SNMP and Beyond: A Survey of Network Performance Monitoring Tools

Paul Moceri, paul.moceri@gmail.com

Abstract
The growing dependence on networks for everyday tasks has created the demand for high performance, reliable networks. Part of achieving the goal of high performance is active monitoring of networks to help in the identification and prevention of network errors. Many tools have emerged to aid in performance monitoring of networks. The most common class of tools is based on the Simple Network Management Protocol (SNMP), a protocol for sending and transmitting network performance information on IP networks. Other types of network performance monitoring tools include packet sniffers, flow monitors and application monitors. Examples of the various monitoring tools are SolarWind's Orion SNMP monitoring platform, Ethereal packet capture tool, Webmetrics' GlobalWatch and Cisco's NetFlow flow monitoring tools.

KeywordsNetwork Performance, Network Monitoring, Network Performance Tools, SNMP, Integrated SNMP Monitoring, Network Flow Monitoring, Application Monitoring, Packet Sniffing, Ethereal, SolarWinds Orion, Cisco NetFlow, Webmetrics.

Table of Contents

1. Introduction

Computer networks have become a huge part of everyday life. The world without computer networks is practically unimaginable. Every action, event and transaction in our modern world at some point crosses a network. And, ever since the days that networks emerged there has been the desire to ensure that they perform optimally. This has lead to the development of numerous network performance monitoring tools and standards. The most common tools are network management system based on standardized network management protocols that give a comprehensive view of a network and all of its devices. Of course, there are other tools that are not as complex as a full network management system but equally useful for monitoring certain aspects of network performance.

This survey paper will cover the basics of network performance monitoring, standards for network management and different types of monitoring tools. It will conclude with a look at several different monitoring tools including commercial and open-source implementations.

1.1 Terminology

The following definitions are important for understanding the basics of network management and performance monitoring and will be used throughout this survey paper.

Agent The software that runs on a managed network device and implements the information and/or management functionality of a management system.

Managed Device Any network device that is capable of participating in a network management system.

Management Information Base (MIB) A hierarchical specification of the management data on a managed network device.

Management Station The software that sends requests to agents and receives traps on behalf of an administrator or management software. Also known as the Manager.

Network-Management System (NMS) A complete hardware and software system that monitors and manages a network.

Simple Network Management Protocol (SNMP) A network protocol that is part of the Internet Protocol suite used to send and receive network management information.

Trap Asynchronous messages sent by agents to managers. May be used for alerts or event notifications. Also known as Notification.

1.2 Overview of Network Performance Monitoring

The most popular means of monitoring network performance are network management systems. A network management system, as depicted in Figure 1, consists of a centralized network management station and management agents running on network devices [Cisco06]. Using a management protocol, the management station polls agents for information about the network devices. Agents return requested information ranging from bandwidth usage to CPU load. Using this information, the network management system provides performance and error reporting to network administrators.

