Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program. For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-250 For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd





11 11-1-1 CISCO BORDERLESS NETWORKS DEPLOYMENT GUIDE SBA

Network Analysis Module Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 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 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.

The Release Notes for a series provides a summary of additions and changes made in the 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 February 2013 is the "February 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 10.5.204.5 255.255.25.0

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

February 2013 Series

Table of Contents

1
1
1
1
2
2
2
6
6
12
18
25

Day 1+ Scenarios	31
Analyzing and Troubleshooting Application Performance	
Configuring Continuous Packet Capture	
Analyzing and Troubleshooting Voice	40
Deploying Pre- and Post- WAN Optimization	43
Summary	49
Additional Information	50
Appendix A: Product List	51
Appendix B: Changes	53

What's In This SBA Guide

Cisco SBA Borderless Networks

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.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

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

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

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 and 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.

In this deployment guide, Cisco Catalyst 6500 Series Network Analysis Module (NAM-3) is deployed in the Cisco Catalyst 6500 Series switch found in LAN core in the campus. NAM-3 takes advantage of backplane integration by simplifying manageability, lowering total cost of ownership, reducing network footprint, and reducing rack space. Cisco NAM-3 monitors traffic on the Cisco Catalyst 6500 switch via two internal 10-Gigabit data ports.

The campus use case utilizes Cisco NAM-3 for the following:

- · Voice and video quality at the campus
- Traffic utilization and application performance between campus to data center and campus to branch
- · Packet capture for troubleshooting
- URL monitoring for web filtering policies, quality of service (QoS) for enforcement of QoS policies
- Application and host analysis in VLAN

The Cisco Prime NAM 2320 appliance is deployed in the data center core connected to Cisco Nexus 5000 series switches. NAM 2320 has the flexibility to connect to any platform (including Catalyst and Nexus series platforms) that supports SPAN/RSPAN/ERSPAN for local switch visibility. The Cisco NAM 2320 appliance monitors traffic on the switches via two 10-Gigabit data port interfaces.

The data center use case utilizes Cisco Prime NAM 2320 for the following:

- Traffic utilization and application performance between data center to campus and data center to branch
- WAN optimization analysis and troubleshooting
- Packet capture for troubleshooting
- · QoS for enforcement of QoS policies
- · Application and host analysis in VLAN

Cisco Prime NAM on Cisco Services Ready Engine (SRE) 710 or 910 series as part of ISR G2 is deployed in the regional office (Figure 1), which helps you monitor, measure, and report on the network's health at the branch level. The branch use case utilizes Cisco Prime NAM SRE for the following:

- · Voice and video quality at the branch
- Traffic utilization and application performance between branch to data center, branch to campus, and branch to branch
- Packet capture for troubleshooting
- URL monitoring for web filtering policies, QoS for enforcement of QoS policies
- Application and host analysis in VLAN

For more information about the Cisco SBA network, see the LAN Deployment Guide, here: http://www.cisco.com/go/sba Figure 1 - Cisco Prime 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. It delivers on-demand historical analysis from the data collected. This category of monitoring includes application recognition, analysis of top conversations, hosts, protocols, differentiated services code points, and virtual LANs (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 voice over IP (VoIP) metrics

Application and Service Delivery with Application Performance Intelligence

In order to accurately assess the end-user experience, Cisco Prime NAM delivers comprehensive application performance intelligence (API) measurements. It analyzes TCP-based client/server requests and acknowledgements in order 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 for which the entire stream, or summaries of data from that stream, is sent to Cisco Prime NAM for monitoring. Cisco Prime NAM can monitor a variety of data sources and compute appropriate metrics. The following figure provides a snapshot of all possible sources of data, and also the various export mechanisms supported by 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, for instance, NAM web GUI, and also providing data to Cisco Prime Infrastructure via representational state transfer (REST)/XML interface.

As Cisco Prime NAM combines both a traffic analyzer (different form factors) and reporting console, the user can leverage NAM as standalone network application performance solution. If several NAMs are deployed in the network, for example, NAM in the data center, campus, and branches, then Cisco Prime Infrastructure offers a solution that allows the user to discover, configure and manage NAMs. Examples of Prime Infrastructure as a multi-NAM management includes a centralized configuration of Network Time Protocol (NTP), application ID and Domain Name System (DNS) configuration, centralized NAM image management, centralized packet capture with alarm triggers, and a single dashboard for consolidation of all NAM traffic information.

Using the SPAN feature, Cisco Prime NAMs can monitor traffic from physical ports, 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. Remote SPAN (RSPAN) or Encapsulated Remote SPAN (ERSPAN) extends troubleshooting to remote parts of the network. The functional use case utilizes Cisco Prime NAM with SPAN for the following:

- Traffic analysis
- Application performance analysis
- Pre-WAN optimization
- · Voice and video Analysis
- · Packet capture

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 NAM interface. The functional use case utilizes Cisco Prime NAM with CEF for the following:

- Traffic analysis
- Application performance analysis
- · Pre-WAN optimization
- · Voice and video analysis
- Packet capture

Cisco Wide Area Application Services (WAAS) Flow Agent from Cisco Wide Area Application Engine (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. The functional use case utilizes Cisco Prime NAM with WAAS Flow Agent data for the following: Pre- and post- WAN optimization.

Cisco IOS NetFlow allows a device to capture a snapshot of the flow in a record. These records provide analysis of real-time and historical traffic usage to obtain a broad view of how the network is performing. The functional use case utilizes Cisco Prime NAM with NetFlow for the following:

- Traffic analysis
- Pre-WAN optimization

Cisco Performance Agent 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. Performance Agent 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. The functional use case utilizes Cisco Prime NAM with Performance Agent for the following:

- Traffic analysis
- Application performance analysis
- Pre- and post-WAN optimization

Deployment Details

This section describes how to configure Cisco Catalyst 6500 Series NAM-3, the Cisco Prime NAM 2320 appliance, and Cisco Prime NAM on Cisco ISR G2 SRE in order to establish network connectivity; how to 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 GUI, and how to perform various system management tasks.

Process

Preparing Cisco ACS for NAM Web User Authentication

- 1. Add NAM to the ACS Network Devices list
- 2. Define the command set permitted by ACS
- 3. Configure the NAM Access Policies

Procedure 1

Add NAM to the ACS Network Devices list

Step 1: Log in to Cisco Access Control Server (ACS) via https://ACS.cisco. local.

Step 2: Navigate to Network Resources > Network Device Groups > Device Type, and then click Create.

Step 3: In the **Name** box, enter a group name for NAM devices. (Example: NAM)

Step 4: In the **Description** box, enter an appropriate description. (Example: NAM Devices)

Device Group - (General	
😛 Name:	NAM	
Description:	NAM Devices	
🖕 Parent:	All Device Types	Select
🗢 = Required fie	lds	

Step 5: Click Submit. The configuration is applied to the ACS.

Step 6: Navigate to Network Resources > Network Devices and AAA Clients, and then click Create.

Step 7: On the Network Devices and AAA Clients configuration page enter the following values.

- Name NAM
- Description HQ Core NAM-3
- · IP 10.4.40.2
- TACACS+ selected
- · Shared Secret SecretKey

Step 8: To the right of the Device Type box, click Select.

Step 9: In the **All Device Types** list, choose the device group (example: NAM) that you created in Step 2, and then click **OK**. This inserts the device type.

Step 10: Click Submit. The NAM is added to the network device list in ACS.





Define the command set permitted by ACS

Step 1: Navigate to Policy Elements > Authorization and Permissions > Device Administration > Command Sets, and then click Create.

Step 2: In the Name box, enter NAM_Full_Access, and then in the Description box, enter Full Access to all NAM Commands.

Step 3: Select Permit any commands that is not in the table below.

Step 4: Using the following table, add all the web commands available on Cisco Prime NAM by entering each data row into the **Grant**, **Command**, and **Arguments** boxes, and then clicking **Add**.

Table 1 - Web commands for Cisco Prime NAM

Grant	Command	Arguments
Permit	web	account
Permit	web	view
Permit	web	capture
Permit	web	collection
Permit	web	alarm
Permit	web	system

Step 5: Click Submit. The configuration of the command set is finalized.

General			
Name:	NAM_Full_Access		
Description:	Full Access to all NAM Com	nds	
Permit any c	ommand that is not in the tab	elow	
Grant	Command	Arguments	-
Permit Permit	web	view A	
Permit	web	capture	
Permit	web	alarm	
Permit	web	system	
Add A	Edit V Replace A D	e	
Grant	Command	Arguments	
Permit	•		
Select Commar	ld/Arguments from Comman	et Allow All Select	
Required field	ds		

Procedure 3

Configure the NAM Access Policies

Step 1: Navigate to Access Policies > Access Services, and then click Create.

Step 2: In the Access Services configuration section, in the **Name** box, enter a name (Example: NAM Admin), and then in the **Description** box, enter a description (Example: NAM Administration Access Services).

Step 3: Select User Selected Service Type, and then in the User Selected Service Type list, choose Device Administration, and then click Next.

General Allowed Protocols				
Step 1 - General				
General				
🖕 Name:	NAM Admin			
Description:	NAM Administration Access Services			
Access Service	Policy Structure			
\bigcirc Based on se	ervice template	Select		
O Based on ex	xisting service	Select		
 User Selected S User Selected S Polic V 	ed Service Type Device Administration v Service Type Service Type cy Structure Identity Identity Group Mapping Authorization			

Step 4: In the Step 2 - Allowed Protocols section, select **Allow PAP/ASCII**, and then click **Finish**.

