
# Customizing Cisco Packet Analyzer

This chapter provides set up details for advanced tools and customization. You can use these tools to take your network monitoring to another level. It provides information about functions that will begin automatically, optional tasks, and other setup tasks you will need to perform for advanced feature configuration.

This chapter contains the following sections:



For information about how to install the product, configure it, and log in, see the installation guide for your specific Packet Analyzer platform.

# Advanced Configuration Overview

Table 7-1 leads you through the advanced configuration steps you can follow for Packet Analyzer. See the description to understand why or when to perform these tasks.

*Table 7-1 Advanced Configuration Overview*

| Action | Description | GUI Location | User Guide Location |
|---|---|---|---|
| **Configure the Managed Device information** | If you want to monitor an extended level of your managed device's data (health and interface information), you can set up your managed device using Packet Analyzer. If you do not set up this feature, your data collection is limited.<br>Depending on your Packet Analyzer platform, managed device health and interface information will display in **Analyze > Managed Device** GUI.<br>For Packet Analyzer platforms, the Packet Analyzer managed device IP address, SNMP, and/or NetConf interface credential must be provided for Packet Analyzer to get managed device health and interface information. | **Setup > Managed Device > Device Information** | See Accessing Device Interface and Health Details, page 7-45. |
| **Configure sites** | A *site* is a collection of hosts (network endpoints) partitioned into views that help you monitor traffic and troubleshoot problems.<br>If you want to limit the view of your network data to a specific city, a specific building, or even a specific floor of a building, you can use the sites function.<br>We recommend that sites are configured using prefix-based subnets instead of based on data source. | **Setup > Network > Sites** | See Configuring Sites, page 7-49. |
| **Define alarms and thresholds** | Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can choose for what types of events you want the software to notify you, and how you want to be notified.<br>Create alarms that will be used for thresholds, then create the thresholds. | **Setup > Alarms > Actions**<br>and<br>**Setup > Alarms > Thresholds** | See Viewing Alarm Actions, page 7-33.<br>See Defining Thresholds, page 7-34. |
| **Configure capture** | Capture allows you to configure up to ten sessions for capturing, filtering, and decoding packet data, manage the data in local or remote storage, and display the contents of the packets.<br>Per file location, you can have only one capture session. We support up to ten capture sessions. | **Capture > Packet Capture/Decode** | See Capturing and Decoding Packets, page 4-1. |

*Table 7-1 Advanced Configuration Overview (continued)*

| Action | Description | GUI Location | User Guide Location |
|---|---|---|---|
| **Configure scheduled export** | You can set up scheduled jobs that generate daily reports at a specified time, in a specified interval, and then e-mail it to a specified e-mail address or addresses.<br>Some windows may not support data export. | In the Interactive Report (left side of the dashboard), click **Export**. Scheduled Export can only be done from a Monitor or Analyze window. | See Scheduling Data Report Exports, page 7-42. |
| **Set up TACACS+ server** | TACACS+ is a Cisco Systems enhancement that provides additional support for authentication and authorization.<br>When a user logs into Packet Analyzer, TACACS+ determines if the username and password are valid and what the access privileges are. For TACACS+ to work, both Packet Analyzer and the TACACS+ server has to be configured. | **Administration > Users > TACACS+** | See Configuring a TACACS+ Server to Support Packet Analyzer Authentication and Authorization, page 5-14. |
| **Change system preferences** | You can change many preferences, such as refresh interval, Top N Entries, Data Displayed, and enabling Audit Trail, as needed. | **Administration > System > Preferences** | See Performing User and System Administration |

# Setting Up Traffic Configurations

To set up Packet Analyzer traffic, you should perform the following:

- Configuring Traffic to Monitor, page 7-3
- (Optional) Setting Up Packet Analyzer Data Sources, page 7-6
- (Optional) Configuring Hardware Deduplication, page 7-29 (For specific Packet Analyzer appliances only)

## Configuring Traffic to Monitor

Packet Analyzer can monitor your network traffic to perform many tasks including helping you to optimize your network resources and troubleshoot performance issues. Before you can monitor data, you must direct specific traffic flowing through a switch or router to the Packet Analyzer software for monitoring purposes.

A switched port analyzer (SPAN) session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic.

Packet Analyzer allows you to create LOCAL SPAN session only. There are limitations of total number of SPAN sessions per managed device platform. See the managed device document for SPAN limitations.

There are three different ways to configure LOCAL SPAN session on the SUP:

- By using SNMP—Packet Analyzer supports SNMPv1, SNMPv2c, and SNMPv3. For the SPAN feature to work under this condition, the managed device must support entity MIB.

- By using NetConf interface—This option is available for Packet Analyzer appliances. You must provide the SSH credential for NetConf interface. The SUP must have SSH enabled and support NetConf. Cisco Nexus OS devices support this NetConf interface.
- By using RISE—This option is available for Packet Analyzer appliance with Nexus 7000 devices only. RISE service must be configured on the Nexus device. After RISE is configured, Packet Analyzer and switch device will sync up automatically.

The following sections describe SPAN sessions on devices running **Packet Analyzer**:


- Understanding How the Packet Analyzer Uses SPAN, page A-3
- Creating a SPAN Session for RISE Appliance, page 7-4
- Creating a SPAN Session for Appliances and other Virtual Platforms, page 7-4
- Editing a SPAN Session for RISE Appliance, page 7-5
- Editing a SPAN Session for Appliances and other Virtual Platforms, page 7-5


## Creating a SPAN Session for RISE Appliance

To create a SPAN session for the VDCs of a managed device in RISE environment:

**Step 1** Choose **Setup > Traffic > SPAN Sessions**.

The SPAN Session window appears.

**Step 2** Select the managed device from the **Managed Device Address** drop-down list.

You can view the VDCs of the managed device, and the SPAN sessions created for each VDC.

**Step 3** Click **Create**.

**Step 4** Select a VDC from the **Managed Device** drop-down list.

**Step 5** Fill in the appropriate information on the Create SPAN Session window.

Depending on your platform, the System Information may display some or all of the fields shown in Table D-1.

**Step 6** Click **Create** to create the SPAN session for the selected managed device.

## Creating a SPAN Session for Appliances and other Virtual Platforms

To create a SPAN session on a switch:

**Step 1** Choose **Setup > Traffic > SPAN Sessions**. The SPAN window displays.

**Step 2** Click **Create**.

The Create SPAN Session Dialog displays. DataPort is the default for the SPAN Type. Contents of this window may be different depending on your Packet Analyzer platform.

**Step 3** Fill in the appropriate information on the Create SPAN Session window. See Table D-1.

**Step 4** To create the SPAN session, click **Submit**. The Active Sessions window displays.

**Step 5** To save the current active SPAN session in the running-configuration to the startup-configuration for switches running Cisco IOS software only, click **Save** in the active SPAN session window.

**Note** For switches running Cisco IOS software, *all* pending running-configuration changes will be saved to the startup-configuration.

**Step 6** To verify the SPAN session was created and to view the data, go to the Top N charts on the Traffic Analysis dashboard (**Monitor > Overview > Traffic Summary**).

## Editing a SPAN Session for RISE Appliance

To edit a SPAN session for the VDCs of a managed device in RISE environment:

**Step 1** Choose **Setup > Traffic > SPAN Sessions**.

The Active SPAN Sessions dialog box displays.

**Step 2** Select a device IP address from the **Managed Device Address** drop-down list.

**Step 3** Select the VDC.

**Step 4** Select the SPAN session to edit, then click **Edit**.

The Edit SPAN Session Dialog Box displays. The fields are described in Table D-2. Depending on your Packet Analyzer platform, there may be different fields that display.

**Step 5** Make the appropriate changes on the Edit SPAN Session window.

## Editing a SPAN Session for Appliances and other Virtual Platforms

You can only edit SPAN sessions that have been directed to the Packet Analyzer. You can only delete certain SPAN sessions using the user interface. Packet Analyzer allows you to edit and delete SPAN sessions that are destined to one of its DATAPORT. ERSPAN sessions on the main screen are for information only. You cannot edit or delete ERSPAN sessions even if the ERSPAN sessions are for Packet Analyzer management interface.

**Note** Editing an existing SPAN session that has multiple SPAN destinations will affect all destinations.

To edit a SPAN session:

**Step 1** Choose **Setup > Traffic > SPAN Sessions**.

The Active SPAN Sessions dialog box displays.

**Step 2** Select the SPAN session to edit, then click **Edit**.

The Edit SPAN Session Dialog Box displays. The fields are described in Table D-2. Depending on your Packet Analyzer platform, there may be different fields that display.

**Step 3** Make the appropriate changes on the Edit SPAN Session window.

# Setting Up Packet Analyzer Data Sources

Data sources are where the traffic sent to Packet Analyzer originates. Some examples of the data sources are:

- Physical dataports of the Packet Analyzer where you get SPAN data
- A specific router or switch that sends NetFlow to the Packet Analyzer
- A WAAS device segment that sends data to Packet Analyzer
- ERSPAN and which goes to Packet Analyzer management port.

Packet Analyzer allows you to combine two or more data sources to generate a consolidated report for analyzing the traffic.

**Caution** If you have configured sites (see Configuring Sites, page 7-49), you can assign data sources to that particular site. If you do this, and you also configure data sources, the two could overlap since sites can also be a primary "view" into data sources. If there is a mismatch between the two, you will not see any data.

**Note** We recommend that you configure a site using subnets instead of selecting a data source. For examples on how to specify a site using subnets, see Configuring Sites Using Subnets, page 7-50.

The following sections contains setup steps and specific information about the types of data sources available:



## Forwarding SPAN Traffic

A switched port analyzer (SPAN) session is an association of a destination port with a set of source ports, configured with parameters that specify the monitored network traffic. Depending on your platform, you can configure multiple SPAN sessions.

For more information about SPAN sessions, see Configuring Traffic to Monitor, page 7-3 or your platform operating system documentation.

## Forwarding ERSPAN Traffic

This section describes how to configure Encapsulated Remote Switched Port Analyzer (ERSPAN) on your remote device as a Packet Analyzer data source. You configure ERSPAN as a Packet Analyzer data source from the remote device command line interface, not the Packet Analyzer GUI.

As an ERSPAN consumer, **Packet Analyzer** can receive ERSPAN packets on its management port from devices such as Cisco routers and switches. Those packets are analyzed as if that traffic had appeared on one of the Packet Analyzer dataports. Packet Analyzer supports ERSPAN versions 1 and 3. Incoming ERSPAN data is parsed by **Packet Analyzer**, stored in its internal database, and presented in the GUI in the same way as traffic from other data sources.

#### Before You Begin

For the Packet Analyzer to receive ERSPAN from an external switch or router, that device must be configured to send ERSPAN packets to the IP address of the Packet Analyzer.

To enable ERSPAN as a data source:


- Enabling Autocreation of ERSPAN Data Sources Using the Web GUI, page 7-7
- Enabling Autocreation of ERSPAN Data Sources Using the CLI, page 7-8
- Aggregating Data Ports Using the Web GUI, page 7-8
- Disabling Autocreation of ERSPAN Data Sources Using the Web GUI, page 7-8
- Disabling Autocreation of ERSPAN Data Sources Using the CLI, page 7-9
- Creating ERSPAN Data Sources Using the Web GUI, page 7-9
- Creating ERSPAN Data Sources Using the CLI, page 7-9
- Deleting ERSPAN Data Sources Using the Web GUI, page 7-11
- Deleting ERSPAN Data Sources Using the CLI, page 7-11
- Configuring ERSPAN on Devices, page 7-12


**Note** Depending on the Cisco IOS/Nexus OS version on the 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.

### Enabling Autocreation of ERSPAN Data Sources Using the Web GUI

There is a convenient autocreate feature for data sources, which is enabled by default. With the autocreate feature, a new data source will automatically be created for each device that sends ERSPAN traffic to the Packet Analyzer, after the first packet is received. Manual creation of ERSPAN data sources using the **Packet Analyzer** GUI or the CLI is typically not necessary. When manually creating a data source, you may specify any name you want for the data source. A data source entry must exist on the **Packet Analyzer** in order for it to accept ERSPAN packets from an external device.

Autocreated ERSPAN data sources will be assigned a name in the format *ERSPAN-<IP Address>-ID-<Integer>*, where *IP Address* is the IP address of the sending device, and *Integer* is the Session-ID of the ERSPAN session on that device. For example, device 192.168.0.1 sending ERSPAN packets with the Session ID field set to 12 would be named *ERSPAN-192.168.0.1-ID-12*. You can edit these autocreated data sources and change the name if desired.

One device can be configured to send multiple separate ERSPAN sessions to the same Packet Analyzer. Each session will have a unique Session ID. **Packet Analyzer** can either group all sessions from the same device into one data source, or have a different data source for each Session ID. When data sources are autocreated, they will be associated with one particular Session ID. When manually created, you can instruct **Packet Analyzer** to group all traffic from the same device into one data source. If you check the **Session** check box, and enter a Session ID in the Value field, the data source will only apply to that specific session. If you leave the check box unchecked, all ERSPAN traffic from the device will be grouped together into this data source, regardless of Session ID.

To configure **Packet Analyzer** to automatically create data sources when it receives ERSPAN packets from an external device, use the following steps. Remember however, that the autocreate feature is turned on by default, so these steps are typically not necessary.

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click **Auto Create** on the bottom left of the window.

**Step 3** Check the **ERSPAN** check box to toggle autocreation of ERSPAN data sources to "on".

**Step 4** Click **Submit**.

### Enabling Autocreation of ERSPAN Data Sources Using the CLI

You can also configure the autocreate feature using the **Packet Analyzer** CLI. The autocreate feature is turned on by default, in most cases these steps are not necessary.

To configure **Packet Analyzer** to automatically create data sources when it receives ERSPAN packets from an external device, use the **autocreate-data-source** command as follows:

```
root@172-20-104-107.cisco.com# autocreate-data-source erspan

ERSPAN data source autocreate successfully ENABLED
```

**Packet Analyzer** will now automatically create a ERSPAN data source for each device that sends ERSPAN packets to it. The data source will have the specific Session ID that is populated by the device in the ERSPAN packets sent to the Packet Analyzer. If the same device happens to send ERSPAN packets to the Packet Analyzer with different Session ID values, a separate data source will be created for each unique Session ID sent from the device.

### Aggregating Data Ports Using the Web GUI

To aggregate the datasources:

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click **Aggregation**.

A pop up window appears.

**Step 3** Click **Submit** to combine two or more datasources for generating a consolidated report to analyze the traffic.

### Disabling Autocreation of ERSPAN Data Sources Using the Web GUI

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click **Auto Create** on the bottom left of the window.

**Step 3** Uncheck the **ERSPAN** check box to toggle autocreation of ERSPAN data sources to "off".

**Step 4** Click **Submit**.

### Disabling Autocreation of ERSPAN Data Sources Using the CLI

To disable autocreation of ERSPAN data sources, use the **no autocreate-data-source** command as follows:

```
root@172-20-104-107.cisco.com# no autocreate-data-source erspan
ERSPAN data source autocreate successfully DISABLED
root@172-20-104-107.cisco.com#
```

### Creating ERSPAN Data Sources Using the Web GUI

To manually configure a ERSPAN data source on the GUI, for example if the autocreation feature is turned off, use the following steps:

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click **Create** along the bottom of the window.

