IPSWITCH

Flow Monitor for WhatsUp Gold v16.2

User Guide

IPSWITCH WhatsUpGold
IT MANAGEMENT MADE SIMPLE

Table of Contents

Using Flow Monitor dashboard reports

CHAPTER 1

Flow Monitor Overview

In This Chapter

Welcome to WhatsUp Gold Flow Monitor

Flow Monitor collects, analyzes, and reports on NetFlow, sFlow, J-Flow (sampled NetFlow), or IP Flow Information Export (IPFIX) data from routers, switches, and other network devices, creating visible trends and patterns in network bandwidth utilization. Flow Monitor offers versatile reporting on the hosts generating and receiving traffic and the applications over which traffic is transmitted.

This help system includes information about the features and benefits of WhatsUp Flow Monitor. For more information, use the Contents, Index, or Search to the left, or select one of the sections below.

- **WhatsUp Flow Monitor Overview**

  Learn about the NetFlow protocol, discover how Flow Monitor works, and view system requirements for Flow Monitor.

- **Configuring Flow Monitor**

  Discover how to configure NetFlow sources to send data to Flow Monitor, define traffic over non-standard ports, manage users, and maintain the Flow Monitor database.

- **Navigating Flow Monitor**

  Find out about the features of the Flow Monitor home page and learn how to search for traffic to or from a specific host.

- **Using Reports**

  Learn about the Flow Interface Details report, the Flow Interface Overview report, the Flow Bandwidth Usage report, and the Flow Log. Explore using dashboard reports in Flow Monitor and in WhatsUp Gold.

What is Flow Monitor?

WhatsUp Gold Flow Monitor is a network traffic monitor that lets you gather, analyze and report on network traffic patterns and bandwidth utilization in real-time.

WhatsUp Flow Monitor:

- Uses network protocols such as NetFlow, sFlow, Jflow and IPFIX to collect and analyze information about the traffic on a router, switch, or other network device.
- User SNMP to collect interface traffic, NBAR, and CBQoS statistics.
- Highlights overall utilization for the LAN or WAN, individual devices, or specific interfaces, and provides information about the users, applications and protocols that consume network resources.
- Provides reports that allow you to:
- View network usage trends to determine when to upgrade hardware to increase network capacity.
- Recognize and correct network configuration issues that may needlessly consume network resources or expose your network to security vulnerabilities.
- Identify traffic which may indicate undesired network usage, such as unauthorized use of peer-to-peer file sharing applications or a denial-of-service attack against your organization.
- Troubleshoot and correct causes of spikes in network traffic before they become problems.

How does Flow Monitor work?

What is Netflow?

NetFlow is a protocol used to collect data about network IP traffic and is used to monitor and record network usage, give indications of traffic routes and provide data in support of traffic accounting, usage-based billing and other network related activities. This data is classified using the concept of a network flow.

A network *flow* is a unidirectional sequence of packets that has the following characteristics in common:

- Source IP address and port number
- Destination IP address and port number
- IP Protocol
- Ingress interface
- IP Type of Service (ToS)

How does NetFlow work?

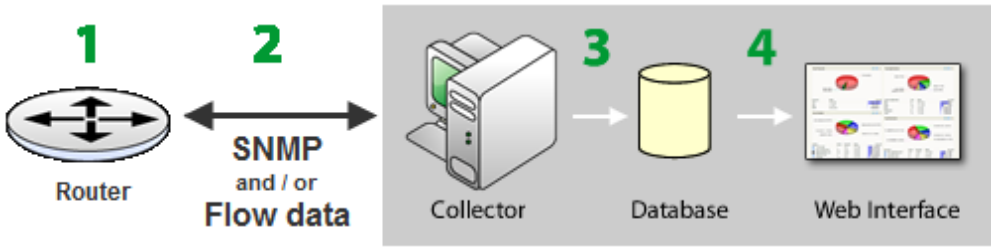
To capture, transmit and analyze NetFlow data, the following NetFlow enabled components must be in place:

- The **NetFlow exporter** observes packet data and creates records from the monitored network traffic and transmits that data to the NetFlow collector.
- The **NetFlow collector** collects the records sent from the exporter, stores them in a local database and forwards the records to an analyzer.
- The **NetFlow analyzer** analyzes the NetFlow records for information of interest, which may include bandwidth usage, policy adherence, and forensic research.

Note: The exporter can be either an included function of the network device, such as the NetFlow export functionality on Cisco routers, or an external probe configured to monitor one or more interfaces on the device, such as the Ipswitch NetFlow Probe.

How does Flow Monitor fit into the NetFlow architecture?

Flow Monitor acts as a flow collector and analyzer, providing a central location for the collection, summarization, storage and analysis of network traffic data. This network traffic data is captured as *flow* data, and is delivered by network monitoring protocols implemented on network devices throughout the network. When a router or other device sends flow data to Flow Monitor, it follows the process shown below.



1. The router gathers information about the traffic that is passing through it and summarizes that data into a NetFlow, sFlow, J-Flow (sampled NetFlow) or IP Flow Information Export (IPFIX) export datagram.
2. The router sends the flow export to Flow Monitor, which acts as a flow collector.

Note: sFlow data is sent every x number of packets (configurable on the sFlow device), whereas all NetFlow data is collected and monitored. This means that sFlow data provides a sampling of network traffic data, whereas NetFlow data provides all network traffic data.

3. The Flow Monitor collector stores the NetFlow, sFlow, J-Flow (sampled NetFlow) or IP Flow Information Export (IPFIX) export in the database.
4. When the report data is viewed on the web interface, Flow Monitor retrieves the data from the database and manipulates it to produce the report.

Tip: Flow Monitor can collect and generate reports for Flow data from multiple devices.

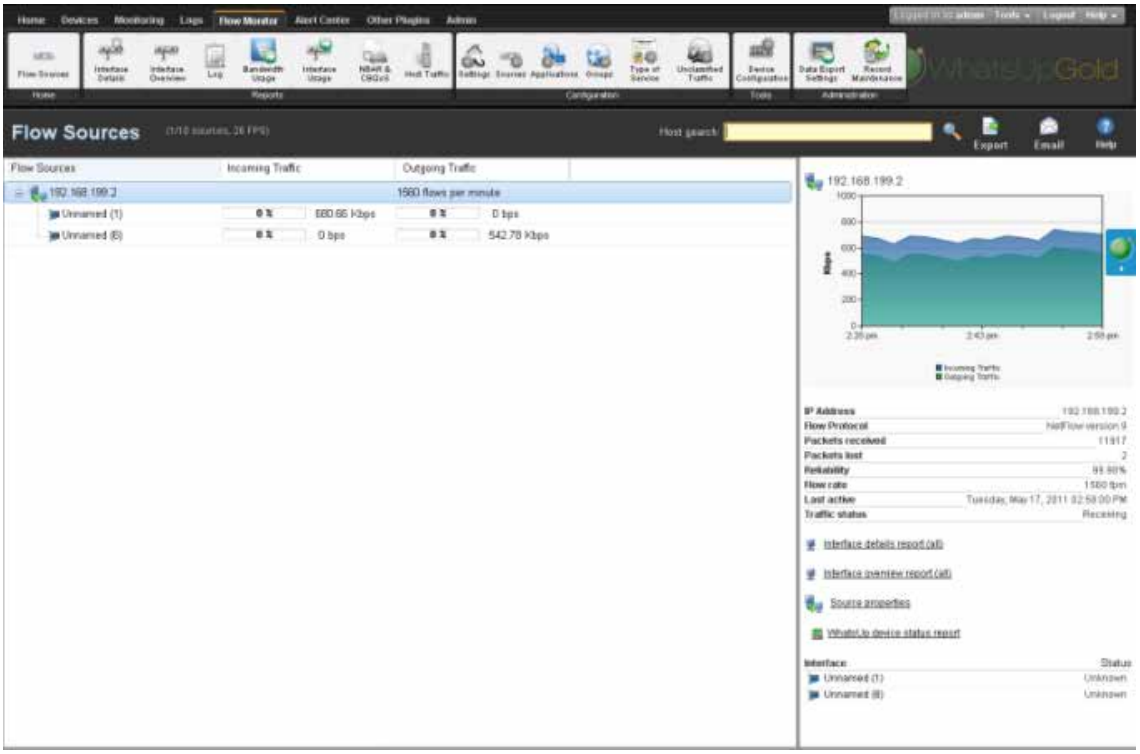
System requirements

WhatsUp Gold Flow Monitor has the same base *system requirements* (*http://www.whatsupgold.com/WUG162releasenotes*) as WhatsUp Gold. In addition, WhatsUp Gold Flow Monitor requires:

- WhatsUp Gold Standard Edition, Premium Edition, MSP Edition, or Distributed Edition
- One or both of the following:
- At least one routing device that supports NetFlow version versions 1, 5, 7, and 9, sFlow versions 2 and 5, J-flow (sampled NetFlow) or IP Flow Information Export (IPFIX).
- A Flow Publisher monitoring a flow source.

Flow Monitor Home

The Flow Monitor Flow Sources page provides a summary of the current usage and status of Flow Monitor sources, and acts as the Home page for the Flow Monitor plug-in. The left and right panes of the content pane display different types of data; Flow Sources on the left and Source and Interface Details on the right. Click **Flow Monitor > Flow Sources** to access the Flow Monitor Flow Sources screen.



Flow Monitor sources

The left pane of the page lists each of the monitored sources and the interfaces associated with each source.

In the Flow Sources title bar, the number of licensed sources and total licenses available is displayed along with the total number of flows per second received by all of the licensed sources. For example, the following (2/10 sources, 65 FPS) indicates that there are 2 licensed sources of 10 available licenses, and that the total flows per second being received by all of the sources is 65 flows per second.

- **Flow Sources**. Routers and switches that have been configured to send flow data to Flow Monitor and are enabled in Flow Monitor are listed in this column. In the list, sources are organized at the top level. Associated interfaces for each source are below the source name. Use the collapse and expand buttons to show or hide source interfaces. For each source, the number of flows per minute (fpm) for Flow devices and samples per minute (spm) for sFlow devices generated by all interfaces on the selected source over the the last period is displayed. When you select a source from the Flow Sources list, its total traffic is displayed in the right pane, along with all of the other information about the source.

Note: Interfaces can be hidden; if you do not see an interface listed on this dashboard report, check to see if it has been hidden via the Flow Interface dialog.

Tip: If you do not see a source listed that you would like to monitor, first go to the Flow Sources dialog to configure source settings. If you still do not see the router listed, check to see that the router is configured to send flow data. For more information, see Configuring Flow Monitor sources or Configuring sFlow sources.

- **SNMP Sources**. SNMP Sources are sources that have been created for the purpose of collecting NBAR and CBQoS statistics from a device using SNMP polling instead of flow data. SNMP Sources appear as normal sources. For information on creating an SNMP source, see Create Flow Source.
- **Aggregate Sources**. Aggregate Sources are individual interfaces existing on one or many Flow Sources that are aggregated into a single logical group that is treated as a separate source for reporting purposes. These sources appear as folders below the Flow Sources. For information on creating an Aggregate Source, see *Creating an Aggregate Source*.
- **Incoming Interface Traffic**. Incoming traffic is reported as a percentage of usage according to the interface's speed, and number of incoming bits per second (bps) based on the last traffic to enter the interface.
- **Outgoing Interface Traffic**. Outgoing traffic is reported as a percentage of usage according to the interface's speed, and as the number of outgoing bits per second (bps) based on the last traffic to leave the interface.

Source and interface details

The right side of the page gives detailed information about a selected source or interface.

Note: If you have not enabled Flow sources at this time, a Welcome dashboard report is displayed on the right side of the Flow Monitor Home page. Consult this dashboard report for information on configuring your routers to send Flow data, and for other general Flow Monitor configuration information.

Source details

Click a source, or device in the list to view the Source details on the right side of the Home page.

- **IP address**. The source router's IP address.
- **Flow protocol**. The version of Flow or sFlow the source uses when exporting flow data.
- **Sample rate**. The rate at which the source is polling interface data.

Note: The sample rate appears only for sources sending sampled Flow data.

- **Packets received**. The number of packets the collector received from the source since the collector service was started.
- **Packets lost**. The number of packets sent from the source but not received by the collector since the collector service was started.
- **Reliability**. The percentage of packets received versus packets lost by the source since the collector service was started.
- **Flow rate**. The number of flows per minute (fpm) reported by the source during the last collection interval.
- **Last active**. The last time traffic was received from the source.
- **Traffic status**. Whether Flow Monitor is receiving traffic from the source; either receiving, or not receiving.

Note: If any traffic has been received within the last 30 minutes, the traffic status displays as receiving.

Use the Source Properties link at the bottom of the source details to view the Flow Source dialog and use the Interface links to view the WhatsUp Gold Interface Details report.

Note: A link for the WhatsUp Gold Interface Details report appears only if the source is monitored in WhatsUp Gold.

Interface details

Click a source device interface in the list to view the Interface details on the right side of the Home page. The Interface Traffic report for the last collection interval is displayed at the top of the interface's details.

- **Last incoming details**. The last time traffic transmitted over the incoming interface.
- **Last outgoing details**. The last time traffic transmitted over the outgoing interface.
- **Interface type**. The type of the interface; for example, Ethernet CSMA/CD.
- **In speed**. The speed at which data is flowing to the interface.

- **Out speed**. The speed at which data is flowing from the interface.
- **Status**. The status of the interface; either Up, Down, or Unknown.

Use the links at the bottom of the interface details to view the Interface Details and Interface Overview reports, as well as the Flow Interface Properties.

Exporting, emailing, scheduling and managing reports

Use the **Export** 

icon, at the top right of the page, to export reports. Use the **Email** 

icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 97).

Host Search

Use the Host Search tool in the upper-right side of the page to locate traffic to or from a host or group of hosts.

To perform a host search:

1. Enter search criteria, such as an IP address or host name, in the **Host search** field.
2. Click the search button  .
   - When a host name is entered for search, the Host Search dialog appears with a list of interfaces where traffic to that host has been logged. You can use the search options in the Host Search dialog to further narrow your search. For more information, see the Flow Monitor Host Search dialog help.
   - When a complete IP address is entered for search, the Select Interface dialog appears with a list of interfaces where traffic to that IP has been logged.

Note: The Domain, Country, and Last Resolved fields may show as Not Available if the IP address is not available in the DNS.

Tip: Use the menu on this page to view and configure parts of the application. For more information, see Using the Flow Home page menu.

CHAPTER 2

Preparing network devices

In This Chapter

Determining which network devices to monitor

When planning your Flow Monitor deployment, it is important to understand which network devices are likely to provide you the information you want. In identifying those devices, questions about the data flowing through an individual device, its location in respect to other network devices and the types of addresses (internal/external) available to that device are all of importance.

Are you interested in monitoring the internet gateway routers connecting to your ISP for application level traffic analysis, performing forensics and diagnostics on a core router of a public facing network, or monitoring your WAN core in order to plan for additional capacity? The answers to these and similar questions about the purpose of your monitoring will provide you with some indication as to which devices in your network are of most interest as potential sources for Flow Monitor.

Once a potential Flow Monitor source has been identified, you should consider the location of the device with respect to other networking devices, particularly those devices that perform network address translation (NAT). Depending on where the source is located relative to the device performing NAT, traffic to and from an internal (private) IP addresses are reported differently in the exported NetFlow data.

- If the device is inside the firewall, or if no firewall exists, the exported flow data includes the internal IP address for devices generating and receiving traffic. This allows you to pinpoint the exact device in the internal network to which the traffic belongs.

- If the device is outside the firewall, the exported flow data aggregates all traffic to and from internal devices and reports it as belonging to a single public address belonging to the device performing the address translation. In this case, you can only determine that an internal device originated or received traffic, but you cannot pinpoint the traffic as belonging to a specific internal device.
- If the device exporting flows is also performing NAT, you can configure the device to export the flow data using either the private or the public translated address, mimicking either of the above scenarios. To see internal IP addresses, configure the device to export data on `ingress` and `egress` for the **internal** interface. To see all traffic reported using the external translated IP address, configure the device to export data on `ingress` and `egress` for **external** interfaces. For more information, see *Manually configuring network devices to export flow data to Flow Monitor* (on page 9).

Other conditions that may also change the nature of the data reported by Flow Monitor include:

- When address translation occurs anywhere in the path between the source and the destination, IP addresses reported are altered to include the translated address. In most cases, this does not present a problem, but it may require monitoring multiple flow-enabled devices to track traffic in complex network environments.
- Virtual private networks and other tunneling technology (such as ESP or SSH) can appear to distort reports. In these cases, Flow Monitor reports large amounts of traffic sent over a small number of flows. This is expected behavior, as VPNs and other tunnels aggregate traffic from multiple connections and funnel it through a single connection.

Manually configuring devices to export flow data to Flow Monitor

Network devices must be configured to generate and send NetFlow data to Flow Monitor. This is accomplished manually using the device's command line interface (CLI), or automatically through the Source configuration dialog (**Flow Monitor > Configuration**) for devices that are NetFlow enabled and have the Cisco NetFlow MIB (OID: 1.3.6.1.4.1.9.9.387).

To manually configure NetFlow enabled devices to send Flow data to Flow Monitor:

Caution: This procedure is an example that applies to a Cisco 1812 router and should not be used for other devices. The process for configuring a device to export Flow data varies widely from device to device and dependent upon your network configuration. Please see your router's documentation to determine the correct process for your device.

- **Step 1**. Open the configuration interface for the router and enter the commands detailed in the following table to configure global options for all interfaces on the router.

Command	Purpose
`enable`	Enters privileged EXEC mode. Enter your password if prompted.
`configure terminal`	Enters configuration mode.
`ip flow-export version <version_number>` ex) `ip flow-export version <version_5>`	Sets the version of the NetFlow protocol that should be used to export data. Flow Monitor supports versions 1, 5, 7, and 9 only.
`ip flow-export destination <IP> <port>` ex) `ip flow-export destination <192.168.2.100> <9999>`	Enables the router to export Flow data. Substitute the Flow Monitor server's IP address for <IP> and the listener port specified in the Flow Monitor Flow Settings dialog for <port>. By default Flow Monitor uses port 9999.

- **Step 2**. Enter the commands detailed in the following table to enable the router to export Flow data about the traffic on an interface. You must repeat these commands for each interface.

Command	Purpose
`interface <interface>`	Enters the configuration mode for the interface you specify. Substitute <interface> with the interface's name on the router.

`ip flow ingress`
- and / or -
`ip flow egress`
	Enables Flow data export. Select the command that best fits your needs.
	§ `ip flow ingress` exports flows of all inbound traffic that uses the interface.
	§ `ip flow egress` exports flows of all outbound traffic that uses the interface.

Tip: If the device exporting Flow data is also performing network address translation (NAT), we recommend exporting egress data from the internal interface so that private network addresses are communicated. Any other configuration results in all private addresses reporting as the public addresses of the device performing the network address translation.

Note: Other options exist for configuring NetFlow. For a complete list of available options, see *Configuring NetFlow* (*http://www.whatsupgold.com/NF_CiscoCfg*) on the Cisco Web site.

Important: In cases where NetFlow Monitor is monitoring data flow between devices that have a long-lived connection, such as router linked between two office sites, you may get spikes in the flow data. Cisco routers by default break and send NetFlow stats every thirty-minutes for long-lived connections. To reduce the data spikes, change the router configuration with the following command:

```
ip flow-cache timeout active <n>
```

Where n is the number of minutes. The minutes should be configured to less than or equal to the NefFlow Data collection interval setting which is 2 minutes by default.

Configuring sFlow enabled devices to export flow data to Flow Monitor

Before you can view meaningful sFlow reports, you must configure sFlow-enabled devices, such as routers or switches, to communicate network activity back to the Flow Monitor listener application. There are two methods to configure sFlow to send data to Flow Monitor:

- Configure the sFlow device with the device OS commands using the command line interface (CLI).
  - or -
- Configure the sFlow device using SNMP commands.

The following examples shows how to configure sFlow devices to send data to Flow Monitor.

Configuring sFlow using the CLI

To configure a sFlow enabled device to send sFlow data to Flow Monitor using the command line interface (CLI):

Caution: This procedure is an example that applies only to an HP ProCurve 3500 switch and should not be used for other devices. The process for configuring a device to export sFlow data varies widely from device to device and is dependent upon your network configuration.

The following example uses CLI configuration to enable sFlow on an HP ProCurve 3500 series switch. The configuration is for Flow Monitor running on a system with IP address 192.168.3.31 and receiving sFlow data on UDP port 9999.

1. Access the sFlow device via the command line interface (CLI).
2. Set the sFlow device IP (sFlow collector) using the following commands.

Command	Purpose
`(config)# sflow 1 destination <ipaddress> <port>`	Sets the sFlow receiving device address (192.168.3.31) and UDP port (9999). For example: `(config)# sflow 1 destination 192.168.3.31 9999`
`(config)# sflow 1 sampling ethernet <interface ID> <sample every n packets>`	Sets the sFlow sample rate for each interface (1-24). One out of every 128 packets will be collected in this example. For example: `(config)# sflow 1 sampling ethernet A1-A24 128`

`(config)# sflow 1 polling ethernet <interface ID> <polling frequency in seconds>`	Sets the sFlow polling interval. Polls every 30 seconds in this example. For example: `config)# sflow 1 polling ethernet A1-A24 30`

Configuring sFlow using SNMP

The following example uses SNMP commands to enable sFlow on an HP ProCurve 2610 series switch. We recommend configuring the sFlow device via the device OS commands from the command line interface (CLI); however, some sFlow devices do not include this capability. In this case, you can use SNMP commands to configure sFlow. This configuration example is for Flow Monitor running on a system with IP address 192.168.3.31 and receiving sFlow data on UDP port 9999.

To configure an sFlow device, using SNMP commands, to send sFlow data to Flow Monitor:

Important: This procedure is an example that applies to an HP ProCurve 2610 switch and should not be used for other devices. The process for configuring a device to export sFlow data varies widely from device to device and is dependent upon your network configuration. Refer to the documentation to determine the correct process for your device.

Important: An sFlow device configured with the SNMP commands typically do not save the configuration to memory. If the device is rebooted, or power is lost, all sFlow configuration is lost and must be manually reset using the SNMP commands. Make sure that you save the SNMP configuration commands for future device configuration.

Note: Make sure that the sFlow device is configured to allow SNMP read/write access and make sure that you have the community string information for read/write access. Refer to the documentation to determine the correct process for your device.

1. Access the sFlow device via the console, Telnet, or SSH management interface.
2. Set the sFlow device IP (sFlow collector) using the following example commands.

Command	Purpose
`setmib sFlowRcvrAddress.1 -o <collector IP address in hexadecimal format>`	Sets the sFlow receiving device address. In this example, the IP address (192.168.3.31) must be provided as a hexadecimal value (C0A8031F). For example: `setmib sFlowRcvrAddress.1 -o C0A8031F` **Important**: The example IP address must be entered as a hexadecimal value. Use an IP to hexadecimal calculator to determine the hexadecimal value for your sFlow collector's IP address. This example IP address breaks down into a hex value as follows: 192 = C0 168 = A8

	3 = 03 31 = 1F
`setmib sFlowRcvrPort.1 -i <port>`	Sets the sFlow receiving device port address. The default Flow Monitor port is 9999. For example: `setmib sFlowRcvrPort.1 -i 9999`
`setmib sFlowRcvrOwner.1 -D <Display String value> sFlowRcvrTimeout.1 -i <Timeout integer value>`	Sets the sFlow receiver owner. The -D is a TYPE-STR identifier that specifies a Display String value. This value can be any string, for example NFmonitor (referring to Flow Monitor application which will receive the sFlow data). The -i is a TYPE-STR identifier that specifies an Integer value. The 100,000,000 value is a timeout value that defines the timeout countdown starting point value (in milliseconds). For example: `setmib sFlowRcvrOwner.1 -D NFmonitor sFlowRcvrTimeout.1 -i 100000000`
Note: Repeat the following settings for each interface on the sFlow device you want to monitor. The last number in the MIB OID represents the interface number.	`setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6.1.2.1.2.2.1.1.1.<interface integer value>` For example: `setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6.1.2.1.2.2.1.1.1.1`
`setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6.1.2.1.2.2.1.1.1.1 -i <sample every n packets>`	Sets the sFlow sample rate. One out of every 128 packets will be collected in this example. For example: `setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6.1.2.1.2.2.1.1.1.1 -i 128`
`setmib 1.3.6.1.4.1.14706.1.1.5.1.3.11.1.3.6.1.2.1.2.2.1.1.1.1 -i <Enable/Disable sFlow integer value>`	Enables sFlow on the device. 1 enables / 0 disables sFlow. For example: `setmib 1.3.6.1.4.1.14706.1.1.5.1.3.11.1.3.6.1.2.1.2.2.1.1.1.1 -i 1`
`setmib 1.3.6.1.4.1.14706.1.1.6.1.4.11.1.3.6.1.2.1.2.2.1.1.53.1 -i <polling frequency in seconds>`	Sets the sFlow polling interval. Polls every 30 seconds in this example. For example: `setmib 1.3.6.1.4.1.14706.1.1.6.1.4.11.1.3.6.1.2.1.2.2.1.1.53.1 -i 30`
`setmib 1.3.6.1.4.1.14706.1.1.6.1.3.11.1.`	Enables sFlow polling. 1 enables / 0 disables sFlow polling. For example:

3.6.1.2.1.2.2.1.1.53.1 -i <Enable/Disable sFlow polling integer value>	setmib 1.3.6.1.4.1.14706.1.1.6.1.3.11.1.3.6.1.2.1.2.2.1.1.53.1 -i 1

For more configuration options for sFlow, see the *NetFlow Settings help http://www.whatsupgold.com/NetFlowSettings*.

About Flexible NetFlow

Cisco IOS Flexible NetFlow provides the next level of flexibility and scalability in monitoring network traffic, bringing a new understanding to who is using the network, what applications they are employing, when they are using the applications, and where the traffic originated.

Important: Unlike traditional NetFlow, Flexible NetFlow does not support SNMP. At this time, Flexible NetFlow can only be configured through the CLI. Any tool used to automatically configure NetFlow using SNMP will not work with Flexible NetFlow.

Flexible NetFlow Components

Flexible NetFlow is implemented using flow monitors, the following is a definition of a flow monitor and its components.

Note: A NetFlow flow monitor is a component used to implement Flexible NetFlow and should not be confused with WhatsUp Flow Monitor, which is a NetFlow collector.

