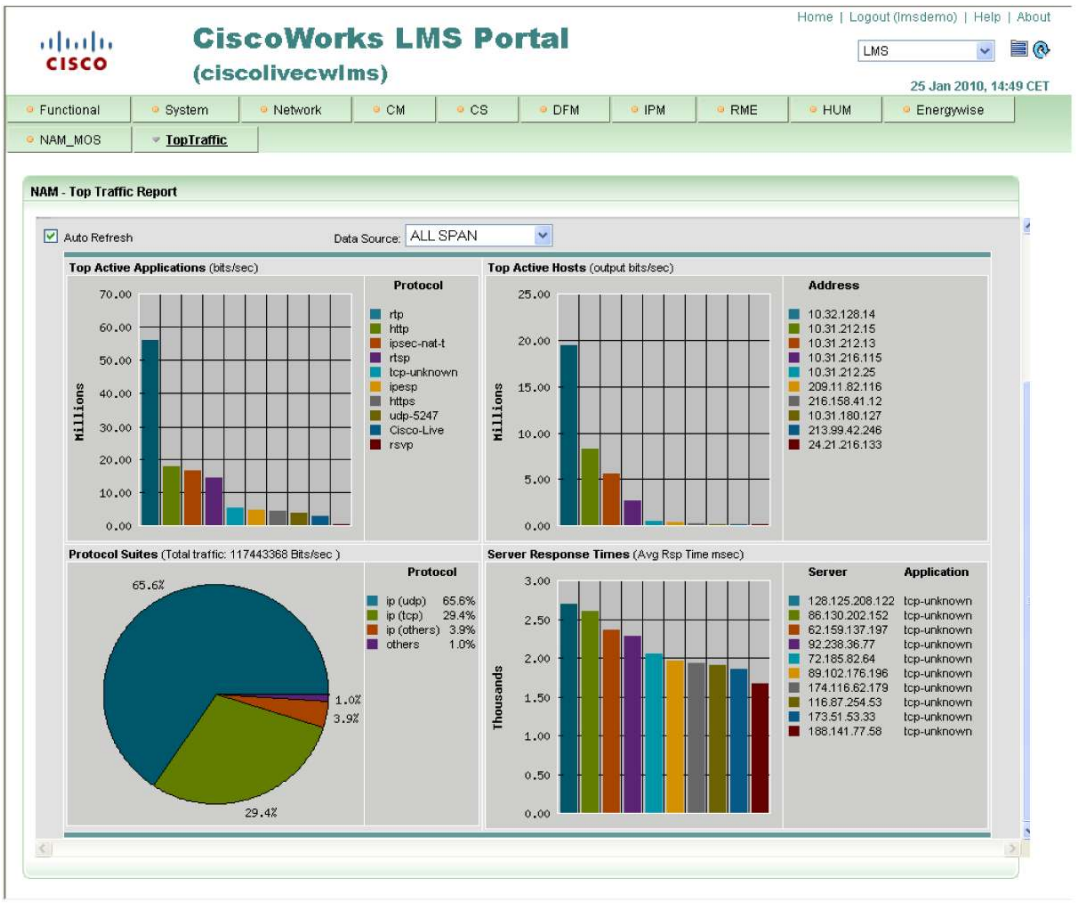


Figure 21. Cisco NAM Portal in CiscoWorks LMS



Summary

Cisco NAM provided real-time monitoring for the network at Cisco Live 2010, Barcelona. Cisco NAM helped ensure exceptional network performance by providing visibility into all data, voice, and video traffic, as well as into key performance indicators. NAM's click-of-a-button troubleshooting capabilities provided the necessary tools to improve Mean Time to Repair (MTTR) for any network issues. Cisco NAM was integrated with Cisco Unified Service Monitor and CiscoWorks LMS for end-to-end manageability of the entire network.

For more information on Cisco NAM visit http://www.cisco.com/go/nam.

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 C11-594769-00 04/10