Next Generation Enterprise WAN Regional WAN Management

Supplemental Guide

June, 2012

For further information, questions and comments please contact ccbu-pricing@cisco.com

Contents

1. Introduction

The Cisco® Next-Generation Enterprise WAN (NGEW) is an end-to-end architecture that provides foundation building blocks for next-generation enterprise networks. The hierarchical design provides the scalability required by large enterprises that can be extended and replicated throughout multiple regions and topologies. This consistency leads to ease of deployment, maintenance, and troubleshooting.

Network management plays an important role within the NGEW architecture. This document outlines Cisco Prime which fills this role within NGEW.

2. Cisco Prime Components

Cisco Prime™ products deliver unified management by supporting an intuitive workflow-oriented user experience and integrated lifecycle operations across Cisco architectures, technologies, and networks. Products in the Cisco Prime portfolio are designed to work together to offer the network administrator a transparent management experience.

Cisco Prime products help IT organizations:

- Simplify network management
- Improve operational efficiency
- Deliver predictable services
- Lower the total cost of ownership

IT organizations can now use Cisco Prime products to manage the NGEW. This overview focuses on how some of the features within Cisco Prime products can help network administrators easily deploy, monitor, and troubleshoot services that are based on the Cisco NGEW blueprint.

3. Day Zero - Challenges of Deploying NGEW Services

One of the first challenges comes when deploying a new branch office and the services that are provisioned on that office. How can Cisco Prime products help provision NGEW branch offices?

Normally a branch office is staged at a central location with just the minimal configuration to come online when installed at the remote branch-office location. This staging may be easy for a small network, but for an enterprise or large enterprise network, it is a very daunting task. How can multiple branch offices be provisioned with the least amount of time and effort? There are two steps to bringing new branch-office locations online: Configuring the network infrastructure to communicate with the branch office and deploying services on top of that infrastructure. The Cisco Prime LAN Management Solution (Cisco Prime LMS) can help with both of these tasks.

3.1 Cisco Prime LMS 4.2 New Capabilities

In addition to the functionality delivered in previous versions of LMS, significant new enhancements and features are being delivered in Cisco Prime LMS Release 4.2 - below is a summary:

Features	Functions	Benefits
Compliance and Audit Management	• An upgradable and customizable compliance engine checks for industrial compliance standards such as HIPAA, SOX, IOS/IEC 27002, NSA, PCI, DHS, DISA, CIS and other corporate, IT, and technology standards • Check and fix compliance violations • Services and capability reports • Lifecycle management reports covering end of sale/life, contracts, and PSIRT	• Extensive modeling of regulatory, corporate, IT, and technology policies • Provides visibility into network's compliance with policies • Identifies critical risks and violations • Prioritizes triage of compliance violations • Recommends fix for a set of known violations based on best practices

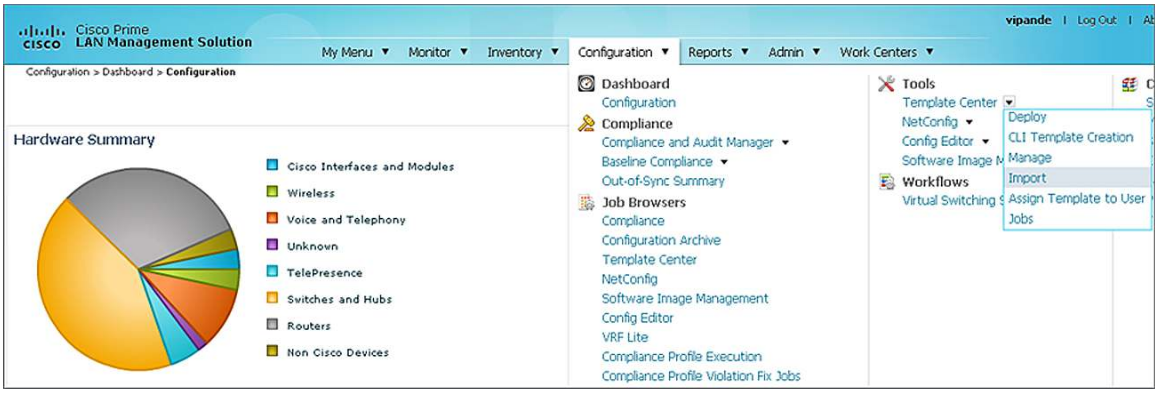
Features	Functions	Benefits
Work Centers	- Enhancements in the Cisco EnergyWise™ Work Center support smart Power Distribution Units (PDUs) and the ability to wake a Cisco EnergyWise host through Wake-on-LAN - Cisco TrustSec™ Work Center has been enhanced to support readiness assessment at the solution level and provides support for Secure Group Access (SGA) configuration - Enhanced Smart Install Work Center supports MAC-based groups and provides the ability to configure Integrated Service Routers (ISRs) as directors	- Take advantage of new borderless network service enhancements and capabilities such as Wake-on-LAN support for Cisco EnergyWise™, Cisco TrustSec™ readiness assessment, and Smart Install support on ISRs
Monitoring	- Generic fault management support across Cisco and non-Cisco devices based on standard instrumentation - Generic trap management support - Simplified poller creation workflow	- Facilitates visibility into the basic faults occurring in the entire wired network infrastructure - Provides visibility into traps that are not programmed into LMS
Configuration	- Embedded tool for creating custom configuration templates - Enhancements in Template Center to support conditional and looping configuration constructs	- Provides ability to create custom configuration templates - Provides better utilization of the configuration template capability to configure multiple interfaces with identical commands
Usability	- Simplified install and getting started workflows - Device center enhancements	- Helps in quickly getting started with managing the network with minimal initial setup overhead

3.2 Deploying NGEW Branch Office Using Cisco Prime LMS

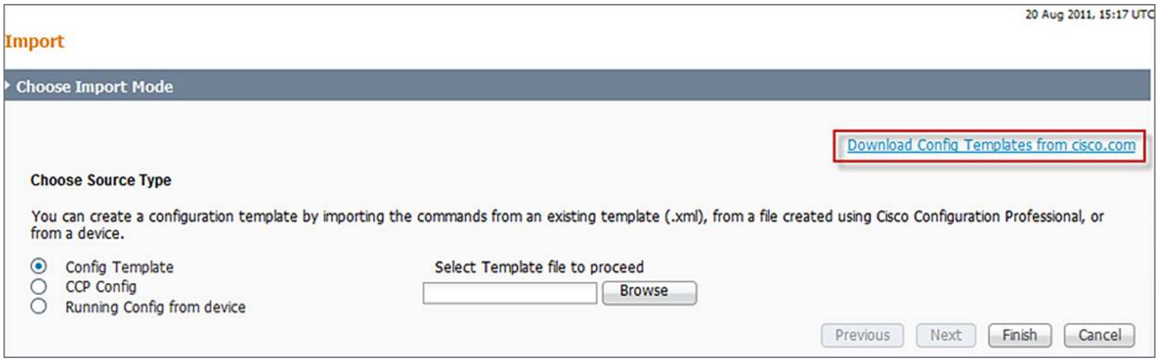
Cisco Prime LMS is the flagship product for managing Cisco and third-party infrastructures. Cisco Prime LMS is used to deploy branch offices, provision services, monitor networks, and report inventory on a NGEW network. NGEW branch offices can be deployed in a matter of minutes using the Cisco Prime LMS configuration template feature. The following is a step-by-step procedure for using the configuration templates to get a branch office operational quickly.

Step 1. Importing NGEW Templates

Cisco Prime LMS 4.2 provides a very convenient way to download and import templates into the application. From the main menu go to **Configuration > Template Center > Import**:



From the Import page, you can see a link **Download Config Templates from cisco.com**.


20 Aug 2011, 15:17 UTC

Import

Choose Import Mode

Download Config Templates from cisco.com

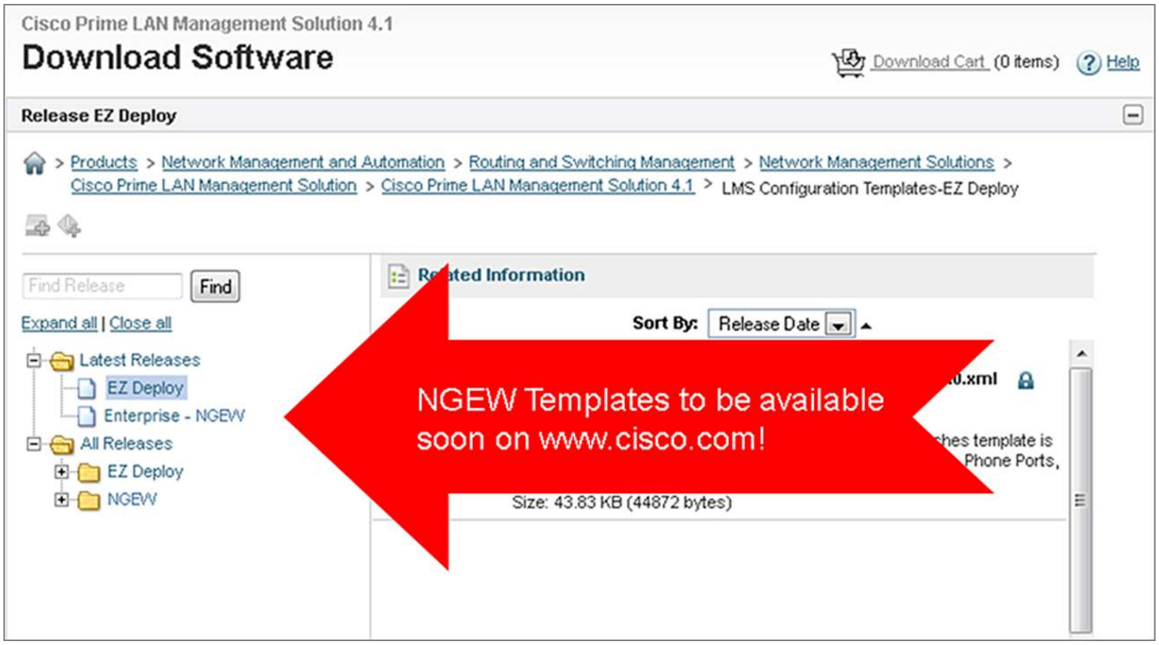
Choose Source Type

You can create a configuration template by importing the commands from an existing template (.xml), from a file created using Cisco Configuration Professional, or from a device.

● Config Template
○ CCP Config
○ Running Config from device

Select Template file to proceed

This link takes you directly to the cisco.com page, where all prebuilt LMS templates are listed. There will be a folder for NGEW in the near future (as shown in the following screenshot) where templates for pretested NGEW configurations can be downloaded.


Cisco Prime LAN Management Solution 4.1

Download Software

Download Cart (0 items) Help

Release EZ Deploy

> Products > Network Management and Automation > Routing and Switching Management > Network Management Solutions > Cisco Prime LAN Management Solution > Cisco Prime LAN Management Solution 4.1 > LMS Configuration Templates-EZ Deploy

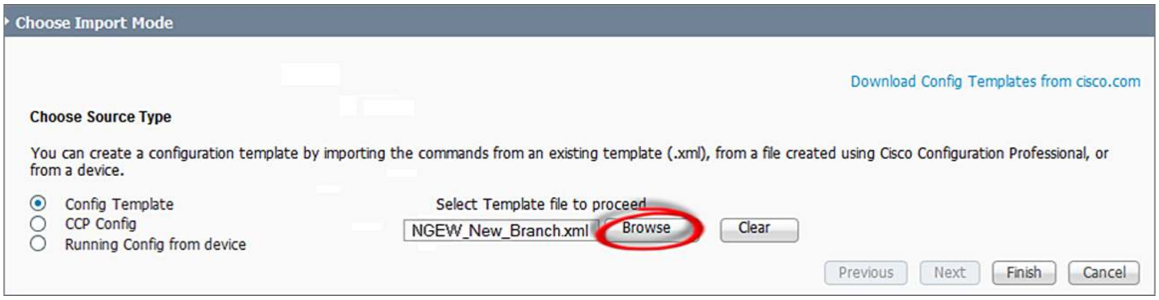
Related Information

Sort By: Release Date

NGEW Templates to be available soon on www.cisco.com!

Size: 43.83 KB (44872 bytes)

After the template is downloaded from cisco.com, the next step is to import the template into LMS using the import mode.


Choose Import Mode

Download Config Templates from cisco.com

Choose Source Type

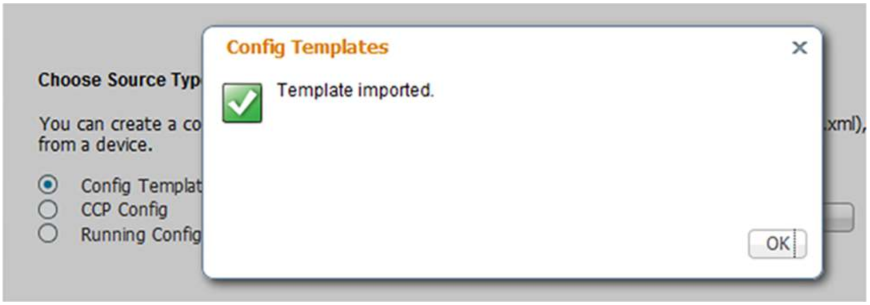
You can create a configuration template by importing the commands from an existing template (.xml), from a file created using Cisco Configuration Professional, or from a device.

● Config Template
○ CCP Config
○ Running Config from device

Select Template file to proceed

NGEW_New_Branch.xml

If you see the pop-up with a green check, you know that you have successfully imported the template.



Choose Source Typ

You can create a co ... xml),
from a device.

● Config Templat
○ CCP Config
○ Running Config

Config Templates ×

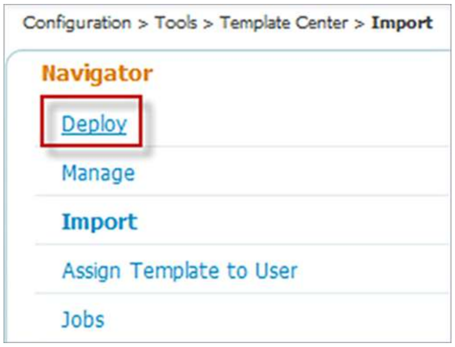
✓ Template imported.

OK

Prebuilt templates can be modified using any text editor to adapt the template to the specifics of your network. You can also create templates from running configurations of existing devices or import them from Cisco Configuration Professional.

Step 2. Deploying NGEW Branch Office

Now you can deploy the imported template using the deploy wizard. Click **Deploy** from the left pane of the configuration template import mode.

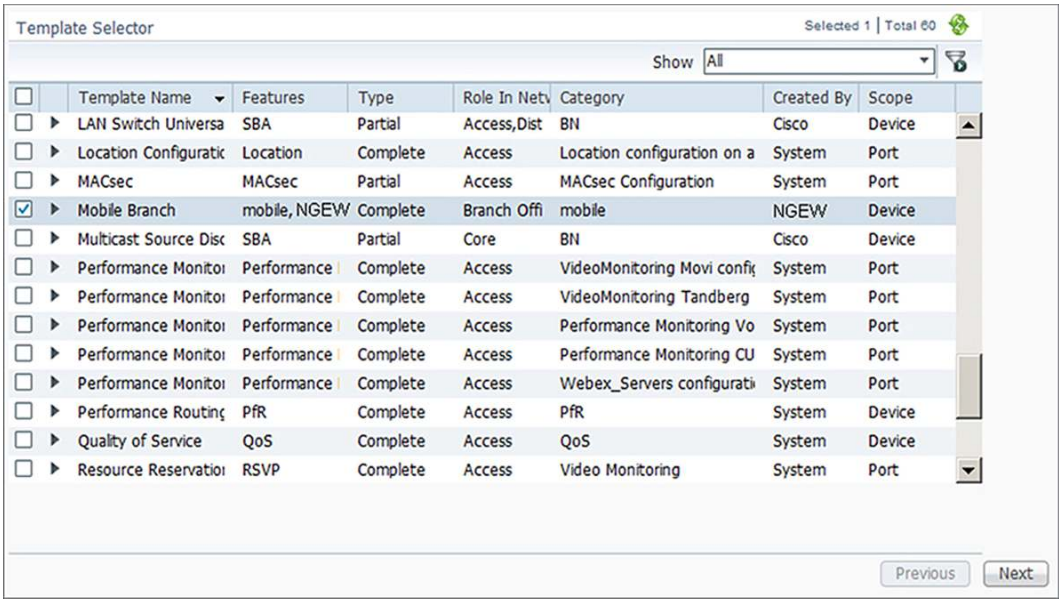


Configuration > Tools > Template Center > **Import**

Navigator

- Deploy
- Manage
- **Import**
- Assign Template to User
- Jobs

Find the NGEW template that was recently imported, and click Next to start the deploy wizard. To see what each template does, simply click the right arrow next to each of the templates.



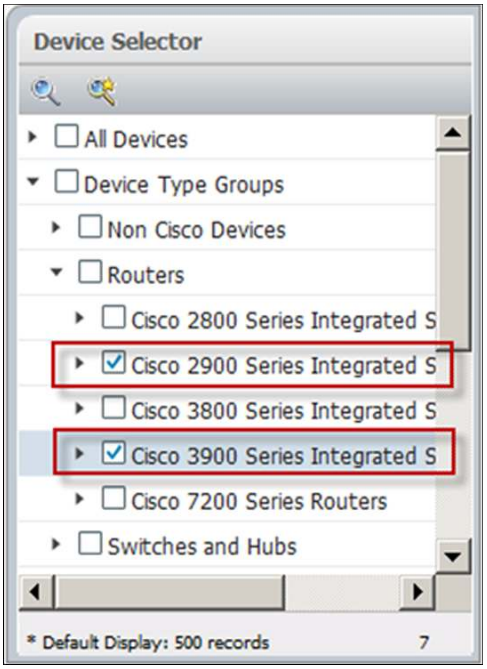
Template Selector — Selected 1 | Total 60

Show: All

□		Template Name	Features	Type	Role In Netv	Category	Created By	Scope
□	▶	LAN Switch Universa	SBA	Partial	Access,Dist	BN	Cisco	Device
□	▶	Location Configuratic	Location	Complete	Access	Location configuration on a	System	Port
□	▶	MACsec	MACsec	Partial	Access	MACsec Configuration	System	Port
☑	▶	Mobile Branch	mobile, NGEW	Complete	Branch Offi	mobile	NGEW	Device
□	▶	Multicast Source Disc	SBA	Partial	Core	BN	Cisco	Device
□	▶	Performance Monitoi	Performance	Complete	Access	VideoMonitoring Movi config	System	Port
□	▶	Performance Monitoi	Performance	Complete	Access	VideoMonitoring Tandberg	System	Port
□	▶	Performance Monitoi	Performance	Complete	Access	Performance Monitoring Vo	System	Port
□	▶	Performance Monitoi	Performance	Complete	Access	Performance Monitoring CU	System	Port
□	▶	Performance Monitoi	Performance	Complete	Access	Webex_Servers configurati	System	Port
□	▶	Performance Routing	PfR	Complete	Access	PfR	System	Device
□	▶	Quality of Service	QoS	Complete	Access	QoS	System	Device
□	▶	Resource Reservatioi	RSVP	Complete	Access	Video Monitoring	System	Port

Previous Next

Select the devices that will be used as the new branch-office routers.

