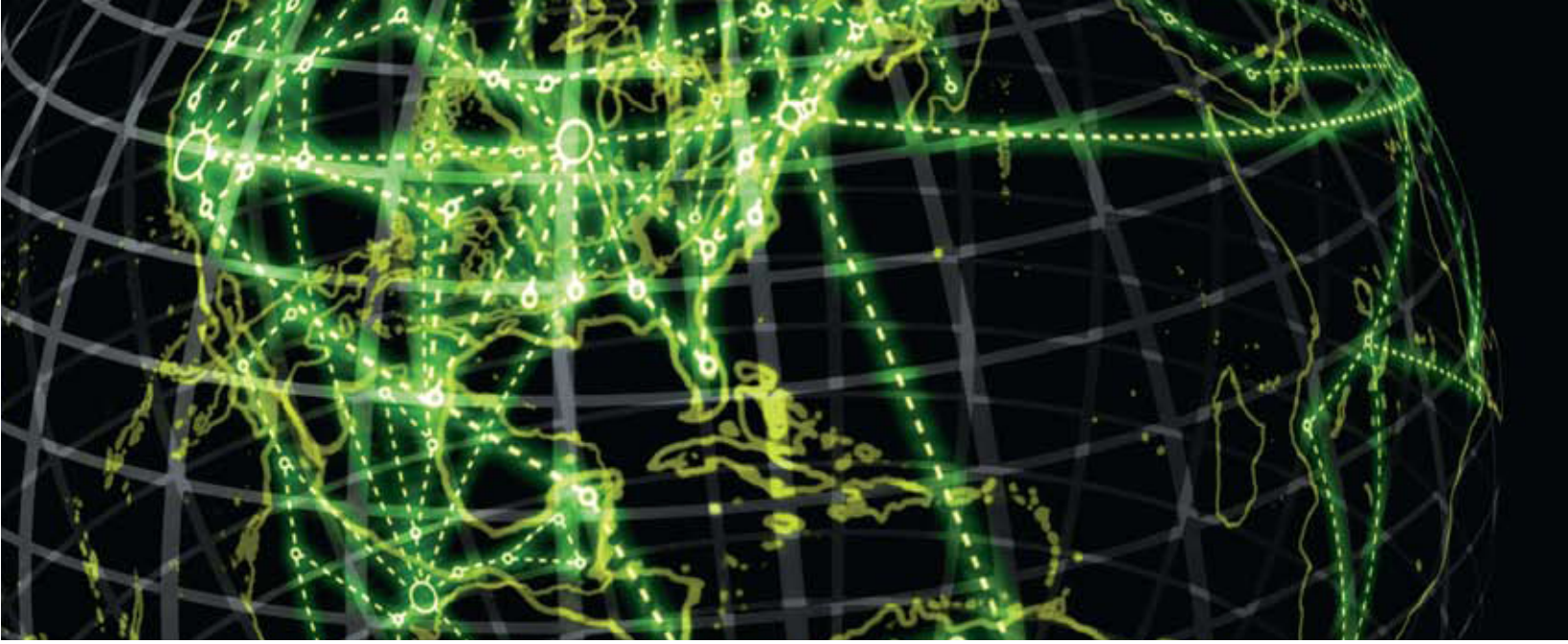


IPSWITCH

Flow Publisher v1.0 Deployment Guide

Learn how to deploy the WhatsUp Flow Publisher.

IPSWITCH WhatsUpGold

CHAPTER 1 Flow Publisher Overview

What is the Flow Publisher? 1
How does the Flow Publisher work? 2
NetFlow Overview 3
Defining a flow 3
NetFlow records 3
NetFlow architecture 4

CHAPTER 2 Deploying the Flow Publisher

Determining which network traffic to monitor 6
Copying network traffic to the Flow Publisher capture interface 7
Capturing NetFlow data from local traffic 8
Mirroring traffic on a network device 9
Copying network traffic using a network tap 12
Installing the Flow Publisher 13
Starting the Flow Console 15
Adding the Flow Publisher to the Flow Console 15
Configuring the Flow Publisher capture interface 15
Using the capture device configuration wizard 16
Configuring the capture device when receiving local traffic 18
Configuring the capture device when receiving bidirectional traffic 18
Configuring the capture device when receiving unidirectional traffic 20
Adding a Flow Collector to a Flow Publisher configuration 22

CHAPTER 1

Flow Publisher Overview

In This Chapter

What is the Flow Publisher? 1
How does the Flow Publisher work? 2
NetFlow Overview 3

What is the Flow Publisher?

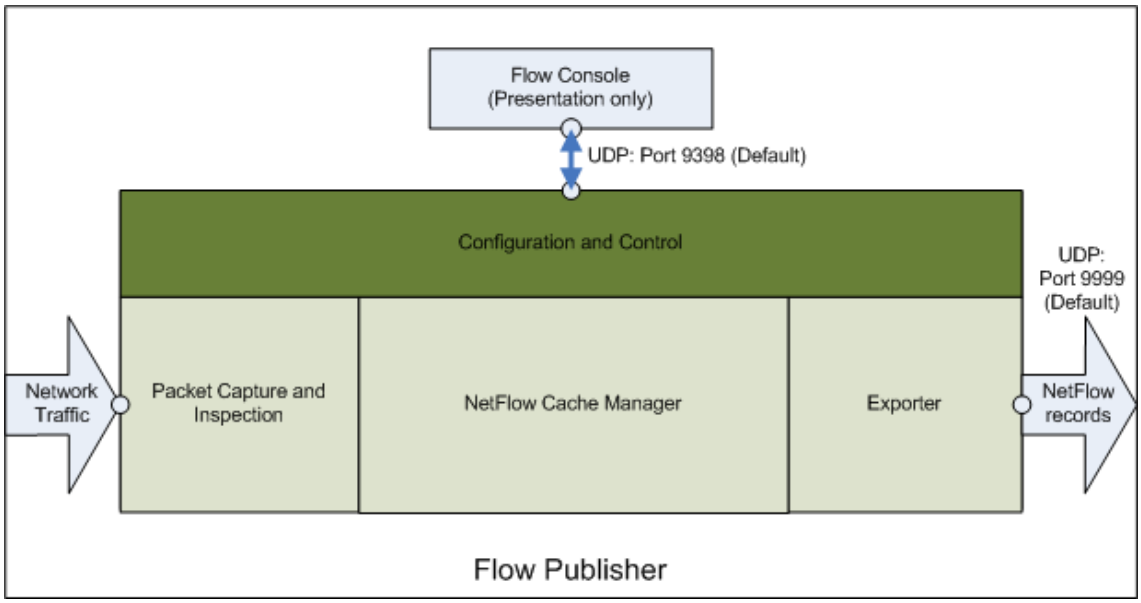
The WhatsUp Flow Publisher is a lightweight, passive, software agent that can be deployed to collect flow data from routers, switches, servers and other points of interest in the network. The Flow Publisher provides flow data and associated statistics for devices that do not support the NetFlow protocol, or where using a NetFlow enabled device to acquire the data is cost prohibitive.

