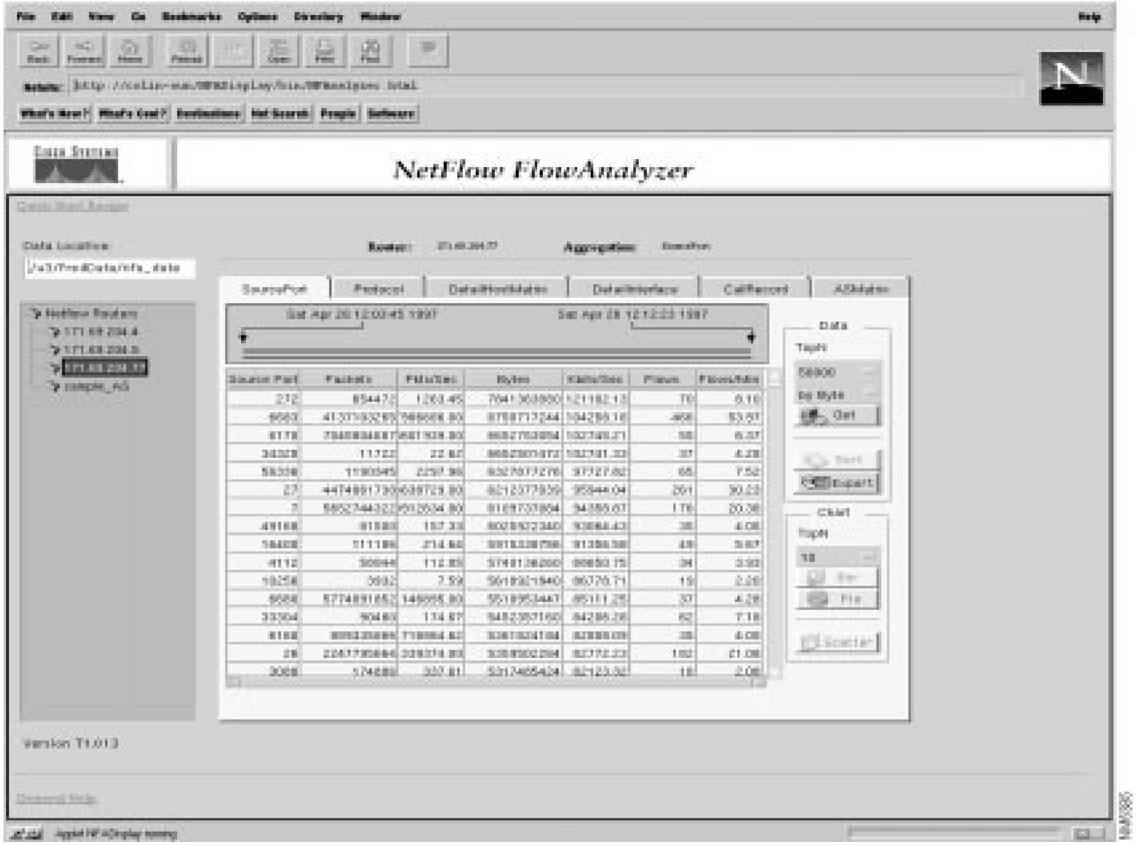
Using the NetFlow FlowAnalyzer Display

This chapter provides information about using the NetFlow FlowAnalyzer to view collected data. The FlowAnalyzer enables you to display detailed traffic statistics from selected routers.

Displaying Collected Data

The FlowAnalyzer displays summarized data from the NetFlow FlowCollector (see Figure 3-1). You can view the summarized data by choosing from a variety of formats and displaying the data in graphs or charts.

