CHAPTER 1

NetFlow FlowAnalyzer Overview

This chapter describes the NetFlow FlowAnalyzer system and its components. This system is used to read, analyze, and display NetFlow switching data collected by the NetFlow FlowCollector application.

NetFlow switching is supported in the following Cisco IOS releases:

Release 11.x (or later) for the following routers:

- Cisco 7000 family of routers with Route/Switch Processor (RSP) 7000
- Cisco 7500 series routers

Release 11.1(5) or later for the following routers:

- Cisco 7200 series routers

Cisco IOS provides expanded security, quality of service, and enhanced traffic management capabilities within the NetFlow switching framework. Related network services are based on managing traffic flows between network layer address pairs visible to the NetFlow FlowCollector application.

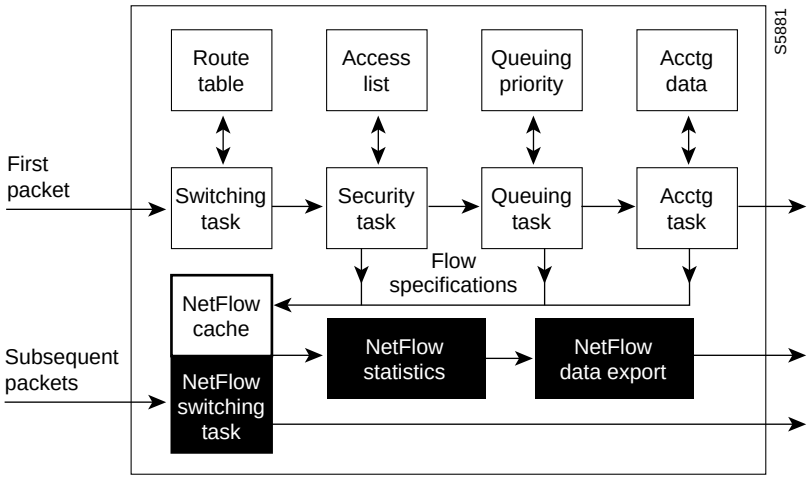
NetFlow Switching

NetFlow switching is a high-performance network-layer switching mechanism that captures as part of its switching function a rich set of traffic statistics, including per-user, per-protocol, per-port, and per-type of service statistics. These statistics can be used for a wide variety of purposes, such as network analysis and planning, accounting, and billing.

NetFlow switching provides network administrators with access to call detail recording information for their data networks. Exported NetFlow data can be used for a variety of purposes, including network management and planning, enterprise accounting and departmental chargebacks, ISP billing, and data warehousing/mining for marketing purposes. NetFlow also provides a highly efficient mechanism for processing security access lists without paying as much of a performance penalty as is incurred with other available switching methods.

Figure 1-1 shows a comparison between conventional network layer switching and NetFlow switching.

Figure 1-1 Conventional Network Layer Switching Versus NetFlow Switching



The NetFlow System

The NetFlow system reads, analyzes, and displays NetFlow switching data collected by the NetFlow FlowCollector application. The NetFlow system includes three main components:

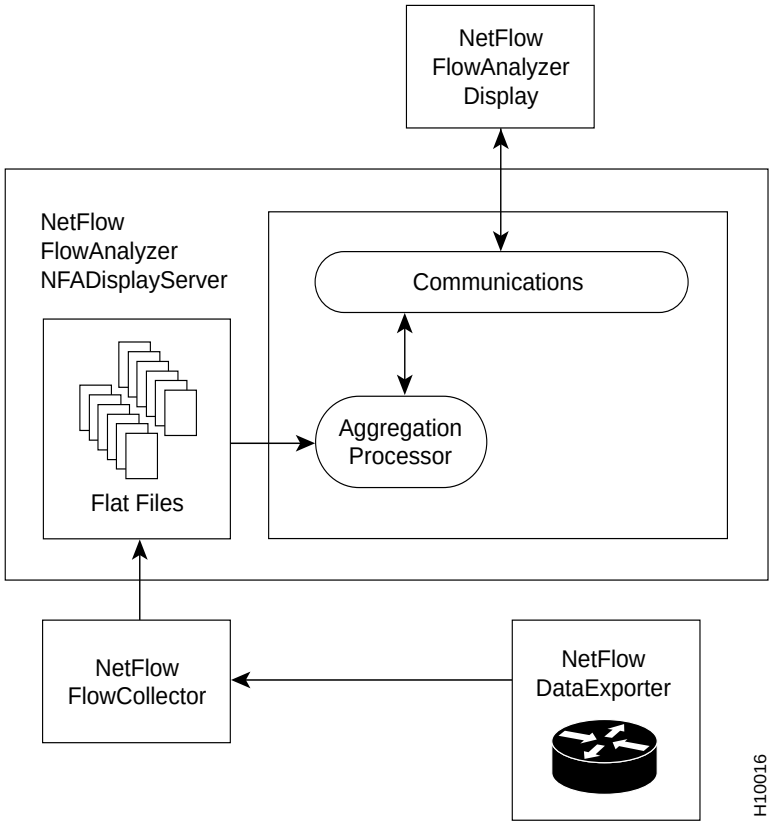
1. NetFlow Data Exporter—Resides in the switch-enabled router and sends data to the FlowCollector's workstation.
2. NetFlow FlowCollector application—Collects the data that is exported from switch-enabled routers running the NetFlow Switching application. The FlowCollector application stores this data in flat files.
3. NetFlow FlowAnalyzer application—Includes a server and user interface.

   NetFlow FlowAnalyzer DisplayServer—Receives requests from the display and summarizes the data collected by the NetFlow FlowCollector for display by the browser-based user interface.

   NetFlow FlowAnalyzer Display User Interface—Displays collected data using a browser.

