Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

Network Analysis and Reporting Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2011 are the "August 2011 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the forum at the bottom of one of the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

What's In This SBA Guide

About SBA

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

For more information, see the *How to Get Started with Cisco SBA* document:

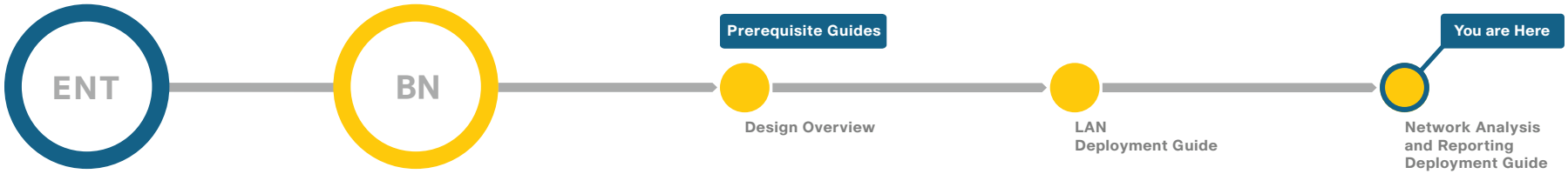
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

About This Guide

This *additional deployment guide* includes the following sections:

- **Business Overview**—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- **Technology Overview**—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- **Deployment Details**—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

Business Overview

Businesses rely on enterprise applications to help ensure efficient operations and gain competitive advantage. At the same time, IT is challenged with managing application delivery in an environment that is dynamic and distributed. The number of business applications is growing, application architectures are increasingly complex, application traffic is proliferating, and traffic patterns are difficult to predict.

In addition, driven by security, regulatory, and economic considerations, enterprises are embracing data center consolidation, server and desktop virtualization, and network and application convergence. Because of this confluence of new business demands, comprehensive application and network-visibility is no longer simply nice-to-have but is business critical. This visibility is now essential to achieving increased operational efficiency and to successfully manage the overall end-user experience.

Technology Overview

Cisco Prime Network Analysis Module (NAM), part of the overall Cisco Prime solution, is a product that:

- Provides advanced network instrumentation on the user-services layer in order to support data, voice and video services.
- Allows network administrators, managers, and engineers to gain visibility into the user-services layer with a simple workflow approach—from monitoring overall network health to analyzing a variety of detailed metrics to troubleshooting with packet-level details.
- Supports network-services layers such as application optimization
- Offers a versatile combination of real-time traffic analysis, historical analysis, packet capture capabilities, and the ability to measure user-perceived delays across the WAN.
- Provides a uniform instrumentation layer that collects data from a variety of sources, and then analyzes and presents the information. This information is available through an onboard web-based graphical user interface, and you can also export it to third-party applications.

From a Cisco SBA enterprise deployment perspective, Cisco Catalyst 6500 Series Network Analysis Module (NAM-1/NAM-2) is deployed in the Cisco Catalyst 6500 Series Switch found in enterprise core (see Figure 1). Cisco NAM-1/NAM-2 takes advantage of backplane integration by simplifying manageability, lowering total cost of ownership, reducing network footprint, and reducing rack space. Cisco NAM-2 monitors traffic on the Catalyst 6500 switch via two internal 1 Gigabit data ports while Cisco NAM-3 monitors traffic via two internal 10 Gigabit data ports.

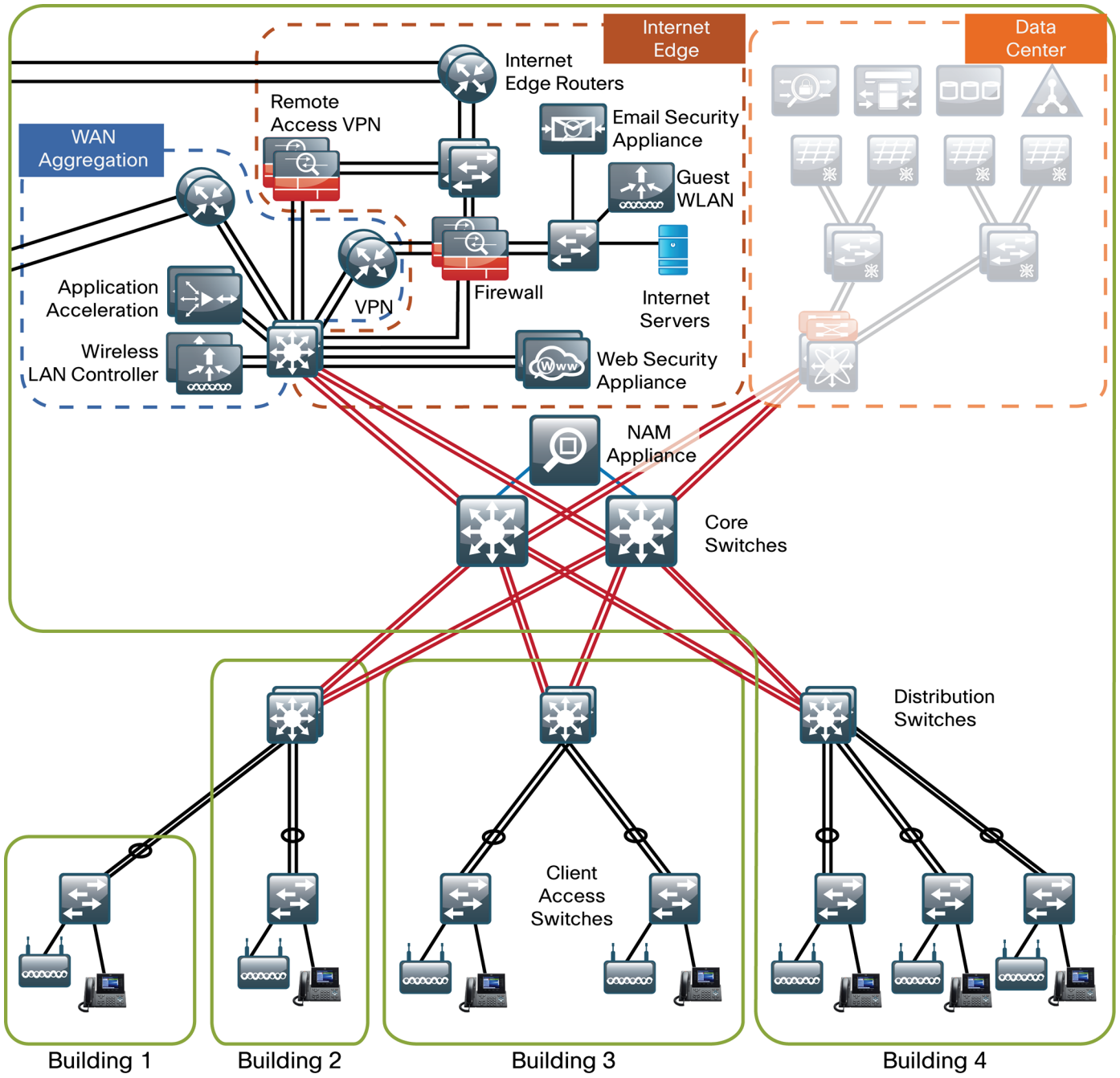
As an alternate option, Cisco NAM 2220 Appliance can be deployed in the enterprise core (see Figure 1). The Cisco NAM 2220 appliance monitors traffic from two Catalyst 6500 series switches via two 10 Gigabit interfaces.

Both Cisco NAM-1/NAM-2 and Cisco NAM 2220's placement is effective in helping you monitor, measure, and report on the network's health at the enterprise core.

Cisco Prime NAM on SRE 700 or 900 series as part of ISR G2 is deployed in the regional office (see Figure 2) to help you monitor, measure, and report on the network's health at the branch level.

For more information regarding the Cisco SBA enterprise network, see the LAN Deployment Guide under "Borderless Networks SBA Guides for Enterprises" on the following page: http://www.cisco.com/go/sba

Figure 1 - Cisco NAM providing network and application intelligence in Cisco SBA



Real-Time and Historical Application Monitoring

Cisco Prime NAM monitors traffic in real time and provides a variety of analytics. Cisco Prime NAM delivers on-demand historical analysis from the data collected. In this category of monitoring are application recognition, analysis of top conversations, hosts, protocols, differentiated services code points, and VLANs. More advanced processing includes:

- Application performance analytics, including response time measurements and various user-experience-related metrics
- Voice quality monitoring, which includes the ability to detect real-time streaming protocol streams and compute the mean opinion score, jitter, packet loss, and other VoIP metrics.

Application and Service Delivery with Application Performance Intelligence

To accurately assess the end-user experience, Cisco Prime NAM delivers comprehensive application performance intelligence (API) measurements. Cisco Prime NAM analyzes TCP-based client/server requests and acknowledgements, to provide transaction-aware response time statistics such as client delay, server delay, network delay, transaction times, and connection status. This data can help you isolate application problems to the network or to the server. It can also help you quickly diagnose the root cause of the delay and thus resolve the problem while minimizing end-user impact.

API can assist busy IT staff in troubleshooting application performance problems, analyzing and trending application behavior, identifying application consolidation opportunities, defining and helping ensure service levels, and performing pre- and post- deployment monitoring of application optimization and acceleration services.

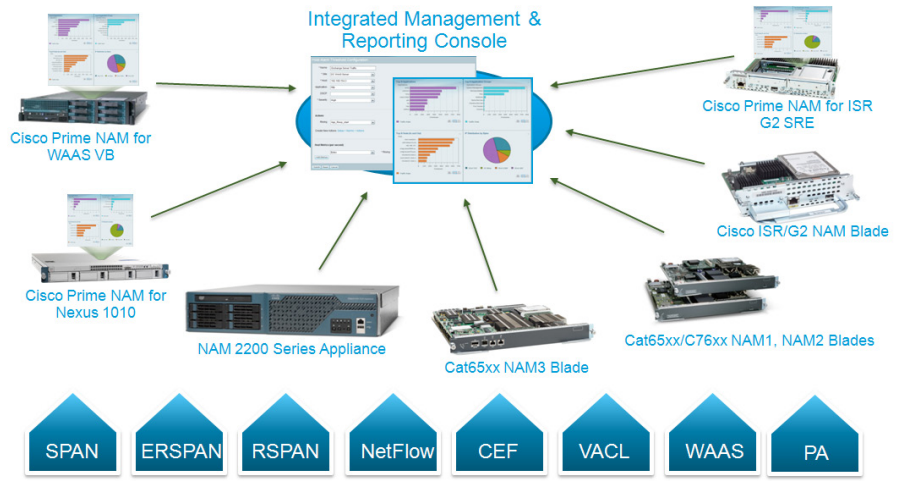
Simplified Problem Detection and Resolution

With Cisco Prime NAM, you can set thresholds and alarms on various network parameters—such as increased utilization, severe application response delays, and voice quality degradation—and be alerted to potential problems. When one or more alarms are triggered, Cisco Prime NAM can send an email alert, generate a syslog or SNMP trap, and automatically capture and decode the relevant traffic to help resolve the problem. Using a browser, the administrator can manually perform captures and view decodes through the Traffic Analyzer GUI while the data is still being captured. The capture and decode capability of the Cisco Prime NAM provides depth and insight into data analysis by using trigger-based captures, filters, decodes, a capture analysis, and error scan toolset in order to quickly pinpoint and resolve problem areas.

Cisco Prime NAM Data Sources and Export Capabilities

In the context of Cisco Prime NAM, a data source refers to a source of traffic whose entire stream, or summaries of data from that stream, is sent to the Cisco Prime NAM for monitoring. Cisco Prime NAM can monitor a variety of data sources and compute appropriate metrics. Figure 2 provides a snapshot of all possible sources of data and also the various export mechanisms supported by Cisco Prime NAM.

Figure 2 - Data sources for Cisco Prime NAM



This figure shows Cisco Prime NAM's role as a mediation layer tool—collecting and analyzing network data from a variety of sources and displaying the results on an integrated management and reporting console and optionally providing data to northbound applications via REST/XML interface.

Using the SPAN feature, Cisco Prime NAMs can monitor traffic from physical ports, virtual LANs (VLANs), or Cisco EtherChannel connections of the local switch or router. To support the selective monitoring of large amounts of traffic or the gathering of traffic from WAN interfaces, VLAN access control list (VACL) can filter traffic before it is sent to Cisco Prime NAMs. NetFlow can provide analysis of real-time and historical traffic usage to obtain a broad view of how the network is performing. Remote SPAN (RSPAN) or Encapsulated Remote SPAN (ERSPAN) extends troubleshooting to remote

parts of the network. Using Cisco Express Forwarding (CEF), Cisco Prime NAM directly monitors and analyzes the WAN data streams from the packets traversing the router interfaces to the internal Cisco NAM interface. WAAS Flow Agent from WAE provides key data about the pre- and post-optimized network. This allows Cisco Prime NAM to identify potential candidates for WAN optimization based on Flow Agent data. Cisco Performance Agent (PA) is a licensed software feature of Cisco IOS that encapsulates application performance analytics, traffic statistics, and WAN optimization metrics in a NetFlow Version 9 template-based format and reports to the Cisco Prime NAM. Cisco PA provides visibility into branch-office applications traffic and performance. By using the instrumentation built into the Cisco infrastructure, Cisco Prime NAM offers more ways to see and understand what's happening on your network.