- **Flow monitors**. Flow monitors are applied to interfaces to perform network traffic monitoring. These flow monitors consist of the following components:
- **Flow records**. A record is a combination of key boxes, used to uniquely define a flow, and nonkey boxes, which are used to provide additional information about a flow, but are not used to define the flow. In Flexible NetFlow, both key and nonkey boxes can be defined in the record definition, which allows for customized data collection.
- **Flow cache**. Collects IP data flow records in a router or switch, analyzes this data and prepares the data for export. Flexible Netflow tracks and monitors multiple NetFlow caches, each configured to monitor specific information.
- **NetFlow exporter**. Exports the data in the flow monitor cache to a remote system, such as Flow Monitor, for analysis and storage. You can create more than one flow exporter, each assigned to one or more NetFlow collectors.
- **NetFlow collector**. An application that utilizes exported data from one or more NetFlow enabled routers or switches, aggregates and filters the data, then performs real-time visualization and analysis of the recorded and aggregated flow data. The WhatsUp Flow Monitor is an example of a NetFlow collector.

Flexible NetFlow records

Flexible NetFlow can track packet information from Layer 3, as well as some Layer 2 information. The Flexible NetFlow record can be customized to monitor data based on your specific monitoring needs. The information available includes:

- Source and Destination MAC addresses
- Source and Destination IP addresses
- Type of Service
- Differentiated Services Code Point (DSCP)
- Packet and byte counts
- Flow timestamps
- Input and output interface numbers
- TCP flags
- Routing information

Where traditional NetFlow provided a strict definition of which boxes in a record are key box, used to define a flow, Flexible NetFlow allows you to define a flow based on the boxes and data you want to monitor, which allows for the ability to export only the data needed by the collector to conduct its analysis and reporting. Additionally, more data is available in Flexible NetFlow than in traditional NetFlow, which allows for extensive customization and flexibility in defining flow records.

Flexible NetFlow and Network Based Application Recognition (NBAR)

Through this definition of flows, it is possible to gather information that can be used by Cisco Network Based Application Recognition (NBAR) to identify application data within a flow and provide flow statistics on the application traffic.

Configuring Flexible NetFlow on a Cisco device

Flexible NetFlow can be used to support the implementation of Cisco Network Based Application Recognition (NBAR) technology. To configure a network device to use Flexible NetFlow, perform with the following configuration steps:

1. Create a flow monitor
2. Define the flow record (use one of the two configuration methods)
3. Create a flow exporter

These tasks are described in the following sections, using an example configuration to illustrate how to complete the tasks from the Cisco IOS command line interface (CLI).

Important: The network device you want to configure must be running a Cisco IOS release that supports Cisco IOS Flexible NetFlow.

Creating a flow monitor

The following example illustrates how to configure a Flexible NetFlow enabled device to utilize Flexible NetFlow in support of NBAR and Flow Monitor application monitoring. For more information see the *Cisco IOS Flexible NetFlow configuration guide* (*http://www.whatsupgold.com/CiscoIOSFlexibleNetFlow*).

To create a flow monitor:

1. Enter the privileged EXEC mode, and then enter the global configuration mode.

```
Router> enable
Router# configure terminal
```

2. Create a flow monitor, and enter the flow monitor configuration mode.

```
Router(config)# flow monitor application-mon
Router(config-flow-monitor)# description app traffic analysis
Router(config-flow-monitor)# cache timeout active 60
```

Defining a flow record

There are two methods to define a flow record to use Flexible NetFlow. The first, and simplest to configure option, is to run a command on the Cisco device to configure sources with a predefined format as follows:

(Option 1) To define a flow record:

- Run the following command on the Cisco device for which you want configure Flexible NetFlow sources:
- `record netflow ipv4 original-input`
  - or -
  `record netflow original-input`

(Option 2) To define a flow record:

1. Enter the privileged EXEC mode, and then enter the global configuration mode.

```
Router > enable
Router# configure terminal
```

2. Enter the flow monitor configuration mode.

```
Router(config)# flow monitor application-mon
```

3. Name the record and enter a description.

```
Router(config-flow-monitor)# flow record nbar-appmon
Router(config-flow-record)# description NBAR Flow Monitor
```

4. Define key boxes, using the `match` keyword.

```
Router(config-flow-record)# match ipv4 tos
Router(config-flow-record)# match ipv4 protocol
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match transport source-port
Router(config-flow-record)# match transport destination-port
Router(config-flow-record)# match interface input
Router(config-flow-record)# match application name
```

Note: By using the application name as a match parameter, you can utilize Network Based Application Recognition (NBAR) to collect statistics and report on network usage by individual applications.

5 Define nonkey boxes, using the `collect` keyword.

```
Router(config-flow-record)# collect interface output
Router(config-flow-record)# collect counter bytes
Router(config-flow-record)# collect counter packets
Router(config-flow-record)# collect transport tcp flags
```

(for networks using the BGP protocol, include the following two commands)

```
Router(config-flow-record)# collect routing source as
Router(config-flow-record)# collect routing destination as
```

6 Enter the flow monitor configuration mode and configure the flow monitor to use the newly configured record.

```
Router(config)# flow monitor application-mon
Router(config-flow-monitor)# record nbar-appmon
```

Creating a flow exporter

When the record is complete, you can create the flow exporter. This component exports records from the flow monitor on the network device to the flow collector, in this case Flow Monitor.

To create a flow exporter:

1 Enter the privileged EXEC mode, then enter the global configuration mode.

```
Router > enable
Router# configure terminal
```

2 Create and describe the flow exporter.

```
Router(config)# flow exporter export-to-ipswitch-flow-monitor
Router(config-flow-exporter)# description Flexible NF v9
```

3 Set the destination flow collector IP address.

```
Router(config-flow-exporter)# destination <Collector IP Address>
```

4 Define the PDU type and destination port.

```
Router(config-flow-exporter)# transport udp 9999
```

Note: Port 9999 is the default port for Flow Monitor

5 Set options for exporter operation.

```
Router(config-flow-exporter)# template data timeout
```

6 Enter the global configuration mode and configure the flow monitor to use the new flow exporter.

```
Router# configure terminal
Router(config)# exporter export-to-ipswitch_flow_monitor
```

About Network Based Application Recognition (NBAR)

Network Based Application Recognition (NBAR) is an application classification engine used to recognize a wide variety of applications. It can detect both Web-based and client-server applications.

NBAR identifies applications and protocols in Layer 4 to layer 7 using the following information:

- Static TCP and UDP port numbers
- Non UDP or TCP IP protocols
- Dynamically assigned TCP and UDP port numbers
- Sub-port classification
- Deep packet inspection

Protocol Discovery is a NBAR feature that collects application and protocol statistics for each interface based on the results of the application identification. Flow Monitor collects these statistics from the interface using Simple Network Management Protocol (SNMP) to poll the NBAR PD Management Information Base (MIB) where these statistics are stored.

The Protocol Discovery feature captures key statistics associated with each protocol in a network. These statistics can be used to define traffic classes and QoS policies for each traffic class.

Configuring NBAR on a Cisco device

You must enable NBAR on each interface from which you want to collect application statistics. The following example describes how to enable NBAR on an interface.

To enable NBAR on an interface:

1. Enter the privileged EXEC mode, then the global configuration mode.

   ```
   Router> enable
   Router# configure terminal
   ```

2. Enable Cisco Express Forwarding (cef).

   ```
   Router(config)# ip cef
   ```

3. Enter the interface configuration mode for the interface on which you want to enable NBAR.

   ```
   Router(config)# interface FastEthernet 0/1
   ```

4. Initiate NBAR protocol discovery on the interface.

   ```
   Router(config-if)# ip nbar protocol-discovery
   ```

5. Exit the interface configuration mode.

   ```
   Router(config-if)# exit
   ```

About CBQoS

Class-based quality of service (CBQoS) is the ability of a network to provide improved services to identified classes of network traffic. These services include supporting dedicated bandwidth, improving loss characteristics, managing network congestion, traffic shaping and setting traffic priorities. CBQoS involves two major components, traffic classes, and traffic policies.

Traffic classes

In the classification of network traffic, a traffic descriptor categorizes a packet as belonging to a group or class. By classifying network traffic, you can divide it into multiple priority levels or classes of service. Traffic classes are created using the `class-map` command which maps protocols and applications to a particular class.

Traffic policies

A traffic policy provides the mapping between the classes and the network controls used to provide the traffic priority, bandwidth guarantee, traffic shaping and other services available to traffic classes. Traffic policies are created using the `policy-map` command and are assigned to a particular interface using the `service-policy` command.

Configuring CBQoS on a Cisco device

To configure class-based QoS (CBQoS) on a Cisco device, perform the following tasks:

- Create the traffic classes using the `class-map` command
- Create the traffic policy using the `policy-map` command
- Attach the traffic policy to an interface using the `service-policy` command.

Note: The following procedures illustrate how to create a traffic class, how to create a traffic policy and how to attach the policy to an interface. The specific commands used to illustrate how these steps may be accomplished on a Cisco router are only for the purposes of this example. For more detailed information on how to implement QoS for your network, see Creating a Traffic Policy in the *Cisco IOS Quality of Service Solutions Configuration Guide* (*http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html*).

To create a traffic class:

1 Enable the privileged EXEC mode and enter the global configuration mode.

```
Router> enable
Router# configure terminal
```

2 Create the class name and enter the configure class map mode.

```
Router(config)# class-map match-any NMclass
```

Note: The `match-any` keyword is used when all of the match criteria in the traffic class must be met in order for a packet to be placed in the specified traffic class.

3 Use one or more match commands to specify the match criteria. Packets that match the specified match criteria will be placed in the traffic class.

```
Router(config-cmap)# match protocol snmp
Router(config-cmap)# match protocol icmp
```

Note: You can repeat the steps that create a class name and specify the match criteria to create as many classes as are needed to define the policy you want to apply to the interface.

4 Exit the class map configuration mode.

```
Router(config-cmap)# exit
```

Example: Class Map configuration

The following is an example of a class map configuration.

```
class-map match-any nm
   match protocol snmp
   match protocol icmp
class-map match-any p2p
   match protocol kazaa2
   match protocol gnutella
   match protocol edonkey
   match protocol bittorrent
   match protocol fasttrack
   match protocol directconnect
   match protocol winmx
class-map match-all FTP
   match protocol ftp
class-map match-any web
   match protocol http
class-map match-any utube
   match protocol http s-header-box "*http://www.youtube.com/*"
```

To create a traffic policy:

1. Enable the privileged EXEC mode and enter the global configuration mode (`config`).

   ```
   Router> enable
   Router# configure terminal
   ```

2. Create the traffic policy and enter the policy-map configuration mode (`config-pmap`).

   ```
   Router(config)# policy-map newPolicy
   ```

3. Specify the name of the class to associate with the policy and enter the policy-map class configuration mode (`config-pmap-c`).

Note: In the policy-map class configuration mode you can define one or more QoS features which supply services supporting dedicated bandwidth, improving loss characteristics, managing network congestion, traffic shaping and setting traffic priorities. For more information see Creating a Traffic Policy in the *Cisco IOS Quality of Service Solutions Configuration Guide* (*http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html*).

```
Router(config-pmap)# class NMclass
```

4. In the policy-map class configuration mode define the QoS features you want to apply to the class.

```
Router(config-pmap-c)# drop
```

Note: You can repeat the steps associating a class with the policy and defining the QoS features to apply to the class as many times as is necessary to create a policy that establishes services for all of the defined classes.

5 Exit the policy-map class configuration mode.

```
Router(config-pmap-c)# exit
```

Example: Traffic policy

The following is an example of a traffic policy:

```
policy-map crTest2
   class p2p
   drop
   class FTP
   drop
   class nm
         set dscp af43
   class web
         set dscp af12
   class utube
         set dscp af43
```

To associate a policy with an interface:

1 Enable the privileged EXEC mode and enter the global configuration mode (`config`).

```
Router> enable
Router# configure terminal
```

2 Select the interface to configure and enter the interface configuration mode.

```
Router(config)# interface GigabitEthernet0/0
```

3 Attach the policy map to the interface.

```
Router(config-if)# service-policy output input newPolicy
```

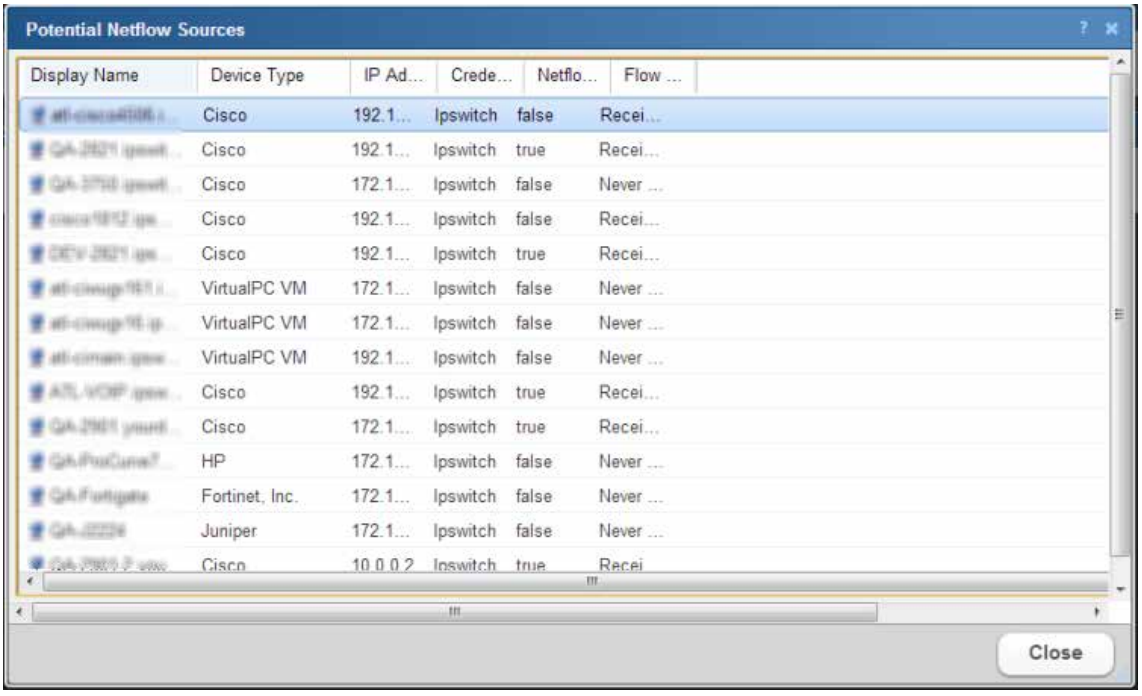
4 Exit the interface configuration mode.

```
Router(config-if)# exit
```

Note: For more information on associating a policy with an interface, see Attaching a Traffic policy to an Interface in the *Cisco IOS Quality of Service Solutions Configuration Guide* (*http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html*).

Viewing potential Flow Monitor sources

The Potential Flow Monitor sources dialog is a list of the routers discovered by WhatsUp Gold that have the potential of being a NetFlow source. When a network device such as a router is discovered and WhatsUp Gold has the necessary credentials to access the device using SNMP, the discovery process determines if the device is NetFlow enabled, and if the NetFlow MIB used to perform remote configuration of the device is available on the device.

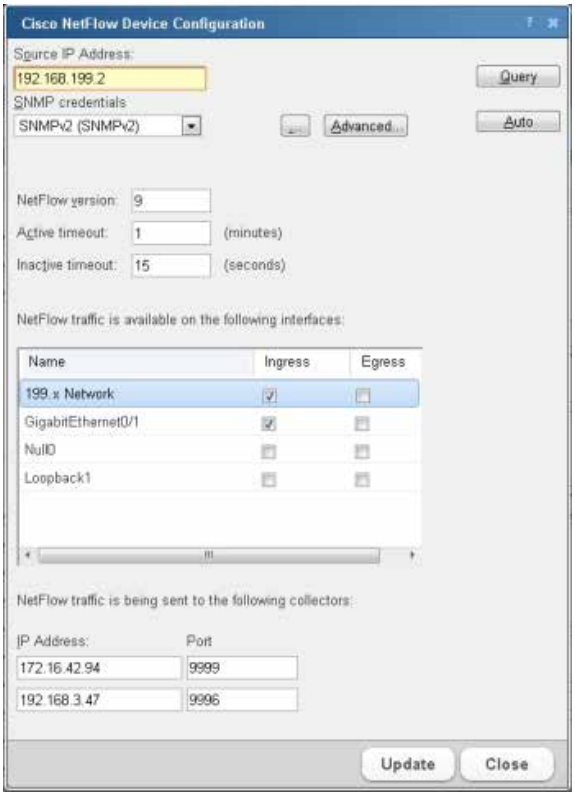


Information about devices that are potential Flow Monitor sources are displayed on this dialog along with the options for selecting a device for configuration using the Cisco NetFlow Device Configuration dialog.

- **Display Name**. The name of the device as provided by the WhatsUp Gold discovery engine.
- **Device Type**. The type of the device. Only Cisco devices can be remotely configured using the Cisco NetFlow Device Configuration dialog.
- **IP Address**. The IP address of the device.
- **Credentials**. The name of the credential that will be used when authenticating with the device.
- **Netflow MIB**. Displays a true if the device has the MIB object with the OID matching the NetFlow MIB. Device can be configured by Flow Monitor if the correct credentials are available.
- **Flow Monitor Status**. Displays the status of the device with respect to Flow Monitor
- Receiving - This device is currently sending flows to Flow Monitor.
- Never Received - This device has never sent flows to our Flow Monitor collector.
- Disabled - This device exists as a source in Flow Monitor, but is disabled.

Using Flow Monitor to Configure Cisco NetFlow Devices

The Cisco NetFlow Device Configuration dialog provides Flow Monitor with the ability to configure a Cisco device to send flow records to Flow Monitor.



Use this dialog to:

- Enter connection information and credentials used to connect to the Cisco device.
- Set the NetFlow version to be used by the flow exporter.
- Set the active and inactive timeouts used for cache management.
- Select the interfaces from which you want the device to collect and send flow data.
- Configure the NetFlow collectors, which in most cases includes Flow Monitor.

Enter the connection information and credentials to connect and authenticate with the Cisco network device.

- **Source IP address**. Enter the IP address of the Cisco NetFlow enabled device from which you want to collect NetFlow statistics.
- **SNMP credentials**. Select or create the SNMP credentials to use, with permission to write, to connect to the Cisco NetFlow enabled device. Click the browse (**...**) button to add, edit or delete SNMP credentials. Click the **Advanced** button to set SNMP timeout and retry parameters.

Tip: When you have selected valid SNMP credentials, the dialog queries the device and populates the NetFlow configuration parameters as well as the interface list. Use the **Query** button to update this information from the Cisco device. A message will appear if you do not have a write credential.

- Click **Auto** to automatically configure the device to collect and send flow data to Flow Monitor. When automatically configured, the device will enable collection of flow data on the device and will add itself as a netflow collector.

Enter the NetFlow configuration parameters to set the NetFlow version and configure the NetFlow cache on the Cisco device.

- **NetFlow version**. Enter the NetFlow version you want the exporter to deliver the flow records.
- **Active timeout**. Enter the Active timeout for flow records in the NetFlow cache. This value determines how long active, long-lived flows are kept in the NetFlow cache before sending to the collector (Range: 1-60 minutes) (Default: 2 minutes).

Important: In cases where NetFlow Monitor is monitoring data flow between devices that have a long-lived connection, such as router linked between two office sites, you may get spikes in the flow data. Cisco routers by default break and send NetFlow stats every thirty-minutes for long-lived connections. To reduce the data spikes, change the router configuration with the following command:

```
ip flow-cache timeout active <n>
```

Where n is the number of minutes. The minutes should be configured to less than or equal to the NefFlow Data collection interval setting which is 2 minutes by default.

- **Inactive timeout**. Enter the Inactive timeout value for flow records in the NetFlow cache. This value is used to ensure that completed or inactive flows are not kept in the NetFlow cache indefinitely. (Range 10 - 600 seconds) (Default: 30 seconds)

The Interface list displays the interfaces that can provide NetFlow data.

- **Name**. Displays the interface name as configured on the Cisco network device.
- **Ingress**. Select this option if you want to collect flow statistics on incoming traffic on this interface.
- **Egress**. Select this option if you want to collect flow statistics on outgoing traffic on this interface.

Note: If you have selected to collect flow statistics from both Ingress and Egress traffic on a single interface, we recommend that you do not select to collect flow statistics from any other interface, otherwise traffic may be duplicated as traffic that is internally routed will appear on two interfaces within the device.

Enter the IP address and port number for the devices collecting Flow Monitor traffic.

- **IP address**. Enter the IP address of the collector.

- **Port**. Enter the Port number on which the collector is listening for flow data. (Default port for Flow Monitor: 9999)

Click **Update** to save the settings.

CHAPTER 3

Managing Flow Sources

In This Chapter

About Flow Sources

Flow *sources* are network devices that use one of the following supported network monitoring protocols to send flow data to Flow Monitor.

- **NetFlow**. A network protocol developed by Cisco Systems and later adopted as an IETF informational standard for collecting IP traffic information. Flow Monitor supports NetFlow versions 1, 5, 7, and 9 as well as Flexible NetFlow, which is based on NetFlow v9. Flexible NetFlow is often used to support Cisco's Network Based Application Recognition (NBAR) technology.
- **sFlow**. A network monitoring technology that provides IP traffic information using packet sampling. Flow Monitor supports sFlow versions 2 and 5.
- **JFlow**. A network protocol developed by Juniper to run on the JUNOSe for collecting IP traffic flow statistics.
- **IPFIX**. An IETF informational standard developed to create a non-proprietary network protocol that is compatible with NetFlow.

Flow sources that utilize these network protocols provide detailed data about individual flows to Flow Monitor gathered from flow records. An example of the types of information that can be contained in a flow record are:

- Version numbers
- Sequence numbers
- Input and output interface indices
- Timestamps for the flow start and finish time, in milliseconds since the last boot.
- Number of bytes and packets observed in the flow
- Layer 3 headers including:
- Source & destination IP addresses
- Source and destination port numbers

- IP protocol
- Type of Service (ToS) value
- The union of all TCP flags observed over the life of the flow (TCP flows).
- Layer 3 Routing information, including:
- IP address of the immediate next-hop along the route to the destination
- Source and destination IP masks (prefix lengths in CIDR notation)

Configuring Flow sources is a three-part process:

1. Configuring Flow devices to send Flow data to Flow Monitor. For more information, see *Manually configuring devices to export flow data to Flow Monitor* (on page 9).
2. Configure Flow Monitor to listen for flow data on the appropriate port. For more information, see *Configuring Flow Monitor to listen for NetFlow data* (on page 28).
3. Setting options for the Flow source in Flow Monitor.

SNMP Polling

While Flow Monitor normally receives flow data from a flow source, it can also poll a source using SNMP to gather data from a network device. Flow Monitor can actively poll a source for the following data:

- **Total interface traffic**. Provides summary data for incoming and outgoing interface traffic.
- **NBAR information**. Provides summary data for each application identified using Cisco Systems Network Based Application Recognition (NBAR) technology.
- **CBQoS information**. Provides summary data for each class in the Quality of Service class map for the interface. Before you can view meaningful reports, you must configure Flow Monitor and Flow-enabled devices, such as routers or switches, to communicate network activity back to the Flow Monitor listener application.

Configuring Flow Monitor to listen for NetFlow data

Use the Listener port settings on the Flow Settings to configure Flow Monitor to listen for NetFlow data. You can enter the TCP/IP port numbers which the Flow Monitor collector service should use to listen for flow information in the **Listener port** box. Flow Monitor can listen on one or more ports, with port 9999 being the default. The sources sending flow information to Flow Monitor must send data using one of these ports.

Note: If you configure Flow Monitor to listen on more than one port or on a port other than the default port, you should verify that the port is not being used by another service and ensure that an exception is added to the firewall if you are using Windows Firewall.

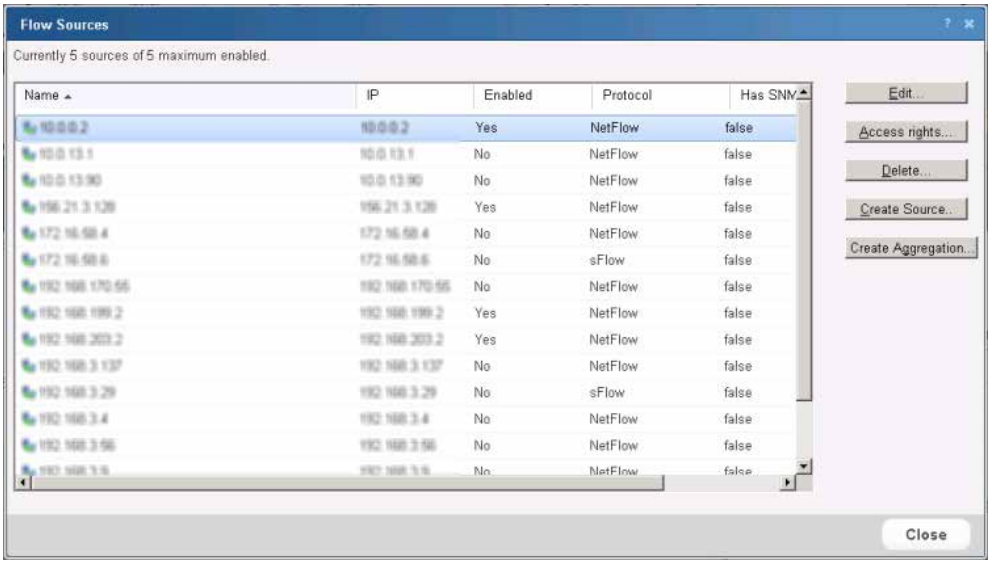
To configure Flow Monitor to listen for NetFlow data:

Note: By default, Flow Monitor listens for Flow data on port 9999. If you want to use that port, you do not need to perform this procedure.

1. Navigate to the Flow Settings dialog (**Flow Monitor > Settings**). The Flow Settings dialog appears.
2. In **Listener port**, enter the port numbers, separated by commas, over which Flow Monitor should listen for Flow data.
3. Click **OK** to save the changes.

Viewing Flow Sources

Use the Flow Sources dialog to view the list of all of the sources that are available in Flow Monitor. This list of sources is automatically updated when the system receives data from sources that have been configured to send flow data to Flow Monitor.



Use the Flow Sources dialog to:

- Access the Flow Source dialog for each change a source's configuration.
- Stop and start data collection from a source.
- Set access rights to the flow data generated by a source.
- Create an SNMP source.
- Create an Aggregate source.

To change a source's configuration, or to stop and start data collection from a source, select a source, then click **Edit**.

To set access rights to flow data from a source, select a source, then click **Access rights**.

Note: If you do not have permissions to manage users, the **Access rights** button is not be visible.

For more information, see Configuring Flow sources.

To Delete a Flow Source, see Deleting Flow Sources below.

Click **Create Source** to create an SNMP Source to poll for NBAR or CBQoS data.

Click **Create Aggregation** to create an Aggregate source.

