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

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.

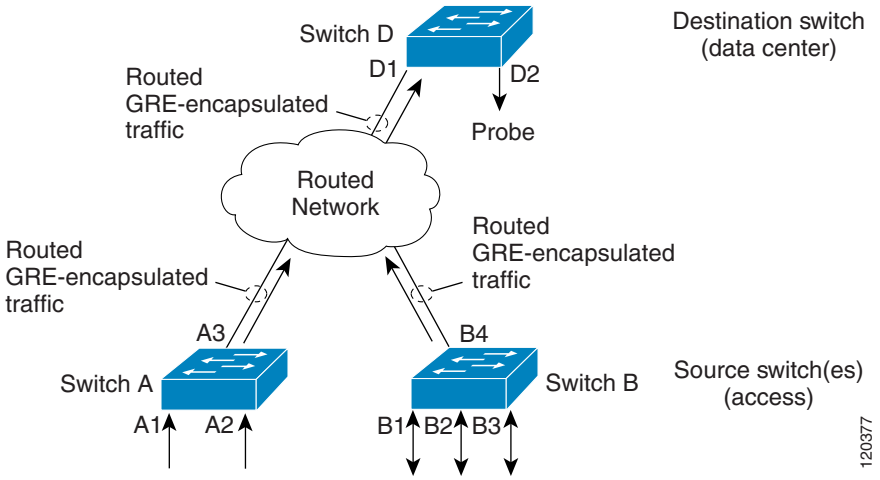
An ERSPAN destination session is defined by the following:

- 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

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

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	**config t**
	
	Example:
	`vsm-nam1# config t`
	`vsm-nam1(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**port-profile** *port_profile_name*
	
	Example:
	`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	**capability l3control**
	
	Example:
	`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	**vmware port-group** *pg_name* **Example:** vsm-nam1(config-port-prof)#vmware port-group erspan vsm-nam1(config-port-prof)#	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. 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. • **pg-name**: 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.
Step 5	**switchport mode access** **Example:** vsm-nam1(config-port-prof)# switchport mode access vsm-nam1(config-port-prof)#	Designates the interfaces as switch access ports (the default).
Step 6	**switchport access vlan** *vlan_id* **Example 1:** vsm-nam1(config-port-prof)# switchport access vlan 2 vsm-nam1(config-port-prof)#	Assigns a VLAN ID to the access port for this port profile and saves the setting in the running configuration.
Step 7	**no shutdown** **Example:** vsm-nam1(config-port-prof)# no shutdown vsm-nam1(config-port-prof)#	Enables the interface in the running configuration.
Step 8	**system vlan** *vlan_id* **Example:** vsm-nam1(config-port-prof)# system vlan 2 vsm-nam1(config-port-prof)#	Associates the system VLAN ID with the port profile and saves it in the running configuration. Must match the VLAN ID assigned to the access port. If it does not match, then the following error message is generated: ERROR: System vlan being set does not match the switchport access vlan 2
Step 9	**state enabled** **Example:** vsm-nam1(config-port-prof)# state enabled vsm-nam1(config-port-prof)#	Enables the port profile in the running configuration. This port profile is now ready to send out ERSPAN packets on all ESX Hosts with ERSPAN sources

	Command	Purpose

Step 10	**show port-profile name** *port_profile_name*
	
	Example:
	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)#
		(Optional) Displays the configuration for the specified port profile as it exists in the running configuration.

Step 11	**copy running-config startup-config** **Example:** vsm-nam1(config-port-prof)# copy running-config startup-config [##] 100% vsm-nam1(config-port-prof)#	(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 **new virtual adapter**.	

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	**config t**
	
	Example:
	`vsm-nam1# config t`
	`vsm-nam1(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**no monitor session** *session-number* **Example:** `vsm-nam1(config)# no monitor session 3`	Clears the specified session.