The network traffic to be captured by the Flow Publisher must be copied to an interface on the server hosting the Flow Publisher. The traffic can be mirrored, using a router's SPAN port or a similar mirroring technique, or the traffic can be copied to the Flow Publisher using a network TAP. The traffic can be copied from a network device, application server or other point of interest within the network. Since the Flow Publisher receives a copy of the network traffic, it does not impact the normal flow of traffic in the network.

For example, you can mirror the traffic from a firewall, prior to network address translation, so that all of the traffic crossing the firewall is captured and sent to the Flow Publisher. Should you have a particular subnet in your network that you would like to monitor for abnormal activity, you can place a network TAP on the segment between the gateway router and the subnet and copy that traffic to the publisher. By narrowing the focus of the network traffic being copied to the publisher, you can obtain a more granular view into network usage, efficiency, network anomalies and security vulnerabilities.

How does the Flow Publisher work?

The Flow Publisher captures packets from network traffic using WinPcap, a packet capture utility. Once captured, the packet header is read and statistics are gathered about the packet. If the packet contains information about a flow that is not active, the gathered statistics are used to create an active flow. Each active flow is placed in the NetFlow Cache and is managed by the NetFlow Cache Manager until the flow expires. After the flow has expired, the flow record is sent to the Exporter for transmission to the NetFlow collector.



Packet capture and inspection

The Flow Publisher uses WinPcap to conduct packet capture and inspection. The WinPcap utility provides the Flow Publisher with the ability to capture raw packets and gather statistical information from these packets. The capture interface, the interface where the Flow Publisher captures the network traffic, can be placed in either Normal mode, where only the traffic associated with the interface will be available for capture, or Promiscuous mode, where all of the traffic in the network segment will be available for capture. The statistical information gathered during this process is then used to create flow records which are placed in the NetFlow cache.

Cache management

The NetFlow cache stores active flow records. A flow record is active once it has been created, and remains active until it has expired. While it is active, the flow record is updated with new statistical data as new packets associated with the specific flow are captured and inspected. A flow expires under the following circumstances; when the TCP connections have reached the end of the byte stream (FIN) or when they have been reset (RST); when the flow has been idle for a specified amount of time; or the flow has been active but is long lived (flows lasting more than 30 minutes). The timeout for active and long lived flows are configurable.

NetFlow record export

Once a NetFlow record has expired, it is placed in a NetFlow datagram for export to the Netflow collector. The Flow Publisher can export the record to several collectors using any of the formats in the supported NetFlow versions. The currently supported versions are NetFlow v1, v5, and v9.

NetFlow Overview

The NetFlow protocol is a proprietary network protocol developed by Cisco Systems and used by the Flow Publisher to capture and transmit statistical data about IP traffic. Within the NetFlow protocol, the flow concept is used to provide context for the statistical data generated about the network traffic.

Defining a flow

NetFlow uses the concept of a flow to capture data about network behavior, such as the source and destination of network traffic, the applications using the network, and the amount of bandwidth being allocated to these applications.

A **flow** is a unidirectional sequence of packets between a given source and destination, defined by a 7-tuple key consisting of the following fields:

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- IP Protocol
- Ingress interface
- IP Type of Service

As statistical information is gathered from the network traffic, the information is placed in a flow record in the NetFlow Cache. A new flow is created when a key field has unique information.

NetFlow records

The NetFlow information gathered by the Flow Publisher is managed by creating records for each flow. Each record is managed in the NetFlow cache. As packets are captured, the statistics pertaining to the active flows are updated. Once a flow has been created and placed in the NetFlow cache, it remains active until it expires. After the flow expires, the flow record is added to a NetFlow Export datagram for transmission to the NetFlow collector.

A **NetFlow record** may include many or all of the following statistics based on the NetFlow version:

- Netflow version
- Flow Sequence (Identifier)
- Input and output SNMP indices
- Flow size in packets and bytes
- Timestamp for flow start and stop times
- Layer 3 header data (Source/Destination IP Addresses, IP protocol)
- Port Numbers
- Type of Service (ToS).
- Layer 3 Routing information (IP address of the next-hop, Source and destination IP masks)
- Multiprotocol Label Switching (MPLS) labels (Netflow version 9 only)
- IPv6 addresses and ports (Netflow version 9 only)

NetFlow architecture

NetFlow as a protocol provides a means of collecting flow data from a network device and forwarding that data to a collector. This flow data must be captured from the network traffic, converted to a standard NetFlow record format, exported to a collector for aggregation, and then analyzed by the proper application to provide information useful in the analysis, planning and management of the network.

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

- **NetFlow exporter** – observes packet data and creates records from the monitored network traffic and transmits that data to the NetFlow collector.
- **NetFlow collector** – collects the records sent from the exporter, stores them in a local database and forwards the records to an analyzer.

- **NetFlow analyzer** – analyzes the NetFlow records for information of interest, which may include bandwidth usage, policy adherence, and forensic research.