Deleting Flow Sources

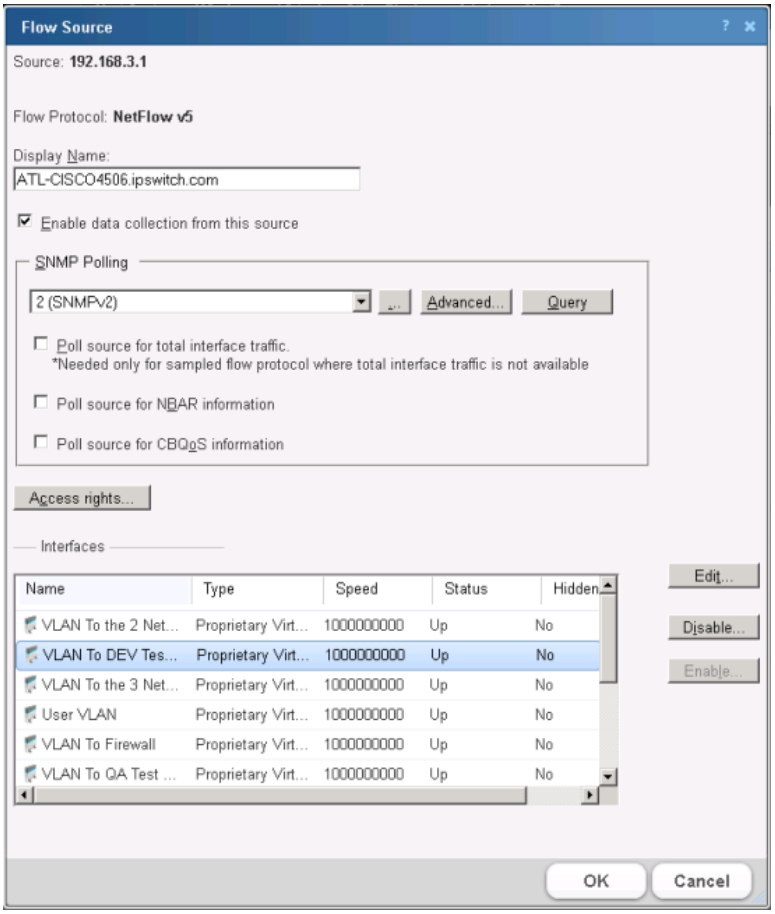
When you no longer want to gather flow data from a source, it can be deleted. When you delete a source, both the configuration information and all flow data associated with the source is deleted.

To delete a flow source:

1. Navigate to the Flow Sources dialog (**Flow Monitor > Flow Sources**).
2. Disable the source.
   a) On the Flow Sources list, select the source you want to delete.
   b) Click **Edit**. The Flow Source edit dialog appears.
   c) Clear the **Enable flow data collection from this source** option.
   d) Click **OK**. The Flow Sources list appears with the source listed as disabled.
3. Delete the source.
   a) Verify that the source you wish to delete is not enabled. The word *No* appears in the Enabled column when the source is not enabled.
   b) Click **Delete**. A delete verification dialog appears.
   c) Click **Yes** to verify that you want to delete the source. The Flow Sources list dialog appears with the source deleted.

Configuring a Flow Source

Use the Flow Source dialog to configure the selected source and the interfaces associated with the source.



The Flow Source dialog provides the options to:

- Enable and disable data collection.
- Configure Flow Monitor to use SNMP to poll the source for total interface traffic, NBAR and CBQoS statistics. You can then select the types of statistics you would like to collect.
- Set access rights to data generated by the source.
- Configure interface properties for interfaces attached to the source.

To navigate to the Flow Source dialog:

1. Navigate to the Flow Sources dialog (**Flow Monitor > Sources**).
2. Select the source you want to configure, then click **Edit**. The Flow Source dialog opens.

The source identifying information is displayed and in some cases can be edited:

- **Source**. The device (source) IP address.
- **Flow Protocol**. Indicates the flow protocol used by the source device.

- **Display Name**. The device (source) display name.

To enable or disable data collection from a source:

1. Select **Enable data collection from this source** to start receiving data from a newly configured, or previously disabled source. (Default).
2. Deselect **Enable data collection from this source**, to stop receiving data from this source.

Note: You must deselect Enable data collection from this source to delete a source. When you delete a source, you will no longer receive data from the source. All data you have collected prior to deleting the source will be maintained in the Flow Monitor database until it is aged out.

To use SNMP polling to collect data from the source:

1. In the SNMP Polling group, select the credential that is valid for the interface from the list, or click the browse (**...**) button to go to the Credentials Library to configure a new set of credentials.

Note: If you select a different set of credentials, the dialog automatically uses the new credentials to update information about the source interfaces. If you receive an error, click **Advanced** to update timeout and retry values, then click **Query** to try the credentials again.

- **Advanced**. Click to configure the device (source) SNMP timeout and retry settings.
- **Query**. Click to use the updated retry and timeout values for the selected SNMP credential.

2. If you want to poll the source for total interface traffic, select **Poll source for total interface traffic**.

Important: When you poll a source for interface traffic, the aggregate of the individual flows is not used to represent total interface traffic. Instead the polled value is used to represent total interface value.

Note: When a source uses packet sampling to collect flow data and the protocol does not provide total interface traffic statistics, the aggregate of individual flow data used to calculate total interface traffic will be inaccurate because the data used in the calculation is sampled, this commonly results in errors in total interface traffic statistics. In this case it is better to select the **Poll source for total interface traffic** to provide more accurate statistics.

Note: To poll a source for interface traffic, the proper SNMP credentials for the interface must be selected, and the NetFlow collector must be configured to collect data from this source.

3. If you want to poll the source for Network-Based Application Recognition (NBAR) statistics, select **Poll Source for NBAR Information**.

Note: The source device from which you want to gather NBAR statistics must be configured to generate NBAR statistics using the `<ip> nbar protocol-discovery` command. For more information, see *Configuring NBAR on a Cisco device* (on page 18).

4 If you want to poll the source for class-based Quality of Service (CBQoS) information, select **Poll Source for CBQoS information**.

Note: The source device from which you want to gather CBQoS statistics must be configured to generate these statistics. For more information, see *Configuring CBQoS on a Cisco device* (on page 19).

To set access rights for the source:

Click **Access Rights** to configure user access to the source and its associated data. The **Flow Source Access Rights** dialog appears. For more information, see *Configuring Flow Source Access Rights* (on page 35).

Note: If you do not have permissions to manage users, the **Access rights** button will not be visible.

Interfaces

Each of the Flow Monitor source's interfaces are listed in the Interfaces list. The following columns provide information about the source interface:

- **Name**. List the unique device interface name.

Note: In the case where the interface name is listed as *Null(0)*, this indicates one of two possibilities:
1) A router has dropped traffic, so traffic does not exit the router and the output interface is named Null(0). **OR** 2) When a router generated (originated) traffic, so traffic has not entered the router and the input interface is named Null(0). In both cases the ifIndex = 0 and as a default convention we name an interface = Null because the interface is none existent.

- **Type**. List the interface type. For example, Ethernet.
- **Speed**. List the interface speed in bits per second (bps).
- **Status**. List the current interface status (Up or Down).
- **Hidden**. List whether the interface is hidden from view on the Flow Monitor Home page (Yes or No) and Interface Details combo-box.

To configure flow interface properties:

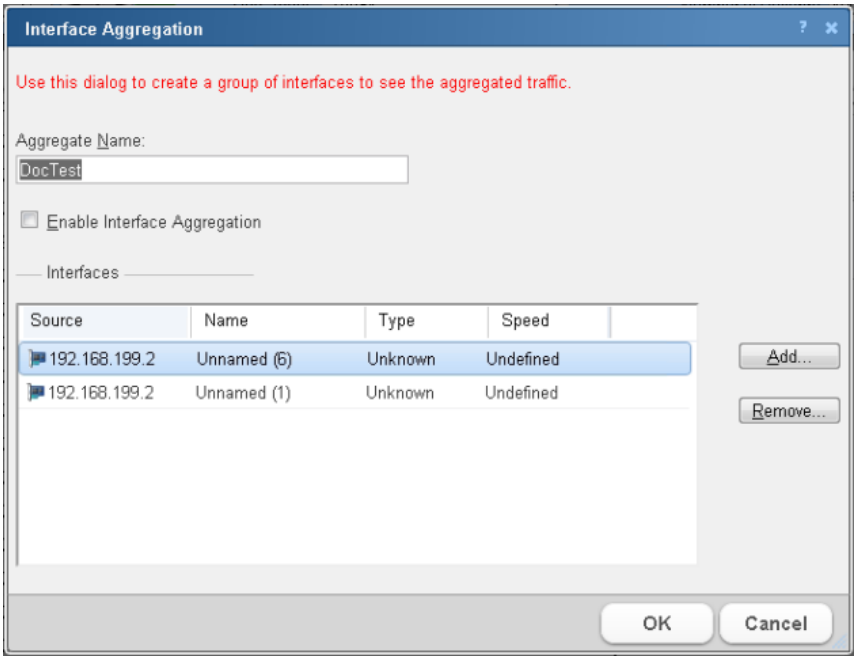
Select an interface from the Interfaces list, then click **Edit**. The Flow Interface dialog appears. For more information, see *Configuring Flow Interface Properties* (on page 36).

To enable/disable multiple interfaces at once:

Ctrl+click each interface name you want to enable/disable and click **Enable**/**Disable**.

Creating an Aggregate source

Use the Create Aggregation dialog to add one or more interfaces from any of the licensed Flow Monitor sources to an aggregate source. An aggregate source combines the data from all of the assigned interfaces, and reports on that data as if it originated from a single Flow Monitor source. This aggregation allows for reporting on data from many, or all, of the interfaces on your licensed Flow Monitor sources without having to manually add the data between reports from individual interfaces.



To create an aggregate source:

1. Navigate to the Flow Sources dialog (**Flow Monitor > Sources**).
2. Click **Create Aggregation**. The Interface Aggregation dialog appears.

Tip: If you want to edit an existing aggregate source, select the aggregate source from the source list and click **Edit**. The Interface Aggregation dialog appears.

3. In the Aggregate Name box, type a name for the aggregate source. This name will appear as the name of the source in the Flow Sources dialog.
4. Select **Enable Interface Aggregation**.

Note: When you enable an interface aggregation, it will use a Flow Monitor source license.

5. Click **Access rights** to set access rights to flow data from the Aggregate source.

Note: If you do not have permissions to manage users, the **Access rights** button is not be visible.

6 Click **Add** to add an interface to the aggregate source. The Add Interface dialog appears.

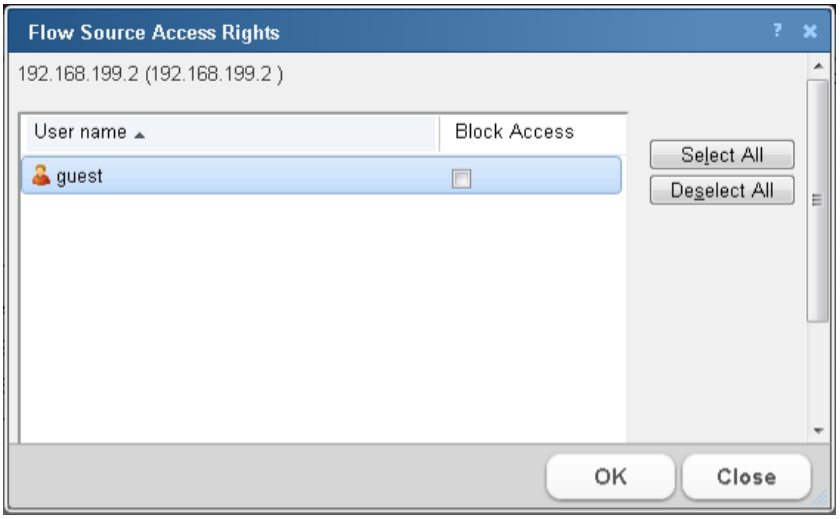
7 Select an interface to add, then click **OK**. The interface will be added to the Interfaces list on the Interface Aggregation dialog.

Tip: If you want to remove an interface from an aggregation, select the interface from the Interfaces list, then click **Remove**.

8 When you have added all of the interfaces you wish to combine using the aggregate source, click **OK**. The aggregate source appears on the Flow Sources list.

Configuring Flow source access rights

Use the Flow Source Access Rights dialog to block access by one or more users to the flow data generated by a particular Flow Monitor source.



Note: In order for a user to be able to block access for other WhatsUp Gold users, the user must have the Manage Users access right (**Admin > Manage Users**). Additionally, the user for which you are trying to block access should not have this right, as this will allow them to block access for other users.

To configure Flow Source access rights:

1 Navigate to the Flow Sources dialog (**Flow Monitor > Sources**).

2 Select the flow source for which you want to configure access rights, then click **Edit**. The Flow Source dialog for that source appears.

3 Click **Access rights**. The Flow Source Access Rights dialog appears.

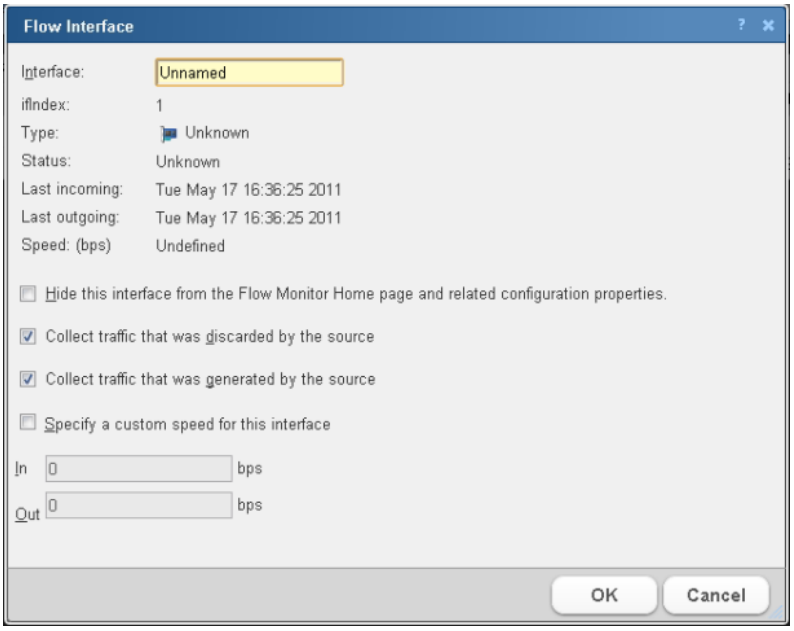
4 Select a user or multiple users from the list of usernames by clicking the Block Access box for that user or user(s).

5 Click **OK** to save changes.

Tip: You can also click **Select All** users to choose all available users, or **Deselect All** users to choose no users.

Configuring Flow interface properties

Use the Flow Interface dialog to view and configure the Flow Monitor properties attributed to the selected interface.



The Flow Interface dialog provides the options to:

- Hide the interface from Flow Monitor Home.
- Configure traffic collection options.
- Allow interface speed specification.
- Configure options for collecting translated addresses on Cisco Adaptive Security Appliance (ASA) devices.

To navigate to the Flow Interface Properties dialog:

1. Navigate to the Flow Sources dialog (**Flow Monitor > Flow Sources**).
2. In the Interfaces group, select the source to which the interface is connected, then click **Edit**. The Flow Source dialog appears.
3. Select the interface you want to edit, then click **Edit**. The Flow Interface dialog appears.

To hide this interface from the Flow Sources dialog:

1. Select **Hide this interface from the Flow Home page and related configuration properties** to hide the selected interface from the Flow Monitor Home page and other menu options in Flow Monitor. This lets you display only those interfaces that are relevant to your bandwidth monitoring requirements.

Note: While selecting this option hides the interface from the source list, Flow Monitor still collects data from the interface.

Tip: You can hide multiple interfaces at one time using the **Enable** and **Disable** buttons in the previous *Flow Source* (on page 31) dialog.

1 Click **OK** to save changes.

To configure traffic retention properties for the interface:

1 Select **Collect traffic that was discarded by the source** to collect data about the traffic that came to the device but was not forwarded by the device. Examples of this type of traffic are ping traffic, telnet connections, routing table updates, and other network management traffic or traffic that was not supposed to travers the device.

2 Select **Collect traffic that was generated by the source** to collect data about the network traffic that is generated by the device. Examples of this type of traffic are any traffic generated by routing protocols.

3 Click **OK** to save changes.

To configure the speed of an interface:

1 Select **Specify a custom speed for this interface**. The **In** and **Out** boxes are enabled.

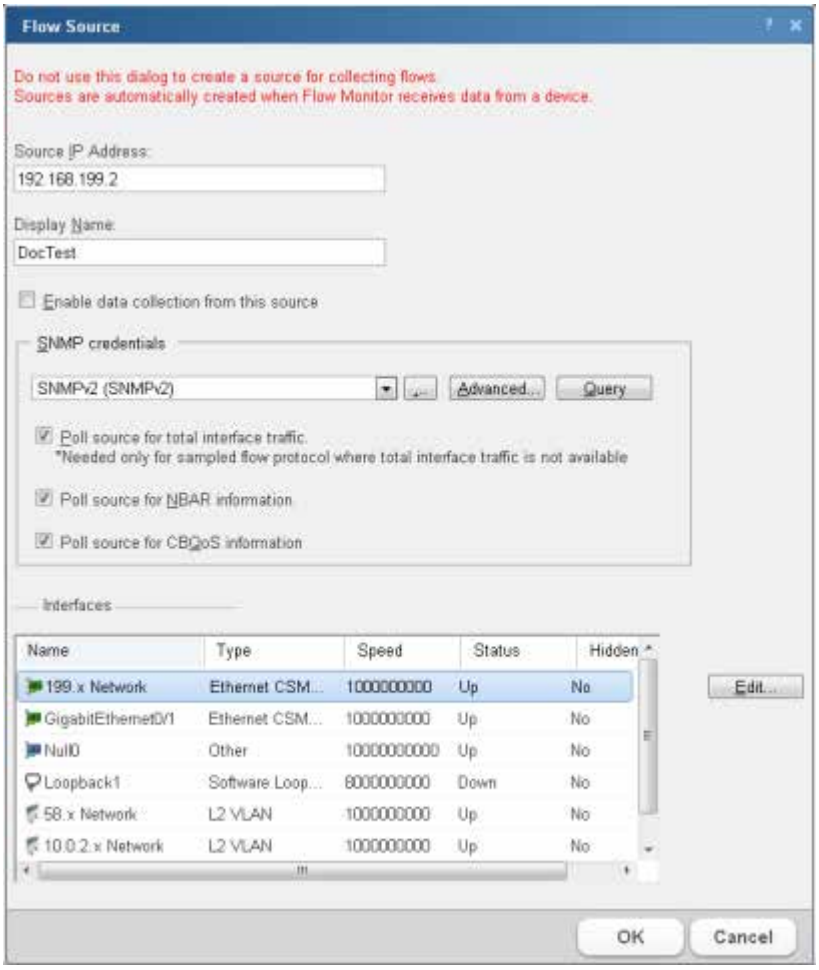
In **In** and **Out**, enter the upper limit of the interface in bps (bits per second). Common interface speeds expressed in bps are:

- 1 Gbps = 1,000,000,000 bps
- 100 Mbps = 100,000,000 bps
- 10 Mbps = 10,000,000 bps

2 Click **OK** to save changes.

Creating flow sources

Use the Flow Source dialog to manually create SNMP sources when detailed flow data is not needed or is unavailable for a particular source.



You can manually create a flow source and configure it to use SNMP to collect the following types of data:

- Total counts for incoming and outgoing interface data.
- CBQoS information.
- Total counts for NBAR data.

To create an SNMP source:

1. Navigate to the Flow Source creation dialog (**Flow Monitor > Sources**).
2. Click **Create Source**. The Flow Source dialog appears.
3. Identify and enable the flow source.
   a) In the **Source IP Address** box, type the IP address of the device you want to make a Flow Monitor source.
   b) In the **Display Name** box, type the name you want to use to identify the flow source.

c) Select **Enable data collection from this source** (this will use a source license).

4 Set SNMP options.

Note: Flow Monitor uses SNMP to query information about the interfaces on the source.

a) Select the appropriate **SNMP credentials**. If the credentials you want to use are not included in the list, click the browse button (**...**) to open the Credentials Library. For more information on configuring credentials, see *Using Credentials* in the WhatsUp Gold User Guide.

b) To set advanced options, such as timeout and number of retries, click **Advanced**. The Advanced dialog appears. Set the appropriate values, then click **OK** to return to the Flow Sources dialog.

c) Select **Query** to query the router using SNMP to get updated names and speeds for available interfaces.

5 Select the data you want to gather using SNMP polling.

§ To collect total interface data, select **Poll source for total interface traffic** (this option is usually not needed).

§ To collect NBAR information, select **Poll source for NBAR information**.

§ To collect CBQoS information, select **Poll source for CBQoS information**.

6 Configure the speed of each interface, which is used to calculate capacity as a percentage of the total interface speed.

a) Select an interface, then click **Edit**. The Flow Interface dialog appears.

b) Select **Hide this interface from the Flow Monitor Home page and related configuration properties** to hide the selected interface from the Flow Monitor Home page and other menu options in Flow Monitor. This lets you display only the interfaces that are relevant to your bandwidth monitoring requirements.

Note: Null(0) interface names are hidden by default because they are not a true source interface. Null(0) interfaces show traffic that a router has dropped or traffic that a router has generated. In both cases the ifIndex = 0 and as a default convention we name an interface = Null because the interface is none existent. If you want Null(0) interface information to display as a source interface, make sure that you uncheck the **Hide this interface from the Flow Monitor Home page and related configuration properties** option.

c) Select **Specify a custom speed for this interface**. The **In** and **Out** boxes are enabled.

d) In **In** and **Out**, enter the upper limit of the interface in bps (bits per second). Common interface speeds expressed in bps are:

§ 1 Gbps = 1,000,000,000 bps

§ 100 Mbps = 100,000,000 bps

§ 10 Mbps = 10,000,000 bps

7 Click **OK** when you have completed configuring the SNMP flow source. The Flow Source dialog closes and the source is added to the Flow Sources list.

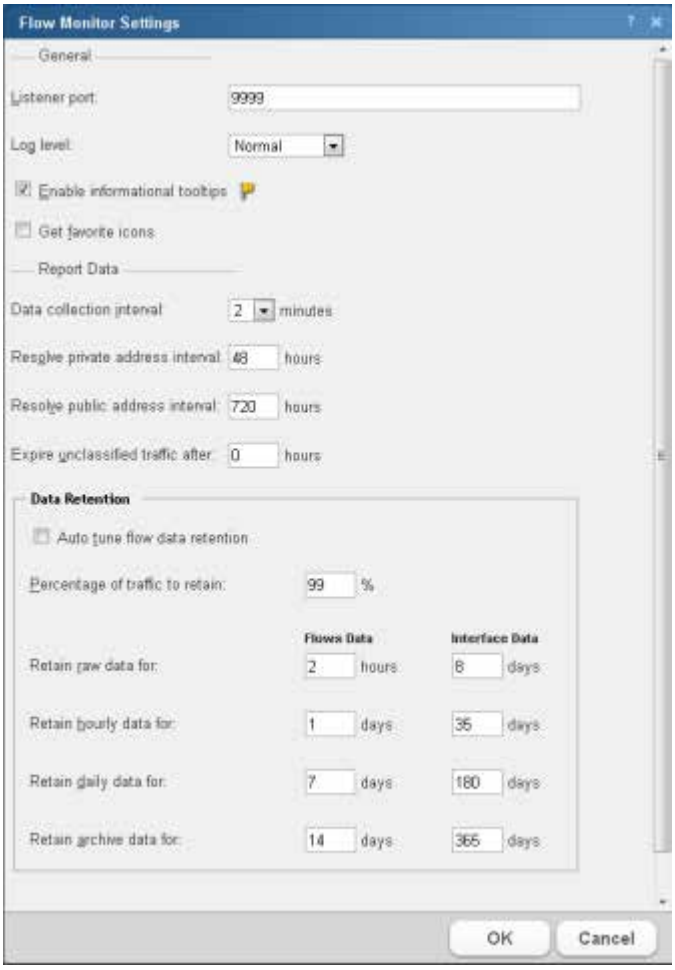
CHAPTER 4

Managing Flow Monitor Settings

In This Chapter

Flow Monitor settings

The Flow Monitor Settings dialog provides general settings, data retention, and data management settings used to configure and manage Flow Monitor.



General

- **Listener port**. Enter the TCP/IP port numbers which the Flow Monitor collector service should use to listen for flow information. Flow Monitor can listen on one or more ports, with port 9999 being the default. The sources sending flow information to Flow Monitor must send data using one of these port numbers.

Note: If you configure Flow Monitor to listen on more than one port, or on a port other than the default port, you should verify that the port is not being used by another service. Additionally, if you are using Windows Firewall, ensure that an exception is added to the firewall.

- **Log level**. Select the level of details you want to write to the log.
  - **Normal**. Select this option to record errors and some general event information.

- **Verbose Logging**. Select this option to record more detailed information than normal logging. This option can create a very large file and may be resource intensive, however, it is especially helpful for troubleshooting issues.
- **Errors Only**. Select this option to record only errors.

- **Enable informational tooltips**. Select this option to enable Flow Monitor to display tooltips with information about possible problems and other information about report details.
- **Get favorite icons**. Select this option to allow Flow Monitor to retrieve and display favicons (favorite icons) from hosts and domains when they are provided.

Note: If you select the **Get favorite icons** option, Flow Monitor makes connections to a host in the domain to retrieve the favicon. This impacts the connections statistics for both the host and the domain.

Report Data

- **Data collection interval**. Select how often Flow Monitor writes raw data from its sources to the database. You may select 1, 2, 3, 4, 5, or 10 minutes. By default, raw data is written to the database every 2 minutes.

Note: Modifying collection interval settings affects the granularity you see in Flow Monitor reports. If the interval is set to 5 minutes, you cannot distinguish traffic collected during the first minute from traffic collected during the fourth minute.

- **Resolve private address interval**. When the Flow Monitor collector service encounters an IP address, it tries to determine information about the host attached to the IP address. After this information is resolved, it is stored in the Flow Monitor database. Enter the interval (in hours) that you want Flow Monitor to wait, before it checks the private IP address again, to resolve information that may have changed for the address. By default, private addresses are resolved every 48 hours.
- **Resolve public address interval**. When the Flow Monitor collector service encounters an IP address, it tries to determine information about the host attached to the IP address. After this information is resolved, it is stored in the Flow Monitor database. Enter the interval (in hours) that you want Flow Monitor to wait, before it checks the public IP address again, to resolve information that may have changed on the address. By default, public addresses are resolved every 720 hours (30 days).

Tip: Because public IP addresses are less likely to be changed, you may want to use longer intervals than used for the **Resolve private address interval** option.

- **Expire unclassified traffic after**. Enter the number of hours after which Flow Monitor should purge unclassified traffic. Unclassified traffic is traffic transmitted over ports that are currently not monitored by Flow Monitor. By default, this option is set to 0 (zero), which causes Flow Monitor to aggregate and retain data for all unclassified ports as a single value; detailed information about the individual unclassified ports over which traffic was transmitted is immediately discarded.

