IPSWITCH

WhatsUpGold

v12.3

NetFlow Monitor User Guide

IPSWITCH

CHAPTER 1 WhatsUp Gold NetFlow Monitor Overview

CHAPTER 2 Configuring WhatsUp Gold NetFlow Monitor

CHAPTER 3 Navigating WhatsUp Gold NetFlow Monitor

CHAPTER 4 Using NetFlow reports

CHAPTER 1

WhatsUp Gold NetFlow Monitor Overview

In This Chapter

What is NetFlow?

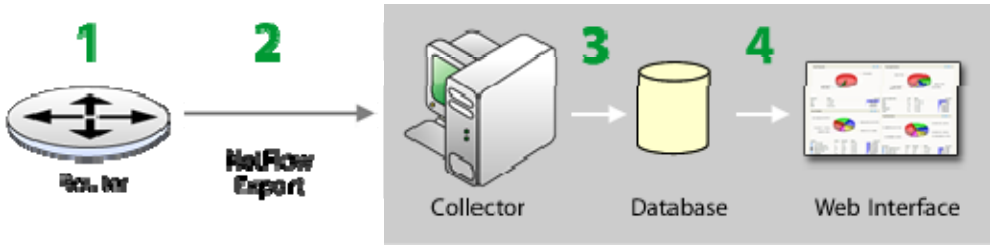
NetFlow is a network protocol that is used to report information about the traffic on a router, switch, or other traffic-conducting network device. NetFlow works by collecting and summarizing the data that is carried over a device, and then transmitting that summary to another device, called a collector, for storage and analysis.

NetFlow Monitor is a software-based NetFlow collector designed for use on servers running Microsoft Windows operating systems. After configuring routers, switches, and other devices to transmit NetFlow summary data to NetFlow Monitor, you can view 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 NetFlow Monitor work?

When a router or other device sends NetFlow data to NetFlow 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 export.
2. The router sends the NetFlow export to the NetFlow Monitor collector.
3. The NetFlow Monitor collector stores the NetFlow export in the database.
4. When the report data is viewed on the web interface, NetFlow Monitor retrieves the data from the database and manipulates it to produce the report.

Tip: WhatsUp Gold NetFlow Monitor can collect and generate reports for NetFlow data from multiple devices.

Supported versions

NetFlow Monitor can receive and interpret data from NetFlow versions 1, 5, and 9.

System requirements

WhatsUp Gold NetFlow Monitor has the same base *system requirements* (http://www.whatsupgold.com/wug123relnotes) as WhatsUp Gold v12.3. In addition, WhatsUp Gold NetFlow Monitor requires:

- WhatsUp Gold v12.3 Standard Edition, Premium Edition, MSP Edition, or Distributed Edition
- At least one routing device that supports NetFlow version 1, 5, or 9
- SQL Server 2005 Standard or Enterprise Edition (recommended)

Note: WhatsUp Gold NetFlow Monitor is more demanding on the database than WhatsUp Gold. While WhatsUp Gold NetFlow Monitor can successfully use SQL Server 2005 Express, we recommend either MS SQL Server 2005 Standard or Enterprise Edition for best performance.

- An additional 2 to 4 GB RAM recommended
- 16 GB (required) to 22 GB (recommended) hard disk space for the databases

Note: If using Microsoft® SQL Server® 2005, the database size is limited by available hard disk space.

CHAPTER 2

Configuring WhatsUp Gold NetFlow Monitor

In This Chapter

Determining which NetFlow sources to monitor

The information that NetFlow Monitor collects is influenced by the location of the NetFlow sources relative to firewalls or other devices that perform network address translation (NAT). In short, the data is dependent on what and how the source sees. Carefully consider which routers or other NetFlow-enabled devices you want to configure to export flows to NetFlow Monitor to ensure that you see the type of data that you want to see.

Depending on where the source is located relative to the device performing NAT, traffic to and from internal (private) IP address are reported differently in the exported NetFlow data.

- If the source is inside the firewall, or if no firewall exists, the exported NetFlow data includes the internal IP address for devices generating and receiving traffic. This allows you to pinpoint the exact device to which the traffic belongs.
- If the source is outside the firewall, the exported NetFlow data aggregate all traffic to and from internal devices and report it as belonging to the public address of the device performing NAT. 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.

- When the device exporting NetFlow flows is also performing NAT, you can configure the device to export the NetFlow data using either the private or the public NAT 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 IP address of the NAT device, configure the device to export data on `ingress` and `egress` for **external** interfaces. For more information, see *Configuring NetFlow sources* (on page 6).

Other conditions may also change the nature of the data reported by NetFlow Monitor.

- If NAT occurs anywhere in the path between the source and the destination, IP addresses reported are altered to include the address of the NAT. In most cases, this does not present a problem, but it may require monitoring multiple NetFlow sources 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, NetFlow 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.

Configuring NetFlow sources

Before you can view meaningful reports, you must configure NetFlow Monitor and NetFlow-enabled devices, such as routers or switches, to communicate network activity back to the NetFlow Monitor listener application.

Configuring NetFlow sources is a three-part process that requires:

1. Setting up NetFlow Monitor to listen for NetFlow data on the appropriate port.
2. Configuring NetFlow devices to send NetFlow data to NetFlow Monitor.
3. Setting options for the NetFlow source in NetFlow Monitor.

To configure NetFlow Monitor to listen for NetFlow data:

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

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. If the NetFlow section is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3. Select **Configure > NetFlow Settings**. The NetFlow Settings dialog appears.
4. In **Listener port**, enter the port number over which NetFlow Monitor should listen for NetFlow data.
5. Click **OK** to save changes.

To configure NetFlow devices to send NetFlow data to NetFlow 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 NetFlow 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>`	Sets the version of the NetFlow protocol that should be used to export data. NetFlow Monitor supports versions 1, 5, and 9 only.
`ip flow-export destination <IP> <port>`	Enables the router to export NetFlow data. Substitute the NetFlow Monitor server's IP address for <IP> and the listener port specified in the NetFlow Monitor NetFlow Settings dialog for <port>.

- **Step 2**. Enter the commands detailed in the following table to enable the router to export NetFlow 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`
- or -
`ip flow egress`
	Enables NetFlow 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 NetFlow 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.

To configure options for NetFlow sources in NetFlow Monitor:

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. If the NetFlow section is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3. Select **Configure > NetFlow Sources**. The NetFlow Sources dialog appears.
4. Select the source from the list, then select **Edit**. The NetFlow Source dialog appears.

Note: If you cannot locate a source in the list, verify that the source device is set up to export NetFlow data properly. All devices sending NetFlow data to NetFlow Monitor automatically appear in the list.

5. In **Display Name**, enter a friendly name for this NetFlow source. This name is used throughout NetFlow Monitor to identify this source.
6. Verify that **Collect data from this source** is selected.
7. Set SNMP options. NetFlow Monitor uses SNMP to query information about the interfaces on the NetFlow 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 NetFlow Sources dialog.
   c) Select **Query** to query the router using SNMP to get updated names and speeds for the available interfaces.
8. 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 **Details**. The NetFlow Interface dialog appears.
   b) Select **Hide this interface from the NetFlow Home page and related configuration properties** to hide the selected interface from the NetFlow Monitor Home page and other menu options in NetFlow Monitor. This lets you display only the interfaces that are relevant to your bandwidth monitoring requirements.
   c) Select **Specify a custom speed for this interface**. The **In** and **Out** fields 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

Note: NetFlow Monitor supports NetFlow versions versions 1, 5, and 9 only. If you export data using other versions of the NetFlow protocol or other protocols that are similar to NetFlow, such as IPFix or sFlow, NetFlow Monitor discards the data.

After you configure the listener port and set up NetFlow sources, NetFlow Monitor begins tracking data and generating reports.

Monitoring traffic on non-standard ports

NetFlow Monitor automatically classifies traffic for most common applications. However, in some cases, you may need to create a custom definition to ensure that NetFlow 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: For traffic to be considered unclassified, both the port that the data is sent from and the port to which it is received must not be classified in the NetFlow Ports dialog. If either of those ports are 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 NetFlow 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 10).

Tip: If NetFlow Monitor detects a large amount of traffic to an unmonitored port, the Top Applications workspace 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 NetFlow Monitor by selecting **GO > Configure > NetFlow Unclassified Traffic**) to view all unclassified traffic since the last hourly rollup.

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

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. If the NetFlow section is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3. Select **Configure > NetFlow Ports**. The NetFlow Ports dialog appears.
4. Click **New** to configure a new port definition. The NetFlow Port dialog appears.
5. In **Port**, enter the port number over which the traffic is sent.
6. 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).
7. Select **Monitor the following protocols on this port**, and then select the protocols that the application uses (**TCP**, **UDP**, or **SCTP**).
8. Click **OK** to save changes.

Configuring data roll-up intervals

NetFlow 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, NetFlow Monitor uses a process of summarizing data at certain time intervals.

By default, NetFlow 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 8 hours.
- After 8 hours, raw data is summarized into hourly averages.
- After 3 days, hourly averages are summarized into daily averages.
- After 14 days, daily data is archived.
- After 93 days, archive data is purged from the archive database.