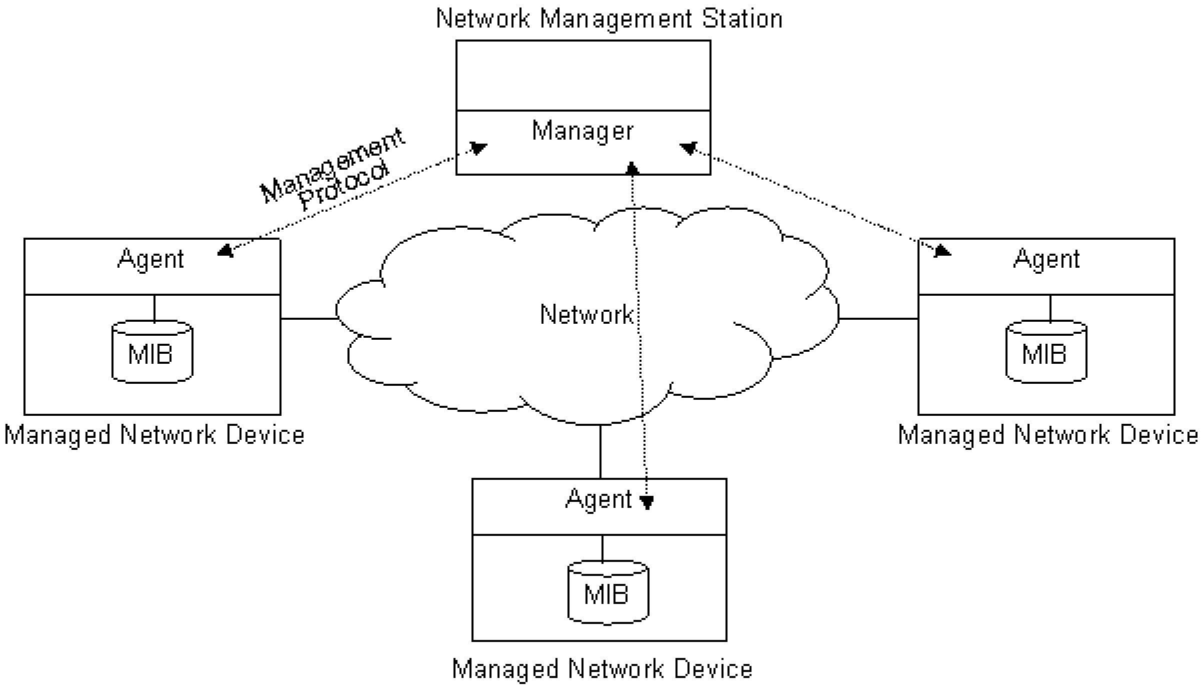

Figure 1 A network management system composed of a management station and several agents.

Network management systems are by no means the only form of network monitoring. This survey will cover several other types of network monitoring tools including packet captures tools, flow monitors and application monitors in addition to network management systems. Before covering specific types of monitoring tools, it is important to understand what information monitoring tools provide to network administrators and the metrics they use.

1.3 Common Performance Metrics

Network performance monitoring tools provide a variety of information to network administrators and engineers through the use of various performance metrics. The most commonly talked about metrics in the networking arena are availability, throughput, bandwidth utilization, and latency (or delay). However, administrators are also often interested in error rates and the performance of network devices including CPU and memory utilization and delay (or latency). Each of these metrics can be classified as *lower is better* (LB), *higher is better* (HB) or *nominal is best* (NB). This classification system is taken from [Jain91] page 40. Table 1 lists the mentioned performance metrics, their classification and a description of why they are useful.

Table 1 Various performance metrics useful for network administration and engineering. Metrics are classified as *lower is better* (LB}, *higher is better* (HB), or *nominal is best* (NB) [Jain91].

Metric	Classification	Description
Availability	HB	Measure of what percentage of the time a network resource is available for use. Clearly, high availability is better because down time is not welcome.
Throughput	HB	A measure of how much data can be sent on or through a network resource in a given time period. Also referred to as available bandwidth. Higher throughput is certainly better from users' and administrators' points of view.

Utilization	NB	Measure of the usage of a link, port, or network resources. Nominal is best because high utilization is accompanied by high delays and low utilization is seen as a poor use of resources.
Delay	LB	The amount of time for a packet to traverse, either one-way or round trip, a network, network segment or network device.
Error Rate	LB	Usually refers to the percentage of packets or bits that contain errors on a network link, segment or device. High error rates can signal to an administrator that there is a problem in the network.

Back to Table of Contents

2.0 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is an application-layer protocol in the Internet Protocol suite defined by the Internet Engineering Task Force (IEFT). As its name suggest, SNMP provides a minimalistic protocol for retrieving network performance data and setting network device parameters. SNMP uses a management station that polls and responds to agents running on network devices. The management station is the device responsible for storing, displaying, or processing the network data collected. This lightweight protocol is widely implemented in network devices and used by network management systems.

2.1 Role of SNMP in Network Performance Monitoring

SNMP provides network management systems with the means to collect network performance data as well as set parameters on network devices as part of administration of those devices. SNMP itself does not process or analysis network traffic information. Rather, it provides the messaging interface that allows network management systems to acquire the information necessary to analyze network performance. In this way, SNMP is a vital component of many network performance monitoring tools. SNMP allows the management station to request network information from agents located on various network devices and also allows those agents to send event notices to the management station. The data objects that SNMP sends are described and stored in a management information base.

2.2 Management Information Base (MIB)

A MIB is a database used to store management information in networks. MIBs are used by network management systems to identify network data objects that are stored, retrieved and set by the system. A MIB uses a hierarchical tree structure to store an extensible collection of data. A subset of Abstract Syntax Notation One (ASN.1) is used to specify an object. The MIB used for SNMP is standardized; however, it allows private organizations to insert custom objects into the structure. Figure 2 shows part of the MIB structure of SNMP. Properties pertaining to Internet devices are found below iso.org.dod.internet (1.3.6.1). An individual organization can extend the standard MIB defined by SNMP by adding to the tree below an assigned node under iso.org.dod.internet.private.enterprises (1.3.6.1.4.1). Cisco for example has been assigned number 9 under enterprises. So, Cisco creates MIBs entries for its own devices under iso.org.dod.internet.private.enterprises.cisco (1.3.6.1.4.1.9).