Important: Be cautious about increasing the time for **Expire unclassified traffic after** value because the database can grow very large as the time is increased.

Note: The collector will purge any unclassified data that has no activity after the **Expire unclassified traffic after** value is satisfied.

You can use the data retention section of the Flow Monitor Settings dialog to set data retention parameters for flow and interface data. Periodic roll-up and archival of flow data minimizes system resources needed for data storage and improves system responsive during data intensive operations.

Data retention settings

Flow data includes many parameters (input and output interfaces, source and destination IP addresses, port numbers, byte rates, flow end times, etc.) which while useful in providing information may quickly fill available storage. Rolling up the data makes for efficient storage, but there may be losses of time related information within individual flows. Flow Monitor provides a data retention scheme that allows the user to choose to either manually tune data retention or to allow Flow Monitor to automatically tune the retention of flow data, which in turn actively manages the growth rate of the Flow Monitor databases. The following parameters are used to control the cleanup of flow data.

- **Auto tune flow data retention**. Select this option if you want Flow Monitor to automatically tune the flow data cleanup settings to manage database size and system performance. This option is selected by default.
- **Percentage of traffic to retain**. Use this option to determine the percentage of raw traffic the collector will write to the database. This option is enabled when you clear the **Auto tune flow data retention** check box.

Caution: While the default settings for data cleanup are conservative, when you modify the roll-up settings it can directly affect the size of the Flow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, and monitor the effects of changes to these settings on database size and application performance.

Note: When you place the cursor in a box to change a value, a message appears at the bottom of the dialog. This message provides information about the number and percentage of the recommended maximum flow records being stored in the Flow Monitor data and archive databases. As you make changes, the message predicts how the change affects the number of records stored in the Flow Monitor data and archive databases.

- **Retain raw data for**. Enter the number of hours of raw flow data you would like to maintain. This setting establishes a sliding time window of raw data that spans the specified period. Raw data that reaches the end of the period is rolled up. The roll up of raw data happens every hour on the hour. After data has been rolled up, Flow Monitor can only report using the hourly summations. By default, raw data is rolled up after 4 hours.

- **Retain hourly data for**. Enter the number of days you would like to maintain hourly data. This setting establishes a sliding time window of hourly data that spans the specified number of days. As hourly data ages beyond this period it is rolled up. The roll up of hourly data takes place daily. After hourly data is rolled up, Flow Monitor can only report aggregated totals for the entire 24-hour block of time. By default, hourly data is maintained for 1 day.
- **Retain daily data for**. Enter the number of days of daily data you would like to maintain before archiving. This setting establishes a sliding time window of daily data that spans the specified number of days. As daily data ages beyond this period, it is archived. Flow Monitor continues to have visibility into archived data with some restrictions. By default, daily data is archived after 3 days.
- **Retain archive data for**. Enter the number of days of daily data you would like to maintain in the archive database. This setting establishes a sliding time window of archived daily data that spans the specified number of days. As the archived daily data ages beyond this period it is purged from the database. After archived data is purged, Flow Monitor can no longer report on the data. By default, archive data is purged from the database after 7 days.

Interface Data Retention Settings

Raw interface data is provided by the flow collector, or the collector can be configured to collect raw interface data directly from the network device when the collector is receiving sampled flow data. This raw interface data is used to represent total interface traffic for the period and to calculate 95th percentile values for the Interface Overview and Interface Usage reports. Because of the data compaction, interface data has a smaller impact on data storage, so it can be maintained for longer periods of time.

The following parameters are used to control the clean up of interface data.

- **Retain raw data for**. Enter the number of days of raw interface data you would like to maintain. This setting establishes a sliding time window of raw interface data that spans the specified number of days. As raw interface data ages beyond this point it is rolled up. After data has been rolled up, Flow Monitor can only report using the summations produced in the roll-up process. By default, raw interface data is rolled up after 8 days.

Caution: While the default settings for data cleanup are conservative, when you modify the roll-up settings it can directly affect the size of the Flow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, and monitor the effects of changes to these settings on database size and application performance.

Important: If 95th percentile values are going to be used for billing purposes, you should maintain a set of raw interface data that matches the billing period to ensure accurate results. To gather the data needed to calculate the 95th percentile values for the interface, set the **Roll up raw data after** setting for Interface Data to match or exceed the billing period.

- **Retain hourly data for**. Enter the number of days you would like to maintain hourly interface data. This setting establishes a sliding time window of hourly interface data that spans the specified number of days. As hourly data ages beyond this period it is rolled up. The roll up of hourly interface data takes place daily. After hourly interface data is rolled up, Flow Monitor can only report aggregated totals for the entire 24-hour block of time. By default, hourly interface data is maintained for 35 days.
- **Retain daily data for**. Enter the number of days of daily interface data you would like to maintain before archiving. This setting establishes a sliding time window of daily interface data that spans the specified number of days. As daily interface data ages beyond this period, it is archived. Flow Monitor continues to have visibility into archived interface data. By default, daily interface data is archived after 180 days.
- **Retain archive data for**. Enter the number of days of daily interface data you would like to maintain in the archive database. This setting establishes a sliding time window of archived daily interface data that spans the specified number of days. As the archived daily interface data ages beyond this period it is purged from the database. After archived interface data is purged, Flow Monitor can no longer report on the data. By default, archive interface data is purged from the database after 365 days.

Click **OK** to save changes.

Configure Flow Monitor to listen for NetFlow data

Use the Listener port settings on the Flow Settings to configure Flow Monitor to listen for NetFlow data. You can enter the TCP/IP port numbers which the Flow Monitor collector service should use to listen for flow information in the **Listener port** box. Flow Monitor can listen on one or more ports, with port 9999 being the default. The sources sending flow information to Flow Monitor must send data using one of these ports.

Note: If you configure Flow Monitor to listen on more than one port or on a port other than the default port, you should verify that the port is not being used by another service and ensure that an exception is added to the firewall if you are using Windows Firewall.

To configure Flow Monitor to listen for NetFlow data:

Note: By default, Flow Monitor listens for Flow data on port 9999. If you want to use that port, you do not need to perform this procedure.

1. Navigate to the Flow Settings dialog (**Flow Monitor > Settings**). The Flow Settings dialog appears.
2. In **Listener port**, enter the port numbers, separated by commas, over which Flow Monitor should listen for Flow data.

Click **OK** to save the changes.

Setting the logging level

Use the Flow Settings dialog to specify the level of information that is recorded for the Flow Log.

Note: The logging level that you specify on the Flow Settings dialog determines the level of data that Flow Monitor records, whereas the logging level that you specify on the Flow Log report page determines the level of data displayed within the report.

Important: Keep in mind that if you choose the Normal or Errors Only levels, you will not be able to view the Verbose level from the Flow Log report page.

To set the Flow Monitor logging level:

1. Navigate to the Flow Settings dialog (**Flow Monitor > Settings**). The Flow Settings dialog appears.
2. Under General, select the **Log level**.
   - **Normal**. Select this option to record errors and some general event information.
   - **Verbose Logging**. Select this option to record more detailed information than normal logging. This option can create a large number of records and may be resource intensive; it is only recommended for use while troubleshooting issues.
   - **Errors Only**. Select this option to record only events that register as errors.
3. Click **OK** to accept changes.

Data retention strategy and tuning

Flow Monitor can process millions of NetFlow records per minute from NetFlow enabled devices and the Flow Publisher, while also gathering interface data through direct SNMP polling of individual devices. The number of flow records retained in raw form directly impacts the size of the Flow Monitor databases and performance of data intensive operations such as report generation and display. Flow Monitor uses data compression, culling, and archival strategies to minimize the impact data retention has on system storage and operations. The following diagram illustrates the different stages of the data retention strategy and the relative impact of each stage on the number of flow records stored in the Flow Monitor databases.

Initial data compression

The first step of the data retention strategy is accomplished during the interval between collections of the raw data. Flow records with the same key data that occur during the interval between consecutive data collections are consolidated into a single flow record. This results in a small reduction in records, with a longer data collection interval creating a larger reduction. Use the **Data collection interval** option to adjust this interval.

Raw data compression

Raw data compression happens during the hourly roll-up. Each hour an hour's worth of raw NetFlow records are aged out of the hourly retention period and are compressed into a single record. While the start and stop times for individual flows may be lost, this compression provides an initial savings in data storage. Use the **Retain raw data for x hours** option to determine how long you want to maintain raw data before rolling it up into an hourly data records.

Culling flow data

The next step in the retention strategy is to cull the flow data so that the smallest flow records are removed from the data to be stored. This is done by ordering the flow records by size, and retaining a percentage of the total number of flow records, based on the size in bytes of the traffic represented by the number of bytes reported by the flows. The system is configured to maintain between 97 and 99 percent of the flow records by size (number of bytes), discarding the bottom 1-3 percent of the flow traffic. While the discarded records represent only a small percentage with respect to the total number of bytes represented by the flow data, they can represent thousands of individual flow records in environments where there are many dropped connections, port scans, or other activity resulting in flows with small byte counts. By culling these records, we can see a large reduction in storage requirements, and a corresponding increase in performance of data intensive operations, all with a minimal reduction in data retention. This culling of flow data takes place when the collector writes raw records and when doing roll-ups from raw to hourly data and from hourly data to daily data. Use the **Percentage of traffic to retain** option to set the percentage of the flow data you want to retain.

Daily flow data compression

Following this culling of data, a data compression takes place during the daily roll-up. Each day, a days worth of hourly roll-ups are aged out of the daily retention period, and are compressed into a single record for the day. Use the **Retain hourly data for x days** option to determine how long you want the hourly roll-up records to be maintained in the Active Flow Monitor database, before they are rolled-up into a daily record.

Flow data archival

Finally, each day, daily data is archived. This archival removes daily data that has aged out of the daily retention period. Each day during the daily roll-up, a daily record is written to the NetFlow Archive and is removed from the NetFlow Active database. Use the **Retain daily data for x days** option to determine how long you want the daily roll-up records maintained in the Active Flow Monitor database before they are archived in the Flow Monitor Archive database.

Data retention tuning

Data retention can be tuned manually, by adjusting the **Data collection interval**, **Percentage of traffic to retain**, and the retention periods for the various stages of the data retention strategy (Raw flow data, hourly flow data and daily flow data), or it can be tuned automatically by selecting the **Auto tune flow data retention** option.

When you have enabled auto tuning of the system (**Auto tune flow data retention** option is selected), the system adjusts the data retention periods to maintain the number of records within a normal range that optimize data storage and system performance. Using information gathered from the database, Flow Monitor approximates the growth rate of the database, and adjusts the retention settings to ensure that the total size of the database is maintained in the recommended band of a minimum of 1 million to a maximum of 10 million flow records. The recommended band is based on storage requirements for each stage in the data retention strategy.

When you manually adjust the Data Retention settings (**Auto tune flow data retention** option is cleared), you are presented with guidance in the message area at the bottom of the dialog as you adjust each setting. This feedback provides you with information about how the current, or proposed setting affects the database size with respect to the maximum recommended database size (10 million records). For the raw data, hourly data, and daily data, the maximum recommended database size is compared against all of the data in these categories and is based on the size of the Flow Monitor Active database. For the Archive daily data after setting, the guidance is based on the size of the Flow Monitor Archive database.

Configuring data retention settings

Flow Monitor is designed to serve two primary purposes:

- To give a minute-by-minute view of recent network traffic.
- To give an overview of historical network traffic.

To accomplish these goals while keeping the size of its database reasonable, Flow Monitor uses a process of summarizing data at certain time intervals.

By default, Flow Monitor rolls up data on this schedule:

- Complete raw data (which is collected every other minute and provides the detailed view of recent traffic) is kept for 4 hours.
- After 4 hours, raw data is summarized into hourly averages.
- After 1 days, hourly averages are summarized into daily averages.
- After 3 days, daily data is archived.
- After 7 days, archive data is purged from the archive database.

To configure the data collection interval:

1. Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).
2. In the **Data collection interval** box, select how often you want Flow Monitor to write raw data from its sources to the Flow Monitor Active database. You may select 1, 2, 3, 4, 5, or 10 minutes. By default, raw data is written to the database every 2 minutes.
3. Click **OK**. The setting is saved and the Flow Monitor Settings dialog closes.

To configure address resolution intervals:

1. Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).
2. In the **Resolve private address interval** box, enter the interval (in hours) that you want Flow Monitor to wait before it checks a private IP address to resolve information that

may have changed for the address since the last private address lookup. By default, private addresses are resolved every 48 hours.

3 In the **Resolve public address interval** box, enter the interval (in hours) that you want Flow Monitor to wait before it checks a public IP address to resolve information that may have changed for the address since the last public address lookup. By default, public addresses are resolved every 720 hours.

4 Click **OK**. The setting is saved and the Flow Monitor Settings dialog closes.

To configure unclassified traffic collection:

1 Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).

2 In the **Expire unclassified traffic after** box, enter the number of hours after which Flow Monitor should purge unclassified traffic. Unclassified traffic is traffic transmitted over ports that are currently not monitored by Flow Monitor. By default, this option is set to 0 (zero), which causes Flow Monitor to aggregate and retain data for all unclassified ports as a single value; detailed information about the individual unclassified ports over which traffic was transmitted is immediately discarded.

3 Click **OK**. The setting is saved and the Flow Monitor Settings dialog closes.

To configure flow data retention:

1 Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).

2 If you want to allow Flow Monitor to automatically manage your data retention settings, select **Auto tune flow data retention** to automatically tune the flow data cleanup settings to manage database size and system performance. This option is selected by default. For more information on tuning flow data retention, see *Data retention strategy and tuning*.

3 If you want to manually manage your data retention settings, clear **Auto tune flow data retention** and set the following settings:

Note: When you manually adjust the Data Retention settings (**Auto tune flow data retention** option is cleared), you are presented with guidance in the message area at the bottom of the dialog as you adjust each setting. This feedback provides you with information about how the current, or proposed setting will affect the database size with respect to the maximum recommended database size (10 million records). For the raw data, hourly data, and daily data, the maximum recommended database size is compared against all of the data in these categories and is based on the size of the Flow Monitor Active database. For the Archive daily data after setting, the guidance is based on the size of the Flow Monitor Archive database.

- **Percentage of traffic to retain**. Use this option to determine the amount of the total hourly data you want to maintain during the hourly roll-up. This option is enabled when you clear the Auto tune flow data retention check box.

Caution: While the default settings for data cleanup are conservative, when you modify the roll-up settings it can directly affect the size of the Flow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, and monitor the effects of changes to these settings on database size and application performance.

- **Retain raw data for**. Enter the number of hours of raw flow data you would like to maintain. This setting establishes a sliding time window of raw data that spans the

specified period. Raw data that reaches the end of the period is rolled up. The roll up of raw data happens every hour on the hour. After data has been rolled up, Flow Monitor can only report using the hourly summations. By default, raw data is rolled up after 4 hours.

- **Retain hourly data for**. Enter the number of days you would like to maintain hourly data. This setting establishes a sliding time window of hourly data that spans the specified number of days. As hourly data ages beyond this period it is rolled up. The roll up of hourly data takes place daily. After hourly data is rolled up, Flow Monitor can only report aggregated totals for the entire 24-hour block of time. By default, hourly data is maintained for 1 day.
- **Retain daily data for**. Enter the number of days of daily data you would like to maintain before archiving. This setting establishes a sliding time window of daily data that spans the specified number of days. As daily data ages beyond this period, it is archived. Flow Monitor continues to have visibility into archived data with some restrictions. By default, daily data is archived after 3 days.
- **Retain archive data for**. Enter the number of days of daily data you would like to maintain in the archive database. This setting establishes a sliding time window of archived daily data that spans the specified number of days. As the archived daily data ages beyond this period it is purged from the database. After archived data is purged, Flow Monitor can no longer report on the data. By default, archive data is purged from the database after 7 days.

4 Click **OK**. The setting is saved and the Flow Monitor Settings dialog closes.

To configure interface data retention:

1 Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).

2 Set the following settings to tune your interface data retention:

Note: Raw interface data is used to represent total interface traffic for the period and to calculate 95th percentile values for the Interface Overview and Interface Usage reports. Because of data compaction, interface data has a smaller impact on data storage, so it can be maintained for longer periods of time.

- **Retain raw data for**. Enter the number of days of raw interface data you would like to maintain. This setting establishes a sliding time window of raw interface data that spans the specified number of days. As raw interface data ages beyond this point it is rolled up. After data has been rolled up, Flow Monitor can only report using the summations produced in the roll-up process. By default, raw interface data is rolled up after 8 days.

Caution: While the default settings for data cleanup are conservative, when you modify the roll-up settings it can directly affect the size of the Flow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, and monitor the effects of changes to these settings on database size and application performance.

Important: If 95th percentile values are going to be used for billing purposes, you should maintain a set of raw interface data that matches the billing period to ensure accurate results. To gather the data needed to calculate the 95th percentile values for the interface, set the Roll up raw data after setting for Interface Data to match or exceed the billing period.

- **Retain hourly data for**. Enter the number of days you would like to maintain hourly interface data. This setting establishes a sliding time window of hourly interface data that spans the specified number of days. As hourly data ages beyond this period it is rolled up. The roll up of hourly interface data takes place daily. After hourly interface data is rolled up, Flow Monitor can only report aggregated totals for the entire 24-hour block of time. By default, hourly interface data is maintained for 35 days.
- **Retain daily data for**. Enter the number of days of daily interface data you would like to maintain before archiving. This setting establishes a sliding time window of daily interface data that spans the specified number of days. As daily interface data ages beyond this period, it is archived. Flow Monitor continues to have visibility into archived interface data. By default, daily interface data is archived after 180 days.
- **Retain archive data for**. Enter the number of days of daily interface data you would like to maintain in the archive database. This setting establishes a sliding time window of archived daily interface data that spans the specified number of days. As the archived daily interface data ages beyond this period it is purged from the database. After archived interface data is purged, Flow Monitor can no longer report on the data. By default, archive interface data is purged from the database after 365 days.

Important: Any changes made to data roll up intervals are not enforced until the Flow Monitor collector service is restarted. For more information, see *Stopping or restarting the collector* (on page 67).

CHAPTER 5

Configuring Applications

In This Chapter

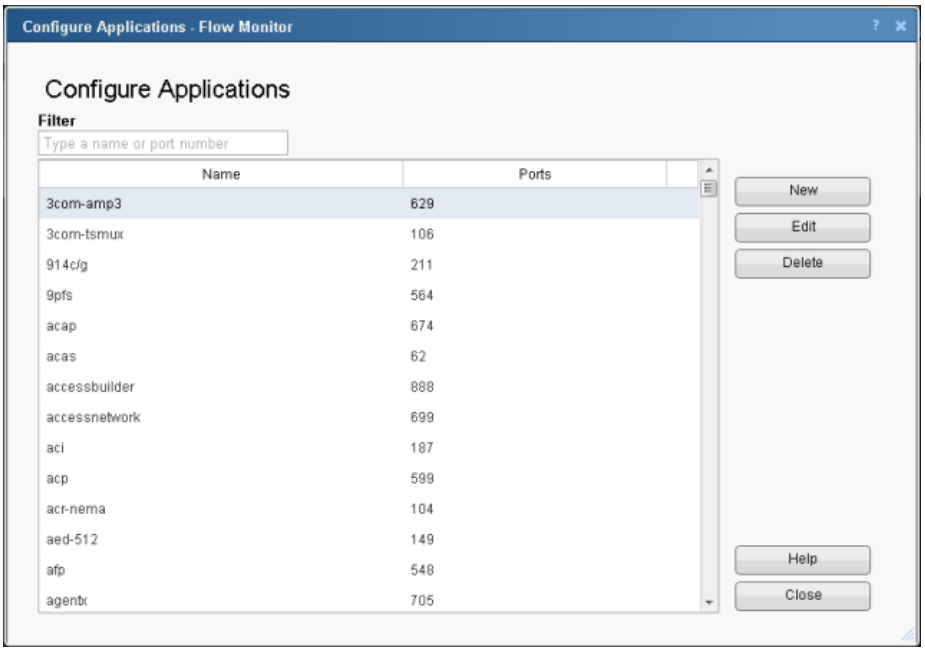
Configuring applications

Use the Configure Applications dialog to create application definitions. Application definitions create a mapping between one or more ports and an application. These port mappings are applied either globally, for all IP addresses, or for a defined subnet. This *network scoping* allows application definitions to have global scope, where the definition is valid for all hosts in a network, or limited scope, where the definition is valid only for a defined subnet.

Flow data is compared with the application definition and is associated with the application based on the following criteria:

- If the network scope is limited to a defined subnet, a flow is classified as belonging to an application when a port number in either the source or destination IP-port pair matches a port mapped to the application, and the corresponding IP address falls within the defined subnet.
- If the network scope is global, a flow is classified as belonging to an application when a port number in either the source or destination IP-port pair matches a port mapped to the application.

The application classified flow data is then used to create the Top Applications report. This report is a Top "n" report that provides the bandwidth and percentage of the interface throughput used by each identified application.



The Configure Applications list provides the following information:

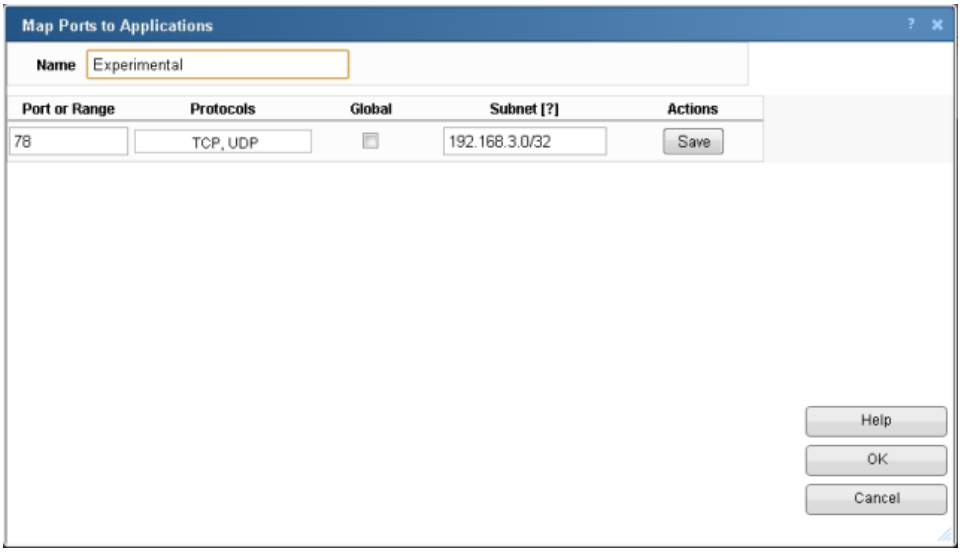
- **Name**. Displays the name assigned to the application. This name can simply identify the application, or it can provide additional information to identify a specific instance of the application.
- **Ports**. Displays the first port associated with the application. If the application definition has more than one port associated with an application, the port will be displayed in parenthesis.

The following controls are provided for filtering, adding, editing and deleting application definitions.

- **Filter**. Enter an application name or port number to filter the application definitions.
- Click **New** to create a new application definition. The Map Ports to Application dialog appears.
- Select an application definition, then click **Edit** to modify an existing application definition. The Map Port to Application dialog appears.
- Select an application definition, then click **Delete** to remove an existing application definition. A delete confirmation message appears. Click **Yes**. The application definition is deleted.
- Click **Close** to close this dialog.

Mapping ports to applications

Use the Map Ports to Application dialog to define applications using port mapping. You can name the application, assign ports and protocols, and define the scope of the application definition within the network. You can map a port or port range to a network, subnet, or individual host. This allows you to configure a port for an application globally (port 80 for http) and on a single host (port 80 for http on 192.168.3.33).



- **Name**. Enter the name of the application. This name can also be used to define an instance of the application that is applied to a specific subnet which is defined in the subnet box.
- **Port**. Enter a port number, or range of port numbers to be mapped to the application. For each port, you can select the protocol and the network scope to be applied.
- **Protocols**. Select the transport protocols used to provide services to the application.
- **Global**. Select this option if port to application mapping is to be applied to the entire network. When this option is selected, the Subnet box is not active. When this option is not selected, the Subnet box is active and a subnet can be defined.
- **Subnet**. When the Global option is not selected this option is available. Use this box to define the subnet to which the application definition is to be applied. The format for defining the subnetwork is the standard Classless Inter-Domain Routing (CIDR) format (10.0.0.0/8). You can map the port(s) to a single host by using a /32 subnet mask.
- **Actions**. The icons displayed in this column provide you with controls to edit or delete a port entry in the application definition.

Monitoring traffic on non-standard ports

Flow Monitor automatically classifies traffic for most common applications. However, in some cases, you may need to create a custom definition to ensure that Flow Monitor properly classifies some traffic. This need is most common when:

- Your device routes traffic for applications that use a proprietary protocol. This may be a custom program that uses a protocol developed in-house to send data across the network or a third-party application that uses its own custom protocol to transmit data.
- Your device routes traffic for standard applications over non-standard ports. Examples include a standard Web server running on a port other than 80 or an FTP client connecting to an FTP server that runs on a port other than 21.

Note: In Flow Monitor, for traffic to be considered "unclassified," both the port from which the data is sent, and the receiving port must not be configured in the Flow Ports dialog. If either the sending or receiving port is classified, the traffic is associated with the application of the classified port.

To accommodate these cases, you can classify traffic that meets specific rules so that Flow Monitor reports that traffic as belonging to a certain application.

Important: You can configure the amount of time unclassified traffic data is kept. For more information, see *Configuring data roll-up intervals* (on page 48).

Tip: If Flow Monitor detects a large amount of traffic to an unmonitored port, the Top Applications dashboard report displays a yellow warning flag that explains the situation and guides you in defining the unmonitored port. This can help you to proactively detect emerging non-standard traffic on your network. You can also use the Unclassified Traffic dialog (available from any page in Flow Monitor by selecting **Configure > Flow Unclassified Traffic**) to view all unclassified traffic rollup.

To define rules for classifying traffic that uses non-standard ports:

1. On the WhatsUp Gold web interface, click **Flow Monitor > Applications**. The Applications dialog appears.
2. Click **New** to configure a new port definition. The Flow Port dialog appears.
3. In **Port**, enter the port number over which the traffic will be sent.
4. In **Application**, enter a name for the traffic that you are classifying. This should be the name of the protocol (for instance, the definition for port 80 includes HTTP as the application).
5. Select **Monitor the following protocols on this port**, and then select the protocols that the application uses (**TCP**, **UDP**, or **SCTP**).
6. Click **OK** to save changes.

CHAPTER 6

Configuring Flow Groups

In This Chapter

Using Flow groups

In some cases, you may prefer to track a range of IP addresses as belonging to a different domain, top level domain, or country than the IP addresses resolve to. For example, internal IP addresses do not usually have host names registered on a domain name server, so Flow Monitor cannot automatically determine their domains, top level domains, or countries.

