AdventNet ManageEngine NetFlow Analyzer

User Guide

www.netflowanalyzer.com
netflow-support@adventnet.com

Table Of Contents

Introduction

ManageEngine™™ NetFlow Analyzer is a web-based bandwidth monitoring tool that performs in-depth traffic analysis using exported NetFlow data.

NetFlow™ technology provides granular details about network traffic that has passed through an interface. NetFlow Analyzer processes this information to show you what applications are using bandwidth, who is using them, and when. Extensive graphs and reports make this information easy to analyze, and also help accelerate the troubleshooting process.

For more information on Cisco NetFlow visit http://www.cisco.com/go/netflow/

This User Guide will help you install NetFlow Analyzer, and get familiar with the user interface. If you are unable to find the information you are looking for in this document, please let us know at support@netflowanalyzer.com

What's New in this Release?

The latest release of NetFlow Analyzer (**5.5.0**) can be downloaded from the website at http://www.netflowanalyzer.com/download.html

New Features in Release 5.5.0

Feature	Description
NBAR based Reporting	NBAR(Network Based Application Recognition) - By intelligent classification of traffic lets you set QoS standard.
Scheduling of Reports	Allows setting of time intervals at which network traffic reports are generated automatically and mailed to desired recipient(s).
NetFlow V9 Support	Basic V9 support.
Associating IP address to application	Associate IP address to an application in addition to port & protocol.
Create Interface Groups	Ability to group interfaces together and monitor traffic.
ToS & TCP_flag	Reports based on TCP flags & TOS can be generated from the Trouble-shooting page.

New Features in Release 5.0

Feature	Description
Threshold-based Alerting	Set up alerts based on link utilization and send emails or SNMP Traps when thresholds are exceeded.
Troubleshooting	Retain raw data for longer time periods (up to 2 weeks) to enable increased visibility into traffic data for troubleshooting and alerts.
Support link	Wide range of options to contact technical support in case of any problems running NetFlow Analyzer.
Enhanced Router Settings	Specify whether router details need to be fetched based on IfName, IfAlias or IfDescription value.
Dashboard View Filter	Filter Dashboard Interface View to display only those interfaces exceeding specific values of incoming or outgoing traffic.
Traffic Graph Filters	Filter daily and weekly traffic graphs to show hour-based traffic details.
Enhanced IP Group Management	Specify interfaces when creating IP groups to further filter traffic details for an IP group.
Localized Versions	NetFlow Analyzer supports French, German, and Spanish along with Chinese and Japanese.

Features in Previous Releases (4.0 to 4.0.2)

Feature	Description
Web-based interface	Generate reports and perform administrative tasks from just a web browser
Support for NetFlow export versions	As of release 4.0.2, NetFlow Analyzer includes support for NetFlow **version 5** and **version 7** exports
Simply "turn on" NetFlow	Simply configure NetFlow export on your router or switch, and see it automatically added on the Dashboard
Real-time Traffic Graphs	View instant graphs of bandwidth utilization per network interface as soon as NetFlow data is received
Historical Trend Reports	Generate daily, weekly, monthly, and custom time period bandwidth reports showing peak traffic patterns

Feature	Description
Bandwidth Usage Reports	View reports showing top applications, top hosts, and top conversations using bandwidth
Consolidated Reports	View bandwidth reports per interface, showing all details on bandwidth usage for that interface
Autonomous Systems Reports	View AS and peering information for routers configured with BGP (useful for service providers)
NetFlow Devices	Categorize devices exporting NetFlow into logical groups and monitor them exclusively
IP Groups	Create departments based on IP addresses, ports, protocols, or interfaces and generate specific bandwidth usage reports
Application Configuration	Identify most standard applications out-of-the-box and configure custom applications to recognize specific traffic
User management	Add users with different privileges, assign device groups, and selectively allow access
Localized setup	NetFlow Analyzer can be installed and run in Chinese and Japanese languages, with support for more languages being added frequently. Check the website for the latest list of languages localized, and also contribute to translation works.

Installation and Setup

System Requirements

This section lists the minimum requirements for installing and working with NetFlow Analyzer.

Hardware Requirements

The minimum hardware requirements for NetFlow Analyzer to start running are listed below.

- 2.4GHz, Pentium 4 processor, or equivalent
- 1GB RAM
- 10GB disk space for the database

Interface	Processor	RAM
Upto 50	2.4 Ghz	1 GB
50 -150	3.4 GHz	2 GB
150 - 400	2 * 3.4 GHz	4 GB
400 - 1000	4 * 3.4 GHz	8 GB

NetFlow Analyzer is optimized for 1024 x 768 resolution and above.

For the device exporting NetFlow, ensure that the NetFlow export version format is exactly the same as the Cisco NetFlow version 5 or version 7 or version 9 format. For information on Cisco devices and IOS versions supporting Netflow, consult the Cisco NetFlow Device Support table.

Software Requirements

Platform Requirements

NetFlow Analyzer can be installed and run on the following operating systems and versions:

- Windows 2000 Server/Professional with SP 4
- Windows XP with SP 1
- RedHat Linux 8.0, 9.0
- SUSE Linux

Supported Web Browsers

NetFlow Analyzer has been tested to support the following web browsers and versions:

- Internet Explorer 5.5 and later
- Netscape 7.0 and later
- Mozilla 1.5 and later

Prerequisites

Before setting up NetFlow Analyzer in your enterprise, ensure that the following are taken care of.

Ports Required

NetFlow Analyzer requires the following ports to be free:

Port Name	Default Port Number	Usage
Web server port	8080	This is the port on which you will connect to the NetFlow Analyzer server from a web browser. You can change this at any time from the Settings tab.
NetFlow Listener port	9996	This is the port on which NetFlow exports are received from routers. You can change this at any time from the Settings tab.
MySQL port	13310	This is the port used to connect to the MySQL database in NetFlow Analyzer. Changing this port requires configuration level changes.

Recommended System Setup

Apart from the System Requirements, the following setup would ensure optimal performance from NetFlow Analyzer.

- Run NetFlow Analyzer on a separate, dedicated PC or server. The software is resource-intensive, and a busy processor can cause problems in collecting NetFlow data.
- Use the MySQL pre-bundled with NetFlow Analyzer that runs on port 13310. You need not start another separate instance of MySQL.

Changing the Default MySQL Port

1. Edit the **mysql-ds.xml** file present in the <*NetFlowAnalyzer_Home*>*/server/default/deploy* directory.
2. Change the port number in the following line to the desired port number:
   `<connection-url>jdbc:mysql://localhost:13310/netflow</connection-url>`
3. Save the file and restart the server.

Installing and Uninstalling

NetFlow Analyzer is available for Windows and Linux platforms. For information on supported versions and other specifications, look up System Requirements.

Installing NetFlow Analyzer

Windows

The Windows download for NetFlow Analyzer is available as an EXE file at http://www.netflowanalyzer.com/download.html

Download the EXE file to your local machine, and double-click it to start installation.Follow the instructions as they appear on screen to successfully install NetFlow Analyzer on to your machine.

Linux

The Linux download for NetFlow Analyzer is available as a BIN file at http://www.netflowanalyzer.com/download.html

1. Download the BIN file and assign **execute** permission using the command: `chmod a+x <file_name>.bin`
   where <*file_name*> is the name of the downloaded BIN file.
2. Execute the following command: `./<file_name>.bin`

During installation if you get an error message stating that the temp folder does not have enough space, try executing this command with the `-is:tempdir` <*directoryname*> option, where <*directoryname*> is the absolute path of an existing directory.
`./<file_name>.bin -is:tempdir` <*directory_name*>

3. Follow the instructions as they appear on the screen to successfully install NetFlow Analyzer on to your machine.

Uninstalling NetFlow Analyzer

Windows

1. Navigate to the Program folder in which NetFlow Analyzer has been installed. By default, this is **Start > Programs > ManageEngine NetFlow Analyzer 5**.
2. Select the option **Uninstall NetFlow Analyzer 5**.
3. You will be asked to confirm your choice, after which NetFlow Analyzer is uninstalled.

Linux

1. Navigate to the *<NetFlowAnalyzerHome>/_uninst* directory.
2. Execute the command `./uninstaller.bin`
3. You will be asked to confirm your choice, after which NetFlow Analyzer is uninstalled.

Starting and Shutting Down

Once you have successfully installed NetFlow Analyzer, start the NetFlow Analyzer server by following the steps below.

Starting NetFlow Analyzer

Windows

Click on **Start > Programs > ManageEngine NetFlow Analyzer 5 > NetFlow Analyzer 5** to start the server.

Alternatively you can navigate to the <*NetFlowAnalyzer_Home*>*bin* folder and invoke the **run.bat** file.

Linux

Navigate to the <*NetFlow Home*>*/bin* directory and execute the **run.sh** file.

When the server is started, a command prompt window opens up showing startup information on several modules of NetFlow Analyzer. Once all the modules have been successfully created, the following message is displayed:

```
Server started.
Please connect your client at http://localhost:8080
```

where 8080 is replaced by the port you have specified as the web server port during installation.

Starting as Service

Windows

If you have chosen the **Start as Service** option during installation, NetFlow Analyzer will run as a service on Windows.

Linux

1. Login as root user.
2. Navigate to the <*NetFlowAnalyzer_Home*>*bin* directory.
3. Execute the **linkAsService.sh** file
4. Then execute the command `/etc/init.d/netflowanalyzer start`

This starts NetFlow Analyzer as a service on Linux.

As far as **Fedora / SUSE** is concerned, please open the **mysql-ds.xml** file under the *server**default**deploy* directory and change the

<connection-url>jdbc:mysql://localhost:13310/netflow </connection-url> to

<connection-url>jdbc:mysql://127.0.0.1:13310/netflow </connection-url>

and restart the NetFlow Analyzer server.

Please follow the instructions below,

1. Navigate to /bin folder and backup (copy) linkAsService.sh to a safe location.
2. Open file linkAsService.sh in a editor and look for the following lines,

   [code:1:f5099fc2e0]for i in {0,6}
   do
   ln -s -f $initvar /etc/rc$i.d/$stopwith
   done
   ln -s -f $initvar /etc/rc5.d/$startwith[/code:1:f5099fc2e0]

3. Edit the above lines as follows, suffixing rc.d folder after /etc/ folder,

   [code:1:f5099fc2e0]for i in {0,6}
   do
   ln -s -f $initvar /etc/rc.d/rc$i.d/$stopwith
   done
   ln -s -f $initvar /etc/rc.d/rc5.d/$startwith
   [/code:1:f5099fc2e0]

4. Save the file.
5. Shutdown NetFlow Analyzer.
6. Execute linkAsService.sh and start NetFlow Analyzer using the command \" /etc/init.d/netflowanalyzer start \"

Shutting Down NetFlow Analyzer

Follow the steps below to shut down the NetFlow Analyzer server. Please note that once the server is successfully shut down, the MySQL database connection is automatically closed, and all the ports used by NetFlow Analyzer are freed.

Windows

1. Navigate to the Program folder in which NetFlow Analyzer has been installed. By default, this is **Start > Programs > ManageEngine NetFlow Analyzer 5**
2. Select the option **Shut Down NetFlow Analyzer**
3. Alternatively, you can navigate to the <*NetFlowAnalyzer_Home*>*bin* folder and invoke the **shutdown.bat** file.
4. You will be asked to confirm your choice, after which the NetFlow Analyzer server is shut down.

Linux

1. Navigate to the <*NetFlowAnalyzer_Home*>*/bin* directory.
2. Execute the `shutdown.sh` file.
3. You will be asked to confirm your choice, after which the NetFlow Analyzer server is shut down.

Accessing the Web Client

NetFlow Analyzer is essentially a bandwidth monitoring tool that uses Cisco NetFlow exports to analyze network traffic and determine bandwidth usage.

Once the server has successfully started, follow the steps below to access NetFlow Analyzer.

1. Open a supported web browser window
2. Type the URL address as **http://<*hostname*>:8080** (where **<*hostname*>** is the name of the machine on which NetFlow Analyzer is running, and **8080** is the default web server port)
3. Log in to NetFlow Analyzer using the default username/password combination of **admin/admin**

Once you log in, you can start managing devices exporting Cisco NetFlow, generate bandwidth reports, and more.

License Information

NetFlow Analyzer comes in two flavors:

- **Free Edition** - collect, analyze, and report on Netflow data from a maximum of **two** interfaces
- **Professional Edition** - collect, analyze, and report on Netflow data from a maximum of n interfaces (where 'n' is the number of interfaces for which NetFlow Analyzer has been purchased)

Once installed, NetFlow Analyzer runs in evaluation mode for 30 days. You can obtain a registered license for NetFlow Analyzer at any time during the evaluation period by contacting NetFlow Analyzer Support.

If you have not upgraded to the Professional Edition by the end of the evaluation period, NetFlow Analyzer automatically reverts to the Free Edition.

Upgrading your License

After obtaining the new license from AdventNet, save it on your computer, and follow the steps below to upgrade your NetFlow Analyzer installation:

1. Log in to the NetFlow Analyzer web client
2. Click **License Management** from Admin Operations
3. Click the **Upgrade License** link present in the top-right corner of the screen
4. In the License window that opens up, browse for the new license file and select it
5. Click **Upgrade** to apply the new license file

The new license is applied with immediate effect. You do not have to shut down or restart the NetFlow Analyzer server after the license is applied.

Configuring Cisco Devices

This section offers a brief guide to setting up NetFlow on a Cisco router or switch. For more detailed information, refer the Cisco web site at http://www.cisco.com/go/netflow. It is recommended that only people with experience in configuring Cisco devices follow these steps.

- Cisco devices with NetFlow support
- Configuring an IOS Device
- Configuring a Catalyst 6000 Series Switch
- Configuring a Native IOS Device
- Configuring a Catalyst 4000 Series Switch
- Configuring NetFlow for BGP

Setting the appropriate time on the router

NetFlow Analyzer stamps the flows based on the router time. It is therefore important to ensure that the time on the router is set properly. Netflow Analyer can handle routers from different time zones automatically, provided the correct time is set.

Whenever the time difference between the NetFlow Analyzer Server and the router is above 10 minutes a warning icon will appear in the home page. When this happens, NetFlow Analyzer will stamp the flows based on the system time of the NetFlow Analyzer server.

In case you see this, please ensure the following on the router:

- Check if the correct time is set on your router. You can check this by logging into the router and typing ***show clock***. You can set the clock time using the command ***clock set hh:mm:ss month date year***
- Check if the time zone and the offset (in Hours and Minutes) for the time zone is set properly (E.g. PST -8 00 for PST or EST -5 00 for EST). You can check this by logging into the router and typing ***show running-config***. You can set the clock time zone and offset using the command ***clock timezone zone hours [minutes]*** (E.g. clock timezone PST -8 00)

To enable NetFlow in an MPLS environment refer Cisco's documentation on MPLS NetFlow

Cisco® NetFlow Device Support

The following charts include information on the various vendors and devices supporting NetFlow version 5 or 7 data export. Use these charts to determine if your devices are compatible with NetFlow Analyzer.

