Quick Reference Guide

About NetFlow™ Technology
Features and Benefits of NetFlow Analyzer
Technical Information
Frequently Asked Questions

TABLE OF CONTENTS

PURPOSE OF THIS GUIDE 3

CONTACT INFORMATION 4

MANAGEENGINE NETFLOW ANALYZER 5

ABOUT NETFLOW™ TECHNOLOGY 6

THE NETFLOW ANALYZER ADVANTAGE 8

NETFLOW ANALYZER FEATURES AND BENEFITS 9

TECHNICAL INFORMATION 12

FREQUENTLY ASKED QUESTIONS 14

Purpose of this Guide

The Quick Reference Guide aims at giving a high-level overview of the NetFlow Analyzer product, the technology behind it, and its key features and benefits. This information is primarily intended for AdventNet partners, resellers, and sales account teams, who need to understand NetFlow Analyzer to a good extent, without spending time searching for information elsewhere.

Contact Information

For comments and queries on this Quick Reference Guide, please contact Raghunandhan, Product Manager, at raghunandhanr@adventnet.com

For information on NetFlow Analyzer and other products from AdventNet, Inc. visit http://www.adventnet.com/

For product-related queries and technical support, contact us at support@netflowanalyzer.com

ManageEngine NetFlow Analyzer

In-depth traffic analysis at a fraction of the cost

NetFlow Analyzer makes enterprise-wide bandwidth monitoring a lot less complicated. Armed with NetFlow data that is exported by leading vendors of routing and switching devices, NetFlow Analyzer shows you the exact nature of traffic flowing across your network, thereby helping you to understand and predict bandwidth requirements for your enterprise needs.

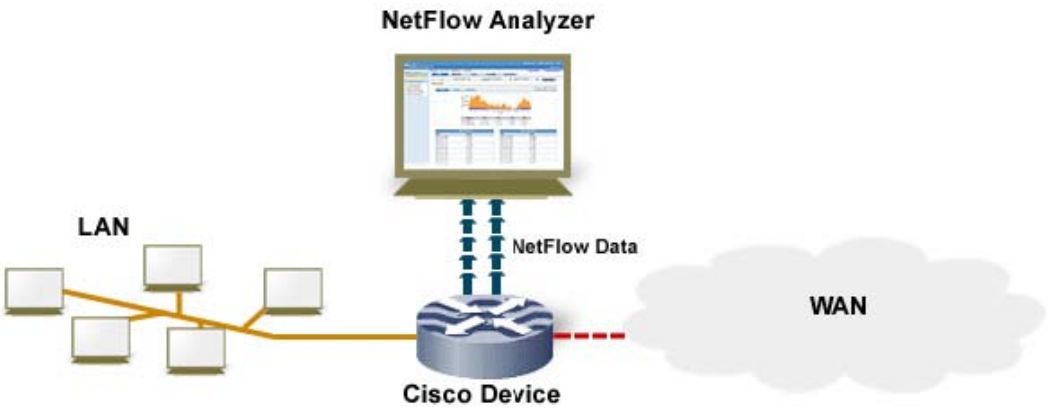

Fig. 1: NetFlow Analyzer analyzes traffic passing through the LAN and WAN segment to give you total insight on what's happening on your network

Before delving into the details of NetFlow Analyzer and how it works, you need to know what NetFlow is all about and how it benefits you in terms of cost and performance.

The following pages give a brief insight into NetFlow technology and how it is the right choice in terms of cost as well as performance for enterprises wanting to measure bandwidth usage across the network.

If you are already aware of NetFlow and its benefits, you can skip this section and go directly to the next section on NetFlow Analyzer.

About NetFlow™ Technology

NetFlow is a network accounting technology that helps answer critical questions regarding IP traffic – who, what, when, where, and how. NetFlow is supported on routers and switches from leading vendors, and is fast becoming the primary network accounting technology of the industry.

NetFlow services capitalize on the flow nature of network traffic to provide detailed traffic accounting information with minimal impact on performance. NetFlow essentially records each traffic flow that enters an interface, and exports this data periodically. Hence exported NetFlow data characterizes the IP traffic that is being forwarded.

According to NetFlow, seven unique keys define a flow. These keys to differentiate one flow from another:

1. Source IP address
2. Destination IP address
3. Source port
4. Destination port
5. Layer 3 protocol type
6. Type of Service byte
7. Input logical interface (ifIndex)

A NetFlow packet is exported as a UDP datagram, approximately 1500 bytes in size. This typically contains 20 – 50 flow records. Packets are sent more frequently if the traffic across NetFlow-enabled interfaces is high.