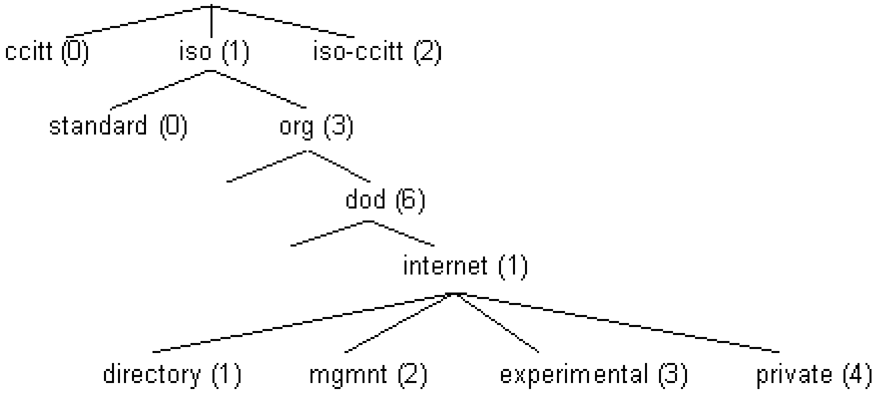

Figure 2 Partial depiction of the MIB naming hierarchy used by SNMP.

2.3 Versions and Interface

SNMP, currently in its third version, was first introduced in 1988. The first version, commonly referred to as SNMPv1, supported five message types which continue to be supported in the current version. The GET REQUEST and GETNEXT REQUEST messages are used by a management station to request the value of a network data object and the next value in a sequence, respectively. GET RESPONSE messages are sent by agents in response to GET and GETNEXT requests. Management stations send SET REQUEST messages to set the value of a parameter on a network device. Finally, agents asynchronously send TRAP messages to notify management stations of events. All management station requests are sent to agents on port 161 and agents send TRAP messages to management stations on UDP port 162. Source and response port numbers are unspecified and can be any unused port. Figure 3 shows how SNMP fits into the network stack. In particular, it shows SNMP on a simple network device that only provides the SNMP application and SNMP on a system that also provides user applications such as HTTP or FTP.

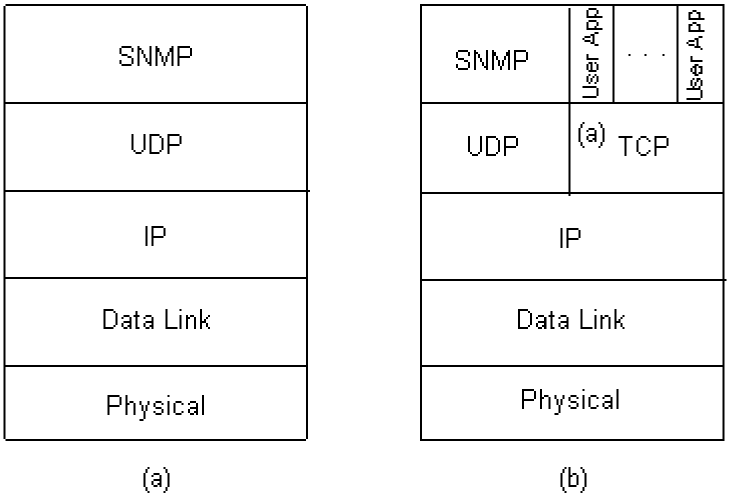

Figure 3 a) SNMP running on top of UDP in a network device. b) SNMP running on top of UDP in a system that also provides user applications.

SNMPv2 added two new message types that are also carried into the SNMPv3. GETBULK made sequential requests more efficient by allowing a management station to request an entire block in a sequence rather than having to iterate over a sequence using GETNEXT. The INFORM message is another version of TRAP that is acknowledged by the management station. SNMPv3 added security to the protocol making it in the preferred version to use. Detailed specification of the standard can be found in IETF [RFC3411] -

[RFC3418]. Table 2 summarizes the message types used by all of the SNMP versions.

Table 2 SNMP message types and description of their functionality. All message types are supported by SNMPv1 and later unless otherwise specified.