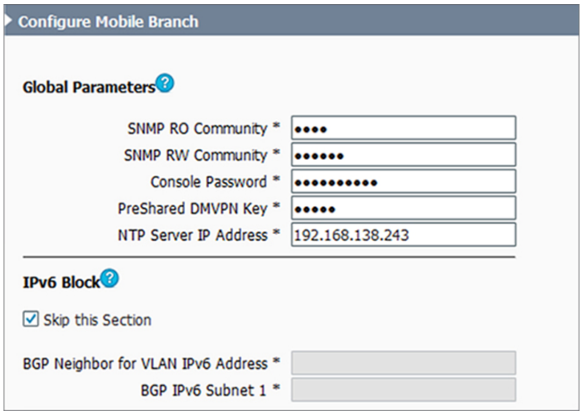


Device Selector

- □ All Devices
- □ Device Type Groups
  - □ Non Cisco Devices
  - □ Routers
    - □ Cisco 2800 Series Integrated S
    - ☑ Cisco 2900 Series Integrated S
    - □ Cisco 3800 Series Integrated S
    - ☑ Cisco 3900 Series Integrated S
    - □ Cisco 7200 Series Routers
  - □ Switches and Hubs

* Default Display: 500 records 7

The next step generates the branch-office configuration. You may need to complete multiple configuration fields within the template. The wizard will prompt you for all information that needs to be unique for this network or a particular device using this template. Grouping of sections helps you quickly enter relevant information. Enter all of the parameters broken down by section.



Configure Mobile Branch

Global Parameters

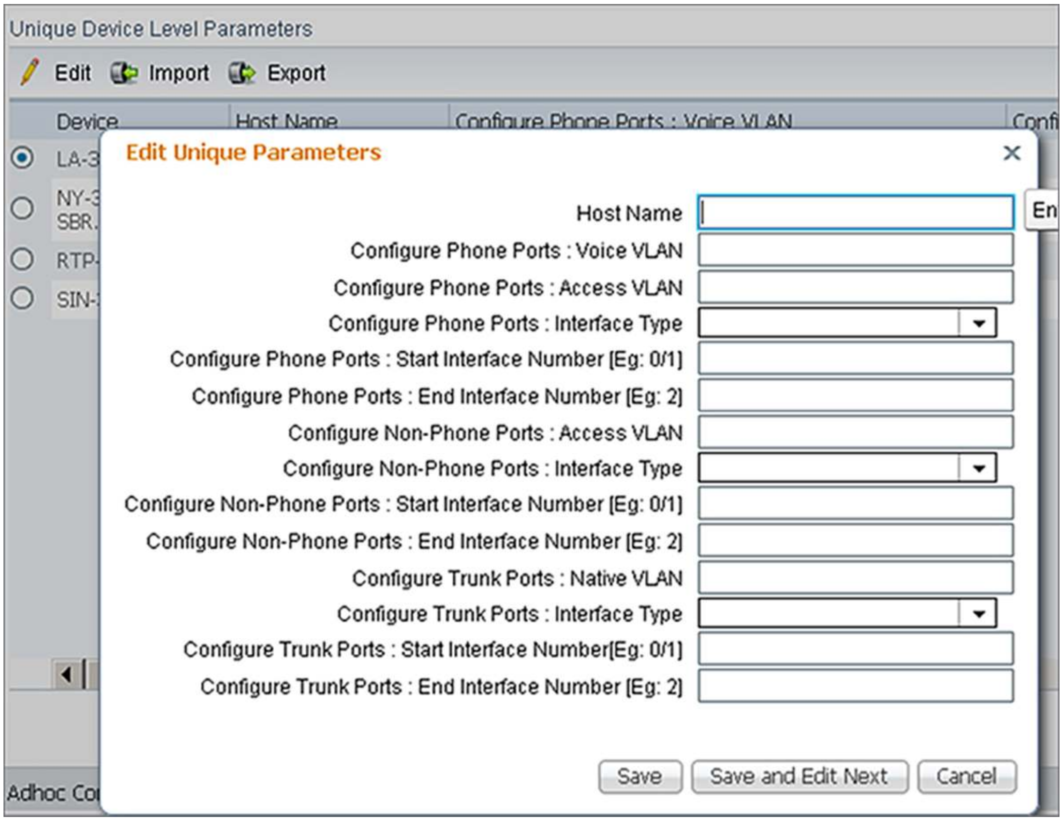
SNMP RO Community *	••••
SNMP RW Community *	••••••
Console Password *	•••••••••••
PreShared DMVPN Key *	•••••
NTP Server IP Address *	192.168.138.243

IPv6 Block

☑ Skip this Section

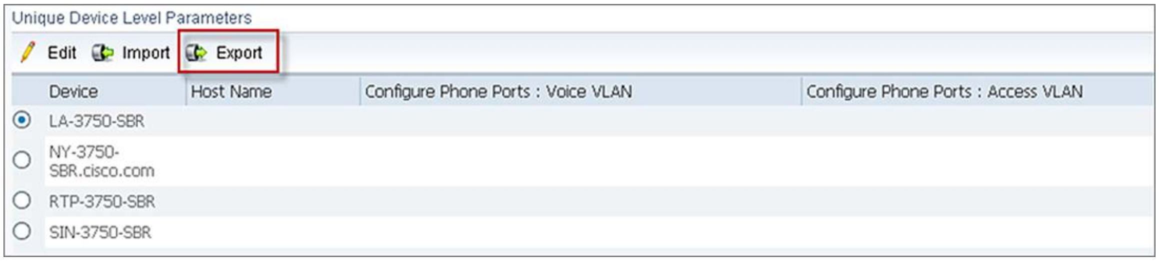
BGP Neighbor for VLAN IPv6 Address *	
BGP IPv6 Subnet 1 *	

The next step allows you to enter unique values one at a time on a per-device basis. This mechanism is most efficient for up to 5 to 10 branch offices.



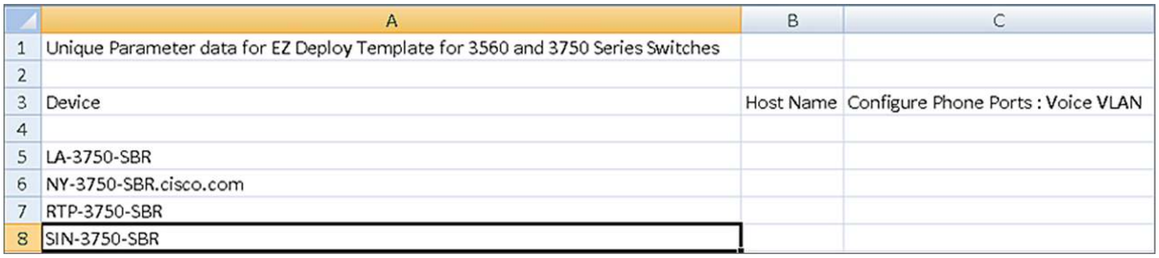
Host Name
Configure Phone Ports : Voice VLAN
Configure Phone Ports : Access VLAN
Configure Phone Ports : Interface Type
Configure Phone Ports : Start Interface Number [Eg: 0/1]
Configure Phone Ports : End Interface Number [Eg: 2]
Configure Non-Phone Ports : Access VLAN
Configure Non-Phone Ports : Interface Type
Configure Non-Phone Ports : Start Interface Number [Eg: 0/1]
Configure Non-Phone Ports : End Interface Number [Eg: 2]
Configure Trunk Ports : Native VLAN
Configure Trunk Ports : Interface Type
Configure Trunk Ports : Start Interface Number[Eg: 0/1]
Configure Trunk Ports : End Interface Number [Eg: 2]

For large-scale deployments of 10+ unique branch offices where the parameters vary, there is another mechanism within the configuration template to help merge the unique variables. If a template has such unique variables, a new wizard is created automatically that allows you to export the file with devices prepopulated.



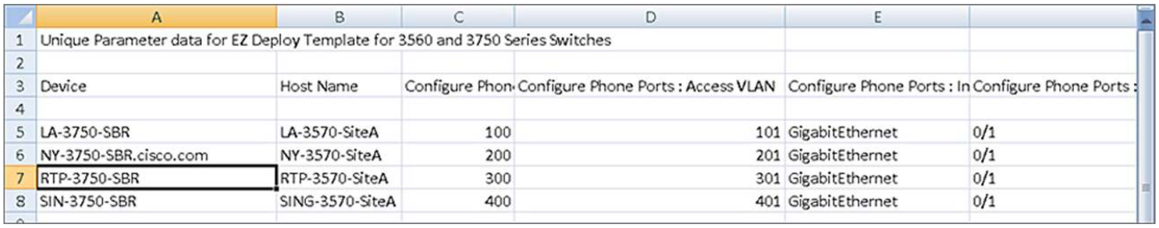
	Device	Host Name	Configure Phone Ports : Voice VLAN	Configure Phone Ports : Access VLAN
●	LA-3750-SBR			
○	NY-3750-SBR.cisco.com			
○	RTP-3750-SBR			
○	SIN-3750-SBR			

Cisco Prime LMS exports a .csv file with devices already populated, making it even easier to fill out using a spreadsheet application.



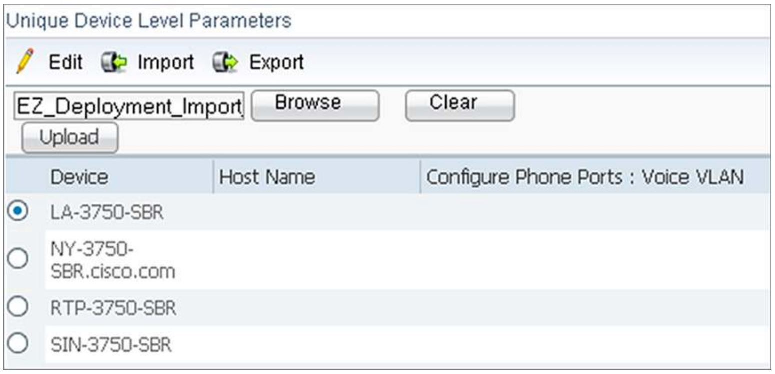
	A	B	C
1	Unique Parameter data for EZ Deploy Template for 3560 and 3750 Series Switches		
2			
3	Device	Host Name	Configure Phone Ports : Voice VLAN
4			
5	LA-3750-SBR		
6	NY-3750-SBR.cisco.com		
7	RTP-3750-SBR		
8	SIN-3750-SBR		

You can then fill in appropriate values:



	A	B	C	D	E	
1	Unique Parameter data for EZ Deploy Template for 3560 and 3750 Series Switches					
2						
3	Device	Host Name	Configure Phon	Configure Phone Ports : Access VLAN	Configure Phone Ports : In	Configure Phone Ports :
4						
5	LA-3750-SBR	LA-3570-SiteA	100	101	GigabitEthernet	0/1
6	NY-3750-SBR.cisco.com	NY-3570-SiteA	200	201	GigabitEthernet	0/1
7	RTP-3750-SBR	RTP-3570-SiteA	300	301	GigabitEthernet	0/1
8	SIN-3750-SBR	SING-3570-SiteA	400	401	GigabitEthernet	0/1

The information may then be reimported by browsing to the .csv file that has all the values filled in.

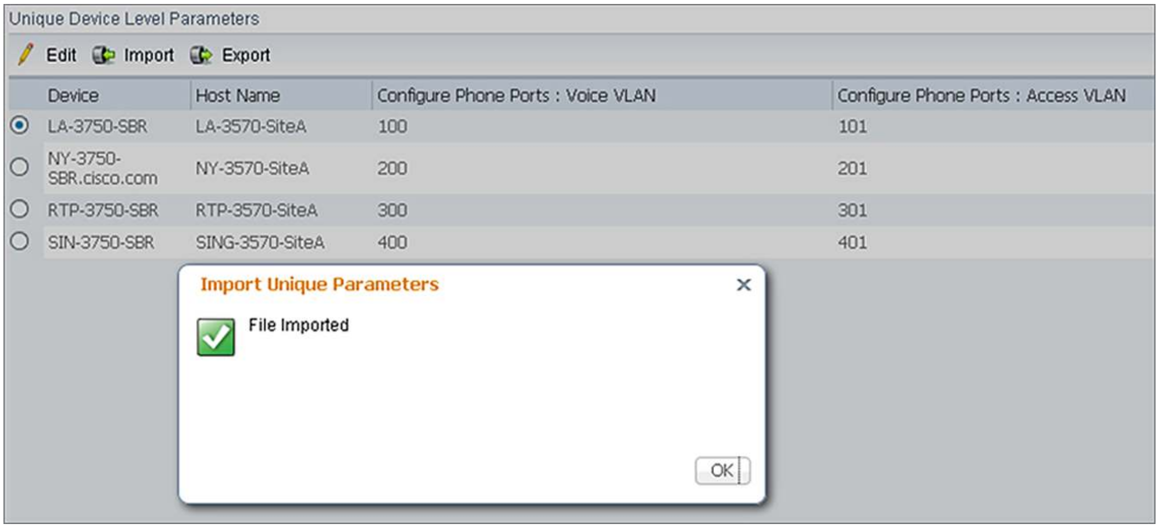


Unique Device Level Parameters

EZ_Deployment_Import

	Device	Host Name	Configure Phone Ports : Voice VLAN
●	LA-3750-SBR		
○	NY-3750-SBR.cisco.com		
○	RTP-3750-SBR		
○	SIN-3750-SBR		

You will see a successful pop-up message with all values filled in against each of the devices.



Unique Device Level Parameters

	Device	Host Name	Configure Phone Ports : Voice VLAN	Configure Phone Ports : Access VLAN
●	LA-3750-SBR	LA-3570-SiteA	100	101
○	NY-3750-SBR.cisco.com	NY-3570-SiteA	200	201
○	RTP-3750-SBR	RTP-3570-SiteA	300	301
○	SIN-3750-SBR	SING-3570-SiteA	400	401

Import Unique Parameters

File Imported

The next step is to add other temporary commands not included in the template. The available commands will differ depending on the type of device and your role-based access permissions. You can then view the final configuration that will be passed to the device in full. This step is the final human check before pushing out the configuration. Cisco Prime LMS does other checks in the back end based on the job attributes to make sure the device and configuration are compatible and ready for the update. After the job is deployed, you can then track the job status by going to **Administrator > Job Status**.

4. Day N - Monitoring and Troubleshooting Infrastructure and Services

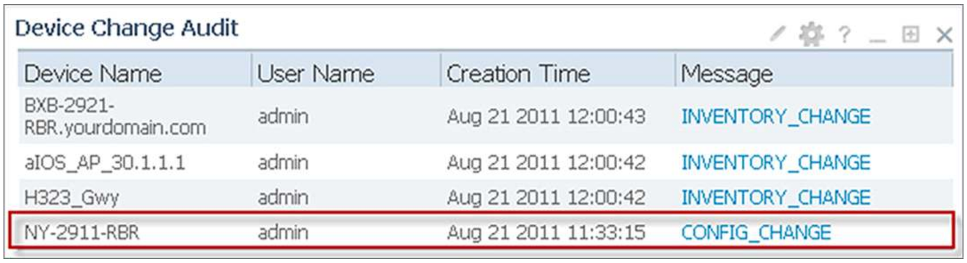
After the NGEW branch office is deployed with all the services enabled, the next task is to make sure that those offices are operating and providing the necessary services. How do you monitor the services that are deployed on the NGEW branch offices and troubleshoot the infrastructure that they run? The Cisco Prime family of products can help monitor and troubleshoot these functions from end to end.

4.1 Infrastructure Monitoring and Troubleshooting

You can use the Cisco Prime LMS to monitor the NGEW infrastructure. With Cisco Prime LMS, you can not only monitor the basic day-to-day operational needs such as device availability, Top-N statistics, and syslogs, but you can also monitor and report on change audits and other inventory-related business needs.