Cisco Routers

Cisco IOS Software Release Version	Supported Cisco Hardware Platforms
11.1CA, 11.1CC	Cisco 7200 and 7500 series, RSP 7200 series
12.0	Cisco 1720, 2600, 3600, 4500, 4700, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series
12.0T, 12.0S	Cisco 1720, 2600, 3600, 4500, 4700, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8600 series
12.0(3)T, 12.0(3)S	Cisco 1720, 2600, 3600, 4500, 4700, AS5300, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8650 series
12.0(4)T	Cisco 1400, 1600, 1720, 2500, 2600, 3600, 4500, 4700, AS5300, AS5800 RSP 7000 and 7200 series uBR 7200 and 7500 series RSM series, MGX8800RPM series, and BPx8650 series
12.0(4)XE	Cisco 7100 series
12.0(6)S	Cisco 12000 series

NetFlow is also supported by these devices Cisco 800, 1700, 1800, 2800, 3800, 6500, 7300, 7600, 10000, CRS-1 and these Catalyst series switches: 45xx, 55xx, 6xxx.

These devices do not support NetFlow: Cisco 2900, 3500, 3660, 3750.

Cisco Switches

NetFlow export is also supported on other Cisco switches when using a NetFlow Feature Card (NFFC) or NFFC II and the Route Switch Module (RSM), or Route Switch Feature Card (RSFC). However, check whether version 5 is supported, as most switches export version 7 by default.

NetFlow Version 9 Support

Supported Platforms

The following platforms support NetFlow Version 9 Data Export :

- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7300 series

- Cisco 7400 series
- Cisco 7500 series
- Cisco 12000 series

Other Vendors

Some of the major vendors supporting NetFlow include:

- Alcatel
- Enterasys Networks
- Extreme Networks - Does not support input/output interface, octets, or first and last times.
- Foundry Networks
- Juniper Networks - Does not support sampling interval attribute. First and last times are stored in seconds rather than milliseconds.
- Riverstone Networks - no native NetFlow support. However, Riverstone provides a converter that translates the LFAP records from their devices into NetFlow.

Configuring NetFlow Export on an IOS Device

Follow the steps below to configure NetFlow export on a Cisco IOS device.


Refer the Cisco Version Matrix for information on Cisco platforms and IOS versions supporting NetFlow

Enabling NetFlow Export

Enter global configuration mode on the router or MSFC, and issue the following commands for **each interface** on which you want to enable NetFlow:

```
interface {interface} {interface_number}
ip route-cache flow
bandwidth <kbps>
exit
```


In some recent IOS releases Cisco Express Forwarding has to be enabled. Issue the command **`ip cef`** in global configuration mode on the router or MSFC for this.

This enables NetFlow on the specified interface alone. Remember that on a Cisco IOS device, **NetFlow is enabled on a per-interface basis**. The `bandwidth` command is optional, and is used to set the speed of the interface in kilobits per second. Interface speed or link speed value is used to later calculate percentage utilization values in traffic graphs.

Exporting NetFlow Data

Issue the following commands to export NetFlow data to the server on which NetFlow Analyzer is running:

Command	Purpose
`ip flow-export destination {hostname|ip_address} 9996`	Exports the NetFlow cache entries to the specified IP address. Use the IP address of the NetFlow Analyzer server and the configured NetFlow listener port. The default port is 9996.
`ip flow-export source {interface} {interface_number}`	Sets the source IP address of the NetFlow exports sent by the device to the specified IP address. NetFlow Analyzer will make SNMP requests of the device on this address.
`ip flow-export version 5 [peer-as | origin-as]`	Sets the NetFlow export version to version 5. **NetFlow Analyzer supports only version 5, version 7 and version 9**. If your router uses BGP you can specify that either the origin or peer AS is included in exports - it is not possible to include both.
`ip flow-cache timeout active 1`	Breaks up long-lived flows into 1-minute fragments. You can choose any number of minutes between 1 and 60. If you leave it at the default of 30 minutes your traffic reports will have spikes. It is important to set this value to **1 minute** in order to generate alerts and view troubleshooting data.
`ip flow-cache timeout inactive 15`	Ensures that flows that have finished are periodically exported. The default value is 15 seconds. You can choose any number of seconds between 10 and 600. However, if you choose a value greater than 250 seconds, NetFlow Analyzer may report traffic levels that are too low.
`snmp-server ifindex persist`	Enables ifIndex persistence (interface names) globally. This ensures that the ifIndex values are persisted during device reboots.

	For more information on BGP reporting in NetFlow Analyzer, look up the section on Configuring NetFlow for BGP

Verifying Device Configuration

Issue the following commands in **normal (not configuration) mode** to verify whether NetFlow export has been configured correctly:

Command	Purpose
`show ip flow export`	Shows the current NetFlow configuration
`show ip cache flow`	These commands summarize the active flows and give an indication of how much NetFlow data the device is exporting
`show ip cache verbose flow`	

A Sample Device Configuration

The following is a set of commands issued on a router to enable NetFlow version 5 on the FastEthernet 0/1 interface and export to the machine 192.168.9.101 on port 9996.

```
router#enable
Password:*****
router#configure terminal
router-2621(config)#interface FastEthernet 0/1
router-2621(config-if)#ip route-cache flow
router-2621(config-if)#exit
router-2621(config)#ip flow-export destination 192.168.9.101 9996
router-2621(config)#ip flow-export source FastEthernet 0/1
router-2621(config)#ip flow-export version 5
router-2621(config)#ip flow-cache timeout active 1
router-2621(config)#ip flow-cache timeout inactive 15
router-2621(config)#snmp-server ifindex persist
router-2621(config)#^Z
router#write
router#show ip flow export
router#show ip cache flow
```

**repeat these commands to enable NetFlow for each interface*

	Please note that NetFlow data export has to be enabled on all interfaces of a router in order to see accurate IN and OUT traffic. Suppose you have a router with interface A and B. Since NetFlow, by default, is done on an ingress basis, when you enable NetFlow data export on interface A, it will only export the IN traffic for interface A and OUT traffic for interface B. The OUT traffic for interface A will be contributed by the NetFlow data exported from interface B. Even if you are interested in managing only interface A, please enable NetFlow data export on A and B. You may subsequently unmanage interface B from the License Management link.

Turning off NetFlow

Issue the following commands in global configuration mode to stop exporting NetFlow data:

Command	Purpose
`no ip flow-export destination {hostname|ip_address} {port_number}`	This will stop exporting NetFlow cache entries to the specified destination IP address on the specified port number
`interface {interface} {interface_number}`	This will disable NetFlow export on the specified interface. Repeat the commands for each interface on which you need to disable NetFlow.
`no ip route-cache flow`	
`exit`	

For further information on configuring your IOS device for NetFlow data export, refer Cisco's NetFlow commands documentation

Configuring NDE on Catalyst 6000 Series Switches

Follow the steps below to configure NDE on Catalyst 6000 Series switches

Configuring NDE on Catalyst 6000 Series Switches

Enter privileged mode on the Supervisor Engine and issue the following commands to configure NDE:

Command	Purpose
`set mls nde {hostname|ip_address} 9996`	Specifies NetFlow Analyzer as the NDE collector and the configured Netflow listener port as the UDP port for data export of hardware-switched packets.
`ip flow-export destination {hostname|ip_address} 9996`	Specifies NetFlow Analyzer as the NDE collector and the configured Netflow listener port as the UDP port for data export of software-switched packets. *
`set mls agingtime long 64`	Breaks up long-lived flows into 1-minute fragments. This ensures that traffic graphs do not have spikes. It is important to set this value to **1 minute** in order to generate alerts and view troubleshooting data.
`set mls agingtime 32`	Ensures that flows that have finished are periodically exported. Ensure that the set value is not too low, else NetFlow Analyzer may report traffic levels that are too low.
`set mls flow full`	This sets the flow mask to full flows. This is required to get useful information from the switch.
`set mls nde enable`	This enables NDE

**To monitor data and statistics about Layer 3 traffic that is switched in software by the MSFC, you must specify the NDE collector and UDP port on the MSFC. This requires that you enter the `ip flow-export destination` command on the MSFC.*

Use the `show mls debug` command to debug the NDE configuration

For more information on configuring NDE on Catalyst 6000 Series switches, refer Cisco's documentation.

Configuring NDE on a Native IOS Device

To enable NDE on a Native IOS device, enter the configure mode on the Supervisor Engine, and follow the instructions for an IOS device. Then issue the following commands to enable NDE.

Configuring NDE

Enter privileged mode on the Supervisor Engine and issue the following commands to enable NDE:

Command	Purpose
`mls nde sender version 7`	Sets the export version. Version 7 is the most recent full export version supported by switches.
`set mls aging long 64`	Breaks up long-lived flows into 1-minute fragments. This ensures that traffic graphs do not have spikes. It is important to set this value to **1 minute** in order to generate alerts and view troubleshooting data.
`set mls aging normal 32`	Ensures that flows that have finished are periodically exported. A lower value may result in NetFlow Analyzer reporting traffic levels that are too low.

In order to put interface an routing information into the Netflow exports, issue the following commands depending on the Supervisor Engine.

Switch Configuration	Lowest IOS (MSFC) Level	Commands
Sup2 or 720	12.1.13(E)	`mls flow ip interface-full` `mls nde interface`
Sup1	12.1.13(E)	`set mls flow ip full`

This information is not available with IOS versions earlier than 12.1.13(E) on the Supervisor Engine 2 or 720

Configuring NDE on 4000 Series Switches

Follow the steps below to configure NDE on a 4000 Series switches.

The 4000 and 4500 series switches require a Supervisor IV with a NetFlow Services daughter card(WS-F4531) and IOS version 12.1(19)EW or above to support NDE.

Configure this device as for an IOS device, but **omit** the `ip route-cache flow` command on each interface. Then issue the following command:

```
ip route-cache flow infer-fields
```

This command ensures routing information is included in the flows. You will not enter the `ip route-cache flow` command on each interface.

A Sample Device Configuration

The following is a set of commands issued on a 4000 Series switch to enable NetFlow version 7 and export to the machine 192.168.9.101 on port 9996 using FastEthernet 0/1 as the source interface.

```
switch>(enable)ip flow-export destination 192.168.9.101 9996
switch>(enable)ip flow-export version 7
switch>(enable)ip flow-export source FastEthernet 0/1
switch>(enable)ip flow-cache timeout active 1
switch>(enable)ip route-cache flow infer-fields
```

Configuring NetFlow for BGP

The Border Gateway Protocol (BGP), defined in RFC 1771, provides loop-free interdomain routing between autonomous systems. (An autonomous system [AS] is a set of routers that operate under the same administration.) BGP is often run among the networks of Internet service providers (ISPs).

In order to get AS info, you need to configure your router to include AS info. AS information collection is resource intensive, especially when configured for origin-AS. In case you are not interested in monitoring peering arrangements, disabling AS collection may improve NetFlow Analyzer performance.

Enabling BGP Routing

Enter the global configuration mode and issue the following commands to enable BGP routing and establish a BGP routing process:

Command	Purpose
`router bgp` *`as-number`*	Enables the BGP routing process, which places the router in router configuration mode
`network` *`network-number`* `[mask` *`network-mask`*`] [route-map` *`route-map-name`*`]`	Flags a network as local to this autonomous system and enters it to the BGP table

Configuring BGP Neighbors

BGP supports two kinds of neighbors: internal and external. Internal neighbors are in the same autonomous system; external neighbors are in different autonomous systems. Normally, external neighbors are adjacent to each other and share a subnet, while internal neighbors may be anywhere in the same autonomous system.

To configure BGP neighbors, issue the following command in router configuration mode:

Command	Purpose
`neighbor {`*`ip-address`*`|`*`peer-group-name`*`} remote-as` *`as-number`*	Specifies a BGP neighbor

BGP Neighbor Configuration Examples

The following example shows how BGP neighbors on an autonomous system are configured to share information.

```
router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99
```

In the example, a BGP router is assigned to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighboring routers. The first router listed is in a different autonomous system; the second neighbor's `remote-as` router configuration command specifies an internal neighbor (with the same autonomous system number) at address *131.108.234.2* and the third

neighbor's `remote-as` router configuration command specifies a neighbor on a different autonomous system.

Including AS Info in Netflow Exports

If you have configured BGP on your network, and want Netflow to report on autonomous systems (AS info), issue the following command on the router in global configuration mode:

Command	Purpose
`ip flow-export destination {hostname|ip_address} 9996`	Exports the Netflow cache entries to the specified IP address. Use the IP address of the NetFlow Analyzer server and the configured Netflow listener port. The default port is 9996.
`ip flow-export {version}[peer-as | origin-as]`	Exports NetFlow cache entries in the specified version format (5 or 7). If your router uses BGP, you can specify that either the origin or peer ASs are included in exports – it is not possible to include both.

Getting Started

Once NetFlow Analyzer has been successfully set up and started in your network, the next thing to do is start receiving Netflow exports from routing devices on your network.

	The Configuring Cisco Devices section contains useful information on how to configure Netflow export on different Cisco routers and switches

As soon as you log in to the NetFlow Analyzer web client, you will see the **Global View - Dashboard View**. This view shows you information on interfaces sending Netflow exports, AS info, as well as traffic information for all IP groups created so far. The Dashboard is populated as soon as Netflow data is received from any interface.

The Global View is divided into two tabs.

1. The Interface View which lists all the interfaces from which Netflow exports are received
2. The Autonomous System View which lists all the autonomous systems configured with each router

Information on IP groups is displayed below the two tabs. From any tab, click the  icon to return to the Global View.

Click the  icon or the **Custom Report** link at the top-left corner of the Global View page to generate a traffic report based on specific criteria across selected interfaces.

Dashboard Interface View

The **Interface View** tab displays information on all interfaces from which NetFlow exports are received.

The default **Router List** shows all the routers and interfaces from which NetFlow exports have been received so far, along with specific details about each interface. The default view shows the first router's interfaces alone. The remaining **routers'** interfaces are hidden. Click the **[Show All]** link to display all **routers'** interfaces on the Dashboard. Click the **[Hide All]** link to hide all interfaces and show only the router names in the Router List.

You can set filters on the Dashboard view to display only those interfaces whose incoming or outgoing traffic values exceed a specified percentage value. Click the **[Filter]** link to specify minimum percentage values for IN or OUT traffic. Click the **Set** button for the changes to take effect. The filter settings are then displayed beside the **[Filter]** link. Click the icon at any time to clear the filter settings and display all interfaces on the Dashboard again.

The purpose of icons and buttons in the Router List are explained below.

