Understanding Packet Analyzer Traffic Sources

Before you can monitor data using Packet Analyzer software, you must direct specific traffic flowing through a switch or router to the **Packet Analyzer**. This appendix explains the various data sources that you can configure for **Packet Analyzer**.

This appendix contains the following topics:

Data Source Overview

Packet Analyzer uses various data sources to deliver its performance troubleshooting functionality:

To understand which methods to use to direct specific traffic to the **Packet Analyzer** software, see Table A-1.

Table A-1 Methods of Directing Traffic

Method	Usage Notes
Switch SPAN[1]	You can direct a set of physical ports, a set of VLANs, or a set of EtherChannels to the Packet Analyzer. Selecting an EtherChannel as a SPAN source is the same as selecting all physical ports comprising the EtherChannel as the SPAN source. On some Packet Analyzer platforms, using SPAN allows for Packet Analyzer configuration without having to use the switch.Forwarding SPAN Traffic, page 7-6.
Switch Remote SPAN (RSPAN)[1]	You can monitor packet streams from remote switches, assuming that all traffic from a remote switch arrives at the local switch on a designated RSPAN VLAN. Use the RSPAN VLAN as the SPAN source for the Packet Analyzer.

Table A-1 Methods of Directing Traffic (continued)

Method	Usage Notes
Encapsulated Remote Switched Port Analyzer (ERSPAN)[1]	You can monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports using ERSPAN. ERSPAN sends traffic to a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. ERSPAN supports source ports, source VLANs, and destination ports on different routers or switches, which provides remote monitoring of multiple routers or switches across your network. See Forwarding ERSPAN Traffic, page 7-6.
NetFlow Data Export (NDE)	Packet Analyzer analyzes NetFlow from Managed Devices (Routers/Switches) You can monitor NetFlow records directly from remote switches or routers. You must configure the NetFlow packet source to the Packet Analyzer from a local switch or remote router using the device CLI. For received NetFlow traffic, a default site will be created including all interfaces from that device. See Configuring Sites, page 7-49. SPAN and NetFlow sources can be in effect simultaneously. See Forwarding NetFlow Traffic, page 7-15.
WAAS	You can access Packet Analyzer 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. See Configuring WAAS Monitored Servers, page 7-67.
SNMP	Used as a southbound interface for configuration and data retrieval from switches and routers. Packet Analyzer uses web services as the northbound interface for data objects. The software continues to support baseline manageability features of SNMP such as MIB-2 and IF-TABLE for the Packet Analyzer, and the health status and interface statistics that can be used by external products like Fault and Configuration Management offerings (for example, CiscoWorks LMS and Prime Infrastructure).
Network Tap Device	Applies to Packet Analyzer appliances only. For details, see your appliance installation guide.
CEF	You can enable CEF traffic monitoring on one or more ports and send the monitored CEF traffic to an UCSE Packet Analyzer. See Understanding How the Packet Analyzer Uses VACLs in Catalyst Switch, page A-4

1.Packet Analyzer can analyze Ethernet VLAN traffic from the following sources: Ethernet, Fast Ethernet, Gigabit Ethernet, trunk port, or Fast EtherChannel SPAN, RSPAN, or ERSPAN source port.

The Data Sources page (**Setup > Traffic > Packet Analyzer Data Sources**) lists the data sources configured for your Packet Analyzer. Table D-2 describes the fields in the Packet Analyzer Data Sources window.

Table A-2 summarizes the traffic sources that are used for Packet Analyzer monitoring.

Table A-2 Summary of Traffic Sources for Packet Analyzer Monitoring

Traffic Source	LAN		WAN	
	Ports	VLANs	Ports	VLANs
VACL capture	Yes	Yes	Yes	N/A
NetFlow Data Export NDE (local)	Yes	Yes	Yes	Yes
NetFlow Data Export NDE (remote)	Yes	Yes	Yes	Yes
SPAN	Yes	Yes	No	No
ERSPAN	Yes	Yes	No	No

Ports and Hardware Details

Cisco Security Packet Analyzer has four dataports. Each dataport can accept one SPAN session. Depending on the managed device operating system (OS) version, the number of SPAN sessions allowed may vary. Most IOS versions support two SPAN sessions. Nexus OS may support more than two SPAN sessions.