**Step 3** From the Type drop-down list, choose **ERSPAN**.

**Step 4** Enter the IP address of the device that will export ERSPAN to the Packet Analyzer.

**Step 5** Give the Data Source a name. This name will appear anywhere there is a Data Source drop-down list.

**Step 6** (Optional) Check the **Session** check box and enter an Session ID into the Value field if the data source should only apply to that specific session. If you leave the check box unchecked, all ERSPAN traffic from the device will be grouped together into this data source, regardless of Session ID.

Devices can be configured with multiple ERSPAN Sessions. The packets exported may have the same source IP address, but the Session ID exported will be a different for each session. If you want to include only one Session in the data source, you must check the "Session" box and provide the value of that Session ID.

**Step 7** Click **Submit**.

### Creating ERSPAN Data Sources Using the CLI

To manually configure a ERSPAN data source on the **Packet Analyzer** using the CLI (for example if the autocreation feature is turned off), use the following steps. Note that when using the CLI, there are two separate phases involved: First, you must create a "device" entry on the **Packet Analyzer** and remember the device ID, and then you must create a data source entry using this device ID. In the **Packet Analyzer** GUI, these two phases for creating ERSPAN data sources are combined together.

**Step 1** Enter the command **device erspan**. You will now be in erspan device subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# device erspan

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@172-20-104-107.cisco.com(sub-device-erspan)#
```

**Step 2** Enter **?** to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-device-netflow)# ?
?                         - display help
address                   - device IP address (*)
```

```
cancel                    - discard changes and exit from subcommand mode
exit                      - create device and exit from sub-command mode
help                      - display help
show                      - show current config that will be applied on exit

(*) - denotes a mandatory field for this configuration.

root@172-20-104-107.cisco.com(sub-device-netflow)#
```

**Step 3** Enter the IP address of the device as shown in this example (required):

```
root@172-20-104-107.cisco.com(sub-device-erspan)# address 192.168.0.1
```

**Step 4** Type **show** to look at the device configuration that will be applied and verify that it is correct:

```
root@172-20-104-107.cisco.com(sub-device-erspan)# show

DEVICE TYPE         : ERSPAN (Encapsulated Remote SPAN)
DEVICE ADDRESS      : 192.168.0.1


root@172-20-104-107.cisco.com(sub-device-erspan)#
```

**Step 5** Type **exit** to come out of the subcommand mode and create the device. Remember the ID value that was assigned to the new device (you will need it to create the data source).

```
root@172-20-104-107.cisco.com(sub-device-erspan)# exit
Device created successfully, ID = 1
root@172-20-104-107.cisco.com#
```

**Step 6** Enter the command **data-source erspan**. You will now be in erspan data source subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# data-source erspan

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@172-20-104-107.cisco.com(sub-data-source-erspan)#
```

**Step 7** Enter **?** to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# ?
?                         - display help
cancel                    - discard changes and exit from subcommand mode
device-id                 - erspan device ID (*)
exit                      - create data-source and exit from sub-command mode
help                      - display help
name                      - data-source name (*)
session-id                - erspan Session ID
show                      - show current config that will be applied on exit

(*) - denotes a mandatory field for this configuration.

root@172-20-104-107.cisco.com(sub-data-source-erspan)#
```

**Step 8** Enter the device ID from Step 4.

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# device-id 1
```

**Step 9** Enter the name you would like for the data source (required):

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# name MyFirstErspanDataSource
```

**Step 10** If desired, supply the specific Session ID for this ERSPAN data source (optional):

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# session-id 123
```

**Step 11** Enter **show** to look at the data source configuration that will be applied and verify that it is correct:

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# show

DATA SOURCE NAME : MyFirstErspanDataSource
DATA SOURCE TYPE : ERSPAN (Encapsulated Remote SPAN)
DEVICE ID        : 1
DEVICE ADDRESS   : 192.168.0.1
SESSION ID       : 123

root@172-20-104-107.cisco.com(sub-data-source-erspan)#
```

**Step 12** Enter **exit** to come out of the subcommand mode and create the data source:

```
root@172-20-104-107.cisco.com(sub-data-source-erspan)# exit
Data source created successfully, ID = 3
```

The data source is now created, and ERSPAN records from the device will be received and accepted by Packet Analyzer as they arrive.

### Deleting ERSPAN Data Sources Using the Web GUI

To delete an existing ERSPAN data source, use the following steps. Note that if the autocreation feature is turned on, and the device continues to send ERSPAN packets to the Packet Analyzer, the data source will be recreated again automatically as soon as the next ERSPAN packet arrives. Therefore, if you wish to delete an existing ERSPAN data source, it is usually advisable to first turn the ERSPAN autocreate feature off, as described earlier.

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Choose the data source you would like to delete.

**Step 3** Click **Delete** along the bottom of the window.

### Deleting ERSPAN Data Sources Using the CLI

To delete a ERSPAN data source using the CLI, use the following steps. Note that when using the CLI, there are generally two separate phases involved. First you should delete the data source, then delete the device if you have no other data sources using the same device (for example with a different Engine ID value). As a shortcut, if you simply delete the device, then all data sources using that device will also be deleted.

**Step 1** Show all data sources so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show data-source

DATA SOURCE ID   : 1
DATA SOURCE NAME : DATA PORT 1
TYPE             : Data Port
PORT NUMBER      : 1
-----------
```

```
DATA SOURCE ID   : 2
DATA SOURCE NAME : DATA PORT 2
TYPE             : Data Port
PORT NUMBER      : 2
-----------

DATA SOURCE ID   : 3
DATA SOURCE NAME : MyFirstErspanDataSource
TYPE             : ERSPAN (Encapsulated Remote SPAN)
DEVICE ID        : 2
DEVICE ADDRESS   : 192.168.0.1
ENGINE ID        : 123
-----------

root@172-20-104-107.cisco.com#
```

**Step 2** Use the **no data-source** command to delete the data source:

```
root@172-20-104-107.cisco.com# no data-source 3
Successfully deleted data source 3
root@172-20-104-107.cisco.com#
```

**Step 3** Show all devices so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show device

DEVICE ID            : 1
DEVICE TYPE          : ERSPAN (Encapsulated Remote SPAN)
IP ADDRESS           : 192.168.0.1
INFORMATION          : No packets received
STATUS               : Inactive
------

root@172-20-104-107.cisco.com#
```

**Step 4** Use the **no device** command to delete the device:

```
root@172-20-104-107.cisco.com# no device 1
Successfully deleted device 1
root@172-20-104-107.cisco.com#
```

Note that if the autocreation mode is on, and the device continues to send ERSPAN packets to the Packet Analyzer, the data source (and device entry) will be recreated again automatically as soon as the next ERSPAN packet arrives. Therefore, if you wish to delete an existing ERSPAN data source, it is usually advisable to first turn the ERSPAN autocreate feature off, as described earlier.

## Configuring ERSPAN on Devices

There are two ways to configure ERSPAN so that the Packet Analyzer receives the data:

- Sending ERSPAN Data to Layer 3 Interface, page 7-13
- Sending ERSPAN Data Directly to the Packet Analyzer Management Interface, page 7-13

**Note** Depending on the Cisco IOS or 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 to Layer 3 Interface

To send the data to a layer 3 interface on the Switch housing the Packet Analyzer, configure the ERSPAN source session. The ERSPAN destination session then sends the traffic to a Packet Analyzer data-port. After performing this configuration, you can select the DATA PORT X data source to analyze the ERSPAN traffic.

**Note** This method causes the ERSPAN traffic to arrive on one of the Packet Analyzer dataports, which is the most efficient method and will not have any adverse effect on the Packet Analyzer's IP connectivity. Therefore, we recommend this method. The configuration below may be different depending on your platform and OS version. See your OS product documentation for additional help.

### Sample Configuration of ERSPAN Source

```
monitor erspan origin ip-address aa.bb.cc.dd global

monitor session 4 type erspan-source
    erspan-id N
    vrf default
    destination ip aa.bb.cc.ii
    source interface Ethernet12/1 bo
    rate-limit auto
    no shut

Interface that is connected to the Packet Analyzer data port:

interface Ethernet12/11
    description connect to 24042400 ee.ff.gg.hh DP2
    mtu 9216
    ip address aa.bb.cc.dd/24
    no shutdown

On Packet Analyzer:
root@appliance-2400-90.cisco.com# data-port 2 ip-address aa.bb.cc.ii
root@appliance-24002404-90.cisco.com# show data-port 2 ip-address
Port number: 2
IPv4 address: aa.bb.cc.ii

root@appliance-2400-90.cisco.com#
```

Where:

- *N* matches the ERSPAN ID at the source switch
- *aa.bb.cc.dd* is the IP address defined at the destination
- *aa.bb.cc.ii* is the IP address of the Packet Analyzer data port
- ee.ff.gg.hh is the IP address of the Packet Analyzer management port

### Sending ERSPAN Data Directly to the Packet Analyzer Management Interface

To send the data directly to the Packet Analyzer 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 Packet Analyzer, 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 Creating ERSPAN Data Sources Using the Web GUI, page 7-9).

**Note** This method causes the ERSPAN traffic to arrive on the Packet Analyzer management port. If the traffic level is high, this could have negative impact on the Packet Analyzer's performance and IP connectivity.

#### Sample Configuration

```
monitor session 1 type erspan-source
no shut
source interface Fa3/47
    destination
        erspan-id  Y
        ip address aa.bb.cc.dd
        origin 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 Packet Analyzer
- *ee.ff.gg.hh* is the source IP address of the ERSPAN traffic

## Forwarding VACL Traffic

You can use VLAN access control (VACL) lists to filter packet data and expand your device's capability beyond the two SPAN session limitation.

VACL can forward traffic from either a WAN interface or VLANs to a dataport on some of the Packet Analyzer platforms. A VACL provides an alternative to using SPAN; a VACL can provide access control based on Layer 3 addresses for IP and IPX protocols. The unsupported protocols are access controlled through the MAC addresses. A MAC VACL cannot be used to access control IP or IPX addresses.

### Configuring VACL on a WAN Interface

Because WAN interfaces do not support the SPAN function, you must use the switch CLI to manually configure a VACL in order to monitor WAN traffic with the Packet Analyzer. This feature only works for IP traffic over the WAN interface.

VACL can also be used if there is no available SPAN session to direct traffic to the Packet Analyzer. In this case, a VACL can be set up in place of a SPAN for monitoring VLAN traffic.

The following example shows how to configure a VACL on an ATM WAN interface and forward both ingress and egress traffic to the Packet Analyzer. These commands are for switches running Cisco IOS version 12.1(13)E1 or higher. For more information on using these features, see your accompanying switch documentation.

```
Cat6509#config terminal
Cat6509(config)# access-list 100 permit ip any any
Cat6509(config)# vlan access-map wan 100
Cat6509(config-access-map)# match ip address 100
Cat6509(config-access-map)# action forward capture
Cat6509(config-access-map)# exit
Cat6509(config)# vlan filter wan interface AM6/0/0.1
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1-4094
Cat6509(config)# analysis module 3 data-port 1 capture
Cat6509(config)# exit
```

To monitor egress traffic only, get the VLAN ID that is associated with the WAN interface by using the following command:

```
Cat6509#show cwan vlan
Hidden      VLAN    swidb->i_number    Interface
1017        94                         ATM6/0/0.1
```

After you have the VLAN ID, configure the Packet Analyzer dataport using the following command:

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1017
```

To monitor ingress traffic only, replace the VLAN number in the capture configuration with the native VLAN ID that carries the ingress traffic. For example, if VLAN 1 carries the ingress traffic, you would use the following command:

```
Cat6509(config)# analysis module 3 data-port 1 capture allowed-vlan 1
```

### Configuring VACL on a LAN VLAN

For VLAN Traffic monitoring on a LAN, traffic can be sent to Packet Analyzer by using the SPAN feature of the switch. However, in some instances when the traffic being spanned exceeds the monitoring capability of the Packet Analyzer, you might want to pre-filter the LAN traffic before it is forwarded. This can be done by using VACL.

The following example shows how to configure VACL for LAN VLAN interfaces. In this example, all traffic directed to the server 172.20.10.221 on VLAN 1 is captured and forwarded to the Packet Analyzer located in slot 3.

```
Cat6509#config terminal
Cat6509#(config)#access-list 100 permit ip any any
Cat6509#(config)#access-list 110 permit ip any host 172.20.10.221
Cat6509#(config)#vlan access-map lan 100
Cat6509#(config-access-map)match ip address 110
Cat6509#(config-access-map)#action forward capture
Cat6509#(config-access-map)#exit
Cat6509#(config)#vlan access-map lan 200
Cat6509#(config-access-map)#match ip address 100
Cat6509#(config-access-map)#action forward
Cat6509#(config-access-map)#exit
Cat6509#(config)#vlan filter lan vlan-list 1
Cat6509#(config)#analysis module 3 data-port 1 capture allowed-vlan 1
Cat6509#(config)#analysis module 3 data-port 1 capture
Cat6509#(config)#exit
```

## Forwarding NetFlow Traffic

Packet Analyzer functions as a NetFlow consumer. You can configure NetFlow on the device side so that Packet Analyzer can receive NetFlow packets 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 Packet Analyzer dataports. **Packet Analyzer** understands NetFlow version 5 and version 9. Incoming NetFlow data is parsed by **Packet Analyzer**, stored in its internal database, and presented in the user interface in the same way as traffic from other data sources.

For **Packet Analyzer** to receive NetFlow packets from an external switch or router, you must configure that device to forward export flow records to the Packet Analyzer's IP address and the correct UDP port number. The default port number on which Packet Analyzer listens for NetFlow packets is port 3000.

This port can be modified using the **Packet Analyzer** CLI, but it is critical that the same port be configured on the Packet Analyzer and the exporting device or devices. Depending on the external device, you may need to enable the NetFlow feature on a per-interface basis.

See the following sections about NetFlow as a data source:

- Understanding NetFlow Interfaces, page A-6
- Understanding NetFlow Flow Records, page A-6
- Managing NetFlow Data Sources, page A-7
- Configuring NetFlow on Devices, page 7-16

### Configuring NetFlow on Devices

The configuration commands for NetFlow devices to export NetFlow packets to Packet Analyzer are platform and device specific. The example configuration commands provided here are the ones most commonly found for devices running Cisco IOS. For more detailed NetFlow configuration information, see your device documentation.

### Enabling Autocreation of NetFlow Data Sources Using the Web GUI

To configure **Packet Analyzer** to automatically create data sources when it receives NetFlow packets from an external device, use the following steps. Remember however, that the autocreate feature is turned on by default, so these steps are typically not necessary.

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click **Auto Create** on the bottom left of the window.

**Step 3** Check the **Netflow** check box to toggle autocreation of NetFlow data sources on.

**Step 4** Click **Submit**.

### Enabling Autocreation of NetFlow Data Sources Using the CLI

Configuration of the autocreate feature is also possible using the **Packet Analyzer** CLI. Remember that the autocreate feature is turned ON by default, so in most cases these steps are not necessary.