You can configure the intervals to roll up data more or less frequently depending on your network's size and traffic volume.

To set data roll up time intervals:

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. If the NetFlow section is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3. Select **Configure > NetFlow Settings**. The NetFlow Settings dialog appears.

4 Under Report Data, customize the roll up intervals to meet your requirements.

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

Note: Modifying collection interval settings affects both the granularity you see in NetFlow 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.

- **Roll up raw data after**. Enter the number of days and/or hours after which raw data collected from your NetFlow devices should be rolled up. This setting determines the number of hours of raw data that can be reported on at any given time. After data has been rolled up, NetFlow Monitor can report data usage for each hour, but detailed granular data (such as bytes, flows, and percentages) is aggregated into a single value for the entire hour. By default, raw data is rolled up after 8 hours.

Caution: Modifying the roll-up settings directly affects the size of the NetFlow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, monitoring the effects on database size and application performance.

- **Roll up hourly data**. Enter the number of days after which hourly data should be rolled up into daily data. After hourly data is rolled up, NetFlow Monitor can only report aggregated totals for entire 24-hour blocks of time. By default, hourly data is rolled up after 3 days.
- **Archive daily data**. Enter the number of days after which daily data should be moved to the archive database. By default, daily data is archived after 14 days.
- **Expire archive data**. Enter the number of days after which daily archive should be purged from the archive database. By default, archive data is purged from the database after 92 days.
- **Resolve private address interval**. When the NetFlow 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 NetFlow Monitor database. Enter the interval (in hours) that you want NetFlow 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 NetFlow 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 NetFlow Monitor database. Enter the interval (in hours) that you want NetFlow 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.

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 NetFlow Monitor should purge unclassified traffic. Unclassified traffic is traffic transmitting over ports that are currently not monitored by NetFlow Monitor. By default, unclassified traffic is expired after 1 hour.

Tip: You can prevent NetFlow Monitor from saving data about unclassified traffic by setting **Expire unclassified traffic after** to 0 (zero). When this option is set to 0 (zero), NetFlow Monitor aggregates and retains data for all unclassified ports as a single value; detailed information about the individual unclassified ports over which traffic was transmitted is immediately discarded.

5 Click **OK** to save changes.

Important: Any changes made to data roll up intervals are not enforced until the NetFlow Monitor collector service is restarted. For more information, see *Stopping or restarting the collector* (on page 14).

Managing users and user rights

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

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

To grant a user the right to view NetFlow 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 From the web interface, select **GO**. The GO menu appears.
2 If the WhatsUp section is not visible, click **WhatsUp**. The WhatsUp section of the GO menu appears.
3 Select **Configure > Manage Users**. The Manage Users dialog appears.
4 Select the user to which you want to grant rights to view NetFlow Monitor reports, then click **Edit**. The Edit User dialog appears.
5 Under User rights, in the NetFlow section, select **Access NetFlow Reports**.
6 Click **OK** to save changes.

To grant a user the right to configure NetFlow Monitor:

1 From the web interface, select **GO**. The GO menu appears.
2 If the WhatsUp section is not visible, click **WhatsUp**. The WhatsUp section of the GO menu appears.
3 Select **Configure > Manage Users**. The Manage Users dialog appears.
4 Select the user you want to allow to configure NetFlow Monitor, then click **Edit**. The Edit User dialog appears.

5 Under User rights, in the NetFlow section, select **Configure NetFlow Monitor**.
6 Click **OK** to save changes.

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

Setting the logging level

You can specify the level of information that is recorded for the NetFlow Log via the NetFlow Settings dialog.

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

To set the NetFlow Monitor logging level:

1 From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2 If the NetFlow section is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3 Select **Configure > NetFlow Settings**. The NetFlow Settings dialog appears.
4 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.
5 Click **OK** to save changes.

Backing up and restoring the NetFlow Monitor databases

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

To access the database utilities:

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

Using the database backup and restore backup utility for NetFlow Monitor

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

Important: You can use this feature with any local instance of SQL Server whose *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 (WHATSUP) (or your customized SQL service) must have write access to the mapped drive.

To change the SQL database logon settings:

1. Click **Start > Control Panel > Administrative Tools > Services**, then double-click the `SQL Server (WHATSUP)` 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, select **Tools > Database Utilities > Back Up NetFlow Current** or **Archive Database**
- or -
select **Tools > Database Utilities > Restore NetFlow Current** or **Archive Database**

Stopping or restarting the collector

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

To stop or restart the NetFlow Collector Service through NetFlow Monitor:

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. Click the NetFlow Monitor icon. The NetFlow Monitor Home page appears.

3 Click the NetFlow Service icon in the bottom right corner of the page. The NetFlow Service dialog appears.
4 Click **Stop** or **Restart**. A progress dialog appears as the NetFlow Data Collector Service stops. After the action is completed, the NetFlow Service dialog appears.
5 Click **OK**.

To restart the NetFlow Collector Service through WhatsUp Gold:

From the main menu of the WhatsUp Gold console, select **Tools > Service > Restart NetFlow collector**. The service restarts.

To stop or restart the NetFlow Collector Service through Windows:

1 Open the Windows **Control Panel**.
2 Select **Administrative Tools > Services**. The Services window appears.
3 Select **Ipswitch NetFlow Collector**, then click **Stop**. The service stops.
4 To restart the service, select **Ipswitch NetFlow Collector** again, then click **Start**. The service starts.

Using NetFlow 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 NetFlow Monitor cannot automatically determine their domains, top level domains, or countries.

To overcome this limitation, NetFlow 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 From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2 If the NetFlow section is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3 Select **Configure > NetFlow Groups**. The NetFlow Groups dialog appears.
4 Click **New**. The NetFlow Group dialog appears.

- or -
Select a group, then click **Edit**. The NetFlow Group dialog appears.

5 Enter or select the appropriate information in the following fields.

- **Group**. Enter a name for the NetFlow group.
- **IP Range Start**. Enter the first IP address for the NetFlow source group range.

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

6 Click **OK** to save changes.

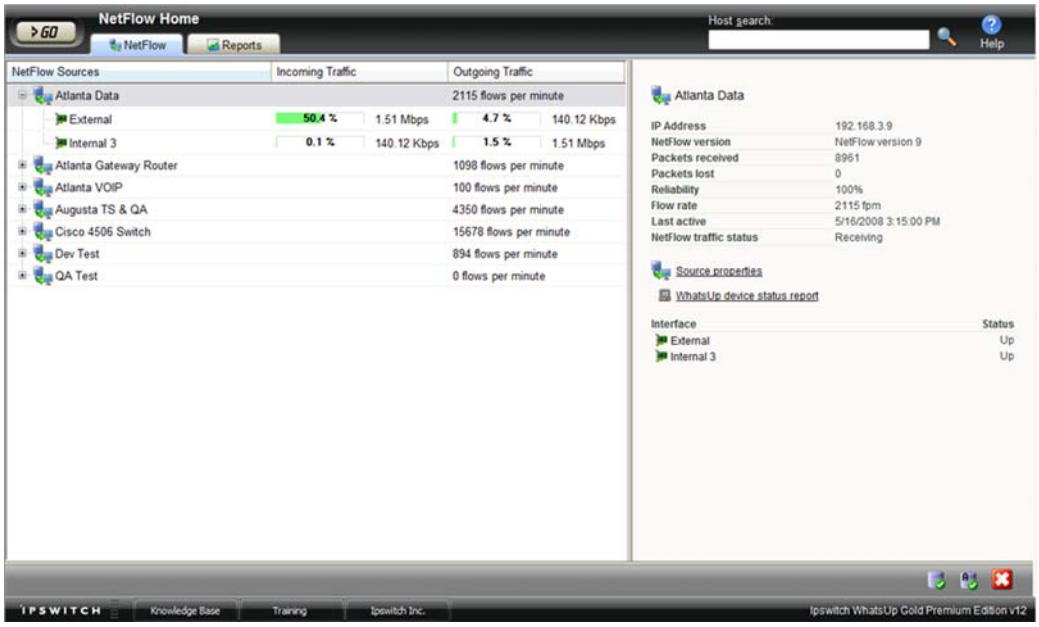
CHAPTER 3

Navigating WhatsUp Gold NetFlow Monitor

In This Chapter

About the NetFlow Home page

The NetFlow Monitor Home page provides overview information about the network sources that NetFlow Monitor is monitoring. Use this page to view high-level information about network traffic and flows and to drill deeper into each interface for more detailed information. You can also access NetFlow Monitor database and Data Collector Service information using the links at the bottom right side of the page.



NetFlow sources

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

- **NetFlow Sources**. Routers and switches that have been configured to send NetFlow data to NetFlow Monitor and are enabled in NetFlow 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) generated by all interfaces on the selected source over the last half hour is displayed.

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

Tip: If you do not see a source listed that you would like to monitor, first go to the NetFlow 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 NetFlow data. For more information, see *Configuring NetFlow sources* (on page 6).

- **Incoming Interface Traffic**. Incoming traffic is reported as a percentage of usage according to the interface's speed, and as the number of incoming bytes per second (bps).
- **Outgoing Interface Traffic**. Outgoing traffic is reported as a percentage of usage according to the interface's speed, and as the number of outgoing bytes per second (bps).