Figure 1-2 shows the NetFlow system and its components.

Figure 1-2 NetFlow System



NetFlow FlowCollector Application

The NetFlow FlowCollector application, the FlowCollector, provides fast, scalable, reliable, and economical data collection from multiple Cisco routers exporting NetFlow data records containing traffic statistics. Data is stored in aggregation schemes for later retrieval and analysis.

Some functions of the FlowCollector include

- NetFlow data collection from multiple routers and flat file creation
- Data volume reduction through filtering and aggregation
- Hierarchical data storage (help client applications to conveniently retrieve data)
- Disk management

Traffic Statistics

The NetFlow data records exported by the routers consist of expired traffic flows containing detailed traffic statistics. These traffic statistics contain information about network Layer 3 sources and destinations, down to the level of individual applications and protocols with end-to-end conversation. This information about the routers

- Assists network managers to monitor network traffic and fine-tune networks by identifying which users and applications need additional bandwidth or a specified quality of service
- Consolidates information that can be used for advanced billing on a per-application and actual usage basis

The following items are included in the traffic statistics:

- Time stamp of the flow
- Source and destination IP address
- Source and destination port number
- Input and output interface number
- Next hop address
- Total bytes in the flow
- Number of packets in the flow
- First and last time stamps of packets that were switched as part of this flow
- Sequence number (version 5 only) src+dst AS (or peer AS), src+dst prefix masks

Aggregation Schemes

The FlowCollector collects detailed traffic statistics and summarizes the data (that is, aggregates the flows) by any of the following aggregation schemes:

- SourceNode
- DestNode
- HostMatrix
- SourcePort
- DestPort
- Protocol
- DetailDestNode
- DetailHostMatrix
- DetailInterface
- CallRecord
- ASMatrix

These aggregation schemes are described in more detail in the chapter entitled “Using the NetFlow FlowAnalyzer Display.”

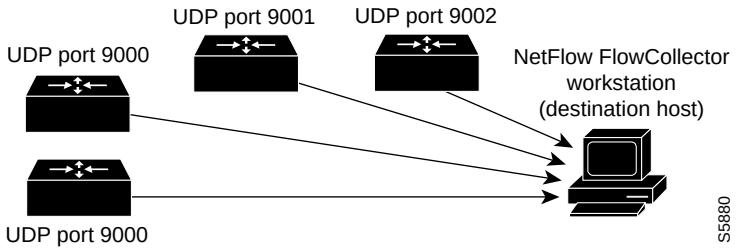
Filters

You can apply filters to the aggregation schemes to customize traffic statistics by specifying one or more of the following fields:

- Srcaddr (network layer IP address of the source)
- Dstaddr (network layer IP address of the destination)
- Nexthop address
- Srcinterface (input interface number (physical interface))
- Dstinterface (output interface number (physical interface))
- Srcport number (transport layer port per RFC 1700)
- Dstport number (transport layer port per RFC 1700)
- Prot
- Protocol

Figure 1-3 shows an example of a typical network of routers with the FlowCollector running on the destination host. Each router is configured with the destination host's IP address and destination UDP port number. After you configure and start the FlowCollector application, the FlowCollector listens to the user-specified UDP ports for NetFlow export datagrams from the routers.

Figure 1-3 FlowCollector Overview



NetFlow Data Exporter

The NetFlow Data Exporter makes possible the bulk export of traffic statistics. A summary of traffic statistics for all expired traffic flows can be exported periodically through datagrams to specified destinations, including traffic probes, management applications, and other data sinks.

NetFlow FlowAnalyzer Application

The NetFlow FlowAnalyzer application, the FlowAnalyzer, is a network management application that includes a server and a user interface. You can use the FlowAnalyzer to display data collected by the NetFlow FlowCollector application.

NetFlow FlowAnalyzer DisplayServer

The FlowAnalyzer DisplayServer program receives requests for traffic statistics from the FlowAnalyzer user interface and provides data collected in flat files created by the FlowCollector. The data is displayed by the NetFlow FlowAnalyzer user interface.

NetFlow FlowAnalyzer User Interface

The FlowAnalyzer user interface uses a browser to display the data collected by the FlowCollector in a variety of formats, including

- Tabular
- Graphical—Summary graph, histogram chart, pie chart
- Numeric data—Listed in descending order
- Nonnumeric data—Listed in ascending order
- Spreadsheet

Users can also specify time intervals and the number of entries to be displayed.

Collector Configuration

Setting Time Zones

You should run the FlowCollector with the UTC (GMT) reference. To run the FlowCollector in this mode, you must edit the nf.resources file and type **yes** on the line that includes GMT_FLAG. For example

```
GMT_FLAG              yes
```

If you do not run the FlowCollector with the UTC reference, you must specify a distinct DataSetPath option for each local time zone of your data collection. For more information about the FlowCollector, refer to the *NetFlow FlowCollector Installation and User Guide*.

Naming Routers

You should specify router names in the decimal-byte format a.b.c.d (for example, 171.69.204.5) to ensure that the analysis module can locate the requested data for that router. The FlowCollector should use the dot-decimal format to avoid data from the same router being stored in more than one location in the database.

To run the FlowCollector in dot-decimal format, you must edit the nf.resources file and type **yes** on the line that includes DEV_DOTTEDADDRESS. For example

```
DEV_DOTTEDADDRESS     yes
```

Data collection and analysis cannot be guaranteed when you are using aliases to name routers. If the FlowCollector cannot obtain the router's alias to identify the router, it uses the decimal-byte format DEV_DOTTEDADDRESS. A database will include a combination of router aliases and decimal-byte formatted router names unless all data collection is done with the DEV_DOTTEDADDRESS format set to yes.