Notes

Deployment Details

This section describes how to configure the Cisco Catalyst 6500 Series Network Analysis Module (NAM-2), Cisco NAM 2220 appliance and Cisco Prime NAM on Cisco ISR G2 SRE to establish network connectivity, configure IP parameters, and how to perform other required administrative tasks by using the Cisco Prime NAM command line interface. This section also provides information about how to get started with the Cisco Prime NAM graphical user interface (GUI) and how to perform various system management tasks.

Process

Configuring the Cisco Catalyst 6500 Series Network Analysis Module (NAM-2)

1. Install Cisco NAM-2
2. Secure Cisco NAM-2
3. Log into the NAM Traffic Analyzer GUI
4. Verify SNMP
5. Verify the managed device parameters
6. Create a SPAN session for capture
7. Set up sites
8. View the home dashboard

Requirements:

- Cisco Catalyst 6500 Series Switch
- Open slot for Cisco NAM-2
- At least one Supervisor – SUP 32, SUP 720, SUP 720-10G or SUP 2T.
- IOS release version – refer to Cisco Catalyst 6500 Series Switch NAM Install and Configuration Note 5.1
- One Cisco Catalyst 6500 Series Network Analysis Module (WS-SVC-NAM-2-250S).

Procedure 1 Install Cisco NAM-2

Step 1: In the Cisco Catalyst 6500 Switch, insert Cisco NAM into any available slot (except the slot reserved for supervisor modules).

Step 2: Verify Cisco NAM is running.

```
C6509-1#show module
Mod Ports Card Type                       Model              Serial No.
--- ----- ------------------------------  -----------------  -----------
1   24    CEF720 24 port 1000mb SFP       WS-X6724-SFP       SAL1016K987
2   8     Network Analysis Module         WS-SVC-NAM-2       SAD1224014K
4   8     DCEF2T 8 port 10GE              WS-X6908-10G       SAL1537PGGQ
5   5     Supervisor Engine 2T 10GE w/ CTS (Acti VS-SUP2T-10G   SAL1534NB4Q

Mod MAC addresses                       Hw     Fw       Sw        Status
--- ----------------------------------- ------ ------------ -----
1  0017.9431.ec4c to 0017.9431.ece7 2.5 12.2(14r)S5 15.0(1)SY  Ok
2  001f.ca08.411a to 001f.ca08.4178 4.3 7.2(1)      5.1(2)     Ok
4  0007.7d90.8950 to 0007.7d90.8a97 1.0 12.2(50r)SYL 15.0(1)SY Ok
5  44d3.ca7b.c840 to 44d3.ca7b.c97d 1.1 12.2(50r)SYS 15.0(1)SY Ok

Mod  Sub-Module             Model     Serial      Hw         Status
---- --------------------------- ------------------ -----------
1  Centralized Forwarding Card WS-F6700-CFC  SAL1103E6RC  3.1  Ok
4  Distributed Forwarding Card WS-F6K-DFC4-E SAL1537PP27  1.0  Ok
5  Policy Feature Card 4       VS-F6K-PFC4   SAL1535P6WS  1.0  Ok
5  CPU Daughterboard           VS-F6K-MSFC5  SAL1537PPAT  1.1  Ok
```

```
Mod   Online Diag Status
----  -------------------
  1   Pass
  2   Pass
  4   Pass
  5   Pass
```

Step 3: Configure a management VLAN for Cisco NAM.

```
vlan [id]
interface vlan [id]
ip address [ip-address] [subnet]
exit
analysis module [slot] management-port access-vlan [id]
end
```

Example:

```
vlan 141
!
interface Vlan141
 ip address 10.4.41.1 255.255.255.252
!
analysis module 2 management-port access-vlan 141
```

Step 4: Open a session into Cisco NAM.

```
session slot [module-number] processor 1
```

Step 5: Log in to Cisco NAM using the username **root** and default password **root**.

```
Cisco Prime Network Analysis Module
nam.localdomain login: root
Password: root
Cisco Network Analysis Module (WS-SVC-NAM-2) Console, 5.1(2)
Copyright (c) 1999-2011 by Cisco Systems, Inc.
```

Step 6: You must change the root password.

```
System Alert! Default password has not been changed!
Please enter a new root user password.
Enter new UNIX password:******
Enter the new password for the root user.
Retype new UNIX password:*******
passwd: password updated successfully
root@nam.cisco.local#
```

Step 7: Configure Cisco NAM for network connectivity:

```
ip address [ip-address] [subnet-mask]
ip gateway [ip-address]
ip domain [domain-name]
ip host [name]
ip nameserver [ip-address]
```

Example:

```
root@nam.localdomain# ip address 10.4.41.2 255.255.255.252
root@nam.localdomain# ip gateway 10.4.41.1
root@nam.localdomain# ip domain cisco.local
root@nam.cisco.local# ip host nam
root@nam.cisco.local# ip nameserver 10.4.48.10
```

Step 8: Verify that the network configuration is as shown.

```
root@nam.cisco.local# show ip
IP ADDRESS:             10.4.41.2
SUBNET MASK:            255.255.255.252
IP BROADCAST:           10.4.41.3
DNS NAME:               NAM.CISCO.LOCAL
DEFAULT GATEWAY:        10.4.48.1
NAMESERVER(S):          10.4.48.10
HTTP SERVER:            DISABLED
HTTP SECURE SERVER:     DISABLED
HTTP PORT:              80
HTTP SECURE PORT:       443
TACACS+ CONFIGURED:     NO
TELNET:                 DISABLED
SSH:                    DISABLED
```

Procedure 2 Secure Cisco NAM-2

To increase security for the NAM, in this section you will:

- Enable Secure Sockets Layer (SSL) on the NAM for secure, encrypted HTTP sessions.
- Enable Secure Shell (SSH) Protocol for secure Telnet to NAM.

Step 1: Download the crypto patch from the following location: http://www.cisco.com/cisco/software/navigator.html

Step 2: Navigate to **Network Management and Automation** > **Network Analysis Module (NAM) Products** > **appropriate NAM form-factor** > **All Releases** > **5** > **5.1.2**.

Step 3: Click **Download Now** on the following file: **nam-app.5-1-2.cryptoK9.patch.1-0.bin**

Step 4: Apply the crypto patch.

Step 5: Copy the crypto patch to a directory accessible to FTP.

Step 6: Install the patch.

```
root@nam.cisco.local# patch [ftp-url]
```

where **ftp-url** is the FTP location and the name of the strong crypto patch.

Example:

```
root@nam.cisco.local# patch ftp://10.4.48.11/nam-app.5-1-2.cryptoK9.patch.1-0.bin
Proceeding with installation. Please do not interrupt.
If installation is interrupted, please try again.
Downloading nam-app.5-1-2.cryptoK9.patch.1-0.bin. Please wait...
ftp://10.4.48.11/nam-app.5-1-2.cryptoK9.patch.1-0.bin (2K)
/usr/local/nam/patch/wor  [########################]      2K
2248 bytes transferred in 0.01 sec (306.60k/sec)
Verifying nam-app.5-1-2.cryptoK9.patch.1-0.bin. Please wait...
Patch nam-app.5-1-2.cryptoK9.patch.1-0.bin verified.
Applying /usr/local/nam/patch/workdir/ nam-app.5-1-2.cryptoK9.patch.1-0.bin. Please wait...
##################################        (100%)
######################################## [100%]
Patch applied successfully.
```

Step 7: Verify that the patch has been installed successfully.

```
root@nam.cisco.local# show patches
MON SEP 20 13:39:58 2010 PATCH: NAM-APP.STRONG-CRYPTO-PATCHK9-5.1.2-0 DESCRIPTION: STRONG CRYPTO PATCH FOR NAM.
```

Step 8: Exit the NAM module session and in the Cisco Catalyst 6500 Switch CLI reboot Cisco NAM to the newly installed image.

```
hw-module module [slot] reset
```

Step 9: Log back into Cisco NAM.

Step 10: Enable SSH for direct access to the appliance.

```
root@nam.cisco.local# exsession on ssh
```

Step 11: Enable the NAM Traffic Analyzer Web Secure Server.

```
root@nam.cisco.local# ip http secure server enable
Enabling HTTP server...
```

Step 12: Enter a web username and password. The default username and password are both **admin**.

```
No web users configured!
Please enter a web administrator username [admin]:admin
New password:*******
Confirm password:*******
User admin added.
```

Step 13: Verify that SSH and HTTPS are enabled as shown.

```
root@nam.cisco.local# show ip
IP ADDRESS:              10.4.41.2
SUBNET MASK:             255.255.255.252
IP BROADCAST:            10.4.41.3
DNS NAME:                NAM.CISCO.LOCAL
DEFAULT GATEWAY:         10.4.48.1
NAMESERVER(S):           10.4.48.10
HTTP SERVER:             DISABLED
HTTP SECURE SERVER:      ENABLED
HTTP PORT:               80
HTTP SECURE PORT:        443
TACACS+ CONFIGURED:      NO
TELNET:                  DISABLED
SSH:                     ENABLED
```

Procedure 3 Log into the NAM Traffic Analyzer GUI

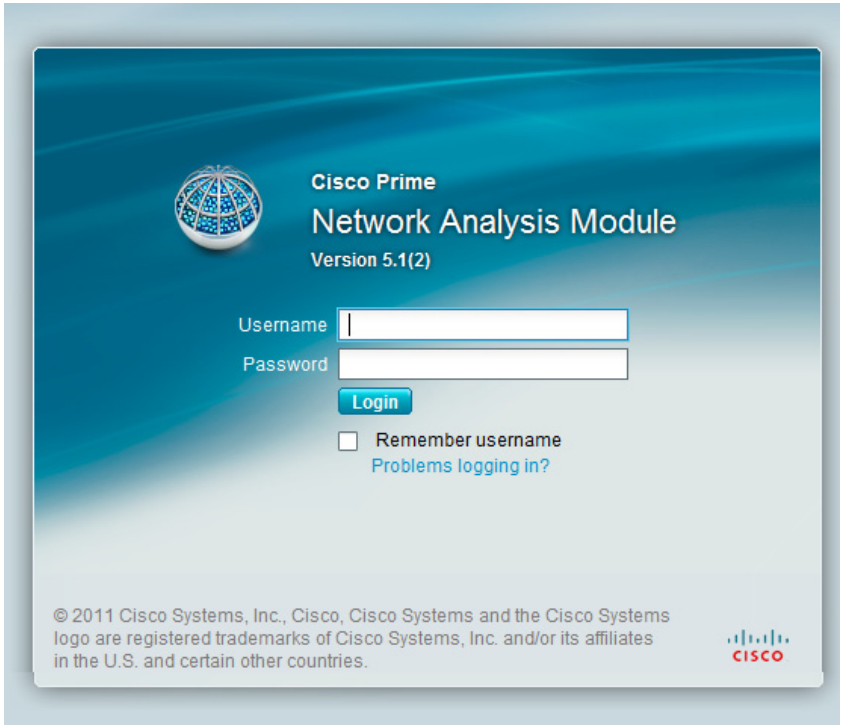
After you have configured the NAM Traffic Analyzer web server and enabled access to it, you should log on. This verifies that the web server is working.

Step 1: In your browser's address box, enter the full hostname of the Cisco Catalyst 6500 Series Network Analysis Module (NAM-2), such as:

https://machine_name.domain

(Example: nam.cisco.local)

Step 2: When the login window appears, enter the administrator username and password, and then click **Login**. The default credentials are **admin/admin**.



Procedure 4 Verify SNMP

Verify that all devices within the Cisco SBA enterprise network, such as the managed device connected to Cisco NAM, have simple network management protocol (SNMP) configured.

Step 1: If necessary, configure SNMP in order to facilitate communication between the managed device and Cisco NAM. Configure the SNMP read-write community strings on the managed device.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Procedure 5 Verify the managed device parameters

Now you need to verify the managed device parameters in Cisco NAM.

Based on the SNMP configuration of the switch, NAM-2 will be able to automatically communicate with its host Cisco Catalyst 6500.

Step 1: Navigate to **Setup > Managed Device > Device Information**.

Step 2: Verify the **SNMP read from chassis** and **SNMP write to chassis** fields show as **OK**.