Source and interface details

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

Note: If you have no enabled NetFlow sources at this time, a Welcome workspace report is displayed on the right side of the NetFlow Home page. Consult this workspace report for information on configuring your routers to send NetFlow data, and for other general NetFlow Monitor configuration information.

Source details

- **IP address**. The source router's IP address.
- **NetFlow version**. The version of NetFlow the source uses when exporting NetFlow 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 for the last half-hour.
- **Last active**. The last time traffic was received from the source.
- **NetFlow traffic status**. Whether NetFlow 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 is displayed as receiving.

Use the links at the bottom of the source details to view the NetFlow Source dialog, and the WhatsUp Gold Device Status report.

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

Interface details

The Interface Traffic report for the last half-hour is displayed at the top of the interface's details.

- **Last active**. The last time traffic transmitted over the 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 NetFlow Interface Properties.

NetFlow Monitor database and service icons

Database and service icons are located in the bottom right of the page. These icons display information about the NetFlow Monitor database, archive database, and NetFlow Monitor service. Position the mouse cursor over an icon to view size and status information. For more information, please see About NetFlow Monitor database and service icons.

Position the mouse cursor over the NetFlow Database icon to view the database edition and current size (in megabytes). Click the icon to view the NetFlow Database Properties.

Position the mouse cursor over the NetFlow Archive Database icon (located to the right of the NetFlow Database icon) to view the archive database edition and current size (in megabytes). Click the icon to view the NetFlow Database Properties.

Position the mouse cursor over the NetFlow Service icon to view the service status. Click the icon to view the NetFlow Monitor Service Properties.

Note: If you are using Internet Information Services as the web server for WhatsUp Gold and it is running as a user that does not have administrative privileges, the web interface cannot interact with Windows services. This means that you cannot view the status of services or start, stop, or restart services from the web interface. In this case, you must log in to Windows to manage services through the Control Panel.

Tip: Use the right-click menu on this page to view and configure parts of the application. For more information, see *Using the NetFlow Home page right-click menu* (on page 20).

Tip: 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. For more information, see *Searching for specific hosts* (on page 22).

About NetFlow Monitor database and service icons

The NetFlow Monitor database, archive database, and service icons are displayed in the lower right corner of the NetFlow Monitor Home page. Position the mouse cursor over an icon to view size and status information.

Icon	Description
	When the database and archive database icons are green, the database sizes are at healthy levels.
	When the database and archive database icon are red, the database sizes are too large, or there is a database error.
	When the NetFlow Monitor service icon is green, the service is running.
	When the NetFlow Monitor service icon is red, the service has stopped.

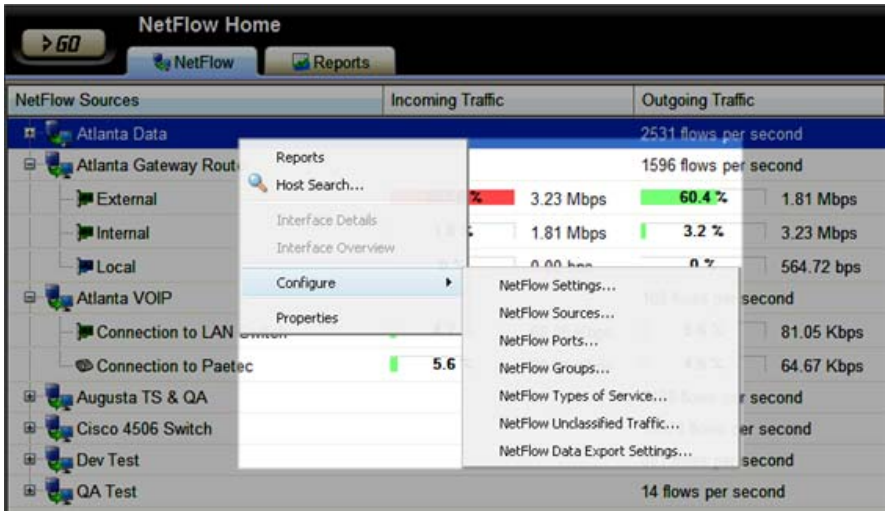
NetFlow Database Properties

To view the properties for the NetFlow Database and Archive Database, click the database or archive database icons.

Using the NetFlow Home page right-click menu

From the NetFlow Monitor Home page, you can right-click on a source or interface to access a right-click menu with links to common tasks.

Note: The right-click menu shows options available for the object on which you right-click. Depending on the object you right-click, the available options may vary.



The right-click menu includes these options:

- **Reports**. Select this option to open the Reports tab.
- **Host Search**. Select this option to open the Host Search dialog. From this dialog, you can search all sources and interfaces for traffic that uses a specific host. For more information, see *Searching for specific hosts* (on page 22).
- **Interface Details**. Select this option to view the Interface Details report for the selected interface. This report is a collection of views that provide quick insight into the traffic transmitting across a specific interface.
- **Interface Overview**. Select this option to view the Interface Overview report for the selected interface. This report is a collection of NetFlow workspace reports that provide a summary of the traffic and utilization of a specific interface.
- **Configure**. Select a configuration option:
  - **NetFlow Settings**. Select this option to configure general settings in the NetFlow Settings dialog.
  - **NetFlow Sources**. Select this option to open the NetFlow Sources dialog. From this dialog, you can view and change a device source configuration or stop and start data collection from a source, select a source and click **Edit**.
  - **NetFlow Ports**. Select this option to open the NetFlow Ports dialog. From this dialog, you can see the definitions of applications (traffic over a given port using one or more protocols) that NetFlow Monitor is monitoring. You can also use this dialog to define new applications.
  - **NetFlow Groups**. Select this option to open the NetFlow Groups dialog. From this dialog, you can create, change, or delete an IP range of devices, in a NetFlow Group, that may not have been automatically associated with a domain, top level domain, or country.
  - **NetFlow Types of Service**. Select this option to open the NetFlow Types of Service dialog. From this dialog, you can view and rename NetFlow Types of Service to make the NetFlow Top Types of Service workspace report more meaningful and easy to identify.

- **NetFlow Unclassified Traffic**. Select this option to open the NetFlow Unclassified Traffic dialog. From this dialog, you can map ports that have not been mapped to an application and are currently unmonitored.
- **NetFlow Data Export Settings**. Select this option to configure the parameters for exporting NetFlow report data.

- **Properties**. Select this option to open either the NetFlow Source Properties dialog, or the NetFlow Interface Properties dialog. From these dialogs, you can view information about the selected source or interface properties.

Searching reports for specific host names

The Host Search tool allows you to search across the interfaces of all sources to find traffic to or from a specific host.

The Host Search tool is available in several locations throughout NetFlow Monitor and WhatsUp Gold. For more information, see Locating the NetFlow Monitor Host Search tool. Although the navigation to the Host Search tool varies, the search process is the same after you navigate to the feature.

To perform a host search from the GO menu:

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. If the NetFlow section of the GO menu is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3. Select **Reports > Host Search**. The Host Search dialog appears.

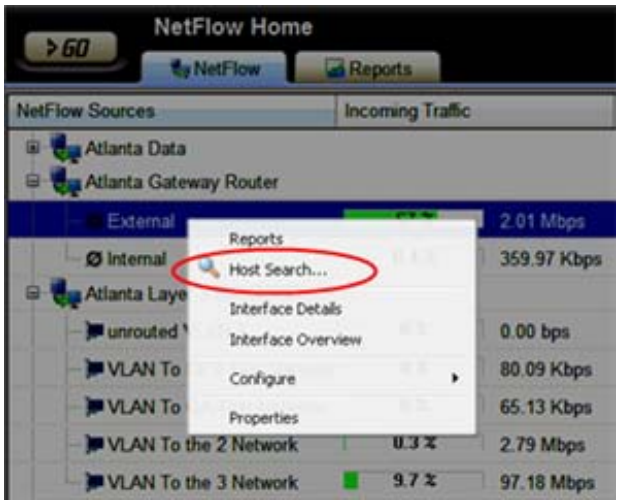
4. Select a search criteria from the list (contains, does not contain, is, is not, starts with, ends with).
5. Enter an alphanumeric search criteria in the blank field.

6 Click **Search**. After the search has completed, the dialog expands to display the search results list.

7 For more detail on a host in the list, select it, then click **OK**. The NetFlow Select Interface dialog for the selected interface appears.

