



## **Cisco Nexus 1000V NAM Virtual Service Blade Installation and Configuration Guide**

NAM 4.2  
April 2010

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-21578-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE 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 TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

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.

*Cisco Nexus 1000V NAM Virtual Service Blade Installation and Configuration Guide*  
© 2010 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## About This Guide iii

---

### CHAPTER 1

#### Overview 1-1

- Configuration Requirements 1-2
- Licensing 1-2
  - Node-Locking Information 1-2
  - Obtaining a License 1-2
  - Installing a License 1-2
  - Licensing Commands 1-3
  - Obtaining Licensing Information 1-3
    - About the NAM GUI 1-3
  - Audit Trail 1-4
  - System Alert 1-4
  - show tech Command 1-4

---

### CHAPTER 2

#### Installing NAM Virtual Blade Software 2-1

- Installing NAM Software on a Nexus 1010 Appliance 2-1

---

### CHAPTER 3

#### Configuring ERSPAN for Traffic Visibility 3-1

- About ERSPAN 3-1
  - ERSPAN Overview 3-1
  - Monitored Traffic 3-3
    - Monitored Traffic Direction 3-3
    - Monitored Traffic 3-3
  - ERSPAN Sources 3-3
    - Source Ports 3-3
    - Source VLANs 3-3
  - ERSPAN Destination Ports 3-3
- Prerequisites for Configuring ERSPAN 3-4
- Restrictions for Configuring ERSPAN 3-4
- Configuring ERSPAN on Cisco IOS Routers 3-4
  - Configuring an ERSPAN Port Profile 3-4
  - Configuring an ERSPAN Session 3-7

Configuring ERSPAN Data Source on the NAM VSB 3-10  
 Configuring a VLAN Data Source for ERSPAN Traffic 3-12  
     Monitoring VLAN Data Source 3-13  
     Deleting a VLAN Data Source 3-14  
 Configuring ERSPAN Reports on the NAM VSB 3-14

**CHAPTER 4**

**Configuring NetFlow for Traffic Visibility 4-1**

Configuring NetFlow on Cisco IOS Routers 4-1  
 Configuring NetFlow Data Source on the NAM VSB 4-2  
 Configuring NetFlow Reports on the NAM VSB 4-4

**CHAPTER 5**

**Configuring and Monitoring the Nexus Virtual Switch as a Managed Device 5-1**

Setting Up the Managed Device Parameters 5-1  
 Monitoring the Managed Device Interfaces 5-2

**CHAPTER 6**

**Troubleshooting 6-1**

Resetting the NAM Password 6-1



## About This Guide

---

**OL-21578-01**

The purpose of this document is to provide detailed steps to install the Cisco Network Analysis Module (NAM) Virtual Service Blade (VSB) on a Nexus 1010 Virtual Services Appliance, and then configure the NAM.

This document contains the following chapters:

- [Chapter 1, “Overview”](#)
- [Chapter 2, “Installing NAM Virtual Blade Software”](#)
- [Chapter 3, “Configuring ERSPAN for Traffic Visibility”](#)
- [Chapter 4, “Configuring NetFlow for Traffic Visibility”](#)
- [Chapter 5, “Configuring and Monitoring the Nexus Virtual Switch as a Managed Device”](#)
- [Chapter 6, “Troubleshooting”](#)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.





# CHAPTER 1

## Overview

---

The Cisco Nexus 1000V NAM Virtual Service Blade (VSB) provides a virtualization technology that enables a Nexus 1010 switch to host other services and applications. The Network Analysis Module (NAM) 4.2 is one such application that can be hosted on a Nexus 1010 switch.

This chapter contains the following sections:

- [About the Nexus 1010 Virtual Services Appliance, page 1-1](#)
- [Configuration Requirements, page 1-2](#)
- [Licensing, page 1-2](#)

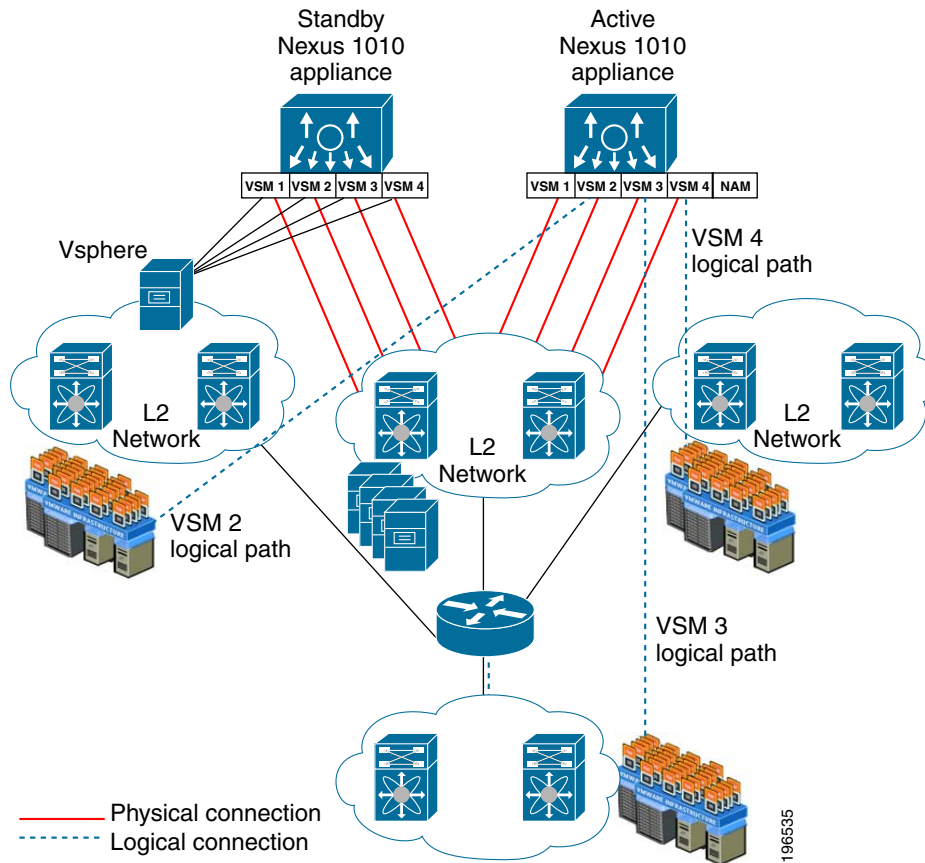
## About the Nexus 1010 Virtual Services Appliance

The Nexus 1010 appliance must have the following minimum resources available for use as a virtual blade:

- 2G RAM
- 53G disk space

[Figure 1-1](#) shows a NAM Virtual Service Blade deployment scenario using Cisco Nexus 1010.

Figure 1-1 Nexus 1010 in NAM VSB Deployment



## Configuration Requirements

Before you begin the software installation, ensure that the devices have been physically installed and set up for the following:

- The Nexus 1010 Virtual Services Appliance has network connectivity through an Ethernet interface and is accessible using the serial console.
- The NAM 4.2 VSB software image is available on the Nexus Virtual Services Appliance.
- The Nexus 1010 Virtual Services Appliance has adequate resources available to run NAM 4.2.