Performing SNMP test from NAM (10.4.41.2) to switch (127.0.0.50)

Name	**C6509-1.cisco.local**
Hardware	**Cisco Systems, Inc. Catalyst 6500 6-slot Chassis System**
Supervisor Software Version	**IOS Version 15.0(1)SY**
System Uptime	**45 days, 03 hours, 16 minutes**
Location	**N/A**
Contact	**N/A**
SNMP read from chassis	**OK**
SNMP write to chassis	**OK**
Mini-RMON on chassis	**Unavailable**
NBAR on chassis	**Unavailable**
VLAN Traffic Statistics on chassis	**Available**
NetFlow Status	**Configuration unavailable**

Procedure 6 Create a SPAN session for capture

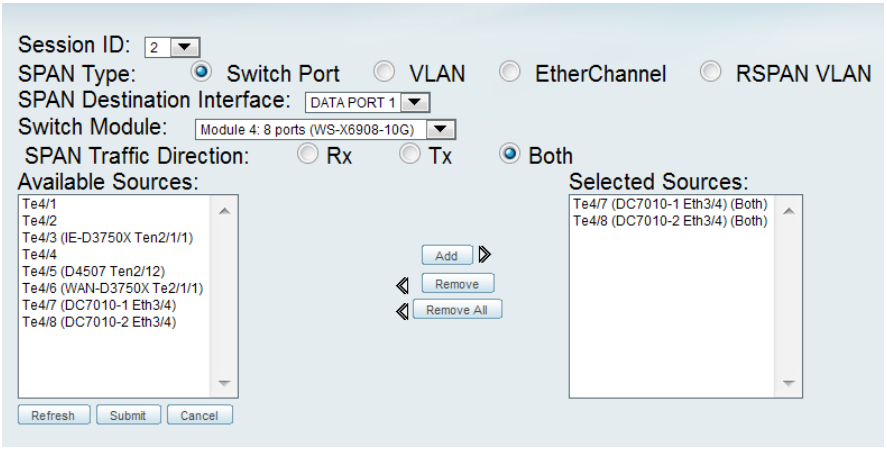
For providing traffic to the NAM-2 for analysis, a SPAN session is required on the managed device. You can use the Cisco NAM GUI to create a SPAN session.

Step 1: Navigate to **Setup > Traffic > SPAN Sessions** and click **Create**.

Step 2: For **SPAN Type**:

- If you want to monitor a physical interface, select **Switch Port**.
- If you want to monitor an EtherChannel interface, select **EtherChannel**.

Step 3: Move the interfaces you want to monitor from **Available Sources** to **Selected Sources**.



Step 4: Click **Submit**. The SPAN session is created.

Step 5: In the active SPAN session window, click **Save**. This saves the SPAN session currently in the running-configuration to the startup-configuration.

	Session ID	Type	Source	Dest. Port	Direction	Status
○	1	port	Te4/7 (DC7010-1 Eth3/4) Te4/8 (DC7010-2 Eth3/4)	Te4/4	Both Both	Active Active
○	2	port	Te4/7 (DC7010-1 Eth3/4) Te4/8 (DC7010-2 Eth3/4)	Gi2/7 (local)	Both Both	Active Active

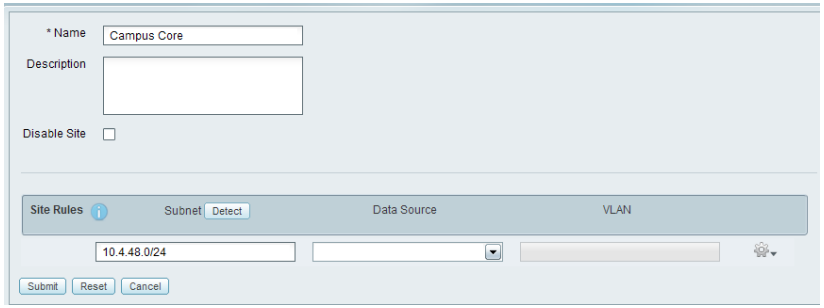
Select an item then take an action → Refresh | Create | Save | Add Dest. Port 1 | Add Dest. Port 2 | Edit | Delete

Procedure 7 Set up sites

To mimic Cisco SBA enterprise network for site-level monitoring, you set up sites in Cisco NAM. You create a site for the campus core and a site for the data center.

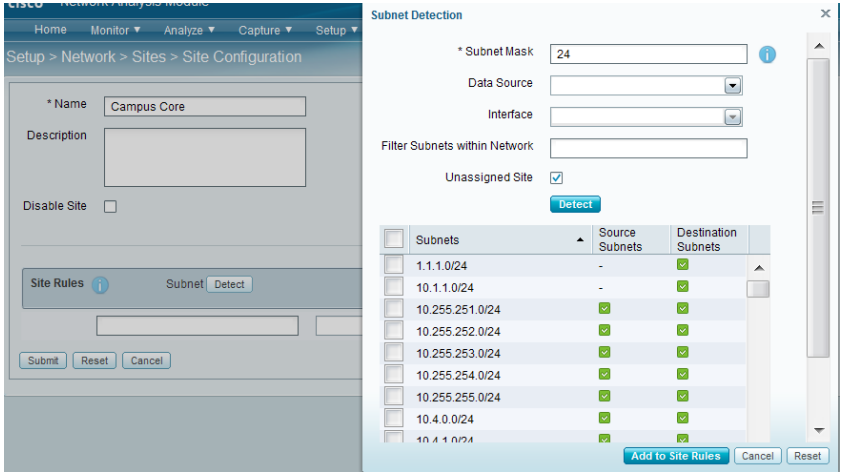
Step 1: Navigate to **Setup > Network > Sites** and click **Create**. The Site Configuration window appears.

Step 2: Specify the site name and the associated subnet, and then click **Submit**.



Step 3: If you want to display all the subnets available as seen by Cisco NAM, click **Detect**.

Step 4: In the **Subnet detection** window enter **Subnet Mask** and click **Detect.** Select the appropriate rows, and then click **Add to Site Rules**.



Procedure 8 View the home dashboard

Step 1: After creating sites, in the menu, click **Home**.

The home dashboard links to Monitor > Overview > Traffic Summary. The Traffic Summary Overview dashboard provides information of Top N Applications, Top N Application Groups, Top N Hosts(In and Out),, IP Distribution by Bits, Top N DSCP and Top N VLAN.

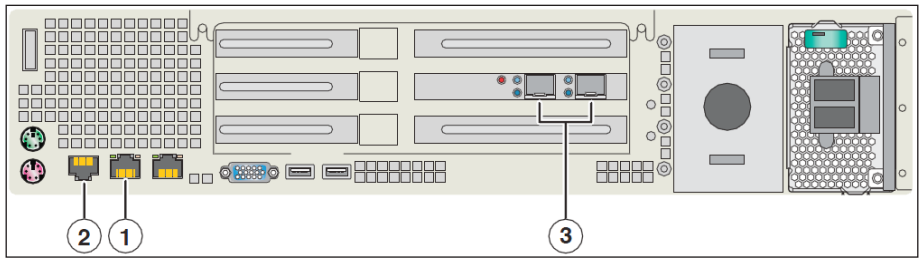
Process

Configuring the Cisco NAM 2220 Appliance

1. Connect the management port
2. Connect a console terminal
3. Connect the monitoring ports
4. Install the Cisco NAM Appliance
5. Secure Cisco NAM 2220
6. Log into the NAM Traffic Analyzer GUI
7. Verify SNMP
8. Configure the managed device parameters
9. Create a SPAN session for capture
10. Set up sites
11. View the home dashboard

First, you set up your Cisco NAM 2220 appliance for connections to a management port, a console terminal, and the monitoring ports.

Figure 3 - Cisco NAM 2220 appliance back panel



Procedure 1 Connect the management port

The Cisco NAM 2220 appliance management port is shown in location #1, an RJ-45 10BASE-T/100BASE-TX/1000BASE-T network interface connector.

Step 1: Connect one end of a Cat5E UTP cable to the management port on the appliance.

Step 2: Connect the other end of the cable to a switch in your network.

Procedure 2 Connect a console terminal

The Cisco NAM 2220 appliance console port is shown in location #2, an RJ-45 serial (console) connector.

Step 1: Connect a console terminal that is using a PC running terminal-emulation software to the console port on the Cisco NAM 2220 appliance.

Procedure 3 Connect the monitoring ports

The Cisco NAM 2220 appliance monitoring ports are shown in location #3, Cisco NAM 2220 Appliance Back Panel. Each monitoring port supports a 10 GB long range (LR) or short range (SR) XFP transceiver module.

Step 1: Connect the Cisco NAM 2220 appliance directly to a switch or router by running a fiber optical cable from a 10 GB Ethernet port on the remote device to the XFP transceiver module on the Cisco NAM 2220 appliance.

Tech Tip

The XFP slot on the right of the Cisco NAM 2220 appliance provides input to logical DataPort 1, and the slot on the left provides input to logical DataPort 2.

Procedure 4 Install the Cisco NAM Appliance

Step 1: Connect to the console of the appliance and log in using the username **root** and default password **root**.

```
Cisco NAM 2220 Appliance (NAM2220)
nam.localdomain login: root
Password: root
Cisco NAM 2220 Appliance (NAM2220) Console, 4.0
Copyright (c) 1999-2008 by Cisco Systems, Inc.
```

Step 2: You must change the root password.

```
System Alert! Default password has not been changed!
Please enter a new root user password.
Enter new UNIX password:******
Enter the new password for the root user.
Retype new UNIX password:******
passwd: password updated successfully
root@nam.cisco.local#
```

Step 3: Configure Cisco NAM for network connectivity.

```
ip address [ip-address] [subnet-mask]
ip gateway [ip-address]
ip domain [domain-name]
ip host [name]
ip nameserver [ip-address]
```

Example:

```
root@nam.localdomain# ip address 10.4.48.34 255.255.255.0
root@nam.localdomain# ip gateway 10.4.48.1
root@nam.localdomain# ip domain cisco.local
root@nam.cisco.local# ip host nam
root@nam.cisco.local# ip nameserver 10.4.48.10
```

Step 4: Verify that the network configuration is as follows.

```
root@nam.cisco.local# show ip
IP ADDRESS:             10.4.48.34
SUBNET MASK:            255.255.255.0
IP BROADCAST:           10.4.48.255
DNS NAME:               NAM.CISCO.LOCAL
DEFAULT GATEWAY:        10.4.48.1
NAMESERVER(S):          10.4.48.10
HTTP SERVER:            DISABLED
HTTP SECURE SERVER:     DISABLED
HTTP PORT:              80
HTTP SECURE PORT:       443
TACACS+ CONFIGURED:     NO
TELNET:                 DISABLED
SSH:                    DISABLED
```

Procedure 5 Secure Cisco NAM 2220

To increase security for the Cisco NAM solution, in this section you will:

- Enable Secure Sockets Layer (SSL) on the Cisco NAM 2220 appliance for secure, encrypted HTTP sessions.
- Enable Secure Shell (SSH) Protocol for secure Telnet to Cisco NAM.

Step 1: Download the crypto patch from the following location: http://www.cisco.com/cisco/software/navigator.html

Step 2: Select **Network Management and Automation** > **Network Analysis Module (NAM) Products** > appropriate NAM form-factor > **All Releases** > 5 > 5.1.2.

Step 3: Click **Download Now** on the following file: **nam-app.5-1-2.cryptoK9.patch.1-0.bin**

Step 4: Apply the crypto patch.

Step 5: Copy the crypto patch to a directory accessible to FTP.

Step 6: Install the patch.

```
root@nam.cisco.local# patch [ftp-url]
```

where ftp-url is the FTP location and the name of the strong crypto patch.

```
root@nam.cisco.local# patch ftp://10.4.48.11/nam-app.5-1-2.cryptoK9.patch.1-0.bin
Proceeding with installation. Please do not interrupt.
```

```
If installation is interrupted, please try again.
Downloading nam-app.5-1-2.cryptoK9.patch.1-0.bin. Please
wait...
ftp://10.4.48.11/nam-app.5-1-2.cryptoK9.patch.1-0.bin (2K)
/usr/local/nam/patch/wor  [########################]      2K
2248 bytes transferred in 0.01 sec (306.60k/sec)
Verifying nam-app.5-1-2.cryptoK9.patch.1-0.bin. Please wait...
Patch nam-app.5-1-2.cryptoK9.patch.1-0.bin verified.
Applying /usr/local/nam/patch/workdir/nam-app.5-1-2.cryptoK9.
patch.1-0.bin. Please wait...
####################################        (100%)
########################################## [100%]
Patch applied successfully.
```

Step 7: Verify that the patch has been installed successfully.

```
root@nam.cisco.local# show patches
MON SEP 20 13:39:58 2010 PATCH: NAM-APP.STRONG-CRYPTO-
PATCHK9-5.1.2-0 DESCRIPTION: STRONG CRYPTO PATCH FOR NAM.
```

Step 8: Reboot Cisco NAM to the newly installed image.

```
root@nam.cisco.local# reboot
```

Step 9: Enable SSH for direct access to the appliance.

```
root@nam.cisco.local# exsession on ssh
```

Step 10: Enable the NAM Traffic Analyzer Web Secure Server.

```
root@nam.cisco.local# ip http secure server enable
Enabling HTTP server...
```

Step 11: Enter a web username and password. The default username and password are both **admin**.

```
No web users configured!
Please enter a web administrator username [admin]:admin
New password:******
Confirm password:******
User admin added.
```