Icon/ Button	Purpose
	Click this icon, or on the router name, to view the interfaces corresponding to the router
	Click this icon to hide the interfaces corresponding to the router
(before Router Name)	Click this icon to change the display name of the device, its SNMP community string, or its SNMP port. You can also choose to get the Interface Name details from one of 3 fields - IfDesc, IfName, or IfAlias.
(before Interface Name)	Click this icon before the interface name to change the display name of the interface, or its link speed (in bps). You can also set the SNMP parameters of the router corresponding to an interface by clicking the link present in the **Note** included below the settings.
	Click this link to troubleshoot an interface. You can troubleshoot only **one** interface at a time. **Note:** Troubleshooting results are shown directly from raw data. Hence results depend on the raw data retention time period set in Settings
	Click this icon to see a quick report for the respective interface. This report shows you all the details about the traffic across that interface for the past one hour
	Indicates that NBAR report is available for the interface

	Clicking the **Stop** button only means that NetFlow Analyzer will drop flows from this device. To stop this device from exporting NetFlow statistics, you need to work on the device directly. See the section on Configuring Cisco Devices for more information.

The Interface Name column lists all the interfaces on a discovered device. Click on an interface to view the traffic details for that interface.

The Status column indicates the current status of that interface.

Icon	Description
	The Status of the interface is unknown and no flows have been received for the past 10 minutes. The interface is not responding to SNMP requests.
	The interface is responding to SNMP requests and the link is up, but no flows have been received for the past ten minutes.

Icon	Description
	The link is up, and flows are being received.
	The interface is responding to SNMP requests and the link is down and no flows are being received.

The IN Traffic and OUT Traffic columns show the **utilization** of IN and OUT Traffic on the respective interfaces for the past one hour. You can click on the IN Traffic or OUT traffic bar to view the respective application traffic graph for that interface.

Dashboard AS View

The **Autonomous System View** displays information on all the autonomous systems (AS) to which a router belongs, along with traffic details for each AS.

	In order to get AS info in this view, you need to configure your router to include AS info. AS information collection is resource intensive, especially when configured for origin-AS. In case you are not interested in monitoring peering arrangements, disabling AS collection may improve NetFlow Analyzer performance.

The **Router List** displays each router along with the AS to which it belongs. Click on the AS Name to view the traffic report for that AS. The Dashboard also shows the organization to which the AS belongs, and the amount of incoming and outgoing traffic for the past one hour.

The purpose of icons and buttons in the Router List are explained below.

Icon/ Button	Purpose
	Click this icon, or on the router name, to view the autonomous systems to which this router belongs
	Click this icon to hide the AS corresponding to a router
	Click this icon before the router name to change the display name of the device, its SNMP community string, or its SNMP port
	Click this icon to see the - Last 1 Hour report, on incoming and outgoing traffic for that AS for the past one hour
	Click this icon to start AS collection
	Click this icon to stop AS collection

IP Groups View

Information on IP groups created so far, is displayed below both the Global View tabs. This is also displayed when the **All Groups** link is clicked on the **IP Groups** pane on the left.

Initially when no IP groups have been created, you will simply see a status message with the option to start creating IP groups.

The **IP Group List** shows all the IP groups that have been created so far. Click the **View Description** link to view descriptive information on all IP groups created. Alternatively you can click the **View Description** link against each IP group to view descriptive information on that IP group alone.

Click the IP Group name to view traffic graphs specific to that IP group. From the traffic graph, you can navigate to see the top applications, top hosts, and top conversations in this IP group.

The **IN Traffic** and **OUT Traffic** columns show the volume of incoming and outgoing traffic in the IP group generated over the past one hour. You can click on the IN Traffic or OUT traffic bar to view the respective application traffic report.

Click the  icon to see a consolidated traffic report for the respective IP group. This report shows you all the details about incoming and outgoing traffic in this IP group in a single report.

Traffic Report

Netflow Traffic Reports

NetFlow Analyzer generates traffic reports in real-time, as soon as NetFlow data is received from an interface.

The traffic reports in NetFlow Analyzer include information on:

- Traffic Trends
- Top Applications
- Top Hosts
- Top Conversations
- AS Traffic Reports

Apart from these pre-defined reports, Custom Reports let you define criteria and generate specific reports on network activity. Consolidated Reports show you overall traffic statistics for an interface or AS as applicable. Troubleshooting Reports let you troubleshoot an interface using raw data directly.

Click the  icon or the **Troubleshoot** link at the top-left corner of the page to troubleshoot this interface.

Real-time Traffic Graphs

NetFlow Analyzer generates traffic graphs as soon as Netflow data is received. The **Traffic** tab shows real-time traffic graphs for incoming and outgoing traffic. Depending on which link was clicked, you can see traffic graphs for an interface or IP group.

Tabs above the traffic graph, let you view the graph in terms of volume of traffic, speed, link utilization, and number of packets received.

	The **Packets** tab shows the number of actual packets of traffic data received. This information is included in exported Netflow data.

You can see traffic graphs for different time periods by choosing the appropriate values from the Time Period box. Use the **From** and **To** boxes to choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate traffic report.

The table below the graph shows the legend, along with total, maximum, minimum, and average traffic values for this interface or IP group, for the selected time period.

The **Traffic IN Details** and the **Traffic OUT Details** show sampled values of traffic generated over the selected time period.

Time Filters

You can choose to see hour-based data in the traffic graphs for daily and weekly reports. To do this, first select the **Last Day Report** or **Last Week Report** option in the top time selection bar. When the respective traffic graph is displayed, the table below the graph includes the  icon next to the **Category** label.

Click the  icon to specify the hourly time interval for which you want to see traffic graphs. Click the **Show** button to set the filter and see hour-based values in the traffic graph as well as the table below. Click the **Reset** button to turn the filter off and switch to the regular traffic graphs.

95-th Percentile

The 95th percentile is the number that is greater than 95% of the numbers in a given set. The reason this statistic is so useful in measuring data throughput is that it gives a very accurate picture of the maximum traffic generated on an interface. This is a standard measure that is used for interpreting the performance data.

The 95th Percentile is the highest value left when the top 5% of a numerically sorted set of collected data is discarded. It is used as a measure of the peak value used when one discounts a fair amount for transitory spikes. This makes it markedly different from the average. The following example would help you understand it better.

Consider if the data collected for CPU Utilization is 60,45,43,21,56,89,76,32,22,10,12,14,23,35,45,43,23,23,43,23 (20 points). This list is sorted in descending order and a single top value, 89, is discarded. Since 1 consitutes 5% of 20, we discarded 1 value in this case. The highest value in the remaining list, 76, is the 95th percentile.

Top Applications

The **Applications** tab shows you the top applications and top protocols for the selected time period. The default view shows the **Top ApplicationIN Report**. This report shows the distribution of incoming traffic application-wise.

Choose between **IN** and **OUT** to display the application-wise distribution of incoming or outgoing traffic respectively.

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate application traffic report.

The table below the graph shows the distribution of traffic per application. You can see what application caused how much traffic, and how much of the total bandwidth was occupied by that application.

The icon next to an application name indicates that that application is not identified by NetFlow Analyzer. When you click on this icon, a window opens up showing the port and protocol details for this application. If it is a valid application you can then add it to the list of applications in the Application Mapping page.

	The icon will be displayed next to an unknown application only in the Last Hour report.

Click on an application's name to see the Top Conversations that contributed to this application's traffic.

The **Show** box above this table lets you choose how many applications need to be displayed. You can set the maximum value for this option from the Settings page.

The pie chart below this table shows what percentage of bandwidth is being used by each application. The icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the icon to save the pie chart as a PDF file.

Viewing Top Protocols

Click the icon or the **Protocol Distribution** link to see the top protocols for the selected interface or IP group, in a new window.

Choose between **IN** and **OUT** to display the protocol-wise distribution of incoming or outgoing traffic respectively.

	This report sorts traffic based on the protocol used, while the **Application IN/OUT Report** sorts traffic based on the application, i.e., the combination of port and protocol.

Click on a protocol's name to see the Top Conversations that used this protocol. The **Show** box above this table lets you choose how many applications need to be displayed. You can set the maximum value for this option from the Settings page.

The pie chart below this table shows what percentage of bandwidth is being used by each protocol. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the  icon to save the pie chart as a PDF file.

Top Hosts

The **Source** tab shows the top source hosts contributing to traffic in the selected time period. The default view shows the **Top SourceIN Report**.

The **Destination** tab shows the top destination hosts contributing to traffic in the selected time period. The default view shows the **Top DestinationIN Report**.

Choose between **IN** and **OUT** to display the top hosts in incoming or outgoing traffic.

	When you drill down from an IP group, traffic is unidirectional, and hence the **IN** and **OUT** options are not available.

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate source or destination traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values.

The **Show** box above this table lets you choose how many hosts need to be displayed. You can set this value from the Settings page.

The pie chart below this report shows what percentage of bandwidth is being used by each host. The icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the icon to save the pie chart as a PDF file.

TOS

Because the Internet by itself has no direct knowledge of optimizing the path for a particular application or user, the IP protocol provides a facility for upper layer protocols to convey hints to the Internet Layer about how the tradeoffs should be made for a particular packet. This facility is the "Type of Service" facility, abbreviated as the "TOS facility".

The TOS facility is one of the features of the Type of Service octet in the IP datagram header. The Type of Service octet consists of three fields. The first 3 bits (0,1,2) are for the first field, labeled "Precedence" , intended to denote the importance or priority of the datagram. The second field, labeled "TOS" , denotes how the network should make tradeoffs between throughput, delay, reliability, and cost.The last field, labeled "MBZ" (for "must be zero") above, is currently unused. The originator of a datagram sets this field to zero (unless participating in an Internet protocol experiment which makes use of that bit). Routers and recipients of datagrams ignore the value of this field.This field is copied on fragmentation.

Specification of the TOS Field

The semantics of the TOS field values (expressed as binary numbers):

1000	**maximize throughput**
0100	**minimize delay**
0010	**maximize reliability**
0001	**minimize monetary cost**
0000	**normal service**

The values used in the TOS field are referred to as "TOS values", and the value of the TOS field of an IP packet is referred to as the "requested TOS". The TOS field value 0000 is referred to "default TOS." Because this specification redefines TOS values to be integers rather than sets of bits, computing the logical OR of two TOS values is no longer meaningful. For example, it would be a serious error for a router to choose a low delay path for a packet whose requested TOS was 1110 simply because the router noted that the former "delay bit" was set.

Although the semantics of values other than the five listed above are not defined , they are perfectly legal TOS values, and hosts and routers must not preclude their use in any way. Only the default TOS is in any way special. A host or router need not make any distinction between TOS values

For example, setting the TOS field to 1000 (minimize delay) does not guarantee that the path taken by the datagram will have a delay that the user considers "low". The network will attempt to choose the lowest delay path available, based on its (often imperfect) information about path delay. The network will not discard the datagram simply because it believes that the delay of the available paths is "too high" (actually, the network manager can override this behavior through creative use of routing metrics, but this is strongly discouraged: setting the TOS field is intended to give better service when it is available, rather than to deny service when it is not).

Use of the TOS Field in Routing

Both hosts and routers should consider the value of the TOS field of a datagram when choosing an appropriate path to get the datagram to its destination.The mechanisms for doing so are discussed in this section.

Whether a packet's TOS value actually affects the path it takes inside a particular routing domain, is a choice made by the routing domain's network manager. In many routing domains the paths are sufficiently homogeneous in nature that there is no reason for routers to choose different paths based up the TOS field in a

datagram. Inside such a routing domain, the network manager may choose to limit the size of the routing database and of routing protocol updates by only defining routes for the default (0000) TOS.

Neither hosts nor routers should need to have any explicit knowledge of whether TOS affects routing in the local routing domain.

Inherent Limitations:

The most important of all the inherent limitations is that the TOS facility is strictly an advisory mechanism. It is not an appropriate mechanism for requesting service guarantees.There are two reasons why this is so:

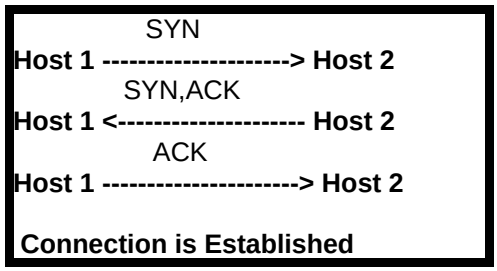
- Not all networks will consider the value of the TOS field when deciding how to handle and route packets.Partly this is a transition issue: there will be a (probably lengthy) period when some networks will use equipment that predates this specification. Even long term, many networks will not be able to provide better service by considering the value of the TOS field. For example, the best path through a network composed of a homogeneous collection of interconnected LANs is probably the same for any possible TOS value. Inside such a network, it would make little sense to require routers and routing protocols to do the extra work needed to consider the value of the TOS field when forwarding packets.
- The TOS mechanism is not powerful enough to allow an application to quantify the level of service it desires. For example, an application may use the TOS field to request that the network choose a path which maximizes throughput, but cannot use that mechanism to say that it needs or wants a particular number of kilobytes or megabytes per second. Because the network cannot know what the application requires, it would be inappropriate for the network to decide to discard a packet which requested maximal throughput because no "high throughput" path was available.

TCP Flags

There are 6 flags - the Urgent Pointer flag, ACK(acknowledgement) flag, Push flag, RST(reset flag), SYN(synchronisation) flag & the FIN(finished) flag.

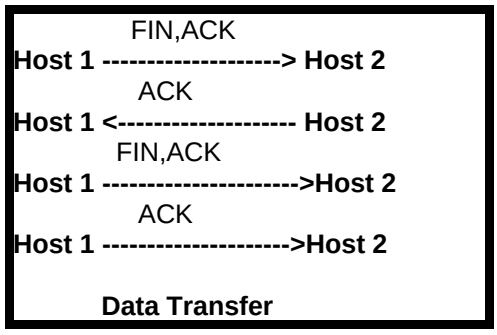
The Urgent Pointer flag identifies the incoming data as 'urgent'. The identified segments are processed immediately by being assigned high priority without waiting till all queued data is processed. The ACKnowledgement flag can be used to acknowledge the successful receipt of packet(s) - either the acknowledgement can be made for every packet received or for every n-th packet received. The Push flag can be used to assign the data the desired priority and is processed either at the Source or Destination. In using the push flag attention need to be paid to the fact that correct data segment handling is done. Also the appropriate priority needs to be set at the two ends of a connection.

When a segment that is not intended for the current connection has arrived the reset flag(RST) can be set . For instance if a remote system were to send a packet to a host to establish connection, and if that service is not supported by the host then the host can reject the request and then set the RST flag indicating that the host has reset the connection.



The fifth flag in the TCP Flag options- the SYN flag is a highly used flag in TCP communication - the SYN flag is initialy sent when establishing the typical 3-way handshake between two hosts as shown above The Host 1 needs to establish contact with Host B using TCP as the protocol. In the course of the 3-way handshake there are 2 SYN flags transmitted . As the connection is set and data is transmitted between the two hosts more SYN flags will be sent and received.