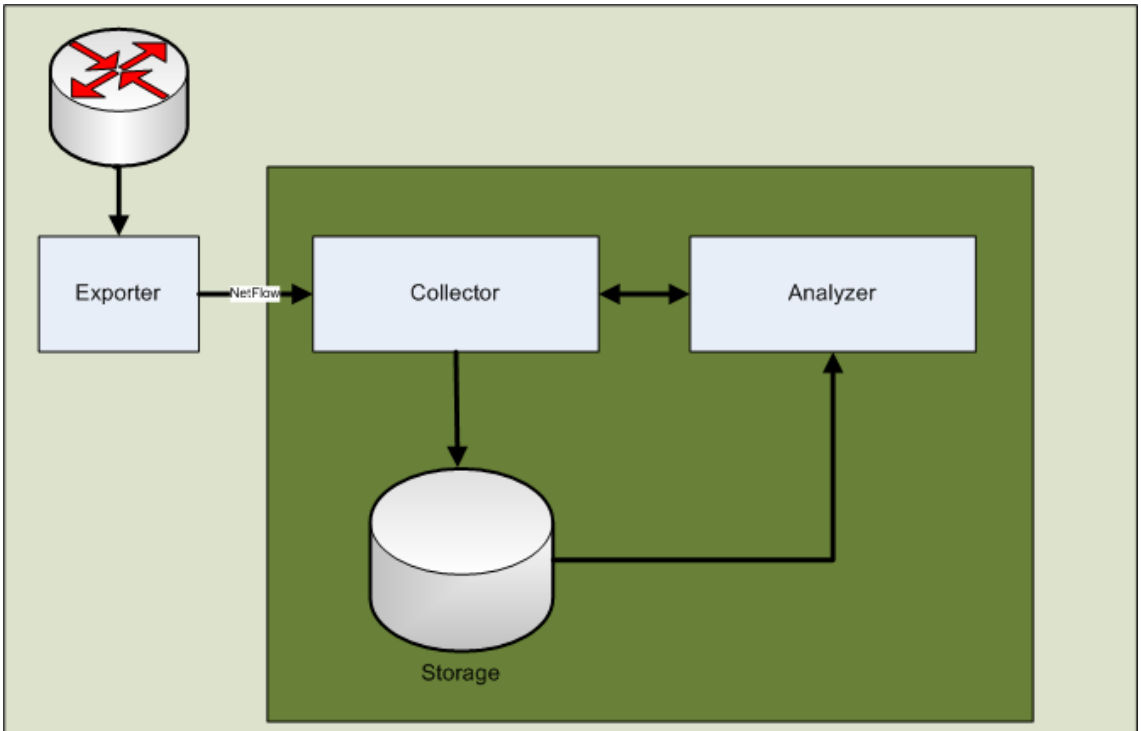


Figure 1: NetFlow Implementation Architecture

The exporter can be either an included function of the network device, such as the NetFlow export functionality on Cisco routers, or it can be an external publisher configured to monitor one or more interfaces on the device, such as the WhatsUp Flow Publisher.

The collector and analyzer can be a single product, or may be implemented by two or more products. An example of a collector and analyzer is the WhatsUp Flow Monitor coupled with Ipswitch WhatsUp Gold to provide real-time monitoring, alerting, and forensic analysis to flow data captured by the WhatsUp Flow Publisher.

CHAPTER 2

Deploying the Flow Publisher

In This Chapter

Determining which network traffic to monitor 6
Copying network traffic to the Flow Publisher capture interface 7
Installing the Flow Publisher 13
Starting the Flow Console 14
Adding the Flow Publisher to the Flow Console 15
Configuring the Flow Publisher capture interface 15
Adding a Flow Collector to a Flow Publisher configuration 21

You must make the following decisions to ensure that the network traffic is delivered to the capture interface:

- Determine the network traffic on which you want to collect NetFlow statistics.
- Choose the method to use to copy and forward the traffic to the Flow Publisher capture interface.

After these decisions are made and the network traffic has been copied to the capture interface, the Flow Publisher can be configured using the Flow Console.

Determining which network traffic to monitor

Determining the network traffic on which to collect NetFlow statistics requires an understanding of where these statistics will provide the most benefit in providing answers to the particular problems you are facing in your network. This determination presupposes a detailed understanding of your network and of how NetFlow statistics can be used to provide information relevant to your particular challenges.

NetFlow statistics provide insight into who is using the network, how often they are using it, how they are connecting, and how the available resources are being used. With this in mind, domains or network segments that are experiencing high traffic volumes, or individual servers that are exhibiting unexplained behavior may be good candidates for statistics gathering. Problems with high traffic volume may be an indication of abuse or may be an indication of a need for network buildout to adequately support valid operations. By gathering and analyzing NetFlow statistics you can get a more accurate picture of the network situation.

Other network segments that are candidates for statistics gathering are those segments in which comprehensive visibility is necessary to provide a complete view of the network usage. In order to adequately manage and protect the network, indepth knowledge of normal usage patterns as well as indications of abnormal behavior are necessary to quickly respond to operational and security related incidents. NetFlow statistics can provide detailed insight into incidents in near real-time and during forensic research following an incident.

Copying network traffic to the Flow Publisher capture interface

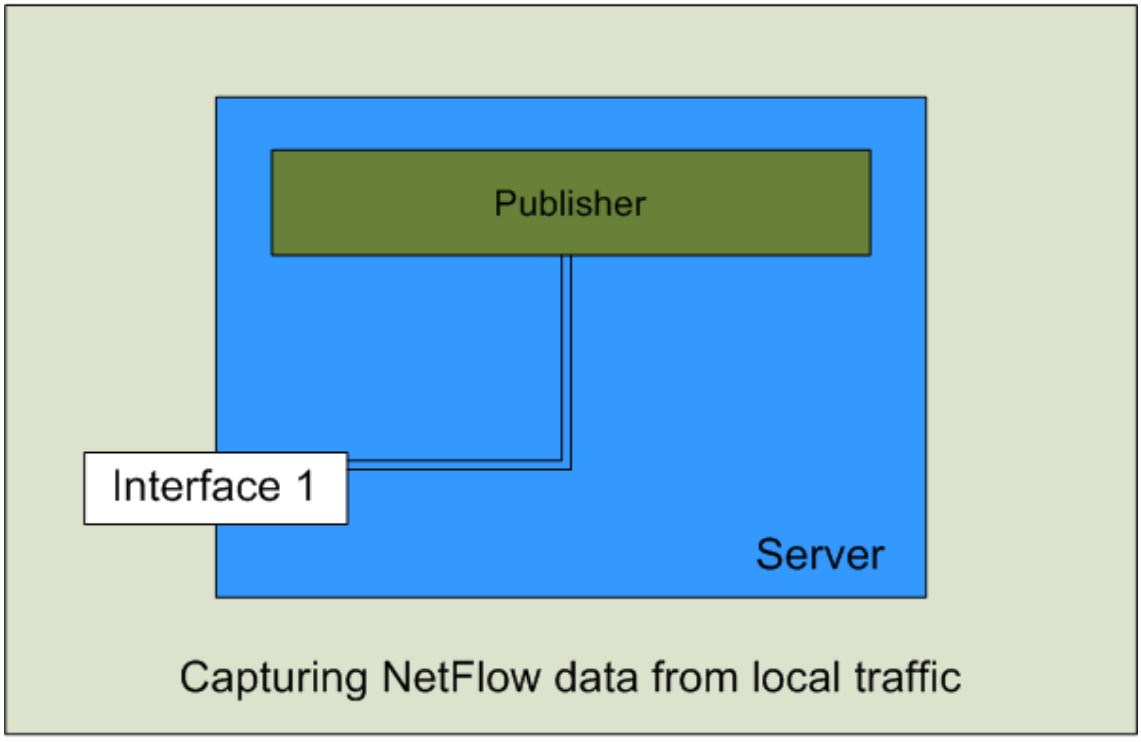
After you have determined the network traffic for which you want to capture and generate NetFlow statistics, you must determine how to copy the traffic to the Flow Publisher capture interface.

