A Survey of Network Performance Monitoring Tools

Travis Keshav -- traviskeshav@hotmail.com

Abstract

In today's world of networks, it is not enough simply to have a network; assuring its optimal performance is key. This paper analyzes several facets of Network Performance Monitoring, evaluating several motivations as well as examining many commercial and public domain products.

Keywords: *network performance monitoring, application monitoring, flow monitoring, packet capture, sniffing, wireless networks, path analysis, bandwidth analysis, network monitoring platforms, Ethereal, Netflow, tcpdump, Wireshark, Ciscoworks*

Table Of Contents

1.0 Introduction

In today's world of networks, it is not enough simply to have a network; assuring its optimal performance is key. Customers who are turned away or disconnected due to any sort of network failure are likely to change vendors or providers. Consequently, network performance monitoring (NPM) must be done to find these errors quickly, so that they can be corrected as soon as possible.

But, as real-world experience with a network will quickly demonstrate, there is no one single factor that explains all difficulties and failures, nor is there any one level of monitoring that can detect every issue. Attackers from both outside and within may have planted viruses or Trojan Horse programs, which can drain company resources or transmit classified data to unauthorized recipients. Misconfiguration of any aspect of the system can introduce artificial or unnecessary bottlenecks in the network, or may simply cause the existing network capabilities to be used inefficiently. Employees may be using the network for their personal interests, in violation of policy. Further issues include the possibility of hardware or software failures within a server, causing either erroneous output or none at all.

NPM is a multi-faceted task, with several areas that must be considered: application/host-based monitoring, flow monitoring, packet capture (sniffing), path/bandwidth analysis, and wireless network monitoring. Additionally, some commercial products have been created in order to address many issues simultaneously, and are entitled network monitoring platforms (NMPs). The remainder of this paper will address these aspects of NPM, as well as presenting several freeware and commercial products that can be used to serve these goals.

Back to Table of Contents

2.0 Application & Host-Based Monitoring

Application and Host-Based Monitoring is used to detect suspicious level on a higher protocol level, checking for such issues as susceptible, outdated programs, as well as applications using ports in an unexpected or undesired manner. Dozens of public domain utilities for application monitoring exist, including MoSSHe and OpenSMART. Two commercial programs that merit mentioning and examination are Vantage and AppMonitor.

2.1 Basis of Application & Host-Based Monitoring

For both network-related and individual computing situations, application monitoring can hold great value. Out-of-date software may be introducing vulnerabilities into the system, which an attacker can easily find and exploit. Perhaps the most common example of these is SQL servers, where attackers continuously find methods to execute external code, with each exploit needing a corresponding fix. However, application monitoring can detect the presence of these issues with equal ease, based upon version numbers and lists of vulnerable releases as found on the Internet. Once found, administrators can be alerted to the problem, and a patch can be applied. Application failure may render services inoperable, and leads to customers frustrated with a provider's inability to deliver the promised capabilities. Application monitoring can detect crashes, and logs specific information about the problems as to allow functionality to be restored as quickly as possible.

Malicious software may be detectable through application monitoring, as such programs will usually not conform to a pre-specified list of valid applications. Additionally, these programs can be detected based upon their port accesses, as these may not correspond with normal activity. This information can be used to direct firewalls or other utilities to limit the activities of harmful software. Finally, application monitoring can easily detect program usage that goes against company policy, just as malicious activity can be detected; for example, most Internet messaging programs run on certain ports and under certain names. If not already blocked by a firewall, such applications can be detected by these characteristics, allowing specialized alerts to be sent from the monitoring system.

These application-level analyses can be extended within larger networks to be on a host level. The subtle distinction is that instead of the monitoring focus being specific applications and processes, all hosts within the network must be considered as separate entities and monitored. Again, it is simply a change of nomenclature based upon scale.

2.2 Public Domain Application & Host-Based Monitoring Tools

The first of these free application monitoring tools is Monotoring with SSH Environment (MoSSHe) [MoSSHe] for Unix. This product is designed by Volker Tanger, and allows for simple server monitoring with low resource costs, with a small download size of only 36 KB. MoSSHe performs checks on various critical services, including DNS, HTTP, SMTP, SNMP, and many others. Additionally, reports can be created, which include information concerning hard drives, log examinations, memory, shell usage, and the status of both normal and zombie processes. These are presented in a comprehensive manner, where alerts can be sent to a given e-mail address when measurements indicate threshold parameters have been exceeded. However, MoSSHe's flexibility is somewhat limited; all reports can only be sent to one address, as opposed to delineating a target based upon the type of alert. Furthermore, some corruption of log files is known to occur, even though this product has gone through dozens of incarnations.

