A Survey of Network Traffic Monitoring and Analysis Tools

Chakchai So-In, *s_chakchai@yahoo.com*

Abstract:

From hundreds to thousands of computers, hubs to switched networks, and Ethernet to either ATM or 10Gbps Ethernet, administrators need more sophisticated network traffic monitoring and analysis tools in order to deal with the increase. These tools are needed, not only to fix network problems on time, but also to prevent network failure, to detect inside and outside threats, and make good decisions for network planning. This paper surveys all possible network traffic monitoring and analysis tools in non-profit and commercial areas. The tools are categorized in three categories based on data acquisition methods: network traffic flow from NetFlow-like network devices and SNMP, and local traffic flow by packet sniffer. The popular tools for each category and their main features and operating system compatibilities are discussed. The feature comparisons on each category are also made.

Keywords:

Network Traffic Monitoring and Analysis Tools, Traffic Flow, NetFlow, sFLow, IPFIX, RMON, Flow-tools, cflowd, flowd, FlowScan, Autofocus, Fluxoscope, pmacct, InMon, snoop, tcpdump, Ethereal, Wireshark, Sniffer, MRTG, Cricket

Table of Contents

1. Introduction

Network monitoring and measurement have become more and more important in a modern complicated network. In the past, administrators might only monitor a few network devices or less than a hundred computers. The network bandwidth may be just 10 or 100 Mbps (Megabit per second); however, now administrators have to deal with not only

higher speed wired network (more than 10 Gbps (Gigabit per sec) and ATM (Asynchronous Transfer Mode) network) but also wireless networks. They need more sophisticated network traffic monitoring and analysis tools in order to maintain the network system stability and availability such as to fix network problems on time or to avoid network failure, to ensure the network security strength, and to make good decisions for network planning.

When a network failure occurs, monitoring agents have to detect, isolate, and correct malfunctions in the network and possibly recover the failure. Commonly, the agents should warn the administrators to fix the problems within a minute. With the stable network, the administrators' jobs remain to monitor constantly if there is a threat from either inside or outside network. Moreover, they have to regularly check the network performance if the network devices are overloaded. Before a failure due to the overload, information about network usage can be used to make a network plan for short-term and long-term future improvement

There are various kinds of tools dealing with the network monitoring and analysis, such as tools used by Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), Sniffing, and Network flow monitoring and analysis. Given the data packet and network traffic flow information, administrators can understand network behavior, such as application and network usage, utilization of network resources, and network anomalies and security vulnerabilities. In this paper, we survey all possible network traffic monitoring and analysis tools in both public and commercial areas. The organization of this paper is as follows.

In section 2, we classified the tools in three categories based on how to retrieve the network flow information: network traffic flow information from network devices (NetFlow-like in section 2.1 and SNMP in section 2.2) and from local traffic network (by packet sniffer in section 2.3). The popular tools for each category with main features and operating system compatibilities are given. In section 3, the feature comparisons for each category are made based on [sFlow03]. Finally, summaries are drawn in section 4.

Since in fact, there are a huge number of monitoring and analysis tools available (in Appendix 7), we also include lists of all possible tools from [1, 2, 3, 4, 5, 6, 7, 8, 9]. However, all tools in this paper focus only on a network traffic monitoring and analysis purpose. A reader can follow the link for further information or click on the references [1] to [9]. However, unlike the purpose of this paper (network traffic monitoring and analysis tools), these links contain other network management and monitoring tools. For example, in [1], the ESnet Network Monitoring Task Force (NMTF) has maintained the updated list of network monitoring tools both LAN and WAN.

The link gathers thousands of tools and classifies into eight main groups: Network Monitoring Platforms (NMP), Monitoring Tools Integrated with NMP, Commercial Monitoring Tools not Integrated with an NMP, Public Domain Network Monitoring Tools, Web Tools, Auxiliary Tools to Enable Monitoring, Analysis, Report Creation or Simulation. For commercial network monitoring tools, there are eight subgroups: Analyzer/Sniffer, Application/Services monitoring, Flow monitoring, FTP, Network security, SNMP tools, Topology, and VOIP (Voice Over IP). And fourteen subgroups are classified for public network monitoring tools: Application Monitoring, Finger Printing, FTP (File Transfer Protocol), Mapping, Monitoring Infrastructures, Packet Capture, Path Characterization, Ping, RRDtool (Round Robin Database Tool) , SNMP, Throughput tools, Traceroute.

In [2], the Cooperative Association for Internet Data Analysis (CAIDA) also provides tools and analyses promoting the engineering and maintenance of a robust, scalable global Internet infrastructure. Network traffic monitoring software and text-based packet monitoring software are listed in [3] with some comments. In [4], the Swiss Education and Research Network makes a list of Flow-Based Accounting Software and brief descriptions for each tool. Some of the network monitoring and management are described briefly in [5]. In category "Network Traffic Monitoring", [6] lists the tools and gives critic for popular tools.

In [7], the Advanced Laboratory Workstation System lists the network monitoring software. The link is no longer maintained, but it is still there. Comlab provides some tools for modeling the user-traffic [8]. Hundreds of traffic monitoring and analysis tools (most of them are in the commercial area) are listed in [9] and [10]. www.tucows.com and www.download.com are well-known websites for downloading software in both commercial and non-profit areas. The tools by searching "network traffic monitoring" and "network traffic analyzer" are listed.

Back to Table of Contents

2. Traffic flow information

In this section, we consider the characteristics of traffic flow information. We group network traffic monitoring and analysis tools into three categories based on data acquisition technique: network traffic flow information from network devices like NetFlow, such as "Cisco NetFlow" and "sFlow", by SNMP such as "MRTG" and "Cricket", and by packet sniffer (Host-bed/Local traffic flow information) such as "snoop" and "tcpdump".

2.1 Network traffic flow information (by NetFlow-liked)

Cisco Systems is a well-known company for enterprise network devices. Cisco Systems was also the first company to develop and sell routers, so the idea of how to retrieve flow information was originally implemented by Cisco Systems. Cisco Systems provides an open but proprietary network protocol running on Cisco IOS (Internetworking Operating System), "Cisco NetFlow", in order to capture network traffic flow information and then send it back to the monitoring hosts. In this section, we describe network traffic flow information from NetFlow-like devices

The reason for "NetFlow-like" is that other networking companies, although they have their own techniques to either retrieve or export network flow information, their features are similar to "Cisco NetFlow". For example, Juniper Networks provides a similar feature for its routers called "cflowd", which is basically NetFlow version 5. Huawei Technology routers also support the same technology called "NetStream". [Wikipedia, NetFlow06]

2.1.1 Cisco NetFlow

"Cisco NetFlow" [Cisco, NetFlow06a]by Cisco Systems: Cisco routers with netflow switching feature can generate network flow records and be exported in either UDP (ser Datagram Protocol) or SCTP (Stream Control Transmission Protocol) packets to NetFlow collectors. NetFlow record is defined as version number (version 5 is commonly used and version 9 is an IETF (Internet Engineering Task Force standard for IPFIX (Internet Protocol Flow Information eXport)), sequence number, input and output interface SNMP indices, timestamps for the flow start and finish time, number of bytes and packets observed in the flow, IP (Internet Protocol) headers (Source and destination IP addresses, Source and destination port numbers, IP protocol, Type of Service value), the union of all TCP (Transport Control Protocol) flags observed over the life of the flow. [Wikipedia, NetFlow06]

The network flow information is very useful not only to understand network behavior, to detect security holes, but also to make good decisions on network planning. For example, source and destination addresses can be used to determine who is originating or receiving the traffic. The application utilizing or distributing can be made from port information. Class of service examines the traffic priority. The packets and byte count show the amount of traffic. Flow timestamps are used to calculate packets and bytes per second. Next hop IP address with BGP (Border Gateway Protocol) shows routing information. Network prefixes can be calculated from subnet mask of source and destination address. The union of TCP flags can implicitly explain a TCP handshake process. [Cisco, NetFlow06b]

Some routers also support more flow information such as source and destination Autonomous System (AS) number. NetFlow version 9 includes all of these fields and optionally includes extra information, such as Multiprotocol Label Switching (MPLS) labels and IP version 6 addresses and port numbers. NetFlow version 9 was also chosen to be a common, universal standard of export for IP flow information from network devices by IPFIX (IP Flow Information Export) IETF working group. [IETF charters (ipfix)06]

NetFlow record is cached when traffic is first passed by Cisco router and sent to the NetFlow collector on the following conditions: first, for TCP traffic, when the TCP connection is terminated (after a RST or FIN is seen), second when the flow is inactive in a certain time (default is 15 seconds), third when the active flow is long lived (30 minutes by default), and finally when the flow table is full. However, these timers can be reconfigured. Moreover, general NetFlow collectors provide a traffic flow aggregation feature. For example, a long-lived FTP download may be broken into multiple flows and the NetFlow collector can combine these flows showing a total FTP traffic.

Once the flow records are exported, the router does not store those flows due to performance reason. Thus, with UDP transmission, there is no retransmission mechanism because of the lost of flow packets. Since collecting NetFlow data

can be very expensive in terms of router's CPU consumption, the huge number of flow data across the network, and the data storage is required; the NetFlow collector is placed just one hop from the router or directly connected. Additionally, "Sampled NetFlow" feature is an option in order for router to look at the packet in every nth packet or randomly selecting interval.

Aside from the recommendations above, to place the NetFlow collector, the location also depends on the location of reporting solution and the topology of the network, but it is placed at the central site, since the implementation of NetFlow from the remote branch is optimal. Normally the switching traffic is consumed about 1 to 5% in order to export the flow records to the collectors. [Cisco, NetFlow06b]

2.1.1.1 Examples of network traffic flow collectors (Flow-tools, cflowd, and flowd)

In this section, the popular tools for NetFlow collectors are described: "Flow-tools", "cflowd", and "flowd". Although "cflowd" is no longer maintained, the flow-collecting concept is used for other flow collectors. The concepts and features for flow collectors are similar; just collect NetFlow information from Cisco routers. Thus, most NetFlow collectors are offered for free charge (NetFlow collector provided by Cisco Systems is just for small fees, but high cost for Cisco NetFlow Analyzer). In table 2.2, a list of other free NetFlow collectors was drawn with main features, operating system compatibility, and input/ output. Most NetFlow collectors include simple flow analyzer such as top ten-protocol summarization and one line statistic summary.