To overcome this limitation, Flow Monitor lets you use Groups to override the domain, top level domain, and country of ranges of IP addresses so that each group can be tracked as a whole. This allows you to easily track sections of your internal network so that you can view reports by divisions, departments, or other groupings.

Tip: After you configure a group, you can use that group's name to filter reports to show only the traffic sent to or received by devices that belong to the group.

To create or edit a group:

1. Navigate to the Flow Groups dialog (**Flow Monitor > Groups**). The Flow Groups dialog appears.
2. Click **New**. The Flow Group dialog appears.

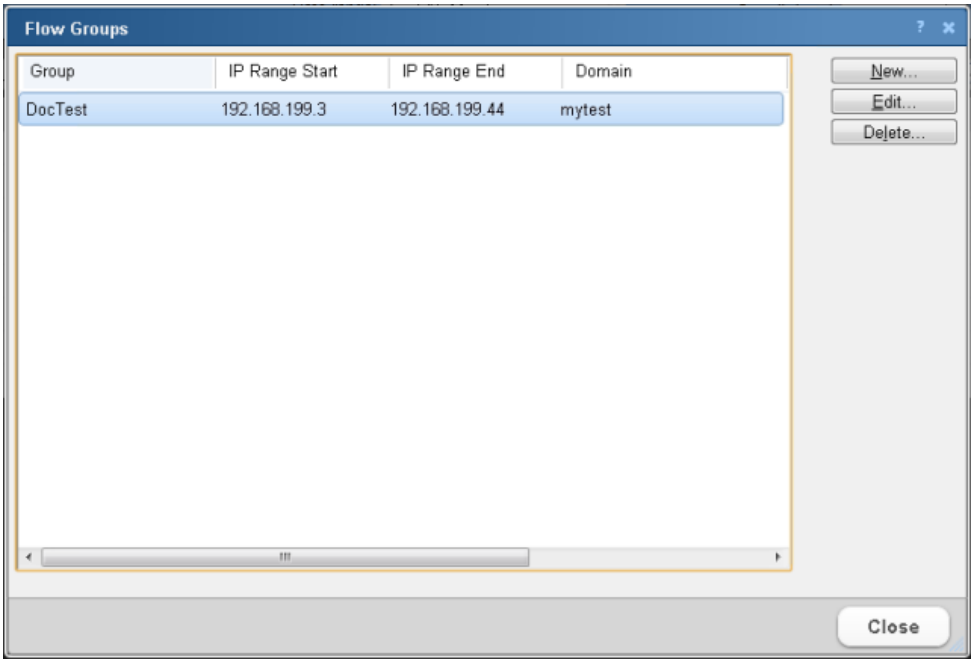
   - or -
   Select a group, then click **Edit**. The Flow Group dialog appears.
3. Enter or select the appropriate information:
   - **Group**. Enter a name for the Flow group.
   - **IP Range Start**. Enter the first IP address for the Flow source group range.
   - **IP Range End**. Enter the last IP address for the Flow source group range.
   - **Domain**. Enter the domain that you want Flow Monitor to report for the specified IP addresses. For example, `yourcompany.com`.
   - **Top Level Domain**. Select the domain that you want Flow Monitor to report for the specified IP addresses. For example, `com`.

- **Country**. Select the country that you want Flow Monitor to report for the specified IP addresses.

4 Click **OK** to save changes.

Using Flow groups

The Flow Groups dialog lists all of your Flow Groups by **Name**, **IP Range**, **Domain**, **Top Level Domain**, and **Country**.



Groups allow you to reclassify groups of devices as belonging to a specific domain, top level domain, and country.

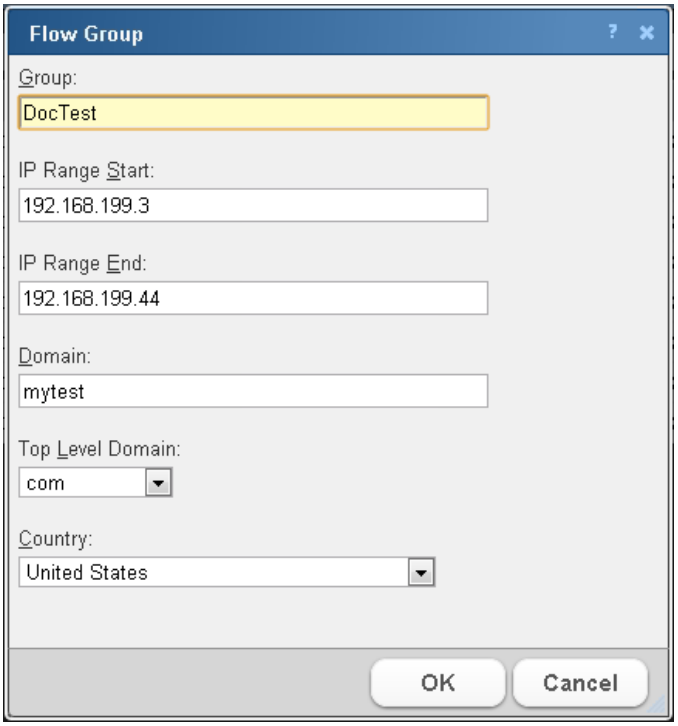
Use this dialog to create, change, and delete Flow groups. After you define a Flow group, the devices associated with the group can be filtered by keywords or viewed as groups in dashboard reports.

To use this dialog:

- To create a new Flow Group, click **New**.
- To change an existing group, select a group, then click **Edit**.
- To remove a group, select a group, then click **Delete**.

Using the Flow Group dialog

Use this dialog to configure a group. Groups allow you to reclassify groups of devices as belonging to a specific domain, top level domain, and country.



Tip: You can group devices that are not automatically associated with a domain, top level domain, or country. For example, you may have a range of local network devices that you want to associate with yourcompany.com.

Enter or select the appropriate information:

- **Group**. Enter a name for the Flow group.
- **IP Range Start**. Enter the first IP address for the Flow source group range.
- **IP Range End**. Enter the last IP address for the Flow source group range.
- **Domain**. Enter the domain that you want Flow Monitor to report for the specified IP addresses. For example, yourcompany.com.
- **Top Level Domain**. Select the domain that you want Flow Monitor to report for the specified IP addresses. For example, com.
- **Country**. Select the country that you want Flow Monitor to report for the specified IP addresses.

Click **OK** to save changes.

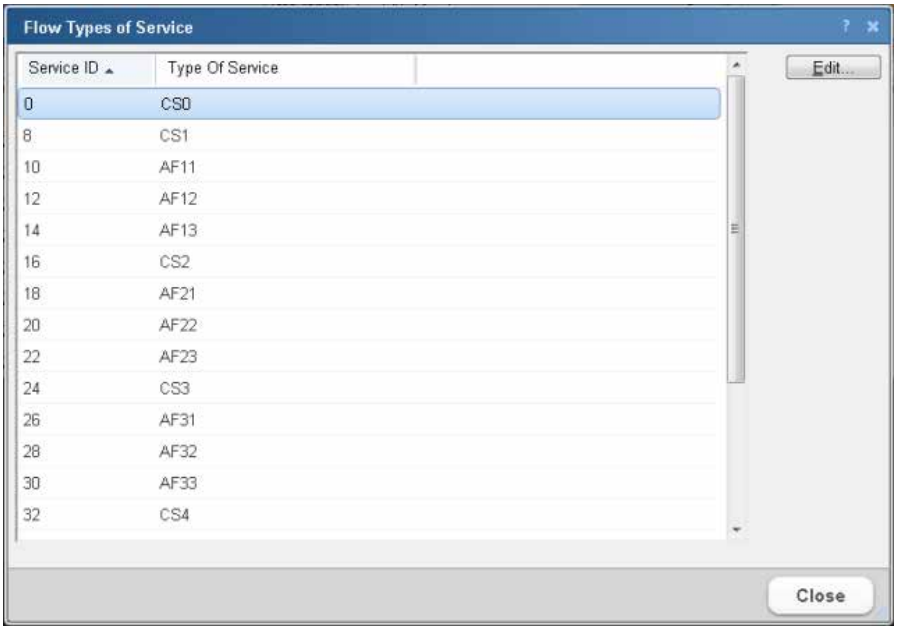
CHAPTER 7

Configuring Type of Service

In This Chapter

Flow Types of Service

The Flow Types of Service dialog lists the Flow Types of Service and their associated service IDs. Types of Service (ToS) is a part of an IP specification that allows routers to use routing protocols that help optimize how data is routed (according to the type of service requested). The ToS is assigned by the routers on your network.



You can assign service type display names to make the Top Types of Service dashboard report more meaningful to you. By default Flow Monitor is configured with the standard types of service.

Renaming a Type of Service

To rename a Type of Service, select it from the list, then click **Edit**.

Editing Flow Type of Service

Use The Edit Type of Service dialog to assign a display name to a Type of Service.

- **Type of service ID**. This is a numeric value that is automatically assigned by the router.
- **Type of service name**. Enter the desired ToS display name. The name assigned here will be displayed in the Flow Types of Service dialog, and the Top Types of Service dashboard report.

Click **OK** to save changes.

CHAPTER 8

Managing unclassified traffic

In This Chapter

Classifying traffic that is considered unclassified

In Flow Monitor, for traffic to be considered "unclassified," both the port from which the data is sent, or the source port, and the receiving, or destination port, are not classified in the Configure Applications dialog. If either the source or destination port is classified, the traffic is associated with the application of the classified port.

You can classify traffic that is considered unclassified by classifying the source and/or destination ports over which the traffic is transmitted via the Flow Unclassified Traffic dialog.

To classify a source port:

1. Navigate to the Unclassified Traffic dialog (**Flow Monitor > Unclassified Traffic**). The Unclassified Traffic dialog appears.
2. Use the list boxes at the top of the dialog to manipulate the port data displayed in this dialog.
   - Select an **Interface** over which unclassified traffic is transmitting.
   - Select a **Traffic direction** (*Inbound*, *Outbound*, *Inbound and Outbound*, *Bounce*) in which the unclassified traffic is traveling.
   - Select a group (*Conversations*; *Source IP*, *Port*; *Source Port*; *Destination IP*, *Port*; *Destination Port*) by which to group the unclassified traffic from the **Group by** box.
   - Select a **Date range** for a specific time period for unclassified traffic.
   - Select a **Number of Records** for unclassified traffic.
3. To begin monitoring a source port, select the port from the list, then click **Classify Src Port**.

To classify a destination port:

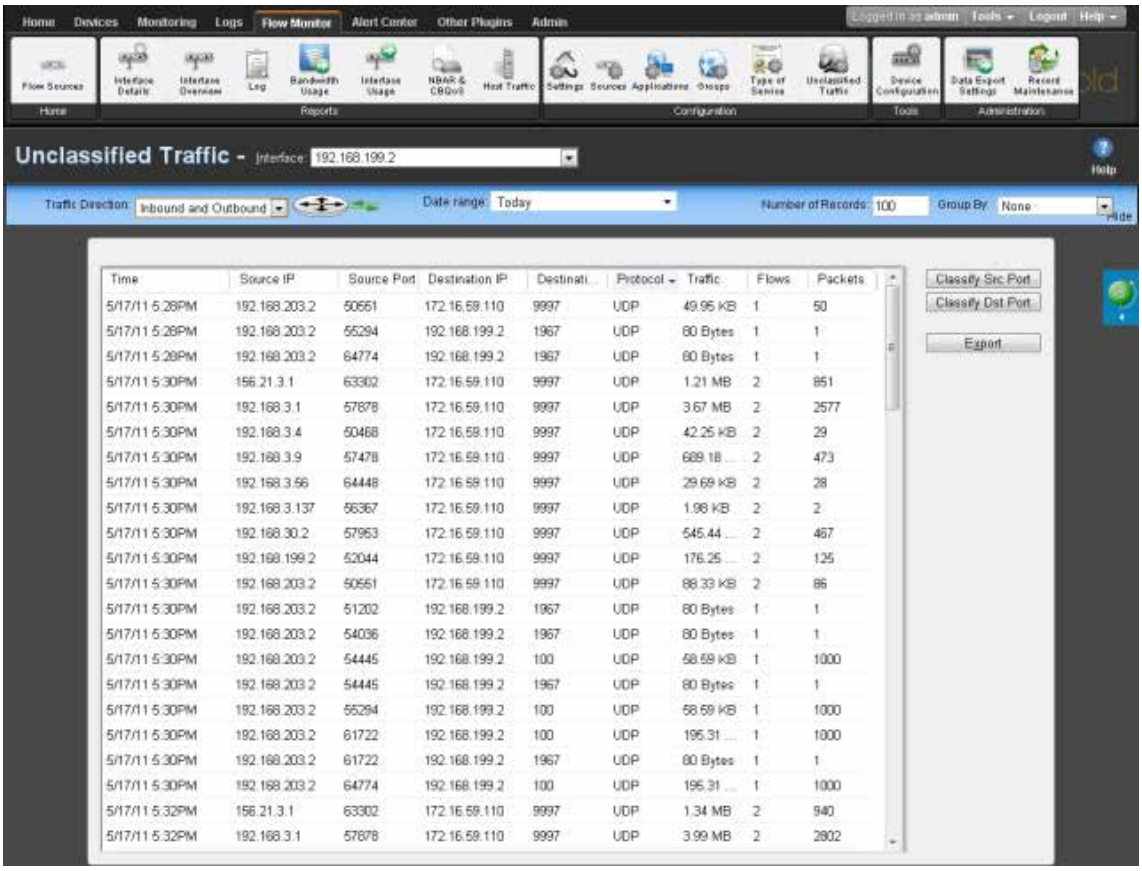
1. Navigate to the Unclassified Traffic dialog (**Flow Monitor > Unclassified Traffic**). The Unclassified Traffic dialog appears.
2. Use the list boxes at the top of the dialog to manipulate the port data displayed in this dialog.
   - Select an **Interface** over which unclassified traffic is transmitting.

- Select a **Traffic direction** (*Inbound*, *Outbound*, *Inbound and Outbound*, *Bounce*) in which the unclassified traffic is traveling.
- Select a filter (*Conversations*; *Source IP*, *Port*; *Source Port*; *Destination IP*, *Port*; *Destination Port*) by which to group the unclassified traffic from the **Group by** box.

3 To begin monitoring a destination port, select the port from the list, then click **Classify Dst Port**.

Using the Flow Unclassified Traffic dialog

Use the Unclassified Traffic dialog to view unclassified traffic by the interface over which the traffic is transmitted.



Note: The ports listed in this dialog have not been mapped to any application. The traffic displayed is the total in bytes for the period since the last hourly roll up time.

Note: In Flow Monitor, for traffic to be considered "unclassified," both the port from which the data is sent, or the source port, and the receiving, or destination port, must not be classified in the Flow Ports dialog. If either the source or destination port is classified, the traffic is associated with the application of the classified port.

The dialog displays unclassified traffic data in the following boxes.

- **Time**. The time which the traffic data was received.
- **Source IP**. The IP from which traffic originates.
- **Source Port**. The port from which traffic originates.
- **Destination IP**. The IP to which traffic is sent.
- **Dst. Port**. The destination port, or port to which traffic is sent.
- **Protocol**. The protocol used to send the traffic.
- **Traffic**. The amount of traffic (in bytes) sent during the conversation between the source IP and the destination IP.

Manipulating dialog data

Use the list boxes at the top of the dialog to manipulate the port data displayed in this dialog.

- Select an **Interface** over which unclassified traffic is transmitting.
- Select a **Traffic direction** (Inbound, Outbound, Inbound and Outbound, Bounce) in which the unclassified traffic is traveling.
- Select the **Date range** for which you want the report to display data.
- Type the **Number of Records** you want the report to display.
- Select a group (Conversations; Source IP, Port; Source Port; Destination IP, Port; Destination Port) by which to group the unclassified traffic from the **Group by** box. Select **None** to display unclassified traffic as it is received.

Classifying ports

If you want to classify a port so that Flow Monitor monitors the port for inbound or outbound traffic, select one of the following options:

- To begin monitoring a source port, select a port from the list, then click **Classify Src Port**.
- To begin monitoring a destination port, select a port from the list, then click **Classify Dst Port**.

Note: After you classify a new source or destination port, only the new traffic will display under the newly classified port(s). Any previously unclassified traffic will not be displayed under the newly classified port(s).

Exporting the Unclassified Traffic report

Click **Export** to create a PDF file containing the contents of the Unclassified Traffic report. You can save the file, or view the file in a PDF viewer.

CHAPTER 9

Configuring Data Export Settings

In This Chapter

Configuring Flow export settings

Use the Flow Export Settings dialog to set the parameters for exporting data from Flow Monitor. You can export data to a text file, Microsoft Excel, or a PDF.

- Select **Export to Text** to export Flow data to text.
- Select **Export to Excel** to export Flow data to Microsoft Excel.
- Select **Export to PDF** to export data to PDF.
- Select **Include report title** to include the report name in the exported data.
- Select **Include column names** to include the column titles in the exported data.
- Select **Include graphs** to include graph(s) with the exported data (available on select reports).

When exporting data to text, set the **Text options**.

- Select the **Column delimiter** that separates the table columns; choose either comma, semicolon, tab, or vertical bar.
- Select the **Text qualifier** in which table text is wrapped; choose either double quote, single quote, or none.

Click **OK** to save changes.

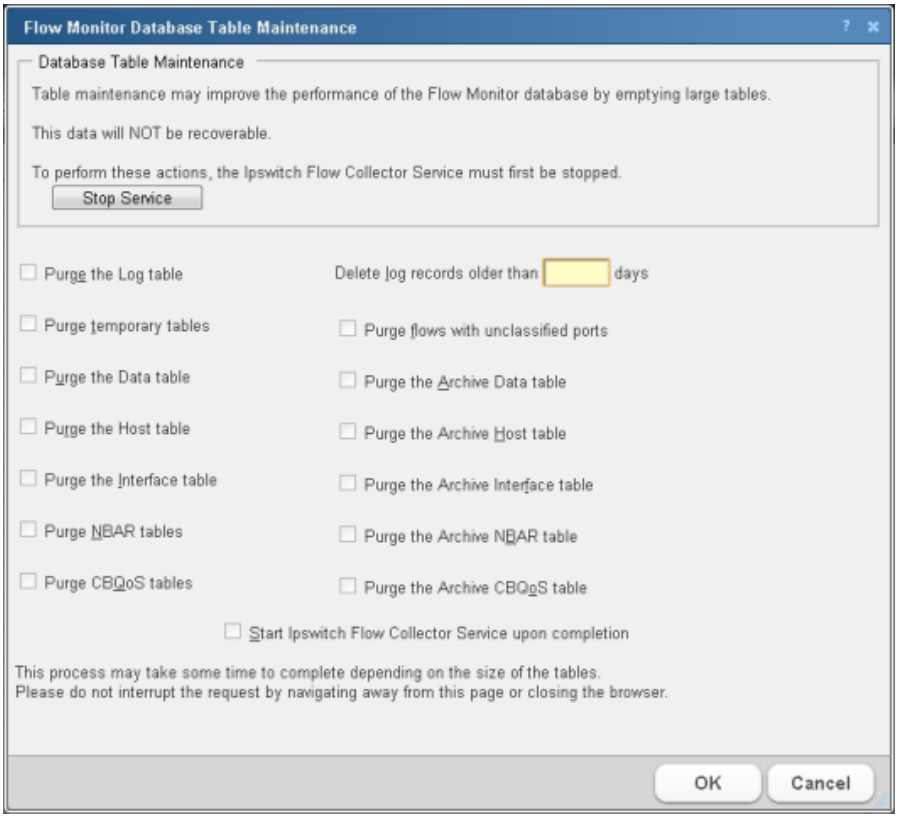
CHAPTER 10

Maintaining Flow Databases

In This Chapter

Configuring Flow database table maintenance

Use the Flow Database Table Maintenance dialog to perform table maintenance on the Flow Monitor database and archive database.



Regularly purging database tables can improve performance of Flow Monitor.

Important: Purged data cannot be recovered. Make sure that you export and save any Flow data you need for your records.

Stopping the Ipswitch Flow Collector service

To perform any of the purge actions listed in this dialog, you must first stop the Flow Collector service.

Click **Stop service** to stop the collector while you perform database maintenance.

Selecting items to purge

When the Ipswitch Flow Collector service has been stopped, you can select the Flow Monitor database tables you want to purge.

- **Purge the log table**. Select this option to purge the log table. The log table holds messages generated by Flow Monitor about the status of Flow Monitor, as well as errors and warnings that have occurred during operations.
- **Purge temporary tables**. Select this option to purge host update and flush tables. These tables temporarily hold data during the configuration and flushing of flow data.
- **Purge the Data table**. Select this option to purge flow data. This table holds flow data gathered from the NetFlow exporter on the Flow Monitor source, this information includes source and destination IP addresses, with traffic values in number of flows, packets and bytes.
- **Purge the Host table**. Select this option to purge host data. This table holds information on hosts discovered during the processing of flow information, and successfully resolved using DNS.
- **Purge the Interface table**. Select this option to purge interface traffic data. This table holds information about interface traffic, including traffic values in number of flows, packets and bytes.
- **Purge NBAR tables**. Select this option to purge NBAR information gathered by Flow Monitor. These tables hold information gathered using NBAR, including application identification as well as traffic values in number of packets and bytes.
- **Purge CBoS tables**. Select this option to purge CBoS information. These tables hold information defining class maps as well as information about the effectiveness of policies based on the defined classes. The effectiveness of the policy is measured by comparing the traffic values in packets, bytes and bit-rate prior to the application of the policy with the traffic values after the application of the policy.
- **Purge flows with unclassified ports**. Select this option to purge flows with unclassified ports from the Data table. Ports are classified by mapping the port to an application.
- **Purge the Archive Data table**. Select this option to purge archived flow data. This table holds archived flow information, includes source and destination host identification as well as traffic values in number of flows, packets and bytes.
- **Purge the Archive Host table**. This table holds archived host information discovered during the processing of flow information.

- **Purge the Archive Interface table**. Select this option to purge interface traffic data. This table holds archived information about interface traffic, including traffic values in number of flows, packets and bytes.
- **Purge the Archive NBAR table**. Select this option to purge NBAR information gathered by Flow Monitor. This table holds archived information gathered using NBAR, including application identification as well as traffic values in number of packets and bytes.
- **Purge the Archive CBQoS table**. Select this option to purge archived CBoS information. These tables hold archived CBQoS information about the effectiveness of policies based on the defined classes.

Maintaining log data during a purge

You can configure Flow Monitor to keep a given number of days of log data during a purge of the Log table.

Enter the number of days of logs you want Flow Monitor to maintain in **Delete log records older than** *xx* **days**. Log data that is older than the configured number of days will be purged from the Log table.

Restarting the Ipswitch Flow Collector service

After you have selected or configured all of the appropriate database table maintenance tasks, select **Start Ipswitch Flow Collector service upon completion**. This restarts the service so that Flow data collection can resume.

Review your selections, then click **OK** to begin database maintenance. The database maintenance process could be lengthy depending on the size of the tables in your Flow Monitor database and archive database.

Important: Do not navigate away from this page or close the Web browser until the process finishes completely. Failure to wait on the process to complete may result in database corruption or data loss.

Stopping or restarting the collector

You can restart the Flow Collector Service through WhatsUp Gold, and Windows.

To restart the Flow Collector Service through WhatsUp Gold:

From the WhatsUp Gold web interface, (**Admin > Admin Panel**) select the Flow Collector service, then click **Stop** or **Restart**.

To stop or restart the Flow Collector through the WhatsUp Services Controller:

1 Go to the WhatsUp Services Controller dialog.

- From the WhatsUp Gold console, go to **Tools > Services Manager**. The WhatsUp Services Controller dialog appears.
  - or -
- From the the Programs menu, click **Ipswitch WhatsUp Gold > Utilities > Service Manager**. The WhatsUp Services Controller dialog appears.

2 In the WhatsUp Services Controller, select **Flow Collector**.

3 Click **Stop** or **Restart**.

Backing up and restoring the Flow Monitor databases

You can use the WhatsUp Gold database utilities to back up and restore the WhatsUp Flow Monitor database and archive database.

To access the database utilities:

From the WhatsUp Gold console main menu, click **Tools > Database Utilities**.

Using the database backup and restore backup utility for Flow Monitor

You can back up your complete Flow Monitor SQL Server database and archive database to any mapped directory you have on your network. Database backups are saved as `.bak` files and can be restored at any time. Restoring a `.bak` file overwrites your current database with the data in a `.bak` file.

Important: You can use this feature with any local instance of SQL Server (default databases are named `Netflow` and `NFArchive`). This feature does not work with remote databases.

Important: We strongly suggest that you backup and restore the Netflow database and archive database as a set. When you backup the Netflow database, you should also backup the archive database. Similarly, when you restore the Netflow database, you should restore the archive database to the version that was most recently generated by the Netflow database.

If you want to back up the SQL database to a mapped drive, the Logon settings for the SQL Server must have write access to the mapped drive (default database name for Flow Monitor is `NETFLOW` and the default database name for Flow Monitor archive is `NFArchive`).

To change the SQL database logon settings:

1 Click **Start > Control Panel > Administrative Tools > Services**, then double-click the SQL Server (`NETFLOW` or `NFArchive`) service. The SQL Service Properties dialog appears.

2 Click the **Log On** tab on the Properties dialog.
3 Change the account logon settings as required.

Note: This is a complete backup and restore, so any change that you make after the backup will be overwritten and lost after restoring a backup.

To access the Database Utilities Backup and Restore features:

From the main menu in the WhatsUp Gold console, click **Tools > Database Utilities > Back Up Flow Monitor Current** or **Archive Database**.
- or -
click **Tools > Database Utilities > Restore Flow Monitor Current** or **Archive Database**.

CHAPTER 11

Managing users and user rights

In This Chapter

Managing users and user rights

User accounts and user rights serve two purposes in Flow Monitor:

- User rights govern who can access Flow Monitor reports from, or add Flow Monitor dashboard reports to, the main WhatsUp Gold web interface.
- User rights govern who can modify the Flow Monitor configuration.

To grant a user the right to view Flow Monitor reports and data:

Note: To complete this procedure, you must be logged in as a user who has been granted the Manage Users right in WhatsUp Gold.

1. Click **Admin > Manage Users**. The Manage Users dialog appears.
2. Select the user to which you want to grant rights to view Flow Monitor reports, then click **Edit**. The Edit User dialog appears.
3. Under User rights, in the Flow Monitor section, select **Access Flow Reports**.
4. Click **OK** to save changes.

To grant a user the right to configure Flow Monitor:

1. Click **Admin > Manage Users**. The Manage Users dialog appears.
2. Select the user you want to allow to configure Flow Monitor, then click **Edit**. The Edit User dialog appears.
3. Under User rights, in the Flow section, select **Configure Flow Monitor**.
4. Click **OK** to save changes.