The sixth & final flag available is the FIN flag which appears when the last packets are exchanged between a connection. When a host sends a FIN flag to close a connection, it may continue to receive data until the remote host has also closed the connection. A typical disconnection is shown below. TCP is a Full Duplex connection so there are two directions of data flow.



After the data transfer is completed the Host 1 sends a packet with the FIN, ACK flags set to Host 2. By this action Host 1 has acknowledged the previous data stream while simultaneously has initiated a TCP closing action to end this connection. After this Host 1's application will not receive any more data and the connection will be closed. Also Host 2 in response to Host 1's request to end the connection sends an acknowledgement back, After this is completed , the Host 2 sends its own FIN,

ACK flags to end the connection. Finally Host 1 acknowledges the request Host 2 made earlier and this way the connection is closed

TCP & Worms

Typically worm sources don't pool the whole network , but randomly try to open from time to time a single host connection. One can use TCP flags and ICMP tracking. When the attacker tries to open the TCP connection to an unused destination IP address the TCP SYN flag is set. If the connection is successful there will be cumulative TCP flags SYN and ACK, if the connection is unsuccessful only flows with SYN flag will be there. Based on the count of the unsuccessful connections for every source IP address outside the network and source, the attacker can be tracked - the one with the most number of connection attempts. If attacker is using UDP protocol and pools the whole network, an excessive number of ICMP messages will then be generated.

Top Conversations

The **Conversation** tab shows the top conversations contributing to traffic in the selected time period.

Choose between **IN** and **OUT** to display the top conversations in incoming or outgoing traffic.

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate conversation traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS names.

The **Show** box above this table lets you choose how many conversations need to be displayed. You can set this value from the Settings page.

The **Group by** box lets you group conversations by source, destination, or application. The default list shows the conversations sorted in descending order of number of bytes of traffic.
The pie charts below this report show the top sources, destinations, and conversations contributing to traffic for the selected time period. The  icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the  icon to save the pie chart as a PDF file.

Custom Reports

Custom Reports let you set several criteria and view specific reports. This is especially useful in finding out the bandwidth utilization of a specific host or application. Custom reports can also tell you details about a certain application and which hosts are using it, thereby helping to troubleshoot, and even detect virus activities.

Click the  icon or the **Custom Report** link on the Dashboard to to set criteria and view custom reports. In the pop-up window that opens up, click the **Select Devices** link to select the routers and/or interfaces whose traffic needs to be analyzed.

Under Report Criteria, you can specify a maximum of three filtering criteria:

- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **Show** box lets you choose how many results to display. You can set this value from the Settings page.

Once you select all the desired criteria, click the **Generate Report** button to display the corresponding traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values. You can also choose to print this report by clicking the  icon or the **Print** link.

	Custom Reports are different from Troubleshooting Reports. You can troubleshoot only **one** interface at a time, whereas Custom Reports can be generated across interfaces. Data for Troubleshooting reports is taken directly from raw data, whose maximum retention period can be set from Settings. But data for Custom Reports is taken from aggregated data in the database.

Consolidated Reports

Consolidated reports let you see all the traffic details for an interface or IP group at one glance. You can then print this report or save it as a PDF file.

Click the **Consolidated Report** link or the  icon to see all traffic details for an interface at one glance. The same report can be accessed from the Global Dashboard when the  icon against an interface or IP group is clicked.

The Custom Selection box lets you select different time periods for the traffic data.

- The **1 Hour Report** and **1 Day Report** options show you traffic details over the past one hour and one day respectively.
- The **8AM to 8PM** option shows you traffic details from 8 a.m. to 8 p.m. of the previous day. This is a peak hour report, based on the normal working hours of an enterprise.

Apart from these options, the **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Once you select the desired time period, click the **Show Report** button to display the corresponding consolidated report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS names. You can also choose to save the report as a PDF file by clicking the  icon, or print it by clicking the  Print icon.

AS Traffic Reports

The Traffic report for autonomous systems shows the amount of incoming and outgoing traffic for that AS, over the past one hour.

Tabs above the traffic graph let you view the graph in terms of volume of traffic, speed, and number of packets received.

You can see traffic graphs for different time periods by choosing the appropriate values from the Time Period box. Use the **From** and **To** boxes to choose custom time periods for the graphs. Use the  icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show Report** button to display the appropriate traffic report.

The table below the graph shows the legend, along with total, maximum, minimum, and average traffic values for this AS for the selected time period.

The **Traffic IN Details** and the **Traffic OUT Details** show sampled values of traffic generated over the selected time period.

Troubleshooting

The **Troubleshoot** link lets you set criteria and view specific details about the traffic across a single interface. Data for Troubleshooting reports is taken directly from raw data. Which means that Troubleshooting reports will be available only for the maximum time period for retaining raw data, configured under Settings.

Click the  icon against an interface on the Dashboard Interface View, or the **Troubleshoot** link present above the traffic graphs for an interface, to open a popup with options to set criteria for viewing reports. In the pop-up window that opens up, click the **Select Devices** link to change the interface that you want to troubleshoot.

Under Search Criteria, enter the criteria on which traffic needs to be filtered. You can enter any of the following criteria to filter traffic:

- Source/Destination Address
- Source/Destination Network
- Source/Destination Nodes
- Application
- Port/Port Range

The **From** and **To** boxes let you choose custom time periods for the report. Use the  icon to select the date and time easily. Ensure that the time period selected, falls within the Raw Data Retention Period set under Settings, otherwise graphs will show no data.

Use the **IN/OUT** box to display values based on IN traffic, OUT traffic, or both IN and OUT traffic. The **Show** box lets you choose how many results to display. You can set this value from the Settings page.

Once you select all the desired criteria, click the **Generate Report** button to display the corresponding traffic report.

The default report view shows the IP addresses of the hosts. Click the **Resolve DNS** link to see the corresponding DNS values. You can also choose to print this report by clicking the  icon or the **Print** link.

NBAR Report

The **NBAR Report** tab lists the various applications in your network and their percentage of the total traffic for the selected time period. The default view shows the **NBAR Application - In Report**. This report shows the distribution of traffic application-wise.

Choose between **IN** and **OUT** to display the application-wise distribution of incoming or outgoing traffic respectively.

The Time Period box lets you choose between last hour, last day, last week, last month, and last quarter's traffic graphs. The **From** and **To** boxes let you choose custom time periods for the graphs. Use the icon to select the date and time easily. The time period for these graphs is based on the current system time. Once you select the desired date and time, click the **Show** button to display the appropriate application traffic report.

The table below the graph shows the distribution of traffic per application. You can see what application caused how much traffic, and how much of the total bandwidth was occupied by that application.

Click the icon (**Supported Applications** link) to see the list of supported applications, in a new window.

Viewing Top Applications

Choose between **IN** and **OUT** to display the protocol-wise distribution of incoming or outgoing traffic respectively.

The pie chart below shows what percentage of bandwidth is being used by each Application. The icon above the pie chart lets you see the pie chart enlarged in a new window. From here, you can click the icon to save the pie chart as a PDF file.

NBAR supported applications

NBAR supports a wide range of network protocols.The following list shows some of the supported protocols:

1. **Peer-to-Peer Protocols**

Peer-to-Peer Protocol	Type	Description
BitTorrent	TCP	File-sharing application
Gnutella	TCP	File-sharing application
Kazaa2	TCP	File-sharing application
eDonkey	TCP	File-sharing application
Fasttrack	TCP	File-sharing application
Napster	TCP	File-sharing application

2. **VoIP Protocols**

VoIP Protocol	Type	Description
SCCP	TCP	Skinny Call Control Protocol
SIP	TCP and UDP	Session Initiation Protocol
MGCP	TCP and UDP	Media Gateway Control Protocol
H.323	TCP and UDP	An ITU-T standard for digital videoconferencing over TCP/IP networks
SKYPE	TCP and UDP	Application allowing telephone conversation over the Internet

3. TCP & UDP stateful protocols

TCP or UDP Stateful Protocol	Type	Description
FTP	TCP	File Transfer Protocol
Exchange	TCP	MS-RPC for Exchange
HTTP	TCP	HTTP with URL, host, or MIME classification
Citrix	TCP	Citrix published application
Netshow	TCP/UDP	Microsoft Netshow
RealAudio	TCP/UDP	RealAudio Streaming Protocol
r-commands	TCP	rsh, rlogin, rexec
StreamWorks	UDP	Xing Technology Stream Works audio/video
SQL*NET	TCP/UDP	SQL*NET for Oracle
SunRPC	TCP/UDP	Sun Remote Procedure Call
TFTP	UDP	Trivial File Transfer Protocol
VDOLive	TCP/UDP	VDOLive streaming video

4. Non- TCP & Non-UDP protocols

Non-UDP or Non-TCP Protocol	Type	Well-Known Port Number	Description
EGP	IP	8	Exterior Gateway Protocol
GRE	IP	47	Generic Routing Encapsulation
ICMP	IP	1	Internet Control Message Protocol
IPINIP	IP	4	IP in IP
IPsec	IP	50, 51	IP Encapsulating Security Payload/Authentication Header
EIGRP	IP	88	Enhanced Interior Gateway Routing Protocol

5. TCP & UDP static port protocols

TCP or UDP Static Port Protocol	Type	Well-Known Port Number	Description
BGP	TCP/UDP	179	Border Gateway Protocol
CU-SeeMe	TCP/UDP	7648, 7649	Desktop videoconferencing
CU-SeeMe	UDP	24032	Desktop videoconferencing
DHCP/Bootp	UDP	67, 68	Dynamic Host Configuration Protocol/Bootstrap Protocol
DNS	TCP/UDP	53	Domain Name System
Finger	TCP	79	Finger User Information Protocol
Gopher	TCP/UDP	70	Internet Gopher Protocol
HTTP	TCP	80	Hypertext Transfer Protocol
HTTPS	TCP	443	Secured HTTP
IMAP	TCP/UDP	143, 220	Internet Message Access Protocol
IRC	TCP/UDP	194	Internet Relay Chat
Kerberos	TCP/UDP	88, 749	The Kerberos Network Authentication Service
L2TP	UDP	1701	L2F/L2TP Tunnel
LDAP	TCP/UDP	389	Lightweight Directory Access Protocol
MS-SQLServer	TCP	1433	Microsoft SQL Servertop videoconferencing
NetBIOS	TCP	137, 139	NetBIOS over IP (Microsoft Windows)
NetBIOS	UDP	137, 138	NetBIOS over IP (Microsoft Windows)
NFS	TCP/UDP	2049	Network File System
NNTP	TCP/UDP	119	Network News Transfer Protocol
Notes	TCP/UDP	1352	Lotus Notes
NTP	TCP/UDP	123	Network Time Protocol
PCAnywhere	TCP	5631, 65301	Symantec PCAnywhere
PCAnywhere	UDP	22, 5632	Symantec PCAnywhere
POP3	TCP/UDP	110	Post Office Protocol
PPTP	TCP	1723	Point to Point Tunneling Protocol

TCP or UDP Static Port Protocol	Type	Well-Known Port Number	Description
RIP	UDP	520	Routing Information Protocol
RSVP	UDP	1698,1699	Resource Reservation Protocol
SFTP	TCP	990	Secure FTP
SHTTP	TCP	443	Secure HTTP
SIMAP	TCP/UDP	585, 993	Secure IMAP
SIRC	TCP/UDP	994	Secure IRC
SLDAP	TCP/UDP	636	Secure LDAP
SNNTP	TCP/UDP	563	Secure NNTP
SMTP	TCP	25	Simple Mail Transfer Protocol
SNMP	TCP/UDP	161, 162	Simple Network Management Protocol
SOCKS	TCP	1080	Firewall security protocol
SPOP3	TCP/UDP	995	Secure POP3
SSH	TCP	22	Secured Shell
STELNET	TCP	992	Secure TELNET
Syslog	UDP	514	System Logging Utility
Telnet	TCP	23	Telnet Protocol
X Windows	TCP	6000-6003	X11, X Windows

For more information click here

NBAR supported platforms & IOS Versions

Platforms & Cisco IOS Versions that currently support **CISCO-NBAR-PROTOCOL-DISCOVERY-MIB** are

- Cisco 1700 Series Router since Release 12.2(2)T
- Cisco 2600, 3600, 7100, 7200 Series Routers since Release 12.1(5)T
- Cisco 3700 and 7500 Series Routers since Release 12.2(8)T

The following Platforms also support NBAR:

- Cisco 800 Series Routers
- Cisco 1800 Series Integrated Services Routers
- Cisco 2600XM Series Router
- Cisco 2800 Series Integrated Services Routers
- Cisco 3700 Series Multiservice Access Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 7300 Series Routers
- Cisco 7400 Series Routers
- Catalyst 6500 Family Switch with a FlexWAN card.

To know the supported IOS versions check here

Admin Operations

NetFlow Analyzer lets you perform many administrative tasks typical of an enterprise network administrator, such as managing a group of routers, handling different users, setting up alerts, etc.

Explore the following sections to know more about the administrative options available in NetFlow Analyzer.

Setting	Description
Alert Profiles Management	Click this link to add new alert profiles or modify existing ones
Scheduler Configuration	Allows setting of time intervals at which network traffic reports are generated automatically and mailed to desired recipient(s)
Device Group Management	Click this link to set up device groups based on devices exporting NetFlow data to NetFlow Analyzer
IP Group Management	Click this link to create IP groups that let you view traffic details for a selected group of devices, applications, or interfaces
User Management	Click this link to create different users for logging in to NetFlow Analyzer and assign access privileges to each user
Application Mapping	Click this link to configure applications based on port-protocol combinations
Settings	Click this link to change default server settings for NetFlow Analyzer and also set up the mail server for sending e-mail notifications
License Management	Click this link to manage the list of devices exporting NetFlow data to NetFlow Analyzer based on the current license applied
Change Password	Click this link to change your own password for logging in to NetFlow Analyzer

Alert Profiles Management

An alert profile is created to set the thresholds for generating alerts. The parameters to be set for creating an alert profile are;

- **Interfaces** - The list of interfaces who's bandwidth utilization must be watched
- **Traffic pattern** - The traffic to be watched - In Traffic, Out Traffic or a Combination of both
- **Application / Port(s)** - You can watch the traffic through all the applications or from a particular application. Similarly, through a single port or a range of ports
- **Threshold Settings** - It has 3 settings namely % utilization, no. of times, and duration.
    - **% Utilization** - When the utilization exceeds this limit, it is noted
    - **No. of time** - The number of times the utilization can be allowed to exceed the threshold before an alert is raised
    - **Duration** - The time period within which, if the threshold is exceeded, the specified number of times an alert is created.