Actually, "Flow-tools" are a combination of network traffic flow collector and flow analyzer. The flow collector can support single, distributed, and multiple servers for NetFlow versions 1, 5, 6, and 14 defined as version 8 subversions. Perl and Python are used as the programming interface. "flow-capture" module is used to collect the NetFlow record (only UDP not SCTP format) from the network devices. This module stores all flows in compress raw format. Then, either "flow-print" or "flow-cat" decodes the compress files for analyzer purpose. Other modules (including in Flow-tools package) with description are shown in table 2.1 [S. Romig et all., 2000]

Table 2.1: Flow-tools package [S. Romig et all., 2000]

Flow-tools modules	Functions
flow-cat	Concatenate flow files. Typically, flow files will contain a small window of 5 or 15 minutes of exports. "flow-cat" can be used to append files for generating reports that span longer periods.
flow-fanout	Replicate NetFlow datagrams to unicast or multicast destinations. "flow-fanout" is used to facilitate multiple collectors attached to a single router.
flow-report	Generate reports for NetFlow data sets. Reports include source/destination IP pairs, source/destination AS number, and top talkers. Over 50 reports are currently supported.
flow-tag	Tag flows based on IP address or AS number. "flow-tag" is used to group flows by customer network. The tags can later be used with "flow-fanout" or "flow-report" to generate customer based traffic reports.
flow-filter	Filter flows based on any of the export fields. "flow-filter" is used in-line with other programs to generate reports based on flows matching filter expressions.
flow-import	Import data from ASCII or "cflowd" format.
flow-export	Export data to ASCII or "cflowd" format.
flow-send	Send data over the network using the NetFlow protocol.
flow-receive	Receive exports using the NetFlow protocol without storing to disk like flow-capture.
flow-gen	Generate test data
flow-dscan	Simple tool for detecting some types of network scanning and Denial of Service attacks (DoS).
flow-merge	Merge flow files in chronological order.

flow-xlate	Perform translations on some flow fields
flow-expire	Expired flows using the same policy of "flow-capture".
flow-header	Display meta information in flow file
flow-split	Split flow files into smaller files based on size, time, or tags.

"cflowd" [cflowd98] is a flow analysis tool for analyzing NetFlow data. The "cflowd" package includes flow collections, storage, and basic analysis modules for "cflowd" and "arts++" libraries. "cflowd" package contains four modules. "cflowmux" module functions as the flow collector to collect UDP data flow from Cisco routers and saves them to shared memory buffers. Then, "cflowd" watches the shared memory and reads a packet buffer when available. "cflowd" uses "CflowRawFlow" class to covert the flow-export packets to "CflowdRawFlow" object, and use "CflowdRawFlow" to generate the tables. To generate time series data for the tabular information (AS matrix, net matrix, protocol table and port matrix, "cfdcollect" retrieves the data from "cflowd" at regular intervals. "cfdcollect" also uses "CflowdServer" class as an interface and writes data in ARTS file.

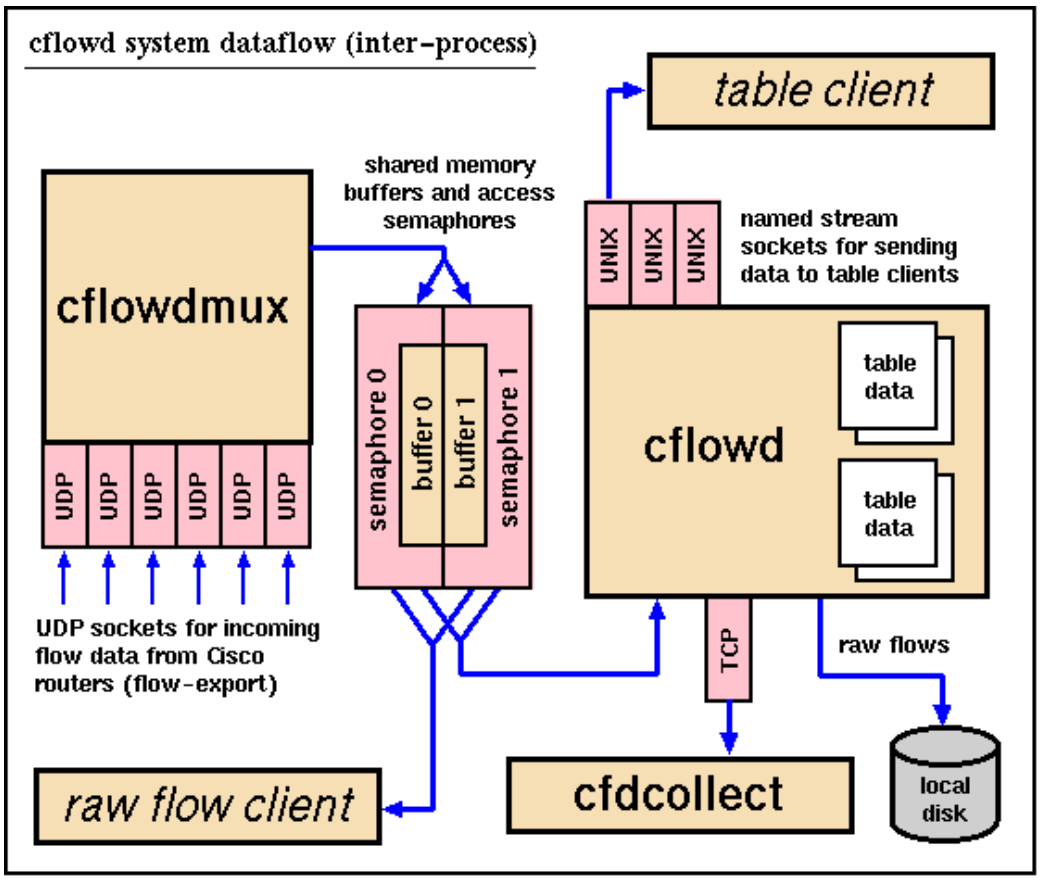

Figure 2.1: "cflowd" data flow [cflowd98]

"flowd" [flowd06] is another NetFlow collector. It supports NetFlow protocol version 1, 5, 7, and 9 in both IPv4 and IPv6 (multicast groups for flow export are also supported). "flowd" is considered secure since "privilege separated" is used to separate the parent process and unprivileged child process. "flowd" stores the data in a compact binary format. The main feature is "flowd" provides the user-friendly interface by Perl and Python.

Table 2.2: Free NetFlow collector tools

Tool	Software/ OS	Input/Output	Functions/ Features
flow	Script	NetFlow/Text	Script for NetFlow-generating software traffic probe
Flowd	UNIX-liked, softflowd and pfflowd for OpenBSD.	NetFlow/ Compact binary format	Simple, fast, and secure NetFlow collector

flowd	BSD-liked, OpenBSD, Linux	NetFlow/ Text or SQL	Flow collector (IPv4 and IPv6 transports) Support NetFlow V9
NFDUMP	BSD-liked	NetFlow/ Text	A set of tools to capture/record, dump, filter, and replay NetFlow (v5/v7/9) data
NEye	Linux, Solaris, AIX, Irix, HP/UX, Mac OS X, Digital Unix, Ultrix, Nextstep	NetFlow v5/ ASCII, MySQL, SQLite	Support various operating systems, make full use of POSIX threads
pcNetFlow	Linux, FreeBSD	NetFlow v5/ Text	A software running on normal PC hosts
NDSAD Traffic Collector	Windows, POSIX, Unix-liked	NetFlow/ Text	Translating captured traffic data into the NetFlow v.5 format.
NFDC	N/A	NetFlow/ PostgreSQL	NetFlow Datagram Collector
New NetFlow Collector	BSD-liked, Linux	NetFlow v5, v7/ Database or Text	New NetFlow collector is a POSIX compliant portable collector for
pfflowd	OpenBSD	NetFlow/ Text	Cisco NetFlow datagram export for OpenBSD.
RENETCOL	Linux	NetFlow v5/ASCII and binary files	NetFlow collector with support for NetFlow v9, IPv6, Multicast, and MPLS.

2.1.1.2 Examples of network traffic flow monitoring and analysis tools (FlowScan, Autofocus, and Fluxoscope)

In this section, the popular tools for network traffic flow monitoring and analysis are described. The tools generate the graph or function as the visualization tools, which provide the summarization and classification of network flow information. These tools generally use captured flow information from other flow collectors such as "FlowScan" (uses data from "cflowd") and "PRTG" (supports all three data acquisition methods). In table 2.3, it also shows other free NetFlow-like grapher tools with the main features, operating system compatibility, and input/ output. "AutoFocus" and "Fluxoscope" are other two popular tools for network traffic flow monitoring and analysis.

We also listed other free network traffic flow monitoring and analysis tools in table 2.4 with their main features, operating system compatibility, input & output, and primary functionalities for flow collector. Some tools also include the report generator features. Since there are a lot of free NetFlow monitoring and analysis tools, a list of available tools with the brief definition and the software link information are made in Appendix 7 (Table 7.1).

For commercial network traffic flow monitoring and analysis tools, table 2.5 shows commercial NetFlow reporting products by [Cisco NetFlow06a]. Most products are used primarily for traffic and security analysis. All companies' targets are enterprise users. "AdventNet" and "Crannog Software" are considered to be in lower price range and both of them support only Windows. Only "Cisco NetFlow Collector" and "HP" support Solaris and Linux. The rest of them support either Linux or Windows except "Arbor Networks" for BSD only and "Micromuse" for Solaris. One more observation is that if the operating system is Solaris, only NetFlow data can be used. Other than these, the list of other commercial tools is made with the software link information in Appendix 7 (Table 7.2).