Another such free utility is the Open Source/System Monitoring And Reporting Tool (OpenSMART) [OpenSMART]. This monitoring tool, designed by Holger Schultheiss and Ulrich Herbst, monitors applications through agents which report information to a central server. These agents run a data collection script, testing processes, services and protocols including sockets, SQL, DNS, SMTP and FTP. The agents return codes and information corresponding to levels such as 'normal', 'warning' and 'fatal', indicating whether performance is acceptable or substandard to a specified degree. OpenSMART then creates a front-end webpage for the user with CGI scripts. This allows users to examine both the individual hosts in the network and all errors discovered through monitoring, with all results timestamped. Especially useful is the capability to create and store maintenance entries, allowing for administrators to indicate that problems have been noted and are in the process of being fixed. Another positive note is that OpenSMART is frequently tested and examined by the developers, in order to add new functionality and eliminate errors. Recently, a stable version 1.0 has been released, with the server portion having been tested on Linux, MySQL, and Apache, where agents can be deployed to virtually any system.

2.3 Commercial Application & Host-Based Monitoring Tools

One suitable product for providers of larger networks is Vantage [Vantage], developed by Compuware. The goal of Vantage is to examine and analyze application performance on a large scale, examining it in regards to overall network performance, such that interactions between the different levels are not ignored. Additionally, Vantage does not limit itself to clients, but monitors across all clients, servers and databases. Another invaluable capability is predictive impact; Vantage can use its previous measurements to determine what the probable effects of further changes would be. Perhaps equally useful is the detailed, descriptive display of results; numerous bar graphs and diagrams are used to present data in a manner that can easily be understood, even by those without significant network experience. However, being a proprietary service, the specific methods used by Vantage are not explicitly discussed. White papers provided by the company explain the business model and how current company behavior directed their aim towards application performance monitoring, but does not provide insight into their software. Unfortunately, this will tend to be a trend in most commercial software examined within this paper.

Another such commercial product is AppMonitor [AppMonitor], created by Webmetrics. This is a novel service that frequently simulates web transactions to assure that a company's web-based applications are operating correctly. AppMonitor complies with all current systems, supporting implementations from the newer Web 2.0/AJAX models to more common methods such as Java and Flash. In its effort to be technologically advanced, alerts are available not only through e-mail, but also by pager and SMS contact. Application reports can be designed to display a variety of factors, with a variety of methods. These not only consist of the standard abilities of analyzing performance and modeling errors based upon time, but also include analysis based upon geographic location, as well as the detailed examination of each step in a transaction. This step-by-step approach assists in determining which part on an online system is causing delays, rather than simply identifying whole process as inefficient. For flexibility, Webmetrics allows various service levels to be purchased depending on the desired amount and intensity of monitoring - however, all options allow detailed graphing and logging of data. Additionally, as determining which specific application performance-monitoring product to purchase can be difficult, AppMonitor permits a 30-day trial, such that its benefits can be seen.

The following table provides a brief summary of Application & Host-Based Monitoring Tools.

	Cost	Download Size	Platform	Notable Informatiom
MoSSHe	Free	36 KB	Linux	Program is missing some functionality; some errors present
OpenSMART	Free	350 KB for Server, 250 KB for Agents	Linux	Support for SQL; CGI-based reports to user on activity
Vantage	~$60,000 [Azoff06]	Unspecified	Linux, Solaris, Windows	Predictive abilities; attempts to broadly analyze applications across network rather than just clients
AppMonitor	$330-$750 per month[Sticky]	None; WebMetrics does testing and sends results	Supports all web-based applications	Support for contemporary web-based applications; detailed transaction-based analysis. Free trial available

Table 1: Summary of Application & Host-Based Monitoring Tools

However, although applications do provide significant insight into a network's operation, they are not the exclusive source of information. Examining network flows and their patterns can be of significant use, as examined within the following section.