To block a user from viewing Flow Monitor data for a specific Flow Monitor source:

1. Click **Admin > Flow Sources**. The Flow Sources dialog appears.
2. Select a source, then click **Access Rights**. The Flow Source Access Rights dialog appears.
3. To block a user or multiple users, select the specific user(s) from the list of usernames by clicking inside a check box in the Block Access column.

Tip: You can **Select All** users, or **Deselect All** users.

4. Click **OK** to save changes.

Note: In order for a user to be able to block access for other WhatsUp Gold users, the user must have the Manage Users access right. Additionally, the user for which you are trying to block access for should not have this right, as this will allow them to block access for other users.

For more information on managing user accounts, see *Managing Users* in the WhatsUp Gold User Guide.

CHAPTER 12

Using Flow Monitor reports

In This Chapter

About the Flow Monitor Reports group

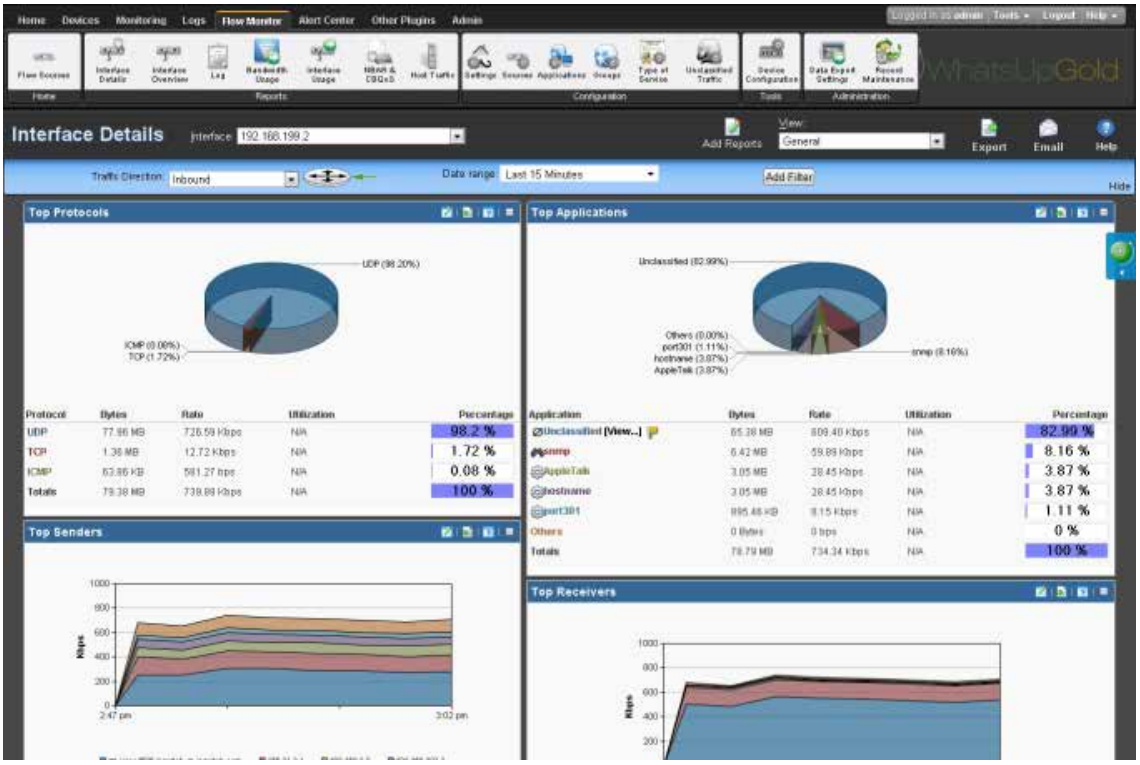
The Flow Monitor Reports group lists the available Flow Monitor reports.

- Interface Details
- Interface Overview
- Flow Monitor Log
- Bandwidth Usage
- Interface Usage
- *NBAR & CBQoS* (on page 95)

To view a report, double-click its title in the list.

About the Interface Details report

The Interface Details report is a collection of dashboard reports that provide insight into the traffic flowing through a specific interface.



When you first access the Interface Details report, it shows the General view for all traffic on the selected interface. You can refine the report in several ways.

- **Select a different interface**. Use the **Interface** list at the top of the page to select the interface for which the report data displays.
- **Changing the traffic direction**. Use the **Traffic direction** list at the top of the page to select a direction for which the report data is displayed.
- **Selecting a different date range**. Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 78).
- **Filter report results**. You can filter the current dashboard reports to show only data matching search criteria. For more information, see *Filtering by keywords* (on page 79). You can also drill-down into certain report entries. For more information, see *Filtering by drilling-down* (on page 80).
- **Managing report views**. Use the **Dashboard View** list at the top of the page to switch between the pre-configured report view and report views you've configured, or to create new report views.

Note: sFlow data is sent every x number of packets (configurable on the sFlow device), whereas typically *all* NetFlow data is collected and monitored. This means that sFlow data provides a sampling of network traffic data, whereas Flow data provides all network traffic data.
sFlow data sampling methods may result in Interface Overview and Interface Detail reports that appear to have more or less traffic than is shown in the Flow Monitor Home page source information. This is because the sampled data shown in the Interface Overview and Interface Detail reports are derived the sampled data and the Flow Monitor Home page source information is derived from the total interface traffic data.

For more information on how to refine the low Interface Details report, see *Filtering data in a view* (on page 77).

Tip: You can view the **Interface Overview** report for the selected interface by clicking Interface Overview at the top of the page.

General view

The Flow Monitor Interface Details' main view is the General view. The General view displays an overview of traffic for the selected interface.

By default, the report contains the following Interface Details dashboard reports:

- Top Protocols
- Top Applications
- Top Senders
- Top Receivers
- Top Conversations

You can add additional Interface Details dashboard reports to the General view, or delete an existing dashboard report from both the **Edit Layout** button and the **Dashboard View** list. For more information, see *Managing report views* (on page 76).

Tip: Click **Edit Layout** to add a dashboard report to the currently selected dashboard view.

Note: Sender dashboard reports are displayed on the left side of the report, while receiver dashboard reports are displayed on the right side. A page with no sender or receiver reports displays dashboard reports in one column.

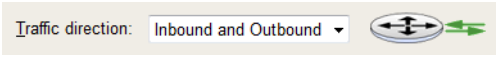
About the Flow Interface Details report

The Interface Details report is a collection of dashboard reports that provide insight into the traffic flowing through a specific interface.

General is the main view for the Flow Interface Details report.

When you first access the Flow Interface Details report, it shows the *General* (on page 74) view for all traffic on the selected interface. You can refine the report in several ways.

- **Select a different interface**. Use the **Interface** list at the top of the page to select the interface for which the report data displays.
- **Changing the traffic direction**. By default, the Flow Interface Details report displays information about traffic inbound to the selected interface. Use the **Traffic direction** list at the top of the page to select a direction for which the report data is displayed. The router icon to the right of the **Traffic direction** list illustrates what direction traffic is traveling in relation to the source. For more information about traffic direction, see Filtering by traffic direction.



- **Selecting a different date range**. Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 78). You can also change the report date and time by using the Report Zoom Tool. For more information, see Report Zoom Tool.

Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

- **Filtering the results by a keyword**. Use the **Add Filter** button to apply a filter by which the report data will sort. For more information, see *Filtering by keywords* (on page 79).

Note: When you are using a type of filter that matches a device using an IP address, you can use CIDR notation to identify a subnet of hosts from which the reports display data. For example, when you select a Sender filter type, you can specify a subnet using 192.168.11.0/24 to display information from all of the hosts in the subnet.

- **Managing report views**. Use the **Dashboard View** list at the top of the page to switch between the pre-configured report view and report views you've configured, or to create new report views.

Selecting and configuring the dashboard reports in this report

In addition to customizing the report data, there are several ways you can configure the individual dashboard reports within the Interface Details report.

- **Editing the dashboard reports displayed within a report view**. Use the **Edit layout** button at the top of the screen to select which reports to display within the report's views.
- **Configure the report**. Use the configure button on a dashboard report menu to change the report configuration. For more information, see *Configuring dashboard reports* (on page 106).
- **Expand and collapse dashboard reports**. Use the collapse and expand buttons on the report toolbar to open and close the dashboard reports within the report.

Note: Collapsing a dashboard report does not remove it from the report. Instead, it collapses the dashboard report data and displays only the dashboard report title bar.

Exporting, emailing, scheduling and managing reports

Use the **Export** 

icon, at the top right of the page, to export reports. Use the **Email** 

icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 97).

Exporting individual dashboard report data

Use the Export button on a dashboard report's menu to export data to either a text file, Microsoft Excel, or a PDF. For more information, see *Exporting report data* (on page 108).

Tip: You can view the **Interface Overview** report for the selected interface by clicking Interface Overview at the top of the page.

Managing report views

You can customize the default view, General, of the Flow Monitor Interface Details report, or create new views tailored to your needs.

To customize an existing view:

1. Navigate to the Interface Details report (**Flow Monitor > Interface Details**).
2. From the **View** list in the toolbar, select the view you want to customize. The view you select appears.
3. In the toolbar, click **Edit View**. The Configure Flow Interface Report dialog appears.

4 Customize the view.

a) In **View**, enter a descriptive name for the view. This name appears in the **View** select list in the toolbar.

b) From the list of available reports, select the checkboxes next to the names of the reports you want to include in this view.

5 Click **OK** to save changes. The customized Flow Interface Details report appears.

To create a new Interface Details report view:

1 Navigate to the Interface Details report (**Flow Monitor > Interface Details**).

2 From the **View** select list in the toolbar, select **Add View**. The Configure Flow Interface Report dialog appears.

3 Configure the new view.

a) In **View**, enter a descriptive name for the view. This name appears in the **View** select list in the toolbar.

b) From the list of available reports, select the checkboxes next to the names of the reports you want to include in this view.

4 Click **OK** to save changes. The Flow Monitor Interface Details report appears and displays the new view.

To delete a Flow Interface Details report view:

1 Navigate to the Interface Details report (**Flow Monitor > Interface Details**).

2 From the **Dashboard View** select list in the toolbar, select the view you want to delete. The view you select appears.

3 From the **Dashboard** select list in the toolbar, select **Delete Current View**. You are prompted to confirm you want to delete the current view.

4 Verify that you want to delete the view, then click **Yes**. The report view is deleted and the Flow Monitor Interface Details report appears.

Selecting an interface

The Flow Monitor Interface Details, Interface Overview, and Bandwidth Usage reports display data in context of a single interface or all the interfaces of one source.

To change the interface for which data is reported:

1 From the toolbar at the top of the screen, click the **Interface** list. A list of all of the available interfaces appears.

2 Select the interface for which you want to view the current report. The report refreshes with data from the selected interface.

Filtering data in a view

You can filter the data in the Interface Details report in several ways.

- Date and time
- Traffic direction
- Keywords

After you apply a filter, the report data refreshes to display data relevant to the applied filter.

Filtering by date and time

By default, the Interface Details report views shows data for the previous fifteen minutes. You can modify this time range by selecting the time frame from the Date range box.

To change the time frame for which the Interface Details report displays data:

1. At the top of the report, select **Date range**. A list of common time periods appears.
2. Select one of the available time periods.
3. If you select **Custom**, the **Start time** and **End time** boxes appear.

> **Note**: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

   a) In **Start time**, select the date and time that corresponds with the beginning of the time period.

   b) In **End time**, select the date and time that corresponds with the end of the time period.

> **Note**: When you set a start and end time for report data, you will most likely see a larger data total than expected. This is because the data displayed is a summation of the start time, or data greater than or equal to the selected start time, and the end time, or data less than or equal to the selected end time.

4. Click **Go** to apply the filter to the report. The report refreshes showing only data from the selected time period.

Filtering by traffic direction

By default, the Interface Detail report displays information about inbound traffic to the selected interface.

The router graphic to the right of the Traffic direction list illustrates the direction traffic is moving in relation to the router.

In the graphic above, the arrow is pointing to the router, illustrating that traffic is moving toward the router, and is therefore *inbound*.

To filter report data by traffic direction:

1. At the top of the report, select **Traffic direction**. A list of available traffic directions appears.
2. Select a traffic direction.

   § **Inbound**. Select this option to show only data that is being sent to the interface.

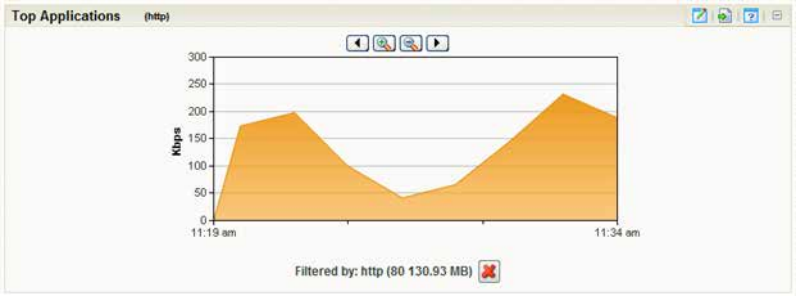
- **Outbound**. Select this option to show only data that is being sent from the interface.
- **Inbound and Outbound**. Select this option to show both inbound and outbound traffic for the interface.
- **Bounce**. Select this option to see traffic that routed into and out of the same interface. In some cases, this may represent a router misconfiguration.

3 After you select a traffic direction, the report refreshes showing only data from traffic that matches your selection.

Filtering by keywords

You can use keyword filters to create complex Flow Monitor interface report views. This is useful when you need to view data about the traffic generated by a specific computer, to a specific domain, etc.

After you apply a filter to the Interface Details report, the dashboard report that coincides with the filter reloads with a time graph for the filtered traffic component. For example, if you apply a filter for the http application, the Top Applications dashboard report displays a time graph of http application use for the time period selected at the top of the Interface Details report.



You can easily determine which dashboard report contains the time graph by looking for the filter enclosed in parenthesis to the right of the dashboard report title name.

Tip: You can remove the applied filter by clicking the red X under the time graph.

To filter by keywords:

1 At the top of the report, select **Add Filter**. Filter boxes appear below the button.
2 Select the type of filter you want to apply.

Note: When you are using a type of filter that matches a device using an IP address, you can use CIDR notation to identify a subnet of hosts from which the reports display data. For example, when you select a Sender filter type, you can specify a subnet using 192.168.11.0/24 to display information from all of the hosts in the subnet.

- **Sender**. Show traffic sent by the specified device. You can match a device using its host name or its IP address.
- **Receiver**. Show traffic received by the specified device. You can match a device using its host name or its IP address.

- **Protocol**. Show traffic that used the specified protocol (such as UDP, TCP, or ICMP).
- **Service**. Show traffic that used the specified type of service.
- **Application**. Show traffic that used the specified application. The keyword must match the application name as configured in the Flow ports dialog.

Tip: You can enter a port number instead of an application name to show all traffic transmitting over a certain port.

- **Sender Domain**. Show traffic sent by hosts on the specified domain.
- **Receiver Domain**. Show traffic received by hosts on the specified domain.
- **Sender Country**. Show traffic sent by devices whose IP addresses are registered to the specified country.
- **Receiver Country**. Show traffic received by devices whose IP addresses are registered to the specified country.
- **Sender Group**. Show traffic sent by the specified group.
- **Receiver Group**. Show traffic received by the specified group.
- **Sender TLD**. Show traffic sent by domains that have the specified top level domain (such as .com, .net, .us, or .uk).
- **Receiver TLD**. Show traffic received by domains that have the specified top level domain (such as .com, .net, .us, or .uk).
- **ICMP Type**. Show traffic by ICMP type.
- **Packet Size**. Show traffic by packet size.
- **Sender ASN**. Show traffic by sender Autonomous System Number (ASN).
- **Receiver ASN**. Show traffic by receiver Autonomous System Number (ASN).
- **NBAR Application**. Show traffic by NBAR application.
- **Port**. Show traffic by port number.

3. Optionally, click **Add Filter** to add additional filters.
4. Click **Apply Filters**. The report refreshes showing only data that matches the filters you have configured.

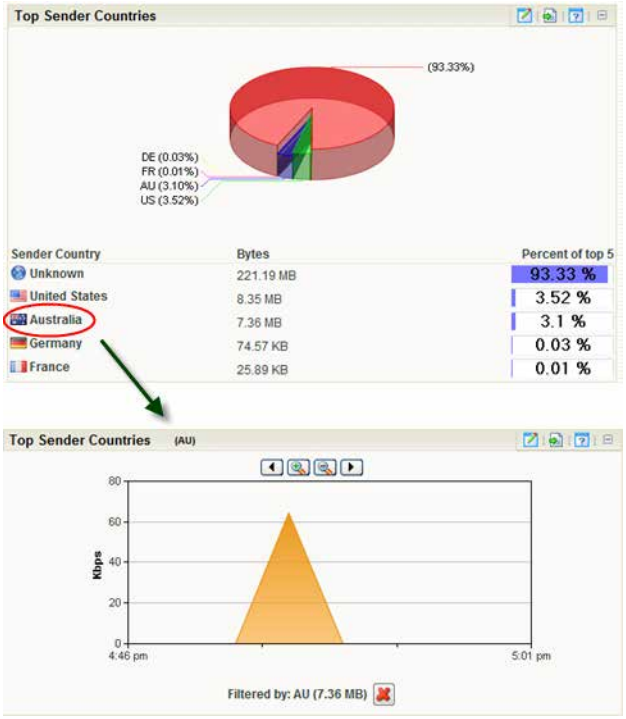
Tip: If you configure a filter incorrectly, you can remove it from the current view by clicking the red X located to the right of the keyword box.

Filtering by drilling-down

Another way to filter report data is by clicking on report entries, or *drilling-down*. This method of report-filtering allows you to dig deeper into data that peaks your interest or raises red flags—with just one click.

When you click an entry in the farthest-left column of an Interface Details dashboard report, the report reloads using the entry as a filter. Also, you can click inside a dashboard graph area to apply a filter.

Similarly to filtering by keywords, after you apply a filter to the report, the dashboard report that coincides with the filter will display a time graph for the filtered traffic component. For example, if you click an entry in the Sender Country column of the Top Sender Countries dashboard report, the dashboard report reloads with a time graph for the country that you clicked.



Several keyword filters coincide with more than one dashboard report and more than one time graph is displayed after the filter is applied. You can easily distinguish which dashboard reports in the Interface Details report are displaying time graphs by looking for the applied filter's name in parenthesis next to a report name.

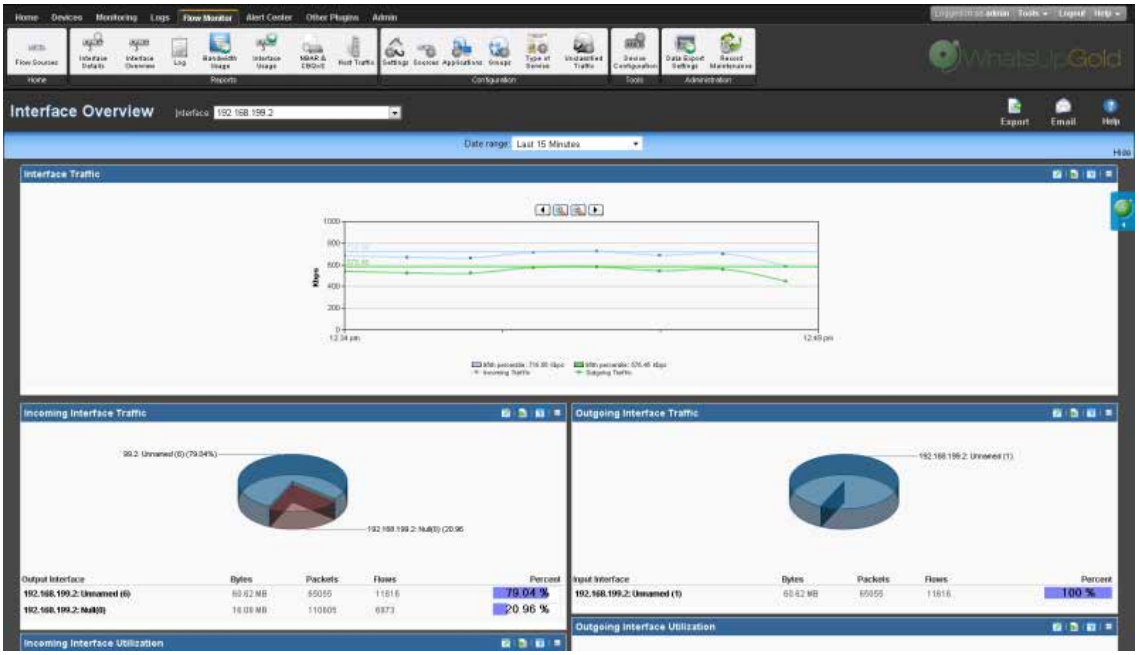
About the Interface Details report options

The Interface Details report has the following options available on the Options menu.

- **Export to PDF**. Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog appears.
- **Email / Schedule Report**. Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports**. Select this option to configure Flow Monitor to run this report on a recurring basis.

About the Flow Monitor Interface Overview report

The Interface Overview report is a collection of Flow dashboard reports that provide a summary of the traffic and utilization of a specific interface.



The Interface Overview consists of individual Flow dashboard reports that highlight both inbound and outbound traffic and utilization for the selected interface or a whole source (all the interfaces in one source).

- Interface Traffic
- Incoming Interface Traffic
- Outgoing Interface Traffic
- Incoming Interface Utilization
- Outgoing Interface Utilization

By default, the report displays data for the last interface you selected from the Source list.

Note: sFlow data is sent every x number of packets (configurable on the sFlow device), whereas typically *all* NetFlow data is collected and monitored. This means that sFlow data provides a sampling of network traffic data, whereas Flow data provides all network traffic data.
sFlow data sampling methods may result in Interface Overview and Interface Detail reports that appear to have more or less traffic than is shown in the Flow Monitor Home page source information. This is because the sampled data shown in the Interface Overview and Interface Detail reports are derived the sampled data and the Flow Monitor Home page source information is derived from the total interface traffic data.

- **Select a different interface**. Use the **Interface** list at the top of the page to select the interface for which the report data displays.

- **Selecting a different date range**. Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 78). You can also change the report date and time by using the Report Zoom Tool. For more information, see Report Zoom Tool.

Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

- **Configure the report**. Use the configure button on a dashboard report menu to change the report configuration. For more information, see *Configuring dashboard reports* (on page 106).

Configuring the dashboard reports in this report

In addition to customizing the report data, you can configure the individual dashboard reports within the Interface Overview report.

- **Expand and collapse dashboard reports**. Use the collapse and expand buttons on the report toolbar to open and close the dashboard reports within the report.

Note: Collapsing a dashboard report does not remove it from the report. Instead, it collapses the dashboard report data and displays only the dashboard report title bar.

Exporting, emailing, scheduling and managing reports

Use the **Export** 

icon, at the top right of the page, to export reports. Use the **Email** 

icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 97).

Exporting individual dashboard report data

Use the Export button on a dashboard report's menu to export data to either a text file, Microsoft Excel, or a PDF. For more information, see *Exporting report data* (on page 108).

Tip: You can view the Interface Details report for the selected interface by clicking **Interface Details** at the top of the page.

About the Interface Overview report options

The Interface Overview report has the following options available on the Options menu.

- **Export to PDF**. Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog appears.
- **Email / Schedule Report**. Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports**. Select this option to configure Flow Monitor to run this report on a recurring basis.

Filtering report data

You can filter the data displayed in the Interface Overview by *time and date* (on page 84). After you apply a date and time filter, the report data refreshes to display data relevant to the applied filter.

Filtering by date and time

By default, the Interface Overview report shows data for the previous fifteen minutes.

To change the time frame for which the Interface Overview report displays data:

1. At the top of the report, select **Date range**. A list of common time periods appears.
2. Select one of the available time periods.
3. If you select **Custom**, the **Start time** and **End time** boxes appear.

Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

   a) In **Start time**, select the date and time that corresponds with the beginning of the time period for which you want to see data.

   b) In **End time**, select the date and time that corresponds with the end of the time period for which you want to see data.

4. Click **Go** to apply the filter to the report. The report refreshes showing only data from the time period selected.

About the Report Zoom Tool

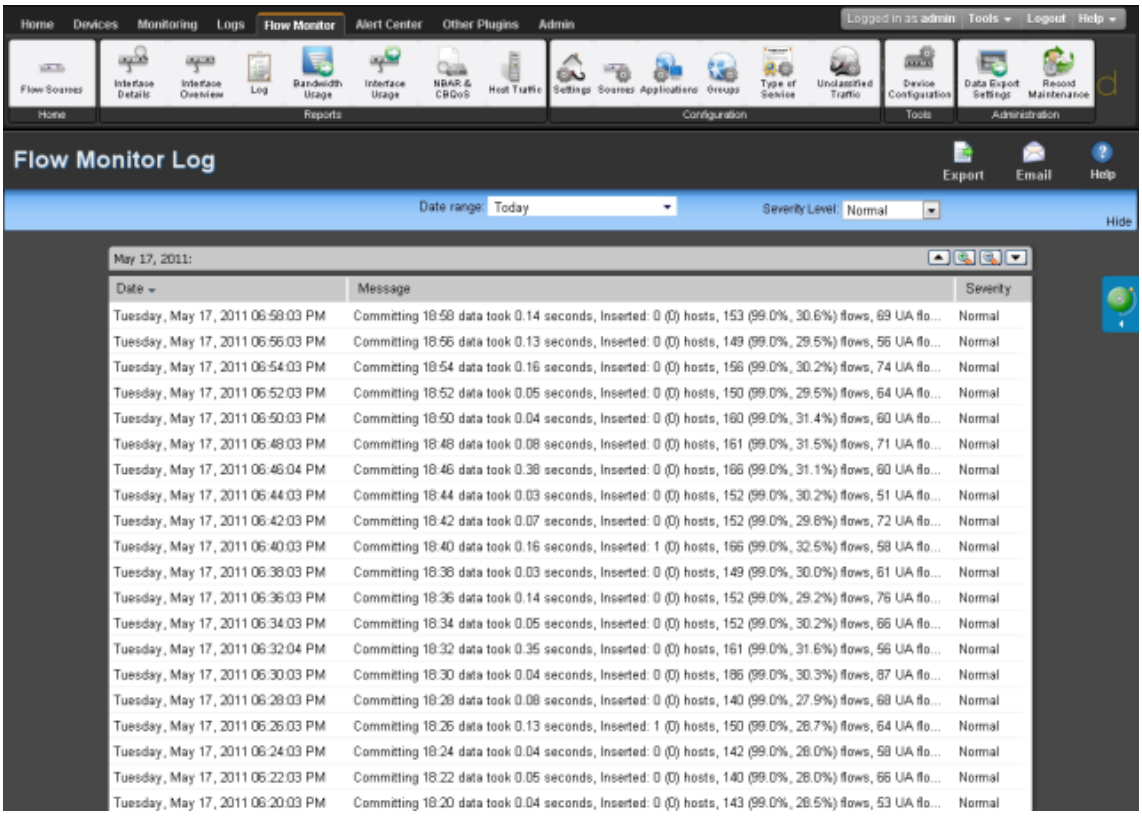
Use the zoom tool to navigate through a report. The zoom tool is tied-in to the report date/time picker and will change the date and time of a report as you page up and down, or zoom in and out.