NetFlow accounts for inbound traffic and unidirectional flows only. Due to this constraint, NetFlow has to be enabled on both interfaces through which traffic flows. Only then, graphs for inbound and outbound traffic can be generated.

Benefits of using NetFlow data in network management

NetFlow allows extremely granular and accurate traffic measurements. Because it is part of the software that runs on the device, NetFlow enables networks to perform IP traffic flow analysis without purchasing custom probes – making traffic analysis economical on large IP networks.

Business benefits offered by NetFlow:

1. Cost effective – NetFlow records are generated by the same device that switches or routes traffic.
2. Scalable – traffic analysis extends only to the number of devices on which NetFlow is enabled.
3. Minimal impact on performance – NetFlow reduces data transfer, by aggregating exchanges between a source and destination as a conversation in a single NetFlow record.

NetFlow records are exported as UDP datagrams. Apart from the significant advantages that UDP provides in speed and simplicity over TCP networks, this also means lower bandwidth requirements for NetFlow data, and reduced platform requirements for devices collecting that NetFlow data.

NetFlow Versions

There are many versions of NetFlow, starting from version 1 to the most recent version 9. Version 5 is the standard and most common version used across the industry.

NetFlow Analyzer currently supports NetFlow **version 5** exports only.

Summary

In summary, NetFlow records provide valuable information about network users and applications, peak usage times, and traffic routing. NetFlow-based traffic accounting is not only cheaper compared to probes, but also more detailed.

Once NetFlow data is collected, it needs to be stored, processed, and presented in such a manner that understanding bandwidth usage, and identifying network bottlenecks becomes a fast and efficient process. This is where NetFlow Analyzer comes into use.

The NetFlow Analyzer Advantage

NetFlow data needs to be collected and correlated before showing graphs and reports. While most free tools can correlate NetFlow data to an extent, collecting it, and storing it for long periods of time requires a robust database setup. Besides that, the collected information needs to be presented in such a way that traffic analysis is quick and efficient.

NetFlow Analyzer does all this and more. The built-in MySQL database is used to store all NetFlow data that is received. This is then processed to retrieve the top values to be shown in the reports. NetFlow Analyzer includes a host of reports that correlate the received NetFlow data to show you details on top hosts, top applications, top conversations, and more. NetFlow Analyzer also includes options to print or save these reports so that you can archive them for future reference.

How it works together:

Essentially NetFlow Analyzer receives exported NetFlow version 5 records, processes them, and generates graphs and reports based on the data received.

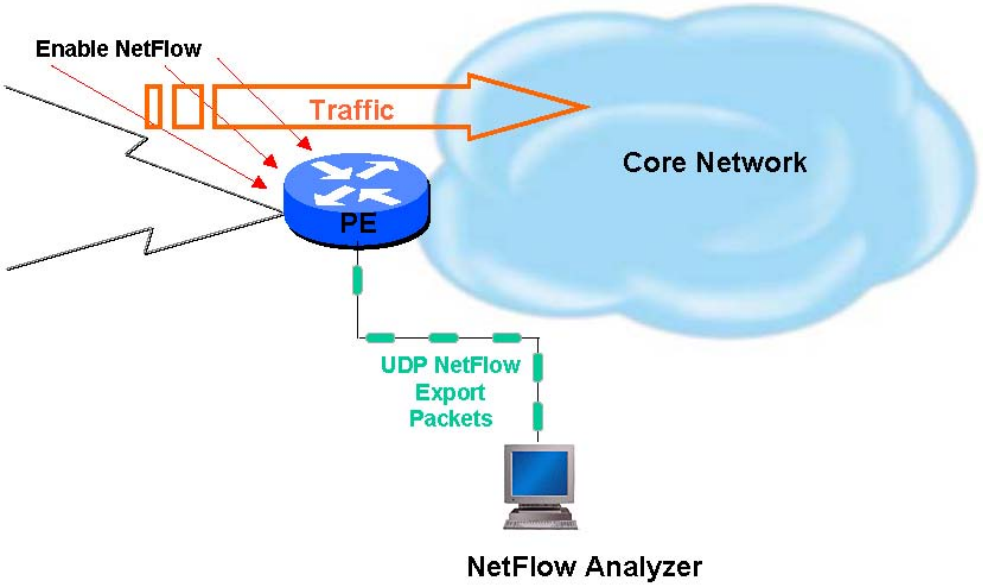

Fig. 2: NetFlow-enabled devices send data as UDP datagrams to NetFlow Analyzer

NetFlow Analyzer does not need any special configurations or additional setup. All you need to do is enable NetFlow on each interface in your router/switch, and direct NetFlow exports to the NetFlow Analyzer server. Once NetFlow Analyzer receives flows from an interface, it is automatically added to the list of interfaces monitored, and traffic graphs are plotted within ten minutes of receiving NetFlow data.