General Allowed Protocols
Step 2 - Allowed Protocols
Process Host Lookup
Authentication Protocols
Allow PAP/ASCI
Allow CHAP
Allow MS-CHAPv1
Allow MS-CHAPv2
Allow EAP-MD5
Allow EAP-TLS
Allow LEAP
Allow PEAP
Allow EAP-FAST
Preferred EAP protocol LEAP

A dialog box regarding the modification of Service Selection policy appears.

Step 5: In the dialog box, click **Yes**. The Service Selection Rules page opens.

Step 6: Click Create. You can now make a rule.

Step 7: In the **Name** box, enter an appropriate name (Example: NAM Admin), and then make sure that, under Status, **Enabled** is selected.

Step 8: Under the Conditions section, select **Protocol**, ensure **match** is selected, and then, next to the Protocol and match boxes, click **Select**.

Step 9: In the dialog box that appears, select Tacacs, and then click OK.

Step 10: In the Conditions section, select Compound Condition.

Step 11: Under Dictionary, ensure **NDG** is selected, and then, to the right of Dictionary, click **Select**.

Step 12: In the dialog box that appears, select **Device Type**, and then click OK.

Step 13: Under Value, in the list, choose **Static**, and then next to the Value box, click **Select**.

Step 14: In the dialog box that appears, in the **All Device Types** list, choose the device group created in Procedure 1, "Add NAM to the ACS Network Devices list," Step 2 (Example: NAM), and then click **OK**.

Step 15: Under Current Condition Set, click Add.

Step 16: Under Results, in the **Service** list, choose the Access Service created in Step 7 (Example: NAM Admin), click **OK**.

Step 17: Ensure the new rule is placed above any default TACACS or RADIUS rules by selecting the rule (Example: NAM Admin), and then pressing the up arrow until it is appropriately placed.

General			
Name: NAM Admin	Status: Enable	d 🛨 \varTheta	
The Customize policy condition	button in the lower r is and results are av	ght area of the policy rul ailable here for use in pol	es screen controls which licy rules.
Conditions			
Protocol:	match	 Tacacs 	Select
Compound Condition:			
Condition:			
NDG		: Type	Select
Operator:	Value:	1)00	
in 🔻	Static	•	
			Select
Current Condition Set:			
Add	IV Edit A Re	place V	
	Device Type in All Devic	Types:NAM	
And > -			
Or>•			=
			-
		Delete	Preview
Results			
Service: NAM Admin	-		

Step 18: Navigate to Access Policies > Access Services > NAM Admin > Identity, and then click Select.

Step 19: On the resulting dialog box, select the identity source intended to be used for authentication on Cisco Prime NAM (Example: AD the Local DB), apply the identity source by clicking **OK**, and then Click **Save Changes**. The Access Service is modified.

Single result selection O Rule based result selection		
Identity Source:	AD then Local DB	Select
	 Advanced Options 	

Step 20: Navigate to Access Policies > Access Services > NAM Admin > Authorization, and then click Create.

Step 21: In the **Name** box, enter an appropriate rule name (Example: NAM Access).

Step 22: Select Compound Condition.

Step 23: In the **Dictionary** list, choose the source of authorization for the NAM web access (Example: AD-AD1), and then, to the right of the Attribute box, click **Select**.

Step 24: In the resulting dialog box, select **ExternalGroups**, and then click **OK**.

Step 25: Under the Value box, click Select.

Step 26: In the dialog box, select the group that you want to have access to the NAM web UI (Example: cisco.local/Builtin/Network Device Admins), and then click **OK**.

Status: Enabled

General

Name: NAM Access



The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

- O

Conditions

Compound Condition:	
Dictionary:	Attribute:
AD-AD1	ExternalGroups Select
Operator: contains any →	Value: cisco.local/Builtin/Network Device Admins
	v
	Select Deselect Clear

Step 27: Click **Add.** The new condition is applied to the current condition set.

Step 28: To the Right of the Shell Profile box, click Select.

Step 29: In the resulting dialog box, select Permit Access, and then click OK.

Step 30: Under the Command Sets box, click Select.

Step 31: In the dialog box, select the command set created earlier in Procedure 2, "Define the command set permitted by ACS," Step 1, (Example: NAM_Full_Access), and then click **OK**.

Step 32: Click OK. The Access Service Authorization saves.

Current Condition Set:		
	Add V Edit A Replace V	
	AD-AD1:ExternalGroups contains any cisco.local/Builtin/Network	
And > • Or > •	E	
	Delete Preview	
Results		
Shell Profile: P	ermit Access Select	
Command Sets:		
NAM_Full_Access		
Select Des	elect	

Notes	

Process		Mod MAC addresses Status	Hw	Fw	Sw
 Configuring the Cisco Catalyst 6500 Series NA 1. Install Cisco NAM-3 2. Log in to NAM Traffic Analyzer GUI 3. Verify SNMP 4. Configure NAM for user authentication 5. Verify the managed device parameters 6. Create a SPAN session for capture 7. Set up sites 	M-3	1 0007.7d90.5050 to 0007.7d90.5067 15.0(1)SY1 Ok 2 e8b7.4829.b0d8 to e8b7.4829.b0e7 15.0(1)SY1 Ok 4 70ca.9bc5.e4f8 to 70ca.9bc5.e4ff 15.0(1)SY1 Ok 5 44d3.ca7b.c840 to 44d3.ca7b.c847 15.0(1)SY1 Ok Mod Sub-Module Mode	1.0 1.1 1.1 1.1 1.1	12.2(18r)S1 12.2(50r)SY 12.2(50r)SY 12.2(50r)SY 12.2(50r)SY Seria	 L S 1
8. View the home dashboard		Hw Status 			
Procedure 1 Install Cisco NAM-3 Step 1: In the Cisco Catalyst 6500 switch, insert	sco NAM-3 into any	<pre>1 Distributed Forwarding Card WS-H 1.0 Ok 2/0 NAM Application Processor SVC- 1.0 Ok 4 Distributed Forwarding Card WS-H 1 1 Ok</pre>	'6K-DFC4 APP-PRO '6K-DFC4	-A SAL15 C-1 SAL16 -E SAL16	34N0K4 063SD2 010BPL
Step 2: Verify Cisco NAM-3 is running. C6509-1#show module Mod Ports Card Type Serial No.	Model	5 Policy Feature Card 4 VS-H 1.0 Ok 5 CPU Daughterboard VS-H 1.1 Ok	6K-PFC4 6K-MSFC	SAL15 5 SAL15	35P6WS 37PPAT
1 24 CEF720 24 port 1000mb SFP SAL1533MAVH 2 4 Trifecta NAM Module		Base PID: Mod Model Serial No. 2 WS-SVC-APP-HW-1 SAL16063ZHB			
SAL16063ZHB 4 8 DCEF2T 8 port 10GE SAL16020LYU 5 5 Supervisor Engine 2T 10GE w/ CTS (SAL1534NB4Q	WS-X6908-10G Acti VS-SUP2T-10G				

Mod Online Diag Status

1 Pass

2 Pass

2/0 Pass

- 4 Pass
- 5 Pass

Step 3: Configure a management VLAN for Cisco NAM-3.

vlan [id]

name [VLAN Name]

interface vlan [id]

description [description]

```
ip address [ip-address] [subnet]
```

```
exit
```

```
analysis module [slot] management-port 1 access-vlan [id] end
```

Example

```
vlan 141
name NAM
!
interface Vlan141
description NAM Management
ip address 10.4.41.1 255.255.255.252
no shutdown
!
```

analysis module 2 management-port 1 access-vlan 141

Step 4: Open a session into Cisco NAM-3.

```
session slot [slot] processor 1
```

Step 5: Log in to Cisco NAM-3 by 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: 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.localdomain#