Page up	Moves the report date forward. For example, clicking the Page up button will move the date from today to tomorrow.

Zoom in	Decreases the amount of time displayed in the report. For example, click the Zoom in button will decrease the display time from 24 hours to 12 hours.
Zoom out	Increases the amount of time displayed in the report. For example, clicking the Zoom out button will increase the display time from 12 hours to 24 hours.
Page down	Moves the report date backward. For example, clicking the Page down button will moved the date from today to yesterday.

About the Flow Log

The Flow Monitor Log is a history of system-wide messages generated by Flow Monitor. When you access the Flow Monitor Log, it shows messages generated during the time period selected at the top of the report. By default, logs are generated at every data flush interval, including statistics about the data saved in the database and the time needed to complete the operation. These log entries provide valuable information about the collection, allowing us to know whether Flow Monitor is handling the load with ease.



Each entry shows the date logged, the message about the activity, and the severity of the entry.

- **Date** displays the date the message was logged.

- **Message** displays the activity message. This message contains the reason for the log entry, other information, such as error number, which may be useful in troubleshooting.
- **Severity** displays the logging level of the entries, either Normal, Verbose, or Errors Only.

Tip: You can sort the data in the report by clicking on a column title.

Changing the report date and time

Use the **Date range** list at the top of the report to select a time frame for the report. By default, the report displays log entries for the previous hour.

Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Monitor Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

Changing the report severity/logging level

Use the **Severity level** list to select a logging level for the report.

- **Verbose** displays all entries (including all three severity levels).
- **Normal** displays entries for Normal and Errors Only.
- **Errors only** displays only error entries.

Note: The logging level that you specify on the Flow Settings dialog determines the level of data that Flow Monitor records, whereas the logging level that you specify on the Flow Log report page determines the level of data displayed within the report.

Important: If you have specified the Normal or Errors Only levels on the Flow Settings dialog, you will not be able to view the Verbose level from the Flow Log report page.

Important: If your log includes an error that reads "It seems the collector is unable to keep up with the amount of traffic received," the amount of traffic you are currently collecting is too great for the Flow Monitor to handle. It is possible that you have a number of Flow sources and/or interfaces too great for the collector to handle. In an effort to reduce traffic, it will help to reduce the percentage of traffic to retain or the number of enabled sources and/or interfaces.

Exporting, emailing, scheduling and managing reports

§ Use the **Export** 

icon, at the top right of the page, to export reports. Use the **Email** 

icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 97).

Filtering report data

You can filter the Flow Monitor Log by two criteria.

§ *Date and time* (on page 87)

§ *Severity level* (on page 88)

After you apply a filter, the report data refreshes to display data relevant to the applied filter.

Filtering by date and time

By default, the Flow Monitor Log shows data for the previous fifteen minutes.

To change the time frame for which the Flow Monitor Log report displays data:

1 At the top of the report, select **Date range**. A list of common time periods appears.

2 Select one of the available time periods.

3 If you select **Custom**, the **Start time** and **End time** boxes appear.

Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

a) In **Start time**, select the date and time that corresponds with the beginning of the time period for which you want to see data.

b) In **End time**, select the date and time that corresponds with the end of the time period for which you want to see data.

Tip: Use the Standard Business Hours feature to set up group reports designed for business hours only. For more information, see Changing the report date range.

4 Click **Go** to apply the filter to the report. The report refreshes showing only data from the time period selected.

Filtering by severity level

By default, the Flow Monitor Log displays data for the Normal severity level.

To change the severity level for which the Flow Monitor Log displays data:

1. At the top of the report, click the **Severity level** list. A list of the three available severity levels appears.
2. Select the severity level for which you want to view report data. The report refreshes with data for the selected severity level.

About the Report Zoom Tool

Use the zoom tool to navigate through a report. The zoom tool is tied-in to the report date/time picker and will change the date and time of a report as you page up and down, or zoom in and out.

Page up	Moves the report date forward. For example, clicking the Page up button will move the date from today to tomorrow.
Zoom in	Decreases the amount of time displayed in the report. For example, click the Zoom in button will decrease the display time from 24 hours to 12 hours.
Zoom out	Increases the amount of time displayed in the report. For example, clicking the Zoom out button will increase the display time from 12 hours to 24 hours.
Page down	Moves the report date backward. For example, clicking the Page down button will moved the date from today to yesterday.

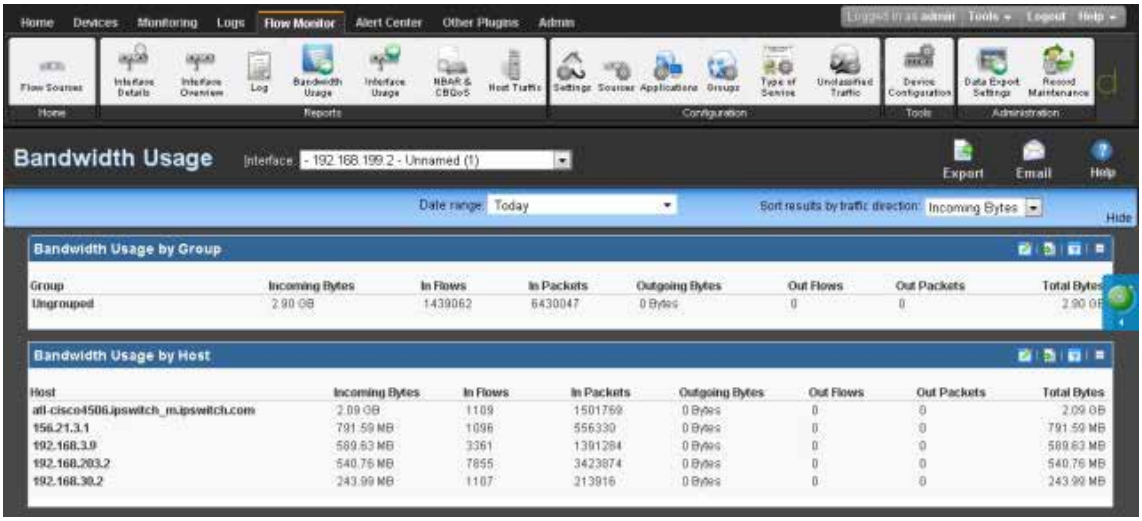
About the Flow Monitor Log options

The Flow Monitor Log report has the following commands available on the Options menu.

- **Export to Text**. Select this command to export the contents of the current view to a text file. The Export to Text dialog appears.
- **Export to PDF**. Select this command to export the contents of the current view to a PDF file. The Export to PDF dialog appears.
- **Export to Excel**. Select this command to export the contents of the current view to an Excel file. The Export to Excel dialog appears.
- **Email / Schedule Report**. Select this command to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports**. Select this command to configure Flow Monitor to run this report on a recurring basis.

About the Flow Bandwidth Usage report

The Bandwidth Usage report displays network bandwidth usage information.



The report consists of Flow Monitor dashboard reports that summarize the incoming and outgoing traffic for Flow Monitor groups and hosts.

- Bandwidth Usage by Group displays bandwidth usage summaries for the top <n> Flow Monitor groups for the selected time period.
- Bandwidth Usage by Host displays bandwidth usage summaries for the top <n> hosts that are using the most bandwidth during the selected time period.

There are several ways you can refine this report.

- **Select a different interface**. Use the **Interface** list at the top of the page to select the interface for which the report data displays.
- **Sort results by traffic direction**. Use the **Sort by traffic direction** list at the top of the page to select a direction for which the report data is displayed. Select Incoming, Outgoing, or Total.
- **Selecting a different date range**. Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 78).

Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Monitor Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

Configuring the dashboard reports in this report

In addition to customizing the report data, there are several ways you can configure the individual dashboard reports within the Bandwidth Usage report.

- **Configure the report**. Use the configure button on a dashboard report menu to change the report configuration. For more information, see *Configuring dashboard reports* (on page 106).
- **Expand and collapse dashboard reports**. Use the collapse and expand buttons on the report toolbar to open and close the dashboard reports within the report.

Note: Collapsing a dashboard report does not remove it from the report. Instead, it collapses the dashboard report data and displays only the dashboard report title bar.

Exporting, emailing, scheduling and managing reports

Use the **Export** 

icon, at the top right of the page, to export reports. Use the **Email** 

icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 97).

Exporting individual dashboard report data

Use the Export button on a dashboard report's menu to export data to either a text file, Microsoft Excel, or a PDF. For more information, see *Exporting report data* (on page 108).

Selecting an interface

The Flow Monitor Interface Details, Interface Overview, and Bandwidth Usage reports display data in context of a single interface or all the interfaces of one source.

To change the interface for which data is reported:

1. From the toolbar at the top of the screen, click the **Interface** list. A list of all of the available interfaces appears.
2. Select the interface for which you want to view the current report. The report refreshes with data from the selected interface.

Filtering report data

You can filter the data in the Bandwidth Usage report two ways.

- *Date and time* (on page 91)
- *Traffic direction* (on page 92)

After you apply a filter, the report data refreshes to display data relevant to the applied filter.

Filtering by date and time

By default, the Bandwidth Usage report shows data for the previous fifteen minutes.

To change the time frame for which the Flow Monitor Interface Details report displays data:

1. At the top of the report, select **Date range**. A list of common time periods appears.
2. Select one of the available time periods.
3. If you select **Custom**, the **Start time** and **End time** boxes appear.

Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Monitor Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

   a) In **Start time**, select the date and time that corresponds with the beginning of the time period for which you want to see data.

   b) In **End time**, select the date and time that corresponds with the end of the time period for which you want to see data.

Tip: You can also change the report date and time by using the Report Zoom Tool. For more information, see *About the Report Zoom Tool* (on page 85).

Tip: Use the Standard Business Hours feature to set up group reports designed for business hours only. For more information, see Changing the report date range.

4. Click **Go** to apply the filter to the report. The report refreshes showing only data from the time period selected.

Filtering by traffic direction

By default, the Bandwidth Usage report displays information about incoming traffic for the selected interface.

To filter report data by traffic direction:

1. At the top of the report, select **Traffic direction**. A list of available traffic directions appears.
2. Select a traffic direction.
   - **Inbound**. Select this option to show only data that is being sent into the interface.
   - **Outbound**. Select this option to show only data that is being sent from the interface.
3. After you select a traffic direction, the report refreshes. After it refreshes, the report shows only data from traffic that matches your selection.

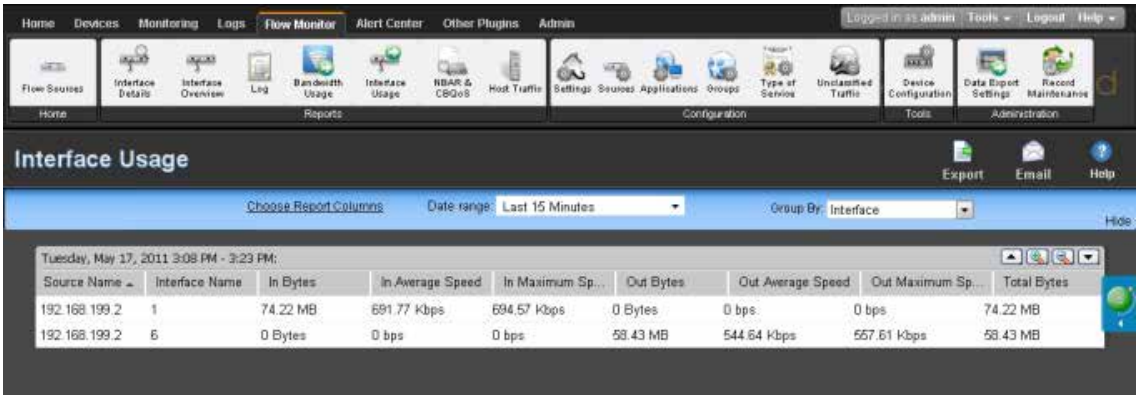
About the Bandwidth Usage report options

The Bandwidth Usage report has the following options available on the Options menu.

- **Export to PDF**. Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog opens.
- **Email / Schedule Report**. Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports**. Select this option to configure Flow Monitor to run this report on a recurring basis.

About the Interface Usage report

The Flow Interface Usage report gives a view of the total amount of incoming and outgoing traffic for source interfaces over the selected time period. Interfaces can be displayed separately, or grouped together by interface name. When you group together by interface name, all interfaces under a single display name are added together, and all data displayed is a total for those interfaces.



The report displays the following usage data for each interface.

- **Interface Name** the display name as configured by the user on the Flow Sources dialog in combination with the interface identifier.
- **Incoming Bytes**. Displays the number of incoming bytes for that interface or interface name over the selected time period.
- **Incoming Average Speed**. Displays the incoming rate in a multiple of bytes per second for the interface over the selected time period.
- **Incoming 95th Percentile**. Displays the results of the 95th percentile calculation for incoming traffic during the selected time period. It is calculated only with raw data, so do not expand the date range to include roll-up data.
- **Incoming Maximum Speed**. Displays the maximum incoming rate in a multiple of bytes per second achieved during the selected time period.
- **Outgoing Bytes**. Displays the number of outgoing bytes for that interface or interface name over the selected time period.
- **Outgoing Average Speed**. Displays the outgoing rate in a multiple of bytes per second for the interface over the selected time period.

- **Outgoing 95th Percentile**. Displays the results of the 95th percentile calculation for outgoing traffic during the selected time period. It is calculated only with raw data, so do not expand the date range to include roll-up data.
- **Outgoing Maximum Speed**. Displays the maximum outgoing rate in a multiple of bytes per second achieved during the selected time period.
- **Total Bytes**. Displays the total number of bytes for that interface or interface name over the selected time period.

By default, the report displays data grouped by interfaces. You can refine the report in several ways.

- **Grouping report data**. Choose to **Group by** *Interface* or *Interface Name.*
- **Selecting a different date range**. Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 78).

Exporting, emailing, scheduling and managing reports

Use the **Export** 

icon, at the top right of the page, to export reports. Use the **Email** 

icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 97).

Configuring the Interface Usage report columns

Use the Configure Interface Usage Report Columns dialog to configure which data you want to appear in each column of the Interface Usage report.

 **Note**: **Column 1** always appears and by default contains the interface name.

For each column, select the data you want to appear. If you do not want data to appear in a column, select **none** for that column.

About the Interface Usage report options

The Interface Usage report has the following options available on the Options menu.

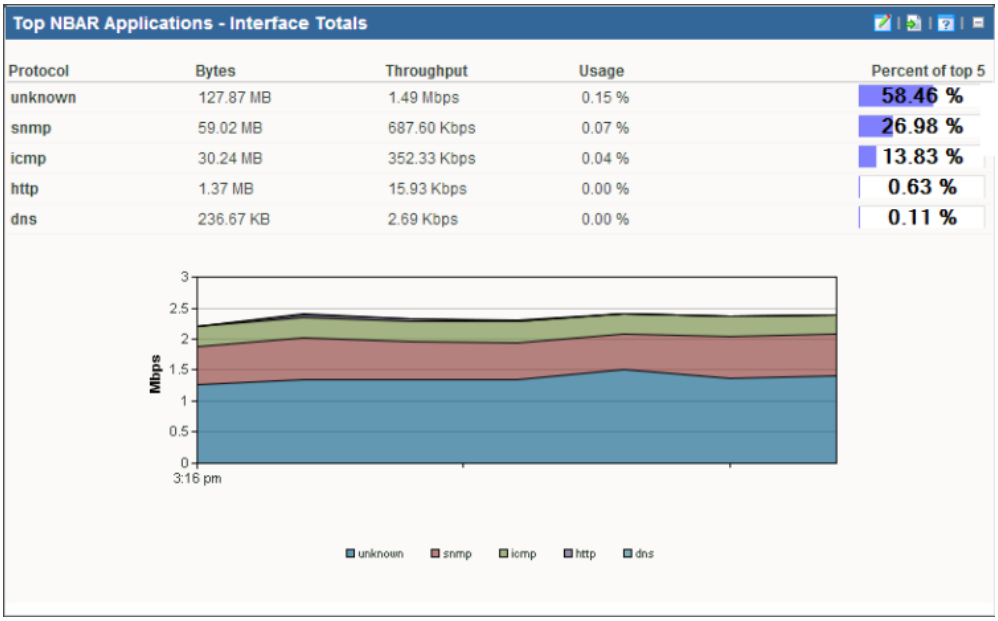
- **Export to Text**. Select this option to export the contents of the current view to a text file. The Export to Text dialog opens.
- **Export to PDF**. Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog opens.
- **Export to Excel**. Select this option to export the contents of the current view to an Excel file. The Export to Excel dialog opens.

- **Email / Schedule Report**. Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports**. Select this option to configure Flow Monitor to run this report on a recurring basis.

About the NBAR and CBQoS Reports

NBAR Report

Cisco Systems Network Based Application Recognition (NBAR) classification engine provides a network device with the ability to recognize applications, including those that dynamically assign TCP or UDP ports. The Top NBAR Applications report displays the top applications as identified using Cisco's NBAR classification engine.



You can choose to display and sort sender traffic by bytes, packets, or flows using the **Display and sort by** option on the report configuration dialog. Providing alternate sorting methods allows you to monitor and identify hosts that are the largest consumers of interface resources other than bandwidth.

- **Application**. Displays the application as identified by Cisco's NBAR classification engine.
- You can select one of the following units to display and sort the specific items in the report using the **Display and sort by** option on the report configuration dialog. The selected option appears as the first column header in the report and is used to sort the top "n" items.
  - **Bytes**. Displays the total number of bytes transmitted for the specific item in the report category for the selected date range.

- **Packets**. Displays the total number of packets for the specific item in the report category for the selected date range.
- **Flows**. Displays the total number of flows for the specific item in the report category for the selected date range.

- **Throughput**. Displays the average bit rate, packet rate or flow rate, in multiples of the selected unit (e.g. Kbps, Mbps, or Gbps) for the specific item in the report category for the selected date range.
- **Usage**. Displays the percentage of the total available bandwidth used by the specific item in the report category for the selected date range.

Note: Utilization is displayed as N/A if a speed is not specified for the interface, or if you have selected to display packets or flows in the report. If you are displaying bytes, you can set the interface speed on the Flow Interface dialog. To navigate to the Flow Interface dialog, click the **Configure** link in the message appearing above the dashboard reports.

- **Percentage**. Displays the percentage of the total traffic for the specific item in the report category for the selected date range.
- **Totals (row title)**. Displays the total of all of the items in the report category, specified and unspecified (**Others**). This row shows the interface totals for each column in the report.

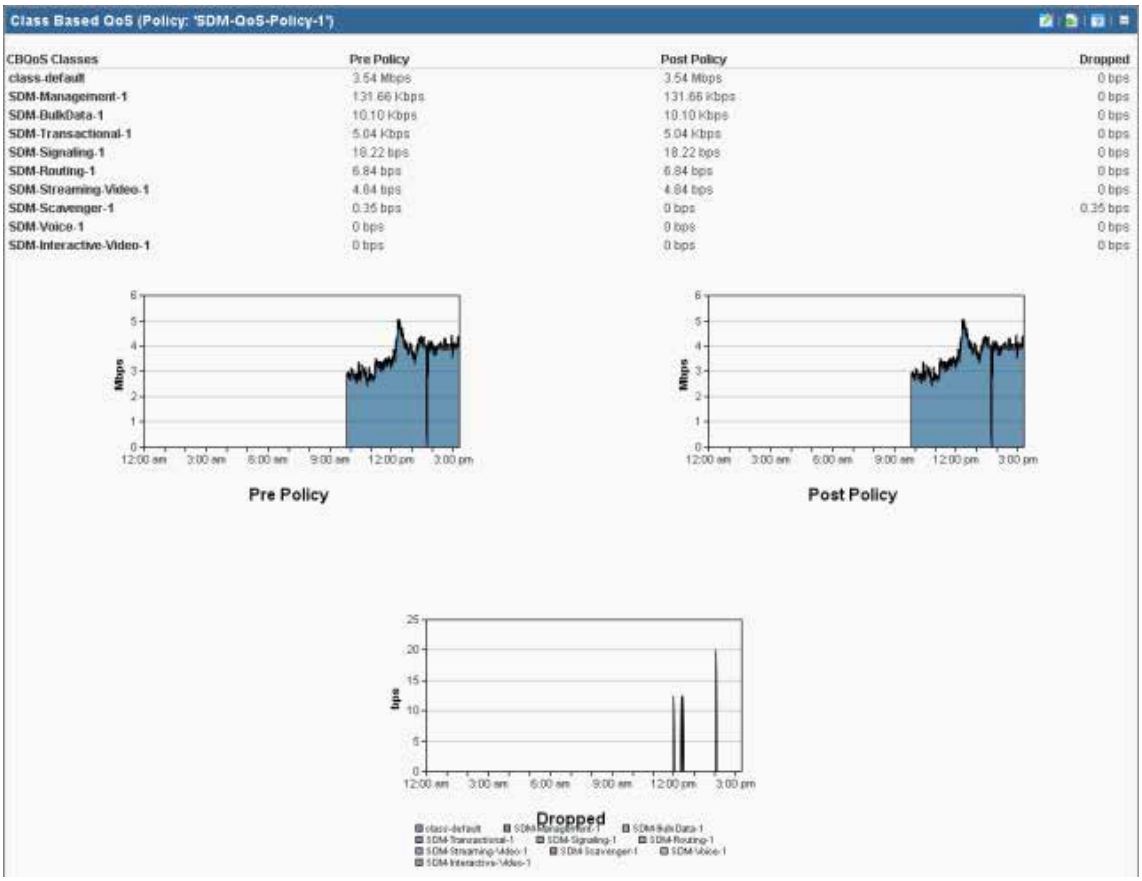
Note: The source device must be configured to generate NBAR information in order for this report to generate data for the source device.

Note: For the **Top NBAR Applications - Flow Details** report, NBAR information generated by the source device is gathered by Flow Monitor from flow data using Flexible NetFlow.

Note: For the **Top NBAR Applications - Interface Totals** report, the NBAR information is gathered from the source device using SNMP polling. The **Poll source for NBAR information** option is available on the Flow Source dialog.

Class Based Quality of Service Report

The Class Based Quality of Service (CBQoS) report provides information about the effectiveness of class-based policies applied to an interface for all of the defined classes.



- **QoS Class Map**. Displays the QoS class name as defined by the policy assigned to the interface.
- **Pre-Policy**. Displays the amount of traffic for the class before the policy is applied.
- **Post-Policy**. Displays the amount of traffic for the class after the policy is applied.
- **Dropped**. Displays the number of bytes dropped as a result of applying the policy to the class.

Note: You must have defined QoS classes and policies on the source device before this report is able to display results.

Note: The CBQoS information generated by the source device must be gathered using SNMP polling for CBQoS information.

Using Scheduled Reports: printing, exporting, and emailing reports

The Flow Monitor Log and Interface Usage reports can be printed and exported to a formatted text file, Microsoft Excel, or a PDF. You can also email reports as a PDF, or send on scheduled intervals. The Flow Monitor Interface Details, Interface Overview, and Bandwidth

Usage reports can be exported as PDF reports and emailed as scheduled reports. Click the Export 

icon, available at the top of each report, to export reports, or the Email 

icon to email a report or manage Scheduled Reports. This option is available to users with user rights for **Manage Scheduled Report** enabled. For more information, see About user rights.

Important: To use the print and export features, make sure client side JavaScript is enabled in your browser's options.

Tip: In some cases, exported reports show more detailed data than the data displayed in the report in the web interface. For example, an exported Excel report my contain more data columns, or a floating data point with higher precision.

To print a report:

While viewing the report you want to print:

- Right-click anywhere inside the report window, then select **Print**.
  - OR -
  From the WhatsUp Gold web interface, click **File > Print**.

To export a report to a text file (full reports only):

While viewing the full report you want to export:

1. On the Report Toolbar, click the **Export** 

icon. The Report Options list appears.
2. Select **Export to Text**.
3. Clear or select the following options: **Include report title**, **Include column names** to either include or remove the report title or column names from the exported file.
4. Select a **Column delimiter** from the list.
5. Select a **Text qualifier** from the list.
6. Click **OK** to export the report to text.

To export a report to Microsoft Excel (full reports only):

While viewing the full report you want to export:

1. On the Report Toolbar, click the **Export** 

icon. The Report Options list appears.
2. Select **Export to Excel**.
3. Clear or select the following options: **Include report title**, **Include column names** to either include or remove the report title or column names from the exported file.
4. Select a **Column delimiter** from the list.
5. Select a **Text qualifier** from the list.
6. Click **OK** to export the report to Excel.

To export a report to a PDF:

While viewing the full report you want to export:

1. On the Report Toolbar, click the **Export** 

icon. The Report Options list appears.
2. Select **Export to PDF**. The Export to PDF dialog appears.
3. Select the following options:
   - **Page size**. Select from the list of page size options.
   - **Auto size**. Enable this option to, generally, make the best automatic adjustment to fit all page content on the PDF.
   - **Page orientation**. Select Portrait or Landscape PDF.
4. Select the **Live links** option if you want to include clickable url links in the PDF report.
5. Click **Export** to export the report to a PDF.

To email a report as a PDF:

While viewing the full report you want to export:

1. From the WhatsUp Gold web interface, on the Report Toolbar, click the **Email** 

icon. The Email list appears.
2. Select **Email/Schedule Report**. The Email Report dialog appears.
3. Enter the following information for the email: **To**, **Subject**, **URL**, select the **PDF Options**. Refer to the dialog help for more information.
4. Click **Send Email** to send a PDF email immediately.

   - OR -

   Click **Schedule** to complete the scheduled email settings.
5. Click **Close**. The Email Report dialog closes.

CHAPTER 13

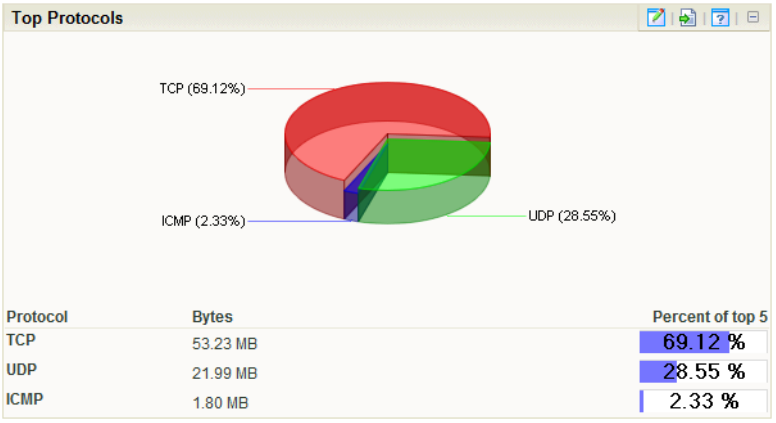
Using Flow Monitor dashboard reports

In This Chapter

Understanding Flow Monitor dashboard reports

Dashboard reports are the individual small reports displayed in several of the Flow Monitor reports and their views. Flow Monitor report views are user-customizable; they let you organize various dashboard reports by the type of information they display.