NetFlow Analyzer Features and Benefits

Simplified bandwidth analysis

NetFlow Analyzer enables comprehensive traffic analysis and bandwidth reporting without deploying expensive and complicated hardware probes. Powerful reports correlate NetFlow data to show you exact details of how bandwidth was used up.

Enhanced Data Storage

Data is stored in both aggregated and non-aggregated formats. The aggregated top 100 is stored forever and provides reports for capacity planning and long term reporting. The non-aggregated (or raw) data can be stored for upto 2 weeks and allows troubleshooting with 1 minute granularity.

Alerting Based on Thresholds

Generates alerts, and sends you an email, when the traffic utilization exceeds pre-defined threshold settings. Forwards SNMP traps to NMS / EMS application for critical alerts in the network.

Understanding bandwidth usage with Traffic Graphs

NetFlow Analyzer displays near real-time traffic graphs based on volume, speed of the link, and link utilization. Reports then break down this traffic into constituent applications, source hosts, destination hosts, and conversation pairs. This means that for a certain link, you can not only see the volume of incoming and outgoing traffic, but also drill down to see what made up that traffic, and who caused it.

The need for Custom Reports

Custom reports let you see details for a specific conversation, host, or application. This gives you the flexibility to drill down to details that you want to see, and also correlate information to understand usage patterns better.

Putting it all together with Consolidated Reports

Consolidated reports give you the complete picture for traffic that has passed through an interface. All the details about incoming and outgoing traffic, the hosts and applications that contributed towards it, and the conversations that accounted for bandwidth usage are shown here. You can print this report, or save it as a PDF file.

Recognizing custom applications using Application Mapping

NetFlow exports include details of the port and protocol involved in the conversation. NetFlow Analyzer combines this information to show application traffic in the traffic reports.

In order to identify and profile traffic for custom applications, you just need to map the ports and protocols used by the application under Application Mapping. Once this is done, custom application traffic is instantly recognized.

Simplified management

Bandwidth reports aside, NetFlow Analyzer offers other features that make it easy to manage different devices, and allow authorized access to a select few.

Managing different devices with Device Group Management

The Device Group Management feature in NetFlow Analyzer lets you group devices logically. Typical enterprise setups would group such devices based on locations, departments, and so on. Data center and NOC setups would typically group such devices based on customer resources.

Device Group Management makes it easy to analyze and account for traffic across a certain set of devices, and also enables selective access to the traffic reports.

Monitoring Departmental Traffic with IP Group Management

The IP Group Management feature lets you monitor departmental, intranet or application traffic exclusively. IP groups can consist of an IP address range or subnet, or a combination of port and protocol. After creating an IP group, you can view the top applications, top protocols, top hosts, and top conversations in this IP group alone.

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, without specifying any port/protocol values.

The traffic reports for each IP group will then show bandwidth usage for that department along with information on top talkers, and top conversations within that department.

Providing authorized access through User Management:

NetFlow Analyzer provides three levels of users with different privileges:

Admin users have full rights to generate reports, add new applications, manage other users, and create groups.
Operator users have the same rights but are assigned to one or more groups.
Guest users are also assigned to one or more groups, but can only generate traffic reports.

This hierarchy lets you manage your network more effectively. While network administrators can be given Admin access, IT teams responsible for one or more groups can be given Operator access. Guest access can be given to managers interested in high-level traffic analysis, or to customers who simply want to you to account for bandwidth usage charges.

Juggling between interfaces with License Management:

NetFlow Analyzer licensing is based on the number of interfaces that you want to manage concurrently. This means that if you have ten interfaces, but are allowed to manage only five, you can stop receiving flows from some interfaces and activate other interfaces. This also helps when some device is down for maintenance or is temporarily shut down.

However, you can only stop NetFlow Analyzer from receiving NetFlow data from an interface. You cannot stop the interface from exporting NetFlow data unless you directly work on the device.

Simplified deployment

Running on different platforms and browsers:

NetFlow Analyzer can be installed and run on Windows and Linux machines* with no change in functionality or user experience. This gives you the flexibility to choose the most appropriate box for setting up NetFlow Analyzer in your network.