Netflow Analyzer calculates the bandwidth utilization of the specified interfaces every minute. If the utilization exceeds the threshold value, the time when it exceeded is noted. Subsequently when it exceeds, the corresponding times are noted. If the number of times the utilization exceeds the specified limit, in the specified time duration, an alert is generated. When an alert is generated, you can also send an email to one / more people or send an SNMP trap to a manager application.

The **Alert Profile Management** option lets you create new alert profiles and manage existing ones (Modify or Delete). The Alert Profiles page lists all existing alert profiles, along with the number of alerts generated for each profile.

The various columns displayed in the Alert Profiles page are described in the table below:

Column	Description
Name	The name of the alert profile when it was created. Click on the alert profile's name to see more information about the alert profile.
Description	Descriptive information entered for this alert profile to help other operators understand why it was created.
Enabled/Disabled	By default all alert profiles are Enabled, which means they are active. Click the icon to disable an alert profile. When this is done, alerts will no longer be generated for that alert profile. Click the icon to enable the alert again.
Last Hour Alerts	Lists the number of alerts generated for this alert profile in the last one hour. Colors are used to represent the number of alerts generated with each severity level. Red - Critical, Orange - Major, Yellow - Warning, and White - All. Click on each color to see the list of alerts generated with that severity.
All Alerts	Lists the total number of alerts generated for this alert profile. Colors are used to represent the number of alerts generated with each severity level. Red - Critical, Orange - Major, Yellow - Warning, and White - All. Click on each color to see the list of alerts generated with that severity.
Clear	Click the icon to clear all alerts generated for this alert profile

Alerts List

The Alerts List is displayed when you click on any color against an alert profile in the Alert Profiles page, or from any link in the **Generated Alerts** box on the left pane. The list shows the alerts that were generated with the respective severity, along with the device that generated the alert, the time the alert was generated, and an option to view more details about the alert.

Click the **Details** link in the View column against an alert to view detailed information about the alert. The pop-up that opens up, shows the traffic graph outlining traffic values ten minutes before and after the alert was generated, along with details on top applications, sources, destinations, and conversations recorded during that time interval.

Operations on Alert Profiles

You can create new alert profiles, modify, or delete existing ones from the Alert Profiles page.

Creating a new Alert Profile

Remember to set the `active timeout` value on the router to **1 minute** so that alerts are generated correctly. Refer the Cisco commands section for more information on router settings.

The steps to create an Alert Profile are;

1. Login to the NetFlow Analyzer client and click "**Alert Profile Management**" under "**Admin Operations**" in the left panel
2. Click "**Add**" to add a new Alert Profile
3. Fill in the following details

Field	Description
Alert Profile Name	Enter a unique name to identify this alert profile
Description	Enter descriptive information for this alert profile to help other operators understand why it was created.
Select Source	By default all interfaces sending NetFlow exports are selected. If you want this alert profile to apply to certain interfaces only, click the **Modify Selection** link. In the pop-up window, select the required devices and interfaces and click **Update** to save your changes.
Define Alert Criteria	Select whether alerts need to be generated based on incoming traffic, outgoing traffic, or both. The default setting is for both.
	Then select the application / port for which the alert has to be generated. This criteria can be very general - Any application traffic can be profiled - or it can be highly specific - Generate the alert only when a specific application, protocol, and/or port is used.
Define Threshold and Action	Enter the threshold conditions (threshold utilization, no. of times it can exceed and the time duration) exceeding which the alert will be generated. You can also specify an action to be taken during the alert creation. - Email - to send a notification to one or more people. - SNMP Trap - to send a trap to the manager application (specify the <server name>:<port>:<community>). For details on configuring trap forwarding, refer to SNMP Trap Forwarding section under Appendix To add more threshold values, click 'Add Row' and add values

4. **Customizing from address**:
5. You can customize the "From Address" from the mail server settings in Settings page.
6. After setting the required thresholds, click '**Save**'

The new alert profile is created and activated. The system watches the utilization and raises alarms when the specified conditions are met.

	Only one alert is generated for a specified time duration. For example, say for a particular interface, the threshold is set as 60% and number of times is set as 3 times and the time duration is set as 30 minutes. Now lets assume that the utilization in that interface goes above 60% and stays above it. Then in 3 minutes, the above conditions will be met and an alert will be generated. The next alert will NOT be generated after 6 minutes, but only in the 33rd minute, if the condition persists. Thus for the specified 30 minutes time duration, only one alarm is generated. This is designed to avoid a lot of repetitive mail traffic.

Modifying or Deleting Alert Profiles

Select an alert profile, and click on **Modify** to modify its settings. You can change all of the alert profile's settings except the profile name. There is also an option to clear all existing alerts for this profile from this page itself. Once you are done, click **Save** to save your changes.

Select an alert profile, and click on **Delete** to delete the profile. Once an alert profile is deleted, all alerts associated with that profile are automatically cleared.

Schedule Reports


It is a good idea to schedule reports to be run at non-peak traffic hours since generation of reports is a resource hungry process especially for large interface numbers.

A Scheduler is configured to set the parameters for automating the generation of reports. The parameters to be set for creating a Scheduler are:

- **Source -** The Interfaces or IP Groups which are the source of traffic.
  - **Interfaces** - The list of interfaces who's bandwidth utilization must be watched. One report will be generated for each interface selected.
  - **IP Groups** - The IP groups who's bandwidth utilization must be watched. One report will be generated for each IP Group created.
- **Report Type** - The type of report to be generated - Consolidated or Custom
- **Report Generation Schedule** - How and when the report is to be generated (e.g.) daily,weekly,monthly,or only once
  - **Generate report on** - This value determines the time when report is to the generated
  - **Generate report for** - This value determines the start and the end time for the report
- **Email Address** - This is the address to which the generated reports will be sent

Netflow Analyzer calculates the bandwidth utilization on the specified interfaces / IP Groups every minute. Based on the schedule opted for, reports are generated at various time intrevals.The **Schedule Reports** feature lets you Create new Schedules and Delete existing ones. The Scheduler List page lists all existing schedules , along with the Schedule details,Status, Report types,and the Last Report Generated time.

The various columns displayed in the Scheduler List page are described in the table below:

Column	Description
Name	The name of the Schedule when it was created. Click on the Schedule's name to see more information about the schedule's configuration.
Schedule Details	Information on when the schedule will run.
Status	By default all schedules are Enabled, which means they are active. Click the icon to disable a schedule. When this is done, reports will no longer be generated for that configuration. Click the icon to enable the schedule again.
Report Type	Whether it is a consolidated report are user-defined Custom report
Last Report Time	This column lists the last time when this schedule was run and a report created.

Operations on Schedule Reports

You can create new schedules or delete existing ones from the Schedule List page.

Configuring a new Schedule

The steps to configure a Schedule are:

1. Login to the NetFlow Analyzer client and click "**Schedule Reports"** under "**Admin Operations**" in the left panel

2. Click "**Add**" to add a new Schedule Profile
3. Fill in the following details

Field	Description
Scheduler Name	Enter a unique name to identify this scheduler.
Description	Enter descriptive information for this scheduler profile to help other operators understand why it was created.
Select Source	By default all managed interfaces sending NetFlow exports are selected. If you want this schedule configuration to apply to certain interfaces only, click the **Modify Selection** link. In the pop-up window, select the required devices and interfaces and click **Update** to save your changes.
	By default all IP Groups are selected. If you want this schedule configuration to apply to certain IP Groups only, click the **Modify Selection** link. In the pop-up window, select the required devices and IP Groups and click **Update** to save your changes.
Report Type	Select whether the reports that need to be generated is consolidated or a customised one .The default setting is Consolidated Report.To opt for Custom Report click on the radio button in front of custom report.
	If you want a customised report then click on the radio button in front of custom report. Opting for Custom report lets you set criteria by using the "Add Criteria" option.Any number of criterion can be set and the rule set to match all the criteria or anyone.
Schedule Report Generation	Select the report generation frequency as one from : Daily, Weekly, Monthly and Only Once. Depending on this the report will be generated at the appropriate time intrevals.
Email Address to Send Reports	Enter the email address to which the generated reports have to be emailed. You can enter multiple email addresses separated by a comma.

4. After setting the required parameters, click '**Save**'

Custom Report :

Opting for custom report lets you set criteria on the basis of which the report will be generated. By clicking on the "**Add Criteria**" button one can set a matching condition on "Source Address, Source Network, Source Nodes, Destination Address, Destination Network, Destination Nodes and Application". To add more criteria click on "**Add Criteria**" again. Having created all the criterions you can decide whether to make the generated report to match all of the criterions created or any of them.

Scheduling Report Generation
The report generation schedule can be chosen from one of the following:

- **Daily** - When you opt for "Daily" you have the option to set the time at which the report should be generated. Also, the report could be generated for the previous day or the last 24 hours. When the "Previous Day" option is opted the report is generated for the time period from 00:00 hours to 23:59 hours of the previous day. You have the option to narrow down this time period by using the time filter -  . For instance if the maximum flow happens during your working hours from 08:00 hours to 18:00 hours you can set it in the window that pops up.

When you opt for the last 24 hours then the report is generated for the flow in the intervening 24 hours (from the time at which the report is to be generated today).

Exclude weekends:

When you choose the Exclude Weekend option with "Previous day", reports will be generated on Tuesday, Wednesday, Thursday, Friday and Saturday. These will be reports pertaining to Monday, Tuesday, Wednesday, Thursday and Friday respectively.

When you choose the Exclude Weekend option with "Last 24 hours", reports will be generated on Monday, Tuesday, Wednesday, Thursday and Friday.

- **Weekly** - When you opt for the "Weekly" option, you have the option to specify the day and time at which the report needs to be generated. The report could be generated for the "Previous Week" or for the "Last 7 Days". By additionally opting for the "Exclude Weekend" the report can be made to include only data corresponding to monday through friday.

  The previous week option would generate the report for the time period Sunday 00:00 hours till Saturday 23:59 hours. When"Exclude Weekends" is enabled the report will be generated for the time period Monday 00:00 hours till Friday 23:59 hours.

  The"Last 7 Days" option would generate the report for the last 7 days from the time at which the report is to be generated. Again, the exclude weekend option would generate for the last 7 days with the data for the weekend (saturday,sunday) excluded. For instance if the report is to be generated at Monday 10:00 am, with the rules set as "last 7 days" and "Exclude weekend" enabled, then the report will be generated for the time period last week's Monday 10:00 hours to Friday 23:59 hours and from this week Monday's 00:00 hours till 10:00 hours.

- **Monthly** - By opting for the "Monthly" option you can set the date of the month along with the time at which the report needs to be generated every month .The report could be generated for the "Previous Month" or for the "Last 30 days". By selecting "Exclude Weekends" the report can be made to include only data corresponding to monday through friday.

  When "Previous Month" option is enabled and the report generation date is set to 5-th of every month at 10:00 hours, then the report will be generated for the whole of last month (first to the last day of the month). When "Exclude weekend" option is enabled then the generated report will exclude all the intervening weekends (saturday & sunday).

  When "Last 30 Days" option is enabled and the report generation date is set to 5-th of every month at 10:00 hours, then the report will be generated from last month's 5-th 10:00 hours till this month 5-th's 10:00 hours. When"Exclude Weekend" option is enabled then the generated report will exclude all the intervening weekends(saturday & sunday).

- **Only Once** - If you wish to generate report only once at a specified time you can do that by opting for "Only Once". The date and time at which the report should be run can be specified. The date & time can be altered by using the icon -  . The report could be generated for the Previous Day, Last 24 Hours, Previous Week, Last 7 Days, Previous Month, or Last 30 Days. When "Previous Day" option is enabled then the  button permits the setting of working hours.

Customizing from address:

You can customize the "From Address" from the mail serever settings in settings.

A note on emailed reports:

A report is generated for each interface / IP Group - 50 such reports are zipped in a single email and mailed. In case of more than 50 interface/ IP Groups selected the report will be sent in multiple emails. The last generated reports for all schedules will be under the folder NetFlow -> Reports.

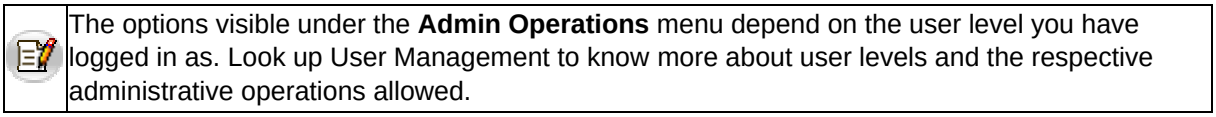
Deleting Schedules

Select a schedule from the Schedule List and click on **Delete** to delete the schedule. Once a schedule is deleted no longer reports are generated at the stipulated intrevals. Deleting a schedule also deletes the corresponding folder.

Device Group Management

NetFlow Analyzer lets you create device groups, which consist of a set of routers. A device group can contain any number of routers, and a router can belong to any number of device groups.

The **Device Group Management** option lets you create, manage, and delete device groups. Initially, when no device groups have been created, you will see a message that lets you start creating device groups.



Creating a Device Group

Follow the steps below to create a new device group:

1. Click the **Add** button to create a new device group
2. Enter a unique name to identify the device group. The same name is displayed in the Device Group menu on the left, and will be listed under Available device groups when managing a user.
3. Use the **Device Group Description** box to enter useful information about the device group
4. Select the routers needed for this device group from the list of available routers displayed

Once all values have been entered, click the **Update** button to create this device group and begin generating traffic reports for the same.

Interface Group:

Interface Group allows you to combine interfaces in order to monitor traffic. This can be useful for grouping multiple sub-interfaces into a single logical entity.Follow the steps below to create a new interface group:

1. Click the **Interface Group** tab at the top right of the Device Group Management page.
2. Enter a name to identify the interface group in the **Interface Group Name** box .
3. Use the **Interface group speed** box to enter the speed limit for the interface group
4. Select the routers needed and the interfaces under them for this interface group. By selecting a router ,by default, all interfaces are selected. You can selectively unselect the unwanted interfaces from the list.
5. Click on **Update** to save the changes.

The Interface group that is created is listed in the Dashboard view in the "Interface View" tab.The Interface group name, the In-Traffic & Out-Traffic for the last 1 hour can be seen in it.By clicking on the interface group name it is possible to further drill down to view further details.

Managing a Device Group

Select an existing device group and click the **Modify** button to modify its properties. You can change all properties of the device group except its name. Once you have made changes to the properties of this device group, click the **Update** button to save your changes.

Select an existing device group and click the **Copy** button to copy its settings. This is useful when you need to create a new device group that includes the same routers as that of this device group. This saves you the trouble of adding the routers all over again. Then follow the same steps as those in creating a new device group.

Select a device group and click the **Delete** button to delete the device group. When a device group is deleted, it is removed from the Device Group List and the Device Group menu. All users assigned to this device group will not see this device group on their Dashboard.