Step 12: Verify that SSH and HTTPS are enabled as shown.

```
root@nam.cisco.local# show ip
IP ADDRESS:              10.4.48.34
SUBNET MASK:             255.255.255.0
IP BROADCAST:            10.4.48.255
DNS NAME:                NAM.CISCO.LOCAL
DEFAULT GATEWAY:         10.4.48.1
NAMESERVER(S):           10.4.48.10
HTTP SERVER:             DISABLED
HTTP SECURE SERVER:      ENABLED
HTTP PORT:               80
HTTP SECURE PORT:        443
TACACS+ CONFIGURED:      NO
TELNET:                  DISABLED
SSH:                     ENABLED
```

Procedure 6 Log into the NAM Traffic Analyzer GUI

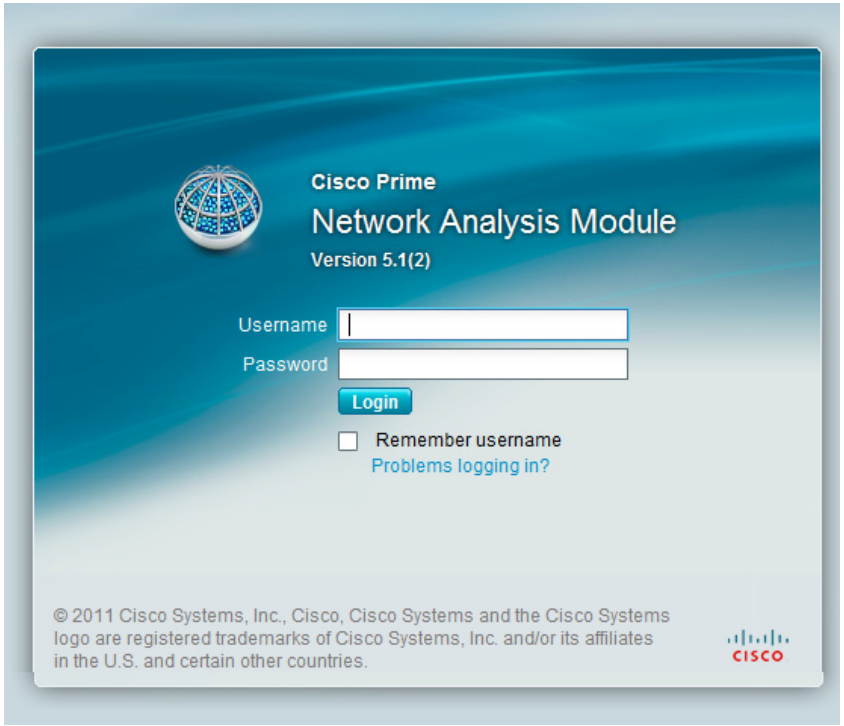
After you have configured the NAM Traffic Analyzer web server and enabled access to it, you should log on. This verifies that the web server is working.

Step 1: In your browser's address box, enter the full hostname of the Cisco NAM 2200 Series appliance, such as:

https://machine_name.domain

(Example: nam.cisco.local)

Step 2: When the login window appears, enter the administrator username and password, and then click **Login**. The default credentials are **admin/admin**



After you connect an output interface of a managed device to the monitoring ports of the Cisco NAM 2220 appliance, you must also configure the managed device to send data to that interface.

Procedure 7 Verify SNMP

Verify that all devices within the Cisco SBA enterprise network, such as the managed device connected to Cisco NAM, have simple network management protocol (SNMP) configured.

Step 1: If necessary, configure SNMP in order to facilitate communication between the managed device and Cisco NAM. Configure the SNMP read-write community strings on the managed device.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Procedure 8 Configure the managed device parameters

Now you need to configure the managed device parameters in Cisco NAM.

Step 1: Navigate to **Setup > Managed Device > Device Information**.

Step 2: Enter the managed device IP address. Enter the same IP address that was configured on the managed device (for example, **10.4.40.252**).

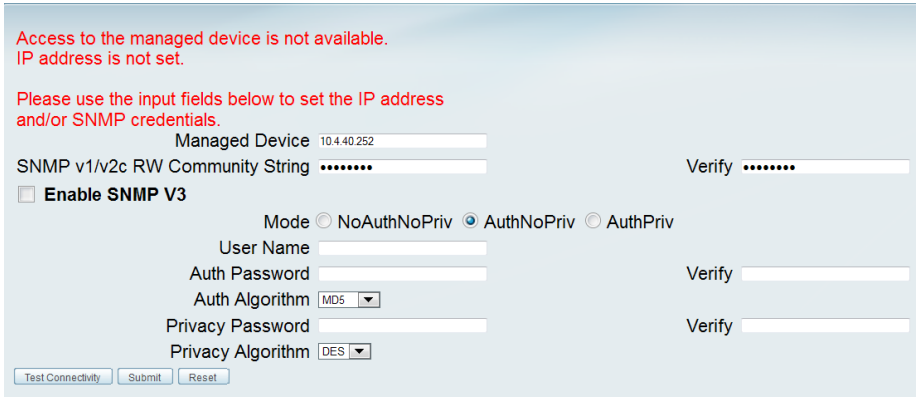
Step 3: Enter the **SNMP v1/v2c RW Community String** Enter the same read-write community string (for example, **cisco123**) that was configured on the managed device, or Cisco NAM won't be able to communicate via SNMP with the managed device.

Step 4: In the **Verify String** box, enter the SNMP read-write community string again.

Step 5: After you enter the managed device parameters, click **Test Connectivity** and the Connectivity Test dialog box opens.

Step 6: On the Connectivity Test dialog box, verify the SNMP Read from Managed Device and SNMP Write from Managed Device parameters have a status of **OK.** Close the window by clicking on **Close**.

Step 7: On the Device Information page, click **Submit**.



Procedure 9 Create a SPAN session for capture

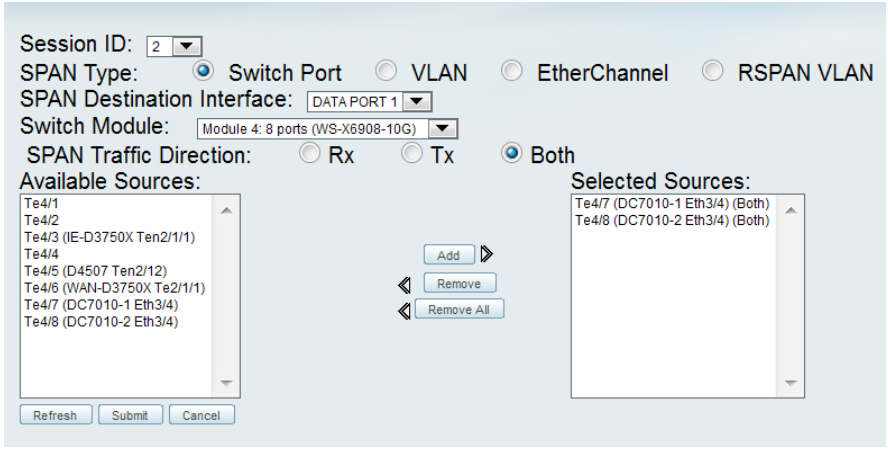
For providing traffic to the Cisco NAM 2220 for analysis, a SPAN session is required on the managed device. You can use the Cisco NAM appliance GUI to create a SPAN session.

Step 1: Navigate to **Setup > Traffic > SPAN Sessions** and click **Create**.

Step 2: For **SPAN Type**:

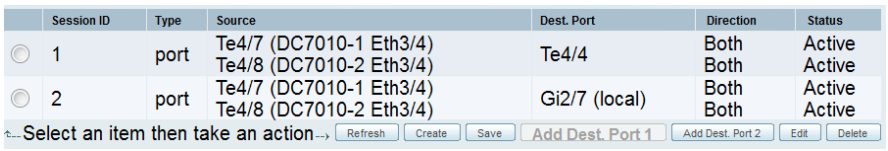
- If you want to monitor a physical interface, select **Switch Port**.
- If you want to monitor an EtherChannel interface, select **EtherChannel**.

Step 3: Move the interfaces you want to monitor from **Available Sources** to **Selected Sources**.



Step 4: Click **Submit**. The SPAN session is created.

Step 5: In the active SPAN session window, click **Save**. This saves the SPAN session currently in the running-configuration to the startup-configuration.

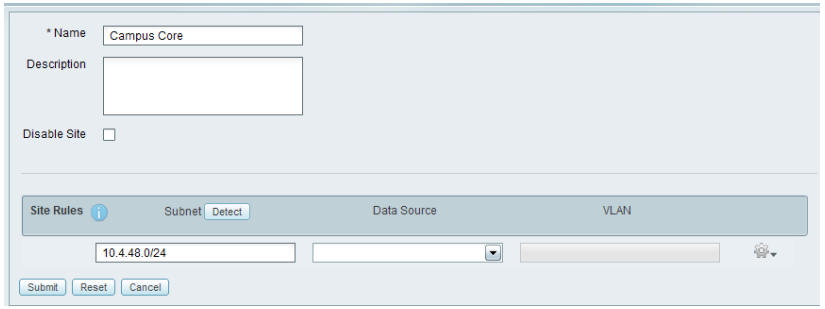


Procedure 10 Set up sites

To mimic Cisco SBA enterprise network for site-level monitoring, you set up sites in Cisco NAM. You create a site for the campus core and a site for the data center.

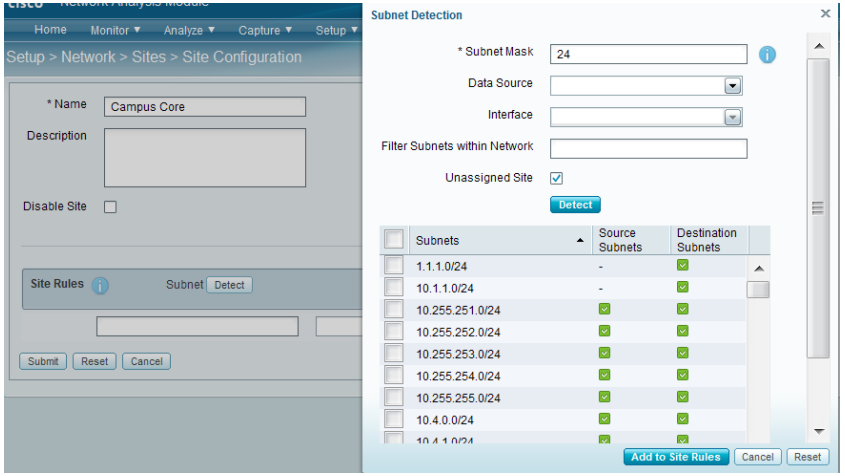
Step 1: Navigate to **Setup > Network > Sites** and click **Create**. The Site Configuration window appears.

Step 2: Specify the site name and the associated subnet, and then click **Submit**.



Step 3: If you want to display all the subnets available as seen by Cisco NAM, click **Detect**.

Step 4: In the **Subnet detection** window enter **Subnet Mask** and click **Detect.** Select the appropriate rows, and then click **Add to Site Rules**.



Procedure 11 View the home dashboard

Step 1: After creating sites, in the menu, click **Home**.

The home dashboard links to Monitor > Overview > Traffic Summary. The Traffic Summary Overview dashboard provides information of Top N Applications, Top N Application Groups, Top N Hosts(In and Out),, IP Distribution by Bits, Top N DSCP and Top N VLAN.

Process

Configuring the Cisco Prime NAM on Cisco ISR G2 SRE

1. Install Cisco Prime NAM on SRE
2. Secure Cisco Prime NAM on SRE
3. Log into the NAM Traffic Analyzer GUI
4. Enable NAM packet monitoring
5. Set up sites
6. View the home dashboard

Requirements:

- Cisco Integrated Services Router (ISR) 2911, 2921, 2951, 3925 or 3945.
- Open slot for either Service Ready Engine (SRE) 700, 710, 900 or 910 module.
- IOS release 15.1(4)M or later.
- Cisco Prime NAM software 5.1(2) for SRE downloaded from www.cisco.com to a local FTP server.

Procedure 1 Install Cisco Prime NAM on SRE

Step 1: Download the Cisco Prime NAM 5.1(2) software from the following location: http://www.cisco.com/cisco/software/navigator.html

Step 2: Navigate to **Network Management and Automation > Network Analysis Module (NAM) Products** > appropriate NAM form-factor > **All Releases > 5 > 5.1.2**.

Step 3: Click **Download Now** on the following file: **nam-app-x86_64.5-1-2.bin.gz.zip**

Step 4: Copy the downloaded image to a local FTP server.

Step 5: Log in to Cisco ISR G2 and configure the SRE interface for router-side (internal) and module-side (NAM management) connectivity.

```
interface sm [slot]/0
ip address [router-side-ip-address] [subnet-mask]
service-module [ip address module-side-ip-address] [subnet-mask]
service-module ip default-gateway [gateway-ip-address]
no shutdown
```

Example:

```
interface sm 4/0
 ip address 10.5.0.17 255.255.255.252
 service-module ip address 10.5.0.18 255.255.255.252
 service-module ip default-gateway 10.5.0.17
 no shutdown
```

Step 6: Verify interface configuration via show run.