4.1.1 Change Management

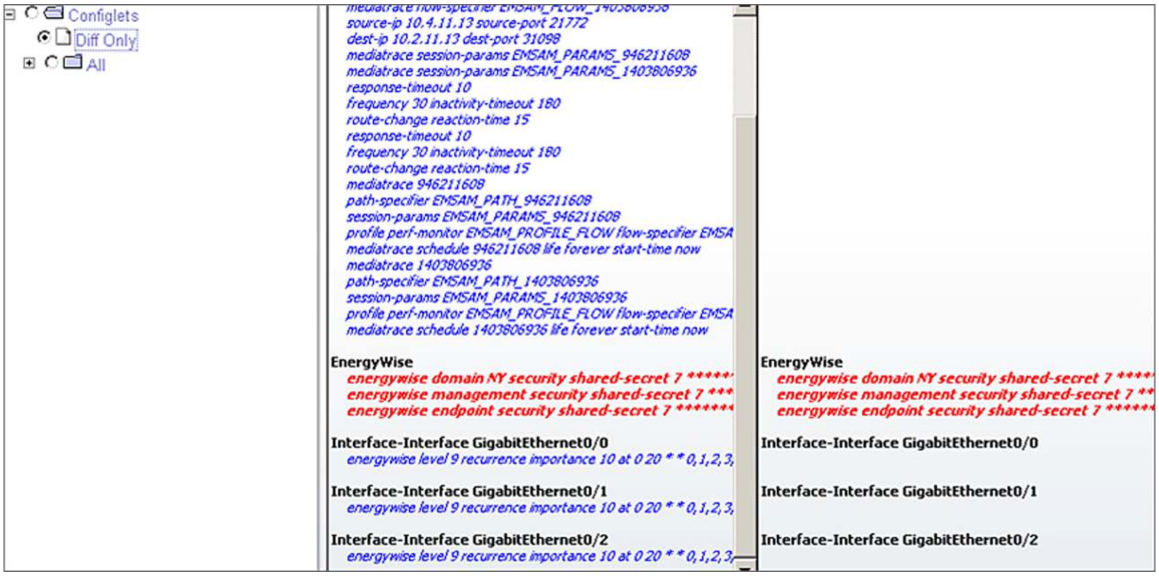
Change management, simply put, refers to retrieving information from the network in real time. These changes could be caused by replacing the device, modules, or cards within the device or other accessories within the device. Upgrading the device software or changing the device configuration would also contribute to a change that is worth tracking. You can easily track all of these changes with Cisco Prime LMS, which includes portlets that automate the task of tracking all types of change audits within the network. The following screenshot shows how you can track Inventory and Configuration audits using one of the portlets in Cisco Prime LMS:



Device Change Audit

Device Name	User Name	Creation Time	Message
BXB-2921-RBR.yourdomain.com	admin	Aug 21 2011 12:00:43	INVENTORY_CHANGE
aIOS_AP_30.1.1.1	admin	Aug 21 2011 12:00:42	INVENTORY_CHANGE
H323_Gwy	admin	Aug 21 2011 12:00:42	INVENTORY_CHANGE
NY-2911-RBR	admin	Aug 21 2011 11:33:15	CONFIG_CHANGE

When you click the **CONFIG_CHANGE**, seeing the difference between the current and prior versions becomes a trivial task. Notice how easy it is to see the difference between the two configs:

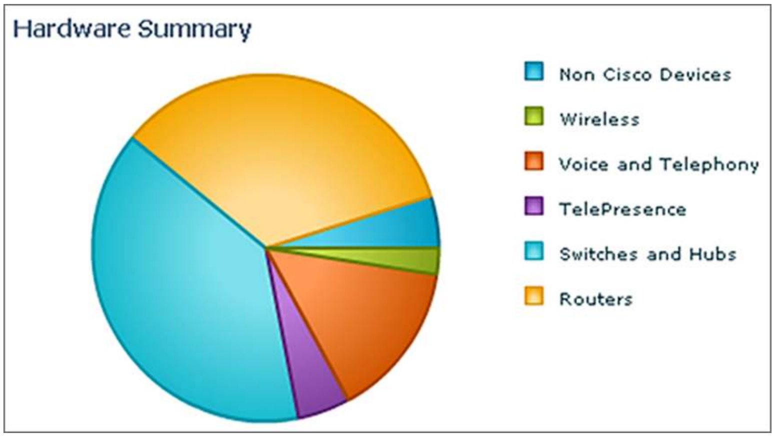


```
   mediatrace flow-specifier EMSAM_FLOW_1403806936
   source-ip 10.4.11.13 source-port 21772
   dest-ip 10.2.11.13 dest-port 31098
   mediatrace session-params EMSAM_PARAMS_946211608
   mediatrace session-params EMSAM_PARAMS_1403806936
   response-timeout 10
   frequency 30 inactivity-timeout 180
   route-change reaction-time 15
   response-timeout 10
   frequency 30 inactivity-timeout 180
   route-change reaction-time 15
   mediatrace 946211608
   path-specifier EMSAM_PATH_946211608
   session-params EMSAM_PARAMS_946211608
   profile perf-monitor EMSAM_PROFILE_FLOW flow-specifier EMSA
   mediatrace schedule 946211608 life forever start-time now
   mediatrace 1403806936
   path-specifier EMSAM_PATH_1403806936
   session-params EMSAM_PARAMS_1403806936
   profile perf-monitor EMSAM_PROFILE_FLOW flow-specifier EMSA
   mediatrace schedule 1403806936 life forever start-time now

EnergyWise
   energywise domain NY security shared-secret 7 *****
   energywise management security shared-secret 7 ***
   energywise endpoint security shared-secret 7 *******

Interface-Interface GigabitEthernet0/0
   energywise level 9 recurrence importance 10 at 0 20 * * 0,1,2,3,

Interface-Interface GigabitEthernet0/1
   energywise level 9 recurrence importance 10 at 0 20 * * 0,1,2,3,

Interface-Interface GigabitEthernet0/2
   energywise level 9 recurrence importance 10 at 0 20 * * 0,1,2,3,
```

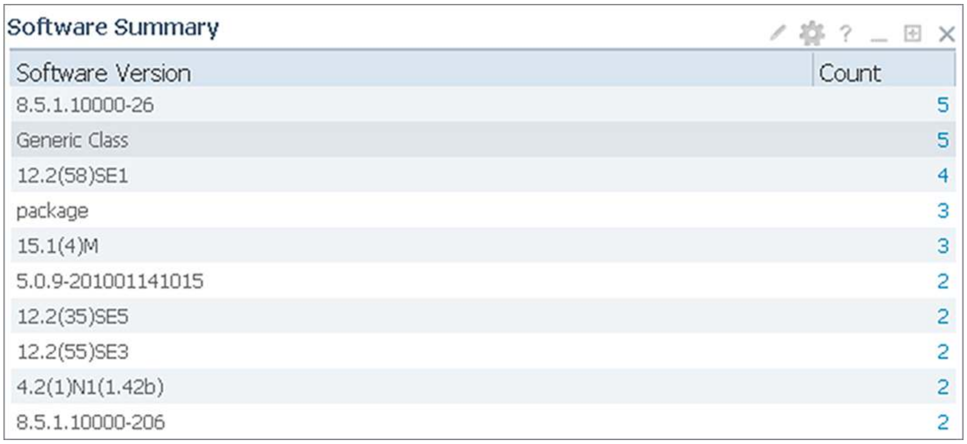
```
EnergyWise
   energywise domain NY security shared-secret 7 *****
   energywise management security shared-secret 7 **
   energywise endpoint security shared-secret 7 ******

Interface-Interface GigabitEthernet0/0

Interface-Interface GigabitEthernet0/1

Interface-Interface GigabitEthernet0/2
```

4.1.2 Inventory and Asset Management

Tracking inventory is just as important as tracking the configuration changes. It is an important business function to maintain an accurate inventory of all devices on the network, including their types, installed options, and versions of software and configuration. Launching the Cisco Prime LMS Inventory dashboard quickly gives a high-level overview. You can see how many routers and switches are in the network. The graphs are clickable to further examine each type of device to see specific chassis, where it is located, and other basic system information. You can collect similar MIB-2 derived information for third-party devices as well.



Having a chart for software images running on network devices also has its own significance. Clicking the number at the right in the screenshot that follows allows access to information similar to that of the hardware inventory. Having a table of all software versions allows you to baseline the network and to quickly spot any devices not running a standardized image.



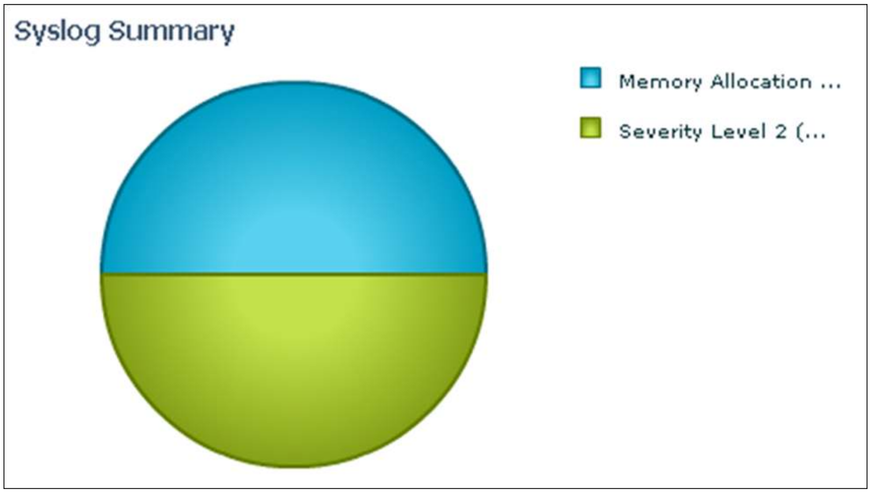
Software Summary

Software Version	Count
8.5.1.10000-26	5
Generic Class	5
12.2(58)SE1	4
package	3
15.1(4)M	3
5.0.9-201001141015	2
12.2(35)SE5	2
12.2(55)SE3	2
4.2(1)N1(1.42b)	2
8.5.1.10000-206	2

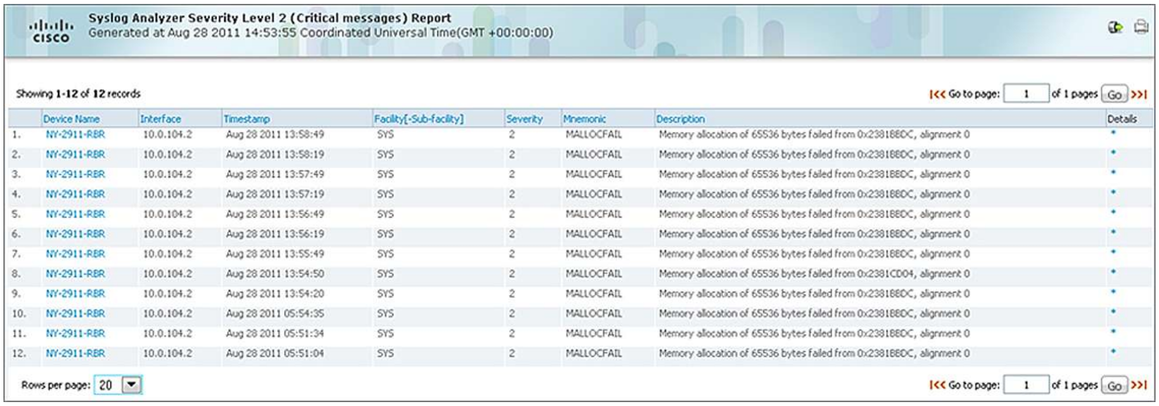
4.1.3 Monitoring and Troubleshooting

Syslog Management

Syslogs are crucial for monitoring the network and network services. Syslogs can provide more detailed information than traps. Cisco Prime LMS takes full advantage of this fact, and helps you sift valuable meaning from the syslogs of a device. With Cisco Prime LMS, many portlets are available to give a clear view of the syslogs sent out by devices on the network. The following screenshot shows that two syslog categories that have been received need attention: memory allocation and severity level 2 syslogs. Syslog portlets are quite flexible, and you can modify them to show only syslogs that are of interest to you. You can filter them by severity or with a custom rule that you create, allowing for generation of an instant view that monitors values pertinent to this network.



As with inventory in Cisco Prime LMS, clicking the syslog type allows you to find more details and see the individual syslogs.

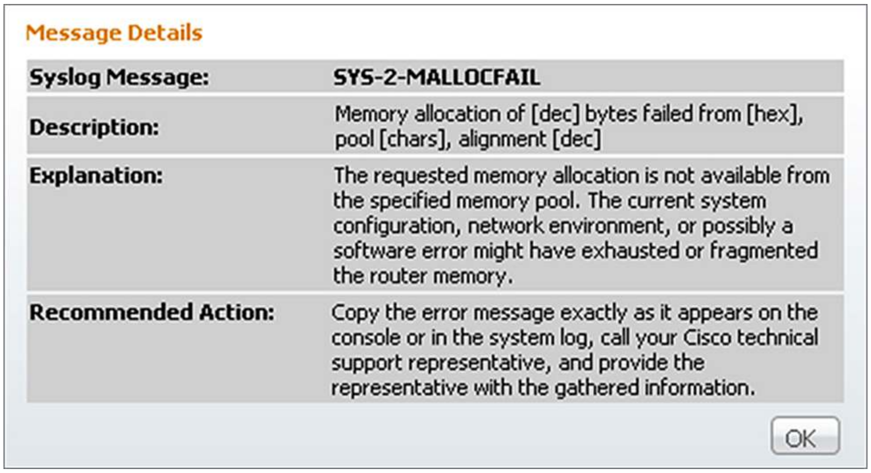

Syslog Analyzer Severity Level 2 (Critical messages) Report
Generated at Aug 28 2011 14:53:55 Coordinated Universal Time(GMT +00:00:00)

Showing **1-12** of **12** records

	Device Name	Interface	Timestamp	Facility[-Sub-facility]	Severity	Mnemonic	Description	Details
1.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:58:49	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
2.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:58:19	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
3.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:57:49	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
4.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:57:19	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
5.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:56:49	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
6.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:56:19	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
7.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:55:49	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
8.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:54:50	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x2381CD04, alignment 0	•
9.	NY-2911-RBR	10.0.104.2	Aug 28 2011 13:54:20	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
10.	NY-2911-RBR	10.0.104.2	Aug 28 2011 05:54:35	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
11.	NY-2911-RBR	10.0.104.2	Aug 28 2011 05:51:34	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•
12.	NY-2911-RBR	10.0.104.2	Aug 28 2011 05:51:04	SYS	2	MALLOCFAIL	Memory allocation of 65536 bytes failed from 0x238188DC, alignment 0	•

cisco
I<< Go to page: 1 of 1 pages Go >>I
Rows per page: 20
I<< Go to page: 1 of 1 pages Go >>I

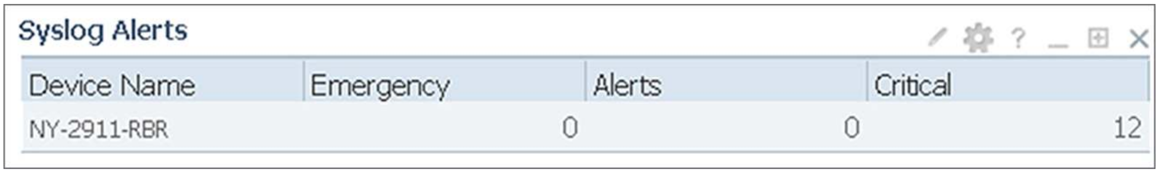
Cisco Prime LMS is linked with cisco.com to give you the most current information about syslog messages. By clicking **Details** (shown in the right column in the previous screenshot), Cisco Prime LMS provides a detailed explanation of the syslog directly from cisco.com as well as recommended actions that you can take.



Message Details

Syslog Message:	**SYS-2-MALLOCFAIL**
Description:	Memory allocation of [dec] bytes failed from [hex], pool [chars], alignment [dec]
Explanation:	The requested memory allocation is not available from the specified memory pool. The current system configuration, network environment, or possibly a software error might have exhausted or fragmented the router memory.
Recommended Action:	Copy the error message exactly as it appears on the console or in the system log, call your Cisco technical support representative, and provide the representative with the gathered information.

Syslog Alerts is another portlet that is quite useful in letting you know the devices that may have problems. The portlet shows any devices sending out Critical severity messages.

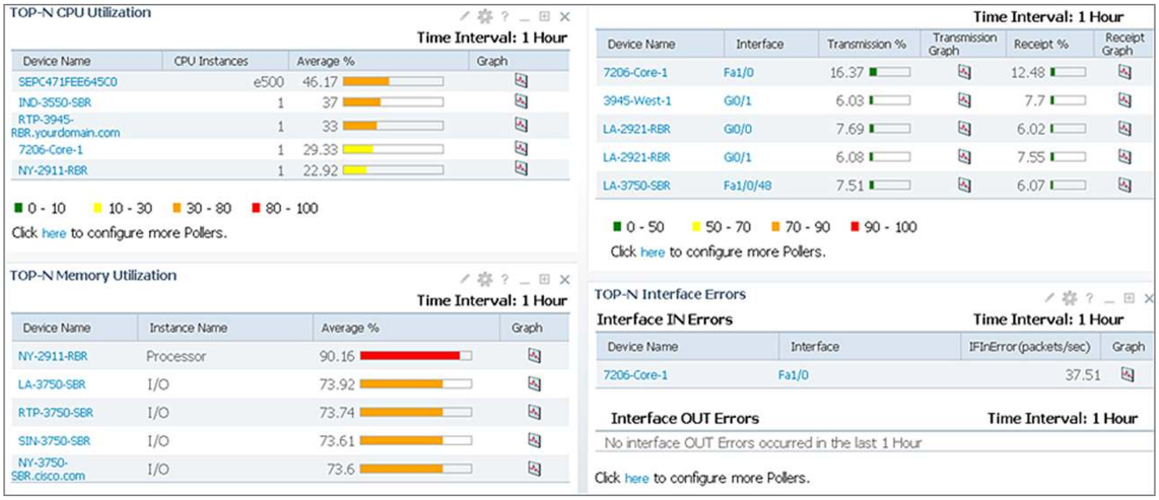


Syslog Alerts

Device Name	Emergency	Alerts	Critical
NY-2911-RBR	0	0	12

Top-N Statistics

The Monitoring dashboard is populated with the Top-N portlets for quickly spotting problems. Cisco Prime LMS has the Top-N portlets for CPU, memory, interface, errors, environmental, and other important statistics to help troubleshoot problems.



TOP-N CPU Utilization

Time Interval: 1 Hour

Device Name	CPU Instances	Average %	Graph
SEPC471FEE645C0	e500	46.17	📈
IND-3550-SBR	1	37	📈
RTP-3945-RBR.yourdomain.com	1	33	📈
7206-Core-1	1	29.33	📈
NY-2911-RBR	1	22.92	📈

🟩 0 - 10 🟨 10 - 30 🟧 30 - 80 🟥 80 - 100

Click here to configure more Pollers.

TOP-N Memory Utilization

Time Interval: 1 Hour

Device Name	Instance Name	Average %	Graph
NY-2911-RBR	Processor	90.16	📈
LA-3750-SBR	I/O	73.92	📈
RTP-3750-SBR	I/O	73.74	📈
SIN-3750-SBR	I/O	73.61	📈
NY-3750-SBR.cisco.com	I/O	73.6	📈

Time Interval: 1 Hour

Device Name	Interface	Transmission %	Transmission Graph	Receipt %	Receipt Graph
7206-Core-1	Fa1/0	16.37	📈	12.48	📈
3945-West-1	Gi0/1	6.03	📈	7.7	📈
LA-2921-RBR	Gi0/0	7.69	📈	6.02	📈
LA-2921-RBR	Gi0/1	6.08	📈	7.55	📈
LA-3750-SBR	Fa1/0/48	7.51	📈	6.07	📈

🟩 0 - 50 🟨 50 - 70 🟧 70 - 90 🟥 90 - 100

Click here to configure more Pollers.