"FlowScan" [D. Plonka, 2000] is visualization tool used to generate a report in HTML format. "FlowScan" is a pack of Perl script modules, which bind a flow collection engine, high performance database, and visualization tool together. Instead of cflowd's "arts++" data aggregation features, "FlowScan" uses RRDtool to store numerical time-series data. RRDtool and RRGrapher modules are used to create an output such as graphs of IP traffic in GIF (Graphic Interchange Format) or PNG (Portable Network Graphics) format.

"FlowScan" uses "cflowd" as a flow collector and "cflowd" components used by "FlowScan" are the "cflowdmux" and

"cflowd" programs. "cflowdmux" receives UDP NetFlow data from routers and passes them to "cflowd", which writes them to storage disks. Another module called "flowscan" (not "FlowScan") does the central processing in the system such as loading and executing report modules. The report module is a Perl module derived from the "FlowScan" class (FlowScan.pm). Another module called "flowdumper" is the utility module used to examine the raw flows manually.

"FlowScan" provides an extra feature dealing with buffer management due to the very high traffic and flood-based DOS attack. It also supports a stateful inspection by the use of heuristics. By analyzing flow information, "FlowScan" can track the state of application session or series of sessions. As a result, "FlowScan" can classify the stateful traffic such as Napster application or passive mode of FTP file transfers. [D. Plonka, 2000]

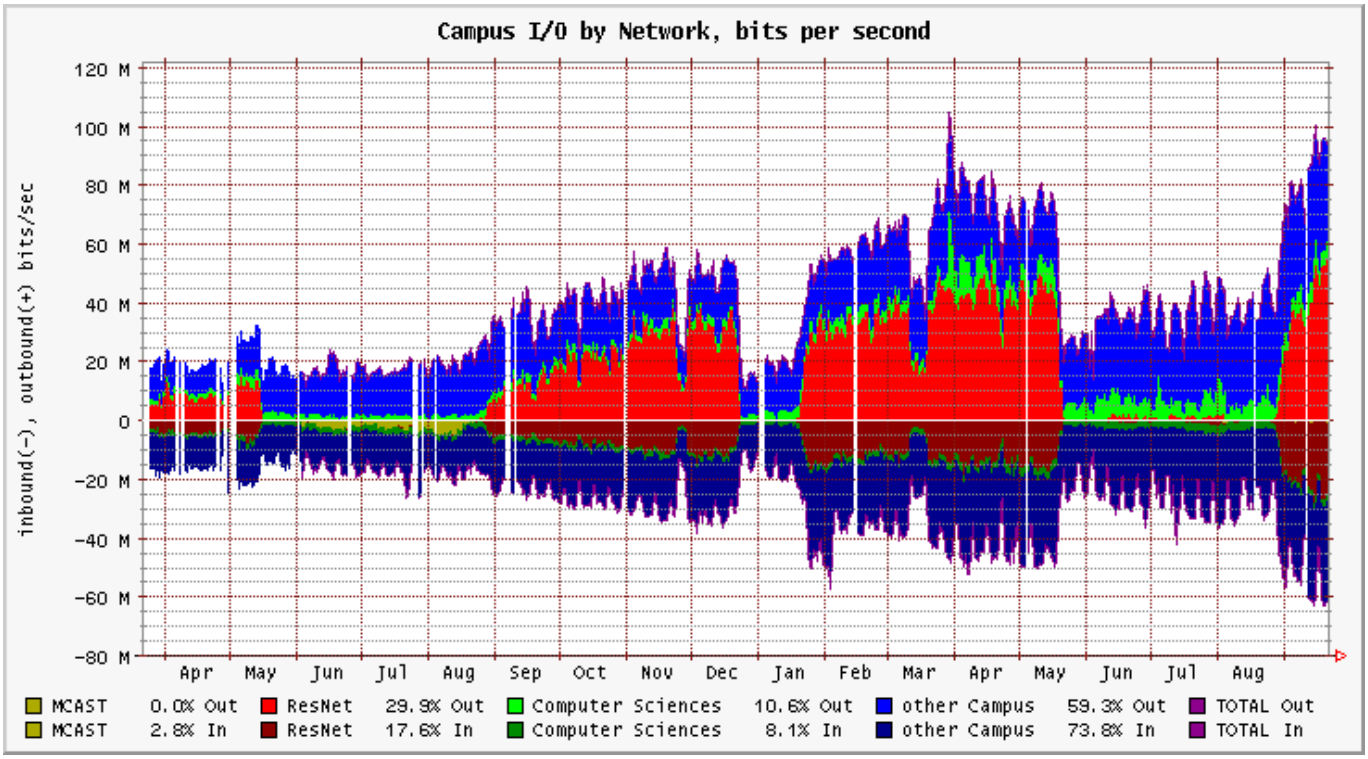

Figure 2.2: Screen snapshot of FlowScan [D. Plonka, 2000]

Next, Paessler Router Traffic Grapher (PRTG) [PRTG06] is a very powerful and low cost tool (starting from $100) for monitoring and bandwidth use for Windows. PRTG provides both free (with three sensors and academic and personal use) and commercial versions. This tool supports all three data acquisition methods: NetFlow-like, SNMP (Not only the bandwidth usage but also CPU usage, disk usage, and temperatures can be monitored.) and packet sniffer (running on promiscuous mode). The administrators can use either Window interface or web interface to configure and monitor the sensors and create reports.

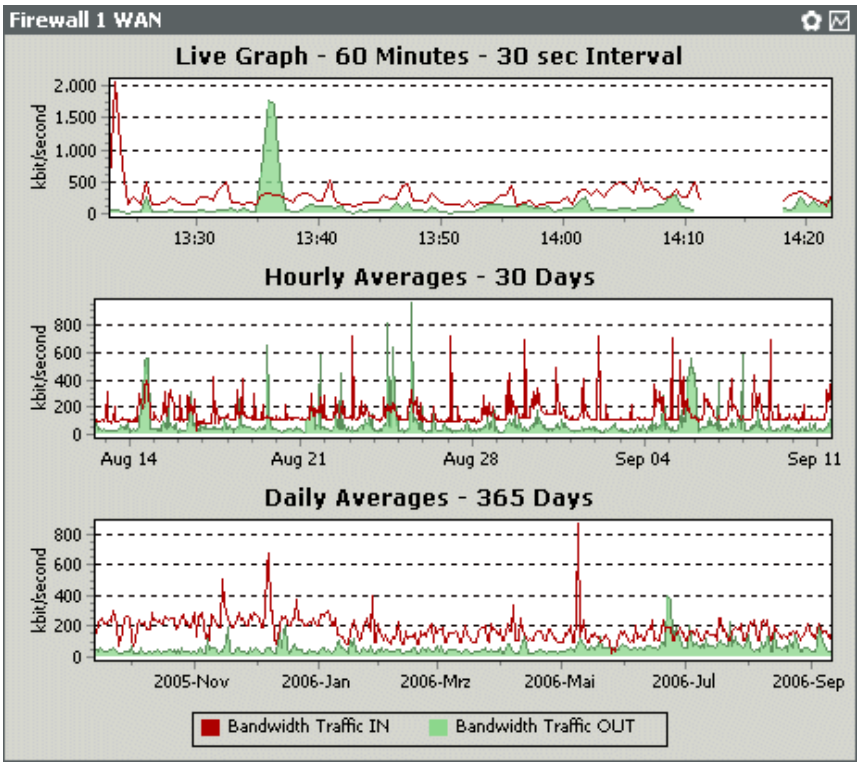

Figure 2.3: Screen snapshot of PRTG [PRTG06]

"AutoFocus" is a traffic analysis and visualization tool. "AutoFocus" analyzes the traffic pattern and provides both textual reports (measured in bytes, packets and flows) and time series plots. The extra feature is that it generates the report with traffic cluster aggregation of the mix of traffic. The traffic mix is defined using the source and destination IP address, source and destination ports and protocol field. RRDtool is used to produce time series plots of the traffic mix. "AutoFocus" can produce reports and plots for various time periods ranging from weeks to half hour intervals. It also supports the user filter. "AutoFocus" supports two types of input: packet header traces and NetFlow data. The flow sampled with both inputs can be applied, but "AutoFocus" only compensates for the sampling in the reports that measure the traffic in bytes and packets, and not for the traffic in flows. [Cristian Estan et all., 2003]

Source IP	Destination IP	Protocol	Source Port	Destination Port	bytes	Unexpectedness(%)
*	*	6	highports	highports	827M	77.7
*	*	17	highports	1434	10.5G	112.6
*	152.249.0.0/16	*	*	*	604M	100
138.0.0.0/9	*	*	*	highports	3.66G	99.4
138.0.0.0/10	*	*	highports	*	3.68G	99.9
138.54.3.58	*	17	3341	1434	2.14G	672.5
138.54.11.4	*	17	7062	1434	950M	1551.3
152.249.56.0/22	*	*	highports	highports	723M	103.4
152.249.191.120	*	17	1959	1434	1.78G	810.0
152.249.191.121	96.0.0.0/8	17	1531	1434	645M	39523.7
152.249.210.3	*	17	4315	1434	2.36G	609.5
152.249.254.152	*	17	3787	1434	1.53G	941.8