## Licensing

The NAM virtual blade software requires you to install a product license in the form of a text file. An evaluation license allows you to use the software for up to 60 days, but you will be unable to log in to the NAM GUI after the evaluation license expires. When using an evaluation license, the NAM login window indicates how many days remain before the evaluation license expires.

## Node-Locking Information

The Cisco NAM license is used for one Nexus 1010 Virtual Services Appliance. When you obtain the license for the appliance, the license is valid only for the appliance with the PID and SN you provide when you obtain the license.

You can get the PID of the appliance using the **show inventory** CLI command.

```
vsm-nam1# show inventory
PID: N1K-674-K9 VID: 0 SN: KQEDKRON
vsm-nam1#
```

## Obtaining a License

To obtain a NAM Virtual Service Blade (VSB) license, go to the following URL:

<http://www.cisco.com/go/license>

Follow the instructions on this page to obtain a NAM VSB license file. You will need the appliance PID and SN to obtain the license file. After you enter the PID and SN or the Product Authorization Key, a license file will be sent to you by e-mail. Store this license file on an available FTP server. Use the **license install** command to install the license after the NAM software installation completes.

## Installing a License

To install a license file, use the **install license** command. See the next section, [Licensing Commands](#), and the *Network Analysis Module Command Reference Guide* for more information about the **install license** command.

The following is an example of the install license command:

```
license install ftp://joseph@computer.com/bin/licenses/NAM_VB_License.lic
```

In this example, the **install license** command fetches the license file, **NAM\_VB\_License.lic**, from the directory **/bin/licenses** of the host computer.com.

## Licensing Commands

This section describes NAM CLI commands used to install and manage the NAM VSB license. You can find more details about these commands in the *Network Analysis Module Command Reference Guide*:

[http://www.cisco.com/en/US/docs/net\\_mgmt/network\\_analysis\\_module\\_software/4.2/command/reference/guide/nam42\\_cmdref.html](http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.2/command/reference/guide/nam42_cmdref.html)



**Note** Technical documentation for NAM 4.2 will be available on [www.cisco.com](http://www.cisco.com) after this product is released to the public.

```
license install ftp://<username>@<host>/<path>/<licensefilename>
```

Use the **license install** command to install a license file.

```
show license
```

Use the **show license** command to display license information for the evaluation license and permanent licenses.

```
config upload ftp://<username>@<host>/<path> [configfilename] [licensefilename]
```

Use the **config upload** command to upload the license file. The *configfilename* and *licensefilename* options are optional.

```
config network ftp://<username>@<host>/<path>/<filename> <licensefilename>
```

Use the **config network** command to restore the license file.

## Obtaining Licensing Information

This section describes how to obtain current NAM VSB licensing information for a Nexus 1010 Virtual Services Appliance. You can obtain licensing information the following ways:

- Clicking **About** in the NAM Virtual Services Blade GUI; see [About the NAM GUI, page 1-4](#)
- Checking the audit trail; see [Audit Trail, page 1-4](#)
- Checking the system alert; see [System Alert, page 1-4](#)
- Using the **show tech** command; see [show tech Command, page 1-4](#)

### About the NAM GUI

When you click **About** in the upper right corner of the NAM VSB GUI, a window displays the software and version installed and information about any license currently installed. If a permanent license is installed, the PID and SN of the Nexus 1010 Virtual Services Appliance is also displayed.

### Audit Trail

The audit trail records any license management activities as well as any modifications to the configuration and other system information. To view the audit trail, click **Admin > Diagnostics**, then click **Audit Trail** in the Contents menu.

### System Alert

System Alerts record any alert generated by the NAM. There are system alert messages sent by the NAM as the days pass prior to the expiration of the Evaluation License. System alert messages are sent when there are 20, 15, 10, 5, 4, 3, 2, and 1 days remaining and again when the license expires.

### show tech Command

The **show tech** CLI command contains a license information section that displays information about the license type and license status.

You can also view the output of the **show tech** command from the NAM VSB GUI by clicking **Admin > Diagnostics > Tech Support**. To locate the license information, search for *licenseinfo*.



## CHAPTER 2

# Installing NAM Virtual Blade Software

---

This chapter provides information about installing the NAM 4.2 VSB software on a supported Nexus 1010 Virtual Services Appliance (N1K-C1010).



### Note

If you ordered a Cisco Nexus 1010 with NAM, the NAM installation media will already be loaded on the appliance. The installation media consists of an ISO file in `bootflash:/repository`.

If you have a Cisco Nexus 1010 without NAM software, and you want to add it, you will need to download it from Cisco.com to a local ftp or http server, and then install it using the command `copy ftp://path/to/nam/nam.iso bootflash:/repository`.

---

This chapter contains the following section:

- [Installing NAM Software on a Nexus 1010 Appliance, page 2-1](#)

## Installing NAM Software on a Nexus 1010 Appliance

---

**Step 1** Log in to the Nexus 1010 and enter virtual blade configuration mode:

```
vsm-nam1# conf t
```

**Step 2** List the contents of the repository.

```
vsm-nam1(config)# dir bootflash:/repository
...
153135104   Jan 20 09:37:17 2010   nam-4-2-1.iso
...

Usage for bootflash://sup-local
 305664000 bytes used
 3685715968 bytes free
 3991379968 bytes total
vsm-nam1(config)#
```

Use the directory listing to enter the correct ISO file that contains the NAM media.

In the example above, "nam-4-2-1.iso" is the filename, and the user is using this command to find the nam install media (an iso file found in `bootflash:/repository`).

**Step 3** Enter the virtual service blade creation mode.

```
vsm-nam1(config)# virtual-service-blade NAM
vsm-nam1(config-vb-config)#
```

**Step 4** Enter the NAM configuration information.

```
vsm-nam1(config-vb-config)# virtual-service-blade-type new
nam-4-2-1.iso
vsm-nam1(config-vb-config)# interface data vlan 3
vsm-nam1(config-vb-config)# enable
Enter vsb image:[nam-4-2-1.iso]
Enter Management IPV4 address: 172.20.122.107
Enter Management subnet mask: 255.255.255.128
IPv4 address of the default gateway: 172.20.122.1
Enter Hostname: nam-vsm1
Setting Web user/passwd will enable port 80. Press Enter[y/n]:y
Web User name: [admin]
Web User password: admin
vsm-nam1(config-vb-config)#
```

**Step 5** The NAM VSB installation will begin. You can use the **show virtual-service-blade summary** command to see the installation in progress.

```
vsm-nam1(config-vb-config)# show virtual-service-blade summary
```

**Step 6** When the status says “POWER ON,” you can log into the NAM console.

```
vsm-nam1# login virtual-service-blade nam
Telnet escape character is '$'.
Trying 127.1.0.18...
Connected to 127.1.0.18.
Escape character is '$'.

Cisco Network Analysis Module

nam.cisco.com login: root
Password:
Last login: Mon Mar 29 15:18:47 2010 from dhcp-171-69-69-187.cisco.com on pts/2

Cisco Virtual Blade on Nexus Appliance (Nexus VB) (R200-1120402) Console, 4.2(1)
Copyright (c) 1999-2010 by Cisco Systems, Inc.

root@nam.cisco.com#
```

---



## CHAPTER 3

# Configuring ERSPAN for Traffic Visibility

---

Encapsulated Remote Switched Port Analyzer (ERSPAN) records provide an aggregate view of the network traffic. When enabled on the branch router or switch, the ERSPAN data source becomes available on the Cisco NAM VSB. ERSPAN provides statistics for applications, hosts, and conversions. You can set up custom data sources for some specific interfaces. ERSPAN can be used to identify business critical applications hosted in the Data Center that are used in the branch.