Step 7: Configure Cisco NAM-3 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
                        255.255.255.252
SUBNET MASK:
IP BROADCAST:
                        10.4.41.3
                        NAM.CISCO.LOCAL
DNS NAME:
DEFAULT GATEWAY:
                        10.4.41.1
NAMESERVER(S):
                        10.4.48.10
HTTP SERVER:
                        DISABLED
HTTP SECURE SERVER:
                        DISABLED
                        80
HTTP PORT:
HTTP SECURE PORT:
                        443
TACACS+ CONFIGURED:
                        NO
TELNET:
                        DISABLED
SSH:
                        DISABLED
```

Step 9: Configure Cisco NAM-3 to sync to a network time server.

time
sync ntp [ntp server]
zone [timezone]
exit

Step 10: Example

root@NAM.cisco.local# time Entering into subcommand mode for this command. Type 'exit' to apply changes and come out of this mode. Type 'cancel' to discard changes and come out of this mode. root@NAM.cisco.local(sub-time)# sync ntp 10.4.48.17 root@NAM.cisco.local(sub-time)# zone PST8PDT root@NAM.cisco.local(sub-time)# exit

Step 11: Verify that the network time configuration is as shown.

root@NAM.cisco.local# show t	zime
NAM synchronize time to:	NTP
NTP server1:	10.4.48.17
NAM time zone:	PST8PDT
Current system time:	Thu Jun 28 16:04:01 PDT 2012

Step 12: Enable SSH for direct access to the appliance.

root@nam.cisco.local# exsession on ssh

Step 13: Enable the Cisco NAM Traffic Analyzer web secure server.

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

Step 14: 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 15: Verify that Secure Shell Protocol (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:	10.4.41.1
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 2

Log in to NAM Traffic Analyzer GUI

After you have configured the NAM Traffic Analyzer web server and enabled access to it, you should log in. 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 NAM-3: https://[machine_name].[domain](Example: nam.cisco.local)

Step 2: When the login window appears, enter the administrator username and password that you configured in Procedure 1, "Install Cisco NAM-3," Step 13, and then click **Login**.

Procedure 3

Verify SNMP

Step 1: Verify that all devices within your network, such as the managed device connected to Cisco NAM, have Simple Network Management Protocol (SNMP) configured.

Step 2: If necessary, configure SNMP in order to facilitate communication between the managed device and Cisco NAM. Configure the SNMP readwrite community strings on the managed device.

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

Procedure 4

Configure NAM for user authentication

Optional

If you have a centralized TACACS+ server, configure secure user authentication as the primary method for user authentication (login) and user authorization (configuration) by enabling AAA authentication for access control. AAA controls all management access to the Cisco NAM (HTTPS).

Tech Tip

A local web administrator was created on Cisco NAM during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable, or if you do not have a TACACS+ server in your organization.

Step 1: On the NAM web UI, navigate to Administration > Users > TACACS+

Step 2: Enter the following values in the TACACS+ configuration page:

- Enable TACACS+ Authentication and Authorization selected
- Primary TACACS+ Server 10.4.48.15
- Secret Key SecretKey
- Verify Secret Key SecretKey

Step 3: Click Submit. The configuration is applied to Cisco NAM.

Enable TACACS+ Authentication and Authorization		
Primary TACACS+ Server	10.4.48.15	
Backup TACACS+ Server		
Secret Key	•••••	
Verify Secret Key	•••••	
Submit Reset		

Procedure 5

Verify the managed device parameters

Now you need to verify the managed device parameters in Cisco NAM-3.

Based on the SNMP configuration of the switch, Cisco NAM-3 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 OK



Tech Tip

If the fields are not OK, perform Procedure 3, "Verify SNMP"

again.

Performing SNMP test from NAM (10.4.41.2) to switch (127.0.0.50)
Name	C6509-1.cisco.local
Hardware	Cisco Systems Catalyst 6500
	9-slot Chassis System
Supervisor Software Version	IOS Version 15.0(1)SY1
System Uptime	1 days, 02 hours, 20 minutes
Location	N/A
Contact	N/A
SNMP read from chassis	ОК
SNMP write to chassis	ОК
Mini-RMON on chassis	Unavailable
NBAR on chassis	Unavailable
VLAN Traffic Statistics on chassis	Available
NetFlow Status	Configuration unavailable

Create a SPAN session for capture

In order to provide traffic to Cisco NAM-3 for analysis, a SPAN session is required on the managed device. You can use the Cisco Prime NAM GUI to create a SPAN session or via CLI from the switch.

On the Cisco Prime NAM GUI:

Step 1: Navigate to Setup > Traffic > SPAN Sessions, and then 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: In the **Switch Module** list, choose the module you wish to select sources from for monitoring. The Available Sources list populates with ports from that module and their relative port descriptions.

Step 4: Move the interfaces you want to monitor from Available Sources to Selected Sources.

Session ID: 1 💌	
SPAN Type: Switch Port VLAN EtherC	hannel 💿 RSPAN VLAN
SPAN Destination Interface: DATA PORT 1 💌	
Switch Module: Module 4: 8 ports (WS-X6908-10G)	
SPAN Traffic Direction: ORx OTx Obt	
Available Sources:	Selected Sources:
Te4/1 (Etherchannel links to D6500VSS) Te4/2 (Etherchannel links to D6500VSS) Te4/3 (IE-D3750X Ten/1/1) Te4/4 Te4/5 (D4507 Te 1/12) Te4/6 (WAN-D3750X Te2/1/1) Te4/8 (Link to DC5548UPb Eth1/19) Te4/8 (Link to DC5548UPb Eth1/19)	Te4/7 (Link to DC5548UPa Eth1/19) (Both) Te4/8 (Link to DC5548UPb Eth1/19) (Both)
Refresh Submit Cancel	

Step 5: Click Submit. The SPAN session is created.

Step 6: In the active SPAN session window, click **Save**. This saves the SPAN session currently in the running-configuration to the startup-configuration.

	Session ID	Туре	Source	Dest. Port	Direction	Status
۲	1	port	Te4/7 (Link to DC5548UPa Eth1/19) Te4/8 (Link to DC5548UPb Eth1/19)	Te2/3 (local)	Both Both	Active Active
tSelect an item then take an action> Refresh Create Save Add Dest. Port 1 Add Dest. Port 2 Edit Delete						

Step 7: The preceding steps apply this configuration for creating a SPAN session on the switch.:

C6500 core# conf term

C6500_core(config)# monitor session 1 source interface Te4/7 - 8 both

C6500 core(config) # monitor session 1 destination analysis-

module 2 data-port 1

C6500 core(config) # end

Procedure 7 Set up sites

Setting up sites in Cisco Prime NAM enables site-level monitoring. You create a site for the campus and a site for the data center.

Step 1: Navigate to Setup > Network > Sites, and then 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 Prime NAM, click **Detect**.

Step 4: In the Subnet Detection window, in the Subnet Mask box, enter the desired value, and then click Detect.



Step 5: Select the appropriate rows, and then click Add to Site Rules.



View the home dashboard

Step 1: After creating sites, from the menu, choose 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.

Step 2: If you want to view the Traffic Summary by a site, in the Interactive Report list, choose Filter, in the Site list, choose campus or data center, and then click Submit.



Process

Configuring the Cisco Prime NAM 2320 Appliance

- 1. Connect the management port
- 2. Connect a console terminal
- 3. Connect the monitoring ports
- 4. Install the Cisco Prime NAM 2320 appliance
- 5. Log in to NAM Traffic Analyzer GUI
- 6. Configure NAM for user authentication
- 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

As illustrated in the following figure, you set up your Cisco Prime NAM 2320 appliance for connections to a management port (#1), a console terminal (#2), and the monitoring ports (#3).

Figure 3 - Cisco Prime NAM 2320 appliance back panel



Procedure 1

Connect the management port

The Cisco Prime NAM 2320 appliance management port, shown in location #10 in Figure 3, is 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 Prime NAM 2320 appliance console port, shown in location #6 in Figure 3, is an RJ-45 serial (console) connector.

Step 1: Connect a console terminal that is using a PC running terminalemulation software to the console port on the Cisco Prime NAM 2320 appliance.

Procedure 3

Connect the monitoring ports

The Cisco Prime NAM 2320 appliance monitoring ports are shown in location #4 in Figure 3. Each monitoring port supports a 10-GB SFP+ transceiver module (single-mode fiber, multi-mode fiber, or passive or active twinaxial cables (except for 5M passive cable).

Step 1: Connect the Cisco Prime NAM 2320 appliance directly to the core switch by running a fiber optical cable from a 10-GB Ethernet port on the remote device to DataPort 1 on the Cisco Prime NAM 2320 appliance.

Tech Tip

The SFP+ slot on the right of the Cisco Prime NAM 2320 appliance provides input to logical DataPort 1, and the slot on the left provides input to logical DataPort 2.

Procedure 4

Install the Cisco Prime NAM 2320 appliance

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

Cisco Prime NAM 2320 appliance (NAM2320) nam.localdomain login: root Password: root Cisco Prime NAM Appliance 2320 ("NAM2320-K9") Console, 5.1(3) Copyright (c) 1999-2012 by Cisco Systems, Inc.

Step 2: 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 10.4.41.2 255.255.255.252 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 4: Verify that the network configuration is as follows.

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:	10.4.41.1
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

Step 5: Configure Cisco NAM for network time.

time sync ntp [ntp server] zone [timezone] exit

Example

root@NAM.cisco.local# time