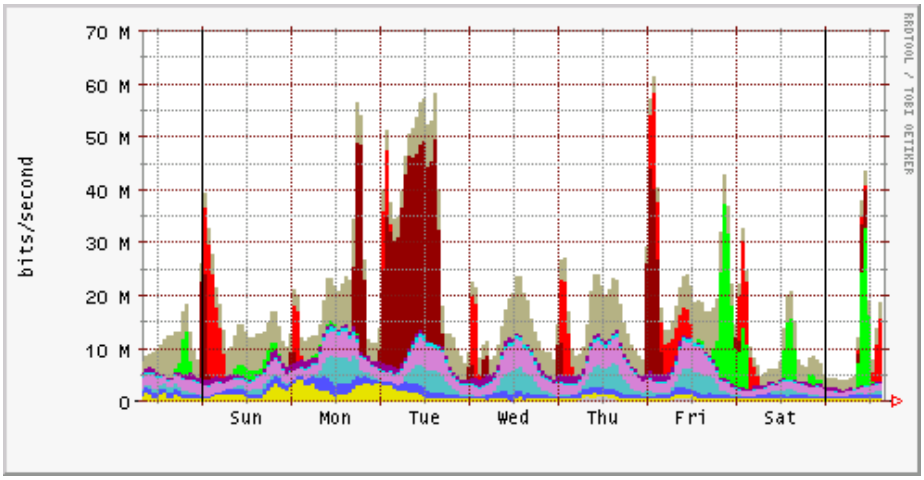

Figure 2.4: Screen snapshot of Autofocus [http://ial.ucsd.edu/AutoFocus/]

"Fluxoscope" (formerly NetFlow listener) is an aggregation and analysis software written in Common Lisp. The main feature provides not only the various types of graphical and textual reports, an interactive Web-based tool, but also the NetFlow accounting processor with an SNMP agent, which can be used to access statistics on the processing of accounting data. It can support multiple NetFlow accounting streams.

A "Listener" module in "Fluxoscope" is used to collect accounting data sent. It provides an aggregation functions to all flows and splits them into time slices, and finally periodically writes data out to files. Like general NetFlow collector, "listener" is better placed near the routers to reduce load and to avoid the data loss. "Data collection and maintenance module" periodically accesses the files that are generated by the "Listener". It also makes a copy of them to the central storage. It supports the data compression and the data over the long period can be summed up. Finally, "Data analysis module" analyzes the data from the central storage in order to generate several kinds of reports, such as tabular data and graphical representations for network monitoring and long-term traffic analysis purpose. [S. Leinen, 2000]

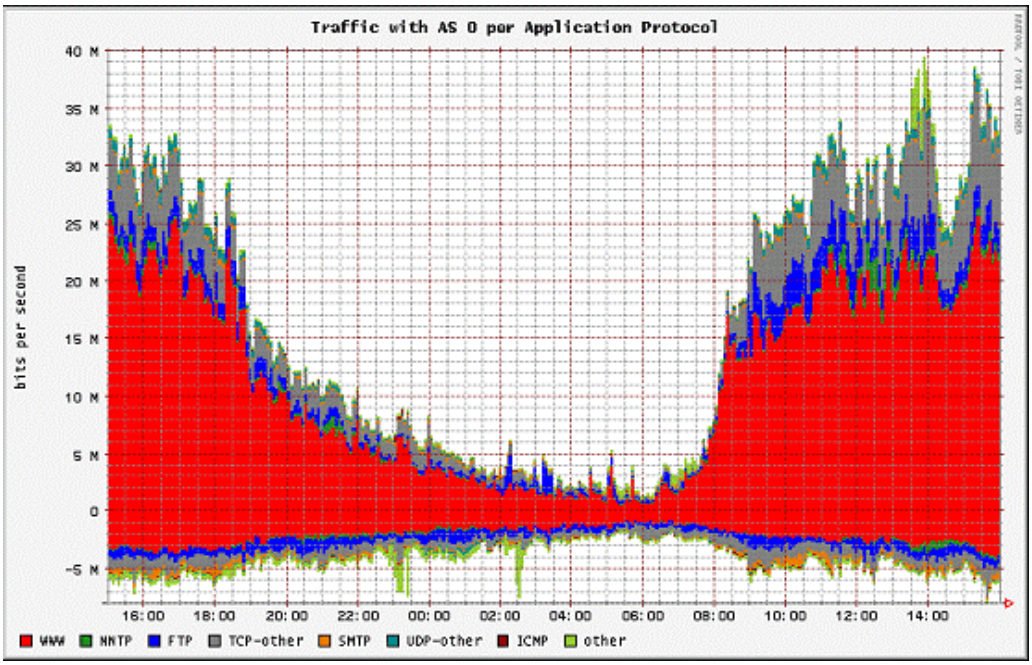

Figure 2.5: Screen snapshot of Fluxoscope [S. Leinen, 2000]

Table 2.3: Free NetFlow grapher tools

Tool	Software/ OS	Requirements	Functions/ Features
F.L.A.V.I.O.	UNIX-liked	Web/ Perl, MySQL	A data grapher for NetFlow data export compatible devices

Flow Viewer	N/A	Web/ Perl, GD, RRDTool	Web-interface to Flow-tools
JKFlow (XML based)	Linux/ Solaris	Web/ RRDTool	WAN-traffic monitoring
NfSen	BSD-liked	Web/ PHP, Perl, RRDTool	a graphical web based front end for the nfdump tools
nfstat	UNIX-liked	Web/ Perl	Weekly human-readable reports from raw NetFlow v5 data
Ntop	UNIX-liked, Linux, BSD-liked, Solaris, MacOS, Windows	Web	Network traffic probe that shows the network usage, similar to what the popular top Unix command. Support NetFlow V9
ng_NetFlow	Apple Mac OS X, Linux, BSD-liked, UNIX-liked	N/A	A netgraph kernel module.
Stager	Unix-liked	Web/ PostgreSQL	A system for aggregation and presentation of network statistics from the Flow-tools package.

Table 2.4: Free NetFlow monitoring and analysis tools

Tool	Hardware(H)/ Software(S)	Input	Output	Monitor(M)/ Capture(C)/ Analysis(A)	Real Time(R)/ Offline(O)
Argus	(S) Linux, Solaris, FreeBSD, MAC, OpenBSD, NetBSD	packet capture files, data from a live interface	Text (log files)	M, C, A: report/ audit	R, O
Autofocus(Cluster)	(S) N/A	packet header traces, NetFlow	GUI (Web*) visualization	A	O
Aflow	N/A	NetFlow	GUI (Web*)	M, C, A	R, O
AsItHappens	(S) Java	SNMP and NetFlow	GUI	M, C	R
CAIDA cflowd	(S) Unix-liked, FreeBSD	flow-export data from one or more Cisco routers	Tabular summaries	M,C, A	R
CoMo	(S) Linux, FreeBSD	NetFlow and other traffic capture sources	N/A	M, C	R
CUFlow	(S) Unix-liked, Debian	NetFlow	Text	M, C	R
CANINE	(S) Linux, MAC, Solaris, Windows	NetFlow	GUI	M, C	R
CoralReef(optical net)	(S) Unix-liked, Linux, FreeBSD	ATM Traffic live	GUI	M, C	O
Cricket	(S) BSD-liked, Linux, FreeBSD, HP-UX	SNMP	GUI (Web*)	A (time-series data)	O
dbFlowc	(S) BSD-liked, Linux, FreeBSD, Solaris, Unix-liked	NetFlow	Text	C (collect flow and store it)	R

EHNT	(S) BSD-liked, Linux, FreeBSD, UNIX-liked	NetFlow	Text	M	R
FlowScan	(S) UNIX-liked	cflowd-format raw	GUI (Web*)	A: report	O
Flow-tools (like cflowd)	(S)Linux	NetFlow	Text	M, C, A: report (Scalable)	R, O
Fluxoscope	(S) N/A	NetFlow	GUI, 3D visualization	M, C, A	R, O
Flamingo	(S) N/A	NetFlow	GUI, 3D visualization	M, C, A	R, O
Flowc	(S) Linux, FreeBSD	NetFlow	SQL, GUI (Web)	M, C, A: report	R, O
Java NetFlow Collect-Analyzer	(S) Java	NetFlow or nProbe data	Raw, JDBC	M, C, A	R, O
JNFA	(S) Java	NetFlow	SQL	M, C, A	R, O
NetFlow Monitor	(S) Linux	NetFlow	GUI (Web)	M, C, A	R, O
NeTraMet (link is no longer valid	(S) Unix-liked, DOS	NetFlow, SNMP	GUI	M, C, A	R, O
Netpy	(S) Linux	NetFlow	GUI (python)	M, C, A	R, O

*based on RRDtool files

Table 2.5: Commercial NetFlow Reporting Products [Cisco, NetFlow06b]

Product Name	Primary Use	Primary User	Operating System	Starting Price Range
Cisco NetFlow Collector	Traffic Analysis	Enterprise, Service Provider	Linux, Solaris	Medium
Cisco CS-Mars	Security Monitoring	Enterprise, SMB	Linux	Medium
AdventNet	Traffic Analysis	Enterprise, SMB	Windows	**Low**
Apoapsis	Traffic Analysis	Enterprise	Linux	Medium
Arbor Networks	Security/Traffic Analysis	Enterprise, Service Provider	BSD	High
Caligare	Traffic/Security Analysis	Enterprise, Service Provider	Linux	Medium
Crannog Software	Traffic Analysis	Enterprise, SMB	Windows	**Low**
***CA Software**	Traffic Analysis	Enterprise, Service Provider	Windows	High
***Evident Software**	Traffic Analysis, Billing	Enterprise	Linux	High
***HP**	Traffic Analysis	Enterprise, Service Provider	Linux, Solaris	High
IBM Aurora	Traffic Analysis/Security	Enterprise, Service Provider	Linux	Medium
InfoVista (Crannog)	Traffic Analysis	Enterprise, Service Provider	Windows	High

IsarNet	Traffic Analysis	Enterprise, Service Provider	Linux	Medium
***Micromuse**	Traffic Analysis	Enterprise, Service Provider	Solaris	High
NetQoS	Traffic/Security Analysis	Enterprise	Windows	High
Valencia Systems	Traffic Analysis	Enterprise	Windows	High
Wired City	Traffic Analysis	Enterprise	Windows	High

* Use Cisco NetFlow Collector

2.1.2 sFlow (pmacct and InMon Traffic Sentinel)

"sFlow" [sFlow03]originally developed by InMon Inc. is an industrial standard mechanism (defined in RFC 3176) to capture traffic from switches and routers. "sFlow" sampling technology was introduced, so the application can monitor traffic flow level at wire speed on all interfaces simultaneously: statistical packet-based sampling of switched or routed packets, and time-based sampling of interface counters. [Wikipedia, sFlow06]

"sFlow" agent running at device combines the interface counter and flow sample into "sFlow" datagram (UDP, default port is 6343) and sent to "sFlow" collectors. The UDP datagram contains the "sFlow" information as version, its originating agent's IP address, sequence number, and how many samples it contains. Unlike Cisco NetFlow originally developed by IP routing accelerate technique which can provides only basic flow information, "sFlow" offers greater scalability and reporting detail in layer 2 to layer 7 information on network traffic.