**Selected versions only.*

The NetFlow Analyzer client is totally web-based. This enables you to access NetFlow Analyzer from anywhere in the network using just a web browser.

Supporting NetFlow version 5 exports:

NetFlow Analyzer supports NetFlow version 5 records only. All Cisco devices exporting NetFlow version 5 records are supported. NetFlow or similar exports from other vendors such as Juniper and Foundry may be supported if the export format is exactly the same as that of Cisco NetFlow version 5.

Getting it to work for you:

NetFlow Analyzer is simple to install and requires no additional configuration or training. All you need to do is enable NetFlow export on your interfaces and direct them to NetFlow Analyzer. Simple and effective, NetFlow Analyzer lets you start analyzing your traffic minutes after setting it up.

Technical Information

System Requirements

Hardware Requirements:

Pentium III – 1 GHz
Disk Space – 150MB for the installation, 20GB for the database
RAM – 512MB

Software Requirements:

Supported Operating Systems:

Windows 2000 Server/Professional with SP4, Windows XP with SP1
RedHat Linux 8.0 and 9.0

Supported Web Browsers:

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

Note: NetFlow Analyzer is optimized for 1024x768 resolution and above.

Ports needed by NetFlow Analyzer

PORT NAME	DESCRIPTION	DEFAULT PORT NUMBER
NetFlow Listener port	This is the port on which NetFlow Analyzer listens for incoming NetFlow packets.	9996
Web Server port	This is the port used to access NetFlow Analyzer from a web browser.	8080
MySQL port	This is the port used to connect to the built-in MySQL database.	13310

Commands to set up NetFlow on a Cisco IOS Router

The following is a partial list of commands to set up NetFlow version 5 data export on a Cisco IOS router. For a more complete description, refer to the NetFlow Analyzer User Guide at http://manageengine.adventnet.com/products/netflow/help/installation/setup-cisco-netflow.html

```
router#configure terminal
(config)#interface <interface name>
(config-if)#ip route-cache flow
(config-if)#exit
(config)#ip flow-export destination <destination IP> <listener port
number>
(config)#ip flow-export source <interface name>
(config)#ip flow-export version 5 (config)#ip flow-cache timeout active
5 (config)#ip flow-cache timeout inactive 15 (config)#snmp-server
ifindex persist (config)#^Z router#write
router#show ip flow export router#show ip cache flow
```

*** Repeat these commands for each interface on which NetFlow has to be enabled*

Please note that NetFlow commands may vary between IOS versions and router series. Please check with the Cisco documentation at http://cisco.com/go/netflow for the latest information on Cisco NetFlow and commands.

Frequently Asked Questions

1. **What is NetFlow?**

   NetFlow is a network accounting technology that enables detailed traffic analysis by recording traffic flows entering an interface.

2. **What is NetFlow Analyzer?**

   NetFlow Analyzer is a web-based application that collects NetFlow exports, processes them, and generates graphs and reports representing NetFlow data.

3. **How does NetFlow Analyzer collect NetFlow data?**

   NetFlow Analyzer listens for incoming NetFlow packets at the specified NetFlow listener port. All you need to do is enable NetFlow on the interfaces, and set the destination IP address to the machine on which NetFlow Analyzer is running.

4. **How can I add a new device to NetFlow Analyzer?**

   You do not need to add devices to NetFlow Analyzer. Once an interface starts sending packets to NetFlow Analyzer, it is automatically added to NetFlow Analyzer.

5. **What happens if I send non-v5 packets to NetFlow Analyzer?**

   NetFlow Analyzer currently supports only version 5 exports. If NetFlow packets with any other version number are received, NetFlow Analyzer will ignore these packets and you cannot see any graphs or reports for the same.

6. **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 NetFlow Analyzer has received no data. Check your router settings in that case.

For more questions and common problems encountered, look up the NetFlow Analyzer online user forum at http://forums.adventnet.com/viewforum.php?f=46

More Information

NetFlow Analyzer web site: www.netflowanalyzer.com

Cisco NetFlow web site: www.cisco.com/go/netflow

NetFlow Analyzer Technical Support

Email: support@netflowanalyzer.com

Phone: +1 888 720 9500

The above information is intended to give you a fairly good idea of NetFlow Analyzer, and how it helps enterprises understand their bandwidth needs. For more information on NetFlow Analyzer and technical queries, contact us at support@netflowanalyzer.com