To configure the **Packet Analyzer** to automatically create data sources when it receives NetFlow packets from an external device, use the following steps:

Use the **autocreate-data-source** command as follows:

```
root@172-20-104-107.cisco.com# autocreate-data-source netflow
NetFlow data source autocreate successfully ENABLED
```

**Packet Analyzer** will now automatically create a NetFlow data source for each device that sends NetFlow packets to it. The data source will have the specific Engine ID that is populated by the device in the NetFlow packets sent to the Packet Analyzer. If the same device happens to send NetFlow packets to the Packet Analyzer with different Engine ID values, a separate data source will be created for each unique Engine ID sent from the device.

### Disabling Autocreation of NetFlow Data Sources Using the Web GUI

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click **Auto Create** on the bottom left of the window.

**Step 3** Uncheck the **Netflow** check box to toggle autocreation of NetFlow data sources off.

**Step 4** Click **Submit**.

### Disabling Autocreation of NetFlow Data Sources Using the CLI

To disable autocreation of NetFlow data sources, use the **no autocreate-data-source** command as follows:

```
root@172-20-104-107.cisco.com# no autocreate-data-source netflow
NetFlow data source autocreate successfully DISABLED
root@172-20-104-107.cisco.com#
```

### Creating NetFlow Data Sources Using the Web GUI

To manually configure a NetFlow data source using the **Packet Analyzer** GUI, for example if the autocreation feature is turned OFF, use the following steps:

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click **Create** along the bottom of the window.

**Step 3** Give the Data Source a name. This name will appear anywhere there is a Data Source drop-down list.

**Step 4** From the Type drop-down list, choose **NetFlow**.

**Step 5** Enter the IP address of the device that will export NetFlow to Packet Analyzer (required).

**Step 6** (Optional) If you know the specific value of the Engine ID on the device you would like to monitor, check the **Engine** check box, and enter the value of the Engine ID. If the **Engine** check box is left unchecked, then all NetFlow records exported by the device will be grouped into the same data source, regardless of the Engine ID populated in the NetFlow packets (in most cases the **Engine** check box can be left blank and you don't have to worry about the Engine ID value).

Some devices have multiple Engines which independently export NetFlow records. For example, on some Cisco routers, NetFlow records can be exported by the Supervisor module as well as individual line cards. The packets exported may have the same source IP address, but the Engine ID exported by the Supervisor will be a different value than the Engine ID(s) exported by the line card(s). If you want to include only one Engine in the data source, you must check the “Engine” box and provide the value of that Engine ID.

**Step 7** (Optional) SNMP v1/v2c RO Community String: If SNMP v1 or v2c will be used to communicate with the device, enter the community string that is configured on the device that is going to export NetFlow packets to the Packet Analyzer.

**Step 8** (Optional) “Enable SNMP v3”: If SNMP v3 will be used to communicate with the device, fill in the fields within the v3-specific dialog.

**Step 9** (Optional) If desired, fill in the SNMP credentials for the device. If valid SNMP credentials are provided, **Packet Analyzer** can upload readable text strings from the device to describe the interfaces on that device rather than just displaying the interfaces as numbers. You may specify either SNMPv2c or SNMPv3 credentials. See Table D-3.

**Step 10** Click **Test Connectivity** to see if the information you provided is accurate.

**Step 11** Click **Submit**.

## Creating NetFlow Data Sources Using the CLI

To manually configure a NetFlow data source on the Packet Analyzer using the CLI, for example if the autocreation feature is turned off, use the following steps. Note that when using the CLI, there are two separate phases involved. First you must create a "device" entry on the Packet Analyzer and remember the device ID. Then you must create a data source entry using this device ID. For convenience, these two phases are combined together when using the GUI to create NetFlow data sources.

**Step 1** Enter the command **device netflow**. You will now be in netflow device subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# device netflow

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@172-20-104-107.cisco.com(sub-device-netflow)#
```

**Step 2** Enter **?** to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-device-netflow)# ?
?                          - display help
address                    - device IP address (*)
cancel                     - discard changes and exit from subcommand mode
community                  - SNMPv2c community string
exit                       - create device and exit from sub-command mode
help                       - display help
show                       - show current config that will be applied on exit
snmp-version               - SNMP version to use to communicate with device
v3-auth-passphrase         - SNMPv3 authentication passphrase
v3-auth-protocol           - SNMPv3 authentication protocol
v3-priv-passphrase         - SNMPv3 privacy passphrase
v3-priv-protocol           - SNMPv3 privacy protocol
v3-sec-level               - SNMPv3 security level
v3-username                - SNMPv3 username

(*) - denotes a mandatory field for this configuration.

root@172-20-104-107.cisco.com(sub-device-netflow)#
```

**Step 3** Enter the IP address of the device as shown in this example (required):

```
root@172-20-104-107.cisco.com(sub-device-netflow)# address 192.168.0.1
```

**Step 4** If desired, enter the SNMP credentials for the device, as in the example below. If you specify snmp-version v2c, then you should enter the community string for the device. If you specify snmp-version v3, then you should enter the security level, username, authentication protocol, authentication passphrase, privacy protocol, and privacy passphrase.

```
root@172-20-104-107.cisco.com(sub-device-netflow)# snmp-version v2c
root@172-20-104-107.cisco.com(sub-device-netflow)# community public
```

**Step 5** Enter **show** to look at the device configuration that will be applied and verify that it is correct:

```
root@172-20-104-107.cisco.com(sub-device-netflow)# show
```

```
DEVICE TYPE         : NDE (Netflow Data Export)
DEVICE ADDRESS      : 192.168.0.1
SNMP VERSION        : SNMPv2c
V2C COMMUNITY       : public
V3 USERNAME         :
V3 SECURITY LEVEL   : No authentication, no privacy
V3 AUTHENTICATION   : MD5
V3 AUTH PASSPHRASE  :
V3 PRIVACY          : DES
V3 PRIV PASSPHRASE  :

root@172-20-104-107.cisco.com(sub-device-netflow)#
```

**Step 6** Enter **exit** to come out of the subcommand mode and create the device. Remember the ID value that was assigned to the new device, you will need it to create the data source!

```
root@172-20-104-107.cisco.com(sub-device-netflow)# exit
Device created successfully, ID = 1
root@172-20-104-107.cisco.com#
```

**Step 7** Enter the command **data-source netflow**. You will now be in netflow data source subcommand mode as shown here:

```
root@172-20-104-107.cisco.com# data-source netflow

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@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

**Step 8** Enter **?** to see all the command options available, as in the example below:

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# ?
?                         - display help
cancel                    - discard changes and exit from subcommand mode
device-id                 - netflow device ID (*)
engine-id                 - netflow Engine ID
exit                      - create data-source and exit from sub-command mode
help                      - display help
name                      - data-source name (*)
show                      - show current config that will be applied on exit

(*) - denotes a mandatory field for this configuration.

root@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

**Step 9** Enter the device ID from Step 4 (required):

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# device-id 1
```

**Step 10** Enter the name you would like for the data source (required):

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# name MyFirstNdeDataSource
```

**Step 11** If desired, supply the specific Engine ID for this NetFlow data source (optional):

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# engine-id 123
```

**Step 12** Enter **show** to look at the data source configuration that will be applied and verify that it is correct:

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# show

DATA SOURCE NAME : MyFirstNdeDataSource
```

```
DATA SOURCE TYPE : NDE (Netflow Data Export)
DEVICE ID       : 1
DEVICE ADDRESS   : 192.168.0.1
ENGINE ID        : 123

root@172-20-104-107.cisco.com(sub-data-source-netflow)#
```

**Step 13** Enter **exit** to come out of the subcommand mode and create the data source:

```
root@172-20-104-107.cisco.com(sub-data-source-netflow)# exit
Data source created successfully, ID = 3
```

The data source is now created, and NetFlow records from the device will be received and accepted by the Packet Analyzer as they arrive.

### Deleting NetFlow Data Sources Using the Web GUI

To delete an existing NetFlow data source, use the following steps. If the autocreation feature is turned on, and the device continues to send NetFlow packets to the Packet Analyzer, the data source will be recreated again automatically as soon as the next NetFlow packet arrives. Therefore, if you wish to delete an existing NetFlow data source, it is usually advisable to first turn the NetFlow autocreate feature off, as described earlier.

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click on the data source you would like to delete.

**Step 3** Click **Delete**.

### Deleting NetFlow Data Sources Using the CLI

To delete a NetFlow data source using the CLI, use the following steps. Note that when using the CLI, there are generally two separate phases involved. First you should delete the data source, then delete the device if you have no other data sources using the same device (for example with a different Engine ID value). As a shortcut, if you simply delete the device, then all data sources using that device will also be deleted.

**Step 1** Show all data sources so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show data-source

DATA SOURCE ID   : 1
DATA SOURCE NAME : DATA PORT 1
TYPE             : Data Port
PORT NUMBER      : 1
-----------

DATA SOURCE ID   : 2
DATA SOURCE NAME : DATA PORT 2
TYPE             : Data Port
PORT NUMBER      : 2
-----------

DATA SOURCE ID   : 3
DATA SOURCE NAME : MyFirstNdeDataSource
```

```
TYPE             : NDE (Netflow Data Export)
DEVICE ID        : 2
DEVICE ADDRESS   : 192.168.0.1
ENGINE ID        : 123
-----------

root@172-20-104-107.cisco.com#
```

**Step 2** Use the **no data-source** command to delete the data source:

```
root@172-20-104-107.cisco.com# no data-source 3
Successfully deleted data source 3
root@172-20-104-107.cisco.com#
```

**Step 3** Show all devices so you can find the ID of the one you want to delete:

```
root@172-20-104-107.cisco.com# show device

DEVICE ID            : 1
DEVICE TYPE          : NDE (Netflow Data Export)
IP ADDRESS           : 192.168.0.1
SNMP VERSION         : SNMPv2c
V2C COMMUNITY        : public
V3 USERNAME          :
V3 SECURITY LEVEL    : No authentication, no privacy
V3 AUTHENTICATION    : MD5
V3 AUTH PASSPHRASE   :
V3 PRIVACY           : DES
V3 PRIV PASSPHRASE   :
INFORMATION          : No packets received
STATUS               : Inactive
------

root@172-20-104-107.cisco.com#
```

**Step 4** Use the **no device** command to delete the device:

```
root@172-20-104-107.cisco.com# no device 1
Successfully deleted device 1
root@172-20-104-107.cisco.com#
```

Note that if the autocreation mode is on, and the device continues to send NetFlow packets to the Packet Analyzer, the data source (and device entry) will be re-created again automatically as soon as the next NetFlow packet arrives. Therefore, if you wish to delete an existing NetFlow data source, it is usually advisable to first turn the NetFlow autocreate feature off, as described earlier.

## 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, then click **Test**. The Device System Information Dialog Box displays. See Table D-4 for a description of the fields.

If the device is sending NetFlow Version 9 (V9) and the **Packet Analyzer** has received the NetFlow templates, then a V9 Templates button appears below the Device System Information window.

**Note** NetFlow v9 templates do not appear in all NetFlow packets. When there are no templates, the **V9 Templates** button does not appear.

# Forwarding CEF Traffic

Cisco Express Forwarding (CEF) is an advanced, layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as Internet, on networks characterized by intensive Web-based applications, or interactive sessions. For more information about CEF and configuring CEF, see the *Cisco IOS Switching Services Configuration Guide*.

You can configure CEF traffic copy and forward it to Packet Analyzer session as a Packet Analyzer data source from the remote device command line interface and not from the Packet Analyzer GUI.

As a CEF consumer, Packet Analyzer can receive CEF packets on its data port from Cisco monitoring interface. Packet Analyzer supports monitoring and analysis of incoming CEF data to be parsed by Packet Analyzer, stored in its internal database, and presented in the GUI in the same way as traffic from other data sources.

### Before You Begin

For the Packet Analyzer to receive CEF traffic from router, the device must be configured to copy and forward the CEF packets to Cisco Packet Analyzer.

To enable CEF as a data source:

- Configure CEF and CEF monitoring on devices
- CEF data port will be auto created on physical port receiving CEF traffic on devices

See the *Cisco IOS Switching Services Configuration Guide, Release 12.2* for CEF configuration examples.

**Note** Depending on the Cisco IOS/Nexus OS version on the managed device, the CLI format for configuring a CEF copy and forward session may be different from what appears in this document. Ensure that your IOS/Nexus OS version supports UCSE platform. Before you create CEF traffic monitoring session on a router, enable Packet Analyzer feature through UCSE CIMC. For list of router platforms and IOS releases support UCSE, see *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine, Release 2.x*.

See Understanding How the Packet Analyzer uses CEF, page A-8 for details of how to configure CEF monitoring.

## Managing WAAS and WAN Traffic

This section contains the following topics about using the **Packet Analyzer** GUI to manage WAAS data sources:



### Understanding WAAS

Cisco Wide Area Application Services (WAAS) software optimizes the performance of TCP-based applications operating in a wide area network (WAN) environment and preserves and strengthens branch security. The WAAS solution consists of a set of devices called Wide Area Application Engines (WAEs) that work together to optimize WAN traffic over your network.

When client and server applications attempt to communicate with each other, the network devices intercept and redirect this traffic to the WAEs to act on behalf of the client application and the destination server.

WAEs provide information about packet streams traversing through both LAN and WAN interfaces of WAAS WAEs. Traffic of interest can include specific servers and types of transaction being exported. **Packet Analyzer** processes the data exported from the WAAS and performs application response time calculations and enters the data into reports you set up.

The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through your network not optimized.

You can use the WAAS Top Talkers Detail Dashboard to analyze the traffic for optimization. See Analyzing Traffic for Optimization Using the Top Talkers Detail, page 3-17 for more information.

Cisco WAAS helps enterprises to meet the following objectives:

- Provide branch office employees with LAN-like access to information and applications across a geographically distributed network.
- Migrate application and file servers from branch offices into centrally managed data centers.
- Minimize unnecessary WAN bandwidth consumption through the use of advanced compression algorithms.
- Provide print services to branch office users. WAAS allows you to configure a WAE as a print server so you do not need to deploy a dedicated system to fulfill print requests.
- Improve application performance over the WAN by addressing the following common issues:
  - Low data rates (constrained bandwidth)
  - Slow delivery of frames (high network latency)
  - Higher rates of packet loss (low reliability)

For more information about WAAS and configuring the WAAS components, see the *Cisco Wide Area Application Services Configuration Guide*.

## Considering Deployment Scenarios

Table 7-2 lists six different deployment scenarios you might consider to monitor the optimized traffic on your WAAS network.

***Table 7-2 WAAS Data Source Configurations***

| | Deployment Scenario | Edge WAE Data Source | Core WAE Data Source |
|---|---|---|---|
| 1 | • Clients in the edge (branch)<br>• Servers in the core (data center)<br>• Packet Analyzer in the edge | Client<br>Client WAN | Server |
| 2 | • Servers in the edge (branch)<br>• Clients in the core (data center)<br>• Packet Analyzer in the core | Server | Client<br>Client WAN |
| 3 | • Servers in the edge (branch)<br>• Clients in the core (data center)<br>• Packet Analyzer in the edge | Server<br>Server WAN | Client |
| 4 | • Clients and servers in the edge (branch) and the core (data center)<br>• Packet Analyzer in the core | Client<br>Server | Client<br>Server<br>Client WAN<br>Server WAN |
| 5 | • Clients and servers in the edge (branch) and the core (data center)<br>• Packet Analyzer in the edge | Client<br>Server<br>Client WAN<br>Server WAN | Client<br>Server |

## Using the WAAS Central Manager

The Cisco WAAS is centrally managed by a scalable, secure, and simple function called the Cisco WAAS Central Manager, which runs on Cisco WAE Appliances. The Cisco WAAS Central Manager provides a centralized mechanism for configuring features, reporting, and monitoring, and can manage a topology containing thousands of Cisco WAE nodes.