This chapter contains the following sections:

- [About ERSPAN, page 3-1](#)
- [Prerequisites for Configuring ERSPAN, page 3-4](#)
- [Restrictions for Configuring ERSPAN, page 3-4](#)
- [Configuring ERSPAN on Cisco IOS Routers, page 3-4](#)
  - [Configuring an ERSPAN Port Profile, page 3-4](#)
  - [Configuring an ERSPAN Session, page 3-7](#)
- [Configuring ERSPAN Data Source on the NAM VSB, page 3-10](#)
- [Configuring ERSPAN Reports on the NAM VSB, page 3-15](#)

## About ERSPAN

### ERSPAN Overview

ERSPAN sessions allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports. ERSPAN sends traffic to a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. ERSPAN supports source ports, source VLANs, and destination ports on different routers, which provides remote monitoring of multiple routers across your network (see [Figure 3-1](#)).

ERSPAN consists of an ERSPAN source session, routable ERSPAN GRE-encapsulated traffic, and an ERSPAN destination session. You separately configure ERSPAN source sessions and destination sessions on different routers.

An ERSPAN source session is defined by the following:

- A session ID
- A list of source ports or source VLANs to be monitored by the session

- The destination and the origin IP addresses, which are used as the destination and source IP addresses of the GRE envelope for the captured traffic, respectively
- An ERSPAN flow ID
- Optional attributes related to the GRE envelope such as IP TOS and TTL.

For a source port or a source VLAN, the ERSPAN can monitor ingress, egress, or both ingress and egress traffic.

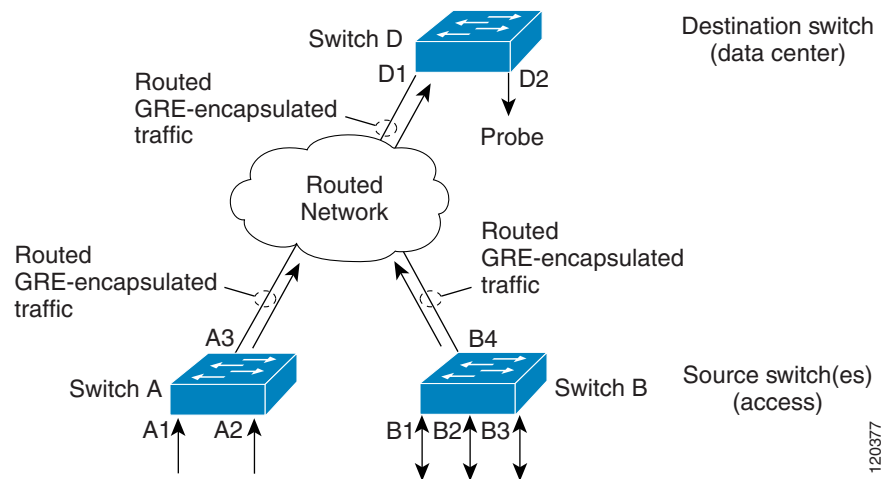
An ERSPAN destination session is defined by the following:

- A session ID
- A list of destination ports
- The source IP address, which is the same as the destination IP address of the corresponding source session
- The ERSPAN flow ID, which is used to match the destination session with the source session

ERSPAN source sessions do not copy ERSPAN GRE-encapsulated traffic from source ports. Each ERSPAN source session can have either ports or VLANs as sources, but not both.

The ERSPAN source sessions copies traffic from the source ports or source VLANs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session. The ERSPAN destination session switches the traffic to the destination ports.

**Figure 3-1 ERSPAN Configuration**



## Monitored Traffic

These sections describe the traffic that ERSPAN can monitor:

- [Monitored Traffic Direction, page 3-3](#)
- [Monitored Traffic, page 3-3](#)

### Monitored Traffic Direction

For a source port or a source VLAN, the ERSPAN can monitor ingress, egress, or both ingress and egress traffic.

### Monitored Traffic

By default, ERSPAN monitors all traffic, including multicast and bridge protocol data unit (BPDU) frames.

## ERSPAN Sources

These sections describe ERSPAN sources:

- [Source Ports, page 3-3](#)
- [Source VLANs, page 3-3](#)

### Source Ports

A source port is a port monitored for traffic analysis. You can configure source ports in any VLAN, and trunk ports can be configured as source ports and mixed with nontrunk source ports.

### Source VLANs

A source VLAN is a VLAN monitored for traffic analysis.

## ERSPAN Destination Ports

A destination port is a Layer 2 or Layer 3 LAN port to which ERSPAN sends traffic for analysis.

When you configure a port as a destination port, it can no longer receive any traffic. When you configure a port as a destination port, the port is dedicated for use only by the ERSPAN feature. An ERSPAN destination port does not forward any traffic except that required for the ERSPAN session. You can configure trunk ports as destination ports, which allows destination trunk ports to transmit encapsulated traffic.

## Prerequisites for Configuring ERSPAN

On the Cisco Nexus 1010 switch, a user can configure ERSPAN source sessions, destination sessions, or both. A device that has only ERSPAN source sessions configured is called ERSPAN source device, and a device that has only ERSPAN destination sessions configured is called ERSPAN termination device.

## Restrictions for Configuring ERSPAN

- The maximum number of ERSPAN sessions on a Cisco Nexus 1010 Virtual Services Appliance is 1024. A Cisco Nexus 1010 can be used as an ERSPAN source device on which only source sessions are configured, an ERSPAN destination device on which only destination sessions are configured, or an ERSPAN source and destination device on which both source and destination sessions are configured. However, the total session number cannot exceed the maximum session number of 1024.
- The maximum port number for each ERSPAN session is 128.
- ERSPAN on Cisco Nexus 1010 Virtual Services Appliance supports Fast Ethernet, Gigabit Ethernet, and Port-channel interfaces as source ports for a source session.
- ERSPAN users on Cisco Nexus 1010 Virtual Services Appliance can configure a list of ports as source or a list of VLANs as source, but cannot configure both for a given session.
- When a session is configured through the ERSPAN configuration CLI, the session ID and the session type cannot be changed. To change them, a user has to first use the **no** version of the configuration command to remove the session and then reconfigure the session.

## Configuring ERSPAN on Cisco IOS Routers

Configure ERSPAN traffic on the Branch edge router. You must enable ERSPAN on both the WAN and LAN interface to provide visibility into traffic flows entering and leaving the branch.