The following example shows the configuration of the internal interface between the Cisco SM-SRE and the router.

```
Router# show running-config interface SM4/0
interface SM4/0
ip address 10.5.0.17 255.255.255.0
service-module ip address 10.5.0.18 255.255.255.252
service-module ip default-gateway 10.5.0.17
hold-queue 60 out
```

Step 7: Install Cisco Prime NAM on a SRE.

```
service-module sm slot/0 install url [url]
```

Example:

```
Router# service-module sm 4/0 install url ftp://10.4.48.11/nam-app-x86_64.5-1-2.bin.gz.zip
```

Step 8: Open a session into Cisco NAM:

```
service-module SM [module number] session
```

Step 9: Log in to Cisco NAM using the username **root** and default password **root**.

```
RS200-3945-1# service-module SM 4/0 session

Cisco Prime Network Analysis Module
nam.localdomain login: root
Password:

Cisco SM-SRE Network Analysis Module (SM-SRE-900-K9) Console, 5.1(2)
Copyright (c) 1999-2011 by Cisco Systems, Inc.
```

Step 10: You must change the root password.

```
System Alert! Default password has not been changed!
Please enter a new root user password.
Enter new password:******
Confirm new password:******
Successfully changed password for user 'root'
root@nam.localdomain#
```

Step 11: Configure NAM for network connectivity.

```
ip domain [domain-name]
ip host [name]
ip nameserver [ip-address]
```

Example:

```
root@nam.localdomain# ip domain cisco.local
root@nam.cisco.local# ip host nam
root@nam.cisco.local# ip nameserver 10.4.48.10
```

Step 12: Verify the network configuration is as follows.

```
root@nam.cisco.local# show ip
IP ADDRESS:             10.5.0.18
SUBNET MASK:            255.255.255.252
IP BROADCAST:           10.5.0.19
DNS NAME:               NAM.CISCO.LOCAL
DEFAULT GATEWAY:        10.5.0.17
NAMESERVER(S):          10.4.48.10
HTTP SERVER:            DISABLED
HTTP SECURE SERVER:     DISABLED
HTTP PORT:              80
HTTP SECURE PORT:       443
TACACS+ CONFIGURED:     NO
TELNET:                 DISABLED
SSH:                    DISABLED
```

Procedure 2 Secure Cisco Prime NAM on SRE

To increase security for the NAM, in this section you will:

- Enable Secure Sockets Layer (SSL) on the NAM for secure, encrypted HTTP sessions.
- Enable Secure Shell (SSH) Protocol for secure Telnet to NAM.

Step 1: Enable SSH for direct access to Cisco Prime NAM on SRE.

```
root@nam.cisco.local# exsession on ssh
```

Step 2: Enable the NAM Traffic Analyzer Web Secure Server.

```
root@nam.cisco.local# ip http secure server enable
Enabling HTTP server...
```

Step 3: Enter a web username and password. The default username and password are both admin.

```
No web users configured!
Please enter a web administrator username [admin]:admin
New password:*******
Confirm password:*******
User admin added.
```

Step 4: Verify that SSH and HTTPS are enabled as shown.

```
root@nam.cisco.local# show ip
IP ADDRESS:             10.5.0.18
SUBNET MASK:            255.255.255.252
IP BROADCAST:           10.5.0.19
DNS NAME:               NAM.CISCO.LOCAL
DEFAULT GATEWAY:        10.5.0.17
NAMESERVER(S):          10.4.48.10
HTTP SERVER:            DISABLED
HTTP SECURE SERVER:     ENABLED
HTTP PORT:              80
HTTP SECURE PORT:       443
TACACS+ CONFIGURED:     NO
TELNET:                 DISABLED
SSH:                    ENABLED
```

Procedure 3 Log into the NAM Traffic Analyzer GUI

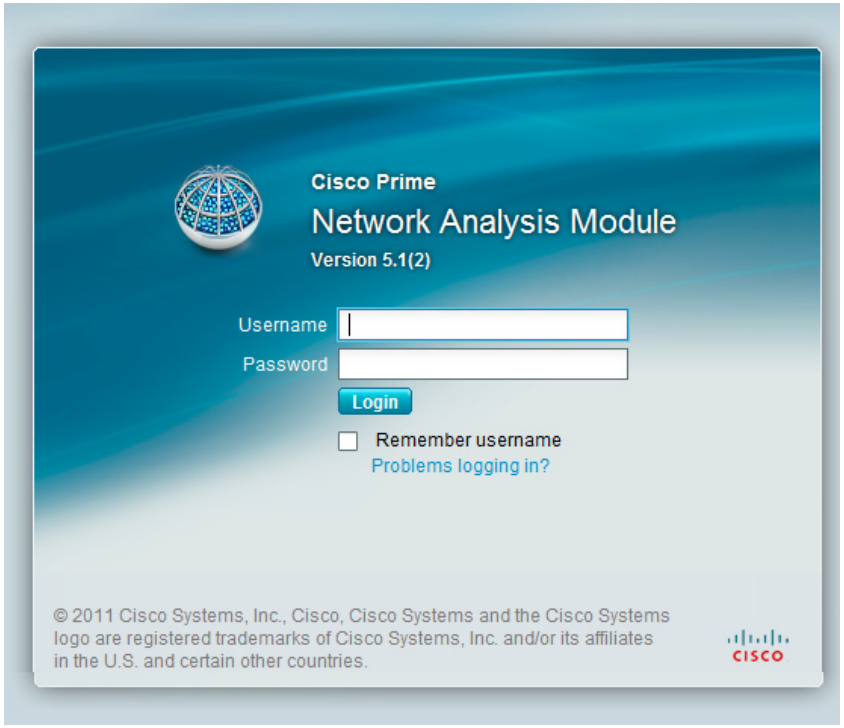
After you have configured the NAM Traffic Analyzer web server and enabled access to it, you should log on. This verifies that the web server is working.

Step 1: In your browser's address box, enter the full hostname of Cisco Prime NAM, such as:

https://machine_name.domain

(Example: nam.cisco.local)

Step 2: When the login window appears, enter the administrator username and password, and then click **Login**. The default credentials are **admin/admin**



Procedure 4 Enable NAM packet monitoring

You can enable NAM packet monitoring on router interfaces that you want to monitor through the internal NAM interface.

Step 1: Enable NAM packet monitoring on an interface. Cisco Express Forwarding sends an extra copy of each IP packet that is received from or sent out on that interface to the NAM through the Service-Ready-Engine interface on the router and the internal NAM interface.

```
ip cef
interface type [slot/port]
 analysis-module monitoring
```

Example:

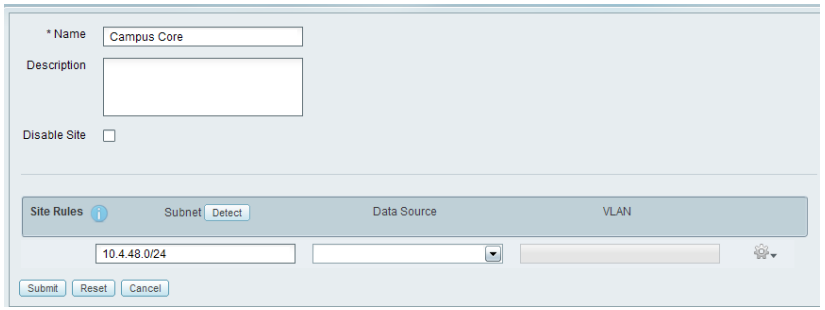
```
ip cef
!
interface GigabitEthernet 0/0
 analysis-module monitoring
```

Procedure 5 Set up sites

To mimic Cisco SBA enterprise network for site-level monitoring, you set up sites in Cisco NAM. You create a site for the campus core and a site for the data center.

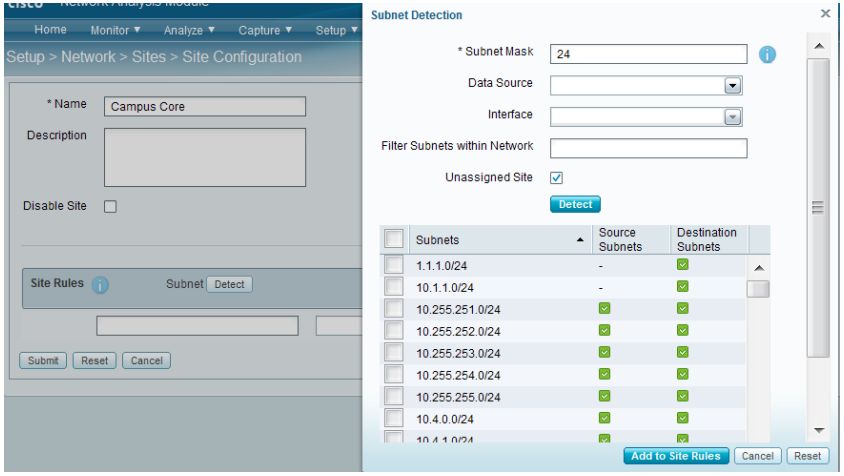
Step 1: Navigate to **Setup** > **Network** > **Sites** and click **Create**. The Site Configuration window appears.

Step 2: Specify the site name and the associated subnet, and then click **Submit**.



Step 3: If you want to display all the subnets available as seen by Cisco NAM, click **Detect**.

Step 4: In the **Subnet detection** window enter **Subnet Mask** and click **Detect.** Select the appropriate rows, and then click **Add to Site Rules**.



Procedure 6 View the home dashboard

Step 1: After creating sites, in the menu, click **Home**.

The home dashboard links to Monitor > Overview > Traffic Summary. The Traffic Summary Overview dashboard provides information of Top N Applications, Top N Application Groups, Top N Hosts(In and Out), IP Distribution by Bits, Top N DSCP and Top N VLAN.

Day 1+ Scenarios

This section walks you through two common analysis scenarios: trouble-shooting poor application performance and troubleshooting poor voice quality.

Process

Troubleshooting Application Performance

1. Monitor SharePoint response time
2. Drill-down SharePoint Response Time
3. Analyze SharePoint response time trend
4. Analyze network vs. server congestion
5. Analyze SharePoint server
6. Set up packet capture session
7. Set up Cisco NAM alarm e-mail
8. Set alarm actions
9. Set alarm thresholds
10. View alarm summary
11. Decode triggered packet capture
12. Scan for packet capture errors

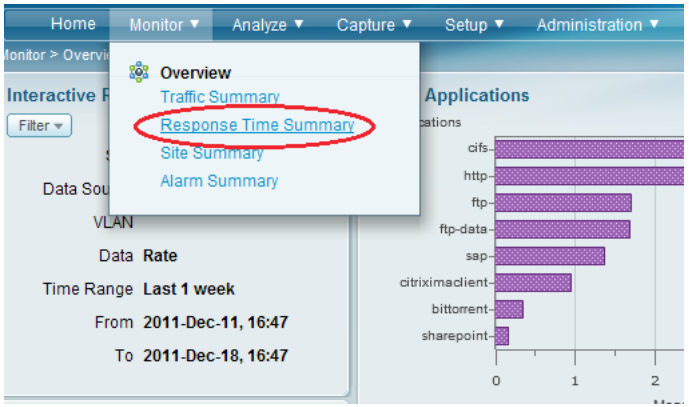
In this scenario, you are an IT network manager responsible for an enterprise network. You have currently deployed the Cisco Catalyst 6500 Series Network Analysis Module (NAM-2) or Cisco NAM 2220 appliance in the Campus Core and have configured a Data Center site.

Users have complained intermittent SharePoint access delays in the last week. You are not sure where the SharePoint performance degradation occurred or why, so you undertake the following procedures.

Procedure 1 Monitor SharePoint response time

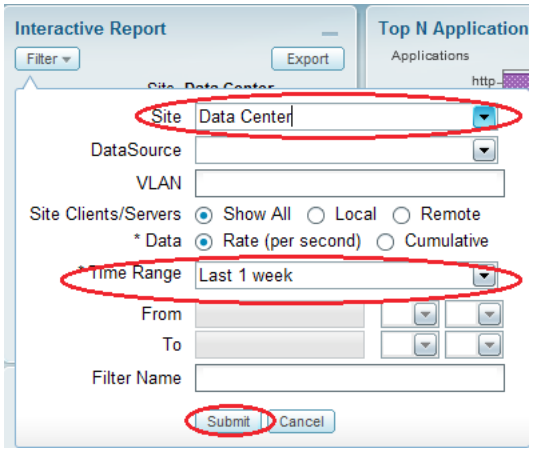
Because all application servers are hosted in the Data Center and clients in the Campus Core are experiencing delays, you obtain an overview of application performance in the Response Time Summary dashboard.

Step 1: Navigate to **Monitor > Overview > Response Time Summary**.