Packet Analyzer is accessible from within the Central Manager interface. Packet Analyzer integration with WAAS Central Manager provides for easier viewing of **Packet Analyzer** reports that are directly associated with Application Response Time measurements through the WAN, in both WAAS optimized and non-optimized environments.

Below is a standard configuration workflow that you can follow.

Prerequisites are that the WAAS Central Manager is installed and functional, and the Packet Analyzer (device or virtual blade) is installed and functional.

**Step 1** From the WAAS Central Manager, configure the Packet Analyzer IP address and login credentials.

**Step 2** From the router or switch, configure the data source(s) for baseline (SPAN).

**Step 3** From the WAAS Central Manager, configure the Site definition. See Configuring Sites, page 7-49 for more information.

**Step 4** In the Monitor section of WAAS Central Manager, one can observe the Top Talkers under the Network Analysis tab. See Analyzing Traffic for Optimization Using the Top Talkers Detail, page 3-17 for more information.

**Step 5** From the WAAS Central Manager, configure the WAAS Flow Agent and branch/data center WAEs.

**Step 6** Create Device Groups for the branch and data center on the WAAS Central Manager, and assign a device to the Device Groups.

**Step 7** Enable the Flow Agent on the WAAS, pointing to the Packet Analyzer IP. Segments are automatically selected (enabled only if Packet Analyzer is configured). **Packet Analyzer** will start to compute baseline ART, protocol distribution, and Top Talkers. See Enabling WAAS Flow Agent, page 7-27.

**Step 8** Turn on WAAS optimization. See Optimizing WAN, page 3-16 for more information.

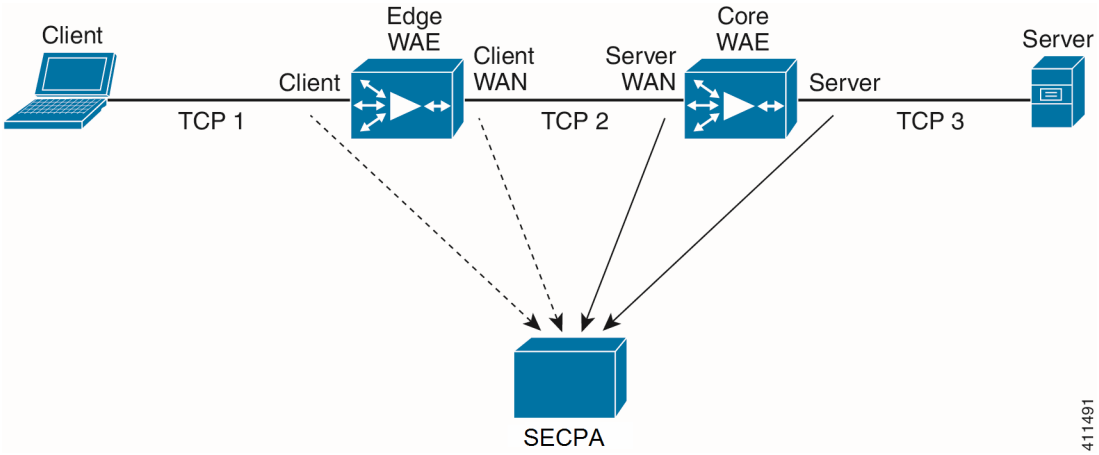
**Step 9** Turn on the Flow Agent and identify the servers to monitor to get ART improvements. See Editing WAAS Data Sources, page 7-28.

## Monitoring Response Time from WAAS Data Sources

**Packet Analyzer** processes the TCP flow data exported from the WAAS and performs application response time (ART) calculations and reports. You use the **Packet Analyzer** GUI to create a WAAS data source to monitor WAAS traffic statistics. In addition to ART, Packet Analyzer monitors and reports other traffic statistics of the WAAS data sources including application, host, and conversation information.

**Packet Analyzer** provides different ART metrics by collecting data at different points as packets flow along their paths. **Packet Analyzer** provides five different collection points, each represented by a WAAS data source. Figure 7-1, WAAS Data Sources (Data Collection Points), shows an example of the data collection points. The solid line represents data exported from a WAAS device and/or directly monitored traffic like SPAN. The broken line represents data exported from a WAAS device only.

***Figure 7-1 WAAS Data Sources (Data Collection Points)***




You can use the **Packet Analyzer** GUI to configure data sources at the locations in the network described in Table 7-3.

*Table 7-3 WAAS Data Collection Points*

| Setting | Description |
|---|---|
| **Client** | This setting configures the WAE device to export the original (LAN side) TCP flows originated from its clients to **Packet Analyzer** for monitoring. To monitor this point, configure a Client data source. |
| **Client WAN** | This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to **Packet Analyzer** for monitoring. To monitor this point, configure a Client WAN data source. |
| **Server WAN** | This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to **Packet Analyzer** for monitoring. To monitor this point, configure a Server WAN data source. |
| **Server** | This setting configures the WAE device to export the original (LAN side) TCP flows from its servers to **Packet Analyzer** for monitoring. To monitor this point, configure a Server data source. |
| **Passthrough** | This setting configures the WAE device to export the TCP flows that are passed through unoptimized. |

You can also configure a data source to use Export Passthrough data. For more information about configuring WAAS data sources, see Editing WAAS Data Sources, page 7-28.

## Monitoring Client Data Sources

By monitoring the TCP connections between the client and the WAE device (Client segment in Figure 7-1), you can measure the following ART metrics:

- Total Response Time as experienced by the client
- Total Transaction Time as experienced by the client
- Bandwidth usage (bits/packets) before optimization
- Number of transactions and connections.
- Network Time broken down into two segments: client-edge and edge-server

To view detailed views of this data, select the **Analyze > Response Time**. > **Detailed Views** submenu.

### Monitoring WAN Data Sources

By monitoring the TCP connections between the edge and core WAE devices (Client WAN and Server WAN segments in Figure 7-1), you can measure the following:

- Bandwidth usage (bits/packets) after optimization
- Network Time of the WAN segment

### Monitoring Server Data Sources

By monitoring the TCP connections between the core WAE devices and the servers (Server segment in Figure 7-1), you can measure the following ART metrics:

- Server Response Time (without proxy acceleration/caching server)
- Network Time between the core WAE device and the servers

**Note** **Packet Analyzer** measures Network Time by monitoring the TCP three-way handshake between the devices.

### Enabling WAAS Flow Agent

Before you can monitor WAAS traffic, you must first configure the WAAS device to export WAAS flow record data to the **Packet Analyzer.** Use the following WAAS command-line interface (CLI) **flow monitor** command to enable the Flow Agent on the WAAS:

**flow monitor tcpstat-v1 host <*secpa IP address*>**

**flow monitor tcpstat-v1 enable**

After you enable flow export to the **Packet Analyzer** using WAAS CLI commands like those above, WAAS devices will be detected and automatically added to the Packet Analyzer's WAAS device list.

You must then configure the WAAS segments you want to monitor as WAAS data sources: Client, Client WAN, Server WAN, and/or Server. See Editing WAAS Data Sources, page 7-28, for more detailed information.

You can also use the WAAS Central Manager to centrally issue WAAS CLI commands to configure a large number of WAEs at one time. **Packet Analyzer** is accessible from within the WAAS Central Manager interface. For more information about WAAS Central Manager, refer to the WAAS technical documentation.

**Note** In addition to configuring the WAAS devices, you must specify which application servers you want to monitor among the servers being optimized by WAAS devices. See Configuring WAAS Monitored Servers, page 7-67, for more detailed information.

For more information about WAAS and configuring the WAAS components, see the *Cisco Wide Area Application Services Configuration Guide*.

This section contains the following topics:

- Deleting a WAAS Data Source, page 7-29

## Adding Data Sources for New WAAS Device

**Packet Analyzer** uses WAAS data sources to monitor traffic collected from different WAAS segments: Client, Client WAN, Server WAN, and Server. Each WAAS segment is represented by a data source. You can set up **Packet Analyzer** to monitor and report other traffic statistics of the WAAS data sources such as application, host, and conversation information in addition to the monitored Response Time metrics.

**Note** This step is not usually necessary because export-enabled WAAS devices are detected and added automatically. See Enabling WAAS Flow Agent, page 7-27, for more information about how to enable WAAS export to the Packet Analyzer.

To manually add a WAAS device to the list of devices monitored by **Packet Analyzer**:

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**.

**Step 2** Click **Create**.

The Packet Analyzer Data Source Configuration Dialog appears.

**Step 3** Choose “WAAS” from the list of Types.

**Step 4** Enter the device IP address in the IP field.

**Step 5** Check the check boxes for the appropriate WAAS Segments. See Table 7-3.

**Step 6** Click **Submit** to add the new WAAS custom data source.

## Editing WAAS Data Sources

**Packet Analyzer** uses WAAS data sources to monitor traffic collected from different WAAS segments: Client, Client WAN, Server WAN, and Server. Each WAAS segment is represented by a data source. You can set up **Packet Analyzer** to monitor and report other traffic statistics of the WAAS data sources such as application, host, and conversation information in addition to the monitored Response Time metrics.

To edit a WAAS device’s custom data source:

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**. The data sources are displayed.

**Step 2** Choose the WAAS device you want to modify, and then click **Edit**.

You can configure the WAAS data sources to monitor the following WAAS segments as shown in Figure 7-1, WAAS Data Sources (Data Collection Points):

- Client—This setting configures the WAE device to export the original (LAN side) TCP flows originated from its clients to **Packet Analyzer** for monitoring.
- Client WAN— This setting configures the WAE device to export the optimized (WAN side) TCP flows originated from its clients to **Packet Analyzer** for monitoring.
- Server WAN—This setting configures the WAE device to export the optimized (WAN side) TCP flows from its servers to **Packet Analyzer** for monitoring.
- Server—This setting configures the WAE device to export the original (LAN side) TCP flows from its servers to **Packet Analyzer** for monitoring.

SPAN data sources might take the place of the WAE Server data sources listed in Table 7-2. For example, if you already configure SPAN to monitor the server LAN traffic, it is not necessary to enable the Server data source on the WAE device.

**Note** The following step is optional and applies only when **Packet Analyzer** is configured to export data to an External Response Time Reporting Console, such as the NetQos Super Agent.

### Deleting a WAAS Data Source

To delete a WAAS custom data source:

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**. The data sources are displayed.

**Step 2** Choose the WAAS custom data source you want to delete, then click **Delete**.

A dialog box displays the device address and asks if you are sure you want to delete the device.

### Auto Create of New WAAS Devices

If you have numerous WAE devices, you can set up **Packet Analyzer** to configure newly discovered WAE devices using a predefined configuration template using the **Packet Analyzer** auto configuration option.

**Note** If most of your WAE devices are edge WAE, you might want to set the auto configuration to be that of the edge device, then manually configure the data center WAE. For example, select the Client segment for monitoring.

To configure WAAS autoconfiguration:

**Step 1** Choose **Setup > Traffic > Packet Analyzer Data Sources**. The data sources are displayed.

**Step 2** Click **Auto Create**.

The Packet Analyzer Data Source Configuration Dialog displays.

**Step 3** Check the **WAAS** check box.

**Step 4** Check the check boxes for the desired Segments. See Editing WAAS Data Sources, page 7-28, for more information.

## Configuring Hardware Deduplication

**Note** This section applies only to Cisco Cisco Security Packet Analyzer 2400appliance.

**Packet Analyzer** supports hardware-based detection of duplicate packets and allows you to configure a single deduplication filter that reduces the amount of duplicate traffic across all adapter ports.

You can use deduplication to eliminate redundant data. This can help to significantly shrink storage requirements and improve bandwidth efficiency on tasks like backup and recovery.

After you enable deduplication, the Packet Analyzer detects and filters the duplicated packets. The packet is identified as duplicated if all inspected segments match another packet within the specific time window.

In addition to the duration-based timeout, there is also a fixed packet-count timeout. There cannot be more than 7 packets between the duplicate packets. If packets 0 and 8 are identical, packet 8 *will* be dropped. If packets 0 and 9 are identical, packet 9 *will not* be dropped.

To configure packet deduplication:

**Step 1** Choose **Setup > Traffic > Hardware Deduplication**.

**Step 2** Check the **Enabled** check box to enable packet deduplication.

Enter a value in the Time Window (1-127 in millisecond (ms)) for the search or buffer period.

The value you set in the Time Window indicates the length of time (ms) in which two packets can be considered duplicates. If the Time Window is 100 ms but two identical packets arrive 120 ms apart, the second packet would not be dropped. If the identical packets arrive 80 ms apart, the second packet would be dropped.

**Step 3** Click to choose a segment of the packet to inspect for deduplication.

The default inspects the entire packet. The second option inspects all segments except the ISL portion of the packet. The third option inspects all segments except the ISL, MAC, and VLAN portions of the packet. The fourth option inspects all segments except the ISL, MAC, and VLAN portions of the packet. The final (bottom) option inspects only the UDP/TCP and payload segments of the packet.

**Note** Regardless of the option you choose, the packet checksum is ignored.

**Step 4** Click **Submit** to enable the settings you have entered, or click **Reset** to cancel any change.

# Setting Up Alarms and Alarm Thresholds

Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. You can choose what types of events for which you want Packet Analyzer to notify you, and how you want to be notified. Monitoring alarms enables you to watch problem areas and collect data on areas such as increased utilization, severe application response delays, and voice quality degradation.

This is the order that you typically follow for setting up alarms and alarm thresholds:

**Step 1** Define the way you would like to be notified when an alarm occurs (by e-mail, trap, trigger capture, or syslog).

- For e-mail server settings: Choose **Administration > System > E-Mail Setting**
- For trap settings: Choose **Administration > System > SNMP Trap Setting**
- For capture session settings: Choose **Capture > Packet Capture/Decode > Sessions**
- For syslog settings: Choose **Administration > System > Syslog Setting**

**Step 2** Define the Alarm Action at **Setup > Alarms > Actions**.

**Step 3** Define the Threshold for this alarm at **Setup > Alarms > Thresholds**.

The tasks for setting up alarms are:

- Configuring Alarm Actions, page 7-31
- Viewing Alarm Actions, page 7-33
- Defining Thresholds, page 7-34

# Configuring Alarm Actions

Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both.

When a threshold's rising water mark is crossed, the alarm condition is met. This triggers the alarm action to take effect.

To configure an alarm action:

**Step 1** Choose **Setup > Alarms > Actions**.

The Alarm Action page displays any configured actions. If none of the four actions (e-mail, trap, capture, or syslog) are configured, you will see `No data available`.