TOP-N Interface Errors

Interface IN Errors

Time Interval: 1 Hour

Device Name	Interface	IFInError(packets/sec)	Graph
7206-Core-1	Fa1/0	37.51	📈

Interface OUT Errors

Time Interval: 1 Hour

No interface OUT Errors occurred in the last 1 Hour

Click here to configure more Pollers.

Cisco Prime LMS has many more tools to help troubleshoot network problems that are beyond the scope of this document. For more information, refer to: http://www.cisco.com/go/lms.

4.2 Services

4.2.1 Collaboration

Cisco Prime Collaboration Manager 1.1, part of the Cisco Prime Network Management portfolio is the Enterprise platform of choice for delivering Integrated Troubleshooting with Enterprise Medianet, Cisco Mediatrace and IP Service-Level Agreement Video Operations. These capabilities are essential when video services are deployed in the branch office, Collaboration Manager can easily discover the video infrastructure and provide overall health. Cisco Prime Collaboration Manager 1.1 allows you to visualize, monitor, and troubleshoot video service for a Next Generation Enterprise WAN deployment.

New Capabilites in Cisco Prime Collaboration Manager 1.1:

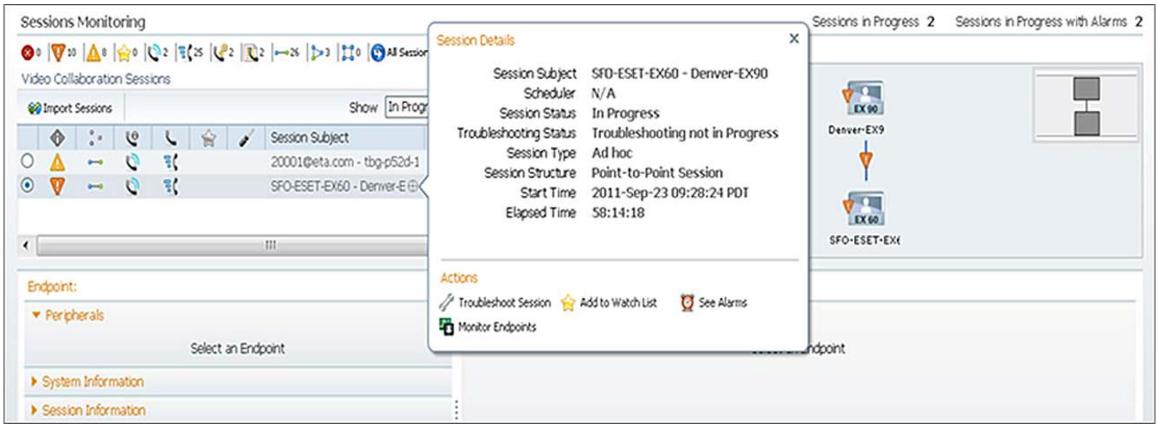
- End-to-end visibility, real-time troubleshooting and inventory support for Cisco TelePresence® EX and C Series (Release 1.0 included Cisco TelePresence System endpoints only)
- Support for scheduled meetings from Cisco TelePresence Management Server (Release 1.0 included Cisco TelePresence Manager)
- At-a-glance executive summaries and out-of-the box simplified use and diagnostic reports
- Ability to initiate Performance Monitoring on-the-fly providing deeper visibility on medianet-enabled networks into flow statistics at hotspots (Release 1.0 introduced Cisco Mediatrace and IP-SLA VO)
- Integration with other Cisco Prime management systems (LMS and NAM) offering critical diagnostic information about the network along the video path

Collaboration Manager provides Real-time visualization of in-progress video collaboration sessions, detailed end-to-end visibility into the media path, at-a-glance executive summaries to identify critical outages, and simple out-of-the-box reporting to view utilization and problem trends. When a network includes medianet-capable devices, Cisco Prime Collaboration Manager provides even deeper network path visibility, down to the granularity of video flow statistics.

To help ensure a superior end-user experience, Cisco Prime Collaboration Manager Speeds troubleshooting and recovery from service-affecting problems, provides detailed analysis to quickly pinpoint service-degrading network devices, delivers reports that help you manage your key assets and track usage. In addition, Cisco Prime Collaboration Manager efficiently validates large-scale deployments. It comprehensively evaluates the inventory, health, and status of Cisco TelePresence endpoints, as well as service and network infrastructure devices.

Collaboration Manager offers an easy way to see how many sessions are active at any time within the video network. Simply go to **Monitor > Session Monitoring** to see the sessions that are in progress in the network. In the screen shot below you can see a video session between Tandberg EX-60 and EX-90.

This screenshot clearly tells you if the endpoint is experiencing any session errors. To further probe the cause of any problems and initiate troubleshooting, use the cursor to hover over the Session Subject and a Session Details screen will pop-up as shown in the screen shot below.

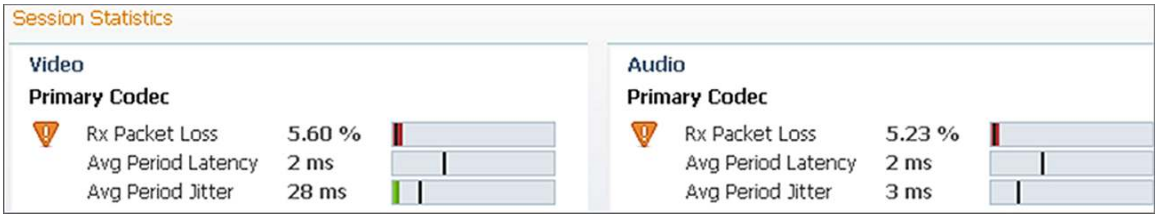


Session Subject
20001@eta.com - tbg-p52d-1
SFO-ESET-EX60 - Denver-E

Session Details

Session Subject	SFO-ESET-EX60 - Denver-EX90
Scheduler	N/A
Session Status	In Progress
Troubleshooting Status	Troubleshooting not in Progress
Session Type	Ad hoc
Session Structure	Point-to-Point Session
Start Time	2011-Sep-23 09:28:24 PDT
Elapsed Time	58:14:18

Click one of the endpoints on the right side to see detailed statistics:



Session Statistics

Video

Primary Codec

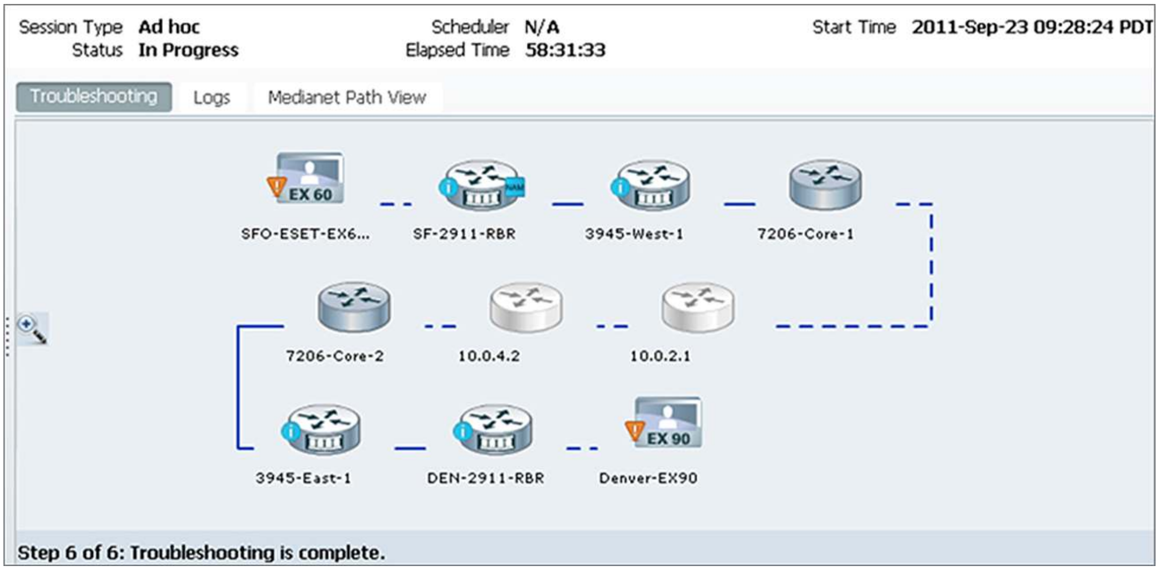
⚠	Rx Packet Loss	5.60 %
	Avg Period Latency	2 ms
	Avg Period Jitter	28 ms

Audio

Primary Codec

⚠	Rx Packet Loss	5.23 %
	Avg Period Latency	2 ms
	Avg Period Jitter	3 ms

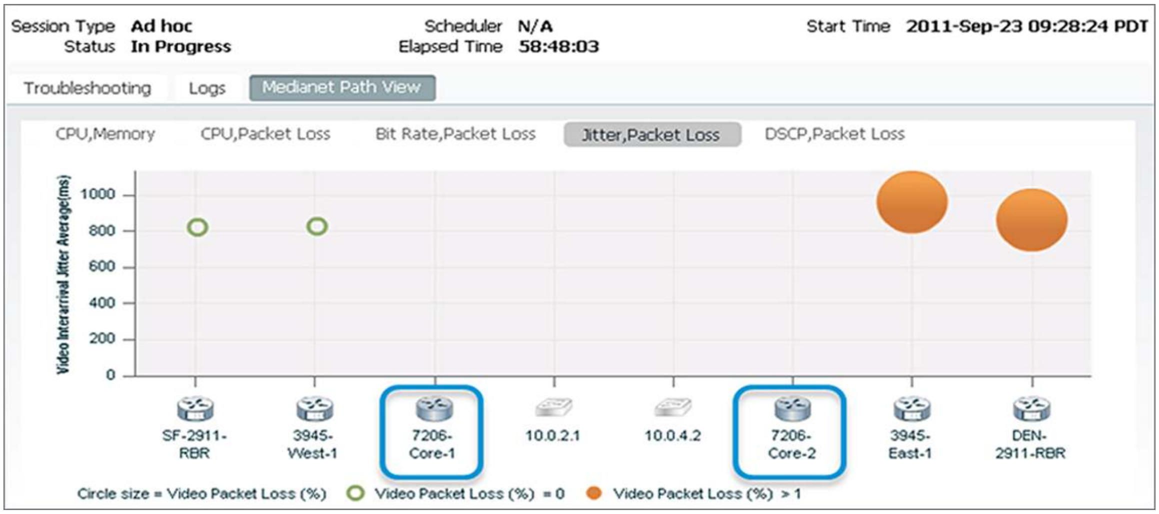
Click **Troubleshoot Session** to let Collaboration Manager quickly identify the areas in the network that might be causing the problem. Collaboration Manager gives you a visual trace between the two endpoints:



Session Type Ad hoc
Status In Progress
Scheduler N/A
Elapsed Time 58:31:33
Start Time 2011-Sep-23 09:28:24 PDT

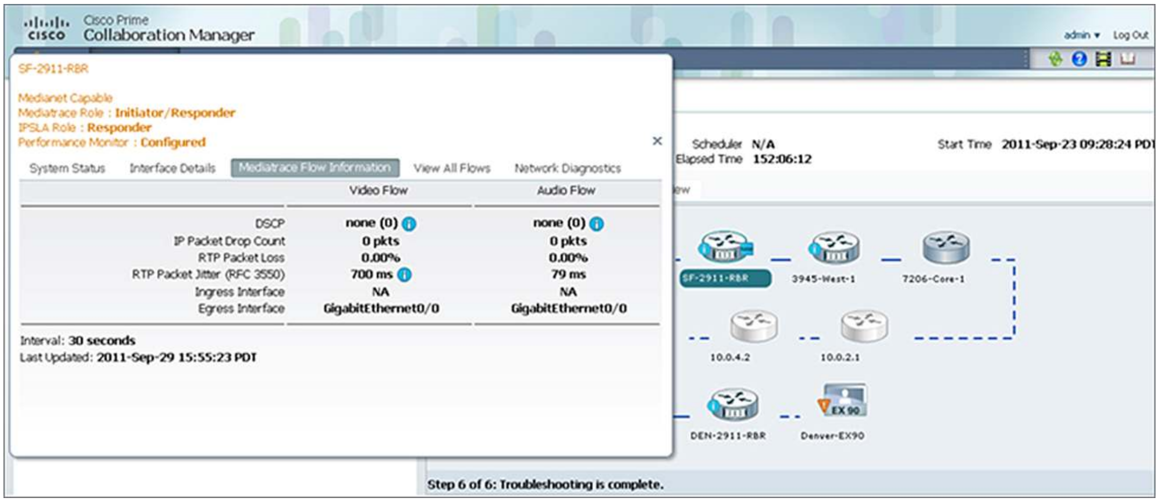
Step 6 of 6: Troubleshooting is complete.

Notice that the device icons change based on the capabilities that are enabled on the devices. Medianet-capable devices have a “film strip” on the edge. Click **Medianet Path View** to instantly see all the intermediate devices on the x-axis. Various other parameters such as CPU, memory, packet loss, and jitter are plotted on the y-axis. The size of the bubble indicates the magnitude of the second variable of the tab. For example, in the screenshot note that jitter is indicated by the y-axis, whereas the size of the bubble indicates packet loss.



Session Type **Ad hoc**
Status **In Progress**
Scheduler **N/A**
Elapsed Time **58:48:03**
Start Time **2011-Sep-23 09:28:24 PDT**

Use the cursor to hover over the bubble to see the severity of the packet loss and, more importantly, where the packet loss is first detected. You can see in the path view in the previous screenshot that there is relatively little packet loss at the 3945-East-1 router as compared to the LA-2921-RBR router. Clicking the bubble provides additional information related to the video flow that can also help in troubleshooting video.



SF-2911-RBR

Medianet Capable
Mediatrace Role : **Initiator/Responder**
IPSLA Role : **Responder**
Performance Monitor : **Configured**

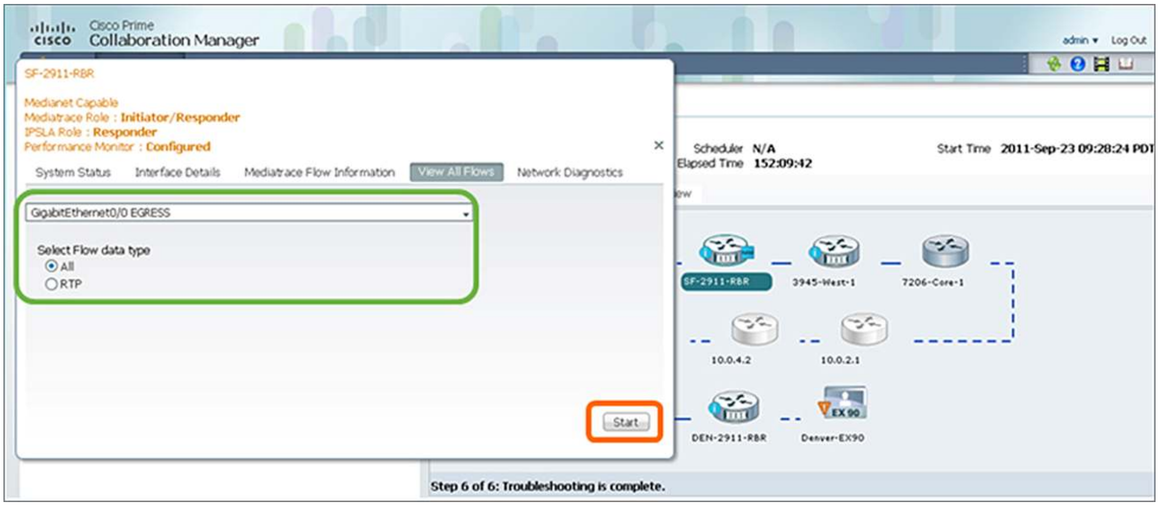
	Video Flow	Audio Flow
DSCP	none (0) ⓘ	none (0) ⓘ
IP Packet Drop Count	0 pkts	0 pkts
RTP Packet Loss	0.00%	0.00%
RTP Packet Jitter (RFC 3550)	700 ms ⓘ	79 ms
Ingress Interface	NA	NA
Egress Interface	GigabitEthernet0/0	GigabitEthernet0/0

Interval: **30 seconds**
Last Updated: **2011-Sep-29 15:55:23 PDT**

Scheduler **N/A**
Elapsed Time **152:06:12**
Start Time **2011-Sep-23 09:28:24 PDT**

Step 6 of 6: Troubleshooting is complete.

Cisco Prime Collaboration Manager 1.1 also provides the ability to the network admin to initiate Performance Monitoring on the fly. Click on the “View All Flows” tab in the above pop-up, select the Flow Data type (All/RTP) and hit “Start”.



SF-2911-RBR

Mediant Capable
Mediatrace Role : **Initiator/Responder**
IPSLA Role : **Responder**
Performance Monitor : **Configured**

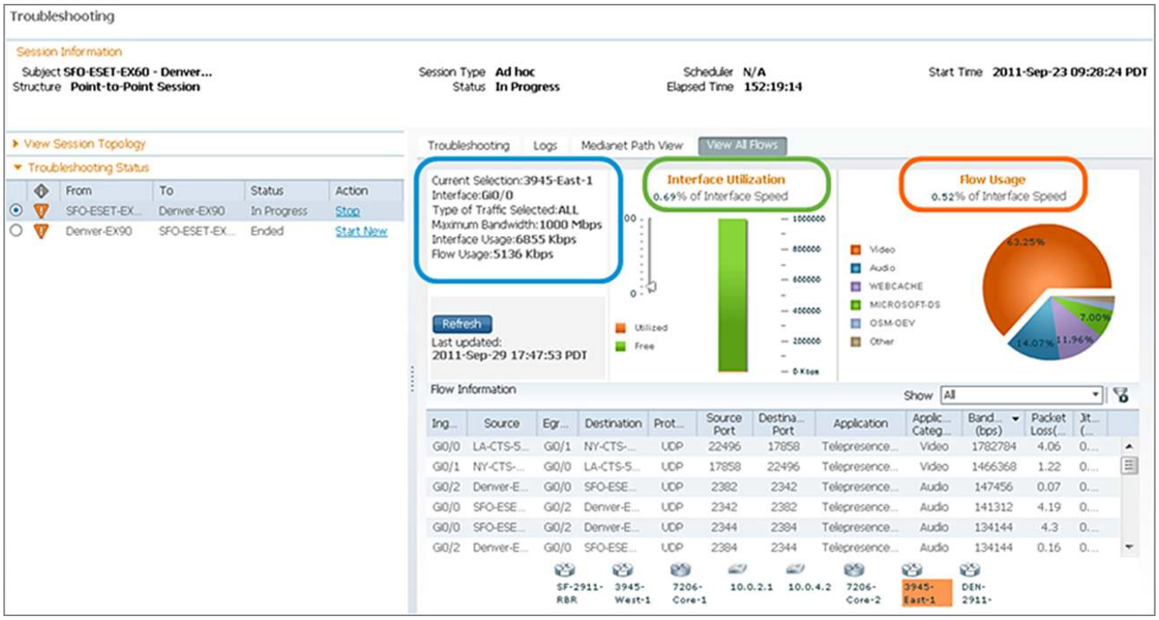
GigabitEthernet0/0 EGRESS

Select Flow data type
◉ All
○ RTP

Scheduler **N/A**
Elapsed Time **152:09:42**
Start Time **2011-Sep-23 09:28:24 PDT**

Step 6 of 6: Troubleshooting is complete.