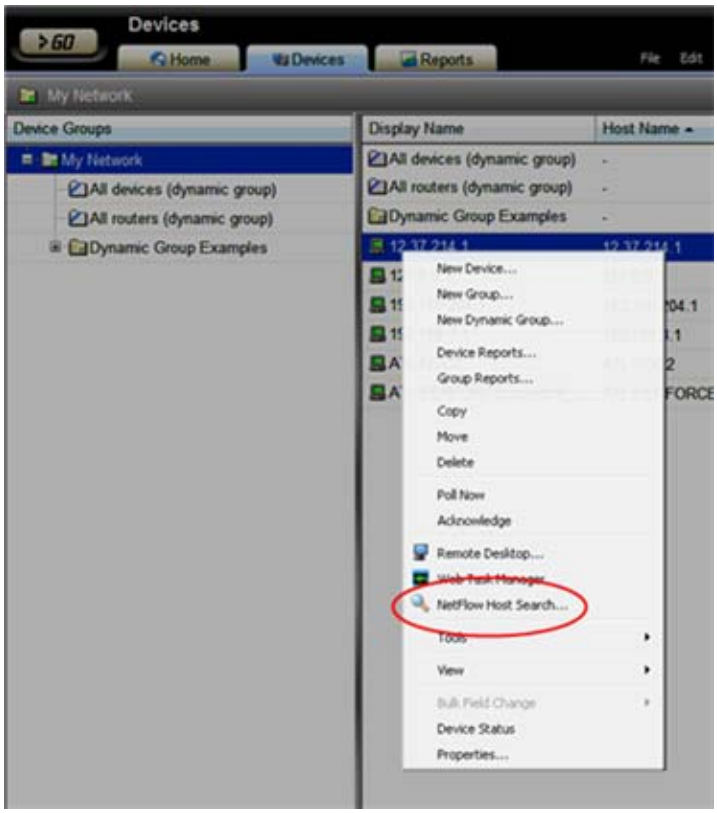
To perform a host search from the right-click menu:

1 From the NetFlow Home page, right-click a source or an interface. The NetFlow Home page right-click menu appears.



- or -

From the WhatsUp Devices tab, right-click a device. The WhatsUp Devices right-click menu appears.



2 Select **Host Search** from the NetFlow right-click menu, or **NetFlow Host Search** from the WhatsUp right-click menu. The Host Search dialog appears.

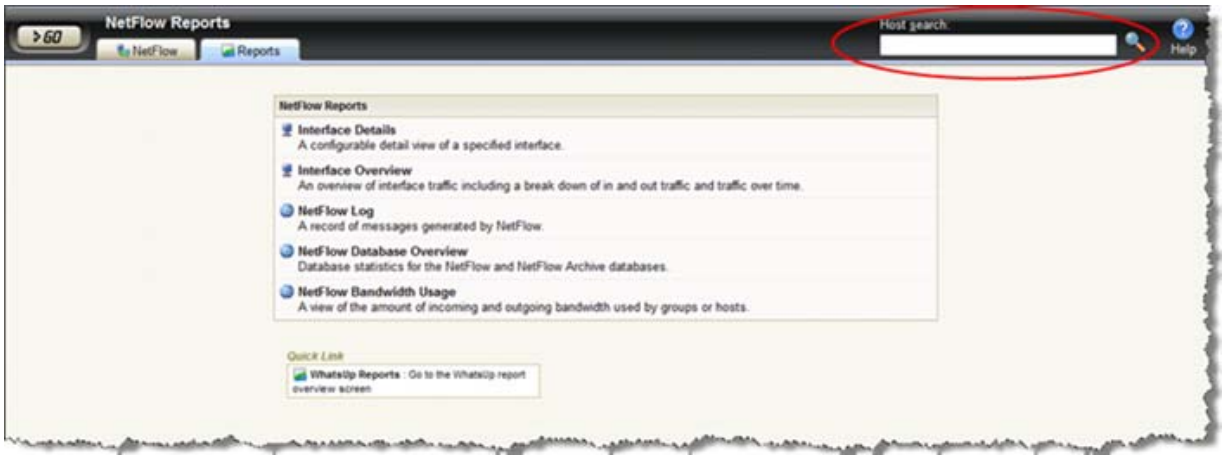
3 Select a search criteria from the list (contains, does not contain, is, is not, starts with, ends with).

4 Enter an alphanumeric search criteria in the blank field.

5 Click **Search**. After the search has completed, the dialog expands to display the search results list.

6 For more detail on a host in the list, select it, then click **OK**. The NetFlow Select Interface dialog for the selected interface appears.

To perform a host search from the NetFlow Home page or Reports tab:



1 From the NetFlow Home page or Reports tab, enter an alphanumeric value in **Host Search**, then press **Enter**. The Host Search dialog appears, populated with the results of the host search.

The default search criteria for the host search is "contains." Adjust the search criteria as needed to perform the search you desire, then click **Search**. The dialog re-populates with the results of the new search.

2 For more detail on a host in the list, select it, then click **OK**. The NetFlow Select Interface dialog for the selected interface appears.

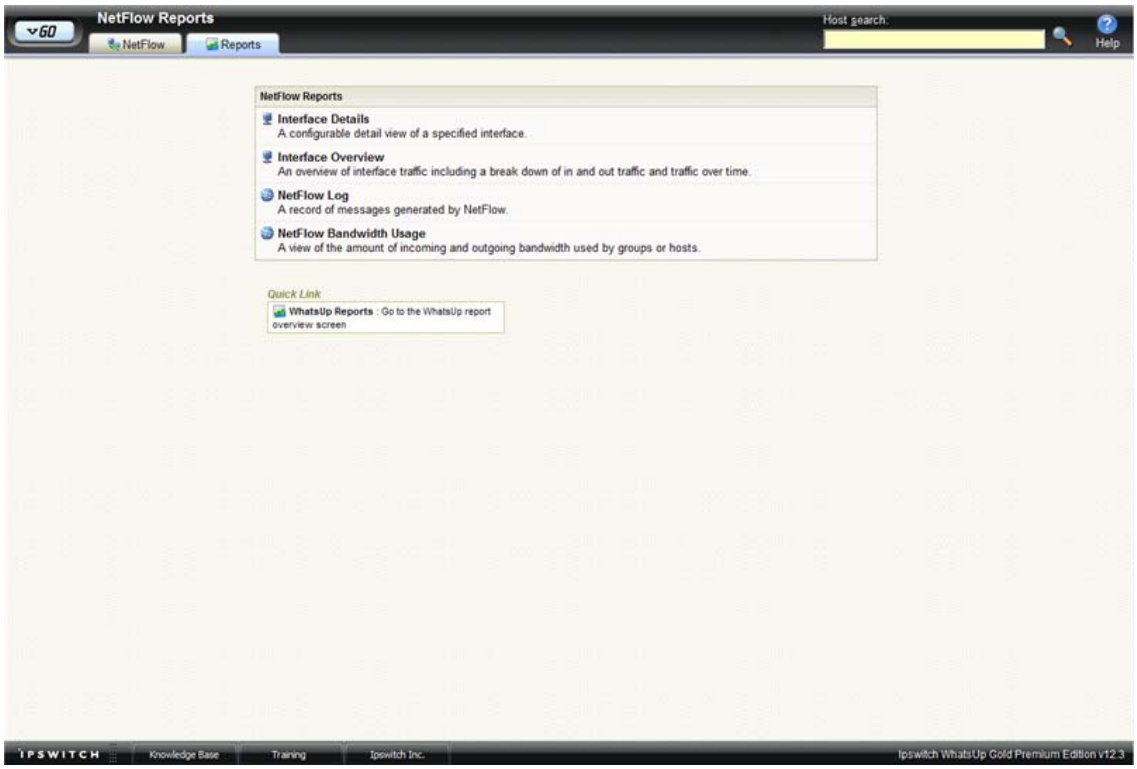
CHAPTER 4

Using NetFlow reports

In This Chapter

About the Reports tab

The NetFlow Monitor Reports tab lists the available NetFlow reports.



These NetFlow Monitor reports are available:

- Interface Details
- Interface Overview

- NetFlow Log
- NetFlow Bandwidth Usage

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

Tip: You can access the WhatsUp Gold reports by clicking the **WhatsUp Reports** Quick Link.

About the Interface Details report

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

When you first access the NetFlow 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 28).
- **Filter report results**. You can filter the current workspace reports to show only data matching search criteria. For more information, see *Filtering by keywords* (on page 30). You can also drill-down into certain report entries. For more information, see *Filtering by drilling-down* (on page 31).
- **Managing report views**. Use the **Workspace 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.

For more information on how to refine the NetFlow Interface Details report, see *Filtering data in a view* (on page 28).

Tip: You can view the **Interface Overview** (on page 32) report for the selected interface by clicking Interface Overview at the top of the page.

General view

The NetFlow 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 workspace reports:

- Top Protocols
- Top Applications
- Top Senders
- Top Receivers
- Top Sender Domains
- Top Receiver Domains

You can add additional Interface Details workspace reports to the General view, or delete an existing workspace report from both the **Edit Layout** button and the **Workspace View** list. For more information, see *Managing NetFlow Interface Details report views* (on page 27).

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

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

Managing report views

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

To customize an existing view:

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. Click the NetFlow Monitor icon. The NetFlow Monitor Home page appears.
3. From the list of NetFlow sources, select an interface. The NetFlow Interface Details report appears.
4. From the **Workspace View** list in the toolbar, select the view you want to customize. The view you select appears.
5. In the toolbar, click **Edit View**. The Configure NetFlow Interface Report dialog appears.
6. 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.
7. Click **OK** to save changes. The customized NetFlow Interface Details report appears.