The options for copying network traffic are to:

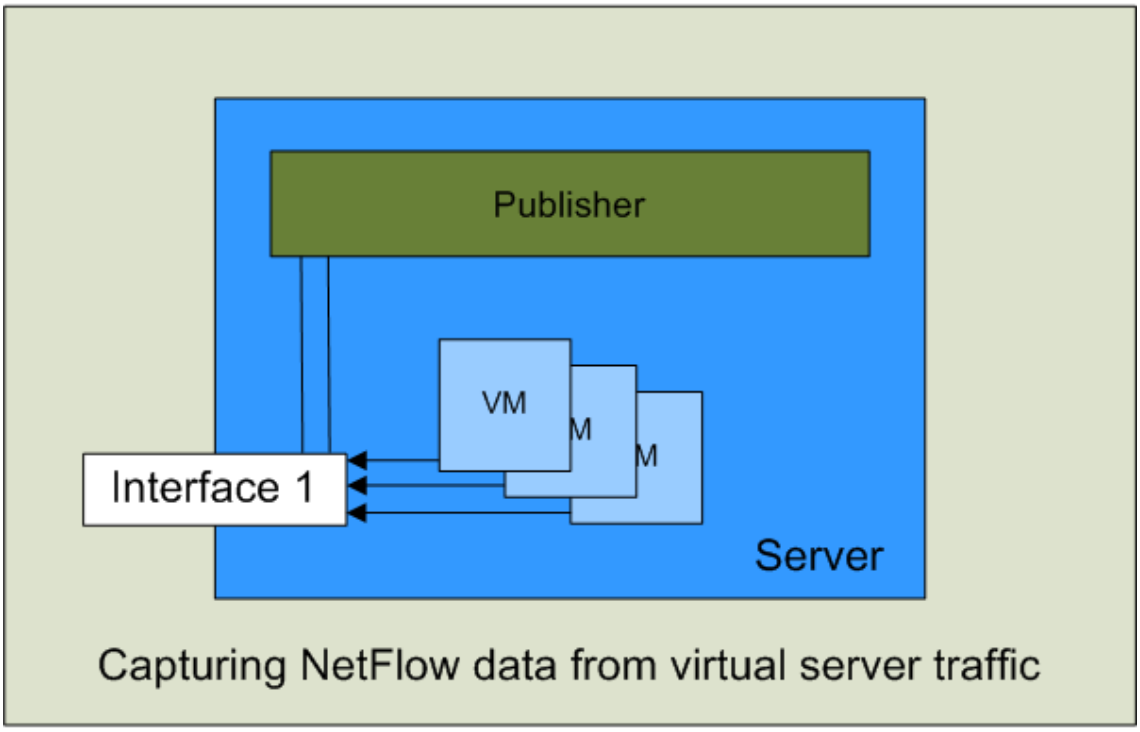
- Capture traffic from a server's local interface.
- Mirror traffic from a network device such as a switch to a Flow Publisher capture interface.
- Use a network TAP to copy the desired network traffic to a Flow Publisher capture interface.

Capturing NetFlow data from local traffic

You can use the Flow Publisher to capture NetFlow data from a local interface by installing the publisher on the server from which you want to collect NetFlow data, configuring the local interface as the capture device and setting the capture mode to Normal. The Flow Publisher will automatically map the local network interface card MAC address as the reference interface.



When you capture traffic on a Virtual Machine (VM), you must consider the capture mode setting based on the traffic from which you want to collect NetFlow data. If you select Normal mode, only the traffic that is addressed to or from the physical machine will be captured. If you select Promiscuous mode, all of the traffic addressed to or from the virtual machines will be captured as well, allowing you to collect NetFlow statistics on the individual virtual machines as well as the physical server.



You can also collect NetFlow statistics on a virtual server by installing NetFlow on the virtual server and configuring the capture mode of the virtual interface to Normal. This configuration will provide NetFlow statistics on all of the traffic to or from the virtual server.

Mirroring traffic on a network device

To Mirror traffic on a switch:

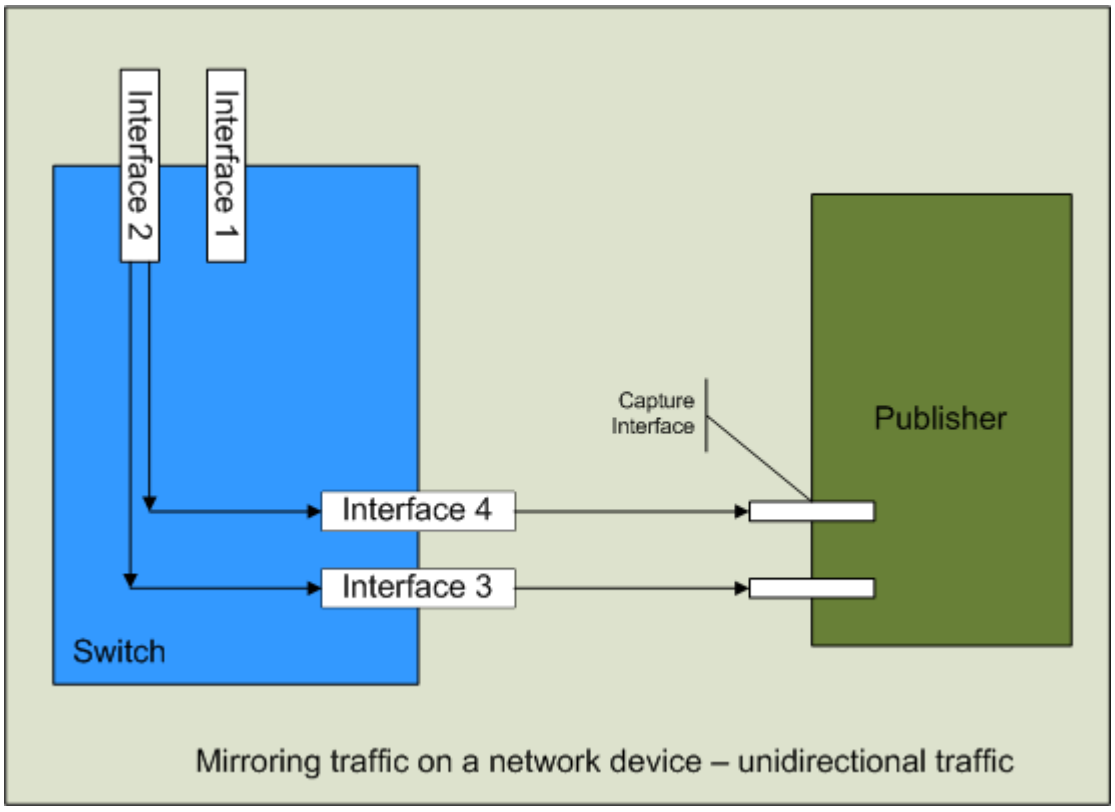
- Enter the configuration mode on the switch
- Create a traffic source
- Route the traffic source to an interface configured to transmit only
- Physically connect the interface to a Flow Publisher capture interface

Creating a traffic source

When you create a traffic source, you may elect to include traffic from a single interface, from an entire Local Area Network (LAN), or Virtual Local Area Network (VLAN). You also have the option to send transmitted (outbound) traffic, send received (inbound) traffic, or send transmitted and received traffic for each interface included in the traffic source.