This will bring up another summary screen which will give you a good idea of how much of the interface capacity etc is being used for this session:



Subject **SFO-ESET-EX60 - Denver...**
Structure **Point-to-Point Session**
Session Type **Ad hoc**
Status **In Progress**
Scheduler **N/A**
Elapsed Time **152:19:14**
Start Time **2011-Sep-23 09:28:24 PDT**

		From	To	Status	Action
◉		SFO-ESET-EX...	Denver-EX90	In Progress	Stop
○		Denver-EX90	SFO-ESET-EX...	Ended	Start New

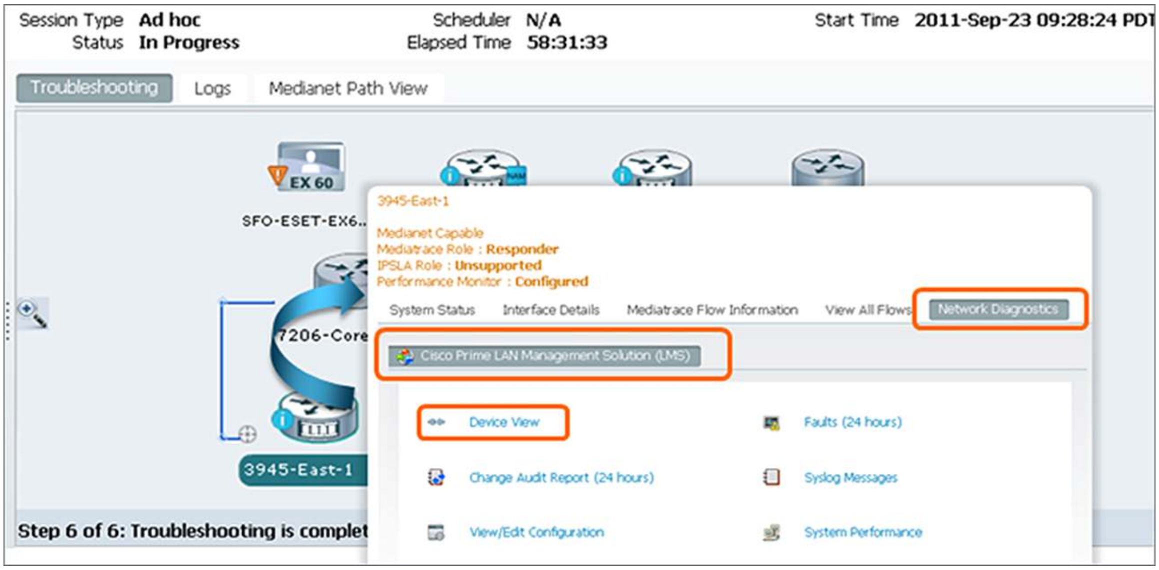
Current Selection:3945-East-1
Interface:Gi0/0
Type of Traffic Selected:ALL
Maximum Bandwidth:1000 Mbps
Interface Usage:6855 Kbps
Flow Usage:5136 Kbps

Last updated:
2011-Sep-29 17:47:53 PDT

Ing...	Source	Egr...	Destination	Prot...	Source Port	Destina... Port	Application	Applic... Categ...	Band... (bps)	Packet Loss(...	Jit... (...
Gi0/0	LA-CTS-5...	Gi0/1	NY-CTS-...	UDP	22496	17858	Telepresence...	Video	1782784	4.06	0....
Gi0/1	NY-CTS-...	Gi0/0	LA-CTS-5...	UDP	17858	22496	Telepresence...	Video	1466368	1.22	0....
Gi0/2	Denver-E...	Gi0/0	SFO-ESE...	UDP	2382	2342	Telepresence...	Audio	147456	0.07	0....
Gi0/0	SFO-ESE...	Gi0/2	Denver-E...	UDP	2342	2382	Telepresence...	Audio	141312	4.19	0....
Gi0/0	SFO-ESE...	Gi0/2	Denver-E...	UDP	2344	2384	Telepresence...	Audio	134144	4.3	0....
Gi0/2	Denver-E...	Gi0/0	SFO-ESE...	UDP	2384	2344	Telepresence...	Audio	134144	0.16	0....

Cisco Prime Collaboration Manager 1.1 also provides Integration with other Cisco Prime management systems (LMS and NAM) offering critical diagnostic information about the network along the video path.

Once you use the “Troubleshoot Session” utility from Session Monitoring as explained earlier in this document, you can click on a Medianet enabled router in the path (ISR-G2 3945 in the screen shot below) → go to “Network Diagnostics” →Cisco Prime LMS → Device View and other links.

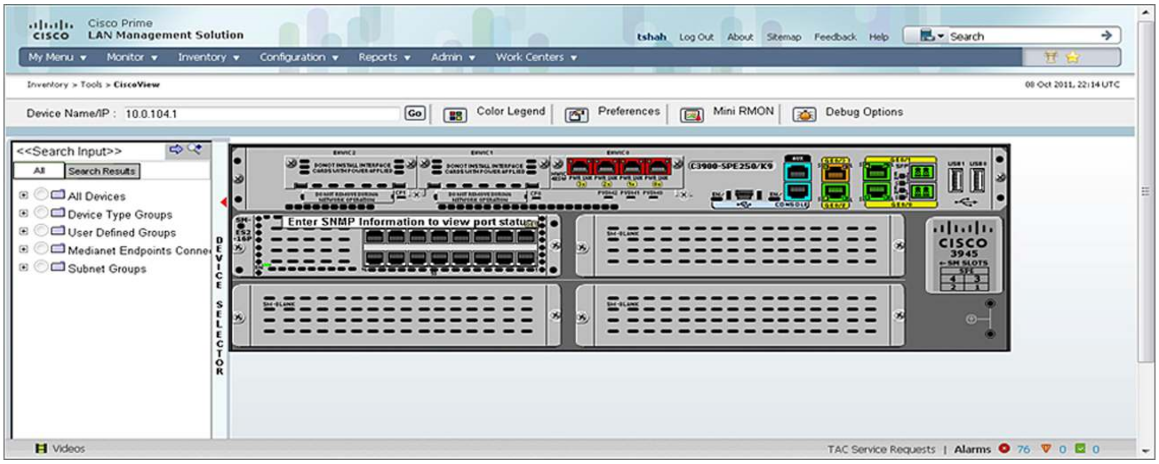


Session Type **Ad hoc** Scheduler **N/A** Start Time **2011-Sep-23 09:28:24 PDT**
Status **In Progress** Elapsed Time **58:31:33**

3945-East-1

Medianet Capable
Mediatrace Role : **Responder**
IPSLA Role : **Unsupported**
Performance Monitor : **Configured**

Step 6 of 6: Troubleshooting is complet

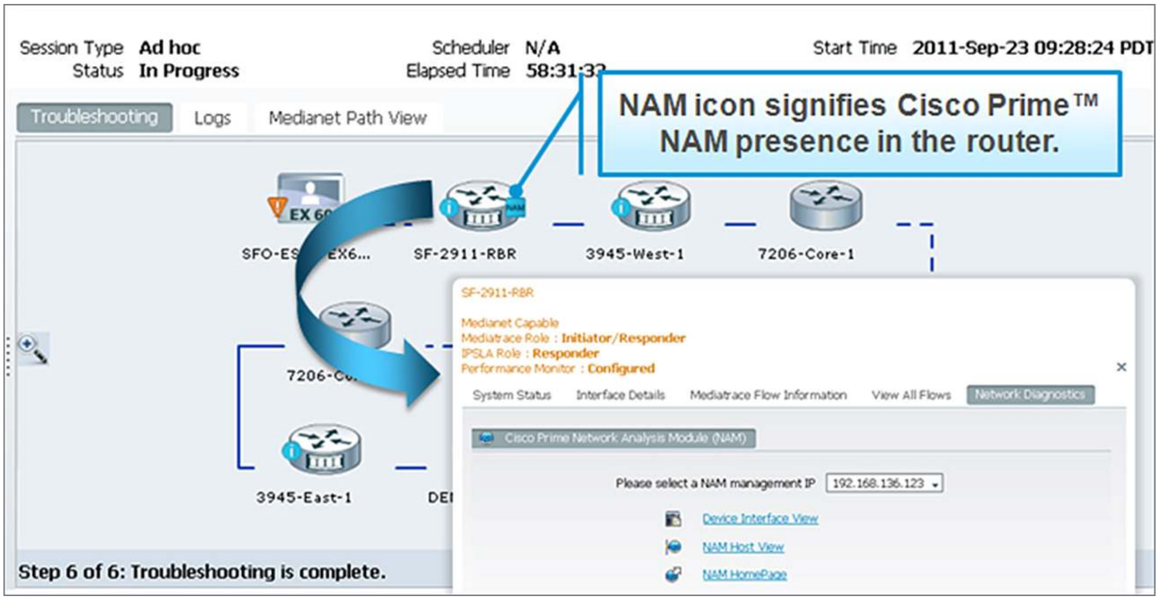


Inventory > Tools > **CiscoView** 08 Oct 2011, 22:14 UTC

Device Name/IP : 10.0.104.1

Enter SNMP Information to view port status

Cisco Prime Collaboration Manager also offers integration with Cisco Prime NAM. Once you use the “Troubleshoot Session” utility from Session Monitoring as explained earlier in this document, you can click on a NAM enabled router in the path (ISR-G2 2911 in the screen shot below) → go to “Network Diagnostics” →Cisco Prime Network Analysis Module (NAM) → Select a NAM IP and then you can get access to multiple options: Device Interface View, NAM Host View & NAM Home Page as shown below:



Session Type **Ad hoc**
Status **In Progress**
Scheduler **N/A**
Elapsed Time **58:31:32**
Start Time **2011-Sep-23 09:28:24 PDT**

NAM icon signifies Cisco Prime™ NAM presence in the router.

SF-2911-RBR

Medianet Capable
Mediatrace Role : **Initiator/Responder**
IPSLA Role : **Responder**
Performance Monitor : **Configured**

System Status
Interface Details
Mediatrace Flow Information
View All Flows
Network Diagnostics
Cisco Prime Network Analysis Module (NAM)

Please select a NAM management IP 192.168.136.123

Step 6 of 6: Troubleshooting is complete.

Cisco Prime Collaboration Manager ver 1.1 Supported Devices:

CPCM 1.1 supports Cisco TelePresence devices such as CTS, Tandberg series and many more. For a complete list of endpoints supported and their supported software versions by CPCM 1.1, please go to the following link: http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration_manager/1.1/supported/devices_alarms/devices.xls

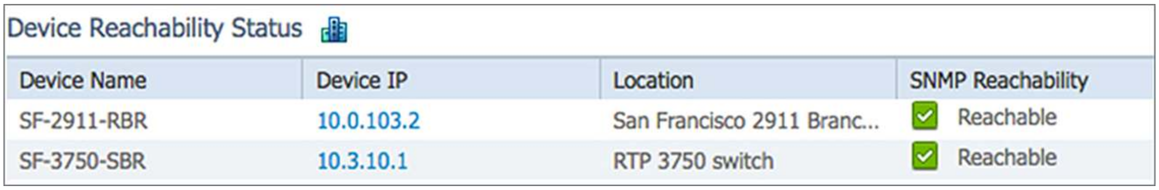
Cisco Prime Collaboration Manager ver 1.1 Supported Alarms and Events:

http://www.cisco.com/en/US/docs/net_mgmt/prime/collaboration_manager/1.1/supported/devices_alarms/events_alarms.xls

4.2.2 Application Visibility

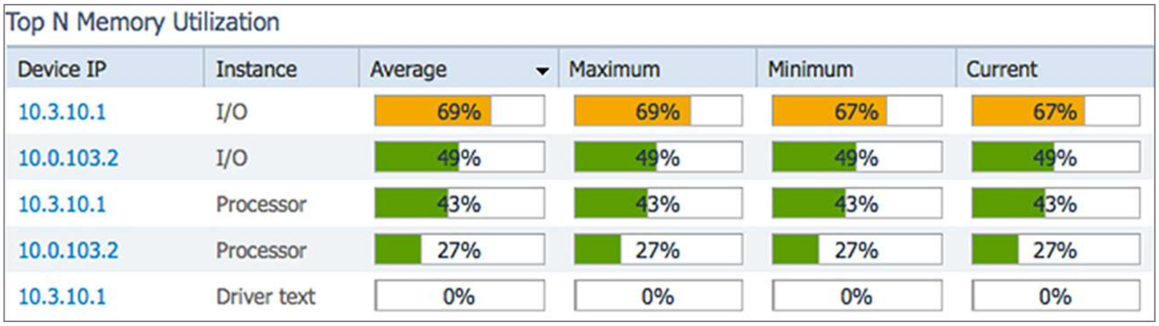
Cisco Prime Assurance Manager collects, normalizes and correlates data across multiple sources of embedded performance instrumentation, such as NetFlow, Network Based Application Recognition (NBAR), Cisco IOS® Software Performance Agent (PA) and Cisco Medianet Performance Monitor. Branch-office and headend devices capable of exporting performance metrics in Flexible NetFlow Version 9 (FNFv9) format can export information to the Cisco Prime Assurance Manager for further analysis. Additionally, CPAM monitors the health and utilization of network devices. All the data collected is presented as views into a particular Site, Interface, Application, Service or End-User while hiding the complexity of managing multiple data sources. These correlated end-to-end views, which bring together network, traffic, application and user information simplifies monitoring and accelerates troubleshooting.

The Site Dashboard below displays the health of network devices in the site, the application traffic in the site, as well as the end-user experience of applications as indicated by the transaction time.



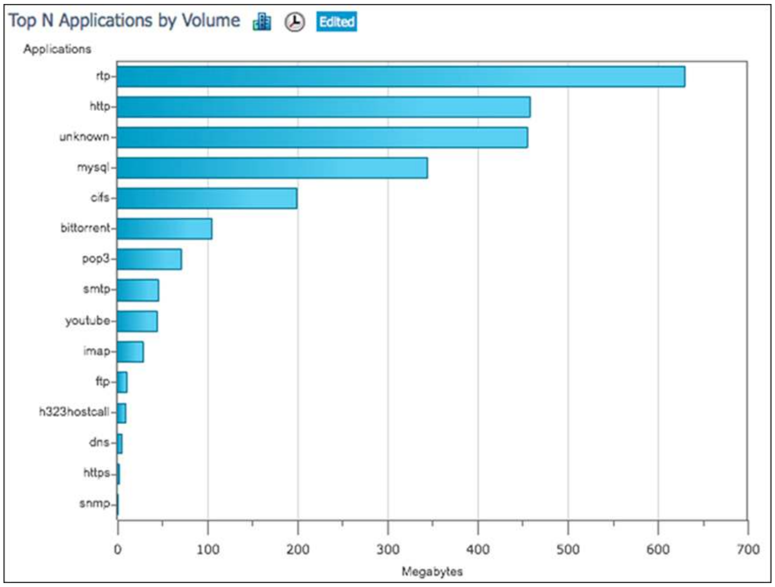
Device Reachability Status

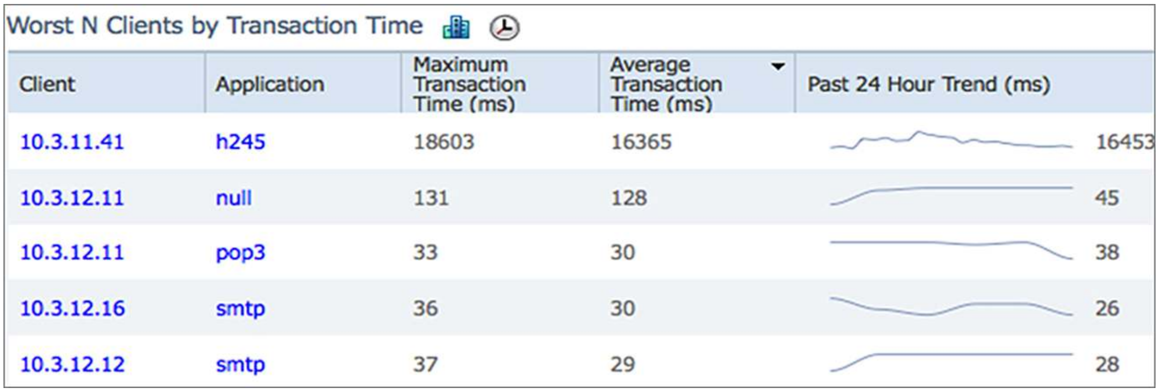
Device Name	Device IP	Location	SNMP Reachability
SF-2911-RBR	10.0.103.2	San Francisco 2911 Branc...	✓ Reachable
SF-3750-SBR	10.3.10.1	RTP 3750 switch	✓ Reachable



Top N Memory Utilization

Device IP	Instance	Average	Maximum	Minimum	Current
10.3.10.1	I/O	69%	69%	67%	67%
10.0.103.2	I/O	49%	49%	49%	49%
10.3.10.1	Processor	43%	43%	43%	43%
10.0.103.2	Processor	27%	27%	27%	27%
10.3.10.1	Driver text	0%	0%	0%	0%