To create a new NetFlow Interface Details report view:

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. Click the NetFlow Monitor icon. The NetFlow Monitor Home page appears.
3. From the list of NetFlow sources, select an interface. The NetFlow Interface Details report appears.

4 From the **Workspace View** select list in the toolbar, select **Add View**. The Configure NetFlow Interface Report dialog appears.

5 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.

6 Click **OK** to save changes. The NetFlow Interface Details report appears and displays the new view.

To delete a NetFlow Interface Details report view:

1 From any workspace view or report in the web interface, select **GO**. The GO menu appears.

2 Click the NetFlow Monitor icon. The NetFlow Monitor Home page appears.

3 From the list of NetFlow sources, select an interface. The NetFlow Interface Details report appears.

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

5 From the **Workspace View** select list in the toolbar, select **Delete Current View**. You will be prompted to confirm you want to delete the current view.

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

Selecting an interface

The NetFlow Monitor Interface Details, Interface Overview, and Bandwidth Usage reports display data in context of a single interface on the source router or switch.

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 NetFlow Interface Details report views shows data for the previous fifteen minutes.

To change the time frame for which the NetFlow 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** fields appear.

Note: NetFlow 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 NetFlow database and the NetFlow 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 click the calendar icon to quickly select a date.

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

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 29).

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.

Filtering by traffic direction

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

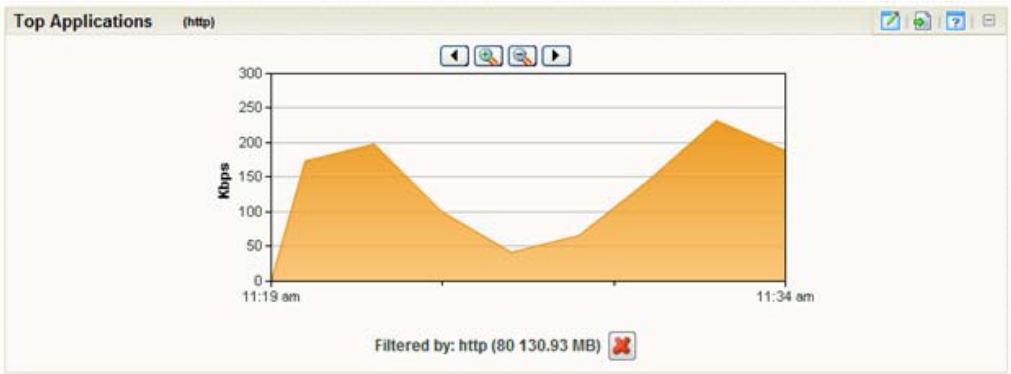
To filter report data by traffic direction:

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.
   - **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 NetFlow 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 workspace 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 workspace 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 workspace report contains the time graph by looking for the filter enclosed in parenthesis to the right of the workspace 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 fields appear below the button.
2. Select the type of filter you want to apply.
   - **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 NetFlow 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).
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.

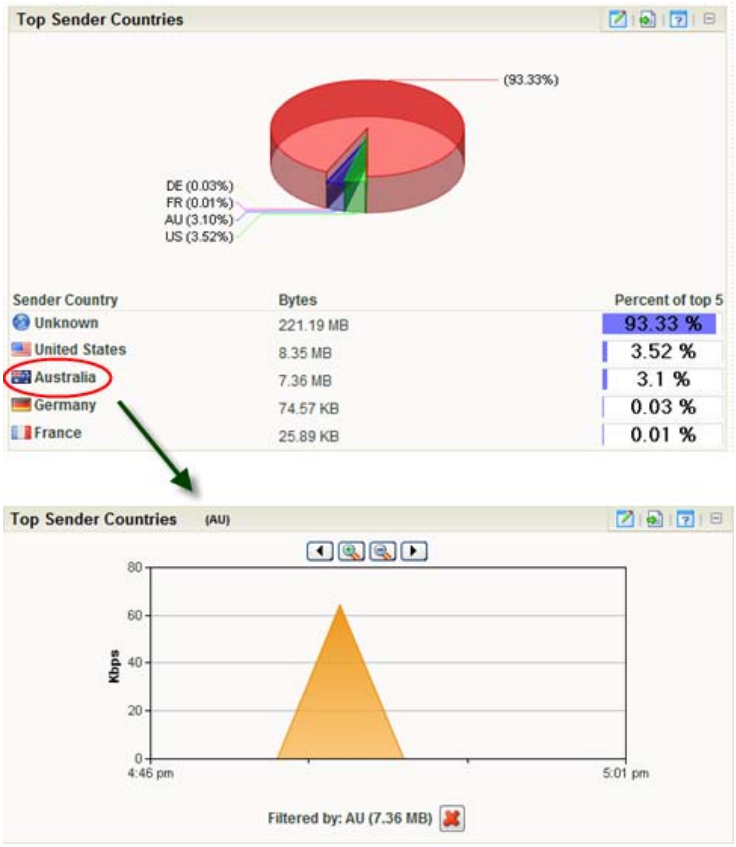
Tip: If you configure a filter incorrectly, you can remove it from the current view by clicking the red X located to the right of the keyword field.

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 workspace report, the report reloads using the entry as a filter. Also, you can click inside a workspace report's graph area to apply a filter.

Similarly to filtering by keywords, after you apply a filter to the report, the workspace 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 workspace report, the workspace report reloads with a time graph for the country that you clicked.



Several keyword filters coincide with more than one workspace report and more than one time graph is displayed after the filter is applied. You can easily distinguish which workspace 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 Overview report

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

The NetFlow Interface Overview consists of individual NetFlow workspace reports that highlight both incoming and outgoing traffic and utilization for the selected interface.

- 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 NetFlow Source list.

There are several ways you can control the data shown in 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.
- **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 28).

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

Filtering report data

You can filter the data displayed in the Interface Overview by *time and date* (on page 33). 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 NetFlow Interface Overview report shows data for the previous fifteen minutes.

To change the time frame for which the NetFlow 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** fields appear.

Note: NetFlow 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 NetFlow database and the NetFlow 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 click the calendar icon to quickly select a date.

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

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 29).

About the NetFlow Log

The NetFlow Log is a history of system-wide messages generated by NetFlow Monitor. When you access the NetFlow Log, it shows messages generated during the time period selected at the top of the report.

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: NetFlow 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 NetFlow database and the NetFlow 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.

Filtering report data

You can filter the NetFlow Log by two criteria.

- *Date and time* (on page 35)
- *Severity level* (on page 36)

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 NetFlow Log shows data for the previous fifteen minutes.

To change the time frame for which the NetFlow 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** fields appear.

Note: NetFlow 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 NetFlow database and the NetFlow 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 click the calendar icon to quickly select a date.

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 NetFlow Log displays data for the Verbose severity level.

To change the severity level for which the NetFlow 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.

Exporting report data

You can export data displayed in the NetFlow Log by clicking the Export button at the top right of the report.

Note: NetFlow data is exported according to the parameters set in the *NetFlow Data Export Settings* (on page 49) dialog.

To export report data:

1 Click the Export 

button. The File Download dialog appears.
2 Click **Save**. The Save As dialog appears.

Enter, or browse to select, the location where you want to save report data. Click **Save**.

About the NetFlow Bandwidth Usage report

The NetFlow Bandwidth Usage report displays network bandwidth usage information.

The report consists of NetFlow workspace reports that summarize the incoming and outgoing traffic for NetFlow groups and hosts.

- Bandwidth Usage by Group displays bandwidth usage summaries for each of your NetFlow groups for the selected time period.
- Bandwidth Usage by Host displays bandwidth usage summaries for NetFlow 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 28).

Note: NetFlow 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 NetFlow database and the NetFlow 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 workspace reports in this report

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

- **Configure the report**. Use the configure button on a workspace report menu to change the report configuration. For more information, see Configure NetFlow dialog.
- **Expand and collapse workspace reports**. Use the collapse and expand buttons on the report toolbar to open and close the workspace reports within the report.

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

Export workspace report data

Use the Export button on a workspace report's menu to export data to either text or Microsoft Excel. For more information, see *Exporting report data* (on page 49).

Selecting an interface

The NetFlow Monitor Interface Details, Interface Overview, and Bandwidth Usage reports display data in context of a single interface on the source router or switch.

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 38)
- *Traffic direction* (on page 38)

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 NetFlow Bandwidth Usage report shows data for the previous fifteen minutes.

To change the time frame for which the NetFlow 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** fields appear.

Note: NetFlow 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 NetFlow database and the NetFlow 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 click the calendar icon to quickly select a date.

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 NetFlow 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.