## Configuring an ERSPAN Port Profile

Use this procedure to configure a port profile on the VSB to carry ERSPAN packets through the IP network to a remote destination analyzer.

### BEFORE YOU BEGIN

- You are logged in to the VSM CLI in EXEC mode.
- This configuration must be completed for all hosts in the vCenter Server.
- You know the name to be used for this port profile.



**Note** The port profile name is used to configure the VMKNIC that is required on each of the ESX hosts.

- You know the name of the VMware port group to which this profile maps.
- You have the VMware documentation for adding a new virtual adapter.

- You have already created the system VLAN and you know its VLAN ID which will be used in this configuration.

## SUMMARY STEPS

1. **config t**
2. **port-profile** *port\_profile\_name*
3. **capability l3control**
4. **vmware port-group** *pg\_name*
5. **switchport mode access**
6. **switchport access vlan** *vlan\_id*
7. **no shutdown**
8. **system vlan** *vlan\_id*
9. **state enabled**
10. (Optional) **show port-profile name** *port\_profile\_name*
11. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>config t</b>  <b>Example:</b> vsm-nam1# config t vsm-nam1(config)#	Places you in the CLI Global Configuration mode.
Step 2	<b>port-profile</b> <i>port_profile_name</i>  <b>Example:</b> vsm-nam1(config)# port-profile erspan_profile vsm-nam1(config-port-prof)#	Creates the port profile and places you into CLI Global Configuration mode for the specified port profile. Saves the port profile in the running configuration.  The port-profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
Step 3	<b>capability l3control</b>  <b>Example:</b> vsm-nam1(config-port-prof)# capability l3control vsm-nam1(config-port-prof)#	Configures the port-profile to carry ERSPAN traffic and saves this in the running configuration.

	Command	Purpose
Step 4	<p><b>vmware port-group</b> <i>pg_name</i></p> <p><b>Example:</b>  vsm-nam1(config-port-prof)#vmware port-group  erspan  vsm-nam1(config-port-prof)#</p>	<p>Designates the port profile as a VMware port group and adds the name of the VMware port group to which this profile maps. Saves the settings in the running configuration.</p> <p>The port profile is mapped to a VMware port group of the same name. When a vCenter Server connection is established, the port group created in Cisco Nexus 1000V is then distributed to the virtual switch on the vCenter Server.</p> <ul style="list-style-type: none"> <li>• <b>pg-name:</b> Port group name. If you do not specify a pg-name, then the port group name will be the same as the port profile name. If you want to map the port profile to a different port group name, use the pg-name option followed by the alternate name.</li> </ul>
Step 5	<p><b>switchport mode access</b></p> <p><b>Example:</b>  vsm-nam1(config-port-prof)# switchport mode  access  vsm-nam1(config-port-prof)#</p>	Designates the interfaces as switch access ports (the default).
Step 6	<p><b>switchport access vlan</b> <i>vlan_id</i></p> <p><b>Example 1:</b>  vsm-nam1(config-port-prof)# switchport access  vlan 2  vsm-nam1(config-port-prof)#</p>	Assigns a VLAN ID to the access port for this port profile and saves the setting in the running configuration.
Step 7	<p><b>no shutdown</b></p> <p><b>Example:</b>  vsm-nam1(config-port-prof)# no shutdown  vsm-nam1(config-port-prof)#</p>	Enables the interface in the running configuration.
Step 8	<p><b>system vlan</b> <i>vlan_id</i></p> <p><b>Example:</b>  vsm-nam1(config-port-prof)# system vlan 2  vsm-nam1(config-port-prof)#</p>	<p>Associates the system VLAN ID with the port profile and saves it in the running configuration.</p> <p>Must match the VLAN ID assigned to the access port. If it does not match, then the following error message is generated:</p> <p>ERROR: System vlan being set does not match the switchport access vlan 2</p>
Step 9	<p><b>state enabled</b></p> <p><b>Example:</b>  vsm-nam1(config-port-prof)# state enabled  vsm-nam1(config-port-prof)#</p>	<p>Enables the port profile in the running configuration.</p> <p>This port profile is now ready to send out ERSPAN packets on all ESX Hosts with ERSPAN sources</p>

	Command	Purpose
Step 10	<p><b>show port-profile name</b> <i>port_profile_name</i></p> <p><b>Example:</b>  vsm-nam1(config-port-prof)# show port-profile  name erspan  port-profile erspan  description:  status: enabled  capability uplink: no  capability l3control: yes  system vlans: 2  port-group: access  max-ports: 32  inherit:  config attributes:  switchport access vlan 2  no shutdown  evaluated config attributes:  switchport access vlan 2  no shutdown  assigned interfaces:   vsm-nam1(config-port-prof)#</p>	(Optional) Displays the configuration for the specified port profile as it exists in the running configuration.
Step 11	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b>  vsm-nam1(config-port-prof)# copy running-config  startup-config  [#####] 100%  vsm-nam1(config-port-prof)#</p>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.
Step 12	Using the VMware documentation, go to vSphere Client and configure a VMKNIC on each ESX Host. Make sure the VMKNIC points to this port profile as a <b>new virtual adapter</b> .	

## Configuring an ERSPAN Session

Use this procedure to configure an ERSPAN session.

### BEFORE YOU BEGIN

- You are logged in to the VSM CLI in EXEC mode.
- You know the number of the SPAN session you are going to configure.
- You have already configured an ERSPAN-capable port profile on the VSM using the “[Configuring an ERSPAN Port Profile](#)” section on page 3-4.
- Using the VMware documentation for adding a new virtual adapter, you have already configured the required VMKNIC on each of the ESX hosts.
- SPAN sessions are created in the shut state by default.
- When you create a SPAN session that already exists, any additional configuration is added to that session. To make sure the session is cleared of any previous configuration, you can delete the session first (see [Step 2, no monitor session](#)).
- This procedure involves creating the SPAN session in ERSPAN Source Configuration mode.

## SUMMARY STEPS

1. **config t**
2. **no monitor session** *session-number*
3. **monitor session** *session-number* **type** **erspan-source**
4. **description** *description*
5. **source** {**interface** *type* | **vlan**} {*number* | *range*} [**rx** | **tx** | **both**]
6. (Optional) Repeat [Step 5](#) to configure additional ERSPAN sources.
7. (Optional) **filter vlan** {*number* | *range*}
8. (Optional) Repeat [Step 7](#) to configure all source VLANs to filter.
9. **destination ip** *ip\_address*
10. (Optional) **ip ttl** *ttl\_value*
11. (Optional) **ip prec** *ipp\_value*
12. (Optional) **ip dscp** *dscp\_value*
13. (Optional) **mtu** *mtu\_value*
14. (Optional) **erspan-id** *flow\_id*
15. **no shut**
16. (Optional) **show monitor session** *session\_id*
17. (Optional) **exit**
18. (Optional) **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	<b>config t</b>  <b>Example:</b> vsm-nam1# config t vsm-nam1(config)#	Places you in the CLI Global Configuration mode.
Step 2	<b>no monitor session</b> <i>session-number</i>  <b>Example:</b> vsm-nam1(config)# no monitor session 3	Clears the specified session.
Step 3	<b>monitor session</b> <i>session-number</i> <b>type</b> <b>erspan-source</b>  <b>Example:</b> vsm-nam1(config)# monitor session 3 type erspan vsm-nam1(config-erspan-source)#	Creates a session with the given session number and places you in the CLI ERSPAN Source Configuration mode. This configuration is saved in the running configuration.
Step 4	<b>description</b> <i>description</i>  <b>Example:</b> vsm-nam1(config-erspan-src)# description my_erspan_session_3 vsm-nam1(config-erspan-src)#	For the specified ERSPAN session, adds a description and saves it in the running configuration. <ul style="list-style-type: none"> <li>• description: up to 32 alphanumeric characters default = blank (no description)</li> </ul>