Step 3	**monitor session** *session-number* **type erspan-source**
	
	Example:
	`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	**description** *description*
	Example:
	`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.
		• description: up to 32 alphanumeric characters default = blank (no description)

	Command	Purpose
Step 5	**source** {**interface** *type* | **vlan**} {*number* | *range*} [**rx** | **tx** | **both**] **Example 1:** vsm-nam1(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx **Example 2:** vsm-nam1(config-erspan-src)# source interface port-channel 2 **Example 3:** vsm-nam1(config-erspan-src)# source interface vethernet 12 both **Example 4:** vsm-nam1(config-erspan-src)# source vlan 3, 6-8 tx	For the specified session, configures the source(s) and the direction of traffic to monitor, and saves them in the running configuration. • type: Specify the interface type—ethernet, port-channel, vethernet. • number: Specify the interface slot/port or range; or the VLAN number or range to monitor. • traffic direction: Specify traffic monitoring to be in one of the following directions: – receive (rx) (the VLAN default) – transmit (tx) – both (the interface default)
Step 6	(Optional) Repeat Step 5 to configure additional ERSPAN sources.	
Step 7	**filter vlan** {*number* | *range*} **Example:** vsm-nam1(config-erspan-src)# filter vlan 3-5, 7	(Optional) For the specified ERSPAN session, configures the VLANs, VLAN lists, or VLAN ranges to be monitored; and saves this in the running configuration. On the monitor port, only the traffic from the VLANs which match the VLAN filter list are replicated to the destination.
Step 8	(Optional) Repeat Step 7 to configure all source VLANs to filter.	
Step 9	**destination ip** *ip_address* **Example:** vsm-nam1(config-erspan-src)# destination ip 10.54.54.1 vsm-nam1(config-monitor-erspan-src)#	Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration.
Step 10	**ip ttl** *ttl_value* **Example**: vsm-nam1(config-monitor-erspan-src)# **ip ttl 64** vsm-nam1(config-monitor-erspan-src)#	(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.
Step 11	**ip prec** *precedence_value* **Example**: vsm-nam1(config-monitor-erspan-src)# **ip prec 1** vsm-nam1(config-monitor-erspan-src)#	(Optional) Specifies the IP precedence value, from 0-7, for the packets in the ERSPAN traffic, and saves it in the running configuration.
Step 12	**ip dscp** *dscp_value* **Example**: vsm-nam1(config-monitor-erspan-src)# **ip dscp 24** vsm-nam1(config-monitor-erspan-src)#	(Optional) Specifies the IP DSCP value, from 0-63. for the packets in the ERSPAN traffic, and saves it in the running configuration.

	Command	Purpose

Step 13	**mtu** *mtu_value*
	
	Example:
	`vsm-nam1(config-monitor-erspan-src)# mtu 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	**erspan-id** *flow_id* **Example:** `vsm-nam1(config-erspan-src)# erspan_id 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	`no shut`
	
	Example:
	`vsm-nam1(config-erspan-src)# no shut`
		Enables the ERSPAN session and saves it in the running configuration.
		
		By default, the session is created in the shut state.

Step 16	**show monitor session** *session_id* **Example:** `vsm-nam1(config-erspan-src)# show monitor session 3`	(Optional) Displays the ERSPAN session configuration as it exists in the running configuration.

Step 17	**exit**
	
	Example:
	`vsm-nam1(config-erspan-src)# exit`
	`vsm-nam1(config)#`
		(Optional) Exits ERSPAN Source Configuration mode and returns you to CLI Configuration mode.

Step 18	**copy running-config startup-config** **Example:** `vsm-nam1(config)# copy running-config startup-config`	(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

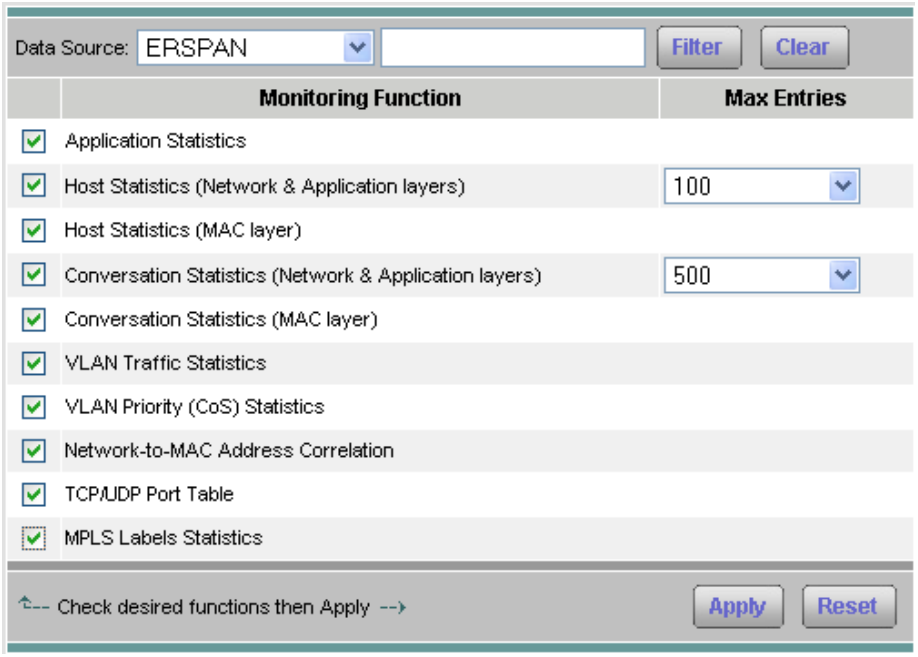
Use the NAM Traffic Analyzer GUI to enable additional ERSPAN monitoring devices.