Message	Usages
GET REQUEST	Used by Manager to retrieve a specific piece of network information.
GETNEXT REQUEST	Used by Manager to iteratively retrieve a sequence of information.
GET RESPONSE	Used by agent to send information to Manager in response to a request.
SET REQUEST	Used by a Manager to initialize or change the value of an management object.
TRAP	Used by agent to report an alert or other asynchronous event to the Manager.
GETBULK	Introduced in SNMPv2 to retrieve a sequence of information as a faster alternative to GETNEXT.
INFORM	Introduced in SNMPv2, an acknowledged version of TRAP.

Because of the various dependencies and levels of adoption of the different versions of SNMP, it is very common to see network devices and network management systems that implement all three version of the standard. In fact, the IETF Network Working Group published an entire RFC on the subject of coexistence of the three versions of SNMP [RFC3584]. This document describes everything from how to convert between MIB formats and parameter mappings to approaches for multi-lingual network support.

Back to Table of Contents

3.0 Types of Monitoring Tools

Network performance monitoring tools vary from simple one device applications to complex hierarchical system. These systems employ a variety of monitoring techniques. Some systems use passive monitoring to gather information about network traffic while others actively poll network devices to gather network performance data. Still, more variation is seen in the network layer that various tools work at. Some tools monitor data link performance while other monitor network performance all the way up to the application layer.

3.1 Integrated SNMP Monitoring Platforms

An integrated SNMP Network Management System is one that leverages SNMP to give a complete view of a network. Integrated monitoring platforms actively collect network information from network devices and analyze the data. Network administrators have the flexibility to decide which parameters they want to monitor and how the information is reported. Most integrated platforms provide graphic reporting, monitoring, and administration of networks allowing easy management and setup of monitoring. Complete monitoring systems provide detailed and comprehensive analysis of network performance. Common performance characteristics include bandwidth utilization, throughput, response time, and error rates as well as CPU load and memory utilization of the network equipment and servers. In addition to real-time monitoring and reporting, SNMP network management systems also provide alerts based on any of the monitored performance characteristics.

3.2 Passive Analysis

Passive network performance tools, also called packet capture tools or packet sniffers, are the class of network tools that do not generate any traffic themselves while collecting data. Instead, the analyzer merely listens to traffic that is on the network. This fundamentally limits the breadth of analysis generated by passive tools because they can only see traffic that is local to the device running the analyzer. For example, in a switched Ethernet environment, a passive system would only see traffic sent to or from its host [PacketSniffer].

3.3 Application and Service Monitoring

Application and service monitoring refers to the class of performance monitoring tools that provide monitoring of individual network applications. Application monitoring depends less on the network equipment and infrastructure and more on the actual servers that provide user services. Such tools provide reporting on application availability, utilization and performance as well as performance characteristics of the underlying server. One common use for application monitoring is website availability monitoring. However, other uses can be built on protocols and services much more complex than HTTP. Database monitoring may consist of transaction rate, server load, memory and disk usage, and concurrent connection count. Administrators can use this information to easily identify and resolve application problems and evaluate infrastructure performance for bottlenecks or excess capacity.

3.4 Flow Monitoring

Instead of looking at traffic from a packet level, flow monitoring analyzes network traffic as flows. Flow monitoring aggregates network traffic based on individual connections, users, protocols, or applications. This allows flow monitoring tools to provide a bigger picture view of a network including specific information on application and connection performance as well as insight into routing and even network security. This view of the network performance aids in network planning as well as traffic engineering because of the traffic trends flow monitoring is able to identify [CiscoNF].

3.5 Comparison of Performance Monitoring Tool Types

Table 3 summaries the different types of monitoring tools and highlights the differences among them. The majority of the types are active which makes them much more comprehensive. Also, the different systems vary a great deal in which layer or layers of the network stack they operate in.

Table 3 Comparison of different types of network performance monitoring tools.

Type	Passive or Active	Network Layer of Operation	Basic Operation
Integrated SNMP Platform	Active	Data Link and Network	A management station polls agents on network devices to gather information about the network
Packet Capture/Sniffing	Passive	Data Link	Listens for and captures packets on a network device for analysis
Application/Service Monitoring	Active	Application	Actively polls applications and application servers to provide performance information
Flow Monitoring	Active	Transport and Higher	Monitor connections and flows on the network for higher layer trends

Back to Table of Contents

4.0 Example Implementations

There are countless different network performance tools of varying type available today. Commercial products as well as open-source projects provide options for monitoring networks. The intent of this survey is not to be a comprehensive listing of performance monitoring tools but rather to give a glimpse of the variety of tools available. A fairly comprehensive list of different tools can be found in [Cottrell06].