Entering into subcommand mode for this command. Type 'exit' to apply changes and come out of this mode. Type 'cancel' to discard changes and come out of this mode. root@NAM.cisco.local(sub-time)# sync ntp 10.4.48.17 root@NAM.cisco.local(sub-time)# zone PST8PDT root@NAM.cisco.local(sub-time)# exit Step 6: Verify that the network time configuration is as shown.

root@NAM.cisco.local# show time

NAM synchronize time to:	NTP
NTP server1:	10.4.48.17
NAM time zone:	PST8PDT
Current system time:	Thu Jun 28 16:04:01 PDT 2012

Step 7: Enable SSH for direct access to the appliance. root@nam.cisco.local# exsession on ssh

Step 8: Enable the Cisco NAM Traffic Analyzer web secure server.

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

Step 9: 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 10: 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:	10.4.41.1
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



Log in to NAM Traffic Analyzer GUI

After you have configured the NAM Traffic Analyzer web server and enabled access to it, you should log in. 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: https://[machine_name].[domain] (Example: nam.cisco.local)

Step 2: When the login window appears, enter the administrator username and password that you configured in Procedure 4, "Install the Cisco Prime NAM 2320 appliance," Step 9, and then click **Login**.



Configure NAM for user authentication

(Optional)

If you have a centralized TACACS+ server, configure secure user authentication as the primary method for user authentication (login) and user authorization (configuration) by enabling AAA authentication for access control. AAA controls all management access to the Cisco NAM (HTTPS).



Tech Tip

A local web administrator was created on the Cisco NAM during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable, or if you do not have a TACACS+ server in your organization.

Step 1: On the Cisco NAM web UI, navigate to Administration > Users > TACACS+.

Step 2: Enter the following values in the TACACS+ configuration page:

- Enable TACACS+ Authentication and Authorization selected
- Primary TACACS+ Server 10.4.48.15
- Secret Key SecretKey
- Verify Secret Key SecretKey

Step 3: Click Submit. The configuration is applied to Cisco NAM.

Enable TACACS+ Authentication and Authorization		
Primary TACACS+ Server	10.4.48.15	
Backup TACACS+ Server]
Secret Key	•••••]
Verify Secret Key	•••••]
Submit Reset		

After you connect an output interface of a managed device to the monitoring ports of the Cisco Prime NAM 2320 appliance, you must also configure the managed device to send data to that interface.

Procedure 7

Verify SNMP

Step 1: Verify that all devices within your network, such as the managed device connected to Cisco NAM, have SNMP configured.

Step 2: If necessary, configure SNMP in order to facilitate communication between the managed device and Cisco NAM. Configure the SNMP readwrite 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. (Example: 10.4.40.252)

Step 3: Enter the **SNMP v1/v2c RW Community String**. You must enter the same read-write community string (example: cisco123) that was configured on the managed device, otherwise 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.** The Connectivity Test dialog box opens.

Step 6: On the Connectivity Test dialog box, verify that the **SNMP Read from Managed Device** and **SNMP Write from Managed Device** parameters have a status of **OK**, and then click **Close**

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

Access to the managed device is not available. IP address is not set.		
Please use the input fields below to set the IP address and/or SNMP credentials. Managed Device 10.440.252		
SNMP v1/v2c RW Community String	Verify	•••••
Enable SNMP V3		
Mode 🔘 NoAuthNoPriv 💿 AuthNoPriv 🔘 AuthPriv		
User Name		
Auth Password	Verify	
Auth Algorithm MD5 💌		
Privacy Password	Verify	
Privacy Algorithm DES -		
Test Connectivity Submit Reset		

Procedure 9

Create a SPAN session for capture

For providing traffic to Cisco NAM 2320 for analysis, a SPAN session is required on the managed device. You can use the Cisco Prime NAM GUI to create a SPAN session or via CLI from the switch.

Tech Tip

Ensure the interface intended to be used as the Remote Destination Port is not shut down before creating the SPAN session. Using the NAM web interface will only configure the monitoring configuration but it will not bring up the interface if it is down.

Step 1: On the Cisco Prime NAM GUI, navigate to Setup > Traffic > SPAN Sessions, and then 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: Select the **Remote Destination Port** to align with optical 10-GB Ethernet port that was used in Procedure 3, "Connect the monitoring ports," Step 1.

Step 4: In the **Switch Module** list, choose the module you wish to select sources from for monitoring. The **Available Sources** list populates with ports from that module and their relative port descriptions.

Step 5: Move the interfaces you want to monitor from Available Sources to Selected Sources.



Step 6: Click Submit. The SPAN session is created.

Step 7: In the active SPAN session window, click **Save**. This saves the SPAN session currently in the running-configuration to the startup-configuration.

	Session ID	Туре	Source	Dest. Port	Direction	Status
0	1	port	Te4/7 (Link to DC5548UPa Eth1/19) Te4/8 (Link to DC5548UPb Eth1/19)	Te4/4	Both Both	Active Active
[↑] Select an item then take an action> Refresh Create Save Edit Delete						

The preceding steps apply this configuration for creating a SPAN session on the Cisco Catalyst 6500 switch.

C6500_core# conf term

C6500_core(config)# monitor session 1 source interface Te4/7 - 8 both

C6500_core(config)# monitor session 1 destination analysismodule 2 data-port 1

C6500 core(config) # end

The preceding steps apply this configuration for creating a SPAN session on the Cisco Nexus 5000 switch.

1. Configuring the Destination Port

N5000_core# conf term N5000_core(config)# interface Te 4/4 N5000_core(config)# switchport monitor N5000_core(config)# end 2. Creating a SPAN Session N5000_core# conf term N5000_core(config)# monitor session 1 N5000_core(config)# source interface Te4/7 - 8 both N5000_core(config)# destination interface Te4/4

N5000 core(config) # end

Procedure 10 Set

Set up sites

Setting up sites in Cisco NAM enables site-level monitoring. You create a site for the campus and a site for the data center.

Step 1: Navigate to **Setup > Network > Sites**, and then 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 the desired value in the Subnet Mask box, and then click Detect.

	Subnet Detection				
Home Monitor▼ Analyze▼ Capture▼ Setup ▼ stup > Network > Sites > Site Configuration	* Subnet Mask	24		1 በ	-
	Data Source				
* Name Campus Core	Interface				
Description	Filter Subnets within Network	1		1	
	Unassigned Site	V		-	
Disable Site		Detect			Ξ
	Subnets	 Source Subnets 	Destination Subnets		
	1.1.1.0/24	-			
Site Rules 👔 Subnet Detect	10.1.1.0/24	-			
	10.255.251.0/24				
	10.255.252.0/24				
Submit Deset Cancel	10.255.253.0/24				
	10.255.254.0/24				
	10.255.255.0/24				
	10.4.0.0/24				
	10 4 1 0/24				-

Step 5: Select the appropriate rows, and then click Add to Site Rules.



Step 1: After creating sites, in the menu, choose 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. **Step 2:** If you want to view the Traffic Summary by a site, in the **Interactive Report** list, choose **Filter**, in the **Site** list, choose **campus** or **data center**, and then click **Submit**.



Process

Configuring Cisco Prime NAM on Cisco ISR G2 SRE

- 1. Install Cisco Prime NAM on SRE
- 2. Secure Cisco Prime NAM on SRE
- 3. Log in to Cisco NAM Traffic Analyzer GUI
- 4. Configure NAM for user authentication
- 5. Enable Cisco NAM packet monitoring
- 6. Set up sites
- 7. View the home dashboard

Requirements:

- Cisco Integrated Services Router (ISR) 2911, 2921, 2951, 3925 or 3945.
- Open slot for either Cisco Service Ready Engine (SRE) 710, or 910
 module.
- Cisco IOS release 15.1(4)M or later.
- Cisco Prime NAM software 5.1(2) for SRE, downloaded from the Cisco website 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 Cloud and Systems Management > Network Analysis Module (NAM) Products, select the appropriate NAM form factor, and then navigate to All Releases > 5 > 5.1.2.

Step 3: On the following file: nam-app-x86_64.5-1-2.bin.gz.zip, click Download Now.

Step 4: Copy the downloaded image to a local FTP server and unzip the contents into a folder.

Step 5: Log in to Cisco ISR G2 and configure the SRE interface for routerside (internal) and module-side (Cisco 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 10.5.0.18 255.255.252
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 Cisco SM-SRE and the router.

Example

Router# show running-config interface SM4/0
interface SM4/0
ip address 10.5.0.17 255.255.255.0
service-module fail-open
service-module ip address 10.5.0.18 255.255.252
service-module ip default-gateway 10.5.0.17

Next, if AAA has been enabled on the router, configure an AAA exemption for Cisco SRE devices.

Configuring an exemption on the router is required because when AAA is enabled on the router, you will be prompted for both a router login and a Cisco NAM login, which can be confusing. Disabling the initial router authentication requires you to create an AAA method, which you then apply to the specific line configuration on the router associated with Cisco SRE. Step 7: Create the AAA login method.

aaa authentication login MODULE none

Step 8: Determine which line number is assigned to SRE. The example output below shows line 67.

Example

RS200-3925-1# show run | begin line con 0 line con 0 logging synchronous

line aux O

line 67

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