**Step 2** Click **Create**.

**Step 3** Enter a Name for the action (up to 63 characters).

**Step 4** Choose the type of alarm action. Packet Analyzer supports any combination of these four actions in one alarm condition:

| Alarm Action | Description | Important Notes |
|---|---|---|
| **E-mail syslog** | An alarm action that e-mails the syslog content of the alarm condition. To avoid e-mail flooding the network, **Packet Analyzer** does not send more than five e-mails in any given hour. | Configure the e-mail address in **Administration > System > E-Mail Setting**. Packet Analyzer alarm mail is sent as a result of Packet Analyzer alarms, not router or switch alarms.<br>Packet Analyzer sends up to five e-mails per hour per function (traffic and NetFlow, voice signaling, RTP, and application response time). Also, in each e-mail, there could be up to five alarm messages. These limits are in place to avoid e-mail overload.<br>If you have configured e-mail alarms and do not receive e-mail, then your Packet Analyzer does not have any alarms.<br>If Packet Analyzer sends you many alarm messages, the e-mail may state, for example, "5 of 2,345 alarm messages." |
| **Trap** | An alarm action that sends Packet Analyzer trap messages to one or more trap servers. Any trap server that has the same community string will receive the trap message. Packet Analyzer uses Cisco Syslog MIB in the trap message. To avoid trap flooding, the limit is ten trap messages per interval. | Choose the SNMP community where you would like traps to be sent. Configure the community string in **Administration > System > SNMP Trap Setting**. After the "Community field appears, choose the community string from the drop-down list. |
| **Trigger capture** | An alarm action to start or stop a pre-defined capture session or stop a capture to save it to a file. | From the Session drop-down, choose the session (the list will be empty if there is no capture session configured in **Capture > Packet Capture/Decode > Sessions**). Click the **Start Capture**, **Stop Capture**, or **Stop Capture and Save to File** radio button. For more details, see Understanding Trigger Capture, page 7-33. |
| **Remote syslog** | An alarm action that sends syslog messages to remote syslog servers. The limit is ten syslog messages per interval to avoid flooding the network. | This will log syslog messages. The default setting is to log syslog messages locally to Packet Analyzer. If you want to log syslog messages to remote servers, set up the destination information at **Administration > System > Syslog Setting**. |

**Step 5** To edit or delete alarm actions, select the alarm and use the appropriate button.

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

The Alarm Action table displays the newly configured action in its list.

# Viewing Alarm Actions

Alarms are predefined conditions based on a rising data threshold, a falling data threshold, or both. 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.

Packet Analyzer supports IPv6 for all alarm functionality.

**Note** You could see two alarms for the same occurrence if both the source and the destination are in the same site.

To see events that have been created, choose **Setup > Alarms > Actions**. See Table D-5 for descriptions of the fields on the Alarm Configuration window.

To configure alarm actions, see Configuring Alarm Actions, page 7-31.

## Understanding Trigger Capture

This section describes how to use a trigger capture to start a capture session based on the alarm parameters you set. For example, you can set alarm parameters on various thresholds to start a capture session which can be used to investigate some kind of questionable network activity.

You must set your alarm threshold parameters so that Packet Analyzer has defined rising or falling numbers that will cause an action, or trigger, to start a capture session. You can also use the stop-and-save and Scheduled Capture option. The actions are defined below:

- Trigger Capture **Start**—An alarm condition occurs based on threshold parameters you have set; the capture session starts automatically.
- Trigger Capture **Stop**: An alarm condition occurs based on the threshold parameters you have set; the capture session stops automatically.
- Trigger Capture **Stop Capture and Save to File**—An alarm condition occurs, stopping the capture session. If the captured packet data is in memory, it is saved to a file. The buffer memory is then clear to wait for next alarm event.
- Trigger Capture **Scheduled Capture**—An alarm condition occurs, starting the capture session on specific date time for certain duration (in minutes).

When an event occurs that you have defined as an alarm threshold, Packet Analyzer stops any existing capture session and saves the captured packets from memory into a file. The capture session then restarts. Packet Analyzer can save up to five files, depending on your local hard disk storage.

Packet Analyzer monitors for threshold parameters every minute. For real-time data, the default is 5 minutes.

# Defining Thresholds

Packet Analyzer can inspect incoming performance records and apply a configured set of thresholds to the most recent interval of data. Using thresholds allows you to target specific network traffic issues and set up notifications that are triggered when certain thresholds are crossed. For example:

- if a server's CPU load exceeds 90%
- if a device or the whole network uses more bandwidth than usual, or
- if the remaining file size on a disk drive is less than 15% or 100 MB.

In general, you should set thresholds so that only severe traffic problems that impact quality of service generate events. These critical events are intended to provide actionable notification of problems to network operators. When setting thresholds try to identify a traffic level that will have a noticeable effect on network service levels. Set a duration that corresponds to an unacceptable period of poor service. The goal is to generate very few, significant events indicating severe problems that require immediate attention. Thresholds are not intended as a reporting tool to generate statistical information about network traffic.

To set up alarm thresholds for variables with values that trigger alarms, see Viewing Alarm Actions, page 7-33.

**Note** You could receive two alarms for the same occurrence if both the source and the destination are in the same site.

You can also decide whether you want to be notified **if the threshold is being crossed just once**, or whether you only want an alarm to be triggered if this state p**ersists for a certain time**. This helps you to ensure an effective network monitoring system, which will not bombard you with unnecessary notifications.

Packet Analyzer Threshold Alarms window (**Setup > Alarms > Thresholds**) displays thresholds you have configured. If you hover over the arrow next to the threshold Name a detailed view of the selected threshold displays.

For descriptions of the fields on the Threshold window, see Table D-6.

You can set up alarm thresholds by defining threshold conditions for monitored variables on the Packet Analyzer.

You can configure the following thresholds:

- Setting Host Thresholds, page 7-35
- Setting Conversation Thresholds, page 7-35
- Setting Application Thresholds, page 7-35
- Setting Response Time Thresholds, page 7-36
- Setting DSCP Thresholds, page 7-36
- Setting RTP Stream Thresholds, page 7-37
- Setting Voice Signaling Thresholds, page 7-37
- Setting NetFlow Interface Thresholds, page 7-38
- Setting Video Stream Thresholds, page 7-38
- Setting MDI Stream Thresholds, page 7-39

**Related Topics**

- Configuring Alarm Actions, page 7-31
- Viewing Alarm Actions, page 7-33

## Setting Host Thresholds

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **Host** tab.

**Step 3** The Host Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table D-7 describes the fields available on this window.

**Note** If you leave a selection blank, it means that the parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

**Step 4** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 5** When finished, click **Submit.**

## Setting Conversation Thresholds

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **Conversation** tab.

**Step 3** The Conversation Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table D-8 describes the fields available in this window.

**Note** If you leave a selection blank, it means that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

**Step 4** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 5** When finished, click **Submit.**

## Setting Application Thresholds

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **Application** tab.

**Step 3** The Application Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table D-9 describes the fields available in this window.

**Note** If you leave a selection blank, it means that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

**Step 4** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 5** When finished, click **Submit.**

## Setting Response Time Thresholds

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **Response Time** tab.

**Step 3** The Response Time Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table D-10 describes the fields available in this window.

**Note** If you leave a selection blank, it means that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

**Step 4** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 5** When finished, click **Submit.**

## Setting DSCP Thresholds

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **DSCP** tab.

**Step 3** The DSCP Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table D-11 describes the fields available in this window.

**Note** If you leave a selection blank, it means that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

**Step 4** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 5** When finished, click **Submit.**

## Setting RTP Stream Thresholds

Packet Analyzer sends syslog, trap, e-mail, and trigger captures for RTP streams that violate stream statistics thresholds on the following metrics:

- Number of Consecutive Packet Loss

  Each RTP packet has an RTP header that contains a sequence number. The sequence number increments by one for each RTP packet received in the same RTP stream. A gap in the sequence numbers identifies a packet loss. If the gap in sequence numbers jump is more than the threshold, the software raises an alarm condition.

- Packet Loss percent

  There are two types of percent packet loss percent: Adjusted Packet Loss and Actual Packet Loss. Actual Packet Loss indicates expected packets that never appear in **Packet Analyzer**. Adjusted Packet Loss includes actual packets lost and packets that arrive with large delay beyond the expected buffer capacity of the endpoint.

- Jitter: Packets delay compare to the expected receiving time
- Concealment Seconds: Seconds in which there is one or more packets lost
- Severe Concealment Seconds: Seconds in which there is more than 5% of packet lost

To set thresholds for RTP streams:

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **RTP Streams** tab.

**Step 3** The RTP Stream Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table D-12 describes the fields available in this window.

**Note** If you leave a selection blank, it means that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

**Step 4** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 5** When finished, click **Submit.**

## Setting Voice Signaling Thresholds

You can set up software to monitor voice call quality. When Cisco Unified Communication Manager's call detail records option is enabled, Cisco IP phones, both SCCP and SIP, will report the call's jitter and packet loss at the end of the call. Packet Analyzer intercepts this information and raises an alarm when the alarm condition crosses the rising threshold.

To set up a voice signaling threshold:

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose **Voice Signaling** tab.

**Step 3** The Voice Signaling Alarm Threshold Configuration window displays. Fill in the fields as appropriate.

Table D-13 describes the fields available under the Voice Signaling Metrics drop-down menu.

**Note** If you leave a selection blank, it means that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

**Step 4** Click **Submit** to set the voice signaling thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 5** When finished, click **Submit.**

## Setting NetFlow Interface Thresholds

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **NDE Interface** tab.

The NDE Interface Alarm Threshold Configuration window displays. The fields are described in Table D-14.

**Note** If you leave a selection blank, it means that parameter will not be considered. If you select **Any**, it will use any of the selections for that parameter, if encountered.

**Step 3** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

## Setting Video Stream Thresholds

Packet Analyzer can monitor the quality of video streams and trigger alarms for video streams that violates stream statistics thresholds. Each video stream contains a series of video frames. The video frames are of different frame type such as I (Intra), P (Predicted) and B (Bi-predictive). I frames are the most important frames in the video. The metrics are given with regard to only I frames or to all frame types. The metrics are as follows:

- Number of Video Frame Loss Count
- I or All frame loss count in the current interval
- Video Frame Loss Percentage
- All frame loss percentage in the current interval

To set thresholds for Video streams:

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **Video Streams** tab.

The Video Stream Alarm Threshold Configuration window displays. Fill the fields as appropriate. Table D-14 describes the fields available in this window.

**Step 3** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 4** Click **Submit** when finished.

## Setting MDI Stream Thresholds

MDI streams are defined as video streams that are carried over MPEG-TS. Packet Analyzer can monitor the quality of MDI streams and trigger alarms for streams that violates stream statistics thresholds on the following metrics:

- Delay Factor: RFC-4445 delay factor.
- Media Loss Rate: RFC-4445 media loss rate.

To set thresholds for Video streams:

**Step 1** Choose **Setup > Alarms > Thresholds**.

**Step 2** Click **Create** and choose the **MDI Streams** tab.

The MDI Stream Alarm Threshold Configuration window displays. Fill the fields as appropriate. The following table describes the fields available in this window.

**Step 3** Click **Submit** to set the thresholds, click **Reset** to reset the thresholds to their default value, or click **Cancel** to remove any changes you might have made.

**Step 4** When finished, click **Submit**.

## Editing or Deleting an Alarm Threshold

You can edit alarm thresholds on an as-needed basis. You can delete thresholds when you no longer need them. Any changes take effect immediately.

To edit or delete an alarm threshold:

**Step 1** Choose **Setup > Alarms > Thresholds**.

The Thresholds table displays.

**Step 2** Select the alarm, then click **Edit** or **Delete**.

**Step 3** Depending on your selection:

- If you selected to edit, the dialog box displays for the type of alarm; for example, **Host Threshold**. Make the necessary changes. Then
  - click **Submit** to save your changes
  - click **Reset** to reset the thresholds to the values set before you edited them, or

  - click **Cancel** to cancel the edit and return to the previous page.
- If you selected to delete, click **OK** to confirm deletion, or click **Cancel** to leave the configuration unchanged.

# Setting Up Data Export

The tasks for setting up data export are:

- Configuring NetFlow Export Templates, page 7-40
- Scheduling Data Report Exports, page 7-42
- Sharing Files, page 7-41

## Configuring NetFlow Export Templates

This section contains the following topics:

- Creating NetFlow Export Templates, page 7-40
- Editing NetFlow Export Templates, page 7-40
- Deleting NetFlow Export Templates, page 7-41

### Creating NetFlow Export Templates

To create NetFlow Export templates:

**Step 1** Choose **Setup > Data Export > NetFlow**.

The NetFlow Export Template page appears.

**Step 2** Click **Create**.

The Export Configuration page appears.

**Step 3** Fill in the fields as described in Table D-33.

**Step 4** Click **Submit** to save your changes.

### Editing NetFlow Export Templates

To edit NetFlow Export templates:

**Step 1** Choose **Setup > Data Export > NetFlow**.

**Step 2** Click the template that you want to edit.

**Step 3** Click **Edit**.

**Step 4** Modify the information as desired.

**Step 5** Click **Submit** to submit to save the changes.

## Deleting NetFlow Export Templates

To delete NetFlow Export templates:

**Step 1** Choose **Setup > Data Export > NetFlow**.

**Step 2** Click the template that you want to delete.

**Step 3** Click **Delete**.

**Step 4** Click **OK** to confirm, or **Cancel** to return to the previous window without deleting.

# Sharing Files

This feature allows you to easily access the Packet Analyzer data files. You can map the Packet Analyzer as a network drive and it will appear like any other folder in your machine. You will be able to only read and delete the files for security and stability reasons.

To share the Packet Analyzer data files:

**Step 1** Check the **Enable** check boxes to enable the SMB and SFTP file sharing services.

**Step 2** Enter the port details for SMB and SFTP services.

**Step 3** Select either **Share** or **Hide** to share or hide the capture files and scheduled reports.

The dataset access behavior varies between SMB and SFTP. If SMB is enabled, and if the dataset is hidden, the directory will not be visible. If SFTP is enabled, and dataset is hidden, the directory will be visible but you will not be able to access or view any files within it.

**Step 4** Click **Submit** to access the shared files via SMB or SFTP using web-user's username and password.

## Using SMB file sharing on Windows

Click **Start** button and provide the Packet Analyzer IP address of the shared object. For example, 172.20.124.164 to access the shared files on Windows operating system.

You can also access the files on Linux and set a customized port too.

## Using SFTP file sharing on Windows

Windows does not support SFTP by default, you must install a third part FTP application, such as Filezilla to use the SFTP file sharing on windows.;

**Step 1** Launch the FTP application and provide the SFTP IP address. For example, 172.20.124.164.

**Step 2** Click **Quickconnect** to access the shared file.

**Note** TACACS users cannot use the file sharing feature. You have to use Packet Analyzer's local web-users to access the shared files.

# Scheduling Data Report Exports

You can use Packet Analyzer to schedule data collection over a period of time for trend analysis and troubleshooting activities and then export the reports to be viewed at your convenience. For example, if you see a spike in application response time on a certain day or time you can set up a scheduled report. The report exports collected data from a specific range of time so that you have a snapshot of what might be causing issues.

You can set up scheduled jobs that will generate a daily report at a specified time, in a specified interval, and e-mail it to a specified e-mail address or addresses.

You can also obtain a report immediately by clicking the **Preview** button, rather than wait for the scheduled time. This report can also be sent after you preview it.