	Command	Purpose
Step 5	<p><b>source</b> {<b>interface</b> <i>type</i>   <b>vlan</b> {<i>number</i>   <i>range</i>} [<b>rx</b>   <b>tx</b>   <b>both</b>]</p> <p><b>Example 1:</b> vsm-nam1(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx</p> <p><b>Example 2:</b> vsm-nam1(config-erspan-src)# source interface port-channel 2</p> <p><b>Example 3:</b> vsm-nam1(config-erspan-src)# source interface vethernet 12 both</p> <p><b>Example 4:</b> vsm-nam1(config-erspan-src)# source vlan 3, 6-8 tx</p>	<p>For the specified session, configures the source(s) and the direction of traffic to monitor, and saves them in the running configuration.</p> <ul style="list-style-type: none"> <li>• <b>type:</b> Specify the interface type—ethernet, port-channel, vethernet.</li> <li>• <b>number:</b> Specify the interface slot/port or range; or the VLAN number or range to monitor.</li> <li>• <b>traffic direction:</b> Specify traffic monitoring to be in one of the following directions: <ul style="list-style-type: none"> <li>– receive (rx) (the VLAN default)</li> <li>– transmit (tx)</li> <li>– both (the interface default)</li> </ul> </li> </ul>
Step 6	(Optional) Repeat <a href="#">Step 5</a> to configure additional ERSPAN sources.	
Step 7	<p><b>filter vlan</b> {<i>number</i>   <i>range</i>}</p> <p><b>Example:</b> vsm-nam1(config-erspan-src)# filter vlan 3-5, 7</p>	<p>(Optional) For the specified ERSPAN session, configures the VLANs, VLAN lists, or VLAN ranges to be monitored; and saves this in the running configuration.</p> <p>On the monitor port, only the traffic from the VLANs which match the VLAN filter list are replicated to the destination.</p>
Step 8	(Optional) Repeat <a href="#">Step 7</a> to configure all source VLANs to filter.	
Step 9	<p><b>destination ip</b> <i>ip_address</i></p> <p><b>Example:</b> vsm-nam1(config-erspan-src)# destination ip 10.54.54.1 vsm-nam1(config-monitor-erspan-src)#</p>	<p>Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration.</p>
Step 10	<p><b>ip ttl</b> <i>ttl_value</i></p> <p><b>Example:</b> vsm-nam1(config-monitor-erspan-src)# ip ttl 64 vsm-nam1(config-monitor-erspan-src)#</p>	<p>(Optional) Specifies the IP time-to-live value, from 1-255, for the packets in the ERSPAN traffic, and saves it in the running configuration.</p>
Step 11	<p><b>ip prec</b> <i>precedence_value</i></p> <p><b>Example:</b> vsm-nam1(config-monitor-erspan-src)# ip prec 1 vsm-nam1(config-monitor-erspan-src)#</p>	<p>(Optional) Specifies the IP precedence value, from 0-7, for the packets in the ERSPAN traffic, and saves it in the running configuration.</p>
Step 12	<p><b>ip dscp</b> <i>dscp_value</i></p> <p><b>Example:</b> vsm-nam1(config-monitor-erspan-src)# ip dscp 24 vsm-nam1(config-monitor-erspan-src)#</p>	<p>(Optional) Specifies the IP DSCP value, from 0-63, for the packets in the ERSPAN traffic, and saves it in the running configuration.</p>

	Command	Purpose
Step 13	<b>mtu</b> <i>mtu_value</i>  <b>Example:</b> vsm-nam1(config-monitor-erspan-src)# <b>mtu</b> 1000 vsm-nam1(config-monitor-erspan-src)#	(Optional) Specifies an MTU size for the ERSPAN traffic, and saves it in the running configuration.
Step 14	<b>erspan-id</b> <i>flow_id</i>  <b>Example:</b> vsm-nam1(config-erspan-src)# <b>erspan_id</b> 51	Adds an ERSPAN ID (1-1023) to the session configuration and saves it in the running configuration.  The session ERSPAN ID is added to the ERSPAN header of the encapsulated frame and can be used at the termination box to differentiate between various ERSPAN streams of traffic.
Step 15	<b>no shut</b>  <b>Example:</b> vsm-nam1(config-erspan-src)# <b>no shut</b>	Enables the ERSPAN session and saves it in the running configuration.  By default, the session is created in the shut state.
Step 16	<b>show monitor session</b> <i>session_id</i>  <b>Example:</b> vsm-nam1(config-erspan-src)# <b>show monitor</b> <b>session</b> 3	(Optional) Displays the ERSPAN session configuration as it exists in the running configuration.
Step 17	<b>exit</b>  <b>Example:</b> vsm-nam1(config-erspan-src)# <b>exit</b> vsm-nam1(config)#	(Optional) Exits ERSPAN Source Configuration mode and returns you to CLI Configuration mode.
Step 18	<b>copy running-config startup-config</b>  <b>Example:</b> vsm-nam1(config)# <b>copy running-config</b> <b>startup-config</b>	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

## Configuring ERSPAN Data Source on the NAM VSB

Use the NAM Traffic Analyzer GUI to enable additional ERSPAN monitoring devices.

- 
- Step 1** Log in to the NAM GUI and choose **Setup > Monitor**.
- Step 2** Click the Data Source drop-down menu and choose ERSPAN.

**Step 3** Check the check boxes for the statistics that you would like to monitor.



**Note** We recommend that you check all check boxes to allow for full monitoring.

Monitoring Function		Max Entries
<input checked="" type="checkbox"/>	Application Statistics	
<input checked="" type="checkbox"/>	Host Statistics (Network & Application layers)	100
<input checked="" type="checkbox"/>	Host Statistics (MAC layer)	
<input checked="" type="checkbox"/>	Conversation Statistics (Network & Application layers)	500
<input checked="" type="checkbox"/>	Conversation Statistics (MAC layer)	
<input checked="" type="checkbox"/>	VLAN Traffic Statistics	
<input checked="" type="checkbox"/>	VLAN Priority (CoS) Statistics	
<input checked="" type="checkbox"/>	Network-to-MAC Address Correlation	
<input checked="" type="checkbox"/>	TCP/UDP Port Table	
<input checked="" type="checkbox"/>	MPLS Labels Statistics	

←-- Check desired functions then Apply -->

Apply Reset

**Step 4** There is a pull-down menu next to Host Statistics (Network & Application layers) and Conversation Statistics (Network & Application layers). You can optionally set the maximums for these statistics.