Step 2: In the Interactive Report panel on the left, select **Filter.**

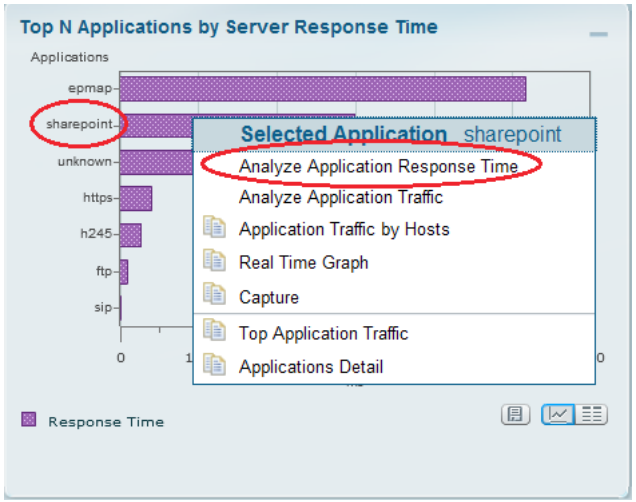
Step 3: In the **Site** list choose **Data Center**, in the **Time Range** list choose **Last 1 week**, and then click **Submit**. You can now view application performance at the Campus Core to the Data Center.



Procedure 2 — Drill-down SharePoint Response Time

Noticing SharePoint's response time degradation (in the Top N Application by Server Response Time report), you drill down to analyze SharePoint.

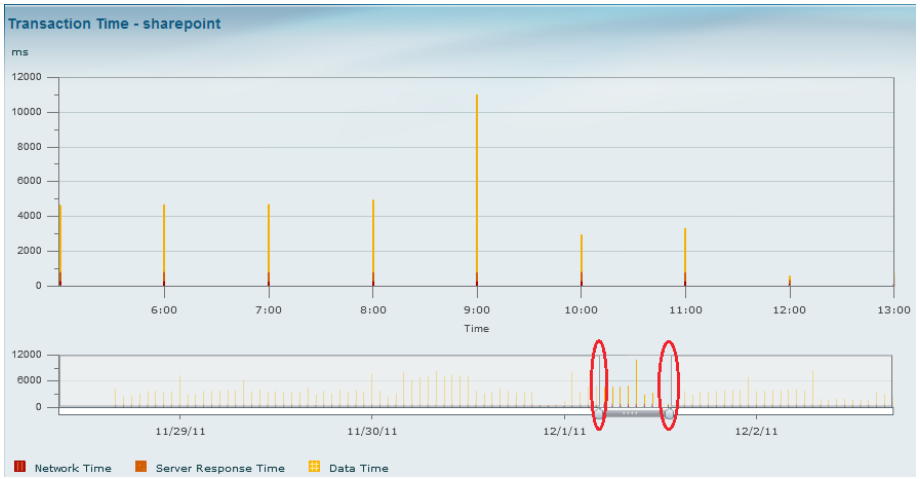
Step 1: In the Top N Applications by Server Response Time report, click **SharePoint**, and then choose **Analyze Application Response Time**.



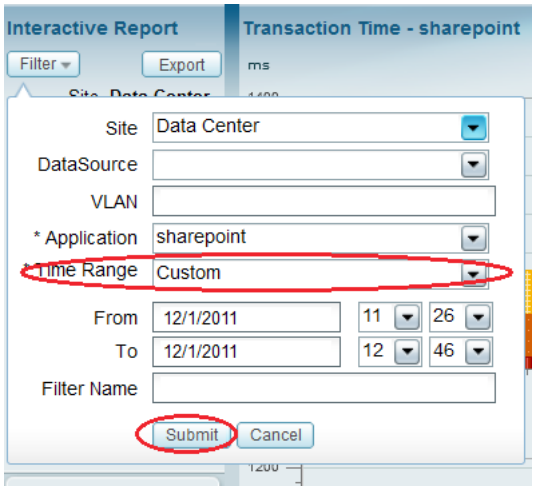
Procedure 3 — Analyze SharePoint response time trend

In the SharePoint response time trend analysis, you observe a spike in overall response time. You zoom in to the time interval and note the clients that were affected, as well as a list of affected servers.

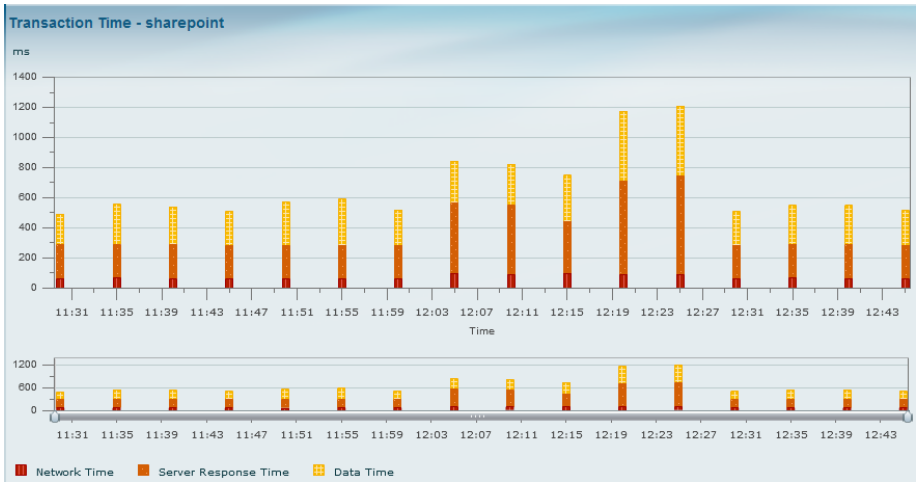
Step 1: In the **Analyze** > **Response Time** > **Application** dashboard, zoom to a spike in SharePoint response time by moving the left slider to a start point of the time-interval of interest and the right slider to the end point of the interval of interest.



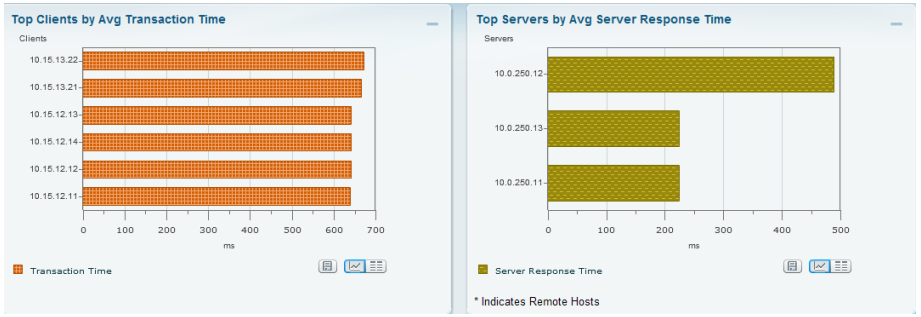
Step 2: Obtain more granular detail. Click **Filter**, and in the **Time Range** list, choose **Custom**. Specify a time range from 12/1/2011 at 11:26 to 12/1/2011 at 12:46, as shown, and then click Submit.



The Transaction Time for application sharepoint appears.



Step 3: Scroll down to view Top clients and servers that were affected by poor SharePoint response time during this interval.

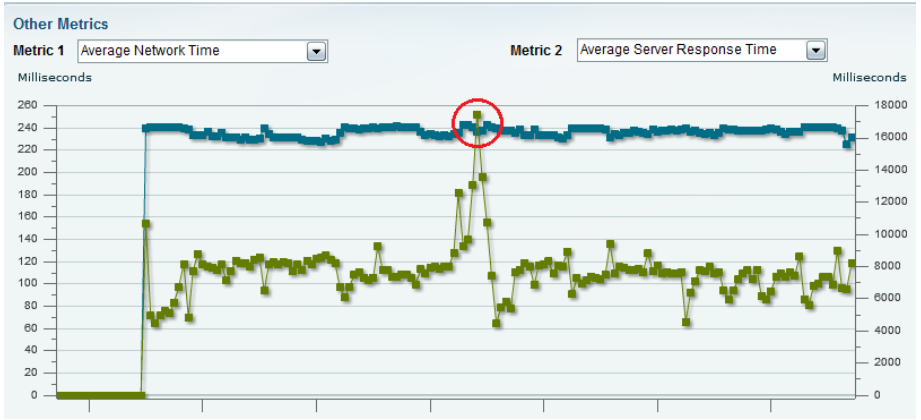


Procedure 4 Analyze network vs. server congestion

To determine if the cause is from a network congestion issue or a server issue, you analyze the network time and the application transaction time. Since the network time is constant (no network delay), you have determined the root cause is an application delay from an overloaded server.

Next you determine if the root cause is from a network delay or server delay.

Step 1: In the Transaction Time report page scroll down further to the **Other Metrics** chart and in the **Metric 1** list, choose **Average Network Time**, which represents network delay. In the **Metric 2** list, choose **Average Server Response Time**, which represents server application delay.



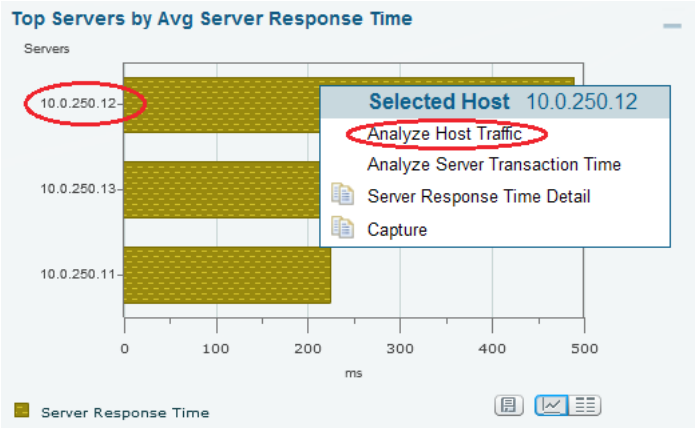
Step 2: Examine the resulting data. Based on the spike in the green line (average server response time) and the consistency of the blue line (average network time), you infer the issue stems from a delay from the application server.

Procedure 5 Analyze SharePoint server

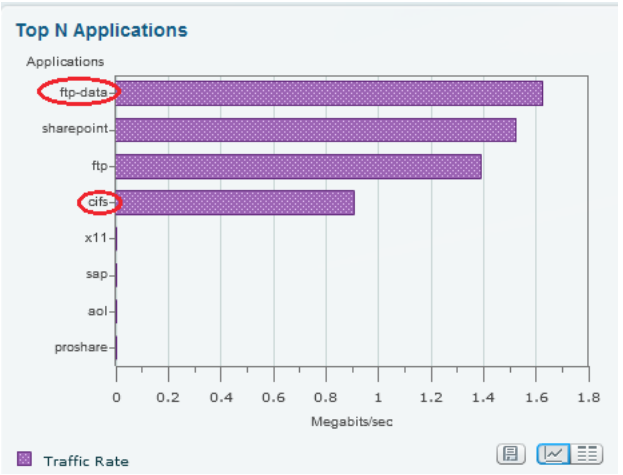
Because you can infer that the issue stems from a delay on the application server, look at applications other than SharePoint that might be causing the delay.

Step 1: Scroll back up and view the Top Servers by Avg Server Response Time chart.

Step 2: Further analyze this server. Click **10.0.250.12**, and then click **Analyze Host Traffic**.



Step 3: From the 10.0.250.12 analysis dashboard, scroll down to view applications running on this server in **Top N Applications**. You notice that in addition to the business-critical application on this server, SharePoint, FTP and CIFS are also running. You realize that many users are downloading the latest Windows 7 patch hosted on this server, which affected SharePoint as well.



Step 4: Take corrective action by ensuring that existing and future Windows patches are hosted on a different server.

Procedure 6 Set up packet capture session

To take a proactive approach moving forward, you create alarms to alert you via e-mail and trigger a packet capture based on SharePoint response time normal trend values.

Step 1: Navigate to **Capture** > **Packet Capture/Decode** > **Sessions** and click **Create**. The Capture Settings window appears.

Step 2: In the **Name** box, type **SharePoint_Capture**

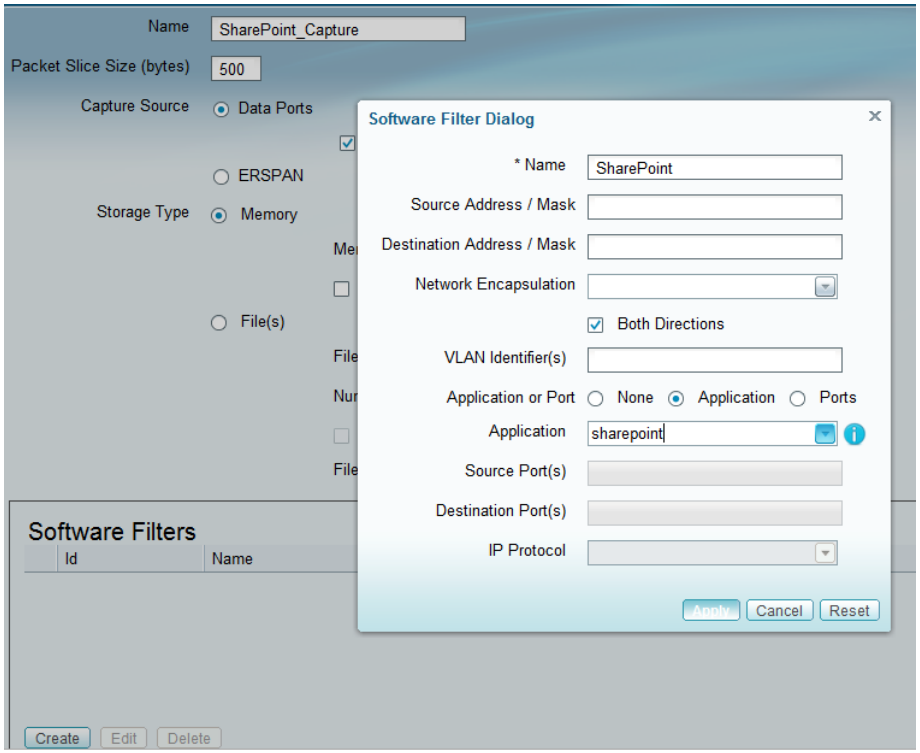
Step 3: Under **Capture Source**, choose **DATA PORTs**. Leave the **Packet Slice Size** at 500 bytes (the default), to limit the size of the capture packets.