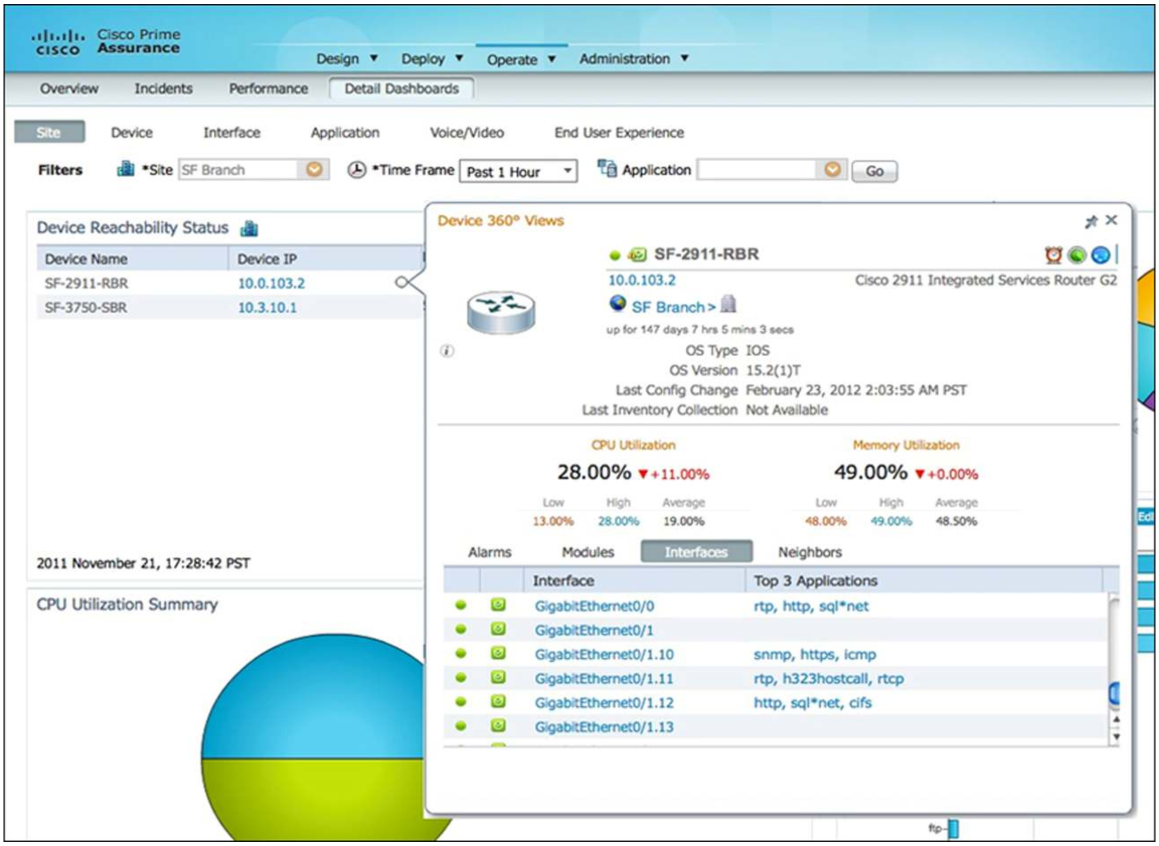




Worst N Clients by Transaction Time

Client	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms)	Past 24 Hour Trend (ms)
10.3.11.41	h245	18603	16365	16453
10.3.12.11	null	131	128	45
10.3.12.11	pop3	33	30	38
10.3.12.16	smtp	36	30	26
10.3.12.12	smtp	37	29	28

Cisco Prime Assurance Manager 1.1 also includes 360 degree views for devices. This further enables effective troubleshooting by bringing together all the device information like health, alarms, events, top application traffic on interfaces, etc into a single view. The troubleshooting context, in this case the site view, is maintained while viewing device specific information in the 360 degree window. As an example this enables the user to correlate the alarms with the configuration change, or identify which are the critical interfaces depending on which applications flow through them.



Cisco Prime Assurance

Design ▼ Deploy ▼ Operate ▼ Administration ▼

Overview Incidents Performance Detail Dashboards

Site Device Interface Application Voice/Video End User Experience

Filters *Site SF Branch *Time Frame Past 1 Hour Application Go

Device Reachability Status

Device Name	Device IP
SF-2911-RBR	10.0.103.2
SF-3750-SBR	10.3.10.1

2011 November 21, 17:28:42 PST

CPU Utilization Summary

Device 360° Views

SF-2911-RBR

10.0.103.2 Cisco 2911 Integrated Services Router G2

SF Branch >

up for 147 days 7 hrs 5 mins 3 secs

OS Type IOS
OS Version 15.2(1)T
Last Config Change February 23, 2012 2:03:55 AM PST
Last Inventory Collection Not Available

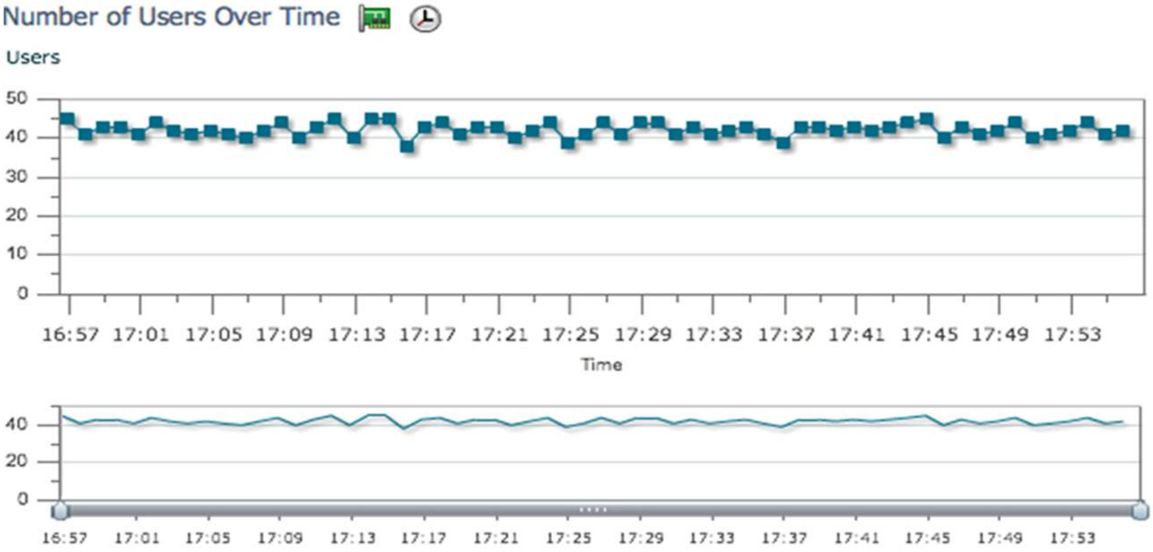
CPU Utilization: 28.00% ▼+11.00% — Low 13.00%, High 28.00%, Average 19.00%

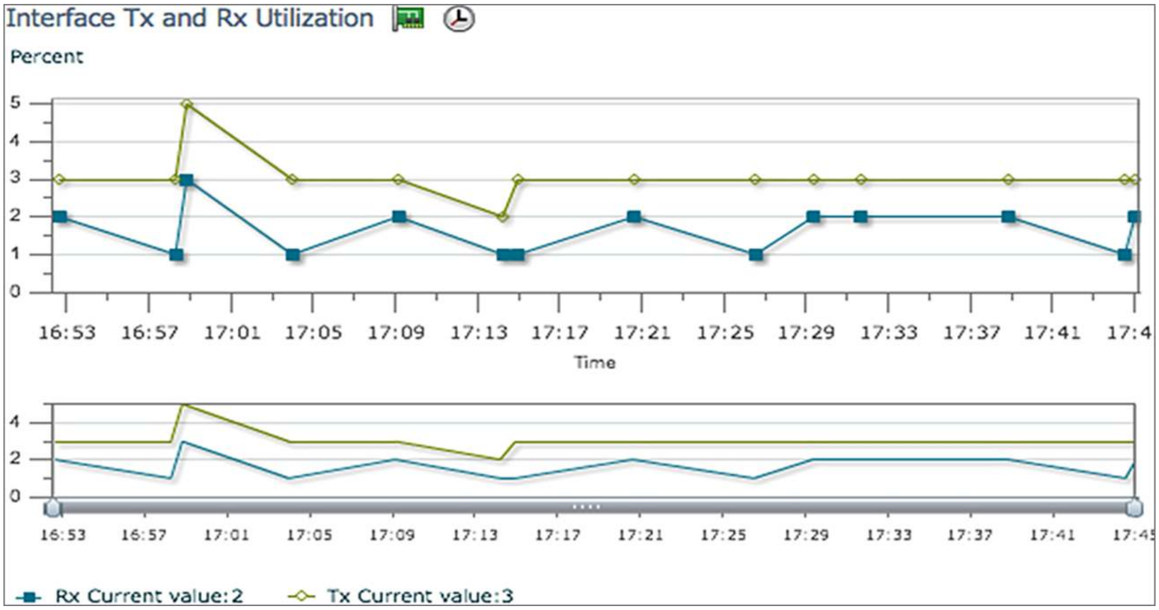
Memory Utilization: 49.00% ▼+0.00% — Low 48.00%, High 49.00%, Average 48.50%

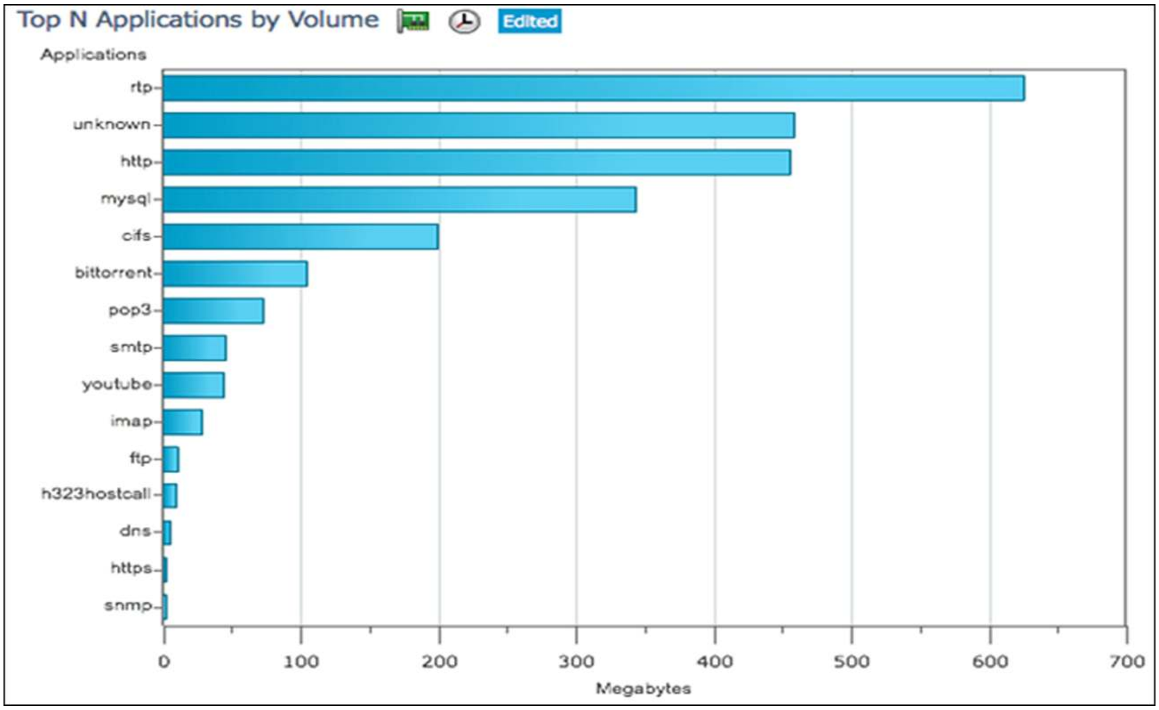
Alarms Modules Interfaces Neighbors

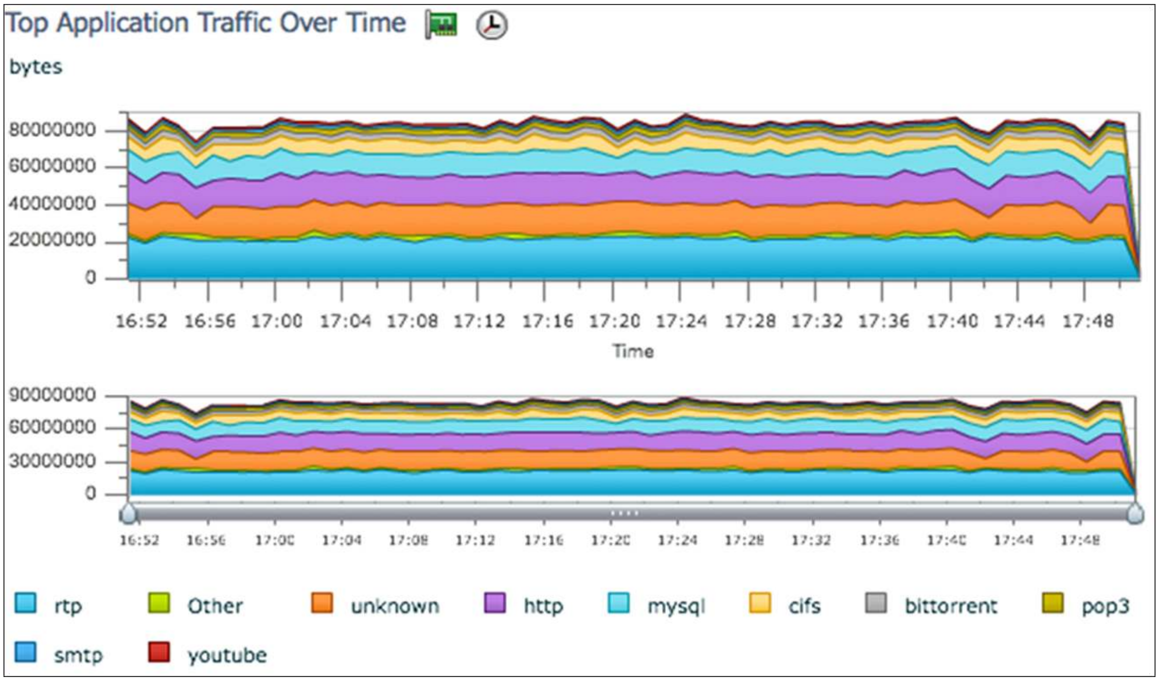
		Interface	Top 3 Applications
●	☑	GigabitEthernet0/0	rtp, http, sql*net
●	☑	GigabitEthernet0/1	
●	☑	GigabitEthernet0/1.10	snmp, https, icmp
●	☑	GigabitEthernet0/1.11	rtp, h323hostcall, rtcp
●	☑	GigabitEthernet0/1.12	http, sql*net, cifs
●	☑	GigabitEthernet0/1.13	

Clicking on a specific interface will bring up the Interface view, which further indicates the number of users on this interface, the interface utilization, the applications flowing through the interface. By selecting the WAN interface, the admin will get insight into trending and baselining of the branch usage.

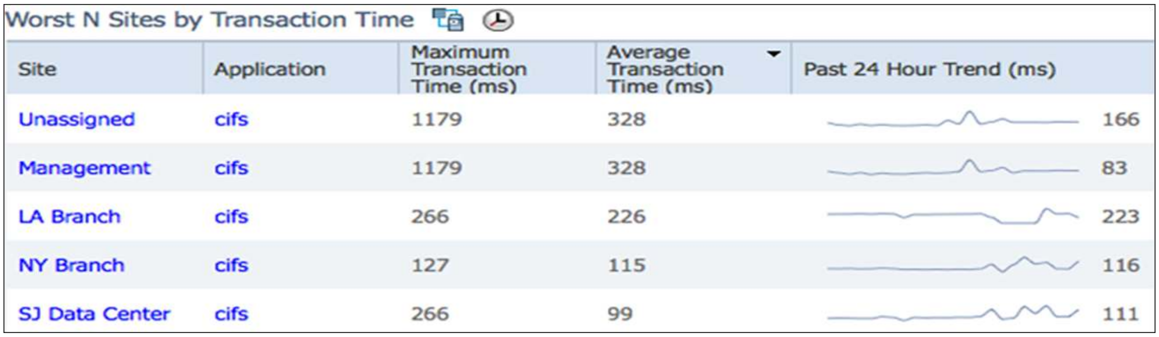



Interface Tx and Rx Utilization
Percent
5
4
3
2
1
0
16:53
16:57
17:01
17:05
17:09
17:13
17:17
17:21
17:25
17:29
17:33
17:37
17:41
17:4
Time
4
2
0
16:53
16:57
17:01
17:05
17:09
17:13
17:17
17:21
17:25
17:29
17:33
17:37
17:41
17:45
Rx Current value:2
Tx Current value:3


Top N Applications by Volume
Edited
Applications
rtp
unknown
http
mysql
cifs
bittorrent
pop3
smtp
youtube
imap
ftp
h323hostcall
dns
https
snmp
0
100
200
300
400
500
600
700
Megabytes

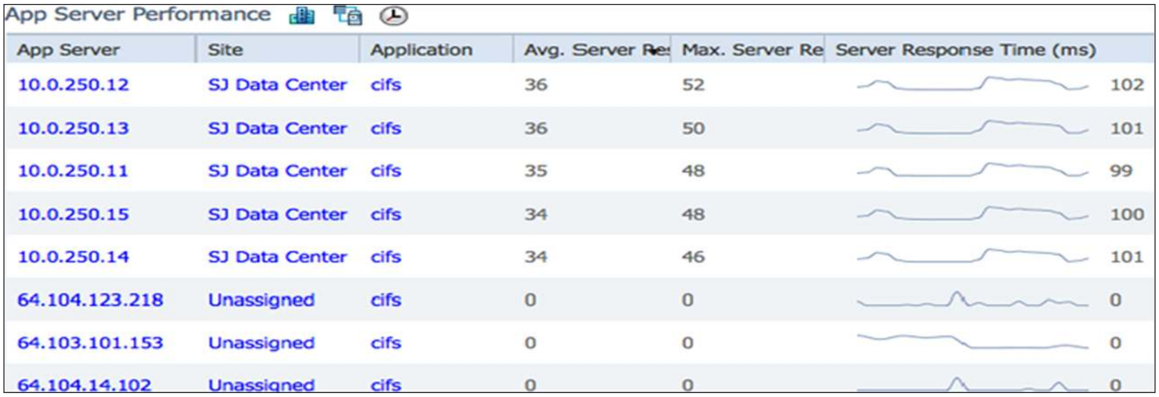


The Cisco Prime Assurance Manager can also provide end-to-end visibility into application health. The Application dashboard shows the sites having the worst experience for the application, cifs in this case. It also shows the health of the application servers, the top users of this application, the application usage trend and tools to further analyze and troubleshoot the application response time (ART).