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

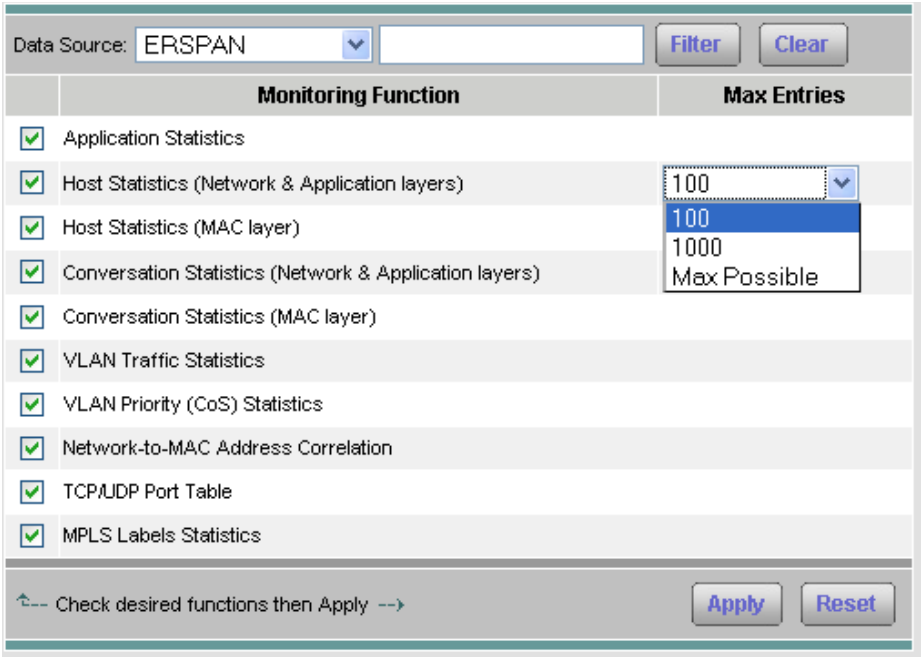
Step 2 Click the Data Source drop-down menu and choose ERSPAN.

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.