CHAPTER 5

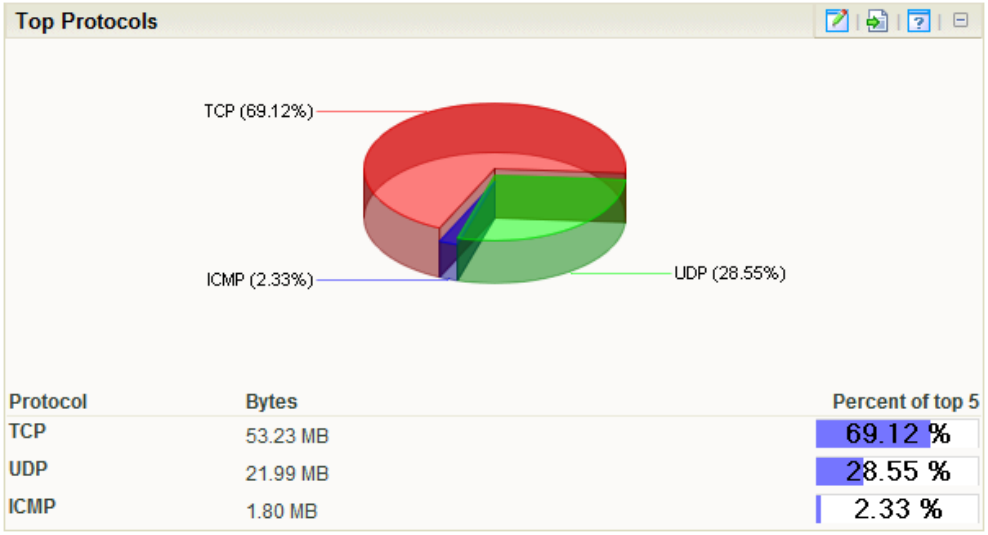
Using workspace reports

In This Chapter

Understanding NetFlow Monitor workspace reports

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

NetFlow workspace reports typically consist of a graph and a table of data related to the graph.



Workspace reports that display data from NetFlow Monitor can be used within NetFlow Monitor report views and WhatsUp Gold workspace views.

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

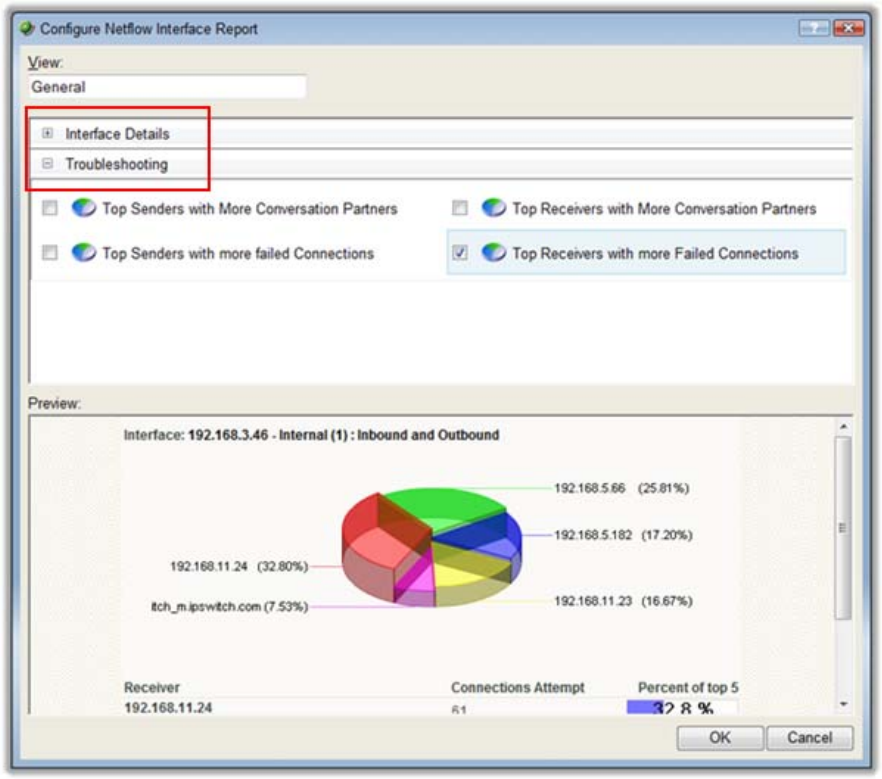
NetFlow workspace report types

There are three types of NetFlow workspace reports.

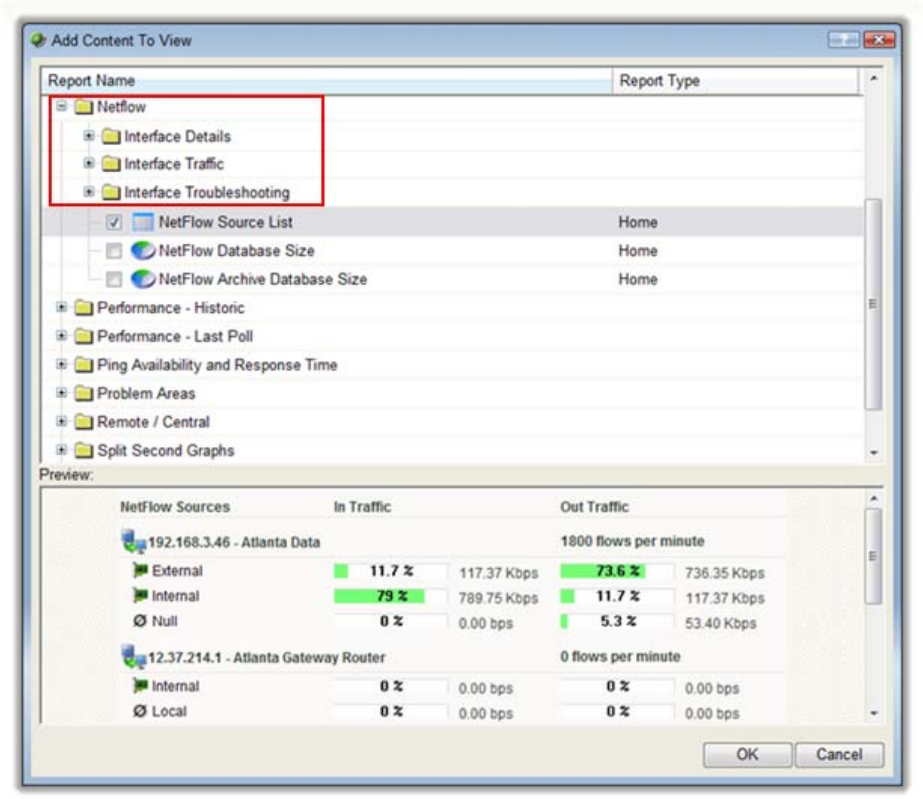
- **Interface Details** workspace reports display summary information about specific details of an interface; for example, applications, protocols, and types of service.
- **Interface Troubleshooting** workspace reports display data that would be useful in troubleshooting bandwidth problems; for example,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

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



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



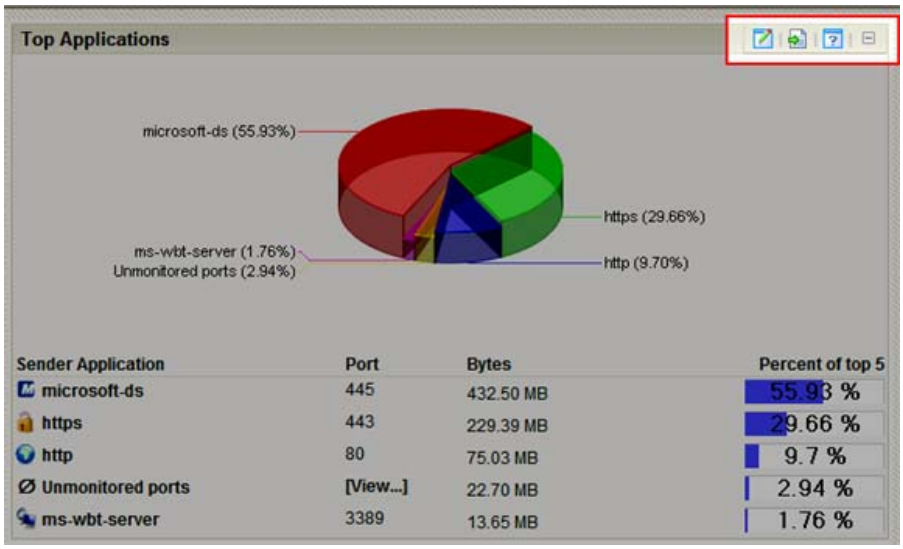
Navigating workspace reports

There are several ways to navigate NetFlow workspace reports.

- *Workspace report menu* (on page 44) gives you options to configure and access help for each workspace report.
- *Links* (on page 44) allow you to apply any criteria shown in a report as a filter.
- *Zoom control* (on page 45) lets you change the amount of data shown in line graphs.
- *Informational tooltips* (on page 46) alert you to conditions which may warrant further investigation.

Using the workspace report menu

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



Workspace 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.