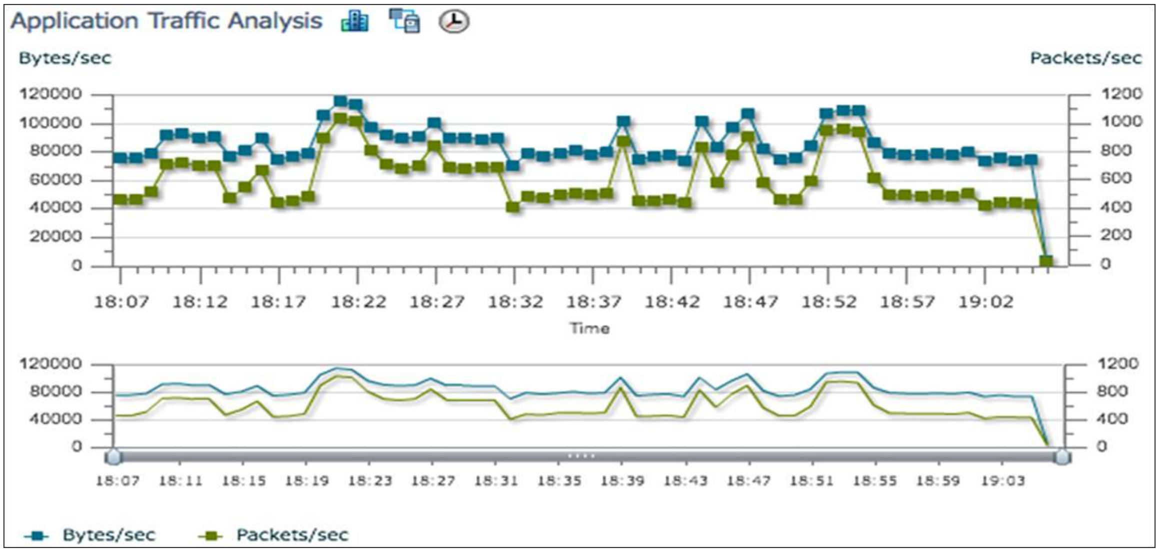
Worst N Sites by Transaction Time

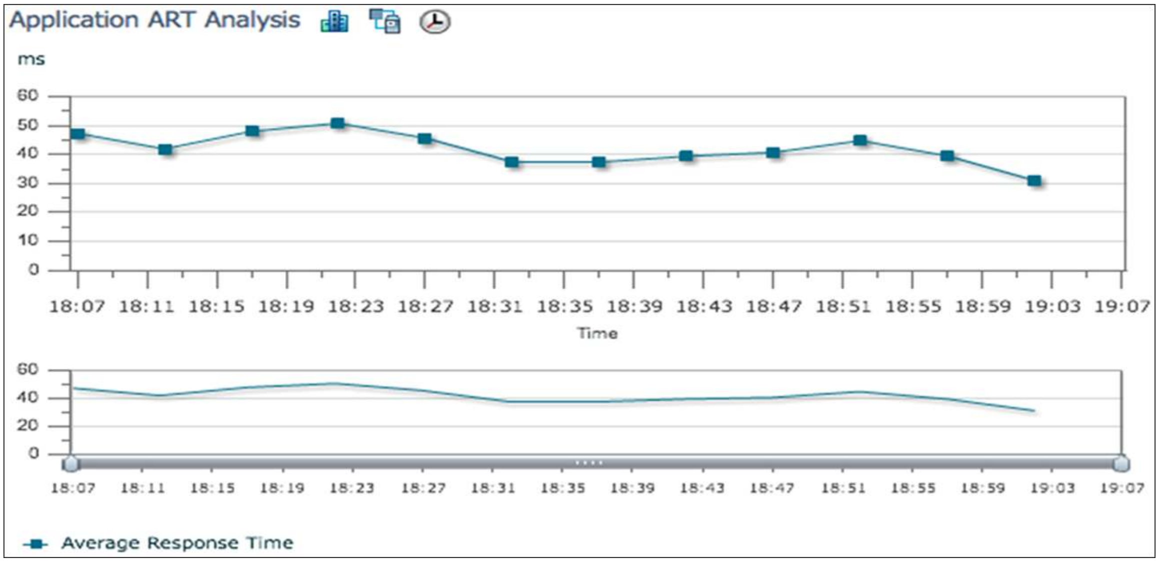
Site	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms)	Past 24 Hour Trend (ms)
Unassigned	cifs	1179	328	166
Management	cifs	1179	328	83
LA Branch	cifs	266	226	223
NY Branch	cifs	127	115	116
SJ Data Center	cifs	266	99	111



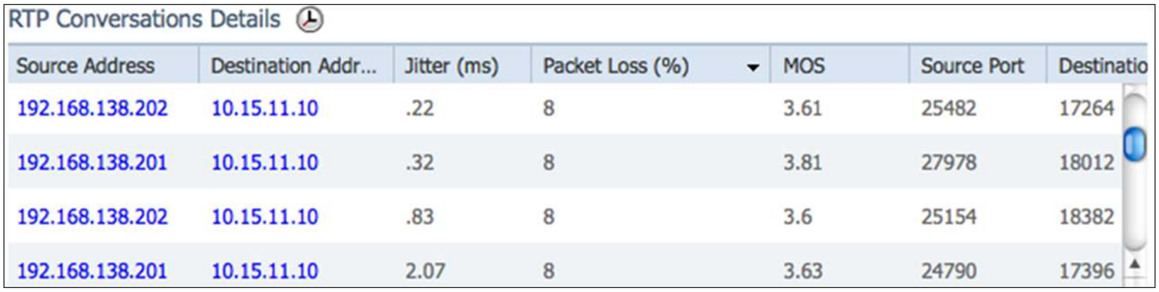
App Server Performance

App Server	Site	Application	Avg. Server Re	Max. Server Re	Server Response Time (ms)
10.0.250.12	SJ Data Center	cifs	36	52	102
10.0.250.13	SJ Data Center	cifs	36	50	101
10.0.250.11	SJ Data Center	cifs	35	48	99
10.0.250.15	SJ Data Center	cifs	34	48	100
10.0.250.14	SJ Data Center	cifs	34	46	101
64.104.123.218	Unassigned	cifs	0	0	0
64.103.101.153	Unassigned	cifs	0	0	0
64.104.14.102	Unassigned	cifs	0	0	0

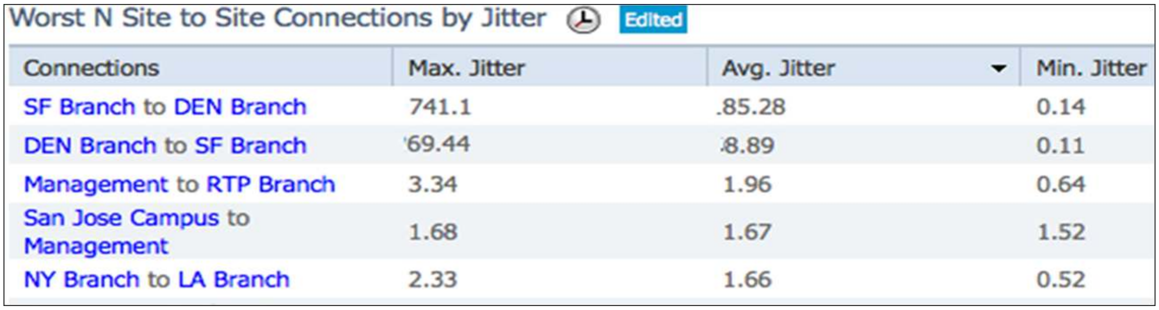




Similar to end-to-end application views, views are also available for end-to-end service performance such as Voice/Video service. The Voice/Video Dashboard shows site-to-site key performance indicators that affect service quality such as jitter and packet loss. In a large network the Cisco Prime Assurance Manager can provide service health between sites, and the Cisco Prime Collaboration Manager can be used to troubleshoot specific video sessions and identify exactly where the jitter/packet loss is getting injected between the sites.

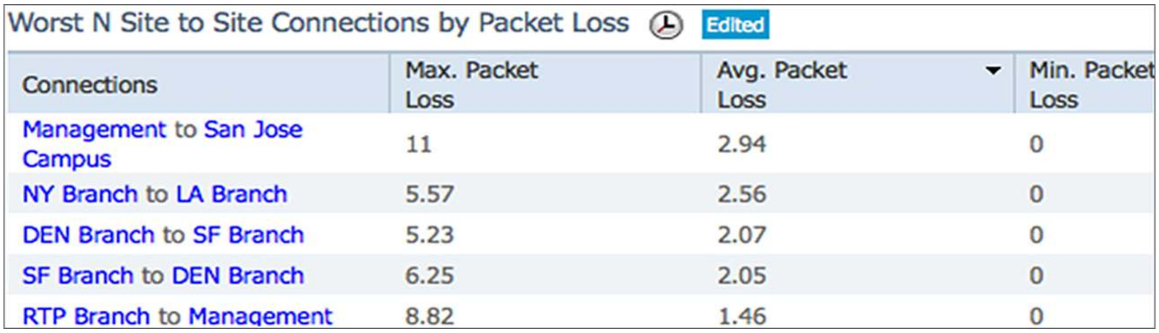

RTP Conversations Details

Source Address	Destination Addr...	Jitter (ms)	Packet Loss (%)	MOS	Source Port	Destinatio
192.168.138.202	10.15.11.10	.22	8	3.61	25482	17264
192.168.138.201	10.15.11.10	.32	8	3.81	27978	18012
192.168.138.202	10.15.11.10	.83	8	3.6	25154	18382
192.168.138.201	10.15.11.10	2.07	8	3.63	24790	17396



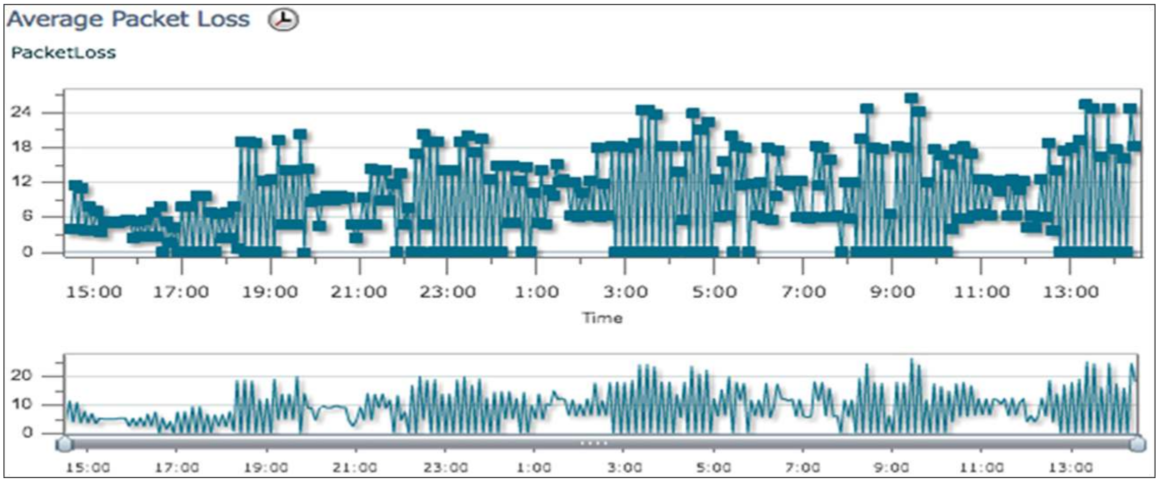
Worst N Site to Site Connections by Jitter Edited

Connections	Max. Jitter	Avg. Jitter	Min. Jitter
SF Branch to DEN Branch	741.1	.85.28	0.14
DEN Branch to SF Branch	'69.44	:8.89	0.11
Management to RTP Branch	3.34	1.96	0.64
San Jose Campus to Management	1.68	1.67	1.52
NY Branch to LA Branch	2.33	1.66	0.52



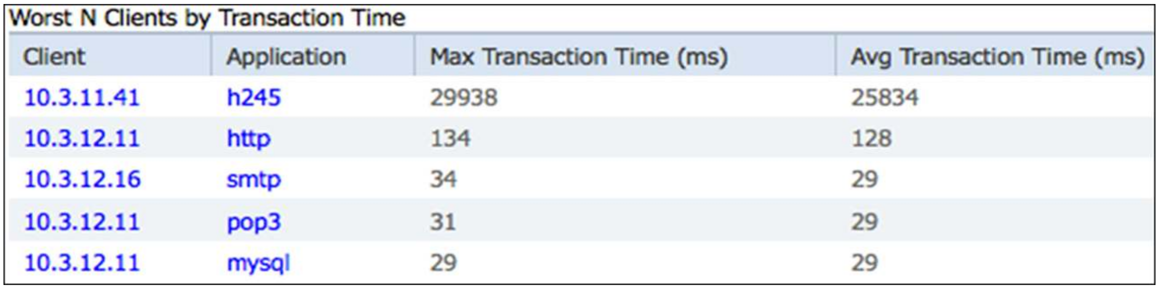
Worst N Site to Site Connections by Packet Loss Edited

Connections	Max. Packet Loss	Avg. Packet Loss	Min. Packet Loss
Management to San Jose Campus	11	2.94	0
NY Branch to LA Branch	5.57	2.56	0
DEN Branch to SF Branch	5.23	2.07	0
SF Branch to DEN Branch	6.25	2.05	0
RTP Branch to Management	8.82	1.46	0



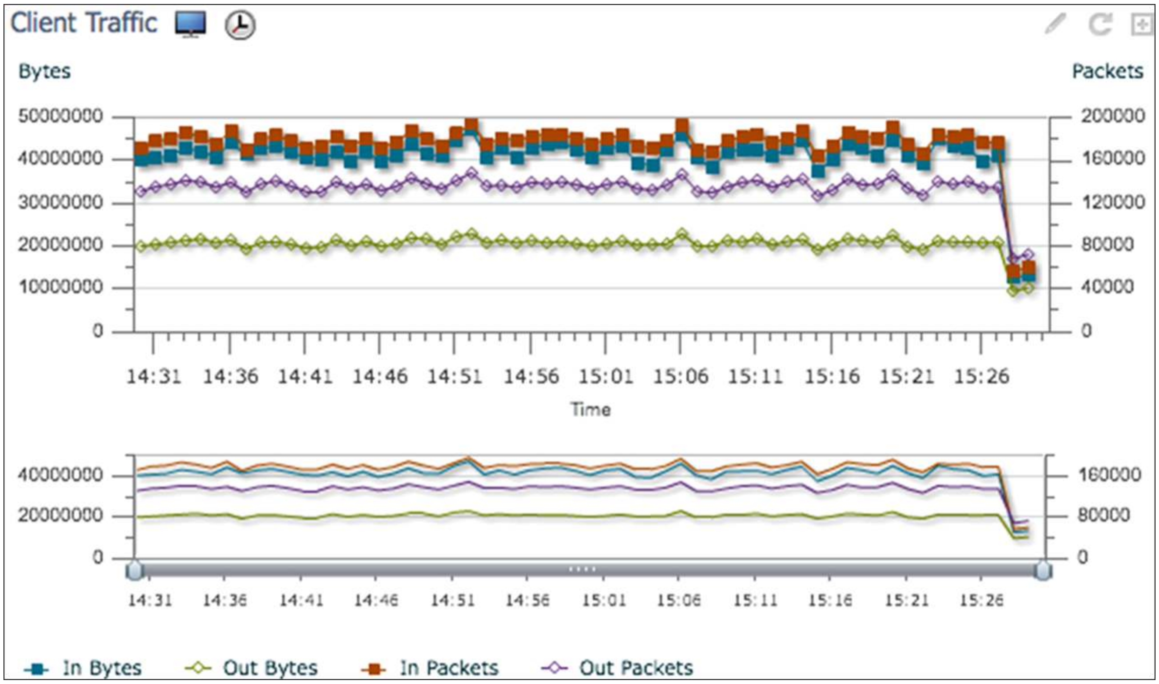
Average Packet Loss

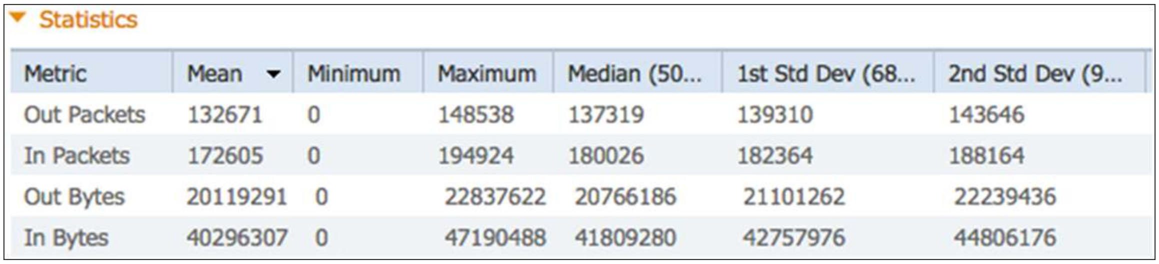
To help troubleshoot end-user experience issues, the Cisco Prime Assurance Manager provides an End-User Experience dashboard, where the specific user's experience can be compared to that of other users from the same site. This helps in insolating the issue to the user, the site, or the application.