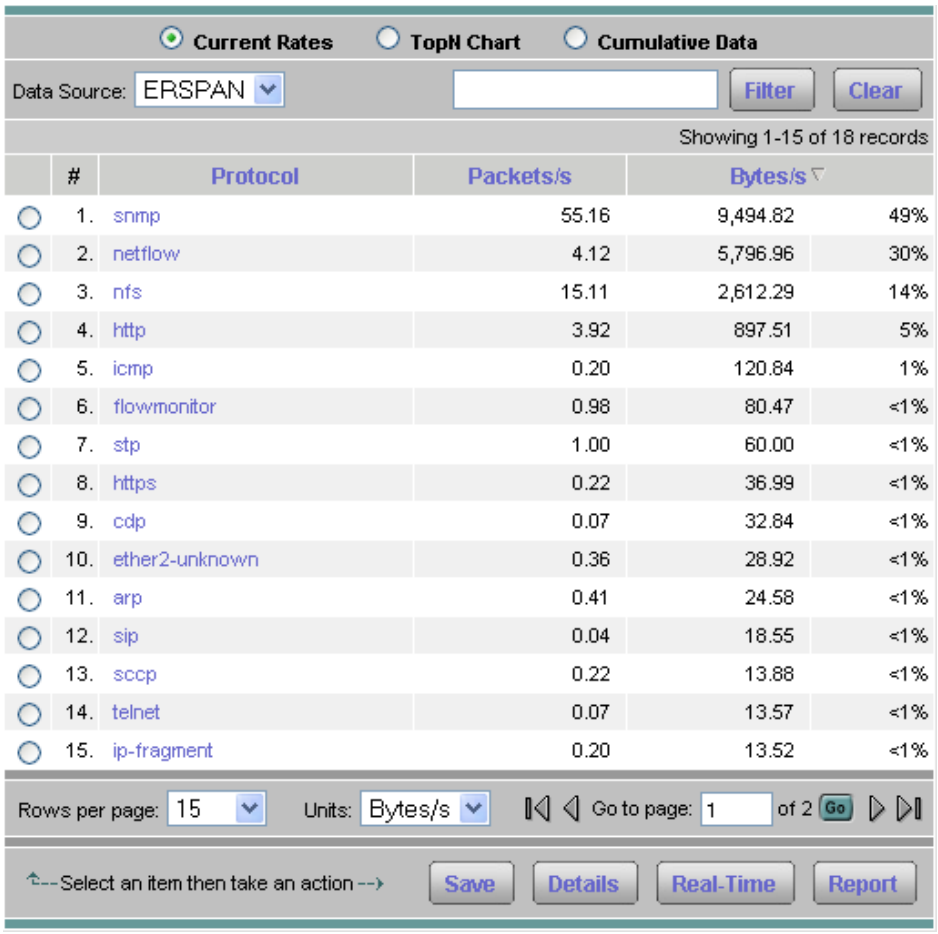
Step 4 There is a pull-down menu next to Host Statistics (Network & Application layers) and Conversation Statistics (Network & Application layers). You can optionally set the maximums for these statistics.



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



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.

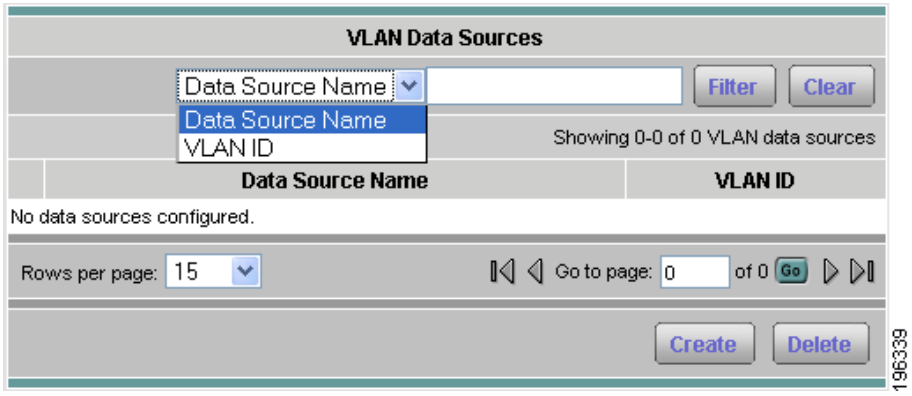
Configuring a VLAN Data Source for ERSPAN Traffic

Step 1 To see which VLANs are available, click **Monitor > VLAN**. In the drop-down menu, make sure ERSPAN is selected.

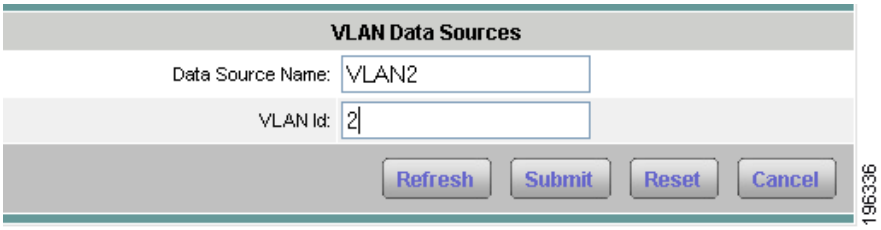
Step 2 Click **Setup > Data Sources**.

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.