Depending on the IOS running on the Supervisor, port names are displayed differently. Newer versions of IOS software display a port name as Gi2/1 to represent a Gigabit port on module 2 port 1. In the VSS, a port name might be displayed as Gi1/2/1 to represent a Gigabit port on switch 1, module2, port 1.

Some Cisco switches do not support SNMP MIB objects that are required by Packet Analyzer when configuring SPAN sessions. On these switches, you can use the switch device CLI command to configure the SPAN session for Packet Analyzer. Alternatively, for the Packet Analyzer only, if the Packet Analyzer managed device supports NetConf interface over SSH, you can configure the Packet Analyzer to use NetConf to configure SPAN sessions on the managed device.

Understanding How the Packet Analyzer Uses SPAN

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. You can configure up to two SPAN sessions in a Catalyst 6500 chassis. Newer Cisco IOS images may support more than two SPAN sessions. Consult the Cisco IOS document for the number of SPAN sessions supported per switch or router.

Table A-3 describes the types of SPAN sources and the possible ways to configure them.

Table A-3 SPAN Sources

SPAN Source	Configured with one of the following:
Any set of physical ports	• **Packet Analyzer** (the GUI) • Switch CLI
Any EtherChannel	• **Packet Analyzer** (the GUI) • Switch CLI
Any set of VLANs configured on the local switch	• **Packet Analyzer** (the GUI) • Switch CLI

See Table D-3 for a description of the fields on the SPAN Sessions window.

Table A-4 lists the possible SPAN states. The SPAN state displays in parenthesis in the Source - Direction column.

Table A-4 Possible SPAN States

State	Description
Active	SPAN source is valid and packet traffic from the source is copied to the SPAN destination (Packet Analyzer Dataport).
Inactive	Packet traffic from the source is not copied to the SPAN destination (Packet Analyzer Dataport).
Up	Supervisor displays this when packets are forwarded to the Packet Analyzer.
Down	Supervisor displays this when packets are not forwarding to the Packet Analyzer.

Note Due to potentially very high volume of ERSPAN traffic from the source, we recommend that you do not terminate the ERSPAN session on the Packet Analyzer management port. Instead, you should terminate ERSPAN on the switch, and use the switch's SPAN feature to SPAN the traffic to Packet Analyzer dataports.

Understanding How the Packet Analyzer Uses VACLs in Catalyst Switch

A VLAN access control list can forward traffic from either a WAN interface or VLANs to a dataport on the Packet Analyzer. 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.

There are two types of VACLs: one that captures all bridged or routed VLAN packets and another that captures a selected subset of all bridged or routed VLAN packets. Catalyst operating system VACLs can only be used to capture VLAN packets because they are initially routed or bridged into the VLAN on the switch.

A VACL can provide access control for all packets that are bridged within a VLAN or that are routed into or out of a VLAN or, with Release 12.1(13)E or later releases, a WAN interface. Unlike regular Cisco IOS standard or extended ACLs that are configured on router interfaces only and are applied on routed packets only, the VACLs apply to all packets and can be applied to any VLAN or WAN interface. The VACLs are processed in the hardware.

A VACL uses Cisco IOS access control lists (ACLs). A VACL ignores any Cisco IOS ACL fields that are not supported in the hardware. Standard and extended Cisco IOS ACLs are used to classify packets. Classified packets can be subject to a number of features, such as access control (security), encryption, and policy-based routing. Standard and extended Cisco IOS ACLs are only configured on router interfaces and applied on routed packets.

After a VACL is configured on a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VACL. Packets can either enter the VLAN through a switch port or through a router port after being routed. Unlike Cisco IOS ACLs, the VACLs are not defined by direction (input or output).