Monitoring Function		Max Entries
<input checked="" type="checkbox"/>	Application Statistics	
<input checked="" type="checkbox"/>	Host Statistics (Network & Application layers)	100
<input checked="" type="checkbox"/>	Host Statistics (MAC layer)	
<input checked="" type="checkbox"/>	Conversation Statistics (Network & Application layers)	100 1000 Max Possible
<input checked="" type="checkbox"/>	Conversation Statistics (MAC layer)	
<input checked="" type="checkbox"/>	VLAN Traffic Statistics	
<input checked="" type="checkbox"/>	VLAN Priority (CoS) Statistics	
<input checked="" type="checkbox"/>	Network-to-MAC Address Correlation	
<input checked="" type="checkbox"/>	TCP/UDP Port Table	
<input checked="" type="checkbox"/>	MPLS Labels Statistics	

←-- Check desired functions then Apply -->

Apply Reset

- Step 5** Click **Apply**.
- Step 6** To monitor the application statistics, go to the Monitor tab and click **Apps**. There are three different ways to view the data (Current Rates, TopN Chart, and Cumulative Data), as shown in [Figure 3-2](#). You can set filters for the data by using the Filter button.

**Figure 3-2 ERSPAN Application Statistics**

The screenshot shows the 'ERSPAN Application Statistics' interface. At the top, there are three radio buttons: 'Current Rates' (selected), 'TopN Chart', and 'Cumulative Data'. Below this is a 'Data Source' dropdown menu set to 'ERSPAN', followed by a search input field, 'Filter', and 'Clear' buttons. The table below shows 15 records of application statistics. The table has columns for '#', 'Protocol', 'Packets/s', 'Bytes/s', and a percentage. At the bottom of the table, there are controls for 'Rows per page' (set to 15), 'Units' (set to Bytes/s), and 'Go to page' (set to 1 of 2). Below the table are buttons for 'Save', 'Details', 'Real-Time', and 'Report'.

#	Protocol	Packets/s	Bytes/s	
1.	snmp	55.16	9,494.82	49%
2.	netflow	4.12	5,796.96	30%
3.	nfs	15.11	2,612.29	14%
4.	http	3.92	897.51	5%
5.	icmp	0.20	120.84	1%
6.	flowmonitor	0.98	80.47	<1%
7.	stp	1.00	60.00	<1%
8.	https	0.22	36.99	<1%
9.	cdp	0.07	32.84	<1%
10.	ether2-unknown	0.36	28.92	<1%
11.	arp	0.41	24.58	<1%
12.	sip	0.04	18.55	<1%
13.	sccp	0.22	13.88	<1%
14.	telnet	0.07	13.57	<1%
15.	ip-fragment	0.20	13.52	<1%

- Step 7** To monitor the network hosts, go to the Monitor tab and click Hosts.
- Step 8** To monitor the network host conversations, go to the Monitor tab and click Conversations.

## Configuring a VLAN Data Source for ERSPAN Traffic

- Step 1** To see which VLANs are available, click **Monitor > VLAN**. In the drop-down menu, make sure ERSPAN is selected.
- Step 2** Click **Setup > Data Sources**.
- Step 3** Click “ERSPAN VLANs” in the left pane.

- Step 4** At the VLAN Data Sources box, choose VLAN ID from the drop-down menu and click the **Create** button.

**VLAN Data Sources**

Data Source Name:  Filter Clear

Data Source Name  
VLAN ID

Showing 0-0 of 0 VLAN data sources

Data Source Name	VLAN ID
No data sources configured.	

Rows per page: 15 Go to page: 0 of 0 Go

Create Delete

196339

- Step 5** At the VLAN Data Sources box, enter the Data Source Name and VLAN ID.

**VLAN Data Sources**

Data Source Name:

VLAN Id:

Refresh Submit Reset Cancel

196336

- Step 6** Click **Submit**.

- Step 7** The dialog box will appear with the VLAN data source now included.

**VLAN Data Sources**

Data Source Name:  Filter Clear

Showing 1-1 of 1 VLAN data sources

Data Source Name	VLAN ID
<input type="radio"/> VLAN2	2

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

Create Delete

196337

## Using a VLAN Data Source

To use the new data source you have just created, you will need to enable it from the Setup menu:

- Step 1** Choose **Setup > Monitor**. The Core Monitoring window appears.
- Step 2** Choose the new VLAN data source from the drop-down menu.

**Figure 3-3** List of Data Sources

	Monitoring Function	Max Entries
<input type="checkbox"/>	Application Statistics	
<input type="checkbox"/>	Host Statistics (Network & Application layers)	100
<input type="checkbox"/>	Host Statistics (MAC layer)	
<input type="checkbox"/>	Conversation Statistics (Network & Application layers)	500
<input type="checkbox"/>	Conversation Statistics (MAC layer)	
<input type="checkbox"/>	VLAN Priority (CoS) Statistics	
<input type="checkbox"/>	Network-to-MAC Address Correlation	
<input type="checkbox"/>	TCP/UDP Port Table	

↑-- Check desired functions then Apply -->

Apply Reset

196338

- Step 3** Check the check boxes for the display functions you would like to see. Typically, you will want to check all boxes. Click **Apply**.
- Step 4** To display the ERSPAN data for your VLAN, choose **Monitor > Apps**, **Monitor > Hosts**, or **Monitor > Conversations**. The newly created VLAN data source will show in the dialog box by default and display the data for that VLAN.

## Deleting a VLAN Data Source

To delete a VLAN data source:

- Step 1** Choose **Setup > Data Sources**.  
The Active SPAN Sessions Dialog displays.
- Step 2** Click **VLANs**.  
The VLAN Data Sources window displays and lists VLAN data sources available on the NAM appliance.
- Step 3** Check the check box of a VLAN data source and click **Delete**.

## Configuring ERSPAN Reports on the NAM VSB

To gain visibility into the top applications and those individuals creating a significant amount of IP phone traffic, you can create Top Applications and Top Hosts reports. Reports like these enable you to view trending of top applications and most active hosts for a particular branch over a period of time.

- 
- Step 1** Log in to the NAM VSB GUI, and click **Reports > Basic Reports**.  
The Basic Historical Reports window displays and lists any currently configured basic reports.
- Step 2** Click **Create** to create a new basic report.
- Step 3** Choose Applications from the list of report types, then click **Next**.
- Step 4** Click to choose Top Applications as shown in [Figure 3-4](#), then choose the ERSPAN Data Source and click **Finish**.