**Tip** Packet Analyzer displays time in preview report based on the browser that initiated the report. So if your browser is in San Jose, CA, the time zone displayed in the report is based on the time zone of that machine. Scheduled email report shows Packet Analyzer server timezone. The data is not based on the Packet Analyzer server time if the two machines are not synchronized. To synchronize your time, see Synchronizing Your System Time, page 5-5.

This section covers the following topics:



## Creating a Scheduled Report Export

Scheduled export of data reports is a convenient way to collect traffic of interest in Packet Analyzer. We strongly recommend you to define your data report time range first and then set your export time right after your report end time. This is the most straight-forward way to use this feature.

To set up a scheduled report and export it to an e-mail address or addresses:

**Step 1** From any Monitor or Analyze window, click **Export** in the Interactive Report pane to select your export preferences. If you want the report to contain filtered data, enter the filters before selecting **Export**.

**Step 2** Enter the Report Name and Report Description. Report name should be at least four characters long.

**Step 3** Enter the e-mail address to which you would like the report to be delivered.

**Step 4** Choose either CSV or PDF as the delivery option.

**Step 5** Choose **Save** to save the report to your local disk.

**Step 6** Choose the Report Time by selecting a time range for the interval of time you want data measured. The time range is limited to a 24 hour period. Any time range that includes midnight will have a *from* time larger than *to* time.

**Step 7** Choose the Export Time (which is the day of the week on which to generate the weekly report and hour that report will be sent). Multiple days are supported. You can also specify what time to start the export.

The actual data time range used to generate the report for export is always the last available and complete time span specified in the Report Time step above. Packet Analyzer does not generate reports using data in any future time. For example:

| Export Time | Report Time | Data Reported and Exported |
|---|---|---|
| If Every Day and Hour is 09:00 | 07:00 to 08:00 | 07:00 to 08:00 the same day (recommended use case) |
| If Monday and Friday and Hour is 03:00 | 05:00 to 05:59 | Sunday and Thursday 05:00 to 05:59 |
| If Every Day and Hour is 00:00 | 18:00 to 01:00 | Starts two days before current day from 18.00 to the next day 1.00 |

**Tip** Set your Export Time to occur right after the end of Report Time. This gives you the most recent data and is the easiest way to use this feature.

**Step 8** Click **Submit** to submit the request for the scheduled job,or click **Preview** to generate the report immediately.

**Note** Remember that report results are based on the local time of the browser that initiated the report.

## Editing a Scheduled Export Job

**Step 1** Choose **Setup > Data Export > Scheduled Exports**.

**Step 2** Click the job you want to edit.

**Step 3** Click **Edit**.

**Step 4** Modify the information as desired.

**Step 5** Click **Submit** to submit the request for the scheduled job.

## Deleting a Scheduled Export Job

**Step 1** Choose **Setup > Data Export > Scheduled Exports**.

**Step 2** Click the job you want to delete.

**Step 3** Click **Delete** to delete the selected job, or click **Delete All** to delete all the jobs.

**Step 4** Click **OK** to confirm, or click **Cancel** to return to the previous window without deleting the job.

## Downloading a Scheduled Report

To download a scheduled report:

**Step 1** Choose **Setup > Data Export > Scheduled Exports**.

**Step 2** Click **Saved Reports** tab.

You will be able to view the saved reports in a tabular format.

**Step 3** Select the reports that you want to download.

**Step 4** Click **Download**.

## Renaming a Scheduled Report

To rename a scheduled report:

**Step 1** Choose **Setup > Data Export > Scheduled Exports**.

**Step 2** Click **Saved Reports** tab.

You will be able to view the saved reports in a tabular format.

**Step 3** Select the reports that you want to rename.

**Step 4** Click **Rename**.

## Deleting a Saved Reports

**Step 1** Choose **Setup > Data Export > Scheduled Exports**.

**Step 2** Click **Saved Reports** tab.

**Step 3** Click the reports you want to delete.

**Step 4** Click **Delete** to delete the selected job, or click **Delete All** to delete all the jobs.

**Step 5** Click **OK** to confirm, or click **Cancel** to return to the previous window without deleting the job.

# Accessing Device Interface and Health Details

You can enable your Packet Analyzer to access interface and health device details if they are available on the device you identify using the Packet Analyzer Managed Device feature.

This section contains the following topics:



## Understanding How Platform-Specific Packet Analyzer Handle Managed Device Data

A managed device can represent a router or switch being monitored by Packet Analyzer. Depending on your Packet Analyzer platform, the managed device is accessed by the Packet Analyzer differently and may support different MIBs based on the device support.

The following details list how Packet Analyzer accesses the managed device:

- For a physical or virtual blade or service module, the managed device is the device in which Packet Analyzer software or hardware is located. The managed device information is automatically updated without user intervention and cannot be modified on the Packet Analyzer. One of the benefits of having a blade or service module is that there is no configuration required for this feature.
- For a physical appliance, you identify the managed device as a switch or router that shares its traffic using SPAN or user credentials. You must enter the device address and either the SNMP credentials or NetConf credentials to configure the Packet Analyzer SPAN session on the managed device. On certain platforms, NetConf is an alternative for Packet Analyzer to configure a Packet Analyzer SPAN session on a managed device which does not support configuring Packet Analyzer SPAN sessions using SNMP. If you choose to use NetConf, you must enable NetConf on the managed device interface and enable SSH to support the SPAN session. This enables you to monitor managed device information such as interface statistics.

For MIB support, see Table D-75 on page D-58.

## Configuring and Viewing Managed Device Information

The managed device information that is required is dependent on your platform device type. For details, see Understanding How Platform-Specific Packet Analyzer Handle Managed Device Data, page 7-45.

For details on how to ensure Packet Analyzer is managing your device interface and other traffic, see:

# Configuring Managed Device Information on Appliances

## Enabling Multi-Managed Device Feature

This feature is available on Cisco Security Packet Analyzer 2400 series appliances. By default, these Packet Analyzer appliances support a single managed device, which could be either a Cisco Catalyst 6000 or Nexus 7000 switch. When the multi-managed device feature is enabled, the Packet Analyzer appliance instead supports one Catalyst 6000 switch per data port.

To enable the multi-managed device feature:

**Step 1** Log into the Packet Analyzer CLI.

**Step 2** Enter the command `managed-device multiple`.

To disable this feature, enter the command **`no managed-device multiple`**.

After you enable this feature, the following Packet Analyzer GUI pages will have a different layout compared to the default single managed device GUI layout:

- **Setup > Managed Device > Device Information**
- **Setup > Traffic > SPAN Sessions**
- **Analyze > Managed Device > Interface**

Additionally, the **Analyze > Managed Device > Health** GUI page will no longer be available.

## Configuring a Managed Device per Packet Analyzer Data Port

After you enable the multi-managed device feature, you can use the Packet Analyzer GUI or CLI to configure a single managed device per Packet Analyzer data port.

**Note** The multi-managed device feature supports only Cisco Catalyst 6000 series switches as managed devices. For Nexus 7000 series switches, RISE provides similar functionality.

To configure the managed device for a Packet Analyzer data port using Packet Analyzer GUI:

**Step 1** Choose **Setup > Managed Device > Device Information**.

The Device Information window shows a list of managed devices that are currently setup in the Packet Analyzer.

**Step 2** Click the **Add** button to add a managed device for Packet Analyzer data port.

See Table D-34 for field descriptions.

**Step 3** Click **Add**.

To edit a managed device using Packet Analyzer GUI:

**Step 1** Choose **Setup > Managed Device > Device Information**.

**Step 2** Select the managed device by clicking the radio button, and then click **Edit**.

See Table D-34 for field descriptions.

**Step 3** Click **Edit**.

**Note** If the mapping from Packet Analyzer data port to Packet Analyzer managed device interface is not set correctly, network functions on the Packet Analyzer managed device (Cisco Catalyst 6000 switch) may be disrupted while configuring a SPAN session for the Packet Analyzer data port.

To configure the managed device for a Packet Analyzer data port using the Packet Analyzer CLI instead:

- For SNMPv2, use the command **`managed-device snmp-v2c`**.
- For SNMPv3, use the command **`managed-device snmp-v3`**. After entering the snmpv3 subcommand mode, enter **`?`** to display a list of subcommands. Use the appropriate subcommands to configure the SNMPv3 parameters as necessary, then use **`exit`** to exit from the subcommand mode and apply the settings.

#### Configuring a SPAN Session

You can configure a SPAN session only from Packet Analyzer GUI.

To add or configure a SPAN session for a managed device:

**Step 1** Choose **Setup > Traffic > SPAN Sessions**.

The window shows a list of SPAN sessions that are currently configured on the managed device.

**Step 2** Select a managed device from the drop-down list.

**Step 3** Click the **Add** to add a SPAN session.

The **Create SPAN Session** window appears.

**Step 4** Fill in the appropriate information in the **Create SPAN Session** window.

See Table D-1 for field descriptions.

**Step 5** Click **Create** to create the SPAN session for the selected managed device**.**

**Note** If the SPAN configuration has been modified from the managed device side, those changes will not be reflected in the Packet Analyzer GUI automatically. Click the **Refresh** button before making SPAN configuration changes to ensure that up-to-date SPAN session information is displayed.

**Warning** **Limitations on SPAN sources, destinations, and traffic rates vary by Catalyst 6000 system and IOS image. Refer to the SPAN configuration document of your managed device to avoid network problems due to SPAN oversubscription.**

## Configuring Managed Device Information on RISE Appliances

For some Packet Analyzer appliance in RISE mode, you must set up your managed device using the Packet Analyzer **Setup > Managed Device > Device Information** window.

To edit your managed device parameters:

**Step 1** Choose **Setup > Managed Device > Device Information**.

The managed devices and the VDC details appear.

**Step 2** Select the short term interval from the **Managed Device Interface Stats** drop-down list and click **Submit**.

When you modify the interval, the existing data will be removed.

**Step 3** Select the managed device and click **Edit**.

**Step 4** Select the VDC which you want to enable/disable and click **Enable/Disable**. To delete or refresh VDC details, click **Delete** or **Refresh**.

## Viewing Managed Device Information

To view the system information for each managed device, choose **Setup > Managed Device > Device Information**.

Depending on your platform, the System Information may display some or all of the fields shown in Table D-19.

### Viewing Managed Device Interface Statistics

Packet Analyzer allows you to view the interface statistics of one managed device at a time. Once the managed device is configured, Packet Analyzer will periodically perform SNMP polling and provide a historical view of traffic statistics on the managed device interface. To view the interface statistics of another device, click the **Filter** button in the Interactive Report window, and select the desired managed device.

To view the interface statistics of a managed device:

**Step 1** Choose **Analyze > Managed Device > Interface**.

**Step 2** Select a managed device from the **Managed Device** drop-down list.

**Step 3** Select the desired time range from the **Time Range** drop-down list.

**Step 4** Click the **Submit** button.

The window shows a graphical representation of interface statistics of the device across the specified time range. The Interface Statistics line chart is updated upon selection of a row in the Interface Statistics table.

# Configuring Network Parameters

This section describes how to set up the network parameters including:

- Configuring Sites, page 7-49
- Setting Interface Speed using NetFlow Interface Capacity, page 7-52

- Configuring DSCP Groups, page 7-53

# Configuring Sites

Cisco Security Packet Analyzer makes it easier to monitor traffic and identify issues across your network by providing a way to manage large campuses using different views of your network, referred to as *sites*.

A *site* is a collection of hosts (network endpoints) partitioned into views. You can limit the view of your network analysis data to a specific city, a specific building, or even a specific floor of a building, and can use sites to focus collection and analysis of data. Sites are optional, but recommended.

See the following sections to set up sites:

- Defining a Site, page 7-49
- Viewing Defined Sites, page 7-49
- Configuring Sites Using Subnets, page 7-50

## Defining a Site

A site can be defined as a set of subnets specified by an address prefix and mask, or using other criteria such as a remote device data source (for example, remote WAE device and segment information).

Configuring Sites Using Subnets, page 7-50 gives specific information about various scenarios.

To set up a site or sites:

**Step 1** Choose **Setup > Network > Sites** and click **Create**.

**Step 2** The Site Configuration window appears. Enter a Name, Description, Subnet, and Data Source as appropriate.

See Table D-20 for field descriptions.

**Step 3** Enter the subnet and data source, then click **Detect** to tell the software to look for subnets in the traffic. See Detecting Site Subnets, page 7-49.

**Step 4** Click **Submit**.

**Note** The "Unassigned" site (with a description of "Unclassified hosts") includes any that do not match any of your site configurations. Sites are classified at the time of packet processing.

### Detecting Site Subnets

When you click the **Detect** button at **Setup > Network > Sites > Sites Configuration**, Packet Analyzer looks for subnets detected within in the past hour. See Table D-21 for information about the fields.

When you click **Detect**, Packet Analyzer finds those subnets that meet the criteria that you entered.

## Viewing Defined Sites

To view already-defined sites:

**Step 1** Choose **Setup > Network > Sites**.

**Step 2** The Sites window appears. Defined sites will be listed in the table.

The fields are described in Table D-22.

## Editing a Site

You can edit sites that have been created. The Unassigned site cannot be edited or deleted.

**Step 1** Choose **Setup > Network > Sites**.

**Step 2** Highlight the site that you have configured.

**Step 3** Click **Edit** and edit the desired field.

The fields are described in Table D-22.

**Step 4** Click **Submit** to save the changes, or click **Reset** and **OK** to reinstate the site's previous settings, or click **Cancel** to cancel any changes and return to the main Sites page.

## Configuring Sites Using Subnets

The site definition is very flexible and can accommodate various scenarios. Packet Analyzer uses the site definition not only for viewing of data, but for data export and data retention as well. The same rule cannot be defined in multiple sites. That is why the preferred way is to define a site using its subnets. See Table 7-4 for examples of site definitions.

**Note** VLAN option is removed from the Site definition.

For details on how Packet Analyzer resolves overlapping IP addresses, see Resolving Ambiguity (Overlapping Site Definitions), page 7-52

***Table 7-4 Site Definition Details***

| Site Definition | Example | Notes |
|---|---|---|
| Subnet (IP address prefix) | *Site Data-Center = subnet 172.20.0.0/16* | Preferred. Normally, subnets alone are sufficient to define a site. |
| Overlapping IP addresses (subnet from data source) | *Site NewYork = subnet 10.11.0.0/16* from *"NetFlow-NewYork"* data source.<br><br>*Site LosAngeles = subnet 10.11.0.0/16* from *"NetFlow-LosAngeles"* data source.<br><br>*Site Sale-Dept = subnet 10.11.0.0/16* from *"DATA PORT 1"* data source.<br><br>*Site Finance-Dept = subnet 10.11.0.0/16* from *"DATA PORT 1"* data source. | In certain scenarios when there are overlapping IP address spaces in the networks (for example, in private networks where hosts from different sites have the same IP addresses), then data sources can be used to differentiate the subnets. |
| WAE device serving the site | For WAAS traffic, you can define a site associated with a WAE device without specifying the site's subnets. Simply select all of the WAAS data sources coming from the WAE device(s) serving that site.<br><br>*Site SanJose = WAE-SJ-Client, WAE-SJ-CltWAN, and WAE-SJ-Passthrough data sources.* | We recommend that you use subnets to specify WAAS-optimized sites. Use this method only if the site's subnets cannot be determined.<br><br>If you are configuring a WAAS device, you will need to add WAAS servers to Packet Analyzer. See Auto Create of New WAAS Devices, page 7-29. |
| Multiple Rules | You can define a site using a combination of multiple rules described in this table. For example, if a site has both optimized and non-optimized traffic, it can be defined using a combination of WAAS data sources and a subnet from a NetFlow data source. | When defining a site using multiple data sources, be careful to make sure that those data sources do not have duplicated traffic to avoid double counting the site traffic statistics. |
| Unassigned site | The Unassigned site includes hosts that do not match any of your site configurations. Sites are classified at the time of packet processing. | Cannot be edited or deleted. |

### Resolving Ambiguity (Overlapping Site Definitions)

Conflicting rules are not allowed in site definitions. Of the following two scenarios, the second one is not allowed.