Unidirectional mirroring

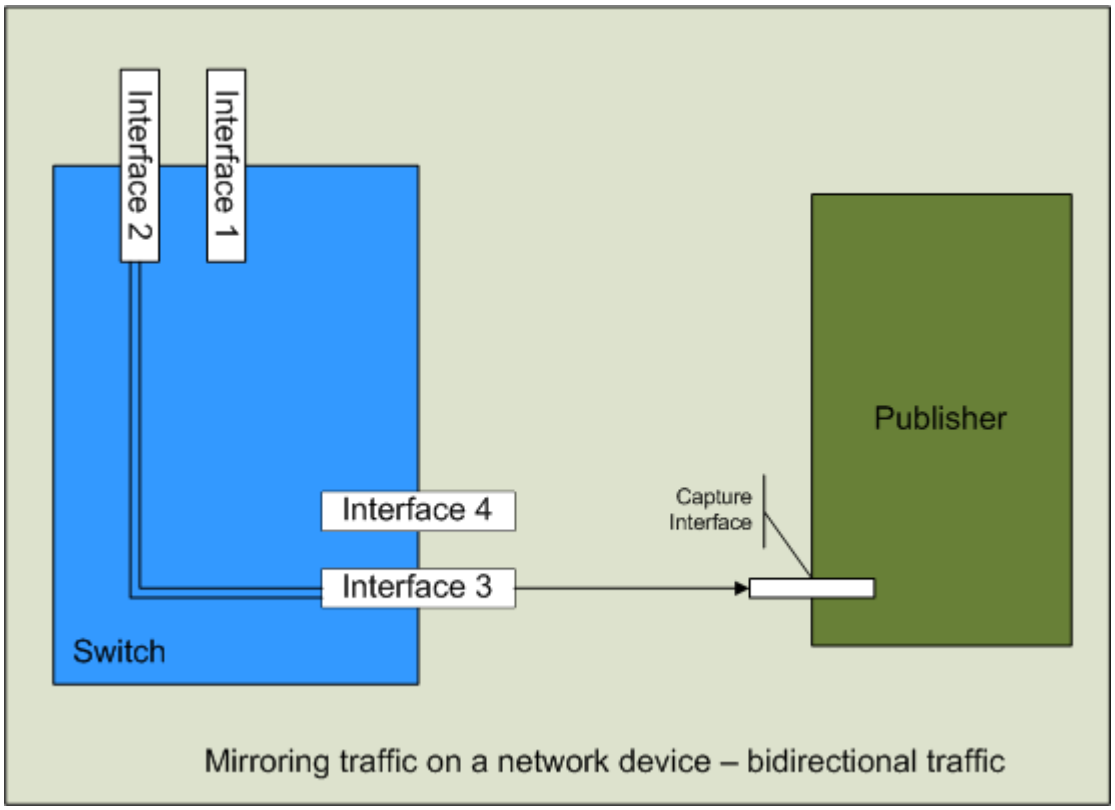
To mirror traffic in a unidirectional manner, all of the received or inbound traffic is mirrored to one interface, and the transmitted or outbound traffic is mirrored to a second interface, effectively providing separate channels for inbound and outbound traffic. The inbound and outbound signals are connected directly, or through a VLAN, to separate capture interfaces on the server hosting the Flow Publisher.



In the diagram above, two traffic sources have been created. One traffic source includes all of traffic received by Interface 2 (inbound traffic) , and the other traffic source contains all of the traffic transmitted from Interface 2 (outbound traffic). The inbound traffic is mirrored to Interface 3 which is physically connected to a capture interface on the Flow Publisher, and the outbound traffic is mirrored to Interface 4 which is connected to a different capture interface on the Flow Publisher. This configuration will ensure that there are no traffic bottlenecks created during peak traffic periods, as can be the case when mirroring bidirectional traffic.

Bidirectional mirroring

If you do not have the network interfaces available to accommodate the unidirectional configuration, or there is a bottleneck in the external link, you may choose to mirror all of the traffic (both inbound and outbound) in a traffic source to a single interface on the switch and connect that interface to a single capture interface on the Flow Publisher.



In the above figure, a single bidirectional traffic source has been created and mirrored to Interface 3. This traffic source contains all of the traffic received by and transmitted from Interface 2 combined. This combined bidirectional traffic is then sent to a single capture interface on the Flow Publisher.

Note: If Interface 2 and Interface 3 have the same bandwidth capacity and Interface 2 simultaneously exceeds 50% of its capacity in both inbound traffic and outbound traffic, Interface 3 may saturate and drop traffic that is in excess of its capacity.

If you choose to mirror bidirectional traffic (both inbound and outbound) to a single interface and forward that to a single capture interface on the Flow Publisher, additional MAC address interface mapping will need to be accomplished when configuring the Flow Publisher in order to determine the direction of the packets in the flow relative to the network or subnet from which the network traffic is being copied.

Example

This example shows how to mirror bidirectional traffic from an interface on a switch to the interface that sends traffic to the Flow Publisher. The router used in this example is a Cisco Cataylst 3560 switch. The traffic from the interface connected to the firewall, labeled gi0/1, will be mirrored to the interface connected to the Flow Publisher, labled gi0/6.

To mirror traffic on the Cisco Catalyst 3560 switch:

1. Connect to the Cisco Catalyst 3560 switch using telnet or other connection protocol.
2. Log in to the Cisco IOS as the device administrator.
3. Enter the configuration mode on the switch.