**Figure 3-4** Setup Report Parameters

The screenshot shows the 'Setup Report Parameters' window in the NAM VSB GUI. It is divided into several sections:

- Application:** This section is selected with a radio button. It contains two dropdown menus: 'Encapsulation' set to 'IP' and 'Protocol' set to '3gpp2-a10'.
- Top Applications** and **Top Application TCP/UDP Ports**: These are unselected radio button options.
- Report Settings**: This section contains several fields:
  - Report Name:** An empty text input field with a 'Customized' checkbox to its right.
  - Data Type:** A dropdown menu set to 'Bytes/sec'.
  - Polling Interval:** A dropdown menu set to '15 minutes'.
  - Data Source:** A dropdown menu set to 'ERSPAN'.

- Step 5** Click **Create** again to create another new basic report.
- Step 6** Choose Hosts from the list of report types, then click **Next**.
- Step 7** Click to choose Top N Hosts, then choose the ERSPAN Data Source and click **Finish**.
-





## CHAPTER 4

# Configuring NetFlow for Traffic Visibility

---

NetFlow records provide an aggregate view of the network traffic. When enabled on the branch router or switch, the NetFlow data source becomes available on the Cisco NAM Virtual Services Blade (VSB). NetFlow provides statistics for applications, hosts, and conversations. You can set up custom data sources for some specific interfaces. NetFlow can be used to identify business critical applications hosted in the Data Center that are used in the branch.

This chapter contains the following sections:

- [Configuring NetFlow on Cisco IOS Routers](#)
- [Configuring NetFlow Data Source on the NAM VSB, page 4-2](#)
- [Configuring NetFlow Reports on the NAM VSB, page 4-3](#)

## Configuring NetFlow on Cisco IOS Routers

Configure NetFlow traffic on the Branch edge router. You must enable NetFlow on both the WAN and LAN interface to provide visibility into traffic flows entering and leaving the branch.

```
config t
interface <interface>
    ip route-cache flow
    exit
ip flow-export version 5
ip flow-export destination <NAM-IP-Address> 3000
```



### Note

---

The UDP port number must be set to 3000.

---

Also make sure the SNMP Read Only community string is configured on the device.

```
snmp-server community <RO-string> RO
```

# Configuring NetFlow Data Source on the NAM VSB

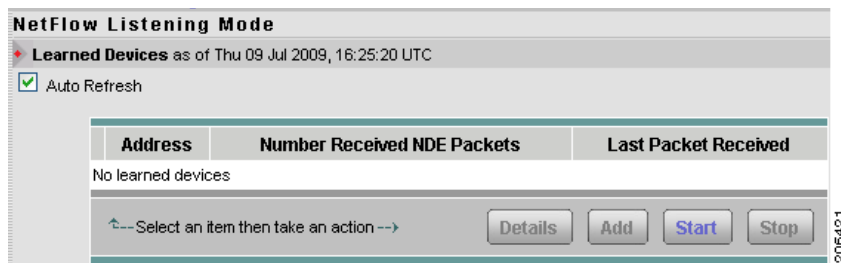
Use the NAM Traffic Analyzer GUI to enable additional NetFlow monitoring devices.

**Step 1** Log in to the NAM GUI and choose **Setup > Data Sources**.

**Step 2** In the Content menu, click **NetFlow -- Listening Mode**.

The NetFlow Listening Mode window displays as shown in [Figure 4-1](#).

**Figure 4-1** NetFlow Listening Mode Window



**Step 3** Click **Start**.

This enables the Cisco NAM VSB to listen to any NetFlow packets being sent to it.

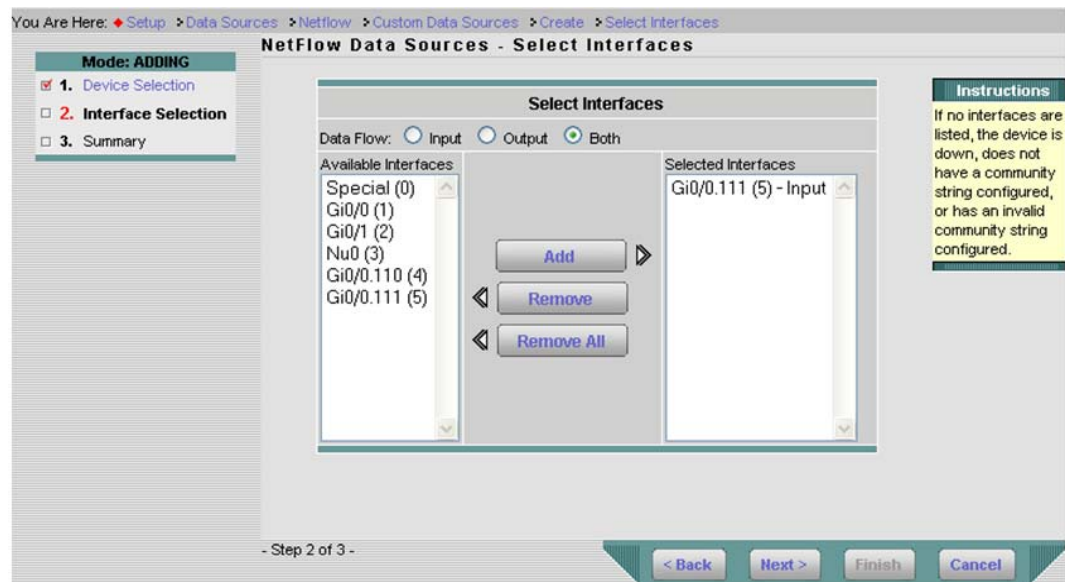
**Step 4** As you see the IP addresses begin to list, select and add the device or devices, and provide the SNMP read community string.

**Step 5** Test for connectivity and SNMP community string from **Setup > Data Sources > NetFlow -- Devices**, then click **Test**.

**Step 6** Add the NetFlow data sources by selecting **Setup > Data Sources > NetFlow -- Custom Data Sources**, then choose a NetFlow device, provide a name, and click **Next**.

**Step 7** Add the interfaces to monitor in this data source as shown in [Figure 4-2](#).

**Figure 4-2** NetFlow Data Sources - Select Interfaces



- Step 8** Click **Next** and review the settings, then click **Finish**.
- Step 9** Click **Setup > Monitor > Core Monitoring**.
- Step 10** Choose the desired data sources with a prefix NDE as NetFlow data sources, and enable collections by clicking **Apply**.

**Figure 4-3** Core Monitoring Functions

Monitoring Function	Max Entries
<input checked="" type="checkbox"/> Application Statistics	Not applicable
<input checked="" type="checkbox"/> Host Statistics (Network & Application layers)	1000
<input checked="" type="checkbox"/> Conversation Statistics (Network & Application layers)	5000
<input checked="" type="checkbox"/> TCP/UDP Port Table	Not applicable

## Configuring NetFlow Reports on the NAM VSB

To gain visibility into the top applications and those individuals creating a significant amount of IP phone traffic, you can create Top Applications and Top Hosts reports. Reports like these enable you to view trending of top applications and most active hosts for a particular branch over a period of time.

- Step 1** Log in to the NAM VSB GUI, and click **Reports > Basic Reports**.  
The Basic Historical Reports window displays and lists any currently configured basic reports.
- Step 2** Click **Create** to create a new basic report.
- Step 3** Choose Applications from the list of report types, then click **Next**.
- Step 4** Click to choose Top Applications as shown in [Figure 4-4](#), then choose the NetFlow Data Source and click **Finish**.