Worst N Clients by Transaction Time

Client	Application	Max Transaction Time (ms)	Avg Transaction Time (ms)
10.3.11.41	h245	29938	25834
10.3.12.11	http	134	128
10.3.12.16	smtp	34	29
10.3.12.11	pop3	31	29
10.3.12.11	mysql	29	29

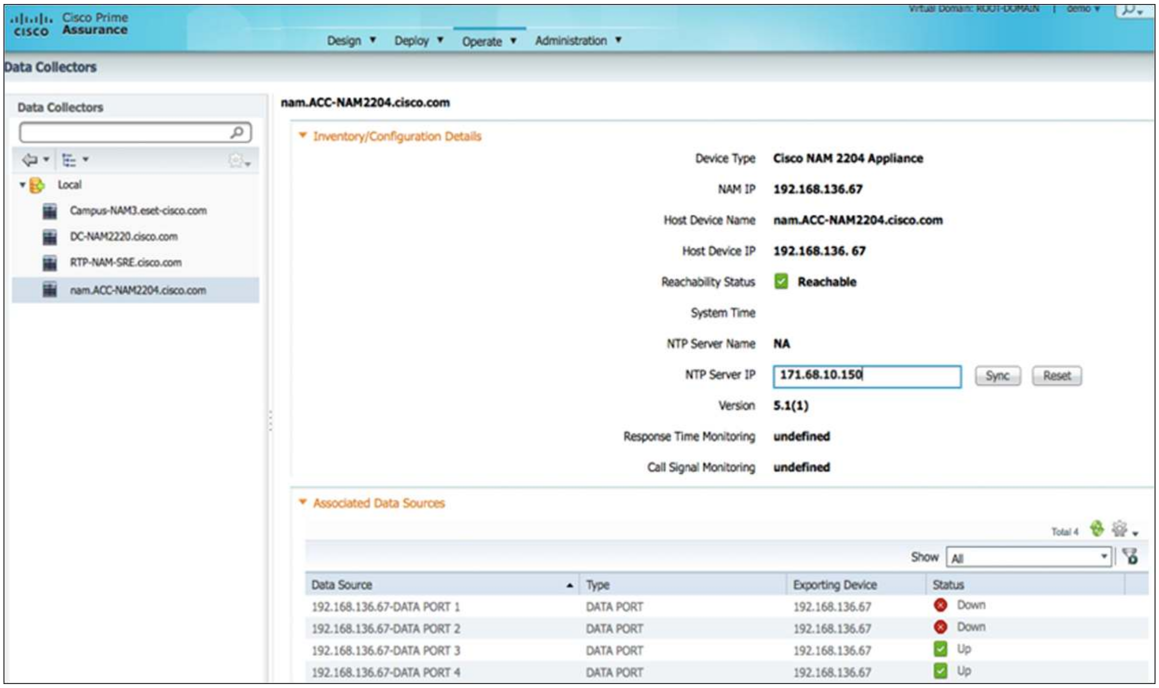




▼ Statistics

Metric	Mean ▼	Minimum	Maximum	Median (50...	1st Std Dev (68...	2nd Std Dev (9...
Out Packets	132671	0	148538	137319	139310	143646
In Packets	172605	0	194924	180026	182364	188164
Out Bytes	20119291	0	22837622	20766186	21101262	22239436
In Bytes	40296307	0	47190488	41809280	42757976	44806176

Another component of the Cisco Prime Assurance portfolio is the **Cisco Prime Network Analysis Module (NAM)**. The NAM can analyze live traffic streams and provide packet analysis capabilities for advanced troubleshooting. For visibility into WAN Optimized environments, the NAM collects information from the Cisco Wide Area Application Services (WAAS) Flow Agent (FA) and the Cisco IOS® Software Performance Agent (PA). NAM provides the network administrator with network performance dashboards such as Top-N applications, application throughput, and application response time. The Cisco Prime Assurance Manager also provides centralized management and reporting of all the NAM data from multiple NAMs.



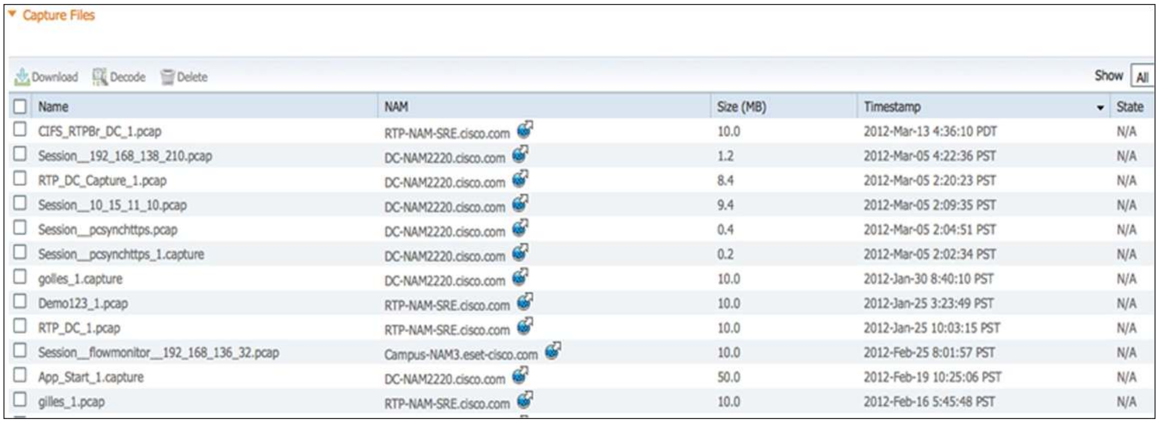
nam.ACC-NAM2204.cisco.com

▼ Inventory/Configuration Details

Device Type	Cisco NAM 2204 Appliance
NAM IP	192.168.136.67
Host Device Name	nam.ACC-NAM2204.cisco.com
Host Device IP	192.168.136. 67
Reachability Status	✓ Reachable
System Time	
NTP Server Name	NA
NTP Server IP	171.68.10.150
Version	5.1(1)
Response Time Monitoring	undefined
Call Signal Monitoring	undefined

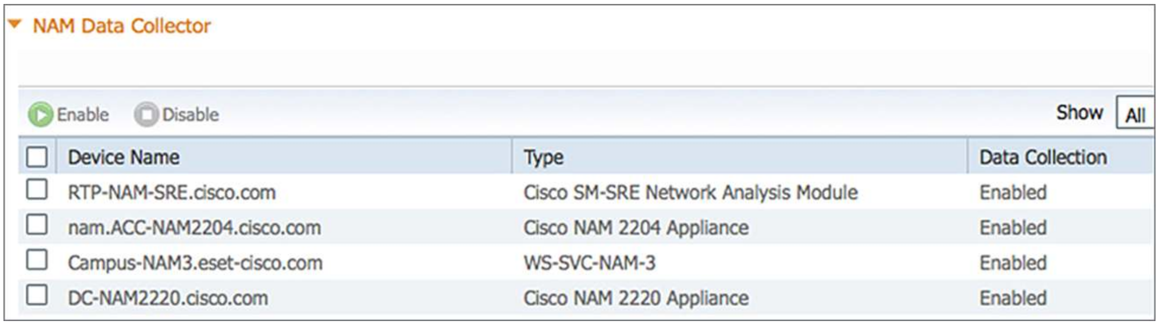
▼ Associated Data Sources

Data Source	Type	Exporting Device	Status
192.168.136.67-DATA PORT 1	DATA PORT	192.168.136.67	⊗ Down
192.168.136.67-DATA PORT 2	DATA PORT	192.168.136.67	⊗ Down
192.168.136.67-DATA PORT 3	DATA PORT	192.168.136.67	✓ Up
192.168.136.67-DATA PORT 4	DATA PORT	192.168.136.67	✓ Up



▼ Capture Files

□	Name	NAM	Size (MB)	Timestamp	State
□	CIFS_RTPBr_DC_1.pcap	RTP-NAM-SRE.cisco.com	10.0	2012-Mar-13 4:36:10 PDT	N/A
□	Session__192_168_138_210.pcap	DC-NAM2220.cisco.com	1.2	2012-Mar-05 4:22:36 PST	N/A
□	RTP_DC_Capture_1.pcap	DC-NAM2220.cisco.com	8.4	2012-Mar-05 2:20:23 PST	N/A
□	Session__10_15_11_10.pcap	DC-NAM2220.cisco.com	9.4	2012-Mar-05 2:09:35 PST	N/A
□	Session__pcsynchttps.pcap	DC-NAM2220.cisco.com	0.4	2012-Mar-05 2:04:51 PST	N/A
□	Session__pcsynchttps_1.capture	DC-NAM2220.cisco.com	0.2	2012-Mar-05 2:02:34 PST	N/A
□	golles_1.capture	DC-NAM2220.cisco.com	10.0	2012-Jan-30 8:40:10 PST	N/A
□	Demo123_1.pcap	RTP-NAM-SRE.cisco.com	10.0	2012-Jan-25 3:23:49 PST	N/A
□	RTP_DC_1.pcap	RTP-NAM-SRE.cisco.com	10.0	2012-Jan-25 10:03:15 PST	N/A
□	Session__flowmonitor__192_168_136_32.pcap	Campus-NAM3.eset-cisco.com	10.0	2012-Feb-25 8:01:57 PST	N/A
□	App_Start_1.capture	DC-NAM2220.cisco.com	50.0	2012-Feb-19 10:25:06 PST	N/A
□	gilles_1.pcap	RTP-NAM-SRE.cisco.com	10.0	2012-Feb-16 5:45:48 PST	N/A



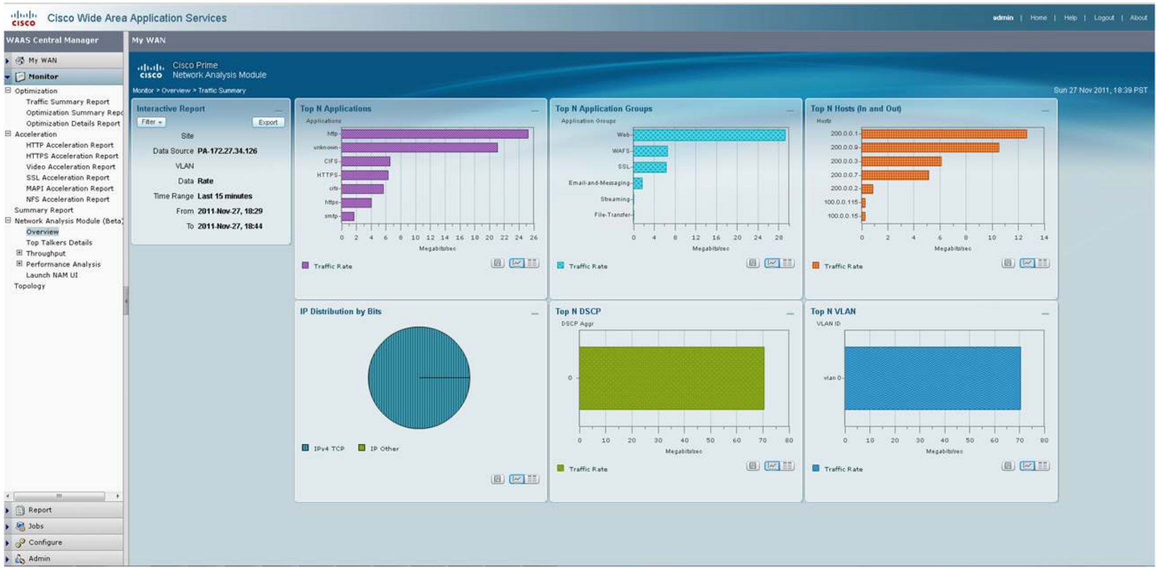
▼ NAM Data Collector

□	Device Name	Type	Data Collection
□	RTP-NAM-SRE.cisco.com	Cisco SM-SRE Network Analysis Module	Enabled
□	nam.ACC-NAM2204.cisco.com	Cisco NAM 2204 Appliance	Enabled
□	Campus-NAM3.eset-cisco.com	WS-SVC-NAM-3	Enabled
□	DC-NAM2220.cisco.com	Cisco NAM 2220 Appliance	Enabled

NAM can also be integrated with Cisco WAAS Central Manager (CM) to provide the network administrator with a combined view of the network performance, user experiences, and optimization statistics.

WAN optimization technology such as Cisco WAAS uses TCP proxy, which splits a TCP connection into multiple segments within the network (client segment, WAN segment, and server segment). Traditional network performance reporting, which relies on Switched Port Analyzer (SPAN), may not be able to accurately provide the application response time. Cisco Prime NAM fully interoperates with Cisco WAAS to correctly report application response time with WAN optimization. The network administrator can use application response time information along with optimization statistics to quantify WAN optimization ROI.

The following screenshot shows the NAM dashboard accessible through Cisco WAAS CM. From the WAAS CM menu, select **Monitor > Network Analysis Module > Overview** to display high-level information about applications at the chosen site such as Top-N Applications, Top-N Hosts, etc.



Interactive Report

Site

Data Source PA-172.27.34.126

VLAN

Data Rate

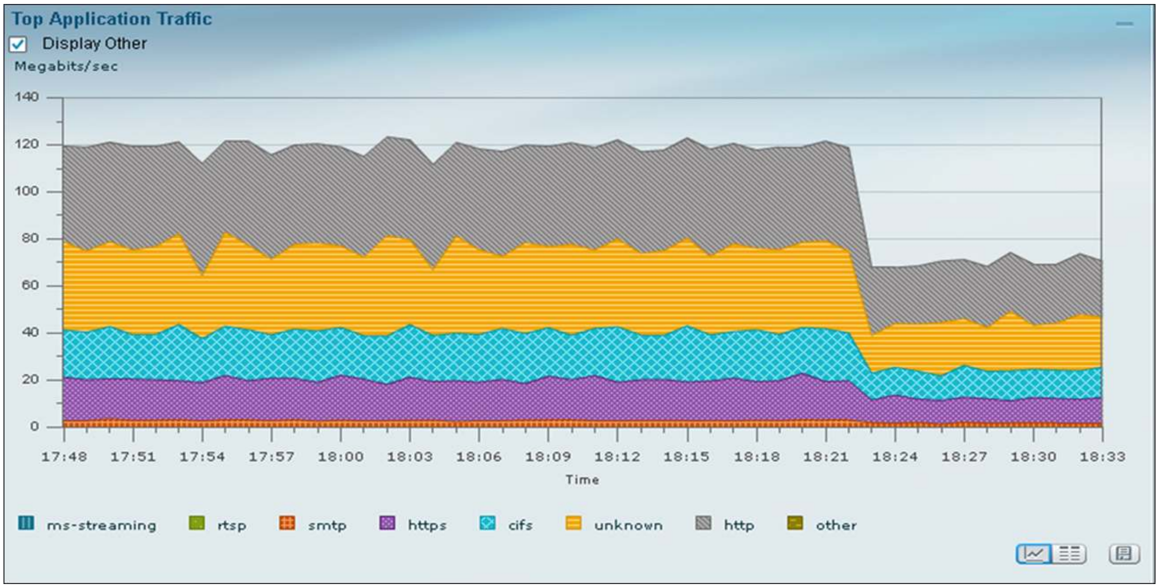
Time Range Last 15 minutes

From 2011-Nov-27, 18:29

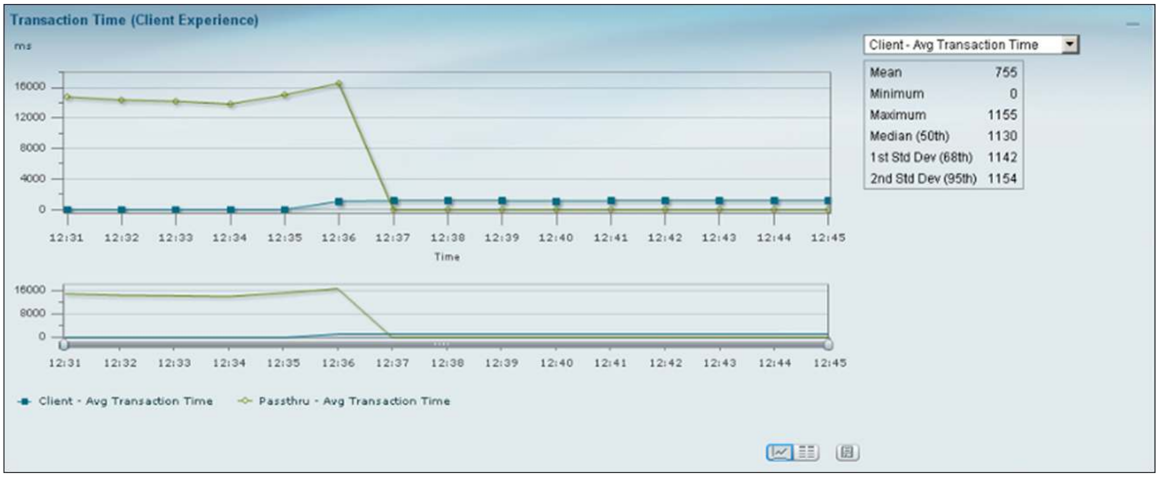
To 2011-Nov-27, 18:44

From the same WAAS Central Manager menu, the network administrator can find more information about the application throughput (volume) over time by selecting **Monitor > Network Analysis Module > Throughput > Top Applications**.

The following screenshot shows the change in traffic rate after applying traffic shaping:



NAM can also provide response-time information that is collected from either Cisco IOS Performance Agent available within a Cisco Integrated Services Routers Generation 2 (ISR G2) router, or WAAS Flow Agent available within all WAAS appliances. Response time provides information about the transaction time and the server delay that is relevant to measuring or quantifying user experience accessing applications. Go to **Monitor > Network Analysis Module > Performance Analysis > Application** to see the transaction time. The screenshot shows a significant improvement in application transaction time after enabling WAN optimization.



Mean	755
Minimum	0
Maximum	1155
Median (50th)	1130
1st Std Dev (68th)	1142
2nd Std Dev (95th)	1154

The table below lists the hardware and software products for NGEW RWAN.

Product List

Role	Hardware or Software	Software Version
Standard branch office	Cisco 2951 Integrated Services Router (ISR) High-density packet voice video digital signal processor module for Cisco Unified Communications Solutions (PVDM3-256)	IOS 15.2(2)T1

Role	Hardware or Software	Software Version
High-end branch office	Cisco 3945 ISR PVDM3-256	15.2(2)T1
Headend router	Cisco ASR 1006 Aggregation Services Router	IOS XE Rls 3.5
Device management and configuration	Cisco Prime LMS	4.2
Video monitoring and troubleshooting	Cisco Prime Collaboration Manager	1.1
Application Visibility	Cisco Prime Assurance Manager	1.1
Application Visibility	Cisco Prime Network Analysis Module (NAM)	5.1(2)
Cisco WAAS management	Cisco WAAS Central Manager	4.4
Call control	Cisco Unified Communications Manager	8.6

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

C07-706128-00 06/12