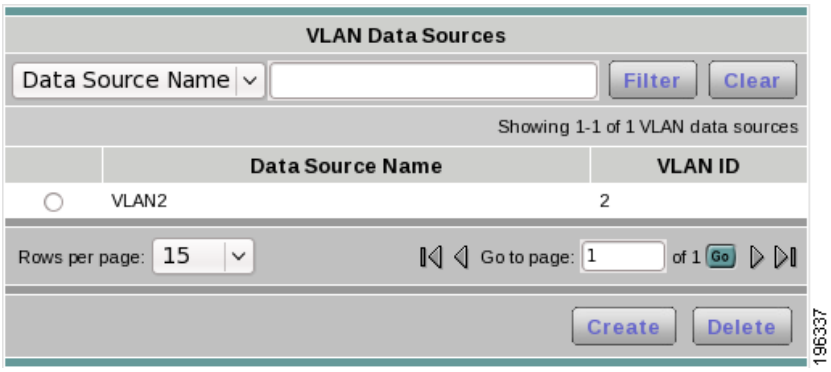


Step 5 At the VLAN Data Sources box, enter the Data Source Name and VLAN ID.



Step 6 Click **Submit**.

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



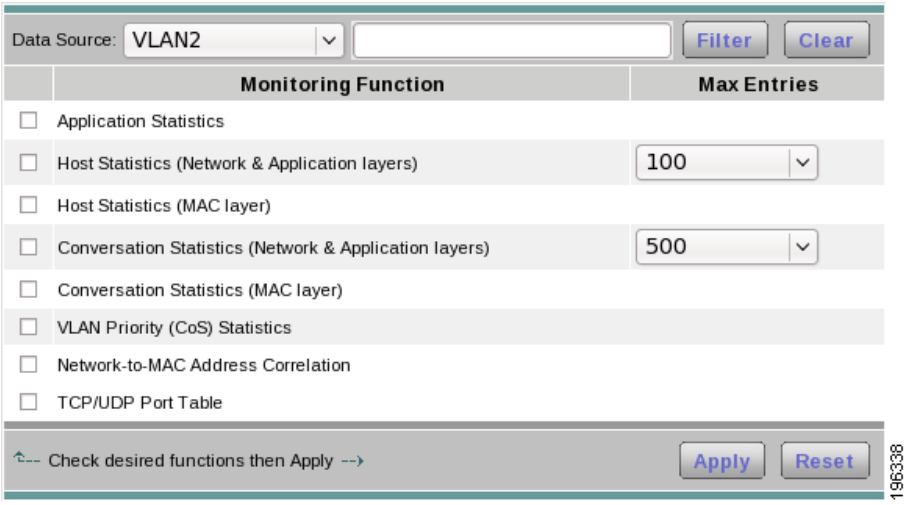
Using a VLAN Data Source

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



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**.

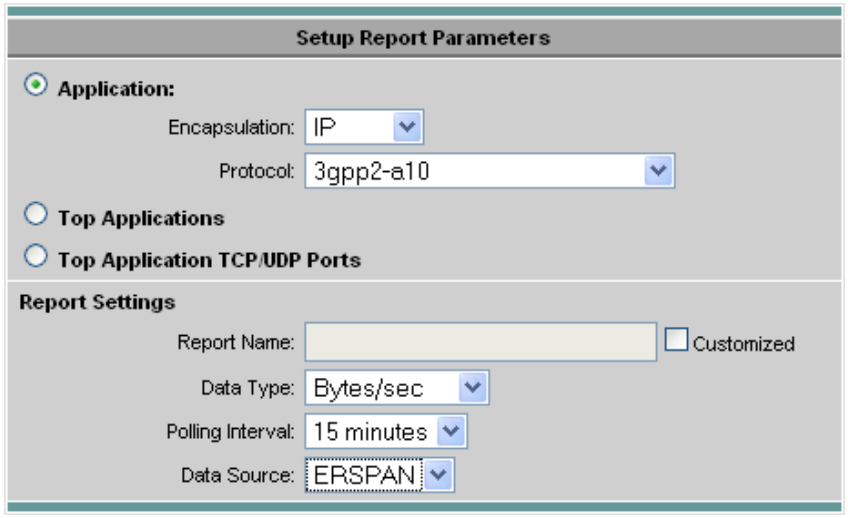
The Basic Historical Reports window displays and lists any currently configured basic reports.

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



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**.