```
stopbits 1
```

flowcontrol software

line vty 0 4

transport preferred none transport input ssh

Step 9: Restrict access to the SRE console by creating an access-list. The access-list number is arbitrary, but the IP address must match the address assigned to the SM interface in the Step 5.

access-list 67 permit 10.5.0.17

Step 10: Assign the method to the appropriate line.

line 67
login authentication MODULE
access-class 67 in
transport output none

Step 11: Install Cisco Prime NAM on Cisco SRE. This command will take about 15 or 20 minutes to complete.

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

Example

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

Step 12: Open a session into Cisco NAM: service-module SM [slot]/0 session

Step 13: Log in to Cisco NAM by 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-910-K9) Console, 5.1(2) Copyright (c) 1999-2011 by Cisco Systems, Inc.

Step 14: 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 15: 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 16: Verify the network configuration is as follows:

root@nam.cisco.local# show ip

roorginam.crsco.rocar#	snow 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

Step 17: Configure Cisco NAM for network time.

time
sync ntp [ntp server]
zone [timezone]
exit

Example

root@NAM.cisco.local# time Entering into subcommand mode for this command. Type 'exit' to apply changes and come out of this mode. Type 'cancel' to discard changes and come out of this mode. root@NAM.cisco.local(sub-time)# sync ntp 10.4.48.17 root@NAM.cisco.local(sub-time)# zone PST8PDT root@NAM.cisco.local(sub-time)# exit

Step 18: Verify that the network time configuration is as shown.

root@NAM.cisco.local# show time	2
NAM synchronize time to:	NTP
NTP server1:	10.4.48.17
NAM time zone:	PST8PDT
Current system time:	Thu Jun 28 16:04:01 PDT 2012

Procedure 2

Secure Cisco Prime NAM on SRE

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

- Enable secure sockets layer (SSL) on Cisco NAM for secure, encrypted HTTP sessions.
- Enable SSH protocol for secure Telnet to Cisco NAM.

Step 1: Enable SSH for direct access to Cisco Prime NAM on Cisco SRE.
root@nam.cisco.local# exsession on ssh

Step 2: Enable the Cisco 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

Log in to Cisco NAM Traffic Analyzer GUI

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

Step 1: In your browser's address box, enter the full hostname of Cisco Prime NAM: https://[machine_name].[domain] (Example: nam.cisco.local)

Step 2: When the login window appears, enter the administrator username and password that you configured in Procedure 2, "Secure Cisco Prime NAM on SRE," Step 3, and then click Login.

Cisco Prime Network Analysis Module Version 5.1(2)
Username
Password
Remember username Problems logging in?
© 2011 Cisco Systems, Inc., Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Procedure 4

Configure NAM for user authentication

Optional

If you have a centralized TACACS+ server, configure secure user authentication as the primary method for user authentication (login) and user authorization (configuration) by enabling AAA authentication for access control. AAA controls all management access to the Cisco NAM (HTTPS).



Tech Tip

A local web administrator was created on the Cisco NAM during setup. This user account provides the ability to manage the device in case the centralized TACACS+ server is unavailable, or if you do not have a TACACS+ server in your organization.

Step 1: On the NAM web UI, navigate to Administration > Users > TACACS+.

Step 2: Enter the following values in the TACACS+ configuration page:

- Enable TACACS+ Authentication and Authorization selected
- Primary TACACS+ Server 10.4.48.15
- Secret Key SecretKey
- Verify Secret Key SecretKey

Step 3: Click Submit. The configuration is applied to Cisco NAM.

Enable TACACS+ Authentication and Authorization				
Primary TACACS+ Server	10.4.48.15			
Backup TACACS+ Server				
Secret Key	•••••			
Verify Secret Key	•••••			
Submit Reset				



Enable Cisco NAM packet monitoring

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

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

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

Example

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



Set up sites

Setting up sites in Cisco NAM enables site-level monitoring. You create a site for the campus and a site for the data center.

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

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

* Name	Data Center			
Description				
Disable Site				
Site Rules	Subnet Detect	Data Source	VLAN	
[10.4.48.0/24			\\$¥.
Submit Res	et Cancel			

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, in the Subnet Mask box, enter the desired value, and then click Detect. Select the appropriate rows, and then click Add to Site Rules.



Step 1: After creating sites, in the menu, choose 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.

Step 2: If you want to view the Traffic Summary by a site, in the **Interactive Report** list, choose **Filter**, in the **Site** list, choose **campus** or **data center**, and then click **Submit**.



Notes

Day 1+ Scenarios

This section walks you through a service-centric assurance approach to monitoring, analyzing and troubleshooting lifecycle for poor application performance, continuous packet capture, poor voice quality, and pre- and post- WAN optimization.

Process

Analyzing and 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 email
- 8. Set alarm actions
- 9. Set alarm thresholds
- 10. View alarm summary
- 11. Decode triggered packet capture
- 12. Scan for packet capture errors

An employee on campus calls the helpdesk because he/she have been experiencing delays with SharePoint (application). As a network engineer, a determination of where the problem lays either stemming from network congestion or severely impacted server needs to be assessed.

Currently the Cisco Catalyst 6500 Series NAM-3 is deployed in the campus and Cisco Prime NAM 2320 appliance is deployed in the data center. Either of these can be used to help with analysis and troubleshooting.

Since all application servers are hosted in the data center, the network engineer has configured a site called Data Center that can be used to filter by in the Interactive Report. You start with Response Time Summary dashboard in order to obtain an overview of application performance and then drill down to analyze if the issue is a result from an impacted server or a network congestion issue.

Once you complete the analysis and resolve the problem, you can take a pro-active approach by leveraging alarms to alert you and to capture packets should this issue happen in the future.

With Cisco NAM 2320 deployed in the data center, you have the option to leverage continuous packet capture and perform packet analysis when needed.

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 2: In the Interactive Report pane on the left, click Filter.

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





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**.



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: Open the dashboard by navigating to Analyze > Response Time > Application, and then 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 by clicking **Filter**, and in the **Time Range** list, choosing **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**.

Interactive Rep	port	Transaction Time - sharepoint		
Filter -	Export	ms		
A Site Data	Contor	1400		
Site	Data Cen	ter 💽		
DataSource				
VLAN				
* Application	sharepoint			
En ime Range	Custom			
From	12/1/2011	11 🗨 26 🗨		
From To	12/1/2011	11 💌 26 💌 12 💌 46 💌		
From To Filter Name	12/1/2011 12/1/2011	11 • 26 • 12 • 46 •		
From To Filter Name	12/1/2011 12/1/2011 Submit	11 26 2 12 46 2 Cancel		

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: On the Transaction Time report page, scroll down further to the **Other Metrics** chart.

Step 2: In the Metric 1 list, choose Average Network Time, which represents network delay.

Step 3: In the **Metric 2** list, choose **Average Server Response Time**, which represents server application delay.



Step 4: 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 by clicking **10.0.250.12**, and then clicking **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 email and trigger a packet-capture based on SharePoint response-time normal-trend values.

Step 1: Navigate to **Capture > Packet Capture/Decode > Sessions**, and then 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). This limits the size of the capture packets.

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

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

Step 6: Enter the following values:

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

Name	SharePoint_Ca	pture			
Packet Slice Size (bytes)	500				
Capture Source	 Data Ports 		Software Filter Dialog	×	
	○ ERSPAN	~	* Name	SharePoint	
Storage Type	 Memory 		Source Address / Mask		
		Me	Destination Address / Mask		
			Network Encapsulation		
	File(s)			Both Directions	
		File	VLAN Identifier(s)		
		Nur	Application or Port	 None Application Ports 	
			Application	sharepoint 💽 🚺	
		File	Source Port(s)		
			Destination Port(s)		
	Name		IP Protocol	•	
				Apply Cancel Reset	
					-
Create Edit Delet	te				

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

Procedure 7 Set up Cisco NAM alarm email

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** box, enter one or more email addresses that will receive the Cisco NAM alarm mail. Use a space to separate multiple email addresses.

Step 4: Click Submit.

Procedure 8

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

* Name	3harePoint_rise				
Actions					
🗹 Email					
Change Ema	ail Server Settings: Administration > System > E-Mail Setting				
🗌 Trap					
Enter Trap Se	Enter Trap Settings: Administration > System > SNMP Trap Setting				
📝 Trigger C	apture				
S	ession SharePoint_Capture				
۲) Start 🔿 Stop				