   ```
   config t
   ```

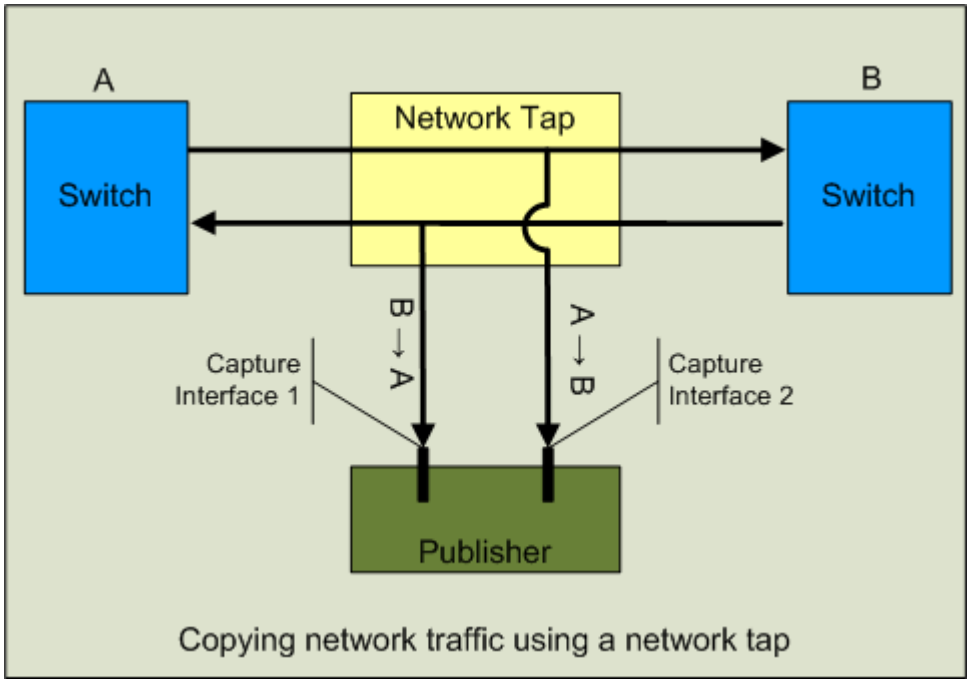
4. Create a monitoring session (1 – 66). The traffic source can be a single interface or vlan and the traffic direction can be tx = transmit, rx = receive, or both.

   ```
   Monitor session 1 source interface gi0/1 both
   ```

5. Send mirrorred traffic to the interface that will send traffic to the Flow Publisher.(gigabit interface gi2/30).

   ```
   Monitor session 1 destination interface gi0/6
   ```

Copying network traffic using a network tap



When you use a network tap to copy traffic to the Flow Publisher, you need to install a network tap in the segment that carries the traffic you want to capture. Next, connect the outputs from the tap directly to the capture interfaces on the Flow Publisher. The network tap will copy the full-duplex traffic and send traffic from each direction on a separate connection to two seperate capture interfaces on the Flow Publisher.

The diagram above provides a representation of how a network tap installed in a network segment connected to a switch delivers the copied network traffic to the Flow Publisher. Output A is a unidirectional signal containing all of the outbound traffic from the switch and Output B is a unidirectional signal containing all of the inbound traffic to the switch. Each of these outputs is connected directly to a separate capture interface on the Flow Publisher.

Installing the Flow Publisher

Prerequisites and recommendations

The following prerequisites and recommendations are provided to esure a smooth installation of Flow Publisher:

- Download *WinPcap version 3.1 or later* http://www.winpcap.org/ and install it on the server hosting Flow Publisher.
- It is recommended that a static IP address be used for the Flow Publisher server interface used to establish communications between the Flow Publisher and the Flow Console as well as Flow Monitor. This will prevent failures in communications between these components and ensure that multiple Flow Monitor source license slots are not assigned to a single Flow Publisher following a restart where a new IP address is assigned by DHCP.
- To ensure proper license mangement, you must install an instance of the Flow Console on the server hosting Flow Monitor and WhatsUp Gold. This instance must be used to configure Flow Monitor as a collector on any of the installed Flow Publisher instances. Other instances of Flow Console can be used to view the Flow Publisher configuration including the Flow Monitor instance configuration.

To install Flow Publisher:

1. Log in directly to Microsoft Windows using the Administrator account (if you do not have an account called Administrator, use an account that has full administrative privileges to the computer).
2. Start the installation program:
   - If you downloaded an electronic version of Flow Publisher, double-click on the downloaded file.
   - If you purchased a Flow Publisher CD-ROM, insert the CD-ROM into the appropriate drive. If it does not run automatically, click **Start**, select **Run**, then enter the CD path followed by `AutoRun.exe (f`or example, `D:\AutoRun.exe`).
3. Read the Welcome screen.

   Click **Next**. The License Agreement dialog appears.
4. Read the license agreement. If you accept the terms of the license agreement, select **I accept the terms of the license agreement**, then click **Next**. The Setup Type dialog appears.
   - To print a copy of the license agreement, click **Print**. The license agreement is sent to the default printer.
   - If you do not accept the terms of the license agreement, click **Cancel** to exit the installation program.

5 Select the type of setup, then click **Next**. The Choose Destination Location dialog appears.

Note: The Complete option installs both WhatsUp Flow Publisher and Console and uses a Flow Publisher license instance. The Custom option allows you to select which program features you want to install. The available feature options are Flow Publisher, Flow Console, or both. If you install the Flow Console only, you will not use a Flow Publisher license instance.

Note: To ensure proper license mangement, you must install an instance of the Flow Console on the server hosting Flow Monitor and WhatsUp Gold. This instance must be used to configure Flow Monitor as a collector.

6 Select the installation directory for the Flow Publisher application files, then click **Next**. If you selected the Complete setup type, the Port Selection dialog appears. If you selected the Custom setup type, the Select Features dialog appears.

Note: The default path is `C:\Program Files\Ipswitch\WhatsUp Flow Publisher`.

Tip: You can install Flow Publisher to a different location. To select a different location, click **Change**.

7 If you selected the Custom setup type, select the options you want to install from the Select Features dialog. The Port Selection dialog appears.

8 In the Port Number field, type the port number where the Flow Publisher will receive configuration data from the Flow Console and click **Next**. The Ready to Install the Program dialog appears.

Note: The default port number is 9398 and should only be changed if there is a conflict with another application or service.

9 Click **Install** to install Flow Publisher. The setup program installs Flow Publisher. When the installation completes, the InstallShield Wizard Complete dialog appears.

10 Select one of the following options.

- Yes, I want to restart my computer now.
- No, I will restart my computer later.

11 Click **Finish**. The setup program closes.

To start the Flow Console:

Click **All Programs** > **Ipswitch WhatsUp Flow Publisher** > **Flow Console**.

Starting the Flow Console

To start the Flow Console from the Start Menu:

Start > All Programs > Ipswitch WhatsUp Flow Publisher > Flow Console

To start and stop the Flow Publisher from a Command Line Interface:

You may need to start and stop a publisher that is not connected to the Flow Console. You can connect to the server hosting the Flow Publisher using ssh or some other remote connection utility and run the command to start or stop the Flow Publisher using the following commands:

- `netflowd -start`
- `netflowd -stop`

Adding the Flow Publisher to the Flow Console

Before you can configure the capture interface, you must add the Flow Publisher to the Flow Console. You can add a Flow Publisher from the Flow Publishers section of the Flow Console.