Step 4: Under Storage Type, choose **Memory,** and in the **Memory Size** field, enter **100**.

Step 5: In the Software Filters pane, click **Create.** The Software Filter Dialog appears.

Step 6: Enter the following values:

- Name—**SharePoint**
- Both Directions—selected
- Application or Port—**Application**
- Application—**sharepoint**



Step 7: Click **Apply**, and then click **Submit.** The capture session is created.

Procedure 7 Set up Cisco NAM alarm e-mail

Step 1: Navigate to **Administration > System > E-Mail Setting**, and then choose **Enable Mail**.

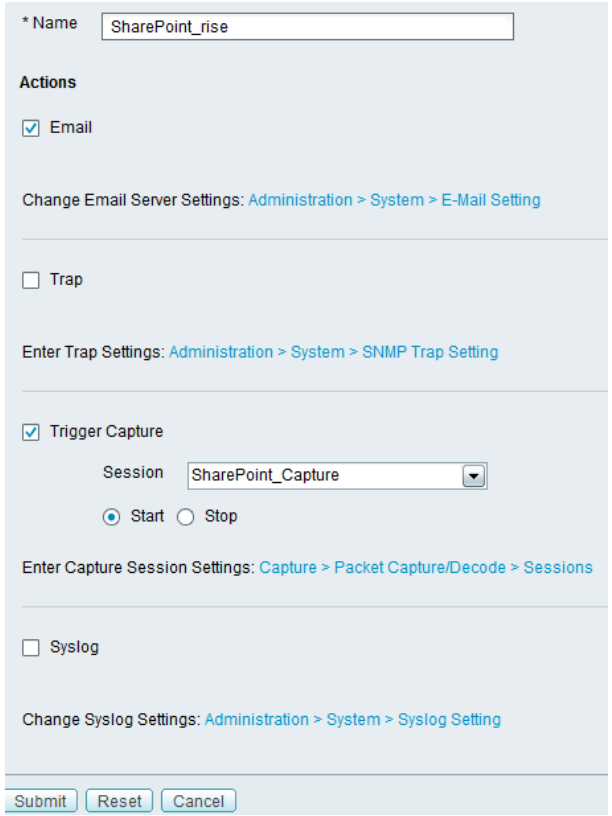
Step 2: Enter the hostname of the **External Mail Server**.

Step 3: In the **Mail Alarm to** field, enter one or more e-mail addresses that will receive the Cisco NAM alarm mail. Use a space to separate multiple e-mail addresses.

Step 4: Click **Submit**.

Procedure 8 Set alarm actions

Step 1: Navigate to **Setup > Alarms > Actions** and click **Create**.



Step 2: Enter a description of the alarm event. (For example, **SharePoint_rise**).

Step 3: Under Actions, select **Email**. When threshold on the rising value is violated, an email alert will be sent to the email you specified in Procedure 7.

Step 4: Select **Trigger Capture**, and under Session, choose **SharePoint_Capture** (configured earlier) and select **Start**. This starts a packet capture when the threshold on the rising value is violated.

Step 5: Click **Submit**.

The Alarm Events table displays the newly configured Alarm Event in its list.

Step 6: To create a second event for the falling edge alarm action, repeat steps 1-5 with the following changes.

- Name—**SharePoint_fall**
- Trigger Capture—**Stop**

Procedure 9 Set alarm thresholds

Step 1: Navigate to **Setup > Alarms > Thresholds**.The Alarm Events table displays any configured Alarm Events.

Step 2: Click **Create**, and then click the **Response Times** tab.

Step 3: Enter a name for the response time threshold (for example, **SharePoint_ResponseTime**).

Step 4: In the **Application** list, choose **sharepoint**.

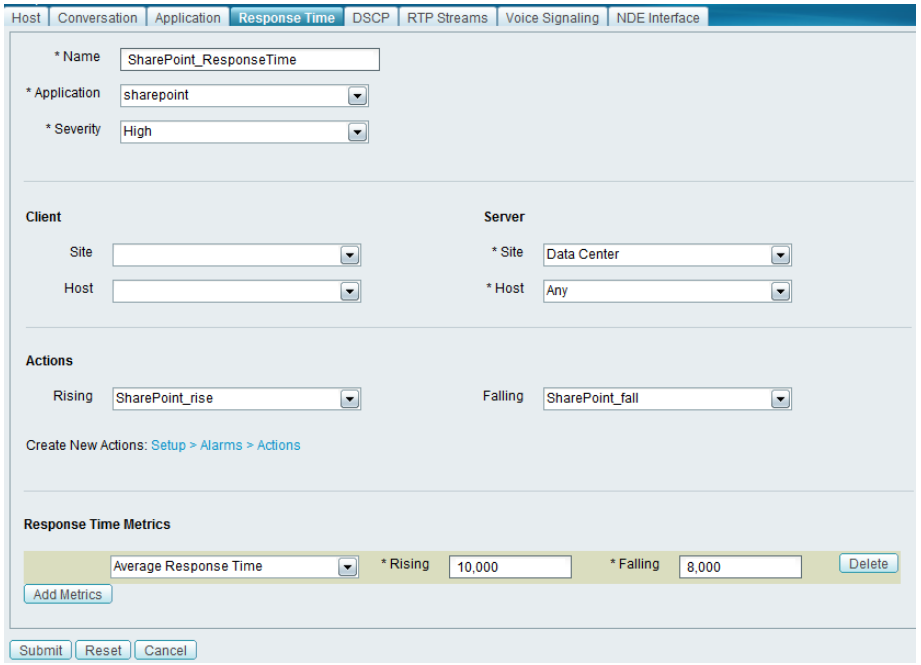
Step 5: Under Server, choose the **Site** as **Data Center** and the **Host** as **Any** (because there is more than one server in the data center hosting SharePoint).

Step 6: Under Actions, choose the alarm actions you created in procedure 8 for the rising edge of the threshold and the falling edge of the threshold. In this example, SharePoint_rise is associated with the rising action and SharePoint_fall is associated with the falling action.

Step 7: Under Response Time Metrics, choose **Average Response Time** and set the **Rising** value to **10,000** milliseconds and **Falling** value to **8,000** milliseconds.

Tech Tip

You can add more metrics for this threshold by clicking Add Metrics.



Step 8: Click **Submit**.

Procedure 10 View alarm summary

When you receive an e-mail alert that SharePoint response time has exceeded your configured threshold, you can use the Cisco NAM dashboard to learn more details of the alarm as well as analyze the triggered packet capture. To help reduce time and effort in analyzing the packet capture, invoke Error Scan to quickly view just the packets with anomalies.

Step 1: Navigate to **Monitor > Overview > Alarm Summary** and view the Top N Applications by Alarm Count chart.

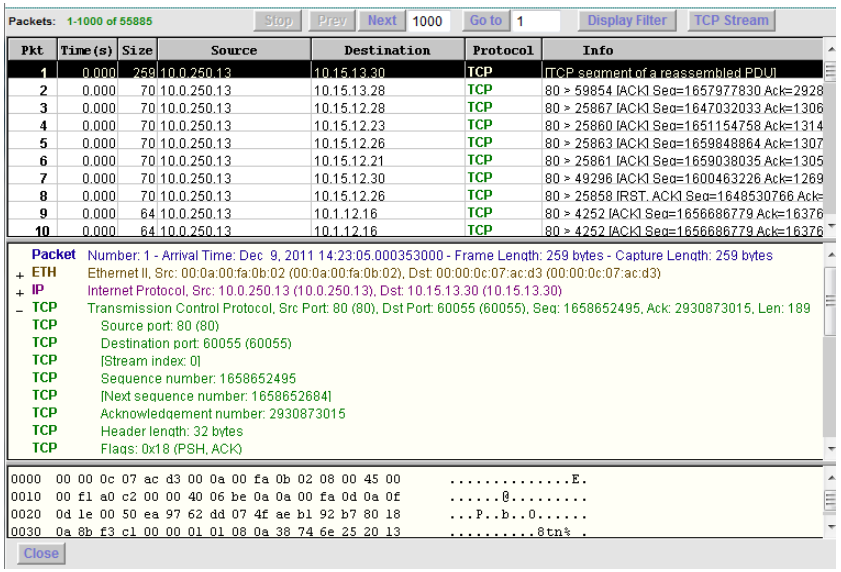
Step 2: Identify the SharePoint application.

Step 3: Click **SharePoint** and click **All Alarms**. Additional details appear.

Procedure 11 — Decode triggered packet capture

Step 1: Navigate to **Capture** > **Packet Capture/Decode** > **Sessions**, and then select the **SharePoint_Capture** (created earlier) that was triggered when the SharePoint threshold was violated.

Step 2: Click **Decode**. A dialog box showing packet decode appears.



Procedure 12 — Scan for packet capture errors

Step 1: Navigate to **Capture** > **Packet Capture/Decode** > **Sessions** and select **SharePoint_Capture**.

Step 2: If the capture is in progress, click **Stop**.

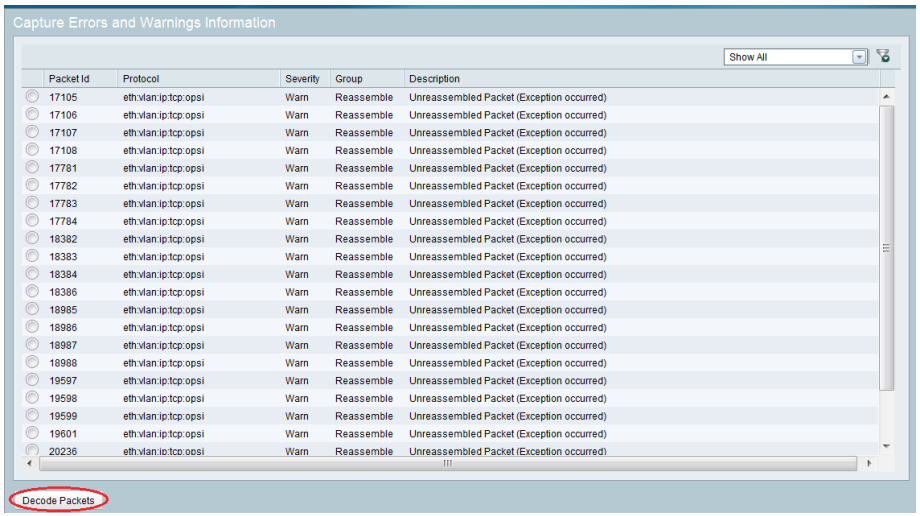
Step 3: Click **Save To File**.

Step 4: In the pop up window, provide a **New File Name** and click **OK.**

Step 5: Navigate to **Capture** > **Packet Capture/Decode** > **Files** and select the **SharePoint_Capture.pcap**.

Step 6: Click **Errors Scan.** The **Capture Errors and Warnings Information** popup screen opens.

Step 7: Select a packet with an anomaly, and then click **Decode Packets**. You can further analyze the packet and continue troubleshooting.



Process

Analyzing and Troubleshooting Voice

1. Enable voice and RTP monitoring
2. Analyze RTP streams
3. View regional office traffic use

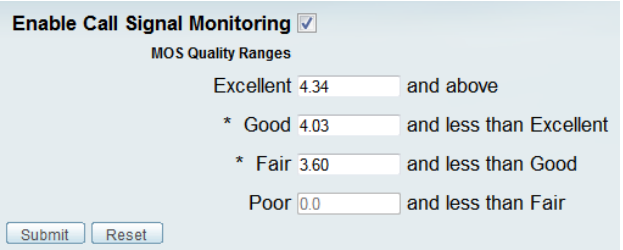
In this scenario, you are an IT network manager responsible for an enterprise network. You currently have deployed the Cisco Prime NAM on Cisco ISR G2 SRE 700 in the Singapore regional office and have configured a regional office site and a Campus Core site.