Enter Capture	e Session Settings: Capture > Packet Capture/Decode > Sessions				
Syslog					
Change Sysl	og Settings: Administration > System > Syslog Setting				
Submit Re	eset Cancel				

Step 2: Enter a description of the alarm event. (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, "Set up Cisco NAM alarm email."

Step 4: Select Trigger Capture.

Step 5: In the **Session** list, choose **SharePoint_Capture** (configured in Procedure 6, "Set up packet capture session"), and then select **Start**. This will start a packet capture when the threshold on the rising value is violated.

Step 6: Click Submit.

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

Step 7: Next, create a second event for the falling edge alarm action, repeat Step 1through Step 6 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 Time tab.

Step 3: Enter a name for the response time threshold. (Example: SharePoint_ResponseTime)

Step 4: In the Application list, choose sharepoint.

Step 5: Under Server, in the Site list, choose Data Center, and then in the Host list, choose 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, "Set alarm actions," 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. In the Rising list, choose 10,000 milliseconds, and then in the Falling list, choose 8,000 milliseconds.



Tech Tip

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

Host Co	onversa	tion Applicatio	n Response	Time DSC	P RTP	Streams Voice	e Signaling	NDE Inte	rface		
* N	lame	SharePoint R	sponseTime		1						
* Applic	ation	abaranaint]						
Applied	auon	snarepoint									
* Sei	verity	High		-							
Client						Server					
	Site			•		* Site	Data Cer	nter			
н	lost [* Host	Any				
							Ally				
Actions											
Actions	. r										
RIS	sing	SharePoint_rise				Falling	SharePo	int_fall		•	
Create f	New Ad	tions: Setup > Ala	arms > Actions								
Respon	se Time	Metrics									
	/	Average Respon	se Time	-	* Rising	10,000		* Falling	8,000		Delete
Add Me	etrics										
Submit	Rese	t Cancel									

Step 8: Click Submit.

Procedure 10 View alarm summary

When you receive an email 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. You can help reduce time and effort in analyzing the packet capture by invoking Error Scan to quickly view just the packets with anomalies.

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

Step 2: Identify the SharePoint application.



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



Decode triggered packet capture

Step 1: Navigate to **Capture > Packet Capture/Decode > Sessions**, and then select the **SharePoint_Capture** (configured in Procedure 6, "Set up packet capture session") that was triggered when the SharePoint threshold was violated.

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

Packets:	1-1000 of	55885		Stop Pre	/ Next	1000	Go to 1	Display Filter	TCP Stream
Pkt	Time(s)	Size	Source		Destinat	tion	Protocol	Info	^
1	0.000	259	10.0.250.13	10.1	5.13.30		TCP	ITCP seament of a rea	ssembled PDUI
2	0.000	70	10.0.250.13	10.1	5.13.28		TCP	80 > 59854 [ACK] Sea:	=1657977830 Ack=2928
3	0.000	70	10.0.250.13	10.1	5.12.28		тср	80 > 25867 [ACK] Sea	=1647032033 Ack=1306
4	0.000	70	10.0.250.13	10.1	5.12.23		TCP	80 > 25860 [ACK] Sea	=1651154758 Ack=1314
5	0.000	70	10.0.250.13	10.1	5.12.26		TCP	80 > 25863 IACKI Sea	=1659848864 Ack=1307
6	0.000	70	10.0.250.13	10.1	5.12.21		тср	80 > 25861 [ACK] Sea	=1659038035 Ack=1305
7	0.000	70	10.0.250.13	10.1	5.12.30		TCP	80 > 49296 [ACK] Sea	=1600463226 Ack=1269
8	0.000	70	10.0.250.13	10.1	5.12.26		тср	80 > 25858 IRST. ACK	l Sea=1648530766 Ack=
9	0.000	64	10.0.250.13	10.1	.12.16		TCP	80 > 4252 [ACK] Sea=1	1656686779 Ack=16376
<u>10</u>	0.000	64	10.0.250.13	10.1	.12.16		ТСР	80 > 4252 [ACK] Sea=1	1656686779 Ack=16376
+ ETH + IP - TCP TCP TCP TCP TCP TCP TCP	Ether Intern So De St Se Act He Fla	met II, 1 net Pro smissi urce p stinatio ream in quenco ext seq knowle ader le ader le	Src: 00:0a:00:fa:(tocol, Src: 10.0.2 on Control Proto- ort: 80 (80) on port: 60055 (6 ndex: 0) e number: 16586 uence number: 1 dgement numbe ngth: 32 bytes 18 (PSH, ACK))b:02 (00:0a:0 50.13 (10.0.25 col, Src Port: 8 0055) (52495 658652684) r: 293087301	0:fa:0b:02), 0.13), Dst: 0 (80), Dst	, Dst: 00:0 : 10.15.13 : Port: 600	0:00:07:ac:d3 30 (10.15.13 55 (60055), 8	3 (00:00:00:07:ac:d3) .30) Jeq: 1658652495, Ack: 2	2930873015, Len: 189
0000 0010 0020 0030 Close	00 00 0c 00 fl a0 0d le 00 <u>0a 8b f3</u>	07 ac c2 00 50 es c1 00	: d3 00 0a 00 1 00 40 06 be (97 62 dd 07 4 00 01 01 08 (fa Ob O2 O8 Da Oa OO fa 4f ae b1 92 Da 38 74 6e	00 45 00 0d 0a 0f b7 80 18 25 20 13	:		E. 	*



Scan for packet capture errors

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

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

Step 3: Click Save To File.

Step 4: On the Save File dialog box, provide a New File Name, and then click OK.

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

Step 6: Click **Errors Scan.** The Capture Errors and Warnings Information dialog box opens.

Step 7: On the Capture Errors and Warnings Information dialog box, select a packet with an anomaly, and then click **Decode Packets**. You can further analyze the packet and continue troubleshooting.

					Show All	
Packet lo	Protocol	Severity	Group	Description		
17105	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
17106	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
17107	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
17108	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
17781	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
17782	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
17783	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
17784	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
18382	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
18383	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
18384	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
18386	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
18985	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
18986	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
18987	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
18988	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
19597	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
19598	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
19599	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
19601	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		
20236	eth:vlan:ip:tcp:opsi	Warn	Reassemble	Unreassembled Packet (Exception occurred)		

Process

Configuring Continuous Packet Capture

1. Create a capture session

The Cisco Prime NAM 2320 appliance can be configured with 24x1-TB hard disk drives, of which, approximately 20 TB are used for packet capture. In this example, the IT manager wants to continuously capture application server traffic. If there is any anomaly detected during the analysis of the dashboards or from the alarms, the IT manager can decode the packet capture that has been running in the background on the NAM.



Create a capture session

Step 1: Navigate to Capture > Packet Capture/Decode > Sessions.

Step 2: Click Create. A packet capture session is created.

Step 3: Enter an appropriate name for the packet capture session (Example: Continous_capture), and then select the appropriate Data Ports to capture (Example: Data port 1 and 2).

Step 4: For storage type, select **Files**, and then enter the appropriate file size (ranging from 1 MB to 2,000 MB).

Step 5: Enter the number of files to be created for this session, and then select **Rotate Files**. Leave the default **File Location** setting to Local Disk.

apture > Packet Capture/Deco	de > Sessions > Configure Capture Session
Name	Continous_capture
Packet Slice Size (bytes)	500
Capture Source	Data Ports
	✓ DATA PORT 1 ✓ DATA PORT 2
	O ERSPAN
Storage Type	O Memory
	Memory Size (MB)
	Wrap When Full
	• File(s)
	File Size (MB) 2,000
	Number Of Files 10
	✓ Rotate Files
	File Location [SAS] Local Disk (19076949 MB free)
0.7	
Software Filters	Name
	No data available
	No data available
Create Edit Dele	te
Submit Banat Cana	
	<u></u>

Step 6: Create packet capture filters. You can use a combination of either hardware filters or software filters, or both, for the capture session.

If you want to use software filters, in the Software Filters section (in the packet capture session), click **Create**, fill in the appropriate filters, click **Apply**, scroll down, and then click **Submit.** The capture session is created.

Name	SharePoint_Ca	pture		
Packet Slice Size (bytes)	500			
Capture Source	 Data Ports 		Software Filter Dialog	×
		V	* Name	SharePoint
Storage Type	 Memory 		Source Address / Mask	
		Me	Destination Address / Mask	
			Network Encapsulation	
	 File(s) 			✓ Both Directions
		File	VLAN Identifier(s)	
		Nur	Application or Port	○ None
			Application	sharepoint 💽 🚺
		File	Source Port(s)	
Software Filters			Destination Port(s)	
Id	Name		IP Protocol	•
				Apply Canaal Baast
Create Edit Delet	e			

If you want to use the hardware filters, in **Capture > Packet Capture/ Decode > Sessions** dashboard, scroll down to the Hardware Filters section, and then click **Create**. In the Hardware Filter dialog box, name this filter Application_Servers.

Step 7: Since the application servers sit in VLAN 2 and 3, select **Type** as VLAN, and then in the Individual VLAN input, enter **2** and **3**.

Next, start continuous packet capture.

Step 8: Once the filters have been applied, select the row Continuous_capture, and then click Start.

Can	ture Sessions						
Tota	al Buffer Memory 20480 MB Allocated 50	00 MB Available 1	5480 MB				
	Name	Start Time	Size (MB)	Packets	State	Location	
	Continous_capture		2000(MB) x 1000	0	Stopped	[SAS] Local Disk	
۲	Sharepoint_Alarm	2012-Sep-29, 00:50:00	5000	97,260	Stopped	Memory	
				Hard	ware Filter Dialog		×
					Name Applica	tion_Servers	
					Type VLAN		
Creat	te Edit Delete Start Stop Clea	r Decode Save To	File	VL	AN Ids Range	0 ·	
					Individual	Is • 2 3	
Har	dware Filters						
	Name	Туре					
۲	Application_Servers	VLAN				Apply Canc	el Reset