Although "sFlow" seems to be an industrial standard, only some routers' companies support such as Alcatel, Allied Telesis, Extreme Networks, Foundry Networks, Hewlett-Packard (HP), Hitachi and NEC. Thus, from our extensive survey, there are not a lot of monitoring and analysis tools available. For example, "Net::sFlow" [Net::sFlow06] is a Perl module to decode "sFlow" datagrams. "sFlow Toolkit" [sFlow Toolkit06] is a collection of network monitoring and analysis tools which bundles the converter tool from "sFlow" packets to NetFlow packets. However, a few commercial tools that support "sFlow" are also NetFlow supported. In addition, the document and technical paper are not available.

"pmacct" [pmacct06] is only free "sFlow" collector we found, but it also supports NetFlow. "pmacct" runs on Linux, BSD-liked, Solaris and embedded systems. It either collects data through NetFlow v1/v5/v7/v8/v9 or "sFlow" v2/v4/v5 and stores the packets to MySQL, PostgreSQL and SQLite. "pmacct" can easily feed data into external tools including RRDtool, GNUPlot, Net-SNMP, MRTG and Cacti. Only HP, Force Network and Foundry Network are tested for "sFlow" data.

For commercial products, we found three popular products available which all support both NetFlow and "sFlow" packets. First, "StealthWatch" by Lancope Inc [Lancope06]is a flow collector for high-speed network. "StealthWatch" can support up to 40,000 flows per second and 1,000 router devices. Second, "Infosim StableNet" [Infosim StableNet06]offers a whole solution for monitoring and reporting on the systems, networks and applications. There is not much detail about the traffic flow information; however, "Inforsim StableNet" technology supports NetFlow, cFlow, sFlow, and Netstream. Finally, "InMon Traffic Sentinel" [InMon Traffic Sentinel06] is a commercial web-based application running on RedHat ES/AS or Fedora that provides real-time and historical analysis of flow information. This tool also supports signature-based intrusion detection and automated NBAD (Network Behavior Anomaly Detection).

2.2 Network traffic flow information (by SNMP) (MRTG and Cricket)

Simple Network Management Protocol (SNMP) is defined by IETF. SNMP is an application layer protocol used to monitor network-attached devices. SNMP works as the manager/agent model. The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is

organized in a tree structure with individual variables, represented as leaves on the branches. A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

SNMP uses five basic messages (GET, GET-NEXT, GET-RESPONSE, SET, and TRAP) to communicate between the manager and the agent. The GET and GET-NEXT messages allow the manager to request information for a specific variable. The agent, upon receiving a GET or GET-NEXT message, will issue a GET-RESPONSE message to the manager with either the information requested or an error indication as to why the request cannot be processed. A SET message allows the manager to reconfigure to the value of a specific variable. The agent will acknowledge with a GET-RESPONSE message to indicate the change or provide an error message to why the change cannot be made. The TRAP message allows the agent to inform the manager of an important event. [DPS Telecom06]

Each SNMP element manages specific objects with each object. Each object / characteristic has a unique object identifier (OID). The OIDs are the combination of numbers separated by decimal points such as "1.3.6.1.4.1.2682.1". The OIDs form a tree structure. The MIB associates each OID with a readable label such as "dpsRTUAState" and various other parameters related to the object. The MIB then serves as a data dictionary used to assemble and interpret SNMP messages. [DPS Telecom06]

SNMP GET message allows the Network Monitor Engine to request information about a specific variable remotely. Upon receiving a GET message, the agent will issue a GET-RESPONSE message to the Network Monitor Engine with either the information requested or an error indication as to why the request cannot be processed. "snmpget" [snmpget05] by Net-SNMP implementation is a snmp get command-line tool for Unix-liked operating systems and Windows. It requests the network entity information and displays the output in text format. "SNMPGet" [SNMPGet03] is another free snmpget tool but provide the user-friendly interface.

As we described above, the network information can be retrieved from the networking device by SNMP, like the network traffic flow information. However, unlike NetFlow-like devices, these devices cannot store all flow and packet information. The network traffic flow information in this category are link utilization, interface bandwidth, and some other information if the device provides. Though the information is just the interface bandwidth, this is very important information since the administrators can monitor the availability of the link, the link usage, and the network usage behavior.

"MRTG" (Multi Router Traffic Grapher) is a visualization tool for SNMP data quires. To generate the output via SNMP agent, input and output object identifiers are queried regularly (the default is 5 minutes). Then, a HTML is created as the output. All figures are in GIF or PNG format. "MRTG" version 3 logs data in RRD (Round Robin Database) in order to limit the amount of log size and also increase the information retrieval efficiency (binary logging). Because of the use of RRD and core C program instead of just Perl in previous version, the limitation of "MRTG" version 3 is about the SNMP performance and so far, it supports up to 600 router ports per 5 minutes. [Tobias Oetiker, 1998]

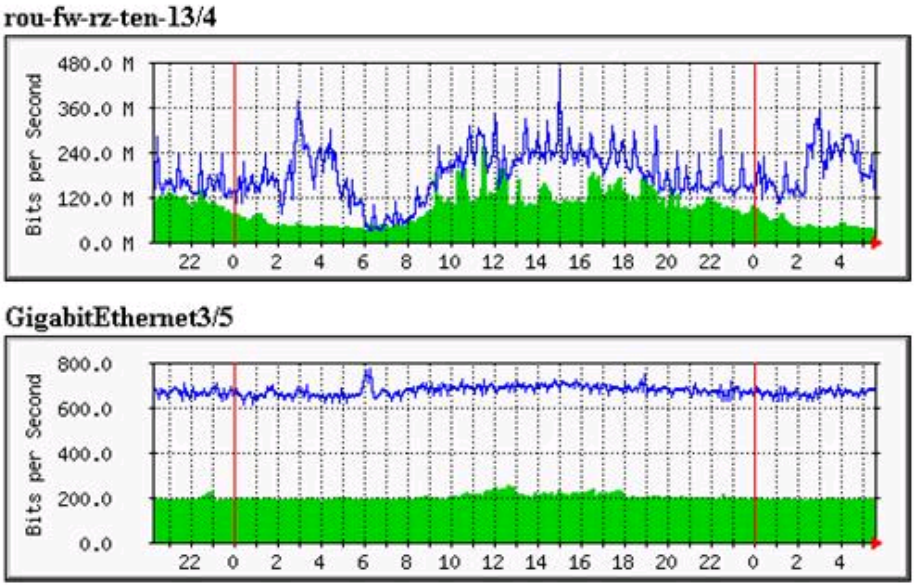

Figure 2.6: Screen snapshot from MRTG

"Cricket" [Cricket06] is a free high performance system for monitoring trends in time-series data written in Perl. "Cricket" has two components, a collector and a grapher. Like "MRTG", "Cricket" collector (snmpget-liked) runs from "cron" (daemon to execute scheduled commands) and stores data into a datastructure RRD. A web-based interface can be used to view graphs of the data. "Cricket" is developed on Solaris under Apache but it works on Linux, HP-UX, variants of BSD, and Windows. "Interface Traffic Indicator" (Inftraf) by Carsten Schmidt [Inftraf 05]is another free network traffic monitoring tool running over SNMP for Windows. "Inftraf" is a tool that requests in and out data (MIB2) from SNMP-capable network interfaces and graph out the incoming and outgoing traffic on an interface in bits per second/ bytes per second or utilization.

2.3 Local traffic flow information (by packet sniffer)

Aside from network flow information from network devices, in this section the local traffic or host-bed traffic flow information is described. Instead of requesting network devices to send the flow information to the monitoring host, we defined the host-bed flow information as the flow in local network, which packet sniffer locally collects the flow information. Originally, "sniffer" is a registered trademarks of Network Associates, Inc. used on their network analyzing products, but today "sniffer" is a well-known name for network monitor and analyzer.

A "sniffer" can be either hardware or software, which mainly intercept and collect the local traffic. After recording the traffic, the "sniffer" provides the function to decode and simply analyze the content of the packets in human readable. The traffic flow information in this category is local, that is, "sniffer" can capture the packet only from the network that "sniffer" attaches to. Therefore, in order to capture more traffic from several networks, some techniques have to be enabled or the network infrastructure might be changed. For example, due to the widespread of installing switch rather than hub, a port mirroring technique has to be enabled in order to make switches forward all the data packets to the "sniffer". Another technique is to place "sniffer" in a core network where all packets the administrator concerns are passed.

Consider the nature of broadcasting network, a network adapter discards a packet, which the destination address does not belong to. However, to capture all traffic, the network adapter will be placed in to promiscuous mode. Though having "sniffer" installed can benefit a lot in term of network troubleshooting, network intrusion detection, network usage, and so on, the limitation of "sniffer" is that it cannot read the encrypted packets. Big issue is about the privacy reason since the administrator can see the content of the packet.