A VACL contains an ordered list of access control entries (ACEs). Each ACE contains a number of fields that are matched against the contents of a packet. Each field can have an associated bit mask to indicate which bits are relevant. Each ACE is associated with an action that describes what the system should do with the packet when a match occurs. The action is feature dependent. Catalyst 6500 series switches and Cisco 7600 series routers support three types of ACEs in the hardware: IP, IPX, and MAC-Layer traffic. The VACLs that are applied to WAN interfaces support only IP traffic.

When you configure a VACL and apply it to a VLAN, all packets entering the VLAN are checked against this VACL. If you apply a VACL to the VLAN and an ACL to a routed interface in the VLAN, a packet coming into the VLAN is first checked against the VACL and, if permitted, is then checked against the input ACL before it is handled by the routed interface. When the packet is routed to another VLAN, it is first checked against the output ACL applied to the routed interface and, if permitted, the VACL configured for the destination VLAN is applied. If a VACL is configured for a packet type and a packet of that type does not match the VACL, the default action is deny.

When configuring VACLs, note the following:

- VACLs and context-based access control (CBAC) cannot be configured on the same interface.
- TCP Intercepts and Reflexive ACLs take precedence over a VACL action on the same interface.
- Internet Group Management Protocol (IGMP) packets are not checked against VACLs.

Note You cannot set up VACL using the Packet Analyzer interface.

For details on how to configure a VACL with Cisco IOS software, see Cisco.com.

For details on how to configure a VACL on a WAN interface and on a LAN VLAN, see Forwarding VACL Traffic, page 7-14.

Understanding How the Packet Analyzer Uses NetFlow

The Packet Analyzer uses NetFlow as a format for the ongoing streaming of aggregated data, based on the configured set of descriptors or queries of the data attributes in Packet Analyzer. NetFlow Data Export (NetFlow) is a remote device that allows you to monitor port traffic on the Packet Analyzer; the Packet Analyzer can collect NetFlow from local or remote switches or routers for traffic analysis.

To use an NetFlow data source for the Packet Analyzer, you must configure the remote device to export the NetFlow packets. The default UDP port is 3000, but you can configure it from the Packet Analyzer CLI as follows:

```
root@nam3-61.cisco.com# netflow input port ?
<port>                    - input NetFlow port number
```

The distinguishing feature of the NetFlow v9 format, which is the basis for an IETF standard, is that it is template-based. Templates provide an extensible design to the record format, a feature that must allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format.

For more detailed information about Packet Analyzer and NetFlow, see Forwarding NetFlow Traffic, page 7-15.

For specific information about creating and managing NetFlow queries, see the *Cisco Security Packet Analyzer API Programmer's Guide* (contact your Cisco account representative if you need to refer to this document).

Understanding NetFlow Interfaces

To use a device as an NetFlow packet data source for the **Packet Analyzer**, you must configure the device itself to export NetFlow packets to UDP port 3000 on the Packet Analyzer. You might need to configure the device itself on a per-interface basis. A NetFlow packet device is identified by its IP address. In the Packet Analyzer, the default UDP port of 3000 can be changed with a **Packet Analyzer** CLI command (see Configuring NetFlow on Devices, page 7-16).

You can define additional NetFlow packet devices by specifying the IP addresses and (optionally) the community strings. Community strings are used to upload convenient text strings for interfaces on the managed devices that are monitored in NetFlow records.

Remote NetFlow packet devices may export information pertaining to any or all of their individual interfaces. The **Packet Analyzer** keeps track of the interface associated with any flow information received from the device. On the NDE Interface Analysis page (**Analyze > Traffic > NDE Interface**), you can view information for any selected interface on the device. This page will display the interface utilization or throughput over time, as well as show the top Applications, Hosts, and DSCP groups in both the input and output directions for the interface.

Understanding NetFlow Flow Records

A NetFlow packet contains multiple flow records. Each flow record has two fields:

- Input SNMP ifIndex
- Output SNMP ifIndex

Note This information might not be available because of NetFlow feature incompatibility with your Cisco IOS version, or because of a NetFlow flow-mask configuration.