Figure 4-4 Setup Report Parameters

**Setup Report Parameters**

Application:  
Encapsulation: IP  
Protocol: 3gpp2-a10

Top Applications

Top Application TCP/UDP Ports

**Report Settings**

Report Name: Top Applications - Bytes  Customized

Data Type: Bytes/sec

Polling Interval: 15 minutes

Data Source: NDE-br-rtr

206426

**Step 5** Click **Create** again to create another new basic report.

**Step 6** Choose Hosts from the list of report types, then click **Next**.

**Step 7** Click to choose Top N Hosts as shown in [Figure 4-5](#), then choose the NetFlow Data Source and click **Finish**.

Figure 4-5 Setup Host Report Parameters

**Setup Host Report Parameters**

Host Name / IP Address:

Host Application:  
Encapsulation: IP  
Protocol: 3gpp2-a10

Top N Hosts

**Report Settings**

Report Name: Top Hosts - Bytes In  Customized

Data Type: Bytes In/sec

Polling Interval: 15 minutes

Data Source: NDE-br-rtr

206426



## CHAPTER 5

# Configuring and Monitoring the Nexus Virtual Switch as a Managed Device

---

A managed device is a switch from which you would like to gather information such as interface statistics. For Nexus virtual networks, virtual interfaces statistics will provide insight into your virtual network.

This chapter contains the following sections:

- [Setting Up the Managed Device Parameters, page 5-1](#)
- [Monitoring the Managed Device Interfaces, page 5-2](#)

## Setting Up the Managed Device Parameters

When you set up a managed device, the NAM retrieves interface information via SNMP from that managed device and displays statistics. For NAM on Nexus VSB, you should set these parameters to point to a Nexus 1000v switch.

- 
- Step 1** In the Content menu, click **Setup > Managed Device Parameters**.
- Step 2** The window will display the dialog box for configuring a managed device, as shown in [Figure 5-1](#).

**Figure 5-1** *Managed Device Parameters*

Managed Device Information	
Name:	VSM-test
Hardware:	Virtual Supervisor Module
Managed Device Software Version:	Version 4.0(4)SV1(3)
Managed Device System Uptime:	2 days, 17 hours, 53 minutes
Location:	N/A
Contact:	N/A
Managed Device:	<input type="text" value="10.10.10.10"/>
SNMP Read-Write Community String:	<input type="text" value="●●●●●●●●"/>
Verify String:	<input type="text" value="●●●●●●●●"/>
<input type="button" value="Test Connectivity"/> <input type="button" value="Apply"/> <input type="button" value="Reset"/>	

- Step 3** Enter the IP address of the Nexus virtual switch you would like to monitor. You must enter the SNMP Read-Write Community String for that switch in both fields.
- Step 4** Click the Test Connectivity button. On the window that appears, make sure that “SNMP Read from Managed Device” and “SNMP Write from Managed Device” both say OK.
- Step 5** Click Close.

## Monitoring the Managed Device Interfaces

Monitoring the managed device interfaces provides per-interface statistics directly from the Nexus switch.

Go to the Monitor tab and then select **Managed device** (see [Figure 5-2](#)). You will see three radio buttons: “Current Rates,” “TopN Chart,” and “Cumulative Data”, with which you can choose how you want to view the data.

Figure 5-2 Monitoring the Managed Device

Showing 1-13 of 13

#	Interface	In % Utilization	Out % Utilization	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	In Non-Unicast/s	Out Non-Unicast/s	In Discards/s	Out Discards/s	In Errors/s
1.	Ethernet3/2	17.52	5.52	3,690.97	3,380.80	2,189,393.98	20%	690,458.37	7.63	0.03	0.00	0.00
2.	Ethernet6/2	1.74	0.56	3,672.68	3,377.18	2,178,402.35	20%	693,866.63	7.63	0.02	0.00	0.00
3.	Ethernet4/2	1.73	0.55	3,638.10	3,336.67	2,162,499.25	20%	685,703.88	7.63	0.03	0.00	0.00
4.	Ethernet5/2	1.73	0.55	3,636.88	3,335.63	2,162,067.38	20%	685,467.78	7.63	0.02	0.00	0.00
5.	Vethernet4	0.00	0.00	3,125.07	395.65	518,756.27	5%	565,344.03	0.00	7.53	0.00	0.00
6.	Vethernet1	0.00	0.00	3,125.02	402.37	518,752.77	5%	574,701.27	0.00	7.63	0.00	0.00
7.	Vethernet3	0.00	0.00	3,125.00	395.62	518,750.00	5%	565,330.27	0.00	7.53	0.00	0.00
8.	Vethernet2	0.00	0.00	2,974.92	395.48	493,819.57	5%	565,147.30	0.00	7.50	0.00	0.00
9.	Vethernet7	0.00	0.00	0.00	3,125.00	4.27	<1%	1,575,000.00	0.02	0.00	0.00	0.00
10.	Vethernet8	0.00	0.00	0.00	3,066.73	4.27	<1%	1,545,952.80	0.02	0.00	0.00	0.00
11.	Vethernet6	0.00	0.00	0.00	3,125.00	0.00	<1%	1,575,000.00	0.00	0.00	0.00	0.00
12.	Vethernet9	0.00	0.00	0.00	3,045.58	0.00	<1%	1,534,646.40	0.00	0.00	0.00	0.00
13.	mgmt0	0.00	0.00	11.88	408.18	0.00	<1%	0.00	0.00	0.00	0.00	0.00

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

Select an item then take an action --> Details Real-Time

To see the statistics for the last interval (the default is 60 seconds), click the “Current Rates” radio button.

To see a chart of the statistics, click the “TopN Chart” radio button.

To see cumulative data from the managed device, click the “Cumulative Data” radio button.





# CHAPTER 6

## Troubleshooting

---

This chapter describes some common problems that occur while setting up the Cisco Nexus 1000V NAM Virtual Service Blade.

- [Resetting the NAM Password, page 6-1](#)

## Resetting the NAM Password

---

**Step 1** From the NAM CLI, execute this command:

```
reboot -helper
```

**Step 2** You will be prompted for Y/N verification that you want to reboot. Click Y, and the NAM will boot into the helper image and display the menu.

```
=====  
Cisco Systems, Inc.  
Network Analysis Module (NAM) helper utility  
Version 4.2(1)  
  
-----  
Main menu  
1 - Download application image and write to HDD  
2 - Download application image and reformat HDD  
3 - Install application image from CD  
4 - Display software versions  
5 - Reset application image CLI passwords to default  
6 - Change file transfer method (currently ftp/http)  
7 - Send Ping  
n - Configure network  
r - Exit and reset Services Engine  
h - Exit and shutdown Services Engine Selection [1234567nh]:
```

**Step 3** At the helper menu, pick **5**, “Reset application image CLI passwords to default.”

**Step 4** Click **r** to reset the NAM.

**Step 5** After the NAM boots back up, you will need to reset the default password when logging in as root.

---