Next, we briefly described most popular "sniffer" tools in public and commercial sides. There are a lot of free packet sniffer tools as we made a list in table 7.2; however, what makes the main different from the commercial is that most of the commercial sniffer tools provide a sophisticated analysis tools, user-friendly interface, and wide variety of

media such as 8802.11a/b, 802.11g, Gigabit Ethernet, and ATM.

2.3.1 Software sniffer (snoop, tcpdump, Wireshark)

In most operating system, the bundled packet sniffer is provided; however, either software (e.g. Microsoft Windows) or hard ware (HP-UX and Solaris) has to be purchased. "snoop" [snoop05] is a simple packet capture tool which is bundled on Solaris operating system. "snoop" is a command line interface and display the packet in text (a summary and multi-line format). The drawback of "snoop" is that it does not reassemble IP fragments. "nettl/ netfmt"[nettl/ netfmt00] is the packet sniffer provided by HP-UX but still in command line. "Microsoft Network Monitor" [MNN06] is the packet sniffer which is bundled with Microsoft Windows. This "sniffer" must be run on Windows NT Server 4.0 or Windows Server 2003, or have Microsoft Systems Management Server installed. This "sniffer" provides the simple graphic user interface. All "sniffer" provided for each operating system can run either in real-time and in batch modes (Logging is saved to a file for further analysis). A simple analyzer is also included for filtering and protocol searching.

"tcpdump" [tcpdump06] is a packet sniffer mainly bundled in Linux operating systems, but also has a lot of distribution with other operating systems, such as Solaris, BSD, Mac OS X, HP-UX and AIX. "WinDump" [WinDump06] can be used in Windows. Like "snoop" and "netttl/netfmt", "tcpdump" runs on standard command line and output to common text file for further analysis. "tcpdump" uses a standard libpcap [libpcap06] library as an application programming interface to capture the packets in user level (WinPcap [WinPcap06] for Win32 platform). Although all packet sniffer can examine the traffic in real-time, the processing overhead is also higher, so it might cause the packet drop. As a result, it is recommended to output raw packets and do some analysis later. However, the problem is the incompatible of the trace format such as "Microsoft Network Monitor" cannot read the trace file from "tcpdump".

Due to the performance concern, "tcpdump" functions only as the traffic-capturing tool, "tcpdump" just captures the packets and saves them in a raw file. There are not so many analysis functions. However, due to the peculiarity of "tcpdump", there are many analysis tools built for it. For example, "tcpdump2ascii" [tcpdump2ascii04] is a Perl script used to convert the output from "tcpdump" raw file to ASCII format. "tcpshow" [tcpshow05] is also a utility to print raw "tcpdump" output file in human readable. "tcptrace" [tcptrace04]is a free powerful analysis tool for "tcpdump". It can produce different types of output such as elapsed time; bytes and segments sent and received retransmissions, round trip times, window advertisements, and throughput. Shawn Osterman at Ohio University wrote this tool.

"Wireshark" [Wireshark06] (formerly Ethereal), this free packet sniffer is much like "tcpdump"; however, it provides a user-friendly interface with sorting and filtering features (a command line version of the utility is "Tshark"). "Wireshark" supports capturing packets in both from live network and from a saved capture file. The capture file format is libpcap format like that in "tcpdump". It supports a various kinds of operating systems such as Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, other Unix-like systems, and Windows. It can also assemble all the packets in a TCP conversation and show you the ASCII (or EBCDIC, or hex) data in that conversation. Packet capturing is performed with the pcap library. The need of promiscuous mode (root permission) still remains.

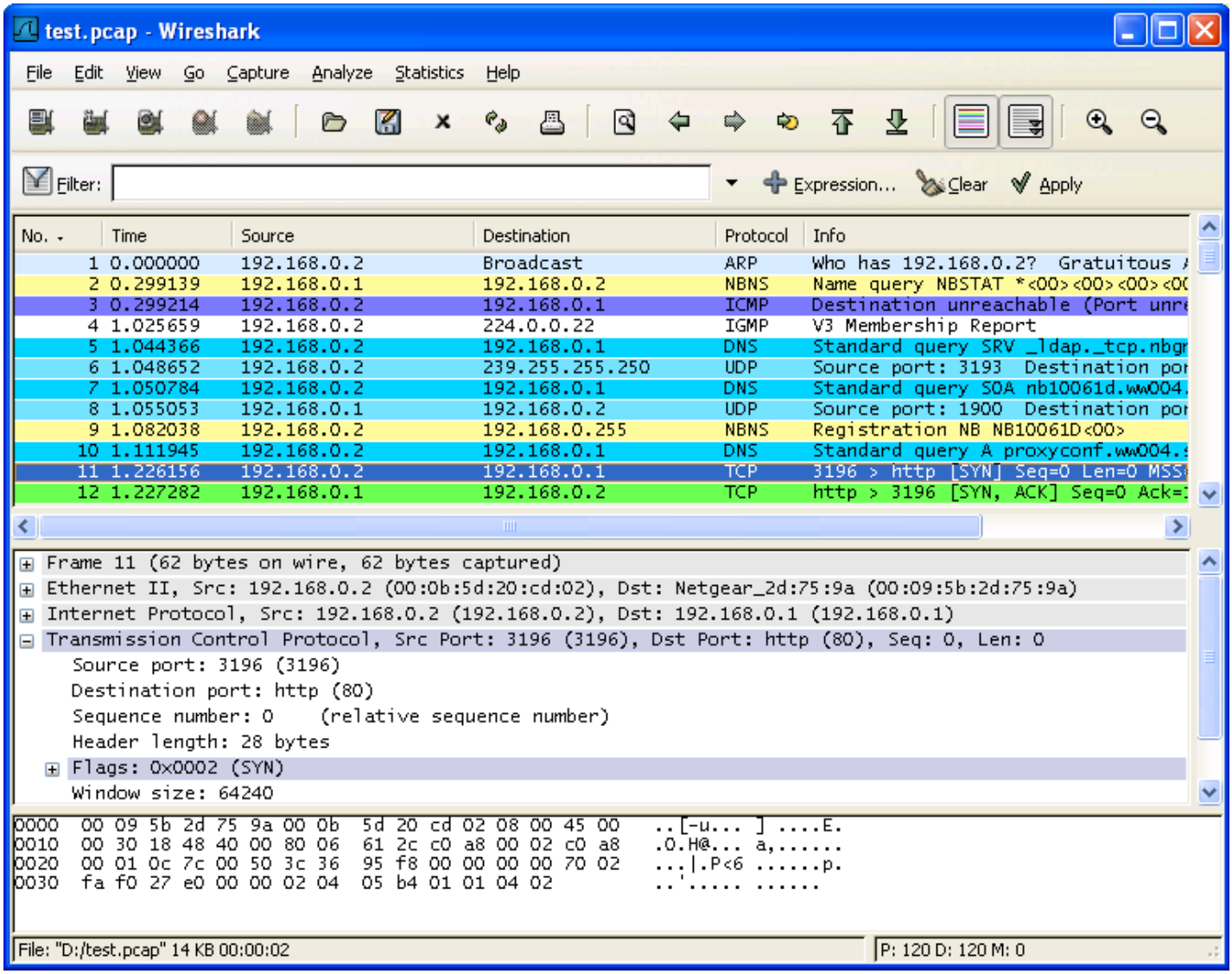

Figure 2.7: Screen snapshot by Wireshark [http://www.wireshark.org/docs/wsug_html]

Most sniffer is for free and provide high performance; however, there are also commercial "sniffer" products which they offer more material and full support with more user-friendly interface and more media supported. As a result, the cost is quite low compared to other kinds of network monitoring tools, i.e. about $200 for "LANWatch". "LANWatch" by Sanstorm Enterprise [LANWatch06] offers the software sniffer with more analysis features and protocol supported such as NetWare, SNA, AppleTalk, VINES, ARP, and NetBIOS.

Due to the prevalent of mobile computers, the new target for most commercial "sniffer" is on wireless networks, since there are not many free "sniffer" applications for wireless networks. For example, although "Wireshark" offers a free sniffer for wired-network, it provides the product called "AirPcap". "AirPcap" is a USB 2.0 wireless capture adapter for Windows system that enables wireless capture with Wireshark. It supports WLAN 802.11b/g. With the external adapter, "AirPcap" can run up to 480Mbps (USP 2.0 bandwidth) with just $200. "OmniAnalysis" [OmniAnalysis06], "WildPackets" offers a complete platform to do a real-time network analysis. The protocol analyzer can support in both wired (EtherPeek) and wireless (AiroPeek) network. This products support Gigabit, 10/100, 802.11 wireless, VOIP, and WAN links diagnostics in real time.

2.3.2 Hardware sniffer (Sniffer)

Although there are a lot of software sniffer available in both freeware and commercial, the question might be asked if hardware sniffer is really needed. Basically, the software sniffer' performance mainly based on the operating system and hardware supported though memory can be added or CPU can be increased, perhaps there might be a bottleneck

such as the disk I/O and memory bandwidth or the operating system call. Thus, the need for monitor and analyzer in enterprise network such as 10Gbps and ATM, hardware sniffer might be required. The hardware sniffer components such as network adapter, memory/disk bandwidth, and buffer management are optimized to do only network monitor and analysis jobs.

"Sniffer" [Sniffer06] by Network Associates, Inc. is an example of the hardware sniffer. It provides the visibility to multi-topology 10/100/1000 Ethernet, 10GbE, WAN, and ATM networks to identify, monitor, measure, and analysis of network problems. "Sniffer" supports real-time analysis, back-in-time analysis, and historical analysis. The logging storage can also be supported for up to four terabytes of storage. Web-based user interface feature allow the administrator do online monitoring remotely.