۲	Worm	Payload Data					
0	te Edit Delete						



In this scenario, you are an IT network manager. You currently have deployed Cisco Prime NAM on Cisco ISR G2 SRE 710 in the Singapore regional office and have configured two sites called regional office and a campus to filter by in the Interactive Report.

To resolve a scenario in which a couple of users have opened a trouble ticket that describes their recent experience of choppy audio during a call, follow the procedures below.

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 Mean Opinion Score (MOS) values.

Enable Call Signal Monitoring 🔽	
MOS Quality Ranges	
Excellent 4.34	and above
* Good 4.03	and less than Excellent
* Fair 3.60	and less than Good
Poor 0.0	and less than Fair
Submit Reset	

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



- Step 1: Navigate to Analyze > Media > RTP Streams.
- Step 2: In the Interactive Report pane on the left, click Filter.

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

Step 4: For **Time Range**, specify the Last 1 hour, and then click **Submit**. The RTP Streams chart appears.



Next, analyze poor MOS values.

Step 5: Use the slider controls on the bar to zoom in to a time interval. In the following figure, there are a total of 41 RTP-streams, with one RTPstream rated as poor MOS value and three RTP-streams rated as 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: If you want to further analyze an RTP-stream, select an endpoint from the Top N RTP Streams by Adjusted Packet Loss % chart, click a datapoint of interest, and then click **RTP Stream Details**.



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

RTP	Stream Information (T	ime Range From	n: 2011-Dec-1	19, 20:15	To: 2011-Dec	-19, 20:31)			
\bigcirc	Source IP Address / Port :	192.168	138.201:2887	74					
	Destination IP Address / Po	ort : 10.15.11	.10:18136						
\bigcirc	SSRC :	1710092	282						
۲	Codec:	G711 UI	aw 64K						
RTP	RTP Stream Stats Summary								
\bigcirc	Duration monitored:		2						
\bigcirc	Worst / Duration Weighted	/ Max MOS :	3.95	5/3.95/3.95					
\bigcirc	Worst / Duration Weighted	/ Min Jitter (ms) :	0.90	0/0.90/0.90					
\bigcirc	Worst / Overall / Min Actual	Packet Loss (%) :	3.6	/ 3.6 / 3.6					
\bigcirc	Worst / Overall / Min Adjust	ed Packet Loss (%): 3.6	/ 3.6 / 3.6					
\bigcirc	Worst / Total / Min Conceal	ment Seconds:	2/2	2/2					
\bigcirc	Worst / Total / Min Severe C	Concealment Seco	nds: 1/1	/1					
RTP	Stream Stats Details								
							[Show All	- 7
	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

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.

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	

Process



Deploying Pre- and Post- WAN Optimization

- 1. Identify performance challenges
- 2. Baseline acceptable app performance
- 3. Send WAAS Flow Agent (FA) to NAM
- 4. Analyze impact of WAN optimization
- 5. Monitor and analyze WAN optimized traffic
- 6. Troubleshoot a WAN-optimized network

IT network managers are tasked with deploying WAN optimization, including data center server and storage consolidation efforts to protect data, increased availability, and a reduction in the number of devices to manage, so the distributed workforce can benefit from LAN-like performance over WAN for enterprise applications. WAN optimization helps employees be more productive and drive bottom-line revenue and profits.

To roll out WAN optimization, the IT network manager needs to identify which site has application performance issues and to be able to quantify the application performance. Once a site is selected for WAN optimization deployment, the IT network manager needs to validate the impact of WAN optimization, monitor ongoing optimization, and troubleshoot WAN optimized traffic. Follow the procedures below to leverage Cisco NAM in order to provide visibility to Cisco Wide Area Application Services (WAAS) lifecycle deployment.

For details about how to deploy WAAS, see the Cisco SBA—Borderless Networks Application Optimization Deployment Guide.

Identify performance challenges

In this procedure you identify sites, application, or hosts with application performance challenges.

Step 1: Navigate to Monitor > Overview > Site Summary dashboard. This dashboard shows sites with highest average transaction time and sites with highest traffic rate.

Step 2: Select sites that would benefit most from WAN optimization. For the initial rollout of Cisco WAAS, this guide uses the San Jose Campus site.



Next, Select application, clients (in a site) or servers (in a site) for WAN optimization.

Step 3: Navigate to Analyze > WAN Optimization > Top Talkers Detail dashboard.

This page provides details on top applications, clients, servers and network links with additional information on connect counts and average transaction time. You can use this page to determine the top application protocols by transaction time, connection count, as well as by data volume and data rate. You can use the Servers chart on this page to add top servers to the Cisco WAAS monitoring list. Application servers with high volume or with high transaction time can be good candidates for WAAS monitoring.

Tech Tip

It is important to select the site and the data sources on this page in order to avoid duplicate counting of the traffic unless the site defined already has a data source filter.

Applications					_	Ne	twork Link	s						
		[Show All	-	8							Show All		1
Applications	Bits/sec	Average Concurre Connections	Average Transaction Time (ms)			с	lient Site	Server S	ite Bits/sec	Average Concurren	t 1	werage Transaction Time	Average Network Tim	e
https	16,644,751.25	159.58	410		^					Connection	ns (ms)	(ms)	
cifs	14,688,633.97	8.16	85			IN	ID Branch	Data Ce	nter - 250,837	-24 -	3	897	80	
http	10,479,568.28	191.61	531					WAAS	470.07	20 4.02		100		
ftp-data	3,260,485.55	61.55			=		nassigned	Operado	ns 178,974	.30 4.83		1,420	0	
sharepoint	2,158,368.24	144.17	1,041			N N	AAS	RTP Bra	nch 100,969	.90 2.28	1	185	36	
sap	1,139,026.91	54.95	58					Data Ce	nter co.o.e.	40.70		10	10	
citriximaclient	917,105.06	54.91	471				ata Center	Internal	60,215.	58 10.76	4	12	40	
pcsync-https	757,852.67	4.52	355			D	ata Center -	LA Bran	h 32,577.	36 0.54	3	95	50	
ftp	686,175.56	308.10	104			N N	AAS	Unanaia	ned 00.700			580	0	
ica	92,765.20	7.50	85				perations on loco	Data Co	neu 20,799.	24 1		,565	v	
unknown	40,087.63	4.45	6,931			c	ampus	Internal	16,135.	16 5.34	4	16	43	
telnet	20,738.40	15.20	87			U	nassigned	NY Bran	ch 14,193.	30 0.44	4	16	2	
bittorrent	16,135.16	5.34	46			D	ata Center -							
veritas-netbackup	15,316.20	2.74	42			N	/AAS	IND BIA	ich 14,100.	52 -			01	
ssh	14,038.09	15.30	470		-	U	nassigned	SF Bran	:h 5,285.1	9 1.83	3	3,670	51	
Clients						Se	rvers							
		[Show All	-	8							Show All	•	
Clients	Bits/sec	Average Concurre Connections	Average Transaction Time (ms)				Servers		Applications	Bits/sec	- Av	erage oncurrent	Average Transa Time (ms)	ction
10.86.148.216	10,488,188.83	0	5,217		^						C	onnections	(iii)	
192.168.152.38	10,438,684.56	0.34	24		=		192.168.1	38.124	https	10,486,239.79	9 -		773	
10.11.102.101	1,257,429.31	15.19	-			E	192.168.1	38.161	cifs	10,438,395.68	3 0.:	24 :	24	
10.11.102.102	1,257,277.57	15.19	1. A. C.			E	10.0.250.1	1	cifs	4,196,299.84	8.	85 8	B3	
10.15.12.22	1,160,454.19	33.17	95				10.0.250.1	2	http	764,483.29	50	.17	908	
10.15.12.21	1,146,013.26	32.78	95				10.0.250.1	4	http	756,751.78	50	.55	893	
10.15.12.24	753,101.77	29.12	94				10.0.250.1	5	http	749,829.03	49	.56	864	
10.15.12.23	750,591,13	28.93	94			E	10.0.250.1	1	http	748,854.10	50	.99	886	

Step 1: Navigate to Analyze > Response Time > Application dashboard.

In the **Filter** list, select the **San Jose Campus** site, the Time Range for **last 1 day**, and Application as **SharePoint**. The resulting analysis can help you understand Sharepoint performance and quantify response time by network time, server response time, and data transfer time. A comparison can be done later after Cisco WAAS is deployed in order to understand the improved application performance.



Procedure 3

Send WAAS Flow Agent (FA) to NAM

After Cisco WAAS is deployed, you need to configure the Cisco WAAS device to send WAAS FA to Cisco NAM.

Step 1: In your browser's address box, enter the full hostname of Cisco WAAS Central Manager, https://[Machine Name].[Domain]:8443 (Example: CM.cisco.local).

Step 2: In **Central Manager > Devices**, select the remote site Wide Area Application Engine (WAE) device.



Step 3: Select Configure > Monitoring > Flow Monitor. This enables FA to Cisco NAM.



Step 4: Enter the IP address of the Cisco NAM appliance, and then click Submit.

Step 5: Select Enable, and then click Submit.

Cisco Wide Are	a Application Services jure > Monitoring > Flow Monitor	Home RS200-1	Device Groups	Devices . Configu	AppNav Cluster: ire 🔻 Moniti	s Locations or I ▼ Admin I ▼		
Flow Monitor Settings f	or WAE, <i>RS</i> 200- <i>WAVE</i> 7541-	1 🥸 Print 🎢	Apply Defaults	👕 Remove D	evice Settings			
Flow Monitor Settings								
Current applied settings from WAE, RS200-WAVE7541-1								
Enable:								
Destination:	10.4.41.2 IP ad	ldress						
Change submitted.						Submit Cancel		

Step 6: Repeat Step 1through Step 4for campus or data center head-end Cisco WAE device.

Step 7: Validate Cisco WAAS FA is received on Cisco NAM by navigating to Setup > Traffic > NAM Data Sources.

Step 8: For the Cisco WAE device deployed at the remote site, define the traffic source as Client, CltWAN, and Passthru (Example: WAEVB674LOWTEST2, as shown in the following figure). For the WAE device deployed at the head-end, define that traffic source as Server, SvrWAN, and Passthru (Example: WAE-1-DC, as shown in the following figure).

192.168.136.43	WAAS	WAE-1-DC (78:e7:d1:7a:b4:f4) Cisco WAAS 4.4.0-b111 [OE574] Last collection: Wed Oct 31 17:58:37 2012 (147436 bytes	ACTIVE	WAE-192.168.136.43-SvrWAN, WAE-192.168.136.43-Server, WAE-192.168.136.43-Passthru