IP Group Management

The IP groups feature lets you monitor departmental, intranet or application traffic exclusively. You can create IP groups based on IP addresses and/or a combination of port and protocol. You can even choose to monitor traffic from specific interfaces across different routers. After creating an IP group, you can view the top applications, top protocols, top hosts, and top conversations in this IP group alone.

This section will help you understand IP Groups and walk you through the steps needed to create and later delete an IP group if needed.

- Understanding IP Groups
- Defining an IP Group
- Operations on IP Groups

Understanding IP Groups

To further understand how the IP grouping feature can help in understanding exclusive bandwidth usage, consider the following two scenarios:

Enterprise Network Scenario

A typical enterprise setup where the main servers and databases are located at a central office, and all branch offices are given appropriate access privileges to these servers.

> **Problem:** You need to track bandwidth used by each branch office while accessing an ERP/CRM application
> **Solution:** Create an IP group for each branch office, along with the port and protocol of the ERP/CRM application running in the central office.
>
> The traffic reports for each IP group will then show details on bandwidth used by the branch office while working with the ERP/CRM application. This information is very useful during traffic accounting and usage-based billing.
>
> **End Note:** If the IP addresses in the branch offices are NATed (network address translated) by the web server, you can view overall bandwidth usage for the branch office, but not that of individual hosts within the IP group.

Campus Network Scenario

A typical campus network with several departments. Here IP addresses are usually not NATed by the web server.

> **Problem:** You need to analyze bandwidth used by each department
> **Solution:** Create an IP group for each department (IP address or address ranges), without specifying any port/protocol values.
>
> The traffic reports for each IP group will then show bandwidth usage by that department along with information on top talkers, and top conversations within that department.

Defining IP Groups

IP groups can be defined based on IP address and/or port-protocol combinations. In addition, you can filter IP group traffic based on interfaces. The following matrix shows the different combinations possible, along with a typical example usage for each combination.

Combination	IP Address	Port/Protocol	Interfaces
IP Address	View bandwidth details for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic details for a range of IP addresses.	View bandwidth details across multiple interfaces, for a range of IP addresses.
Port/Protocol	View Web (80/TCP, 80/UDP) traffic details for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic generated across the network	View Web (80/TCP, 80/UDP) traffic generated across multiple interfaces.
Interfaces	View bandwidth details across multiple interfaces, for a range of IP addresses.	View Web (80/TCP, 80/UDP) traffic generated across multiple interfaces.	[Not possible]

Creating an IP Group

The **IP Group Management** link in the **Admin Operations** box lets you create, modify, and delete IP groups. Click this link, and then click **Create** to create a new IP group. Fill in the following information and click **Add** to add the new IP group to the current list of IP groups.

Field	Description
IP Group Name	Enter a unique name to identify this IP group
IP Group Description	Enter descriptive information for this IP group to help other operators understand why it was created.
IP Group Based on	Select whether you want to define this IP group based on IP address or port-protocol combination. If you want to define the IP group based on both IP address and port-protocol, select both options.
Specify IP/IP Range/Network	Select the IP address, address range, or network that this IP group is based on. Use the **Add Row** and **Remove Row** buttons to specify additional IP address options.
Filter based on Port/Protocol	*(This option is shown if you have selected the **Port/Protocol** option in step 3)* Enter the port numbers or port range in the **Port Number** field. Select the protocol in the **Protocol** field. Use the **Add Row** and **Remove Row** buttons to specify additional port-protocol options. *See Note below.
Select Interfaces	If you need to filter this IP group further, based on different interfaces, click this link and select the different devices and interfaces whose traffic needs to be included in this IP group.
IP Group Speed	Enter the interface speed (in bits per second) for calculating percentage of traffic for this IP group.

If you add a new combination of ports and protocol, a popup opens stating that this combination of ports and protocol has not been mapped to any application. Add the combination as a new application in the same popup, and click **Update** to update the Application Mapping list with the new application.

Managing IP Groups

Click the **IP Group Management** link in the **Admin Operations** box to view the list of IP groups currently active. Select the IP group that you want to modify, and click the **Modify** button to edit its settings. Once you are done, click **Add** to save and activate the new changes.

To delete an IP group, select the IP group and click the **Delete** button. Deleting an IP group removes the IP group from the list of IP groups managed. All users assigned to this IP group will not see this IP group listed on their Dashboard.

User Management

The **User Management** option lets you manage different users with varying access privileges. You can assign different users to different device groups and IP groups, and allow them to manage the assigned groups exclusively. You can choose from three types of users in NetFlow Analyzer - Administrator, Operator, and Guest. You can create any number of users of each type, and assign them to any number of device groups and IP groups.

The administrative privileges for each user are described below:

Privilege	Administrator	Operator	Guest
View all available devices and IP groups	✓	✗	✗
Create, modify, or delete device groups or IP groups	✓	✗	✗
Modify Runtime Administration properties	✓	✗	✗
Change other users' passwords	✓	✗	✗
Manage licensed interfaces	✓	✗	✗
Apply different licenses	✓	✗	✗
Create other Administrator users	✓	✗	✗
Create other Operator users	✓	✗	✗
Create other Guest users	✓	✓ *	✗
Add, modify, or delete Alerts	✓	✓	✗
Enabling and Disabling Alerts	✓	✓	✗
Add, modify, or delete applications	✓	✓	✗
Change device settings	✓	✓	✗
View traffic reports	✓	✓	✓
View custom reports	✓	✓	✓
Assigned to one or more device groups or IP groups	✗	✓	✓
Scheduling of Reports	✓	✗	✗
NBAR Configuration	✓	✗	✗
Viewing NBAR Reports	✓	✓	✓

- only within the assigned group
-

Adding a New User

On the User Management page, click the **Add** button to add a new user. Fill in the following fields and click the **Add User** button to create this user.

Field	Description
User Name	Enter the unique user name for the user. This name will be used to log in to the NetFlow Analyzer web client.
Password, Retype Password	Enter a password for this user. The password should be at least 6 characters long, and all characters are allowed.
Access Level	Select the Access Level for the user. Remember that access levels will be available depending on your own access permissions. For example, if you have logged in as an Administrator, all three access levels will be available in the Access Level options box.
Available Groups	Select the device groups to assign to this user and move them to the Selected Groups.
Available IP Groups	Select the IP groups to assign to this user and move them to the Selected IP Groups.

Click on the user name at any time on the **User Management** page to view the corresponding user name, access level, and assigned device groups and IP groups.

Changing User Passwords

Only an Administrator user can reset the password of any other user. To assign a new password to a user, click on the  icon or the **Assign New** link.
Enter a new password, confirm it, and click the **Update** button for the new password to take effect.

	If you have logged in as an Admin user, you can change your own password in the same way as described above. If you have logged in as an Operator user or a Guest user you can change your password by selecting the Change Password option in the **Admin Operations** menu.

Editing User Details

Click on the  icon against a user, to edit the user's details.

	You can only modify the device groups and IP groups which have been assigned to the user. You **cannot** modify the user name or the access level, irrespective of your own access level.

Once you are done, click the **Update** button to save your changes.

Deleting a User

Click the  icon against a user name to delete the respective user. Once a user is deleted, all details of this user are permanently deleted.

Application Mapping

The **Application Mapping** option lets you configure the applications identified by NetFlow Analyzer. You can add new applications, modify existing ones, or delete them. Please see the Additional Notes on Application Mapping section to understand this feature more clearly. Also it is possible to associate an IP address with an application.

Adding an Application

Follow the steps below to add a new application:

1. Click the **Add** button to add a new application
2. Enter the port number of the new application. To enter a port range, separate the start and end points of the range with a hyphen. (eg.) 1400-1700
3. Choose the protocol from the list of protocols
4. Choose one of the options from IP Address / IP Network / IP Range. Depending on what you opt a set of fields are enabled and should be filled.
    - If you opt for **IP Address** then you have to enter the address in the IP Address box.
    - If you opt for **IP Network** then you have to enter the IP Network and IP Netmask details.
    - If you opt for **IP Range** then you have to enter the Start IP, End IP and IP NetmaskEnter a unique name for the application
5. The Application Name has to be entered finally by which the IP address is associated with an application.

Ensure that the combination of port number and protocol is unique. If not, the older application mapping will be deleted.

Once you are done, click the **Update** button to save your changes.

Modifying an Application

Select an application and click the **Modify** button to modify its properties.

You can only change the name of the application. If you need to change the port or the protocol, you have to delete the application, and add it as a new application.

Once you are done, click the **Update** button to save your changes.

Deleting an Application

Select an application and click the **Delete** button to delete it. The application is permanently deleted, the corresponding port is freed, and can be assigned to another application.

Additional Notes on Application Mapping

Applications are categorised based on the source address, destination address, source port, destination port and protocol values in the flow record.These values are matched with the list of applications in the Application Mapping.

The check is done first with the smaller of the 2 ports (source port / destination port), and if no match is found the bigger of the 2 ports is mapped

Application mappings created with specific IP address / IP Range / IP Network is given higher priority over applications mappings with no IP address. For example assume you have 2 application mappings as below:

Port	Protocol	IP Address / IP Range	Application
80	TCP	10.10.1.0(255.255.255.0)	APP1
80	TCP	Any	APP2

If a flow is received with source address 10.10.10.10 and Port as TCP-80 then it is classified as APP1. Only TCP-80 flows from non-10.10.10.0 network will be classified as APP2.

Application mappings created with single port is given higher priority over applications mappings with port range. For example assume you have application mappings as below:

Port	Protocol	IP Address / IP Range	Application
80	TCP	any	APP1
70 - to - 90	TCP	any	APP2

If a flow is received with Port as TCP-80 then it is classified as APP1.

Applications are categorised based on the source address, destination address, source port, destination port and protocol values in the flow record.

The smaller of the 2 ports (source port / destination port) and protocol is matched with the port-protocol in the application mapping list

If no match is found, the bigger of the 2 ports (source port / destination port) and protocol is matched with the port-protocol in the application mapping list.

If no match is found, the smaller of the 2 ports (source port / destination port) and protocol is matched with the port range-protocol in the application mapping list.

If no match is found, the bigger of the 2 ports (source port / destination port) and protocol is matched with the port range-protocol in the application mapping list.

If no match is found, the application is categorized as protocol_App (as in TCP_App or UDP_App)

In case the protocol is not available in the application mapping list, the application is categorized as Unknown_App

The sequence in which the mappings are checked is as follows:

1. Application mapping with specific IP address / IP Range / IP Network is matched.
2. Application mapping with no IP address and single port number / port range.

Settings

The Settings option includes several server configuration settings that you can configure from the user interface.

NetFlow Analyzer Settings

Option	Default Value	Requires server restart	Description
Default SNMP Community	public	no	The SNMP community string used to query devices sending NetFlow exports
Default SNMP write community	-	no	The SNMP write community is used to enable / disable NBAR on the interfaces from the User Interface. If you have provided the SNMP write community during installation the field is prepopulated with the content
Default SNMP Port	161	no	The SNMP port used to query devices sending NetFlow exports
NetFlow Listener Port	9996	yes	The port on which NetFlow Analyzer listens for NetFlow exports. You need to configure devices to send NetFlow exports to this port. In case you are exporting NetFlow from multiple routers, please configure multiple listener ports. You can specify upto 5 listener ports, each seperated by a comma. You will need to restart the NetFlow Analyzer server when you change the listener port.
Webserver Listener Port	8080	yes	The port used to access NetFlow Analyzer from a web browser.
Record Count	50	no	The default record count is 50 but the maximum number of records that can be kept in the database for all traffic data is 100. This is also the maximum value that can be selected from the **Show** box in all traffic reports.
Retain raw data for	1 day	no	The default period for which raw data is retained. Troubleshooting and Alert Details graphs are populated from raw data. Hence a higher value here, means more visibility in both these graphs.The maximum period for which you can store raw data is 1 month.(earlier it was 2 weeks).

Raw Data Settings

NetFlow Analyzer classifies data into 2 types namely Aggregated Data and the Raw Data.

Aggregated Data represents the total IN and OUT traffic, the top 100 application and the top 100 conversation for each interface for every 10 minute intervals. Data is progressively stored in 10 minute, 1 hour, 6 hour, 24 hour and weekly data points for older data - the most recent data is available with 10 minute granularity and data older than 90 days is available in weekly granularity.

This mechanism of storing the top 100 is done to ensure that the database does not grow infinitely. The amount of hard disk space required to store the aggregated data forever is about 150 MB per interface.

In addition to the aggregated data, NetFlow Analyzer 5 allows you to store all raw netflow data for upto 1 month. The time period for which you can store this raw data (Raw Data Period) depends on the number of flows received by NetFlow Analyzer and the amount of free disk space available on your computer. Each flow is about 60 bytes. Troubleshooting and Alert reports are generated from Raw data since it provides high level of granularity.

NetFlow Analyzer indicates the flows received per second in the Raw Data Settings tab on the Settings link. You should set the raw data period based on the calculation below:

$$\text{Raw Data Period (in hours)} = \frac{\text{Free hard disk space - (150 MB * No. of Managed Interfaces)}}{\text{60 Bytes * 3600 seconds * Flows Per Second}}$$

You can use the recommendation provided by the software to set you Raw data storage period. The maximum raw data storage period is 1 month(earlier it was 2 weeks).

Mail Server Settings

These settings are important when e-mail notifications have to be sent for alerts generated.

Option	Default Value	Description
Outgoing SMTP Server	smtp	The name of the outgoing SMTP server used to send e-mails
Port	25	The port number on the outgoing server that is used to send e-mails
Default e-mail ID	(optional)	The default e-mail address to which e-mail notifications have to be sent. Separate multiple e-mail addresses by a comma (,). If mail id is not provided, then a mail is received with the From address as **netflowreport@localdomain.com**
Requires authentication	unchecked	Select this checkbox if the mail server needs authentication
User Name	(optional)	The authentication user name for the mail server
Password	(optional)	The corresponding password for mail server authentication

NBAR Data Storage Settings

This parameter lets your decide how long you want NBAR data to be stored. The maximum period is 2 months

License Management

The **License Management** option lets you manage the interfaces exporting NetFlow data to NetFlow Analyzer, depending on the license that you have purchased.

The options visible under the **Admin Operations** menu depend on the user level you have logged in as. Look up User Management to know more about user levels and the respective admin operations allowed.

The status box at the top of the page indicates the type of license currently applied, the total number of interfaces currently managed, and the number of days remaining for the license to expire.

Look up Licensing to know more about upgrading your license.

The Router List shows all the routers and interfaces from which NetFlow exports are received, and whether they are managed or not.

Managing a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Once you have selected the required interfaces, click the **Manage** button to manage these interfaces. This means that flows received from these interfaces will be processed by NetFlow Analyzer, and traffic graphs and reports can be generated.

The maximum number of interfaces that can be managed, depends on the current license applied.

Unmanaging a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Click the **Unmanage** button to unmanage these interfaces. This means that flows received from these interfaces will be dropped by NetFlow Analyzer. Once unmanaged, these interfaces will not be seen on the Dashboard or be listed in device groups. However they will still be listed in the Router List in the License Management page.