However, since the performance of personal computer and peripheral such as CPU, memory, and disk have been increasing, the software sniffer is more convenient and popular. From [CAIDA06], there are a few hardware sniffers. However, it seems that only "Sniffer" and "Protocol Analyzer & Exerciser for Advanced Switching Interconnect" by HP are available. "LinkView" and "Shomiti" have no longer access.

Back to Table of Contents

---

3. Comparison of traffic flow information

From all three-traffic flow information by data acquisition techniques we categorized above, from [sFlow03] Table 3.1 shows the comparison of network flow information techniques. We added the sniffer technique in the table. RMON (Remote Monitoring) [RFC 2819, 2000] represents the use of SNMP since RMON is standard used in networking devices such as router, which allows the remote monitoring and management. The standard RMON supports the nine RMON groups of: Statistics, History, Alarms, Hosts, Host Top N, Traffic Matrix, Filters, Packet Capture, and Events. Traffic Matrix and Packet Capture can be used for network flow information.

In the table, Sniffer can be used to capture and analyze the traffic locally, so the information about BGP4 and networking device information cannot be retrieved, and it cannot use SNMP feature. For RMON, since the purpose of RMON is to fetch information from network devices and perhaps to remotely reconfigure the device, only the packet information beyond layer three is available. It does not do much on characterizing traffic patterns and applications. Compared NetFlow and sFlow, it seems that sFlow is much better than NetFlow; however, the documents and utility tools of sFlow are not widespread; there are just a few free tools for sFlow collector and other than that, there are all commercials. Together with NetFlow version 9 chosen to be IPFIX standard, we still see the difficulty for sFlow as a good competitor for NetFlow.

[sFlow03] also claims that to implement NetFlow feature, the networking device is better high performance that results in high cost; however, "fprobe" [fprobe06] and "Softflowd" [Softflowd06]is a small NetFlow probe, which it keeps listening on an interface using libpcap, aggregate the traffic and export NetFlow V5 datagram to a remote collector for processing. "nProbe" [nProbe06] provides the NetFlow probe supporting Gigabit network and simply runs on Unix, Windows, or MaxOS X. Like "fprobe", packet capture uses libpcap. The only limitation is that since the probe does not run on the router, the administrators have to provide AS information. However, "nProbe" provides the utility to extract AS information from Juniper routers. "nProbe" also offers the hardware version named "nBox" with a web configuration interface. Since it is Linux based system, the hardware cost is quite low.

Table 3.1: Comparison of network flow information techniques [sFlow03]

	Sniffer	**RMON (4 groups)**	**RMON II**	**NetFlow**	**sFlow**
Packet Capture	Y	N	Y	N	P
Interface Counters	Y	P	P	N	Y
Protocols:					
Packet headers	Y	N	P	N	Y
Ethernet/802.3	Y	N	Y	N	Y

IP/ICMP/UDP/TCP	Y	N	Y	Y	Y
IPX	Y	N	Y	N	Y
Appletalk	Y	N	Y	N	Y
Layer2:					
Input/Output interface	Y	N	N	Y	Y
Input/Output priority	Y	N	N	N	Y
Input/Output VLAN	Y	N	N	N	Y
Layer3:					
Source subnet/prefix	Y	N	N	Y	Y
Destination subnet/prefix	Y	N	N	Y	Y
Next hop	N	N	N	Y	Y
BGP4					
Source AS	N	N	N	P	Y
Destination AS	N	N	N	P	Y
Destination Peer AS	N	N	N	P	Y
Communities	N	N	N	N	Y
AS Path	N	N	N	N	Y
Real-time data collection	Y	Y	Y	P	Y
Configuration without SNMP	N	N	N	Y	Y
Configuration via SNMP	N	Y	Y	N	Y
Low Cost	Y	Y	N	N	Y
Scalable	N	P	N	N	Y
Wire-speed	Y	Y	P	P	Y

N: Feature not supported, P: Feature partially supported, Y: Fully supported

Back to Table of Contents

---

4. Summary

As the network keeps growing, the need of network monitoring and analysis tools have been increasing. The administrators' jobs are to not only monitor if there is a network failure and fix the network problem on time, but also avoid the network failure because of network overload or outside threat. The network traffic information is used to meet the administrators need. For example, network utilization and network traffic characteristics can detect security vulnerabilities. And, the type of application consuming bandwidth can be used for network planning.

In this paper, we categorized network traffic into three categories: network traffic from NetFlow-like devices, network traffic from SNMP, and local traffic from packet sniffers. Some popular free and commercial tools are described with their features and operating system compatibility detail. A comparison based on these categories has been made that uses each technique depending on what the administrators want. For example, SNMP is more suitable for remote management and configuration, but less information can be retrieved to do further network traffic analysis. A packet sniffer is a local tool where the device is attached. NetFlow-like information is very useful for further analysis, but the limitations remain, such as high cost implementation and privacy concerns.

Back to Table of Contents

---

5. References

[Cisco, NetFlow06a] Cisco Systems, "Cisco CNS NetFlow Collection Engine". http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/index.html

[Cisco, NetFlow06b] Cisco Systems, "Cisco NetFlow site reference". http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd80406232.shtml

[Wikipedia, NetFlow06] Wikipedia, "NetFlow," Free encyclopedia 2006. http://en.wikipedia.org/wiki/NetFlow

[sFlow03] sFlow, "Traffic Monitoring using sFlow", 2003. http://www.sflow.org/

[RFC3176, 2001] P. Phaal, S. Panchen, and N. McKee, "InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks", Request for Comments: 3176, September 2001. http://www.rfc-archive.org/getrfc.php?rfc=3176

[Wikipedia, sFlow06] Wikipedia, "sFlow", Free encyclopedia 2006. http://en.wikipedia.org/wiki/SFlow

[S. Romig et all., 2000] S. Romig, M. Fullmer, and R. Luman., "The OSU flowtools package and CISCO NetFlow logs", In Proceedings of the 14th Systems Administration Conf, LISA 2000. http://www.usenix.org/events/lisa00/full_papers/fullmer/fullmer_html/

[cflowd98] CAIDA, "cflowd: Traffic Flow Analysis Tool". http://www.caida.org/tools/measurement/cflowd/design/design-1.html

[flowd06] "Flowd" http://www.mindrot.org/projects/flowd/

[IETF charters (ipfix)06] IETF charters, "Internet Protocol Flow Information eXport", 2006. http://www.ietf.org/html.charters/ipfix-charter.html, http://tools.ietf.org/wg/ipfix/

[D. Plonka, 2000] D. Plonka, "Flowscan: A network traffic flow reporting and visualization tool", In USENIX LISA, December 2000. http://www.usenix.org/events/lisa00/full_papers/plonka/plonka_html/index.html

[PRTG06] "Paessler Router Traffic Grapher". http://www.paessler.com/

[S. Leinen, 2000] S. Leinen, "Fluxoscope - A System for Flow-based Accounting", Deliverable ID: CATI-SWI-IM-P-000-0.4, March 2000. http://www.tik.ee.ethz.ch/~cati/deliv/CATI-SWI-IM-P-000-0.4.pdf

[Cristian Estan et all., 2003] Cristian Estan, Stefan Savage, and George Varghese, "Automatically Inferring Patterns of Resource Consumption in Network Traffic". SIGCOMM 2003. http://www.cs.ucsd.edu/users/cestan/papers/p0403-estan.pdf

[R. Sabatino, 1998] R. Sabatino, "Traffic Accounting using NetFlow and Cflowd", Fourth International Symposium on Interworking, Ottawa, Canada, July 1998. http://archive.dante.net/pubs/dip/32/32.pdf

[Tobias Oetiker, 1998] Tobias Oetiker, "MRTG: The Multi Router Traffic Grapher", LISA 1998. http://www.usenix.org/publications/library/proceedings/lisa98/full_papers/oetiker/oetiker.pdf

[Net::sFlow06] Elisa Jasinska, "Net::sFlow - decode sFlow datagrams". http://search.cpan.org/~elisa/Net-sFlow-0.05/sFlow.pm

[sFlow Toolkit06] InMon Cooperation, "sFlow Toolkit". http://www.inmon.com/technology/sflowTools.php

[pmacct06] "pmacct now integrates sFlow and NetFlow probes". http://www.pmacct.net/

[Lancope06] Lancope Network Behavior Analysis (NBA) and response http://www.lancope.com/

[Infosim StableNet06] Infosim StableNet Network Management made Easy http://www.infosim.net/

[InMon Traffic Sentinel06] "InMon Traffic Sentinel Complete network visibility and control".

http://www.inmon.com/products/trafficsentinel.php

[Wikipedia RMON06] Wikipedia, "RMON", Free encyclopedia 2006. http://en.wikipedia.org/wiki/Rmon

[RFC2819, 2001] PS. Waldbusser, "Remote Network Monitoring Management Information Base", Request for Comments: 2819, May 2000.http://www.rfc-editor.org/rfc/std/std59.txt

[DPS Telecom06] DPS Telecom http://www.dpstele.com/library/#tutorials

[snmpget05] "snmpget - communicates with a network entity using SNMP GET requests". http://net-snmp.sourceforge.net/docs/man/snmpget.html

[SNMPGet03] "CCSchmidt Software Network Monitoring Software and Utilities". http://software.ccschmidt.de/index.html

[Inftraf05] "CCSchmidt Software Network Monitoring Software and Utilities". http://software.ccschmidt.de/

[Cricket06] "Cricket: high performance, extremely flexible system for monitoring trends in time-series data". http://cricket.sourceforge.net/

[Sniffer06] Sniffer InfiniStream.http://www.networkgeneral.com/Products_details.aspx?PrdId=20046117180712

[OmniAnalysis06] OmniAnalysis. http://www.wildpackets.com/products/omni/overview

[tcpdump06] "tcpdump". http://www.tcpdump.org/

[WinPcap06] "WinPcap". http://www.winpcap.org/

[WinDump06] "WinDump". http://www.winpcap.org/windump/install/

[MNN06] "Microsoft Network Monitor". http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netmon/netmon/network_monitor.asp