4.1 Integrated SNMP: SolarWinds' Orion Network Performance Monitor

SolarWinds provides a variety of network management solutions ranging from individual monitoring tools to complete, full-featured monitoring platforms. Orion is their comprehensive monitoring solution built on SNMP. The Orion management application features a web interface with real-time monitoring of availability, bandwidth utilization, network latency and many other network performance metrics. The system automatically summarizes data and prioritizes events and alerts for easy monitoring and troubleshooting. Each event, statistic or alert also has a drill-down feature which provides all of the details on a given piece of information. This interface is also customizable with the ability to visually map network components and links, further easing the process of monitoring and finding errors.

Despite the complexity and variety of information provided by Orion, the program is still easy to use. As discussed above, SNMP only provides the messaging format used in a network management system; individual devices must still be configured to work with a particular management system. So, Orion includes auto-discovery and auto-configuration features that simplify the process of adding network devices to be monitored. This is only a brief overview of Orion. Complete details of the Orion Network Performance Monitor can be found at [SolarWinds]

4.2 Passive Capture Tool: Ethereal

Ethereal is an open source packet capture tool for Ethernet networks that captures packets off of network interface cards for analysis. Although Ethereal does not calculate performance statistics on captured traffic, it does analyze individual packets and determines their type as well as values of fields specific to individual protocols. It also provides filtering of packets based on protocol as well as other characteristics such as addresses and port numbers [Ethereal]. Ethereal is a two-piece software program available on the Windows, Mac and Unix operating systems. A capture library enables Ethereal to capture packets off the network interface while a graphic user interface allows administrators to view and analyze captured packets.

4.3 Application and Service Monitoring: Webmetrics GlobalWatch

Webmetrics GlobalWatch provides performance and availability monitoring for a variety of web applications including static and dynamic webpages, DNS, web transactions, Java and flash applets and more. Webmetrics utilizes a network of globally distributed monitoring agents to continuously poll websites and gather performance information. This agent network allows Webmetrics to obtain performance measurements such as response time, throughput, and availability from a similar vantage point as actual users. Webmetrics customers can use this information to monitor real user experience and react to errors and performance degradation [Webmetrics].

4.4 Network Flow Monitoring: Cisco IOS NetFlow

Cisco IOS NetFlow is a complete network monitoring system used to collect and analyze network flows. NetFlow relies on routers to collect information on network flows which are identified as packet sequences that share the same IP protocol and source and destination addresses and ports. Flow information from all network devices is sent to a NetFlow collector to be analyzed. Cisco's IOS NetFlow application uses this NetFlow information to provide a variety of information and services including user and application monitoring, network planning, traffic engineering, usage accounting, and security analyzing [CiscoNF]. Compared to an SNMP-based monitoring platform, NetFlow is able to give a much more detailed view of the network user behavior and usage patterns.

Though originally developed by Cisco, other network equipment vendors support NetFlow in their products. IEFT has even created an RFC for IP Flow Information eXport (IPFIX) which is based off of Cisco's NetFlow version 9 [RFC3954]. Not all network administrators need the detailed network view provided by a flow monitoring tool; however, NetFlow is becoming a much more common tool in the network administrator's toolbox [Zwers06].

Back to Table of Contents

5.0 Summary

Network performance monitoring is an important part of network functionality. Society has become dependent on networks and their ability to perform optimally is crucial. As a result, numerous network performance monitoring tools have emerged. Many of these are based on the standardized management protocol SNMP and provide administrators a complete view of a network and it performance.

SNMP provides the messaging capability for management systems to collection network data for analysis. First introduced in 1988, SNMP is now in its third version and provides a secure messaging format. SNMP monitoring tools are some of the most flexible and comprehensive because of their ability to selectively poll any network device for exactly the information they need. SolarWind's Orion Network Performance Monitor is one example of an SNMP-based performance monitoring tool.

However, many other types of tools are also available. Ethereal provides a tool for capturing and analyzing individual packets off of a network. Webmetrics GlobalWatch is an application performance monitoring tool that utilizes distributed agents to continuously monitor the performance of web applications. And finally, network flow monitoring tools provide an increasingly popular means of monitoring network performance. Cisco's NetFlow architecture provides flow monitoring, aggregation, and analysis and has even gone to IETF as an Internet draft. As the trend towards higher performance networks continues, more comprehensive monitoring tools like NetFlow will become as commonplace as SNMP today.