Deleting a router/interface

To select the router and all its interfaces check the checkbox next to the router name. To select a specific interface, check the checkbox next to the interface name.

Click the **Delete** button to delete these interfaces. This means that these interfaces are completely removed from all screens of the NetFlow Analyzer client.

However, if flows are still being sent from these interfaces to NetFlow Analyzer, they will reappear in the Dashboard. To prevent this, you need to disable NetFlow export from those interfaces.

Licensing New Interfaces

If a NetFlow packet is received from a new interface, and the number of interfaces presently managed is less than that allowed in the current license, this interface is listed under Router List on the Dashboard with a message saying new flows have been received. You need to then click the **License Management** option and change this interface's status to Managed in order to include this interface in

the list of managed interfaces, and also generate traffic graphs and reports for the same.
If a NetFlow packet is received from a new interface, and the number of interfaces presently managed is equal to that allowed in the current license, you need to either unmanage any other managed interfaces, and then manage this interface, or leave this interface in **New** status. In any case graphs and reports can be generated only for managed interfaces.

At any time you can buy more licenses by clicking on the **Buy Online** image.

Change Password

The **Change Password** option lets you change your own password for logging in to NetFlow Analyzer. This is available as a separate option in the Admin Operations menu, for users logged in as Operator or Guest. For Admin users, the password can be changed from the User Management page itself.

Enter the new password, confirm it, and click the **Update** button to save your changes.

Enter the new password when you log in again into NetFlow Analyzer. Your present session will not be terminated until you explicitly log out or your session expires.

Contacting Technical Support

Click the **Support** link on the top-left corner of the NetFlow Analyzer client screen, to see a wide range of options to contact the NetFlow Analyzer Technical Support team in case of any problems.

Option	Description
Request Technical Support	Click this link to submit a form from the NetFlow Analyzer website, with a detailed description of the problem that you encountered
Create Support Information File	Click this link to create a ZIP file containing all the server logs that the Technical Support team will need to analyze your problem. You can then send this ZIP file to support@netflowanalyzer.com or upload it to our server via FTP.
Troubleshooting Tips	Click this link to see troubleshooting tips for common problems encountered by users.
User Forums	Click this link to go to the NetFlow Analyzer user forum. Here you can discuss with other NetFlow Analyzer users and understand how NetFlow Analyzer is being used across different environments
Need a Feature	Click this link to submit a feature request from the NetFlow Analyzer website
Toll-free Number	Call the toll-free number **+1 888 720 9500** to talk to the NetFlow Analyzer Technical Support team directly

Frequently Asked Questions

For the latest list of Frequently Asked Questions on NetFlow Analyzer, visit the FAQ on the website or the public user forums.

Installation

1. When I try to access the web interface, another web server comes up. How does this happen?
2. How can I change the MySQL port in NetFlow Analyzer from 13310 to another port?
3. Can I install and run NetFlow Analyzer as a root user?
4. Is a database backup necessary, or does NetFlow Analyzer take care of this?
5. How do I update patch in Linux ?

Router Configuration

1. Why can't I add a router to NetFlow Analyzer?
2. My router has been set up to export NetFlow data, but I still don't see it on the Dashboard.
3. I've deleted a router and all its interfaces through the License Management page but it still comes up on the Dashboard.
4. What's the difference between unmanaging and deleting an interface?
5. How to Configure SNMP community in router?
6. How do I set the router time in SYNC with the NFA server?

Reporting

1. The graphs are empty
2. What is Aggregate data and Raw data ? How to set Raw data ?
3. Some of the applications are labeled as "TCP_App" or something similar. What is that?
4. Why are only the top 5 or 10 values shown in the reports? What if I want more detail?
5. The graphs show only IN traffic for an interface, although there is both IN and OUT traffic flowing through that interface. Why's that?
6. Why are some interfaces labeled as IfIndex2,IfIndex3, etc.?
7. The total bandwidth usage seems to decrease depending on the length of the report.Why is that?

NBAR

1. Which features are not supported by NBAR?
2. Any restrictions on where we can configure NBAR?
3. What Does NBAR Performance Depend On?
4. Is performance dependent on the number of interfaces that NBAR is enabled on? Does the link speed of the interface(s) that NBAR is enabled?
5. I am able to issue the command "ip nbar protocol-discovery" on the router and see the results. But NFA says my router does not support NBAR, Why?
6. How do I verify whether my router supports CISCO-NBAR-PROTOCOL-DISCOVERY-MIB?

V9

1. What is NetFlow Version 9?
2. What is the memory impact on the router?
3. "Receiving non V5/V7/V9 packets from the following devices: Click here for further details.." What does this mean?

4. Is version 9 backward compatible ?
5. What is the performance impact of V9?
6. What are the restrictions for V9?
7. How do I configure NetFlow Version 9?

Technical Information

1. How is traffic information stored in the NetFlow Analyzer database?
2. How do I reset the admin password ?
3. How are ports assigned as applications in NetFlow Analyzer?
4. Do I have to reinstall NetFlow Analyzer when moving to the fully paid version?
5. How many users can access the application simultaneously?
6. NetFlow Analyzer logs out after a period of inactivity. How do I avoid that?
7. How to create DBInfo log file ?
8. Why the interface shows 100% utilization ?
9. What information do I need to send to NFA support for assistance?
10. How to safely migrate NFA installation to different machine ?
11. What do I do if my NFA server becomes slow ? (or) How do I improve my NFA system performance ?
12. Why NFA says router time not is SYNC and stops collecting data ?
13. How do I buy NetFlow Analyzer?

Installation

1. **When I try to access the web interface, another web server comes up. How does this happen?**

   During installation, NetFlow Analyzer checks if the selected port is in use by another application. If at that time, the other webserver was down, it will not get detected. Either disable the other web server, change its server port, or change the NetFlow Analyzer web server port.

2. **How can I change the MySQL port in NetFlow Analyzer from 13310 to another port?**

   Edit the mysql-ds.xml file in the /server/default/deploy directory. Change the port number in the line jdbc:mysql://localhost:13310/netflow to the desired port number, save the file, and restart the server.

3. **Can I install and run NetFlow Analyzer as a root user?**

   NetFlow Analyzer can be installed and started as a root user, but all file permissions will be modified and later you cannot start the server as any other user.

4. **Is a database backup necessary, or does NetFlow Analyzer take care of this?**(or)**How to back-up data in NetFlow Analyzer ?**

   NetFlow Analyzer includes a database backup utility that you can use to make a backup of the database.There are 2 ways of backup :

   1. You can execute the script "backupdb.bat" / "backupdb.sh" which can be found under /adventnet/me/netflow/troubleshooting. This will created a back up of the database in a zip format. When you want to restore. You have to extract the zip to the /adventnet/me/netflow directory. This is a slow process.

2. You can copy the folder /adventnet/me/netflow/mysql/data to a different location and to restore you can copy it back to the same location. This is a fast process.

In both the above process the version of NFA should be the same.

5. How do I update patch in Linux ?

Please use the command "sh UpdateManager.sh -c" and follow the instructions to upgrade NetFlow Analyzer.

Router Configuration

1. **Why can't I add a router to NetFlow Analyzer?**

   NetFlow Analyzer does not choose which routers or interfaces to monitor. Devices are auto-discovered. All you need to do is set up your interfaces to send NetFlow data to the specified port on NetFlow Analyzer. Once NetFlow Analyzer starts receiving NetFlow data, you can see the device and its interfaces listed on the Dashboard.

2. **My router has been set up to export NetFlow data, but I still don't see it on the Dashboard.**

   There are a number of things you can check here:
   - Check if NetFlow is enabled on the device, and that it has started sending flows.
   - Check if your router is exporting NetFlow data to the port on which NetFlow Analyzer is listening.
   - Check if the router is exporting NetFlow version 5 data. Flows with any other version will be discarded.

3. **I've deleted a router and all its interfaces through the License Management page but it still comes up on the Dashboard.**

   This happens because NetFlow packets are still being received from that router. Unless you configure the router itself to stop exporting NetFlow data to NetFlow Analyzer it will reappear on the Dashboard

4. **What's the difference between unmanaging and deleting an interface?** (or) **When do I unmanage a device and when do I delete it from the License Management page?**

   If you need to temporarily stop monitoring a router/interface, unmanage it from License Management. In this case, the router/interface is still shown under License Management.

   If you need to permanently stop monitoring a router/interface, disable NetFlow exports from the interface/router and then delete it from License Management.In this case, the router/interface is not displayed on any of the client screens unless new flows are sent from it.

5. How to Configure SNMP community in router?

For configuring SNMP, follow the steps below

1. Logon on to the router.
2. Enter into the global configuration mode
3. Type the command snmp-server community public RO (to set public as Read-Only community)
4. Press ctrl and Z
5. Type the command write mem

6. **How do I set the router time in SYNC with the NFA server?**

   Whenever the time difference between the NetFlow Analyzer Server and the router is above 10 minutes a warning icon will appear in the home page. When this happens, NetFlow Analyzer will stamp the flows based on the system time of the NetFlow Analyzer server. In case you see this, please ensure the following on the router:

   1. Check if the time zone and the offset (in Hours and Minutes) for the time zone is set properly (E.g. PST -8 00 for PST or EST -5 00 for EST). You can check this by logging into the router, going into the configure terminal and typing show running-config. You can set the clock time zone and offset using the command clock timezone zone hours [minutes] (E.g. clock timezone PST -8 00)

   2. After checking the time zone, check if the correct time is set on your router. You can check this by logging into the router and typing show clock. You can set the clock time using the command clock set *hh:mm:ss* month date year There is no queueing mechanism is done on heavy periods.

Reporting

1. **The graphs are empty**

   Graphs will be empty if there is no data available. If you have just installed NetFlow Analyzer, wait for at least ten minutes to start seeing graphs. If you still see an empty graph, it means no data has been received by NetFlow Analyzer. Check your router settings in that case.

2. **What is Aggregate data and Raw data ? How to set Raw data ?**

   As far as aggregated data is concerned, NetFlow Analyzer maintains the top 'n' flows for every ten minutes slot. The record count determines this 'n' values. By default it is set to 50. You may set your own criteria for this purpose. you can change this from the Settings option.

   Apart from this NetFlow Analyzer allows you to store raw data (all flows -not just the top n) for upto one month.

   1. Aggregated data is stored in 5 levels of tables - 10 Min, Hourly, 6 Hour, 24 Hour and Weekly tables and reports for different periods need to access the corresponding table. For example, very recent reports need to access the 10 Min table and old reports need to access the Weekly table. You can access the table MetaTable to determine the table which contains data for the required time period
   2. Raw data is stored in dynamically created tables and data pertaining to different devices (routers) reside in different table for different periods of time. You can access the table RawMetaTable to determine the table which contains data for the required report.

3. **Some of the applications are labeled as "TCP_App" or something similar. What is that?**

   If an application is labeled as "TCP_App" or something similar, it means that NetFlow Analyzer has not recognized this application (i.e.) the combination of port and protocol is not mapped as any application. Once you add these applications under Application Mapping they will be recognized.

4. **Why are only the top 5 or 10 values shown in the reports? What if I want more detail?**

   NetFlow Analyzer shows the top 50 results in all reports by default. You can see up to 100 results in each report by changing the Record Count value in the Settings page.

5. **The graphs show only IN traffic for an interface, although there is both IN and OUT traffic flowing through that interface. Why's that?**

   Check if you have enabled NetFlow on all interfaces through which traffic flows. Since NetFlow traffic accounting is ingress by default, only IN traffic across an interface is accounted for. To see both IN and OUT traffic graphs for an interface, you need to enable NetFlow on all the interfaces through which traffic flows.

6. **Why are some interfaces labeled as IfIndex2,IfIndex3, etc.?**

   This happens if the device/interface has not responded to the SNMP requests sent by NetFlow Analyzer. Check the SNMP settings of the interface or manually edit the interface name from the Dashboard. NetFlow Analyzer uses port 161, and the *public* community string as default SNMP values. If the SNMP settings of your device are different, click the  icon next to the device/interface in the Dashboard Interface View to change the values. If you need to change this globally, enter the new values in the same fields under Settings..

7. **The total bandwidth usage seems to decrease depending on the length of the report. Why is that?**

   NetFlow Analyzer aggregates older data in less granular format and due to this reason some of the spikes may not show in older reports. While reports pertaining to last day is generated from tables with 10 minute granularity, reports pertaining to last week is generated from tables with 1 hour granularity

   For example, data in 10 minute table pertaining to 10:00, 10:10, 10:20, 10:30, 10:40 and 10:50 would all be aggregated and moved into hourly data tables for one data point pertaining to 10:00.

   While the total data volumes is correct, the traffic rates will be averaged over this period. So:

   10:00 -> volume transferred 100MBytes, ten minute average rate 1,333Kbits/s
   10:10 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s
   10:20 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s
   10:30 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s
   10:40 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s
   10:50 -> volume transferred 1MByte, ten minute average rate 13.3Kbits/s

   When aggregated into the one hour table, we get:

   10:00 -> volume transferred 105MBytes, one hour average rate 233Kbits/s

   The spike up to 1,333Kbits/s has been lost by this averaging process; as the data get aggregated into longer and longer time periods, so this average value will decrease further.

   This is the reason for the reduction in the reporting of bandwidth usage over time.

NBAR

1. **Which features are not supported by NBAR ?**

   The following features are not supported by NBAR:
   - More than 24 concurrent URLs, HOSTs or MIME type matches
   - Matching beyond the first 400 bytes in a URL

- Non-IP traffic
- Multicast and other non-CEF switching modes
- Fragmented packets
- Pipelined persistent HTTP requests
- URL/HOST/MIME/ classification with secure HTTP
- Asymmetric flows with stateful protocols
- Packets originating from or destined to the router running NBAR

2. **Any restrictions on where we can configure NBAR?**

   You can't configure NBAR on the following logical interfaces:
   - Fast EtherChannel
   - Interfaces that use tunneling or encryption
   - VLANs
   - Dialer interfaces
   - Multilink PPP

   Note: NBAR is configurable on VLANs as of Cisco IOS Release 12.1(13)E, but supported in the software switching path only.

3. **What Does NBAR Performance Depend On?**

   Several factors can impact NBAR performance in software-based execution.

   A. **Router Configuration**
   1. Number of protocols being matched against it
   2. Number of regular expressions being used
   3. The complexity of packet inspection logic required

   B. **Traffic Profile** (Packet Protocol Sequence)
   1. The number of flows
   2. Long duration flows are less expensive than shorter duration flows
   3. Stateful protocol matches are more performance impacting than static port applications

4. **Is performance dependent on the number of interfaces that NBAR is enabled on? Does the link speed of the interface(s) that NBAR is enabled on affect performance ?**

   No. NBAR performance is not dependent on the number of interfaces that NBAR is enabled on or the link speed of those interfaces. Performance is dependent on the number of packets that the NBAR engine has to inspect, how deep into the packet it has to look to perform regular inspection.