Figure 3-1 FlowAnalyzer Display User Interface



Data Location: /u3/FredData/nfs_data

Sat Apr 26 12:03:45 1997 — Sat Apr 26 12:12:23 1997

Source Port	Packets	Pkts/Sec	Bytes	Kbits/Sec	Flows	Flows/Min
272	854472	1263.45	7041363800	121182.13	70	8.16
6663	4137193265	588688.80	8758717244	104259.18	466	53.57
8178	7945834487	681928.80	8652753854	102745.21	58	6.57
38328	11722	22.82	8662301972	102781.33	37	4.28
58336	1190345	2297.96	8327077276	97727.82	65	7.52
27	4474891730	639729.80	8212377939	95944.04	261	30.23
7	5852744322	512634.80	8109737864	94355.67	176	20.36
49168	81580	157.33	8025502340	93684.43	36	4.08
16408	111186	214.60	5915328756	91356.58	49	5.67
4112	50044	112.85	5749138200	86850.75	34	3.92
10258	3932	7.59	5618921840	86776.71	19	2.20
6666	5774891652	148666.80	5518953447	85111.26	37	4.28
33304	90461	174.67	5482357160	84285.28	62	7.18
6168	8093258664	718684.82	5361924184	82885.09	35	4.05
26	2267795664	328374.80	5358502284	82772.22	182	21.06
3068	174686	337.81	5317485424	82123.32	18	2.08

On the left side of the FlowAnalyzer display, the Data Location field shows a path name for collection files. This is the path name that you specified in the HTML file when you installed the FlowAnalyzer. If you have more than one collector running, you can enter a new path name used by a different collector process.

Below the Data Location field is a list of NetFlow routers, each one identified by either its IP address or its textual alias. Router aliases are defined in the file

```
/opt/CSCOnfa/NFAServer/imported_files/Router_aliases.txt
```

For more information about router aliases, refer to the chapter entitled “Installing and Setting Up the NetFlow FlowAnalyzer.”

You can display collected data for a router in a variety of formats, including graphs and charts. From the Data area, click on the **Get**, **Sort**, or **Export** button to retrieve data. From the Chart area, click on the **Bar**, **Pie**, or **Scatter** button to display the data.

Get Data

To retrieve collected data perform the following steps:

Step 1 In the Data Location field, enter the data path that contains the collected data you would like to analyze. Press **Return**.

Step 2 Select a router from the NetFlow Routers tree structure (located below the Data Location field). The display shows the aggregation schemes available for the selected router.

Step 3 Select an aggregation scheme by clicking its corresponding tab.

Step 4 Select a specific period of time to display by moving the Start time arrowhead (left arrowhead) and the Stop time arrowhead (right arrowhead).

Step 5 Select from the Data area the number of data entries you would like to display by clicking on the Top N choice box. (The default value is 100.)

Step 6 Select how the data is sorted using the **by Byte** choice box. You can also sort **by Packet** or **by Flows**. (The default is **by Byte**.)

Step 7 Click the **Get** button to retrieve the collected data. The data is displayed in tabular format. You can sort this data and then display it as a graph or chart, or export the data to a file.

Sort Data

To sort the collected data, perform either one of the following options:

Option 1: Click the heading for the data column that you would like to sort, then click the **Sort** button.

Option 2: Double-click on the data column heading that you would like to sort.

Nonnumeric data is sorted in ascending order (alphabetically), and numeric data is sorted in descending order.

Export Data

To export collected data to a spreadsheet file, perform the following steps:

Step 1 Click the **Export** button to save the collected data to a spreadsheet file.

Step 2 Enter the filename and click the **OK** button to begin exporting the data.

The filename used is the first nonspaced word entered. For example, if you enter the filename "my new data" the spreadsheet file name used is "my.CSV," ignoring any characters after the first space.

The files exported from the AnalyzerDisplay are located in the `/opt/CSCOnfa/NFAServer/exported_files` directory, where the DisplayServer is running. The following output shows a typical directory location for exported files:

```
/opt/CSCOnfa/NFAServer/exported_files or
{DisplayServerBaseDir}/exported_files
```

Graphing Collected Data

Graph the collected data as a bar chart, bar graph, pie chart, or scatter graph.