192.168.136.53	WAAS	WAE-2-DC (00:26:55:ae:94:90) Cisco WAAS 4.4.0-b111 [OE574] Last collection: Wed Oct 31 17:58:34 2012 (147436 bytes	ACTIVE	WAE-192.168.136.53-Passthru, WAE-192.168.136.53-Client, WAE- 192.168.136.53-CltWAN
172.20.122.224	WAAS	WAEVB674LOWTEST2 (00:21:5e:28:85:78) Cisco WAAS 4.1.3-b55 [OE674] Last collection: Wed Oct 31 17:57:50 2012 (188 bytes	ACTIVE	WAE-172.20.122.224-Client, WAE- 172.20.122.224-CltWAN, WAE- 172.20.122.224-Passthru

Next, configure the application servers for Cisco WAE to monitor and send relevant information to Cisco NAM.

Step 9: Navigate to Setup > Monitoring > WAAS Servers.

Step 10: As you did in Procedure 1, "Identify sites, application or hosts with application performance challenges," Step 2, you can use the application server information and add it (for instance, IP addresses) in the table.

Setup > Monitoring > WAAS Servers
Filter Response Time for all Data Sources by Monitored Servers
Select All
192.168.156.194
192.168.156.214
171.68.96.116
192.168.137.86
192.168.156.234
192.168.156.230
192.168.156.140

Step 11: Navigate to Setup > Traffic > NAM Data Sources and validate the status of Cisco WAAS FA is Active.



Tech Tip

If the Data Source is still Inactive, validate Procedure 3, "Send WAAS Flow Agent (FA) to NAM," again. You can check the Cisco WAAS FA packets counter on the Cisco WAE appliance to see if there are any drops by using the following command: show statistics flow monitor tcpstat-v1. Also, check that firewall policies are not blocking the ports that WAE and Cisco NAM use for data and control connection.

Analyze impact of WAN optimization

In order to display the pre- and post- WAN optimization in the dashboard, log onto Cisco WAAS Central Manager and disable optimization policy for the *before* trend. Once Cisco NAM collects a sufficient amount of data over a period of time, enable the optimization policy for the *after* trend.

Step 1: In Central Manager > Configure > Acceleration > Enabled Features, clear TFO Optimization and HTTP Accelerator.

alulu a satura a	Home Device Groups D	
cisco Cisco Wide Area App	lication Services	RS200-WAVE7541-1 V
Devices > RS200-WAVE7541-1 > Configure > A	cceleration > Enabled Features	
S Print 🎢 Apply Defaults 🔟 Rei	move Settings 🔇 Refresh	
Current applied settings from Device, R	\$200-WAVE7541-1	
TFO Optimization		
TFO Optimization		
Data Redundancy Elimination	DRE Settings	\oplus
Persistent Compression		
Accelerator Ontimization		
CIES Accelerator		
CIES Print Accelerator	Accelerator Ontimization	
EPM Accelerator	Accelerator optimization	
HTTP Accelerator	HTTP Setting	ıs ⊕
ICA Accelerator	ICA Settings	Ð
MAPI Accelerator	MAPI Setting	
Encrypted MAPI Traffic Optic	mization Mandatory En	cryption Configuration
NFS Accelerator		
SMB Accelerator	SMB Settings	⊕
SSL Accelerator		
Video Accelerator	Video Setting	as ⊕
Advanced Settings		
Blacklist Operation		
Blacklist Server Address Hold Time: *	60	(minutes) (1-10080)
		_
Submit Reset		

Step 2: After 30 minutes, select **TFO Optimization** and **HTTP Accelerator** again.

Step 3: Navigate to the Analyze -> WAN optimization -> Application Performance Analysis dashboard.

Step 4: Select the Client and Server site, along with application protocol. You can filter the data further by selecting the appropriate server IP address.

This dashboard shows overall trending of the client transaction time over time, as well as showing response time changes before (light green) and after (dark green) Cisco WAAS optimization. In addition, this report provides data compression ratio and connection counts over time information, all of which are important parameters in evaluating the overall impact of WAAS.





Monitor and analyze WAN optimized traffic

Step 1: Navigate to Analyze > WAN Optimization > Conversation Multi-segments.

This dashboard provides details in a table format, including the breakdown of network time on client LAN, WAN, and server LAN, as well as server response time and average transaction time.

Step 2: Filter information based on site, client IP, server IP, or application by using the Interactive Report Filter.

This level of detail greatly helps in problem isolation—administrators can determine whether a performance issue is caused by a congested WAN, slow server, or poor compression.

Audi-Segment													
												Show All	•
Client	Client Site	Server	Server Site	Application	Average Client Network Time (ms)	Average WAN Network Time (ms)	Average Server Network Time (ms)	Average Server Response Time (ms)	Average Transaction Time (ms)	Max Transaction Time (ms)	Client Traffic + Volume (bits/sec)	WAN Traffic Volume (bits/sec)	Server Traffic Volume (bits/sec)
10.1.12.12	RTP Branch	10.0.250.13	Data Center	sap	240	1	20	631	646	984	106.38	6.05	85.05
10.1.12.12	RTP Branch	10.0.250.11	Data Center - WAAS	sap	240	1	21	455	557	1,012	106.37	6.22	90.27
10.1.12.11	RTP Branch	10.0.250.12	Data Center - WAAS	citriximaclient	240	1	21	519	521	953	106.15	6.99	83.07
10.1.12.11	RTP Branch	10.0.250.12	Data Center - WAAS	sap	241	1	21	423	545	1,015	105.85	6.44	101.08
10.1.12.11	RTP Branch	10.0.250.13	Data Center - WAAS	sap	239	1	21	369	571	921	105.63	6.22	96.06
10.1.12.11	RTP Branch	10.0.250.11	Data Center - WAAS	citriximaclient	240	1	20	573	580	1,071	105.46	6.88	101.33
10.1.12.11	RTP Branch	10.0.250.15	Data Center - WAAS	sap	240	1	21	603	621	897	105.31	6.30	89.98
10.1.12.12	RTP Branch	10.0.250.14	Data Center - WAAS	sap	240	1	21	402	587	736	105.09	6.14	89.85
10.1.12.12	RTP Branch	10.0.250.15	Data Center - WAAS	sap	240	1	21	502	574	887	103.72	6.01	93.08
10.1.12.11	RTP Branch	10.0.250.13	Data Center - WAAS	citriximaclient	240	1	21	395	486	1,001	99.65	6.23	93.58
10.1.12.14	RTP Branch	10.0.250.13	Data Center - WAAS	sharepoint	240	1	20	758	28,776	82,278	98.06	1.18	36.56
10.1.12.14	RTP Branch	10.0.250.11	Data Center - WAAS	sharepoint	241	1	21	289	20,070	80,776	97.94	1.39	15.14
10.1.12.11	RTP Branch	10.0.250.14	Data Center - WAAS	sharepoint	216	1	20	569	73,382	110,876	97.80	1.16	24.35
10.1.12.12	RTP Branch	10.0.250.14	Data Center - WAAS	sharepoint	216	1	20	619	66,640	92,469	97.67	1.20	48.69
10.1.12.14	RTP Branch	10.0.250.12	Data Center - WAAS	sharepoint	241	0	21	516	30,335	80,377	97.67	1.38	60.88
10.1.12.13	RTP Branch	10.0.250.11	Data Center - WAAS	sharepoint	241	1	20	635	45,931	104,881	97.67	0.74	24.35
10.1.12.11	RTP Branch	10.0.250.13	Data Center	sharepoint	213	1	20	449	53,550	87,165	97.65	0.93	24.35

Procedure 6

Troubleshoot a WAN-optimized network

If you notice any anomaly in the analysis in Procedure 5, "Monitor and analyze WAN optimized traffic," you can invoke Cisco NAM's packet capture to do a packet analysis. For details about how to set up a packet capture, see Procedure 6, "Set up packet capture session," in the "Analyzing and Troubleshooting Application Performance" process earlier in this guide.

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.





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/partner/products/ps5740/ Products_Sub_Category_Home.html

Product portfolio:

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

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

Cisco NAM 2300 Series appliances

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

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

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

Installation 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 NAM 2300 Series appliances

http://www.cisco.com/en/US/partner/docs/net_mgmt/network_analysis_ module_appliance/2300/installation/guide/2300-series-install-config.html

Cisco Prime Network Analysis Module (NAM) for Cisco 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) and 5.1(3) user guides

http://www.cisco.com/en/US/partner/docs/net_mgmt/network_ analysis_module_software/5.1.3/user/guide/nam_ug_book.html

Cisco Prime Network Analysis Module 5.1(2) software download

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



Appendix A: Product List

Network Management

Functional Area	Product Description	Part Numbers	Software	
LAN Core NAM Appliance	Cisco Prime NAM 2320 Appliance (With 16x1TB STAT II Drives)	NAM2320-K9	5.1(3)	
LAN Core NAM 6500 Module	Cisco Catalyst 6500 Series Network Analysis Module (NAM-3)	WS-SVC-NAM3-6G-K9	5.1(2)	
Remote-Site NAM SRE	Cisco SRE 910 with 4-8 GB RAM, 2x 500 GB 7,200 rpm HDD, RAID 0/1, dual- core CPU configured with ISR G2	SM-SRE-910-K9	5.1(2)	
	Cisco Prime NAM Software 5.1 for ISR G2 SRE SM	SM-NAM-SW-5.1-K9		
	Cisco SRE 710 with 4 GB RAM, 500 GB 7,200 rpm HDD, single-core CPU SM-SRE-710-K9 configured with Cisco ISR G2			
	Cisco Prime NAM Software 5.1 for ISR G2 SRE SM	SM-NAM-SW-5.1-K9		

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

LAN Core Layer

Functional Area	Product Description	Part Numbers	Software
Modular Core Layer Switch	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	IP services license
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
	Cisco Catalyst 6500 8-port 10GbE Fiber Module w/ DFC4	WS-X6908-10G-2T	

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.1(3)N1(1a)
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	Layer 3 License

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software	
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M5	
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	securityk9 license	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	datake license	
	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9		
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9		
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9		
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9		

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We replaced Cisco NAM-2220 with the Cisco NAM-2320 appliance.
- We added Continuous Packet Capture and Pre- and Post- WAN Optimization to Day 1+ Scenarios.



Feedback

Please use the feedback form to send comments and suggestions about this guide.



cisco.

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITH-OUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS ON TO CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CINSC.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)