Configuring Cisco Prime NAM

This chapter provides details about the post installation tasks that you might need to perform.

- Configuring ERSPAN for Traffic Visibility, page 1
- Configuring NetFlow for Traffic Visibility, page 3
- Configuring and Monitoring the Nexus Virtual Switch as a Managed Device, page 4

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 Prime 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:

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).

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.

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.

Configuring ERSPAN on the Cisco Nexus 1000V

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.

Refer to "Configuring Local SPAN and ERSPAN" in the Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1) SV1(4)

Configuring ERSPAN Data Source on the Cisco Prime NAM VSB

You must configure ERSPAN on the Cisco Prime NAM VSB so that the Prime NAM receives data.

See the Sending ERSPAN Data Directly to the Cisco Prime NAM Management Interface, on page 2 about using ERSPAN as a data source:

Note Depending on the NX-OS version on your managed device, the CLI format for configuring an ERSPAN session may be different than what appears in this document. For details on using ERSPAN as a data source, see your specific OS product documentation.

Sending ERSPAN Data Directly to the Cisco Prime NAM Management Interface

To send the data directly to the Cisco NAM management IP address (management-port), configure the ERSPAN source session. No ERSPAN destination session configuration is required. After performing this configuration on the Catalyst 6500 switch, when ERSPAN packets are sent to the NAM, it will automatically create a data source for that packet stream.

If the autocreate feature is not enabled, you will have to manually create the data source for this ERSPAN stream of traffic. See the Forwarding ERSPAN Traffic section Customizing Cisco Prime NAM chapter in the Cisco Prime NAM 6.1 User Guide for detailed procedures.

Note This method causes the ERSPAN traffic to arrive on the Cisco Prime NAM management port. If the traffic level is high, this could have negative impact on the Cisco Prime NAM's performance and IP connectivity. This might also have an impact on the general network performance.

Sample Configuration

```
monitor session 1 type erspan-source
no shut
source interface Fa3/47
destination
erspan-id  Y
ip address aa.bb.cc.ddorigin ip address ee.ff.gg.hh
```

Where:

- Interface fa3/47 is a local interface on the erspan-source switch to be monitored
- *Y* is any valid span session number
- *aa.bb.cc.dd* is the management IP address of the Cisco Prime NAM
- *ee.ff.gg.hh* is the source IP address of the ERSPAN traffic

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 Prime NAM. 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.

As a consumer, the Cisco Prime NAM can receive NetFlow packets on its management port from devices such as Cisco routers and switches. Those records are stored in its collection database as if that traffic had appeared on one of the Cisco Prime NAM data ports. The Cisco Prime NAM understands NetFlow v1, v5, v6, v7, v8, and v9.

See the following sections:

- Configuring NetFlow on Cisco IOS Routers, on page 3
- Configuring NetFlow Data Source on the Cisco Prime NAM for Nexus 1110, on page 4
- Testing NetFlow Devices, on page 4

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. You can change this using the NAM CLI. See the Cisco Prime Network Analysis Module Command Reference Guide

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

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

Configuring NetFlow Data Source on the Cisco Prime NAM for Nexus 1110

See the Customizing Cisco Prime NAM chapter in the Cisco Prime NAM User Guide available at http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-analysis-module-software/products-user-guide-list.html, for detailed procedures.

Testing NetFlow Devices

You can test the SNMP community strings for the devices in the Devices table. To test a device, select it from the Devices table under Setup > Traffic > NAM data Sources, then click **Edit**. Enter the parameters and click Test Connectivity.

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. Cisco Prime NAM supports only one managed device and Nexus 1110 only supports one Cisco Prime NAM Virtual Blade as primary.

Setting Up the Managed Device Parameters

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

To view the switch information, choose **Setup** > **Managed Device > Device Information**.

Table 1: Switch Information

Field	Description
SNMP Test information	Displays the IP address of the Cisco Prime NAM and the switch that the SNMP test occurred on.
Name	Name of the switch.
Hardware	Hardware description of the switch.
Supervisor Software Version	Current software version of the Supervisor.
System Uptime	Total time the switch has been running.

Field	Description
Location	Physical location of the switch.
Contact	Contact name of the network administrator for the switch.
SNMP read from switch	SNMP read test result.
SNMP write to switch	SNMP write test result.
Mini-RMON on switch	For Cisco IOS devices, displays the status if there are any ports with Mini-RMON configured (Available) or not (Unavailable).
NBAR on switch	Displays if NBAR is available on the switch.
VLAN Traffic Statistics on Switch	Displays if VLAN data is Available or Unavailable. **Note** Catalyst 6500 Series switches require a Supervisor 2 or MSFC2 card.
NetFlow Status	For Catalyst 6500 Series devices running Cisco IOS, if NetFlow is configured on the switch, Remote export to Cisco Prime NAM <address> on port <number> displays, otherwise the status will display Configuration unknown.

This section describes how to set router/managed device parameters.

SUMMARY STEPS

1. Choose **Setup** > **Managed Device > Device Information**.
2. Click the **Test Connectivity** button to perform an SNMP test. Click **Close** when finished.
3. Click **Submit** to submit the information and close the window.

DETAILED STEPS

Step 1 Choose **Setup** > **Managed Device > Device Information**.
The Router System Information displays as shown in the following table.

Some of the fields below may not be available when using a Nexus 1000V as a managed device.

Table 2: Router/Managed Device System Information

Field	Description
Name	Name of the router.

Field	Description
Hardware	Hardware description of the router.
Managed Device Software Version	Current software version of the router.
Managed Device System Uptime	Total time the switch has been running.
Location	Physical location of the router.
Contact	Name of the network administrator for the router.
Managed Device	IP address of the router.
SNMP v1/v2c RW Community String	Name of the SNMP read-write community string configured on the router
Verify String	Verify the SNMP .
Enable SNMP V3	Check the check box to enable SNMP Version 3 (starting with NAM 5.0, you have the ability to manage devices with SNMPv3). If SNMPv3 is not enabled, the community string is used.
Mode: No Auth, No Priv	SNMP will be used in a mode with no authentication and no privacy.
Mode: Auth, No Priv	SNMP will be used in a mode with authentication, but no privacy.
Mode: Auth and Priv	SNMP will be used in a mode with both authentication and privacy.
User Name	Enter a username, which will match the username configured on the device.
Auth Password	Enter the authentication password associated with the username that was configured on the device. Verify the password.
Auth Algorithm	Choose the authentication standard which is configured on the device (MD5 or SHA-1).
Privacy Password	Enter the privacy password, which is configured on the device. Verify the password.
Privacy Algorithm	Enter the privacy algorithm, which is configured on the device (AES or DES).

Step 2 Click the **Test Connectivity** button to perform an SNMP test. Click **Close** when finished.

Step 3 Click **Submit** to submit the information and close the window.

Monitoring the Managed Device Interfaces

Monitoring the managed device interfaces provides per-interface statistics directly from the Nexus switch. Go to the Analyze > **Managed Device > Interfaces** .

To change the interval, go to the Interactive Report on the left side of the screen and click the Filter button.