Back to Table of Contents

References

The following references are roughly arranged in order of usefulness and relevance to the above paper.

[RFC3411] D. Harrington, R. Presuhn, B. Wijnen. "RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks" IETF, Network Working Group, December, 2002. http://tools.ietf.org/html/rfc3411
The first of eight RFCs that form a full definition of SNMPv3.

[RFC3418] R. Presuhn. "RFC 3418: Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)" IETF, Network Working Group, December, 2002. http://tools.ietf.org/html/rfc3418
The eighth RFC of eight that form a full definition of SNMPv3.

[RFC1155] M. Rose, K. McCloghrie. "RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets" IETF, Network Working Group, May, 1990. http://tools.ietf.org/html/rfc1155
Describes the structures and identification used to define management information in SNMPv1.

[RFC1156] K. McCloghrie, M. Rose. "RFC 1156: Management Information Base for the Simple Network Management Protocol (SNMP)" IETF, Network Working Group, December, 2002. http://tools.ietf.org/html/rfc1156
The definition of the initial Management Information Base (MIB) for SNMPv1.

[RFC1157] J. Case, M. Fedor, M. Schoffstall, J. Davin. "RFC 1157: A Simple Network Management Protocol (SNMP)" IETF, Network Working Group, December, 2002. http://tools.ietf.org/html/rfc1157
The SNMPv1 definition as published by IEFT.

[Cottrell06] Cottrell, Les. "Network Monitoring Tools." SLAC, Stanford University. October 29, 2006. http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html
A comprehensive list of network monitoring tools and links to more information for each tool.

[Jain91] Jain, Raj. "The Art of Computer Systems Performance Analysis" New York: John Wiley & Sons, Inc., 1991.
Full textbook that covers experimental design, measurement, simulation and modeling.

[SolarWinds] "Orion Network Performance Monitor Datasheet" SolarWinds, accessed November 2006. http://solarwinds.net/resources/datasheets/OrionDatasheet.pdf
Overview of features and functionality of the Orion Network Performance Monitor from SolarWinds.

[Ethereal] "Ethereal: A Network Protocol Analyzer" Website. Ethereal, Inc. November 11, 2006. http://www.ethereal.com/
Offical website of the Ethereal Network Protocol Analyzer. Contains feature information as well as documentation.

[Webmetrics] "Application Monitoring and Web Transacation Monitoring" Webmetrics website. Accessed November 28, 2006. http://www.webmetrics.com/globalwatch.html
Offical website of Webmetrics. Contains product information.

[Stallings98] Stallings, W. "SNMPv3: A Security Enhancement for SNMP."IEEE Communications Surveys & Tutorials, vol. 1, no. 1, Fourth Quarter 1998 pp. 2-17. http://www.comsoc.org/livepubs/surveys/public/4q98issue/stallings.html
Overview of SNMPv3 and the security improvements it provides to SNMP.

[Cisco06] "Network Management Basics." Cisco Systems Inc, Octber 12, 2006. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm
Basic overview of network management systems.

[PacketSniffer] "Packet sniffer - Wikipedia." Wikimedia Foundation, Inc, accessed November 25, 2006. http://en.wikipedia.org/wiki/Packet_sniffer
Definition and overview of packet sniffers and packet capture tools.

[CiscoNF] "Cisco IOS NetFlow" Cisco Systems Inc, accessed November 20, 2006.

http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
Homepage for Cisco's IOS NetFlow network monitoring solution.

[RFC3954] B. Claise, Ed. "RFC 3954: Cisco Systems NetFlow Services Export Version 9" IETF, Network Working Group, October, 2004. http://tools.ietf.org/html/rfc3954
Full protocol definition of Network services export protocol version 9.

[Zwers06] Zwers, Joe. "sFlow vs. NetFlow: What is the big difference and which should you support?" Enterprise Networks & Servers. November, 2006.
http://www.enterprisenetworksandservers.com/monthly/art.php?2812
An article that compares NetFlow and similar technology sFlow.

Back to Table of Contents

Acronyms

HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
MIB	Management Information Base
NMS	Network Management System
RFC	Request For Comments
SNMP	Simple Network Management Protocol
SNMPvN	Simple Network Management Protocol version N
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USM	User Security Model

Back to Table of Contents

This report is available on-line at http://www.cse.wustl.edu/~jain/cse567-06/net_traffic_monitors2.htm
List of other reports in this series
Back to Raj Jain's home page