To add a Flow Publisher:

1. On the Flow Publishers section, click **Add**. The Add Flow Publisher dialog appears.
2. In the **IP** box, enter the IP address of the server hosting the Flow Publisher.
3. In the **Port** box, enter the port number where the Flow Console will connect to the Flow Publisher.
4. Click **OK** to add the Flow Publisher. The Flow Publisher appears in the Flow Publishers list of the Flow Console.

Configuring the Flow Publisher capture interface

To configure the Flow Publisher capture interface use the Capture Devices tab of the Flow Console. There are several configuration options that are available for identifying traffic direction based on the type of traffic received by the capture interface.

To configure the capture mode on the capture interface:

- In the **Capture Mode** list, select the capture mode for the capture interface.

Note: If you are collecting traffic from the local server, the capture mode for the local interface should be placed in Normal, so you will see only the traffic received by and sent from the local interface.

Note: The default capture mode is promiscuous. This mode allows the capture of all packets entering the interface, regardless of whether the traffic is addressed to the interface.

Using the capture device configuration wizard

The Capture Device Configuration Wizard provides a quick and easy way to configure the capture device. The wizard will step you through the decisions that need to be made about how you would like to capture and report on the network traffic captured by Flow Publisher.

Capturing local traffic using the wizard

To configure the capture device using the wizard when capturing local traffic:

1. On the **Capture Devices** tab, click **Wizard**. The Flow Capture Device Wizard appears.
2. If you want to capture flows with this device, select **Yes, capture flows with this device**, otherwise click **No, do not capture flows with this device**.

Note: If you select **No, do not capture flows with this device**, the Capture Mode setting on this device is placed in **Not Capturing** mode.

3. In the **Capture all traffic visible at this device?** section, select **No. Capture the device's traffic only**, then click **Next**. The summary information dialog appears.

Note: If you select **No, Capture the device's traffic only**, the Capture Mode setting on this device is placed in **Normal** mode.

Note: The summary includes information about how you have elected to capture traffic on the capture device and how the source of the data will be reported to Flow Monitor.

4. Click **Finish**. The wizard applies the capture device settings to the Flow Publisher and closes.

Capturing traffic copied from an external source using the wizard

When you are mirroring traffic from a network switch, or tapping a network segment and sending a copy of that traffic to Flow Publisher, you can use the wizard to configure the capture device to capture and report on this traffic.

To configure the capture device using the wizard when receiving traffic copied from an external source:

1. On the Capture Devices tab, click **Wizard**. The Flow Capture Device Wizard appears.
2. If you want to capture flows with this device, select **Yes, capture flows with this device**, otherwise click **No, do not capture flows with this device**.

Note: If you select **No, do not capture flows with this device**, the Capture Mode setting on this device will be placed in **Not Capturing**.

3. In the **Capture all traffic visible at this device?** section, select **No. Capture all traffic visible at this device**, then click **Next**. The automatic interface mapping selection dialog will appear.

Note: If you select No, capture all traffic visible at this device, the Capture Mode setting on this device is placed in Promiscious mode.

4. If you want to enable automatic reference mapping, select **Yes, use automatic interface mapping** in the automatic interface mapping selection dialog, then click **Next**. The summary information dialog appears.
5. If you want to perform reference mapping manually, perform the following steps:
   a) Select **No. Manually assign the interface mapping**, then click **Next**. The Interface Map selection dialog appears.
   b) On the Interface Map selection dialog, select the MAC addresses of the interfaces you want to use as a reference interface, then click **Next**. The summary information dialog appears.

Note: If you choose to leave the MAC address and the associated interface field blank, the Flow Publisher will report all of the captured traffic as incoming to the capture device using the psuedo-interface number as the source identifier.

6. Click **Finish**. The wizard applies the capture device settings to the Flow Publisher and closes.

Configuring the capture device when receiving local traffic

When the Flow Publisher is installed on a server with the purpose of collecting traffic from that server, the local device is both the capture device and the reference device. The Flow Publisher is configured automatically, but the configuration may need to be adjusted in some cases. The following procedure discusses how to manually configure the publisher.

To manually configure the capture device when receiving local traffic:

1. On the **Flow Publishers** list, select the Flow Publisher for which you want to configure the capture device.
2. Select the **Capture Devices** tab. The capture device list appears.
3. On the capture device list, select the device you want to configure.
4. Click **Configure**. The Configure Capture Device dialog appears.
5. If you wish to manually configure the capture device, ensure that **Use automatic interface mapping** is not checked.
6. In the **Interface map** field, enter or select the MAC address and device ID defining the device you want to use as the reference device.
7. Click **OK**. The Configure Capture Device dialog closes.

To configure the capture mode on the capture device:

- In the Capture Mode list, select the capture mode for the capture device.

Note: If you are collecting traffic from the local server, place the capture mode for the local device in Normal, so you see only the traffic received by and sent from the local server.

Note: The default capture mode is promiscuous. This mode allows the capture of all packets entering the device, regardless of whether the traffic is addressed to the device.

Configuring the capture device when receiving bidirectional traffic

When the capture device receives bidirectional traffic, meaning that it contains both inbound and outbound traffic, you must define a reference device. The reference device establishes a point of view, or plane which is used as a point of reference to determine traffic direction. Traffic that identifies the reference device as the destination will be classified as inbound traffic and traffic that identifies the reference device as the source will be classified as outbound traffic.

When **Use automatic interface mapping** is checked, the system inspects the traffic to determine if there is an device through which a majority of the captured traffic passes. If it can detect such an device, the device is placed in the **interface map**, and is used as the reference device.

When **Use automatic interface mapping** is not checked, you must manually define a reference device by adding the device to the **Interface map** box on the Configure Capture Device dialog. The system provides a list of the device MAC addresses for those devices with the highest percentage of appearances as either the source or destination in the traffic copied to the capture device.

To manually configure a capture device when receiving bidirectional traffic:

1. On the **Flow Publishers** list, click the Flow Publisher for which you want to configure the capture device.
2. Select the **Capture Devices** tab. The capture device list appears.
3. On the capture device list, select the device you want to configure.
4. Click **Configure**. The Configure Capture Device dialog appears.
5. If you wish to manually configure the capture device, ensure that **Use automatic interface mapping** is not checked.
6. In the **Interface map** field, enter or select the MAC address and device ID defining the interface you want to use as the reference device.
7. Click **OK**. The Configure Capture Device dialog closes.