1.2.3.0/24 from DATASOURCE1 = SiteA

**1.2.3.0/24 from DATASOURCE1 = SiteB**

Using a prefix is the preferred method. Data source is secondary. In the following two scenarios, the first would receive the higher priority.

**1.2.3.0/24 = Site D**

WAE1-Client datasrc = Site E

The longest prefix has higher priority (same data source). In the following two scenarios, the first would receive the higher priority.

**1.2.3.0/24 from DATASOURCE1 = Site A**

1.2.0.0/16 from DATASOURCE1 = Site C

The more refined (specific) rule has higher priority. In the following two scenarios, the first would receive the higher priority.

**1.2.3.0/24 from DATASOURCE1 = Site A**

1.2.3.0/24 (any datasrc) = Site D

# Setting Interface Speed using NetFlow Interface Capacity

After you have set up NetFlow data sources (see Forwarding NetFlow Traffic, page 7-15), you can go to the NDE Interface Capacity window at **Setup > Network > NDE Interface Capacity** to specify the speed of each interface. This allows the software to calculate interface utilization on the NDE Interface Traffic Analysis window (**Analyze > Traffic > NDE Interface**). Otherwise, the Packet Analyzer software can only display the throughput of the interface, but cannot show its utilization.

The interface name and speed will be automatically discovered by the Packet Analyzer if you configure the device SNMP credentials in **Setup > > Create > Type: NETFLOW**.

To add a new or edit an existing interface, continue to Creating or Editing a NetFlow Interface, page 7-52.

## Creating or Editing a NetFlow Interface

To add a new interface if it has not been automatically discovered, at the NetFlow Data Export (NetFlow) Interface Capacity window (**Setup > Network > NDE Interface Capacity**), click **Add**. Then fill in the fields as described in Table D-23.

**Note** It is normally not necessary to manually create NetFlow interfaces. They should be discovered automatically when the device sends NetFlow packets to the Packet Analyzer.

To edit an existing interface, choose the device, then click **Edit**. Fill in the fields as described in Table D-23.

# Configuring DSCP Groups

Differentiated services monitoring (DiffServ) is designed to monitor the network traffic usage of Differentiated Services Code Point (DSCP) values. To monitor DSCP, you must configure at least one aggregation profile, and one aggregation groups associated with each profile. This section describes how to set up the DSCP groups.

You can define two or three different groups of traffic, and assign the various DSCP values to each group. Or you can assign one particular value for the first group and give it a name, and then assign all the rest to the other (or default) group and give that a name.

For detailed information about setting DSCP values, see *Implementing Quality of Service Policies with DSCP*:
http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

The following tasks help you set up and manage the DSCP groups:

- Creating a DSCP Group, page 7-53
- Editing a DSCP Group, page 7-53
- Deleting a DSCP Group, page 7-54

## Creating a DSCP Group

To create a DSCP Group:

**Step 1** Choose **Setup > Network > DSCP Groups**.

The DSCP Groups table displays.

**Step 2** Click **Create**.

The DSCP Group Configuration window displays.

**Step 3** Fill in the fields as described in Table D-24.

Table D-25 shows the available formats and associated values.

**Step 4** Click **Submit** to save your changes.

## Editing a DSCP Group

To edit a DSCP group:

**Step 1** Choose **Setup > Network > DSCP Groups**.

The DSCP groups window displays.

**Step 2** Select the profile to edit, then click **Edit**.

**Step 3** Make the necessary changes, then click **Submit** to save your changes, or click **Reset** to cancel.

### Deleting a DSCP Group

To delete a DSCP group, select the profile from the DSCP Groups table, then click **Delete**.

# Configuring Application Classification

Packet Analyzer provides two ways of enhancing how your traffic is displayed in the dashboard and reports. Packet Analyzer uses application classification to:

- Expand the number of application's for which Packet Analyzer can provide down to Layer 7 application details. See Adding More Detail into Dashboard and Application Reports.
- Create custom applications using a list of rules based on HTTP URL or Server /Port definition. This is referred to as the *classic* application classification model. See Creating Deeper Visibility Into Application Traffic, page 7-56.

You can use one or both of these methods to ensure Packet Analyzer provides the level of traffic detail you need.

## Adding More Detail into Dashboard and Application Reports

You can add more detail enable deep packet inspection to see Layer 7 application visibility by using application classification. To understand more about application classification and Layer 7 application visibility, see About Deeper Application Classification.

In order to enable application classification for deep packet inspection in Packet Analyzer:

**Step 1** Choose **Setup > Classification > Applications Settings**. Then select the Deep Packet Inspection check box in order to enable your Packet Analyzer dashboards to display key critical details, such as hostname and port, in your traffic captures and reports.

**Step 2** (Optional). Select **New** in the Protocol Pack pane to download the latest NBAR2 Protocol Pack (PP). The PP is a single compressed file that contains the rules used for classifying traffic when Deep Packet Inspection is enabled. Packet Analyzer stores the default plus one additional PP.

**Step 3** Enter the PP URL to download the PP files.

This URL supports ftp, http[s], scp, and sftp protocols. The User Name and Password fields are used only if the server requires authentication. Alternatively, the username and password can be specified directly within the following URL:

ftp://username:password@hostname/

You can also download the PP files under the **Cisco Security Packet Analyzer Software** product links at the CCO software download location at following URL:

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

**Timesaver** Use **Downloads Home >Products > Cloud and Systems Management > Cisco Security Packet Analyzer Products > Cisco Security Packet Analyzer Software** to locate the protocol pack.

**Step 4** To revert back to the default protocol when a previous protocol pack is no longer needed, choose **Restore Default**.

## About Deeper Application Classification

This release of Packet Analyzer supports a more comprehensive, or deep, application classification method. This method allows you to see more details in your monitoring dashboards and packet captures (including application names, interface details, and so on).

To expand the level of application information your Packet Analyzer can monitor and analyze, enable the deeper level of application classification and download application signature updates when you need them.

In addition to providing the application name, this method also brings attributes to simplify application management for both classification and reporting. Application categorization, for example, allows the grouping of similar applications.

When this method is enabled you can view extracted information from applications such as HTTP URL, HTTP User Agent, and SIP URL, for export or classification.

**Note** Depending on your installation or upgrade method you may need to enable deep packet inspection.

You can use protocol packs to add new and update existing application signatures. Packet Analyzer support of protocol packs allows you to see any new and updated application signatures in Packet Analyzer traffic monitoring. For more details on Protocols Packs, see About Protocol Packs and Application Classification, page 7-55.

You can also use the Packet Analyzer CLI to change the classification status to use the deeper application classification method and check which classification setting your Packet Analyzer is using.

For details about what application signatures are in specific protocol pack versions, see Network-Based Application Recognition Q&A on Cisco.com.

## About Protocol Packs and Application Classification

Packet Analyzer uses Cisco's Network-Based Application Recognition to recognize and classify a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/User Datagram Protocol (UDP) port assignments. The support of Protocol Packs (PP) allow you to update your application signatures so that dashboard and traffic data provide the most detailed information available. Packet Analyzer Protocol Packs can be found in the CCO software download location. These are the only protocol packs you should use with Packet Analyzer.

You do not need a license to download a protocol pack for Packet Analyzer. For this release, updating the protocol pack may cause a temporary interruption of operation for several seconds, similar to changing the system time.

To view the Packet Analyzer Protocol Pack version, choose **Setup > Classification > Applications Settings**.

To turn on deep application classification in Packet Analyzer, choose **Setup > Classification > Applications Settings** and select **Deep Packet Inspection**. For details, see Adding More Detail into Dashboard and Application Reports, page 7-54.

If you choose not to use the deep application classification method, Packet Analyzer defaults to a less comprehensive classification method that may not include all applications or protocols.

## About Packet Analyzer Classic Deep Packet Application Classification

This section covers how you can customize your Packet Analyzer to provide a deeper level of visibility into the application data presented in the dashboard and reports.

Packet Analyzer uses the application ID classification system. When defining applications, you can view and select from a list of protocols and port numbers, and candidate IP addresses and port numbers for the traffic being analyzed. You can also create URL-based application classifications. For an in depth overview of application types, see Understanding Application Traffic, page 7-58.

You can also configure custom applications using the Application Programming Interface (API), also referred to as the North Bound Interface (NBI). This is needed to ensure uniform application classification across a number of Packet Analyzer. See your customer service representative for details on how to get access to the NBI documentation.

To set up classifications use the following tasks:

- Creating Deeper Visibility Into Application Traffic, page 7-56
- Configuring Application Groups, page 7-60
- Filtering Encapsulations, page 7-61

# Creating Deeper Visibility Into Application Traffic

This section provides details into the application classification method known as Network Based Application Recognition (NBAR) classic.

You can use Packet Analyzer to monitor pre-determined or custom applications in your Data Center so that your traffic analysis is more focused and therefore optimal.

Without configuring application classification, applications running on a certain servers or specific ports are classified as *unknown*. This means that you may not have enough insight into the monitoring traffic. After configuring your application or ports, you can gain visibility into those application details on the monitoring screens. Similarly for the URL-based applications, instead of having all web traffic being grouped under the HTTP URL, you can specify a more granular layer of monitoring by using the application and port.

This section describes the following tasks:

- Creating Custom Applications, page 7-57
- Editing Custom Application Classifications, page 7-57
- Adding More Detail into Dashboard and Application Reports, page 7-54
- Deleting an Application Rule, page 7-58
- Understanding Application Traffic, page 7-58

To find out more about Layer 7 visibility and deep packet inspection, see Adding More Detail into Dashboard and Application Reports, page 7-54.

## Creating Custom Applications

You can create a custom applications using the list of rules based on HTTP URL, Protocol, or Server IP addresses. If you create a custom application, you can later edit it if you choose. Standard, pre-defined applications cannot be edited.

For details on application types or other options, see Understanding Application Traffic, page 7-58.

To create a new application classification:

**Step 1** Choose **Setup > Classification > Applications** and select **Create**..

For a description of the Applications window, see Table D-27.

**Step 2** Enter an application classification name.

**Step 3** (Optional) Enter an application description that gets displayed in the view table. There is a 75 character limit.

**Step 4** (Optional) You can skip the Selector value. This is an arbitrary number, unique within an engine-id. It will be automatically assigned if left blank.

**Step 5** Select the application classification rule type drop-down menu.

**a.** To choose a Server/Port application rule, select **Server/Port** in the Application Classification Rule drop-down menu.

Then select the definition drop-down menu to enter the following required information.

- To choose a Server, Protocol, and Port or Port Range, select the drop-down menu then enter the required information.
- To choose a protocol, select **Any**, **TCP**, **UDP**, or **Both TCP & UDP**.
- To choose a port or port range, enter the required information.

**b.** To choose the URL-based application rule, select **HTTP URL** in the Application Classification Rule drop-down menu then enter the required information. (See Understanding URL-Based Application Classification, page 7-59 for additional field details.)

**Tip** You can also add or remove multiple rule definitions to this application classification by clicking the gear icon and selecting **Insert new rule** or **Delete**.

**Step 6** Click **Submit** to create the new application classification signature.

You can now monitor the new applications using the Interactive Report filter with the application dashboards.

## Editing Custom Application Classifications

In Packet Analyzer you can only modify the custom, or user-defined, applications, and not the preconfigured system applications. You can only edit an application for which it states *Custom* in the Engine ID column.

To edit an application:

**Step 1** Choose **Setup** > **Classification** > **Applications**.

**Step 2** Select the application to edit, and click **Edit**.

The Application configuration window displays.

**Step 3** Make the desired changes.

**Step 4** Do one of the following:

- To accept the changes, click **Submit**.
- To leave the configuration unchanged, click **Cancel**.
- To delete the application rule, click **Delete**.

## Deleting an Application Rule

You may want to delete an application rule when you are no longer using it in your network.

To delete an application rule, simply select it from the Application list, then click **Delete**.

You cannot delete preconfigured system applications, only custom applications.

## Understanding Application Traffic

This section contains information on application types, rules, and other details you may find helpful.

There are two types of application classification rules:

1. *Server/Port* rules defines a a server IP address. For server-based application classification, Packet Analyzer analyzes traffic for the candidate IP addresses and port number or numbers you specify. You can also define port or protocol-based application (for example, based on a TCP port). You can create additional ports to enable Packet Analyzer to handle additional traffic for standard applications. Port ranges for IP are 1-255 for IP. TCP and UDP port ranges are1-65535.
2. *HTTP-based URL* rules define URL-based application extensions to the existing list of supported applications. When the URL in an HTTP request matches the criteria of a URL-based application, the traffic is classified as that protocol. The HTTP request is a URL on any port that is part of the iana-l4:http protocol, or protocol named http under the *iana-l4* engine ID.

**Tip** To create Protocol or Server IP Address applications, you can check the Application Configuration table in **Analyze > Traffic > Application**. To create an HTTP URL-based application, you can analyze the incoming URLs on **Analyze > Traffic > URL Hits**. NBAR is enabled through CLI and GUI.

Packet Analyzer recognizes an application based on either:

- An application which resides on a specific server IP address—You can filter using an IP address, a protocol, and a port or range of port numbers. After configuring the server information, the monitoring dashboard displays more detailed application information instead of just the *unknown* grouping.

- A set list of application IDs—The protocol, port number, or port number range, along with the focused inspection of traffic (for example, voice signaling traffic or FTP), heuristics (for example, DCE-RPC or SUN-RPC), or standardized application identifiers exported by Cisco platforms with NetFlow.

  If Packet Analyzer is not able to recognize an application using any of these mechanisms, the application type of the traffic is reported as ***unknown***. You can configure the application reported as unknown to create custom applications.

- A custom application based on a URL-based HTTP request—You can include URL Host, or URL Path and allows you to gain additional visibility instead of grouping all web traffic HTTP. For details, see Understanding URL-Based Application Classification, page 7-59.

To add custom applications and view or edit any user-defined applications, choose **Setup > Classification > Applications**.

**Caution** There is no limit on the number of URL-based applications that can be created. It is important to consider that these types of applications use large amounts of CPU bandwidth and may impact your performance if too many are defined.

Table D-26 describes the fields on the Applications view page.

## Understanding URL-Based Application Classification

URL-based applications are extensions to the list of applications. When the URL in an HTTP request (a URL on any port that is part of the iana-l4:http protocol, or protocol named *http* under the *iana-l4* engine ID) matches the criteria of a URL-based application, the traffic is classified as that protocol. The device interface statistics are collected by regularly (once a minute) polling the ifTable statistics of all interfaces on the managed device.