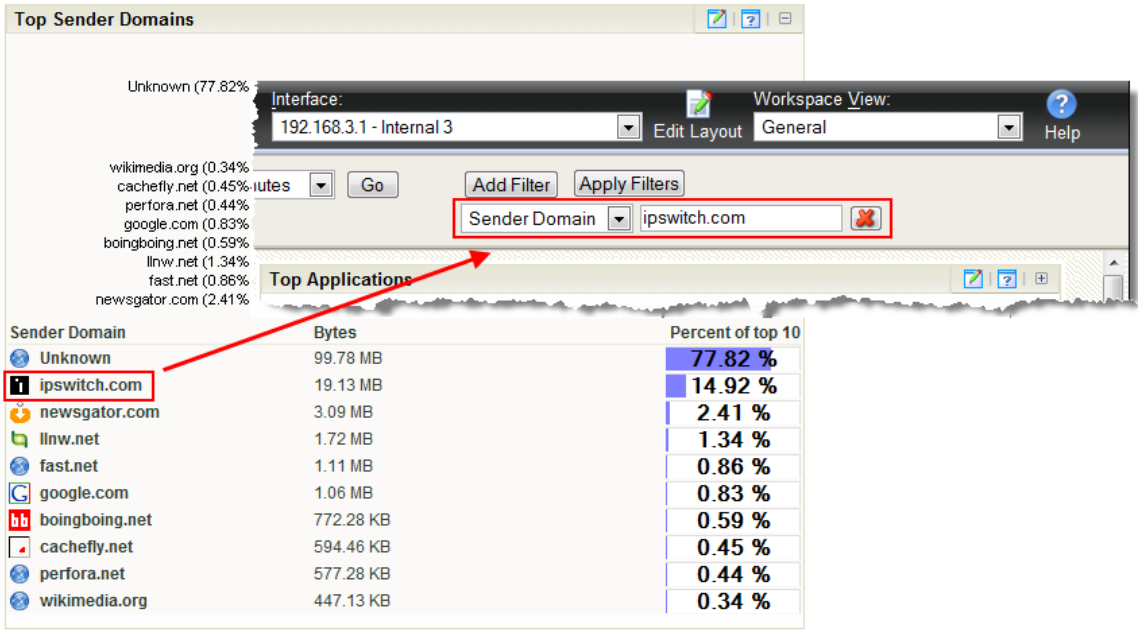

Click the **Expand** button to expand the report within the workspace view.


Click the **Collapse** button to collapse the report within the workspace view. Collapsing a report does not remove it from the workspace view.

Using links in NetFlow workspace reports

Each NetFlow workspace 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 workspace report's rows (or on a pie graph's wedges, or a bar graph's bars), the NetFlow Interface Details report appears with the selected data applied as a filter.

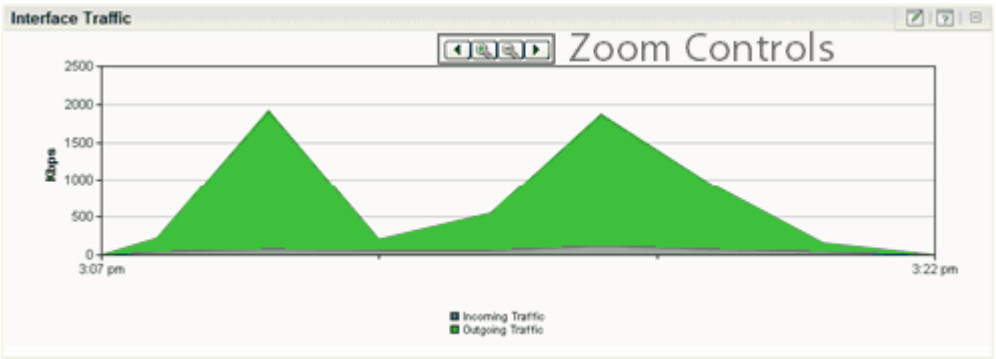
For example, as illustrated in the graphic below, if you click on `ipswitch.com` in the Top Sender Domains workspace report, the NetFlow Interface Details report appears with a Sender Domain filter set to `ipswitch.com`.



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

Using zoom controls on line graphs

Workspace 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 workspace report.



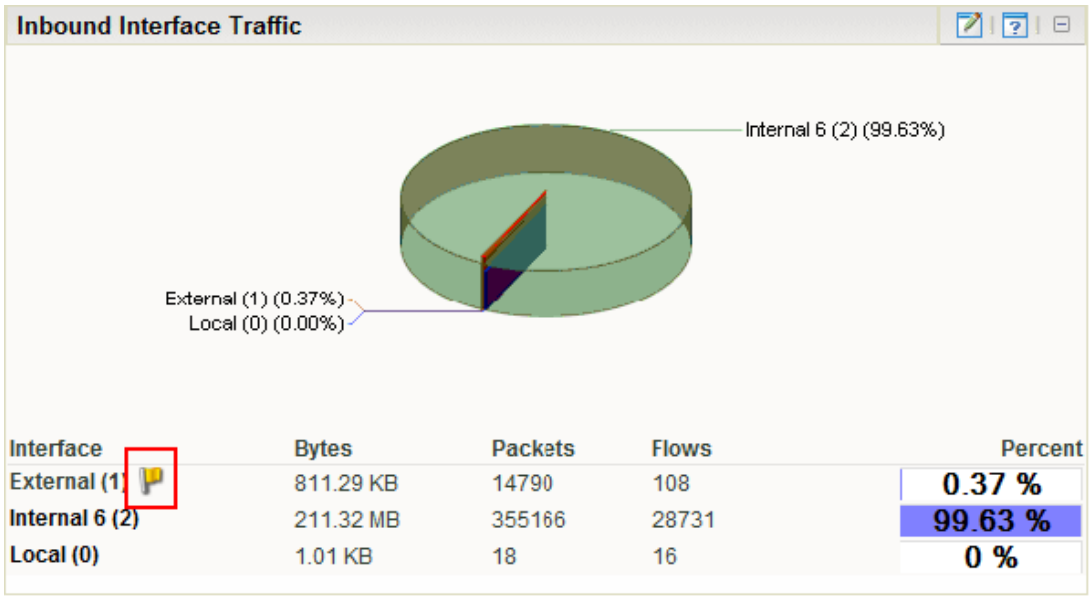
Zoom controls

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 NetFlow 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 NetFlow Monitor. It is not possible to disable individual tooltips.

To disable informational tooltips throughout NetFlow Monitor:

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. If the NetFlow section is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3. Select **Configure > NetFlow Settings**. The NetFlow Settings dialog appears.
4. Clear **Enable information tooltips**.
5. Click **OK** to save changes.

Configuring workspace reports

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

To configure a NetFlow workspace report in NetFlow Monitor:

1. In the title bar of the workspace report pane, click the Configure button . The Configure Report dialog appears.
2. Enter or select the appropriate information in the following fields.
   - **Report name**. Enter a title for the workspace report. This name appears in the title bar of the workspace report's pane.
   - **Maximum rows to return**. Enter the number of records you would like displayed in the workspace report.
   - **Display**. Select the type of data you would like displayed within the workspace report (Chart and data, Data only, Chart only).
   - **Chart type**. Select the type of chart you would like the report to display.
   - **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 NetFlow workspace report in WhatsUp Gold:

1. In the title bar of the workspace report pane, click **Menu > Configure**. The Configure Report dialog appears.
2. Enter or select the appropriate information in the following fields.
   - **Report name**. Enter a title for the workspace report. This name appears in the title bar of the workspace 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 rows to return**. Enter the number of records you would like displayed in the workspace report.
   - **Display**. Select the type of data you would like displayed within the workspace report (Chart and data, Data only, Chart only).

- **Chart type**. Select the type of chart you would like the report to display.
- **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 workspace report. If a filter is applied, only data that meets the filter criteria is displayed in the workspace report. After clicking, filter fields appear below the button.

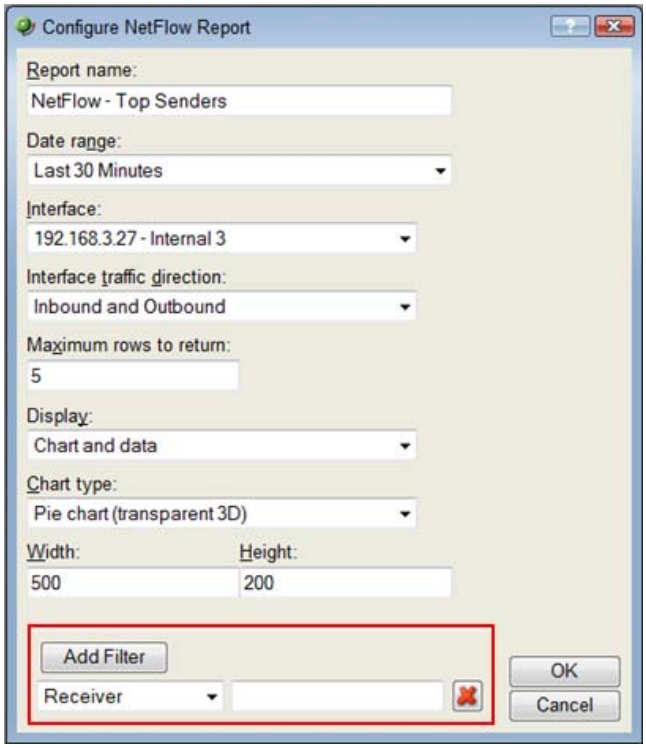
  Select the type of filter you want to apply. If appropriate, select a secondary filter type from the second filter field. For more information on filters, see *Filtering NetFlow Monitor workspace reports in WhatsUp Gold* (on page 48).