To configure the capture mode on the capture device:

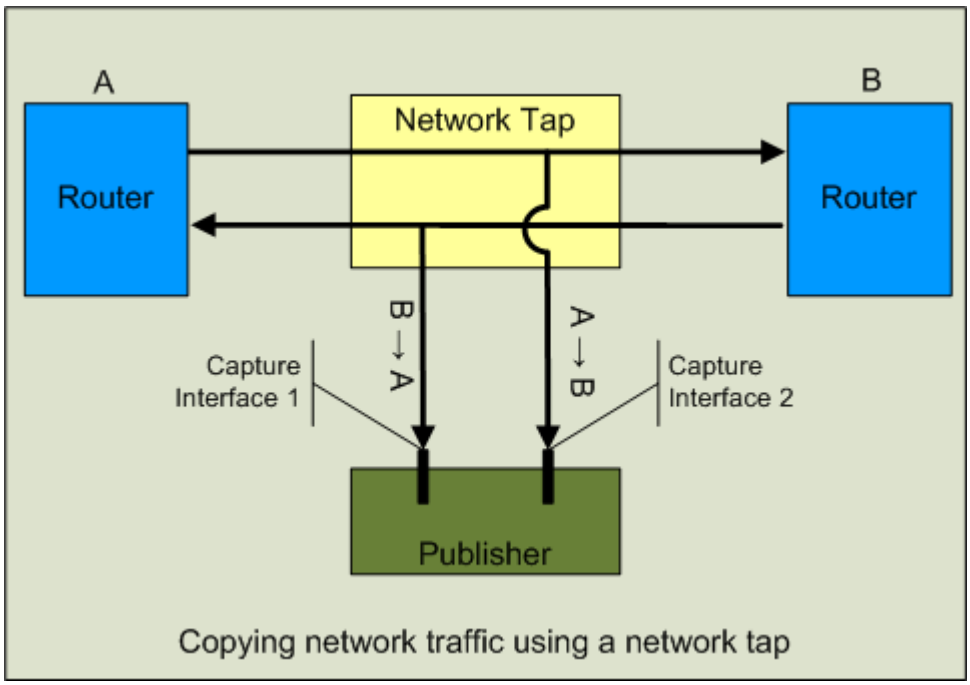
- In the Capture Mode list, select the capture mode for the capture device.

Note: If you are collecting traffic from the local server, place the capture mode for the local device in Normal, so you see only the traffic received by and sent from the local server.

Note: The default capture mode is promiscuous. This mode allows the capture of all packets entering the device, regardless of whether the traffic is addressed to the device.

Configuring the capture device when receiving unidirectional traffic

When each direction of a full-duplex traffic source is delivered to a separate capture device, with traffic in one direction being copied to one capture device and traffic in the other direction being copied to a separate capture device, you must configure interface identifiers for the two capture devices. This will ensure that the traffic received on one capture device is seen as being opposite in direction when compared to the traffic received on the other capture device.



To configure each capture device correctly, you must identify an inbound and outbound interface. An interface identifier can be the pseudo-interface, the SNMP index, or an identifier you create and assign to the interface. The default setting is for the pseudo-interface value to be used as both **In Interface** and **Out Interface**.

When a pair of interfaces carry unidirectional traffic from the same traffic source, we recommend that the same interface identifiers be used to configure both capture devices. This ensures that the Flow Publisher can determine the direction of the traffic being received from each of the capture devices relative to the other. When configuring the pair of interfaces, the interface identifier for the **In interface** on one capture device should be the interface identifier for the **Out interface** on the second capture device and vice versa.

To configure the capture device when receiving unidirectional traffic:

1. On the **Flow Publishers** list, click on the Flow Publisher for which you want to configure the capture device.
2. Select the **Capture Device** tab. The capture device list appears.
3. Select the interface you wish to configure and click **Configure**. The Configure Capture Device dialog appears.

4 Assign an interface identifier to the **In interface** using one of the following methods.

a) If you want to use the Pseudo interface value, ensure that the value in the Pseudo interface field is present in the **In interface** field.

b) If you want to use the SNMP index of the capture device, click **Use snmp index** for the **In interface** field.

c) If you want to assign a value, enter a unique value into the **In interface** field.

5 Assign an interface identifier to the **Out interface** using one of the following methods.

a) If you want to use the Pseudo interface value, ensure that the value in the **Pseudo interface** field is present in the **Out interface** field.

b) If you want to use the SNMP index of the capture device, click **Use snmp index** for the **Out interface** field.

c) If you want to assign a value, enter a unique value into the **Out interface** field.

6 When you have defined the values for the interface identifiers, click **OK**. The Configure Capture Device dialog closes.

To configure the capture mode on the capture device:

- In the Capture Mode field, select the capture mode you want the capture device to operate from the **Capture Mode** pull-down menu.

Note: If you are collecting traffic from the local server, the capture mode for the local interface should be placed in Normal, so you will see only the traffic received by and sent from the local server.

Note: The default capture mode is promiscuous. This mode allows the capture of all packets entering the interface, regardless of whether the traffic is addressed to the interface.

Adding a Flow Collector to a Flow Publisher configuration

You can add a collector from the **Flow Collectors** tab of the Flow Console. When you add a collector, it is associated with the selected Flow Publisher in the Flow Publisher list. The IP address and port number describe where the publisher will send the NetFlow data. You must configure Flow Monitor to receive the NetFlow data on this interface and port, since the publisher will send the information regardless of whether the collector is configured to receive the information.

To add a Flow Collector:

1. On the Flow Publishers list, select the publisher to which you want to add the Flow Collector.
2. Select the **Flow Collectors** tab. The Flow Collectors list appears.
3. On the **Flow Collectors** tab, click **Add**. The Add Collector dialog appears.
4. In the **IP** box, enter the IP address of the server hosting the collector.
5. In the **Port** box, enter the port number you want the Flow Publisher uses when communicating to the collector.

Note: the default port number for communications between the publisher and Flow Monitor is port number 9999.

6. In the **Display Name** box, enter the name you want to assign to the collector. This name is displayed in the **Name** field of the Flow Collectors list.
7. In the **Version** list, select the NetFlow version to use in formatting the NetFlow data to be sent to the collector.
8. If the server hosting the Flow Publisher has more than one interface available, and you want to define an interface other than the primary interface to communicate with the collector, perform the following:
   a) In the **NetFlow source** box, enter the IP address of the server hosting the Flow Publisher uses when communicating to the collector.
   b) In the **NetFlow source port** box, enter the port number for the Flow Publisher uses when communicating with the collector.
9. Click **OK** to add the collector. The collector appears in the Flow Collectors list in the Flow Console.

Copyright notice

This document was published on Monday, November 09, 2009 at 18:13.