A URL-based application can be used the same way as any other application. For example, a URL-based application can be used in collections, captures, and reports.

An incoming URL is matched against the criteria of the configured URL-based applications in the order of the selector in ascending order. When a match is found, the remaining URL-based applications are not considered.

A URL consists of the following parts:

- a host (host.domain.com)
- a path (dir_secpa/dir_name)
- an argument/content type

**Tip** Content-type argument should rarely be used in combination with the other two fields. It can be used alone, for example to identify WAP traffic you could define an application with a content type of **wap.**. In almost all other cases, we recommend you use host and path only.

### Example—Creating an URL-Based Application

This example provides steps on how to create a URL to allow you to control the displayed traffic data. For example, the URL *www.cisco.com/go/secpa* are broken down when sent to the web server into two fields: a host field (*www.cisco.com*) and a path field (*/go/secpa*). By defining different values for the fields in the application, you can control the granularity of URLs that are classified as this new

application. If you want to group all traffic to *www.cisco.com* together and only define the host part, then use the host only part. If you have multiple hosts that map to the same end resource and only want to define the path part., then use only the path entry (*go/secpa*).

To collect traffic for a particular host and path for the URL **http://cisco.com/go/secpa** enter:

- the *host* part is **host.domain.com**, for example, **Cisco.com**
- the *path* part is **/go/secpa**
- the *argument* part is **null/empty**

In the configuration of an URL-based application, the path part and the argument path are combined and called the *path part*. For detailed descriptions, see Table D-31.

**Note** The host, path, and argument parts of a URL are matched against the corresponding POSIX regular expressions specified in the application definition. For details on regular expression syntax, refer to the IEEE Std.

# Configuring Application Groups

An application group is a set of applications that can be monitored as a whole. The following topics help you set up and manage the application group:

- Creating an Application Group, page 7-60
- Editing or Deleting an Application Group, page 7-60
- Deleting an Application Group, page 7-61

## Creating an Application Group

To create an application group:

**Step 1** Choose **Setup >Classification > Application Groups**.

The Application Groups window displays.

**Step 2** Click **Create** and enter the name in the Application Group Name field.

**Step 3** Use the next Application field and the **Filter** button to narrow the list of selectable applications. For example, if you enter *bittorrent*, all applications with that name appear in the list below.

**Step 4** Select an application and click **Add**. Applications appear in the Selected Applications box.

You can select multiple applications at once by using the Shift button, and then click **Add.**

**Step 5** Click **Submit** to save your changes.

## Editing or Deleting an Application Group

To edit or delete an application group:

**Step 1** Choose **Setup > Classification > Application Groups**.

**Step 2** Select the Application Group by clicking the radio button, then click **Edit** or **Delete**.

**Note** You can only delete one application group at a time.

### Deleting an Application Group

To delete an application group, simply select the application and then click the **Delete** button.

## Filtering Encapsulations

Using encapsulation gives you increased flexibility when trying to view different types of application traffic (such as counting or grouping). The encapsulation settings affect how traffic of certain IP-based tunneling protocols are treated.

You can use this software to set up the way you want to view different types of encapsulations in network traffic for the following protocols:

- CAPWAP Data—Control And Provisioning of Wireless Access Points
- ERSPAN—Encapsulated Remote Switched Port Analyzer
- FabricPath
- GRE—IP over GRE tunneling (Generic Routing Encapsulation)
- GTP—GPRS (General Packet Radio Service) Tunneling Protocol
- IP.IP4—IP4 over IP4/IP6
- IP.IP6—IP6 over IP6
- IPESP—IP with Encapsulating Security Payload
- L2TP Data—Layer 2 Tunneling Protocol
- LISP Data—Locator/ID Separation Protocol
- LWAP Data—Lightweight Access Point Protocol
- MPLS—Multiprotocol Label Switching
- OTV—Overlay Transport Virtualization
- PPPoE—Point to Point Protocol over Ethernet
- Segment ID—Rule to match one or more fields with a regular expression.
- SGT—Security Group Tag
- VNTAG—Virtual Network Tag
- VxLAN—Virtual Extensible LAN

To filter encapsulations:

**Step 1** Select **Analyze > Traffic > Encapsulation**.

**Step 2** From the Interactive Report pane, click **Filter** to display the filter options,

**Step 3** Use the available options to select filtering for the encapsulation traffic reports. Unavailable options will be grayed out.

**Step 4** Enter whether you want to include filtering on the site and specify the data source.

**Step 5** Select encapsulation options to filter on including the time range.

**Step 6** If you add a filter name, the filter is saved below the Interactive Report pane for reuse.

**Step 7** Click **Submit** to run the filter and update the Encapsulation Traffic graphs and Top N dashboards based on your filter settings.

If you want to revert to the previous settings since your last submission, click **Reset**.

# Setting Up Packet Analyzer Monitoring

This section discusses how to set up monitoring over and above the default monitoring parameters. You can customize these monitoring parameters.

To set up Packet Analyzer monitoring perform these tasks:


- Setting Aggregation Intervals, page 7-62
- Configuring Response Time, page 7-63
- Setting Up Media Monitoring, page 7-64
- Creating RTP Filters, page 7-65
- Configuring URL Collections, page 7-65
- Configuring WAAS Monitored Servers, page 7-67


## Setting Aggregation Intervals

Packet Analyzer has short-term and long-term aggregation intervals . Aggregated data is displayed in the dashboards if the query is longer than one day.

The purpose of gathering short term aggregation interval data is for troubleshooting. It has a finer granularity than long term data (by default, the short term aggregation interval for Traffic/Media is one minute, and short term response time interval is five minutes).

The purpose of gathering long term interval data is for trending analysis. The smallest aggregation interval for long term data is one hour (60 minutes).

**Caution** If you modify the aggregation intervals, existing collected data that is not in the same aggregation interval will be completely removed. Data will then start being collected from the beginning again at the moment the intervals are modified and applied.

Traffic and Media refer to applications, hosts, RTP streams, and voice calls monitoring. Response Time refers only to application response time. Packet Analyzer does not support long term aggregations of data for the following media: conversations, RTP streams, and voice signaling calls monitoring.

To set up aggregation intervals:

**Step 1** Choose **Setup > Monitoring > Aggregation Intervals**.

**Step 2** Choose the desired durations for Short Term Interval and Long Term Interval.

**Step 3** Check the **Collect only hosts from user-defined sites (exclude hosts from Unassigned site)** check box if you want the Packet Analyzer long term data to contain information only for hosts classified to the user-defined sites. This check box only applies to the long term data; short term always collects all hosts.

**Note** Enabling the "Collect only hosts from user-define sites" option can significantly speed up report queries, because it excludes unclassified hosts' statistics from the database.

When you first start the Packet Analyzer, in monitoring windows that show site information, you will see a site named "Unassigned" and with a description of "Unclassified Hosts." The Unassigned site includes any that do not match the site configurations. By default, long-term storage will include data for all sites, including the Unassigned site. In some cases, you may not want to view long term data of hosts that are not in your network, in which case you would check the check box.

**Step 4** Click **Submit**.

The aggregation intervals determine how much data can be stored in the Packet Analyzer database. See Table 7-5 for information about short and long-term data retention. This calculation is based on a worst case scenario where tables are full or almost full. It is based on recommended database sizes.

***Table 7-5 Data Retention***

| | Short-Term Aggregated Data (Normal) | Short-Term Aggregated Data (Minimum) | Long-Term Aggregated Data (Normal)[1] | Long-Term Aggregated Data (Minimum) |
|---|---|---|---|---|
| All supported platforms | 72 hours | 14 hours | 100 days (with default polling interval) | 30 days (with default polling interval) |

1. Can depend on how the user configures the LT polling interval. The more frequent polling, the shorter the duration.

# Configuring Response Time

To configure the timing parameters for response time data collections:

**Step 1** Choose **Setup > Monitoring > Response Time**.

The Response Time Configuration page displays. The settings you make on this window comprise the time distribution in microseconds for the detailed Response Time data collection.

**Step 2** Check the **Enable Response Time Monitor** check box.

**Step 3** After Monitored Server Filter, you will see **Disabled** or **Enabled**. If a WAAS server has been configured under **Setup > Monitoring > WAAS Servers**, you will see **Enabled**. Click **Configure Filter** to configure a filter if you need to enable your monitor server filter.

**Step 4** Enter the Response Time values as described in Table D-30.

**Step 5** Accept the default settings or change the settings to the values you want to monitor. Click **Submit** to save your changes.

# Setting Up Media Monitoring

This section covers the following topics:

- Setting up Voice Monitoring
- Setting up Video Monitoring

## Setting up Voice Monitoring

You can use the Mean Opinion Score (MOS) to quantify the perceived level of quality you are receiving in your network voice traffic. This allows you to assess the work of codes, or algorithms, which compress audio traffic to save on bandwidth utilization but may result in a drop in quality.

After you set up the software to monitor voice data, you will be able to view the collected voice data under **Analyze > Media**. For more information on viewing the voice data, see Analyzing Media, page 3-32.

**Note** Voice monitoring features are supported with Cisco IP telephony devices only.

To set up voice monitoring:

**Step 1** Choose **Setup > Monitoring > Media**.

The Media Monitoring page displays.

**Step 2** Check the **Enable Call Signal Monitoring** check box.

**Step 3** Accept the default MOS Score value range or modify the values as you prefer. See Table D-30.

**Note** To report jitter and packet loss for the SCCP protocol, you must enable CDR on Cisco Unified Communications Manager. For more information on Cisco Unified Communications Manager, see the Cisco Unified Communications Manager documentation. http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

**Step 4** Click **Submit** to save your changes, or click **Reset** to cancel and revert to the previous settings.

## Setting up Video Monitoring

You can use the Media Delivery Index (MDI) to quantify the perceived level of quality you are receiving in your network video traffic. This allows you to assess the work of codecs, or algorithms, which compresses audio traffic to save bandwidth utilization but may result in a drop in quality. After you set up the software to monitor video conversation data, you will be able to view the collected video stream data under **Analyze > Media**.

To set up video monitoring:

**Step 1** Choose **Setup** > **Monitoring > Media**.

The Media Monitoring page displays.

**Step 2** Check the **Enable Video Signal Monitoring** check box.

**Step 3** Accept the default MDI quality range or modify the values as you prefer. See Table D-30.

**Step 4** Accept the default codec streams quality range or modify the values as you prefer.

**Step 5** Click **Submit** to save your changes, or click **Reset** to cancel and revert to the previous settings.

**Note** You can enable the video signaling monitoring only when voice signaling monitoring is enabled, and when you disable voice signaling monitoring, video signaling monitoring also gets disabled.

# Creating RTP Filters

When the software is initially started, RTP stream traffic will automatically start being monitored. Packet Analyzer enables you to monitor all RTP stream traffic among all SPAN traffic, without having to know the signaling traffic used in negotiating the RTP channels. RTP Stream Monitoring is enabled by default under **Setup > Monitoring > RTP Filter**. To disable it, uncheck the **Enable RTP Stream Monitoring** check box and click **Submit** to apply the change.

To create an RTP filter:

**Step 1** Choose **Setup** > **Monitoring > RTP Filter**.

**Step 2** Click **Create**.

**Step 3** From the drop-down menu, choose the protocol (IP or IPv6).

**Step 4** Enter the Source Address, Source Mask, Destination Address, and Destination Mask.

**Step 5** Click **OK**.

# Configuring URL Collections

The URL collection listens to traffic on TCP port 80 of a selected data source and collects URLs. Any protocol which has its master port set to TCP port 80 can be used for URL collections. URL collection can be enabled on multiple data sources such as Data Port(s), CEF Data Port(s) and ERSPAN.

A URL, for example: ***http://host.domain.com/intro\?id=123***, consists of a host part (**host.domain.com**), a path part (**intro**), and an arguments part (**?id=123**).

**Note** Since the argument is matched against a regular expression, a literal *?id=123* is not a valid regular expression. The ? needs to be escaped with a backslash character, \ , so the actual regular expression needed is *\?id=123*.

The collection can be configured to collect all parts or it can configured to collect only some of the parts and ignore others.

This section contains the following procedures:

- Enabling a URL Collection
- Changing a URL Collection
- Disabling a URL Collection

## Enabling a URL Collection

To enable a URL collection:

**Step 1** Choose **Setup > Monitoring > URL.**

**Step 2** Provide the information described in Table D-31.

You can enter a partial name of a data source and click **Filter** to find data sources that match. Choose **Clear** to return to the entire list of data sources.

**Note** Depending on which radio button option is collected, the format of the URL varies. For example, the leading *http:* part is only present if the *host* part is collected. Keep this variable in mind, when configuring a *match only* expression.

**Step 3** Check the **Recycle Entries** check box to recycle entries.

**Step 4** Select the check box for one of the following:

- Collect complete URL (Host, Path and Arguments)—You might use this if you are a network security engineer and suspect a virus infection may be caused by a website. This information could be used to identify which web page has the virus embedded and how it may have spread. It can also be shared for further analysis to help create a solution to stop the spread.
- Collect Host only (ignore Path and Arguments)—You might use this if your network administrator changed your firewall policies to block certain hosts.
- Collect Host and Path (ignore Arguments)
- Collect Path and Arguments (ignore Host)
- Collect Path only (ignore Host and Arguments)

**Step 5** Click **Submit** to save your changes, or click **Reset** to cancel.

## Changing a URL Collection

To change a URL collection:

**Step 1** Choose **Setup > Monitoring > URL**.

**Step 2** Change the URL Collection Configuration field information as described in Table D-31.

**Note** Changing any parameters and applying the changes flushes the collected URLs and restarts the collection process.

**Step 3** Click **Submit** to save your changes, or click **Reset** to cancel.

## Disabling a URL Collection

When you disable URL collection monitoring, all collection stops immediately and any collection that was in progress is deleted.

To disable a URL collection:

**Step 1** Choose **Setup > Monitoring > URL**.

**Step 2** Uncheck the **Enable** check box.

**Step 3** Click **Submit**.

# Configuring WAAS Monitored Servers

WAAS monitored servers specify the servers from which WAAS devices export traffic flow data to the Packet Analyzer monitors. To enable WAAS monitoring, you must list the servers to be monitored by Packet Analyzer using the WAAS device's flow monitoring.

You must configure WAAS monitored servers to enable Packet Analyzer to monitor WAAS traffic. Packet Analyzer displays status of WAAS devices as *pending* until you set up WAAS monitored servers.

To configure a WAAS monitored server:

**Step 1** Choose **Setup > Monitoring > WAAS Servers**. The WAAS Servers page displays.

**Step 1** Check the **Filter Response Time for all Data Sources by Monitored Servers** check box if you want Packet Analyzer to compute response time data only for the servers from this list for all data sources, including non-WAAS data sources. All other servers will be ignored in response time monitoring views. This enables you to reduce Packet Analyzer workload and to improve its overall performance.

**Step 2** Click **Add** and enter the server IP address in the Server Address field. You can paste multiple IP addresses here as well.

**Tip** Specify the WAAS monitored servers from which WAAS devices export traffic flow data to the Packet Analyzer monitors. Do ***not*** use the WAE device IP address.

**Step 3** Click **Submit**.