In most cases, turning on NetFlow on an interface populates the NetFlow cache in the device with flows that are in the *input* direction of the interface. As a result, the input SNMP ifIndex field in the flow record has the ifIndex of the interface on which NetFlow was turned on. Sample NetFlow Network, Figure A-1, shows a sample network configuration with a NetFlow router.

Figure A-1 Sample NetFlow Network

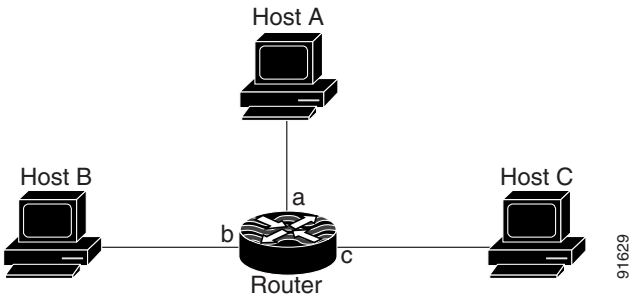

Table A-5 lists the reported flows if NetFlow is enabled on interface a.

Table A-5 Reporting Flow Records

Input Interface	Output Interface	Are Flows Reported?
a	b	Yes
a	c	Yes
b	c	No
b	a	No
c	a	No
c	b	No

Managing NetFlow Data Sources

A data source entry must exist on **Packet Analyzer** in order for it to accept NetFlow records from an external device. Data source entries may be created manually using the **Packet Analyzer** web GUI or the CLI. When manually creating a data source, you may specify any name you want for the data source.

For convenience, manual creation of NetFlow data sources is not necessary. There is an “autocreate” feature which is enabled by default. With the autocreate feature, a new data source will automatically be created for each device which sends NetFlow packet traffic to the Packet Analyzer when the first packet is received.

Autocreated NetFlow data sources will be assigned a name in the format *NetFlow-<IP Address>-ID-<Integer>*, where *<IP Address>* is the IP address of the exporting device, and *<Integer>* is the Engine-ID that the device populates in the packets (part of the NetFlow Data Export standard). An example might be “NetFlow-10.10.0.1-ID-12” for device 10.10.0.1 sending NetFlow packets with the Engine ID field set to 12. You can edit these autocreated data sources and change the name if you want to, as well as optionally specifying SNMP credentials for the device, as described later in this guide.

Understanding How the Packet Analyzer Uses 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 intercepts and redirects 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 and other metrics calculations and enters the data into reports you set up.

The WAEs examine the traffic and using 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 Central Manager GUI to centrally configure and monitor the WAEs and application policies in your network. You can also use the WAAS Central Manager GUI to create new application policies so that the WAAS system will optimize custom applications and less common applications. Packet Analyzer is accessible from within the Central Manager interface. The Cisco 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. See Using the WAAS Central Manager, page 7-25.

For more information about WAAS data sources and managing WAAS devices, see Understanding WAAS, page 7-23.

Understanding How the Packet Analyzer uses CEF

Packet Analyzer uses CEF to monitor all IP traffic on a router interface. For Cisco 2900 Series or Cisco 3900 Series Integrated Services Router Generation 2 (Cisco ISR G2) support Packet Analyzer, you can configure to monitor CEF traffic on many data ports to copy and forward all IP traffic to Packet Analyzer monitoring interface on a Cisco ISR G2.

The Cisco Unified Computing Server type E (Cisco UCSE) can host Packet Analyzer and other services. See UCSE product introduction for more details:

http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-e-series-servers/index.html

For the list of router platforms and IOS releases support UCSE, see section “Verifying Compatibility” in *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine.*

Understanding UCSE Physical Interfaces

Internal PCIE/MGF ports are named as GE0/GE1 and the front panel ports are named as GE2/GE3.

In CIMC GUI, PCIE/MGF ports are named as GE1/GE2 and front panel ports are named as GE3/GE4.