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

3 Click **OK** to save changes.

Filtering NetFlow Monitor workspace reports in WhatsUp Gold

You can apply filters to many NetFlow workspace reports in WhatsUp Gold using the workspace report configuration dialog.



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

Workspace 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

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

Exporting workspace report data

Exporting report data

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

Note: NetFlow data is exported according to the parameters set in the *NetFlow Data Export Settings* (on page 49) 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 the export settings

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

To configure the NetFlow Monitor export settings:

1. From any workspace view or report in the web interface, select **GO**. The GO menu appears.
2. If the NetFlow section is not visible, click **NetFlow**. The NetFlow section of the GO menu appears.
3. Select **Configure > NetFlow Data Export Settings**. The NetFlow Export Settings dialog appears.

4 Select the desired options.

- Select **Export to Text** to export NetFlow data to text.
- Select **Export to Excel** to export NetFlow data to Microsoft Excel.
- 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 the Text options:
  - **Column delimiter**. Select the character type you want to use to separate fields 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 field data from column delimiters. The text qualifier options are: Double Quote, Single Quote, or None.

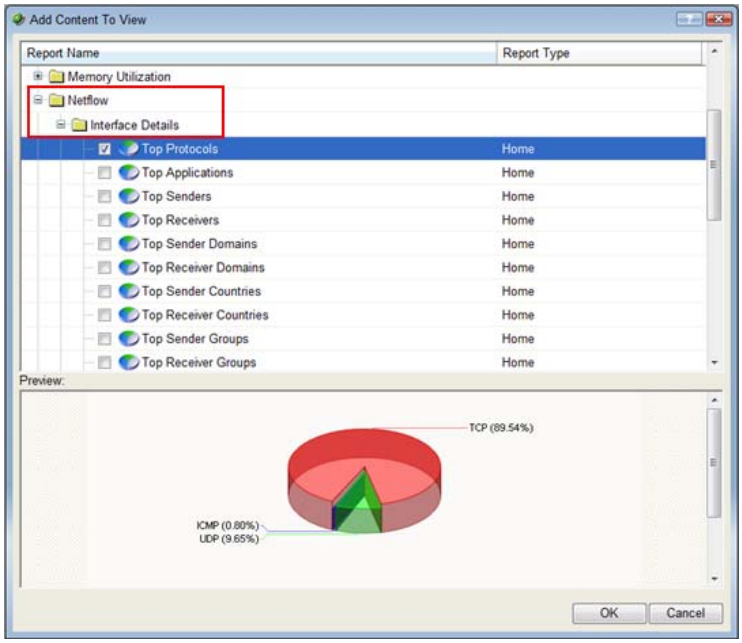
5 Click **OK** to save changes.

Linking to NetFlow Monitor reports from WhatsUp Gold workspace reports

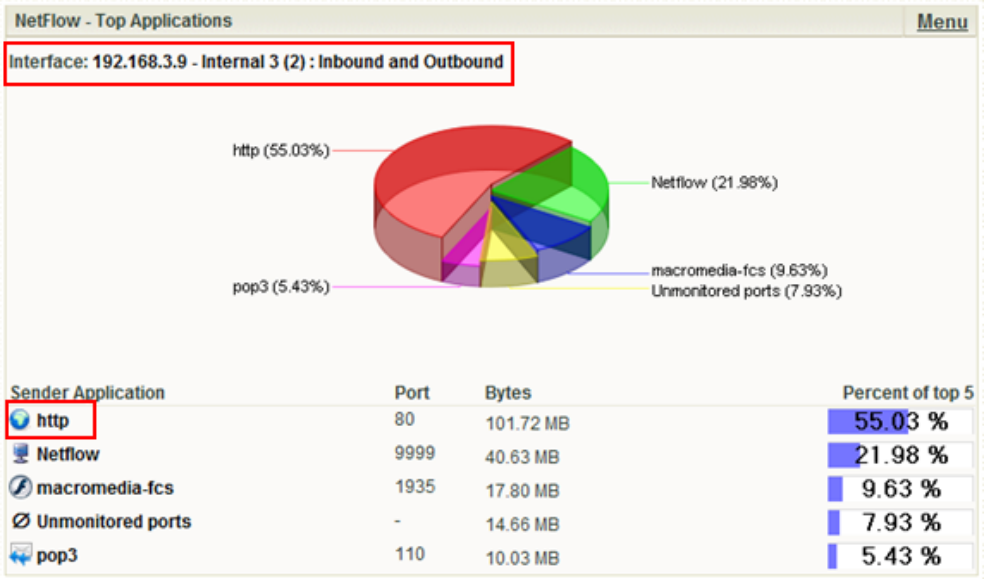
There are several ways to connect to NetFlow Monitor reports from WhatsUp Gold.

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

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



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



- Click the interface name at the top of the workspace report. The Interface Details report for the selected interface appears.

  - or -

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

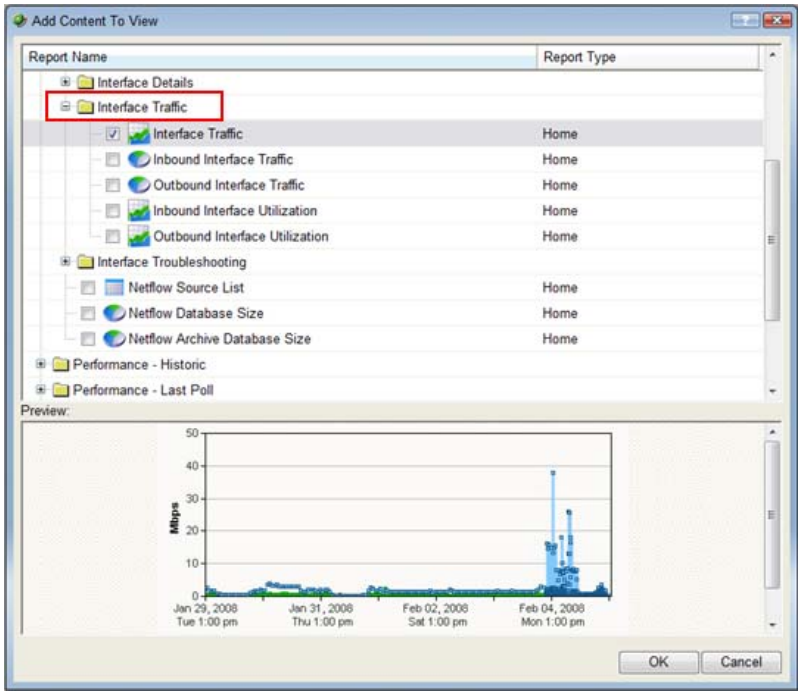
  - or -

- Click in the workspace 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 workspace reports in WhatsUp Gold

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



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

Finding more information and updates

Following are information resources for WhatsUp Gold. This information may be periodically updated and available on the *WhatsUp Gold Web site* (http://www.whatsupgold.com/support/index.asp).

- **NetFlow Monitor Release Notes**. The NetFlow Monitor release notes provide an overview of the product, system requirements, and known issues for the current release. The notes also contain instructions for installing, upgrading, and configuring NetFlow Monitor. The release notes are available in the *WhatsUp Gold plug-ins documentation* (http://www.whatsupgold.com/wugplugins).

- **WhatsUp Gold Release Notes**. The release notes provide an overview of changes, known issues, and bug fixes for the current release. The notes also contain instructions for installing, upgrading, and configuring WhatsUp Gold. The release notes are available at **Start > Programs > Ipswitch WhatsUp Gold > Release Notes** or on the *WhatsUp Gold web site* (http://www.whatsupgold.com/wug123relnotes).
- **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.
- **WhatsUp Gold Getting Started Guide**. This guide provides an overview of WhatsUp Gold, information to help you get started using the application, the system requirements, and information about installing and upgrading. The Getting Started Guide is available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/wug123gsg).
- **WhatsUp Gold User Guide**. This guide describes how to use the application out-of-the-box. It is also useful if you want to read about the application before installing. To view or download the User Guide, select **Help > WhatsUp Gold User Guide** or download it from the *WhatsUp Gold web site* (http://www.whatsupgold.com/wug123ug).
- **Additional WhatsUp Gold guides**. For a listing of current and previous guides and help files available for WhatsUp Gold's multiple versions, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/support/guides.aspx).
- **WhatsUp Gold optional plug-ins**. You can extend the core features of WhatsUp Gold by installing plug-ins. For information on available plug-ins and to see release notes for each plug-in, see *WhatsUp Gold plug-ins documentation* (http://www.whatsupgold.com/wugplugins).
- **Licensing Information**. Licensing and support information is available on the *MyIpswitch licensing portal* (http://www.myipswitch.com/). The web portal provides enhanced web-based capabilities to view and manage Ipswitch product licenses.
- **Knowledge Base**. Search the Ipswitch Knowledge Base of technical support and customer service information. The knowledge base is available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/wugTechSupport).
- **User Forum**. Use the online user group forums to interact with other WhatsUp Gold users to share helpful information about the application. The User Forums are available on the *WhatsUp Gold web site* (http://forums.ipswitch.com/).

Copyright notice

This document was published on Tuesday, September 30, 2008 at 13:18.