Flow Monitor dashboard reports typically consist of a graph and a table of data related to the graph.



Dashboard reports that display data from Flow Monitor can be used within Flow Monitor report views and WhatsUp Gold dashboard views.

Note: While you can determine which dashboard reports appear in dashboard views in Flow Monitor and WhatsUp Gold, Flow Monitor report views are more structured than WhatsUp Gold dashboard views. In WhatsUp Gold, you can position dashboard reports anywhere within a view; in Flow Monitor, report positions cannot be modified. As a rule, sender dashboard reports display on the left side of the report, while receiver dashboard reports display on the right side. Further, a page with no sender or receiver reports displays dashboard reports in one column.

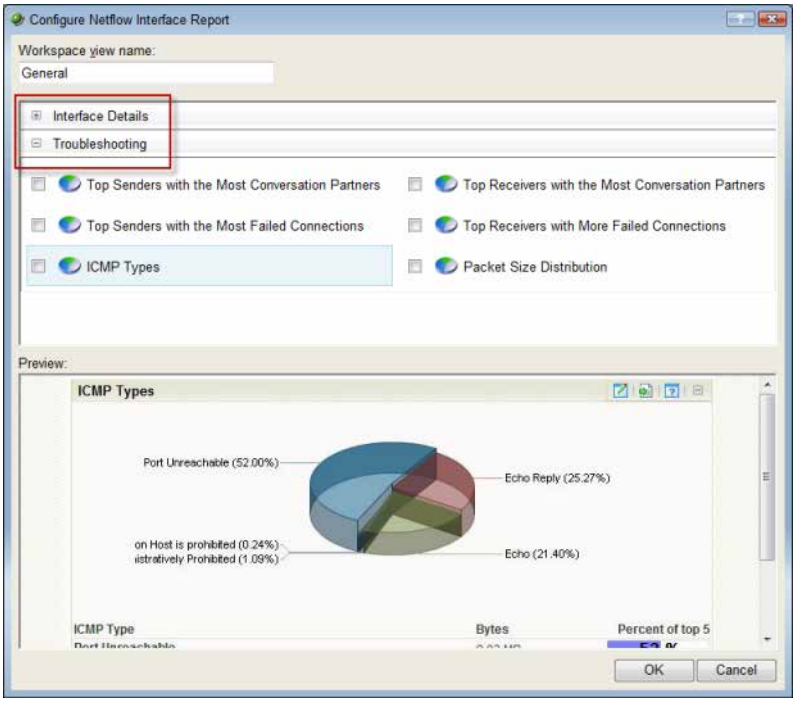
Flow Monitor dashboard report types

There are three types of Flow Monitor dashboard reports.

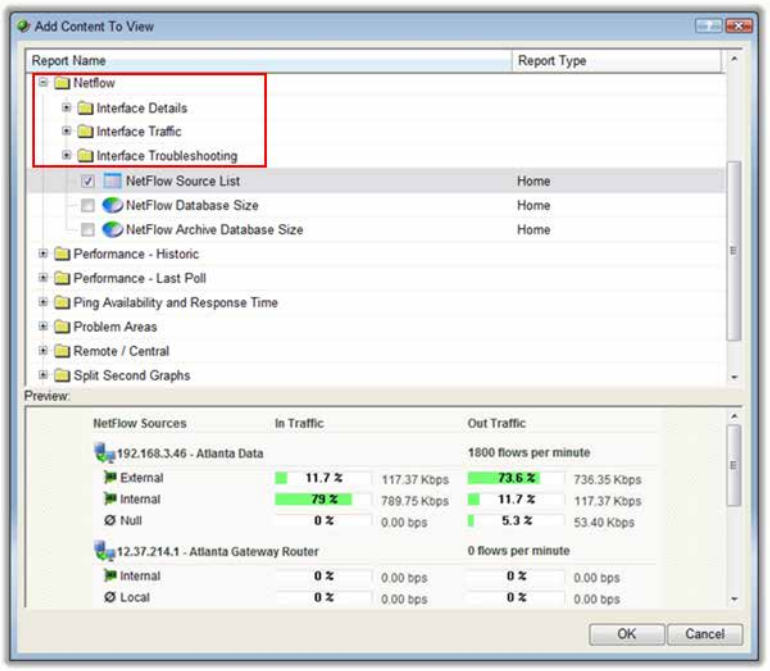
- **Interface Details** dashboard reports display summary information about specific details of an interface; for example, applications, protocols, and types of service.
- **Interface Troubleshooting** dashboard reports display data that would be useful in troubleshooting bandwidth problems, for example, failed connections.
- **Interface Traffic** dashboard reports display summary information about an interface's incoming and outgoing traffic.

These types vary depending from where in the application you modify your report and dashboard views.

If you add dashboard reports to the Interface Details report in Flow Monitor, you see Interface Details and Troubleshooting categories on the Configure Flow Interface Report dialog.



If you add dashboard reports to a dashboard view in WhatsUp Gold, you see Interface Details, Interface Troubleshooting, and Interface Traffic on the Add Content To View dialog.



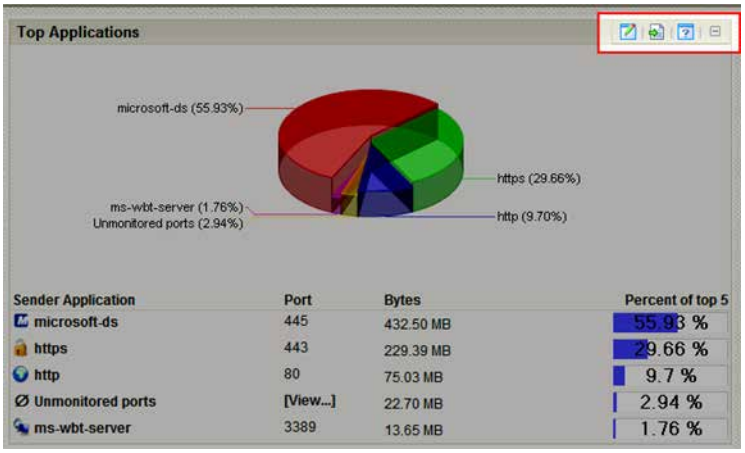
Navigating dashboard reports

There are several ways to navigate Flow Monitor dashboard reports.

- *Dashboard report menu* (on page 103) gives you options to configure and access help for each dashboard report.
- *Links* (on page 103) allow you to apply any criteria shown in a report as a filter.
- *Zoom control* (on page 104) lets you change the amount of data shown in line graphs.
- *Informational tooltips* (on page 105) alert you to conditions which may warrant further investigation.

Using the dashboard report menu

Each dashboard report has a menu on the right side of its title bar. Using the dashboard report menu, you can view help for the report, configure the report, export the report data, or expand and collapse the report.



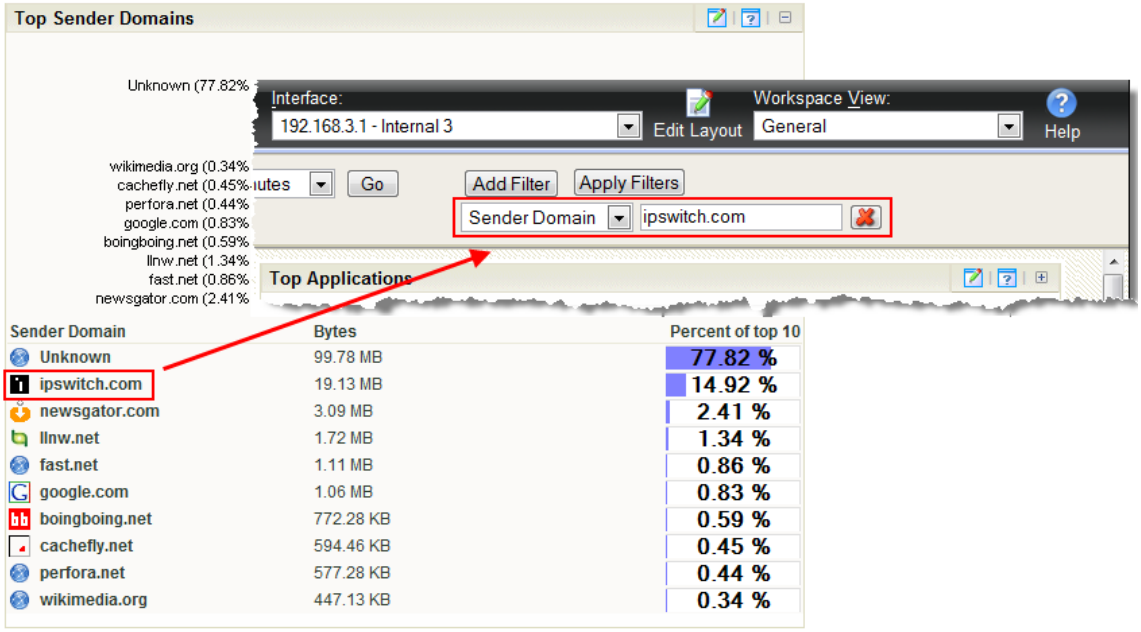
Dashboard report menu buttons

- Click the **Configure** button to open the Configure dialog for the report.
- Click the **Export** button to export report data.
- Click the **Help** button to view the help for the report.
- Click the **Expand** button to expand the report within the dashboard view.
- Click the **Collapse** button to collapse the report within the dashboard view. Collapsing a report does not remove it from the dashboard view.

Using links in Flow Monitor dashboard reports

Each Flow Monitor dashboard report contains links that allow you to refine the data displayed in the report. When you click on the data in the first column of one of the dashboard report's rows (or on a pie graph's wedges, or a bar graph's bars), the Flow Interface Details report appears with the selected data applied as a filter.

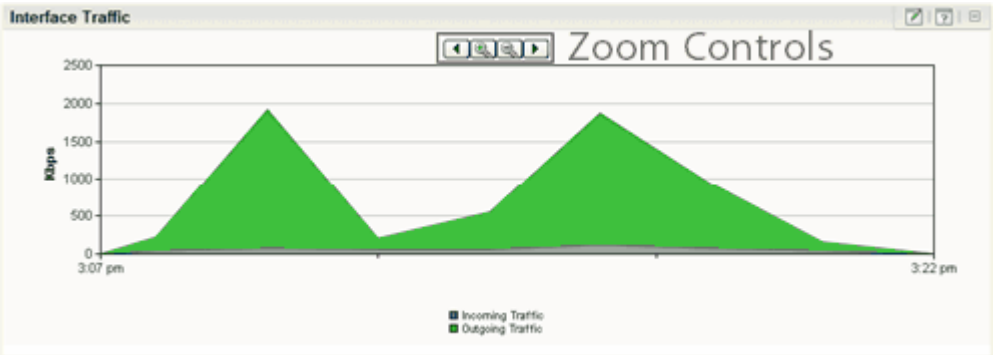
For example, as illustrated in the graphic below, if you click on `ipswitch.com` in the Top Sender Domains dashboard report, the Flow Interface Details report appears with a Sender Domain filter set to `ipswitch.com`.



If you are viewing the Flow Interface Details report with a filter applied, clicking a link in a dashboard report refreshes the report with the selected data applied as an additional filter (the previously applied filters remain).

Using zoom controls on line graphs

Dashboard reports that include line graphs, such as the Interface Traffic report, allow you to adjust the window of time for which data is reported using the zoom controls. These controls are located at the top center of the dashboard report.



Zoom controls

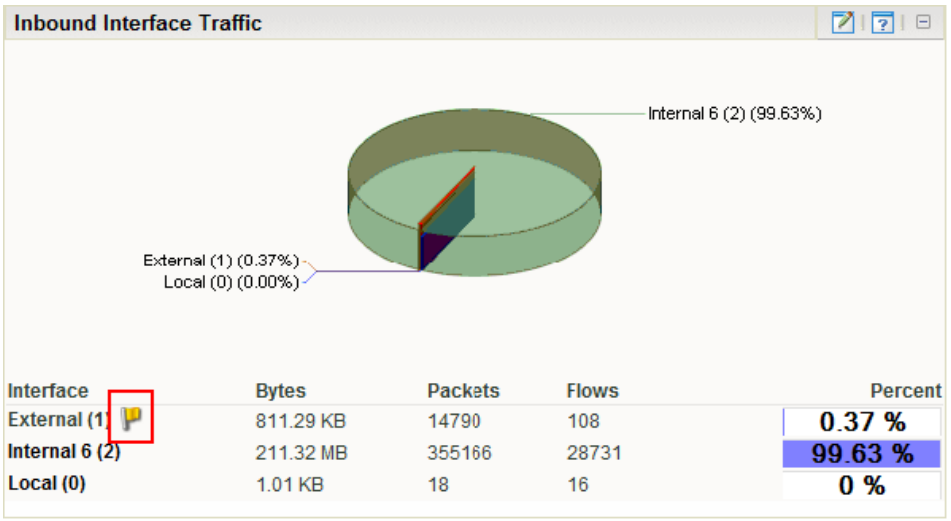
Page left — Moves the graph time frame backward by 50% of the total time of the graph. For example, if the graph shows data from 3:00 PM to 4:00 PM, clicking Page left shifts the time frame of the graph to 2:30 PM to 3:30 PM.

Zoom in — Decreases the amount of time displayed in the report by 50%. For example, if

	the report is displaying data for one hour, clicking the Zoom in button decrease the display time to 30 minutes. The report must display at least 30 minutes. If you attempt to zoom in on a report that shows 30 minutes, the report refreshes but the time frame is not changed.
Zoom out	Increases the amount of time displayed in the report. For example, if the report is displaying data for 30 minutes, clicking the Zoom out button increases the display time to 1 hour.
Page right	Moves the graph time frame forward by 50% of the total time of the graph. For example, if the graph shows data from 3:00 PM to 4:00 PM, clicking Page right shifts the time frame of the graph to 3:30 PM to 4:30 PM.

Using informational tooltips

In some reports, when Flow Monitor detects traffic patterns that may indicate a problem that requires intervention, a yellow warning flag icon is displayed.



Position the mouse cursor over the yellow flag icon to view an information tooltip about the specific issue, including links to related reports and specific help topics that may help resolve the issue.

If you do not want to see information tooltips, you can disable them throughout Flow Monitor. It is not possible to disable individual tooltips.

To disable informational tooltips throughout Flow Monitor:

1. On the WhatsUp Gold web interface, click **Flow Monitor > Settings**. The Flow Monitor Settings dialog appears.
2. Clear **Enable information tooltips**.
3. Click **OK** to save changes.

Configuring dashboard reports

The process for configuring dashboard reports varies depending on where in the application the dashboard report is viewed.

To configure a Flow Monitor dashboard report in Flow Monitor:

1. In the title bar of the dashboard report pane, click the Configure button . The Configure Report dialog appears.
2. Enter or select the appropriate information:
   - **Report name**. Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
   - **Maximum number of Items to display**. Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by** Bytes, Packets, or Flows. All other items in the category are included in the *'Others'* category, and are displayed when **Include 'Others'** is selected.
   - **Display**. Select the display type you want to use in the dashboard report. Choose Chart and data, Data only, or Chart only.
   - **Chart type**. Select the type of chart you would like the report to display. Choose Pie chart, Pie chart (3D), Pie chart (transparent 3D), Bar chart, Bar chart (horizontal), Bar chart (transparent 3D), or Stacked Time graph.
   - **Width**. Specify how wide, in pixels, the graph or chart should appear.
   - **Height**. Specify how tall, in pixels, the graph or chart should appear.
   - **Time graph scale**. Select the transfer speed format for which you want to view data. Choose Auto scale, bps, Kbps, Mbps, or Gbps.
     - **Minimum value**. Enter a minimum value for the graph.
     - **Maximum value**. Enter a maximum value for the graph.
3. Click **OK** to save changes.

To configure a Flow Monitor dashboard report in WhatsUp Gold:

1. In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
2. Enter or select the appropriate information:
   - **Report name**. Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
   - **Date range**. Select the timeframe for the traffic about which you want to see a report. You can select either the last 5, 15, or 30 minutes, or the last hour.
   - **Interface**. Select the router interface that is used by the traffic you want to see in this report.
   - **Interface traffic direction**. Select a direction for which the report will display data for the selected interface (In, Out, or Both).
   - **Maximum number of Items to display**. Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top

values based on the sort option selected in **Display and Sort by** Bytes, Packets, or Flows. All other items in the category are included in the *'Others'* category, and are displayed when **Include 'Others'** is selected.

- **Display**. Select the display type you want to use in the dashboard report. Choose Chart and data, Data only, or Chart only.
- **Chart type**. Select the type of chart you would like the report to display. Choose Pie chart, Pie chart (3D), Pie chart (transparent 3D), Bar chart, Bar chart (horizontal), Bar chart (transparent 3D), or Stacked Time graph.
- **Width**. Specify how wide, in pixels, the graph or chart should appear.
- **Height**. Specify how tall, in pixels, the graph or chart should appear.
- **Filter**. Click this button to apply a filter to the dashboard report. If a filter is applied, only data that meets the filter criteria is displayed in the dashboard report. After clicking, filter boxes appear below the button.

  Select the type of filter you want to apply. If appropriate, select a secondary filter type from the second filter box. For more information on filters, see *Filtering Flow Monitor dashboard reports in WhatsUp Gold* (on page 107).

Note: Filters applied here are listed at the top of the dashboard report in **Current filters**.

3 Click **OK** to save changes.

Filtering Flow Monitor workspace reports in WhatsUp Gold

You can apply filters to many Flow Monitor dashboard reports in WhatsUp Gold using the dashboard report configuration dialog.

Filtering is essentially drilling down to find more detailed information in a dashboard report.

Dashboard reports available for filtering in WhatsUp Gold:

- Top Senders
- Top Receivers
- Top Protocols
- Top Types of Service
- Top Applications
- Top Sender Domains
- Top Receiver Domains
- Top Sender Countries
- Top Receiver Countries
- Top Sender Groups
- Top Receiver Groups
- Top Sender TLD
- Top Receiver TLD
- ICMP Types

- Packet Size Distribution
- Top NBAR Applications
- Top Port
- Top Sender ASN
- Top Receiver ASN

Applied filters are listed in **Current Filter**.

Exporting dashboard report data

Exporting report data

You can export data displayed in dashboard reports by clicking the Export button on the dashboard report menu.

Note: Flow Monitor data is exported according to the parameters set in the *Flow Data Export Settings* (on page 108) dialog.

To export report data:

1. Click the Export button. The File Download dialog appears.
2. Click **Save**. The Save As dialog appears.
3. Enter, or browse to select, the location where you want to save report data. Click **Save**.

Configuring export settings

Use the Flow Export Settings dialog to configure the parameters for exporting report data. Each time you export Flow Monitor data, it will use the parameters set in this dialog. You can export data to a text file, Microsoft Excel, or a .PDF.

To configure the Flow Monitor export settings:

1. Click **Flow Monitor > Data Export Settings**. The Flow Export Settings dialog appears.
2. Select the desired options.
   - Select **Export to Text** to export Flow Monitor data to text.
   - Select **Export to Excel** to export Flow Monitor data to Microsoft Excel.
   - Select **Export to PDF** to export data to .PDF.
   - Select **Include report title** to include the report name in the exported data.
   - Select **Include column names** to include the column titles in the exported data.
   - Select **Include graphs** to include graph(s) with the exported data (available on select reports).
   - Select the Text options:

- **Column delimiter**. Select the character type you want to use to separate boxes for each set of data when reports are exported. The delimiter options are: Comma, Semicolon, Tab, or Vertical Bar.
- **Text qualifier**. Select the quote type you want to use to separate box data from column delimiters. The text qualifier options are: Double Quote, Single Quote, or None.

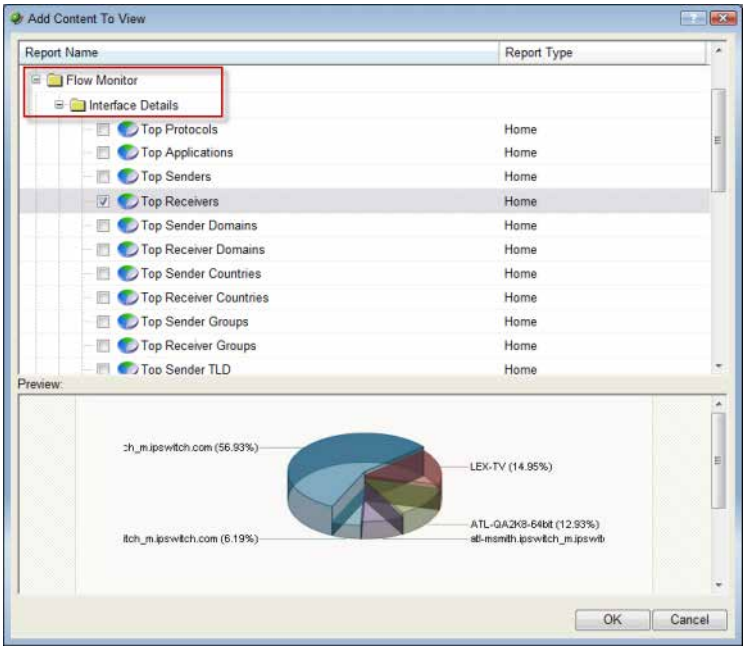
3 Click **OK** to save changes.

Linking to Flow Monitor reports from WhatsUp Gold workspace reports

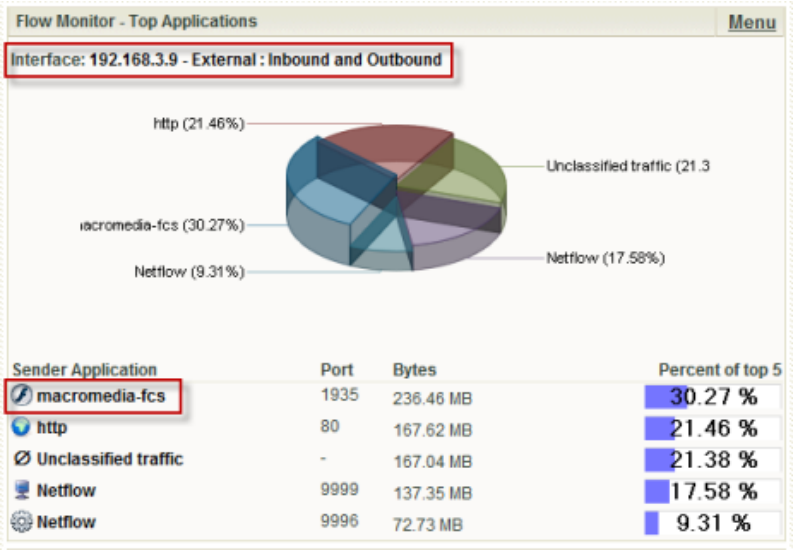
There are several ways to connect to Flow Monitor reports from WhatsUp Gold.

Linking to the Interface Details report from dashboard reports in WhatsUp Gold

The Interface Details dashboard reports in WhatsUp Gold link to the Interface Details report in Flow Monitor. The Interface Details dashboard reports can be found on the WhatsUp Gold dashboard report picker under **Flow Monitor**.



To link to the Interface Details report from an Interface Details dashboard report:



§ Click the interface name at the top of the dashboard report. The Interface Details report for the selected interface appears.

- or -

§ Click an entry in the far left column of the dashboard report. The Interface Details report for the selected interface appears. The entry that you click is applied to the report as a keyword filter.

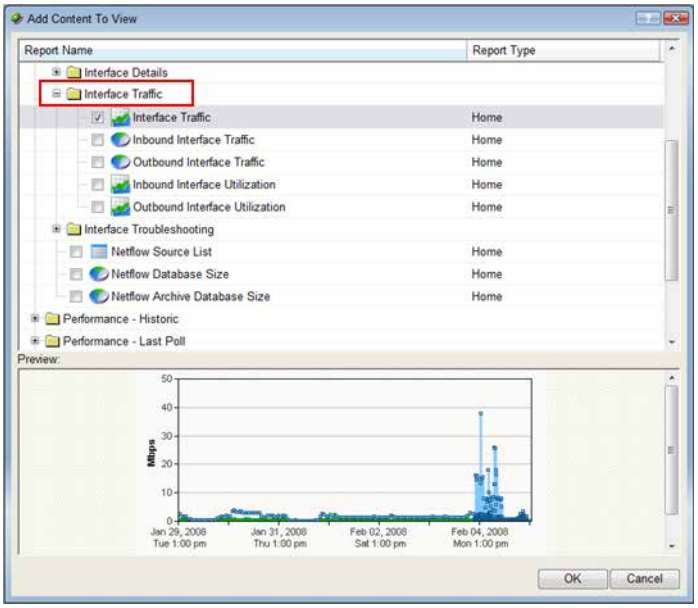
- or -

§ Click in the dashboard report's graph area. The Interface Details report for the selected interface appears.

Note: Any applied filters carry over to the Interface Details report.

Linking to the Interface Overview report from dashboard reports in WhatsUp Gold

Interface Traffic dashboard reports in WhatsUp Gold link to the Interface Overview report in Flow Monitor. Interface Traffic dashboard reports can be found on the WhatsUp Gold dashboard report picker under **Flow Monitor**.



To link to the Interface Overview report from an Interface Traffic dashboard report, click the interface name at the top the dashboard report. The Interface Overview report for that interface appears.

Finding more information and updates

The following are information resources for WhatsConfigured. This information may be periodically updated and available on the *WhatsUp Gold web site* (*http://www.whatsupgold.com/support/index.aspx*).

- **Release Notes**. The release notes provide an overview of changes, known issues, and bug fixes for the current release. The release notes are available on the *WhatsUp Gold web site* (*http://www.whatsupgold.com/WUG162releasenotes*).
- **Application Help for the console and web interface**. The console and web help contain dialog assistance, general configuration information, and how-to's that explain how to use the features. The Table of Contents is organized by functional area, and can be accessed from the main menu or by clicking **Help** in the console, or the **?** icon in the web interface.
- **Additional WhatsUp Gold resources**. For a listing of current and previous guides and help available for WhatsUp Gold products, see the *WhatsUp Gold web site* (*http://www.whatsupgold.com/support/guides.aspx*).

- **Licensing Information**. Licensing and support information is available on the *WhatsUp Customer Portal* (*http://www.whatsupgold.com/wugCustPortal*). The web portal provides enhanced web-based capabilities to view and manage Ipswitch product licenses.
- **Technical Support**. Use the WhatsUp Gold Support Site for a variety of WhatsUp Gold product help resources. From here you can view product documentation, search Knowledge Base articles, access the community site for help from other users, and get other Technical Support information. The Support Site is available on the *WhatsUp Gold web site* (*http://www.whatsupgold.com/support/index.aspx*).

Copyright notice

This document was published on Wednesday, July 24, 2013 at 09:18.