[nettl/ netfmt00] "HOW TO TAKE A NETWORK TRACE ON HP-UX". http://www.compute-aid.com/nettl.html

[snoop05] "snoop". http://docs.sun.com/app/docs/doc/816-5166/6mbb1kqh9?a=view

[tcpdump2ASCII04] "tcpdump2ASCII". http://www.Linux.org/apps/AppId_2072.html

[tcpshow05] "tcpshow: Network Security Tools". http://www.tcpshow.org/

[tcptrace04] "tcptrace". http://jarok.cs.ohiou.edu/software/tcptrace/tcptrace.html

[tcpstat04] "tcpstat". http://www.frenchfries.net/paul/tcpstat/

[Wireshark06] "Wireshark". http://www.wireshark.org/

[Softflowd06] "Softflowd". http://www.mindrot.org/softflowd.html

[fprobe06] "fprobe". http://sourceforge.net/projects/fprobe/

[nProbe06] "nProbe". http://www.ntop.org/nProbe.html

[Deri, L. and Suin, S. et all., 2000] Deri, L. and Suin, S., "Effective traffic measurement using ntop", Finsiel SpA, Italy, Communications Magazine, IEEE Volume: 38, Issue: 5, On page(s): 138-143, May 2000. http://citeseer.ist.psu.edu/337108.html

[V. Jacobson et all., 1993] V. Jacobson, C. Leres, and S. McCanne, "tcpdump dump traffic on a network", UNIX man page, 1993. http://www.tcpdump.org

[Pande, Bet all., 2005] Pande, B., Gupta, D., Sanghi, D., and Jain, S.K., "The network monitoring tool PickPacket," Information Technology and Applications, 2005. ICITA 2005. Third International Conference, Volume 2, Page(s):191 - 196 vol.2 4-7 July 2005.http://citeseer.ist.psu.edu/687576.html

[Hong, J.W., 2004] Hong, J.W. "Internet traffic monitoring and analysis using NG-MON", POSTECH, Advanced Communication Technology, 2004. The 6th International Conference, Volume: 1, page(s): 100- 120, 2004. http://ieeexplore.ieee.org/iel5/9073/28786/01292840.pdf

[Junejo, N., 2004] Junejo, N., Junejo, N.A., and Unar, M.A., "MENeT a monitoring and protocol analysis tool for LAN", Advances in Wired and Wireless Communication, page(s):63 - 66, 2004. http://ieeexplore.ieee.org/iel5/9131/28948/

[Ioannidis, S et all., 2002] Ioannidis, S., Anagnostakis, K.G., Ioannidis, J., and Keromytis, A.D., "xPF: packet filtering for low-cost network monitoring", Department of Computer and Information Science, Pennsylvania Univ., Philadelphia, PA, USA, High Performance Switching and Routing, 2002. Merging Optical and IP Technologies, page(s): 116- 120, 2002. http://www1.cs.columbia.edu/~angelos/Papers/xpf.pdf

[Priyantha Pushpa Kumara and Gihan V Dias, 2002] Priyantha Pushpa Kumara and Gihan V Dias, "LEARNStat: A Network Traffic Monitoring Utility", INET2002. http://www.inet2002.org/CD-ROM/lu65rw2n/papers/p06.pdf

[Costas Courcoubetis and Vasilios A. Siris, 2002] Costas Courcoubetis and Vasilios A. Siris, "Procedures and Tools for Analysis of Network Traffic Measurements", 2002. http://citeseer.ist.psu.edu/courcoubetis02procedures.html

[Wu-chun Feng et all., 2001] Wu-chun Feng, Hay, J.R., and Gardner, M.K., "MAGNeT: monitor for application-generated network traffic", Computer and Computational Science Division, Los Alamos Nat. Lab., NM, Computer Communications and Networks, 2001. Proceedings. Tenth International Conference, page(s): 110-115, 2001. http://ieeexplore.ieee.org/iel5/7587/20684/00956227.pdf

[Malgosa-Sanahuja, J et all., 2001] Malgosa-Sanahuja, J., Cano, M.D., Cerdan, F., and Garcia-Haro, J., "TAT: traffic analysis tool for the statistical study of IP networks", Department of Infomation Technology and Communication, Polytech. University of Cartagena; Communications, Computers and signal Processing, 2001. PACRIM. 2001 IEEE Pacific Rim Conference, Volume: 2, page(s): 579-582 vol.2, 2001. http://citeseer.ist.psu.edu/737234.html

[McGregor, T et all., 2000] McGregor, T., Braun, H.-W., and Brown, J., "The NLAMR network analysis infrastructure", Waikato University, Hamilton, Communications Magazine, IEEE Volume: 38, Issue: 5, page(s): 122-128, May 2000. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=841836

Tool Collections

[1] ESnet Network Monitoring Task Force (NMTF), "Network Monitoring Tools". http://www.slac.stanford.edu/xorg/nmtf/, http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html

[2] CAIDA, "CAIDA Measurement and Analysis Tools". http://www.caida.org/tools/measurement/, http://www.caida.org/tools/taxonomy/, http://www.caida.org/tools/taxonomy/workload.xml

[3] "Network traffic monitoring software". http://www.topology.org/comms/netmon.html

[4] SWITCH, The Swiss Education & Research Network, "Network Monitoring and Analysis : Flow-Based Accounting". http://www.switch.ch/tf-tant/floma/, http://www.switch.ch/tf-tant/floma/software.html

[5] "Network Monitoring/Management". http://www.cotse.com/tools/netman.htm

[6] "Network Traffic Monitoring". http://www.monitortools.com/traffic/ (http://www.monitortools.com/)

[7] Advanced Laboratory Workstation System, "Network and Network Monitoring Software". http://www.alw.nih.gov/Security/prog-network.html

[8] Comlab, "Tools for modeling the user-traffic". http://www.comlab.uni-rostock.de/research/tools.html

[9] "Traffic Monitoring Software". http://www.programurl.com/software/traffic-monitoring.htm

[10] "Traffic Monitor and Analyzer Tools".http://traffic-analyzer.qarchive.org/, http://traffic-monitor.qarchive.org/

[11] "Tucows.com". http://tucows.com/ (search for network traffic monitoring, network traffic analyzer)

[12] "Download.com". http://www.download.com/ (search for network traffic monitoring, network traffic analyzer)

Research Laboratories

[13] Bell Labs Internet Traffic Research. http://cm.bell-labs.com/cm/ms/departments/sia/InternetTraffic/index.html

[14] Universita' degli Studi di Napoli "Federico II" (Italy), "Network Tools and Traffic Traces". http://www.grid.unina.it/Traffic/index.php

[15] LBNL's Network Research Group. http://ee.lbl.gov/

Back to Table of Contents

---

6. List of Acronyms

HTML	HyperText Markup Language
WMI	Windows Management Instrumentation
ATM	Asynchronous Transfer Mode
Gbps	Gigabit per second
Mbps	Megabit per second
NMTF	Network Monitoring Task Force
RMON	Remote Monitoring
SNMP	Simple Network Management Protocol
NMP	Network Monitoring Platforms
CAIDA	Cooperative Association for Internet Data Analysis
LAN	Local Area Network
WAN	Wide Area Network
UDP	User Datagram Protocol
TCP	Transport Control Protocol
SCTP	Stream Control Transmission Protocol
FTP	File Transfer Protocol
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information eXport
AS	Autonomous System
BGP	Border Gateway Protocol
MPLS	Multiprotocol Label Switching
CPU	Central Processing Unit
RFC	Request for Comments
VLAN	Virtual Local Area Network
ICMP	Internet Control Message Protocol

IPX	Internetwork Packet Exchange
IETF	Internet Engineering Task Force
MIB	Management Information Base
PDU	Protocol Data Unit
NMTF	Network Monitoring Task Force
RRDtool	Round Robin Database Tool
VOIP	Voice Over Internet Protocol
GUI	Graphic User Interface
PNG	Portable Network Graphics
OID	Object identifier
EBCDIC	Extended Binary-Coded Decimal Interchange Code
ASCII	American Standard Code for Information Interchange
IOS	Internetworking Operating System

Back to Table of Contents

7. Appendix A: List of Network Traffic Monitoring and Analysis Tools

Table 7.1: Free NetFlow utility tools

Tool	OS	Functions
flow2rrd	N/A	A "Flow-Tools" toolkit for storing NetFlow data in an Round-Robin-Database
NetFlow2MySQL, NetFlow2XML	Linux, FreeBSD	NetFlow2MySQL is software to store contents of NetFlow packets into MySQL databases. NetFlow2XML is software to convert NetFlow packets into XML format.
Panoptis	Unix-liked	Uses NetFlow accounting data to detect (Distributed) Denial of Service attacks
SiLK	Linux, Solaris, OpenBSD, Mac OS X	A collection of NetFlow tools (by CERT/NetSA (Network Situational Awareness)) to assist the security analysis in large networks
UDP Samplicator	N/A	A redistribution NetFlow data stream to multiple receivers
UPFrame	Linux, FreeBSD	This NetFlow processing framework for real-time processing

The tables below are tools, the lists are made from [1] to [10] but only for network traffic monitoring and analysis purpose from [1] to [10]. **All descriptions are from the references.**

Please Click Here to go to Table 7.2 to 7.7

- Table 7.2: Free network monitoring and analysis tools
- Table 7.3: Free network utility tools
- Table 7.4: Free network monitoring and analysis tools (protocol specific)
- Table 7.5: Commercial NetFlow monitoring and analysis tools
- Table 7.6: Commercial network monitoring and analysis tools
- Table 7.7: Commercial network monitoring and analysis tools (protocol specific)

Back to Table of Contents

This report is available on-line at http://www.cse.wustl.edu/~jain/cse567-06/net_traffic_monitors3.htm

List of other reports in this series
Back to Raj Jain's home page