Bar Graph

To display a bar graph for the collected data, perform the following steps:

Step 1 Click the heading for the data column that you would like to display.

Step 2 Select from the Chart Area the TopN data entries to be graphed.

Step 3 Click the **Bar** button to display the TopN data entries in a summary graph.

Pie Chart

To display a pie chart for the collected data, perform the following steps:

Step 1 Click the heading for the data column that you would like to display.

Step 2 Select from the Chart Area the Top N data entries to be graphed.

Step 3 Click the **Pie** button to display the TopN data entries in a pie chart.

Scatter Graph

To display a scatter graph for the collected data, perform the following steps:

Option 1: Select a row then select the data column to identify the specific data cell that you would like to graph, then click the **Scatter** button to display that specific data cell in a scatter graph.

Option 2: Double-click on the specific data cell that you would like to display in a scatter graph.

Aggregation Schemes

The aggregated data for a selected router is organized into tables that have many columns, and those tables are labelled with tabs. Table 3-1 lists the names of the tables and briefly summarizes each table's contents.

- Each table is made up of seven or more columns. The six columns on the right side of the table are the same for every table except CallRecord. They display statistics (packet, packet/second, byte, kilobits/second, flows, and flows/minute).
- One column (or more) on the left side of each table identifies the subset of network traffic to which those counters and rates apply.

Table 3-1 Aggregation Schemes

Table Name	Key (Heading)	Description
Source Node	Source	The IP address of the host from which the measured traffic originates.
DestNode	Destination	The IP address of the host to which the measured traffic is delivered.
HostMatrix	Source Destination	The combination of a particular source node and destination node pairs. The IP addresses at each end of the measured traffic.
Protocol	Protocol	The network protocol used for the traffic that is measured by the counters and rates displayed in the other six columns of the table. The collector identifies these flows using assigned Internet protocol numbers and well known ports.
DetailDestNode	Destination SrcPort DestPort Protocol	The IP address of the Destination host, the port numbers at the two endpoints (SrcPort and DestPort), and the Protocol used.
DetailHostMatrix	Source Destination SrcPort DestPort Protocol	The combination of particular source node and destination node pairs. Source host and Destination host IP addresses, the port numbers at both endpoints (SrcPort and DestPort), and the protocol used.
DetailInterface	Source Destination Input Output Next Hop	The combination of specific source node and destination node. Source host and destination host IP addresses, Input interface and Output interface information for the end point (either the ifIndex value or MIB description), and the IP address of the Next Hop router.
Source Port	SrcPort	The port on the source host from which the measured traffic originates.
DestPort	DestPort	The port on the destination host to which the measured traffic is delivered.
CallRecord	Source Destination	The source and destination IP addresses, the duration of call activity, and counts of records, packets, bytes, and flows. The six standard statistical columns are not included in this table. The IP address * is a mask functioning as a wildcard address. • If the destination IP address is *, it refers to all calls from the Source IP address, which must be a specific address. • If the Source IP address is *, it refers to all calls to the Destination IP address, which must be a specific address. ActiveTime is the sum of the duration (hold time) of all calls, derived from the time of the first and last packet in the flow. The data categories associated with the CallRecord table are ActiveTime Records Packets Bytes Flows
ASMatrix	Source AS Dest AS	The source and destination of each autonomous system (AS).

Interpretation of Protocol Ports

Table 3-2 shows that protocol ports are defined differently depending upon the direction of traffic flow.

Table 3-2 Protocol Ports Defined

Direction of Flow	Assignment of Port Numbers
Source to Destination	The well-known port numbers defined in RFC 1700, October 1994.
Destination to Source	An arbitrary number assigned by the host to identify the session. (This number may accidentally fall in the range of registered ports defined in RFC 1700, so it is not a guaranteed diagnostic that the direction of flow is from the destination to the source.)