In order to resolve a scenario where a couple of users have opened a trouble ticket describing experience of choppy audio into a call in the last couple of days, follow the procedures in this process.

Procedure 1 Enable voice and RTP monitoring

Step 1: Navigate to **Setup** > **Monitoring** > **Voice**.

Step 2: Ensure that **Enable Call Signal Monitoring** is selected and that you are satisfied with the default MOS values.



Step 3: Navigate to **Setup** > **Monitoring** > **RTP Filter** and ensure that **Enable RTP Stream Monitoring** is selected.

Procedure 2 Analyze RTP streams

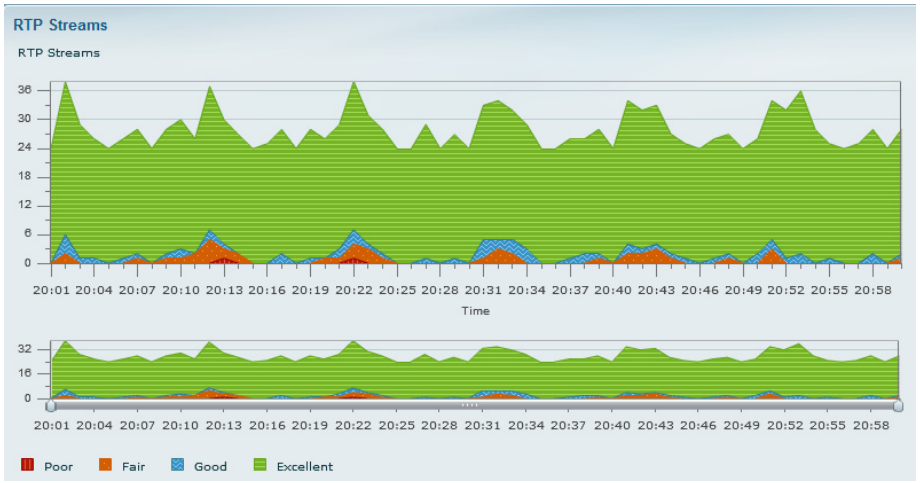
Step 1: Navigate to **Analyze** > **Media** > **RTP Streams**.

Step 2: In the Interactive Report panel on the left, click **Filter**.

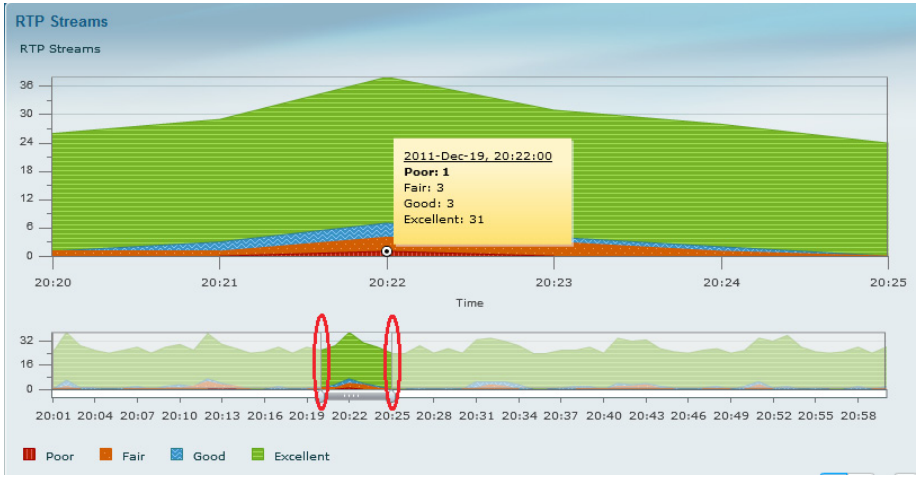
Step 3: Under **Site**, specify the regional office site under **Site**.

Step 4: For **Time Range**, specify the last 1 hour and click **Submit**.

The RTP Streams chart appears.

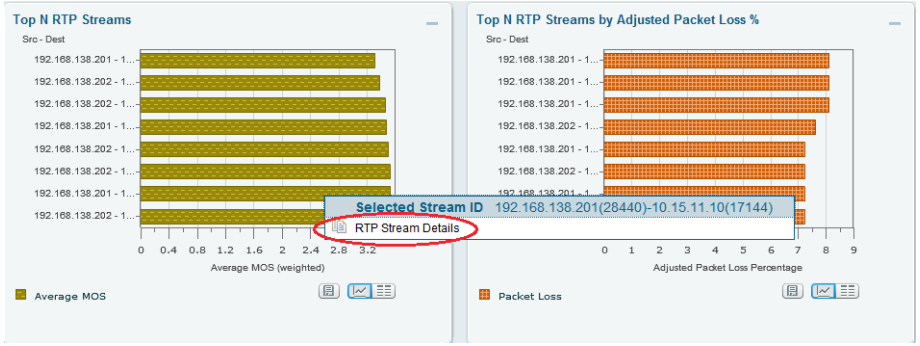


Step 5: To analyze poor MOS values, use the slider controls on the bar to zoom in to a time interval. In the following figure, there are a total of forty-one RTP streams with one RTP stream rated with a poor MOS value and three RTP streams rated with a fair MOS value.

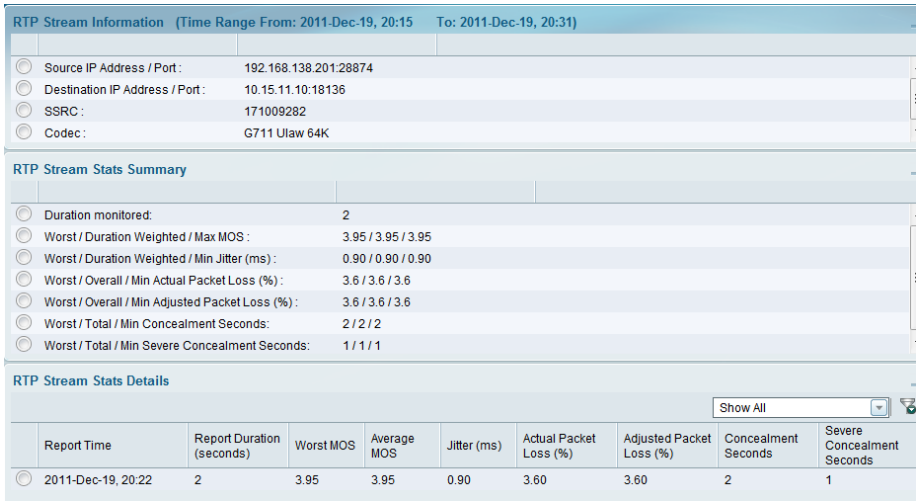


Step 6: Scroll down to view the Top N Source/Destination Endpoints, Top N RTP Stream, and Top N RTP Streams by Adjusted Packet Loss % charts.

Step 7: To further analyze a RTP Stream, select an endpoint from the Top N RTP Streams by Adjusted Packet Loss % chart, click on a data-point of interest, and then click **RTP Stream Details**.



A new dialog box appears, providing various RTP Stream information such as codec, MOS, jitter, packet loss, RTP Stream Stats Summary and RTP Stream Stats Details.



RTP Stream Information (Time Range From: 2011-Dec-19, 20:15 To: 2011-Dec-19, 20:31)

Source IP Address / Port :	192.168.138.201:28874
Destination IP Address / Port :	10.15.11.10:18136
SSRC :	171009282
Codec :	G711 Ulaw 64K

RTP Stream Stats Summary

Duration monitored:	2
Worst / Duration Weighted / Max MOS :	3.95 / 3.95 / 3.95
Worst / Duration Weighted / Min Jitter (ms) :	0.90 / 0.90 / 0.90
Worst / Overall / Min Actual Packet Loss (%) :	3.6 / 3.6 / 3.6
Worst / Overall / Min Adjusted Packet Loss (%) :	3.6 / 3.6 / 3.6
Worst / Total / Min Concealment Seconds:	2 / 2 / 2
Worst / Total / Min Severe Concealment Seconds:	1 / 1 / 1

RTP Stream Stats Details

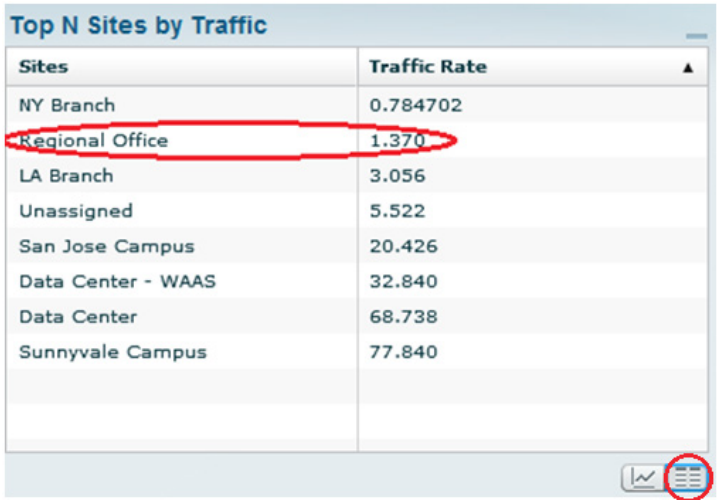
Show All

Report Time	Report Duration (seconds)	Worst MOS	Average MOS	Jitter (ms)	Actual Packet Loss (%)	Adjusted Packet Loss (%)	Concealment Seconds	Severe Concealment Seconds
2011-Dec-19, 20:22	2	3.95	3.95	0.90	3.60	3.60	2	1

Procedure 3 View regional office traffic use

Step 1: Navigate to **Monitor > Overview > Site Summary**.

Step 2: In the Top N Sites by Traffic chart grid view, observe Regional Office traffic use.



Top N Sites by Traffic

Sites	Traffic Rate ▲
NY Branch	0.784702
Regional Office	1.370
LA Branch	3.056
Unassigned	5.522
San Jose Campus	20.426
Data Center - WAAS	32.840
Data Center	68.738
Sunnyvale Campus	77.840

Notes

Summary

Cisco Prime NAM offers flexibility in different network deployments with various form factors. This—coupled with built-in analytics for real-time monitoring, historical analysis, and threshold-based proactive troubleshooting—provides unmatched visibility into existing networks, ensures reliable delivery of applications, provides a consistent user experience, improves operating efficiency, maximizes IT investments, anticipates infrastructure changes, and helps scale to an appropriate network.

Notes

Additional Information

Cisco Prime Network Analysis Module

http://www.cisco.com/go/nam

Cisco Prime Network Analysis Module Product Family Data sheets

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps5740/ps5688/ps10113/data_sheet_c78-642316.html

Product Portfolio:

Cisco Catalyst 6500 Series Network Analysis Module (NAM-3)

http://www.cisco.com/en/US/products/ps11659/index.html

Cisco Catalyst 6500 Series Network Analysis Module (NAM-1/NAM-2)

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html

Cisco NAM 2200 Series Appliances

http://www.cisco.com/en/US/products/ps10113/index.html

Cisco Prime Network Analysis Module (NAM) for ISR G2 SRE

http://www.cisco.com/en/US/products/ps11658/index.html

Install and Configuration Guides:

Cisco Catalyst 6500 Series Network Analysis Module (NAM-3)

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/5.1_2/switch/installation/guide/instcfg.html

Cisco Catalyst 6500 Series Network Analysis Module (NAM-1/NAM-2)

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/5.1/switch/configuration/guide/Cisco_Catalyst_6500_Series_Switch_and_Cisco_7600_Series_Router_NAM_Installation_and_Configuration_Note,_5.1.html

Cisco NAM 2200 Series Appliances

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_appliance/5.1/2220/Cisco_NAM_Appliances_Installation_and_Configuration_Note_2220,_5.1.html

Cisco Prime Network Analysis Module (NAM) for ISR G2 SRE

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/5.1/sm_sre/SM_SRE_incfg_5_1.html

Cisco Prime Network Analysis Module 5.1(2) User Guides

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/5.1_2/user/guide/NAM_UG512.html

Cisco Prime Network Analysis Module 5.1(2) Software Download

http://www.cisco.com/cisco/software/navigator.html

Appendix A: Cisco Prime Network Analysis Module Deployment Guide Product List

Functional Area	Product	Part Numbers	Software Version
Network Management	Cisco Catalyst 6500 Series Network Analysis Module (NAM-1/ NAM-2)	WS-SVC-NAM-2-250S	NAM 5.1(2)
Network Management	Cisco NAM 2200 Series Appliance	NAM2204-RJ45 Cisco NAM 2204 Appliance with 4x1 Gigabit RJ-45 ports NAM2204-SFP Cisco NAM 2204 Appliance with 4x1 Gigabit SFP ports NAM2220 Cisco NAM 2220 Appliance with 2x10 Gigabit XFP ports	NAM 5.1(2)
Network Management	Cisco Prime Network Analysis Module (NAM) for ISR G2 SRE	SM-NAM-SW-5.1-K9* *Hardware is based on SRE module. Only Cisco Prime NAM software is required.	NAM 5.1(2)

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.**

B-0000147-1 1/12