5. **I am able to issue the command "ip nbar protocol-discovery" on the router and see the results. But NFA says my router does not support NBAR, Why?**

   Earlier version of IOS supports NBAR discovery only on router. So you can very well execute the command "ip nabr protocol-discovery" on the router and see the results. But NBAR Protocol Discovery MIB(CISCO-NBAR-PROTOCOL-DISCOVERY-MIB) support came only on later releases. This is needed for collecting data via SNMP. Please verify that whether your router IOS supports CISCO-NBAR-PROTOCOL-DISCOVERY-MIB.

6. **How do I verify whether my router supports CISCO-NBAR-PROTOCOL-DISCOVERY-MIB?**

   a) You can check CISCO-NBAR-PROTOCOL-DISCOVERY-MIB supported platforms and IOS using the follwoing link.
   http://tools.cisco.com/ITDIT/MIBS/AdvancedSearch?MibSel=250073

b) Alternately , you can execute "show snmp mib | include cnpd " command at router to know the implemeted mib objects in the router. If the router supports CISCO-NBAR-PROTOCOL-DISCOVERY-MIB, then the above command gives the following objects.

cnpdStatusEntry.1
cnpdStatusEntry.2
cnpdAllStatsEntry.2
cnpdAllStatsEntry.3
cnpdAllStatsEntry.4
cnpdAllStatsEntry.5
cnpdAllStatsEntry.6
cnpdAllStatsEntry.7
cnpdAllStatsEntry.8
cnpdAllStatsEntry.9
cnpdAllStatsEntry.10
cnpdAllStatsEntry.11
cnpdAllStatsEntry.12
cnpdTopNConfigEntry.2
cnpdTopNConfigEntry.3
cnpdTopNConfigEntry.4
cnpdTopNConfigEntry.5
cnpdTopNConfigEntry.6
cnpdTopNConfigEntry.7
cnpdTopNConfigEntry.8
cnpdTopNStatsEntry.2
cnpdTopNStatsEntry.3
cnpdTopNStatsEntry.4
cnpdThresholdConfigEntry.2
cnpdThresholdConfigEntry.3
cnpdThresholdConfigEntry.4
cnpdThresholdConfigEntry.5
cnpdThresholdConfigEntry.6
cnpdThresholdConfigEntry.7
cnpdThresholdConfigEntry.8
cnpdThresholdConfigEntry.9
cnpdThresholdConfigEntry.10
cnpdThresholdConfigEntry.12
cnpdThresholdHistoryEntry.2
cnpdThresholdHistoryEntry.3
cnpdThresholdHistoryEntry.4
cnpdThresholdHistoryEntry.5
cnpdThresholdHistoryEntry.6
cnpdThresholdHistoryEntry.7
cnpdNotificationsConfig.1
cnpdSupportedProtocolsEntry.2

V9

1. **What is NetFlow Version 9?**

   This format is flexible and extensible , which provides the versatility needed to support new fields and record types. This format accommodates new NetFlow-supported technologies such as NAT, MPLS,BGP next hop and Multicast.The main feature of Version 9 Export format is that it is template based.

2. **What is the memory impact on the router due to V9?**

   The memory used depends upon the data structures used to maintain template flowsets. As the implementation does not access the NetFlow cache directly the memory used is not very high.

3. **"Receiving non V5/V7/V9 packets from the following devices: Click here for further details.." What does this mean?**

   If you get this message on the user interface, it means that NetFlow packets with versions other than version 5/7/9, are being received by NetFlow Analyzer. Check your router settings to make sure that **only** version 5/7/9 NetFlow exports are being sent to NetFlow Analyzer. This is because NetFlow Analyzer supports only NetFlow version 5/7/9 exports.

4. **Is version 9 backward compatible ?**

   Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, then you must configure Version 5 or Version 8.

5. **What is the performance impact of V9?**

   Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets requires additional processing.

6. **What are the restrictions for V9?**

   Version 9 allows for interleaving of various technologies. This means that you should configure Version 9 if you need data to be exported from various technologies (such as Multicast, DoS, IPv6, BGP next hop, and so on).

7. **How do I configure NetFlow Version 9?**

   Please refer the following document for configuring netflow version 9
   http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00805e1b4a.html

Technical Information

1. **How is traffic information stored in the NetFlow Analyzer database?**

   For each report, NetFlow Analyzer stores traffic information in a different manner. The following tables describe the data storage pattern for the various reports generated by NetFlow Analyzer.

   Traffic reports

Time Interval	Granularity
within last 6 hours	1 minute
more than 6 hours, but less than last 26 hours	10 minutes
more than 26 hours, but less than last 8 days	1 hour
more than 8 days, but less than 32 days	6 hours
more than 32 days, but less than last 92 days	24 hours
more than 92 days	1 week

Application traffic reports

(Application tab, Application IN/OUT graphs, Consolidated Reports)

Time Interval Granularity → within last 2 hours ↓	10 minutes
more than 2 hours, but less than last 8 days	1 hour
more than 8 days, but less than last 21 days	6 hours
more than 21 days, but less than last 90 days	24 hours
more than 90 days	1 week

Source, Destination, Conversation traffic reports

(Source, Destination, and Conversation tabs and IN/OUT graphs; Drill down graphs from Application, Source, Destination, and Conversation reports, Consolidated Reports,Custom reports)

Time Interval	Granularity
within last 1 hour	1 minute
more than 1 hour, but less than last 3 days	1 hour
more than 3 days, but less than last 21 days	6 hours
more than 21 days, but less than last 90 days	24 hours
more than 90 days	1 week

2. How do I reset admin password?

Please ensure that the server is running before doing the below steps:

1. Open a command prompt
2. Go to the \mysql\bin directory
3. Type mysql -u root --port=13310
4. Type use netflow
5. Execute the following query:
   update AaaPassword, AaaLogin, AaaAccount, AaaAccPassword setAaaPassword.PASSWORD='Ok6/FqR5WtJY5UCLrnvjQQ==', AaaPassword.SALT='12345678' where AaaLogin.LOGIN_ID = AaaAccount.LOGIN_ID and AaaAccount.ACCOUNT_ID =AaaAccPassword.ACCOUNT_ID and AaaPassword.PASSWORD_ID =AaaAccPassword.PASSWORD_ID and AaaLogin.NAME = 'admin' ;
6. Type quit to quit mysql
7. Type exit to exit command prompt
8. Login as admin / admin. You can change the password again if you wish.
9. How are ports assigned as applications in NetFlow Analyzer?

   A NetFlow export contains information on the protocol, source port, and destination port. When a flow is received, NetFlow Analyzer tries to match the port and protocol in the flow, to an application in the following order:

2. The smaller of the source and destination port numbers, to the list of ports configured to each application in the Application Mapping list
3. The larger of the source and destination port numbers, to the list of ports configured to each application in the Application Mapping list
4. The smaller of the source and destination port numbers, to the port ranges configured to each application in the Application Mapping list

5. The larger of the source and destination port numbers, to the port ranges configured to each application in the Application Mapping list

   If a matching application is still not found, then depending on the protocol received in the flow, the application is listed as ***<protocol>*_App**. (eg.) TCP_App if a flow is received with TCP protocol, and unmatched source and destination ports. If the protocol received in the flow is also not recognized by NetFlow Analyzer, the application is listed as **Unknown_App**.

	A single flow can be categorized as a single application only. In case of a conflict, applications with an exact match for the port number will be accounted for.

3. **Do I have to reinstall NetFlow Analyzer when moving to the fully paid version?**

   No, you do not have to reinstall or shut down the NetFlow Analyzer server. You just need to enter the new license file in the Upgrade License box.

4. **How many users can access the application simultaneously?**

   This depends only on the capacity of the server on which NetFlow Analyzer is installed. The NetFlow Analyzer license does not limit the number of users accessing the application at any time.

5. **NetFlow Analyzer logs out after a period of inactivity. How do I avoid that?**

   You can change the time-out value to a higher value than the default (30 minutes) by increasing the parameter **session-timeout**.
   <session-config>
   <session-timeout>30</session-timeout>
   </session-config>
   under ***<NFA_Home>*/AdventNet/ME/NetFlow/server/default/conf/web.xml**
   Change the value 30 to your desired time-range - say, 600. You will have to restart NFA server for this to take effect.

6. **How to create DBInfo log file ?**

   1. Please ensure that NFA is running.
   2. Navigate to /Troubleshooting directory and execute the file DBInfo.sh / DBInfo.bat
   3. It creates a "Info.log" file in the same folder. Please send us the "info.log" file.

7. **Why the interface shows 100% utilization ?**

   Please refer this link for a brief explanation of 100% utilization:
   http://forums.adventnet.com/viewtopic.php?t=10908&highlight=100

8. **What information do I need to send to NFA support for assistance?**

   1. Please run your logziputil.bat / logziputil.sh (under the troubleshooting folder). This will create a zip file under the support folder please send us the zip file.
   2. Send us the .err file under the Mysql\data folder.
   3. Also send your Machine configuration.

9. How to safely migrate NFA installation to different machine ?

Please follow the steps below to move your installation,

1. Copy the data folder in /mysql folder of the installation that you wish to move, to a safe location.
2. Install NetFlow Analyzer in the new location, start it once and shut it down.
3. Replace the data folder in /mysql folder of the new installation with the data folder of the old installation.
4. Start NetFlow Analyzer.

10. **What do I do if my NFA server becomes slow ?** (or) **How do I improve my NFA system performance ?**

Please refer this link for a brief note on database tuning
:http://forums.adventnet.com/viewtopic.php?t=9455

11. Why NFA says router time not is SYNC and stops collecting data ?

Please follow these steps to fix this issue:

1. In case you see this, please ensure the following on the router:Check if the correct time is set on your router.
   You can check this by logging into the router and typing ***show clock***. You can set the clock time using the command ***clock set hh:mm:ss month date year***. Check if the time zone and the offset (in Hours and Minutes) for the time zone is set properly (E.g. PST -8 00 for PST or EST -5 00 for EST). You can check this by logging into the router, going into the ***configure terminal*** and typing ***show running-config***. You can set the clock time zone and offset using the command ***clock timezone zone hours [minutes]*** (E.g. clock timezone PST -8 00)
2. The time sync issue may be related to high CPU load and reducing the IP group can help. Each address / range / network will be checked seperately. So, 4 addresses of 10.10.10.1, 10.10.10.2, 10.10.10.3 and 10.10.10.4 will add more overload than creating the same as a single IP range of 10.10.10.1 to 10.10.10.4. While associating interfaces you are better off selecting "All interfaces" wherever appropriate since in that case no check will be done with the interface in the flow. In your case, since you had 180 interfaces associated, the code had to check for these 180 interfaces in each flow received.

13. **How do I buy NetFlow Analyzer?**

You can buy NetFlow Analyzer directly from the AdventNet Online Store, or from a reseller near your location. Please see the website at http://www.netflowanalyzer.com/ for more information on purchasing options

Appendix

1. Working with SSL
2. SNMP Trap Forwarding

Working with SSL

The SSL protocol provides several features that enable secure transmission of Web traffic. These features include data encryption, server authentication, and message integrity.

You can enable secure communication from web clients to the NetFlow Analyzer server using SSL.

	The steps provided describe how to enable SSL functionality and generate certificates only. Depending on your network configuration and security needs, you may need to consult outside documentation. For advanced configuration concerns, please refer to the SSL resources at http://www.apache.org and http://www.modssl.org

Stop the server, if it is running, and follow the steps below to enable SSL support:

Generating a valid certificate

1. Generate the encryption certificate and name it as **server.keystore**
2. Copy the generated **server.keystore** file to the <*NetFlowAnalyzer_Home*>/server/default/conf directory

Disabling HTTP

When you have enabled SSL, HTTP will continue to be enabled on the web server port (default 8080). To disable HTTP follow the steps below:

1. Edit the **server.xml** file present in <*NetFlowAnalyzer_Home*>/server/default/deploy/jbossweb-tomcat50.sar directory.
2. Comment out the HTTP connection parameters, by placing the `<!--` tag before, and the `-->` tag after the following lines:

```
<!-- A HTTP/1.1 Connector on port 8080 -->
<Connector port="8080" address="${jboss.bind.address}"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>
```

Enabling SSL

1. In the same file, enable the HTTPS connection parameters, by removing the `<!--` tag before, and the `-->` tag after the following lines:

```
<!-- SSL/TLS Connector configuration using the admin devl guide
keystore
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```

2. Replace the default values for the following parameters as follows:

Default Value	New Value
keystoreFile= "${jboss.server.home.dir}/ conf/chap8.keystore	keystoreFile= "${jboss.server.home.dir}/ conf/server.keystore
keystorePass="rmi+ssl"	keystorePass="pqsecured"

Changing the web server port

1. Edit the **sample-bindings.xml** file present in <*NetFlowAnalyzer_Home*>/server/default/conf directory
2. Replace the default values for the following parameters as follows:

Default Value	New Value
<xsl:variable name="portHttps" select="$port + 363"/>	<xsl:variable name="portHttps" select="8443"/>
</delegate-config> <binding port="8080"/> </service-config>	</delegate-config> <binding port="8443"/> </service-config>

Verifying SSL Setup

1. Restart the NetFlow Analyzer server
2. Verify that the following message appears:

```
Server started.
Please connect your client at http://localhost:8443
```

3. Connect to the server from a web browser by typing `https://`<*hostname*>`:8443` where <*hostname*> is the machine where the server is running

SNMP Trap Forwarding

The alerts generated by Netflow Anlayzer can be forwarded as a trap message to any manager application. This helps in consolidating all the network alerts in a single place in the manager application.
The steps for the manager application to get the traps, forwarded by Netflow Analyzer, are;

1. Configure a particular port in the manager application to listen for SNMP traps
2. In Netflow Analyzer alert profile form, select alert action as '***SNMP Trap***' and specify <Server Name>:<Port No.>:<Community>
    - **<Server Name>** - The name or IP address of the server in which the manager application is running
    - **<Port No.>** - The port number at which the manager application is listening for the traps
    - **<Community>** - The community string of the manager application

After the configuration, one trap is sent to the manager application, for every alert generated. A trap contains an OID and a system description.

AdventNet provides a MIB file with the OIDs and their descriptions for all the traps that can be forwarded. The manager application can parse this MIB file and get meaningful messages for the forwarded traps.

The steps for the manager application to decode the meaning of each of the OIDs, are;

- Copy ADVENTNET-NETFLOWANALYZER-MIB file from <NetFlow Analyzer Home>/lib directory and save it in the system where the manager application is running
- Load the MIB file, ADVENTNET-NETFLOWANALYZER-MIB in the manager application
- Make the required configuration in the manager application, such that the OIDs are parsed and meaningful info is got.