Back to Table of Contents

3.0 Flow Monitoring

Flow monitoring serves to examine the transit of data through a network, looking for patterns of traffic that indicate hostile attacks, periods of frequent use, or simply that all is working as intended. Although the number of public domain products for flow monitoring is somewhat limited, two of these are Argus and NetraMet. A more commonly known service is the commercial NetFlow by Cisco. Additionally, a product called sFlow assists with high-bandwidth networking.

3.1 Basis of Flow Monitoring

In many cases, the levels of traffic within a network mean just as much as the specific data transmitted. Malicious users launching denial of service attacks may be sending packets that all appear valid when examined by alternative means, but flow monitoring reveals the intent when examining the quantity of packets being sent. Such flows should be identified, filtered and eliminated, such that the network is not unnecessarily burdened. Flow monitoring can also reveal the source, destination, and ports of traffic, allowing for identification of policy violating traffic, such as an employee playing online games at the office.

A more common usage of flow monitoring is to determine peak usage and traffic patterns. If an administrator only knows that that the network is sometimes overburdened, the response might be to buy additional servers. However, this might not be necessary - the peak usage times can be determined through flow monitoring, and this information can be used to schedule a shift of some of the load to Content Delivery Networks (CDNs) during such periods in advance. Additionally, the issue might simply be that data is being routed within the network incorrectly or inefficiently, creating unnecessary bottleneck links. Flow monitoring will identify such cases, presenting information that shows how load balancing can be used to solve such problems. Similarly, when certain aspects of a network are of higher importance, their flows and effects can be isolated for distinct analysis.

3.2. Public Domain Flow Monitoring Tools

While flow monitoring is an essential part of NPM, utilizing free tools can be sufficient. One of these is Argus [Argus], a real-time flow monitoring service created by QoSient. This tool can run on Linux, Mac OS X, Solaris, and various BSD systems. Argus analyzes flows and reports on a variety of metrics, including connectivity, capacity, loss, delay, and jitter, as well as protocol-specific information for IPv4 and TCP flows. Records are stored as C structure data types, which then can be read in through XML for better viewing. However, one complaint against Argus is that these files, even in their XML-translated form, are still somewhat complex and inefficiently large for human analysis. Other output formats and capabilities are not sufficiently detailed or described. Counterbalancing these flaws is the fact that several improvements have been made in recent versions, including improved accuracy and reliability, as well as support for reading in alternative data formats. Given the inadequate availability of independent flow monitoring tools, even given Argus's drawbacks, including a somewhat unprofessional website, it still merits consideration.

Another public domain flow monitoring tool is NetraMet [NetraMet], developed by Thomas Lindh and Nevil Brownlee at the University of Auckland for use on both Linux and Windows machines. NetraMet creates a set of entities called meters. These meters are implemented as SNMP agents executing the Realtime Traffic Flow Measurement (RTFM) Meter Management Informational Base (MIB), as described in RFC2723 [RFC2723], measuring traffic flows and compiling and storing data. Meter readers gather data from meters for aggregation and analysis, while Managers deliver configuration rules to meters and meter readers. The Simple Ruleset Language (SRL) is used for detailed specifications of which protocols and address prefixes are to be measured, and how much data will be stored per flow - this can be as simple as filtering based upon only source and destination, and as complicated as specifying target address masks and interfaces. Rules can be cached for improved speed, while preserving accuracy. However, several issues exist with NetraMet. One of these is that the output format of data is not sufficiently described, even though this is essential - good measurement is irrelevant where it is not comprehensible. Additionally, the status of this project is very much in question; the original home page for the NetraMet project could not be used as a link within this paper as it is currently non-operational. Although NetraMet can be found and downloaded from other sources, its lack of a central site significantly decreases its reliability. Consequently, regardless of its strengths, it can only be recommended with reservations.

3.3 Commercial Flow Monitoring Tools

As can be seen in the preceding section, independent public domain tools for flow monitoring are somewhat inadequate. In fact, many free tools exist only to feed off Cisco's product, NetFlow [NetFlow]. As might be expected, this protocol is quite complex, but attempts to solve any possible flow monitoring needs that might exist. Through NetFlow's monitoring, the effects of newly introduced entities in a network can be analyzed, unauthorized traffic can be identified, and the quality of service (QoS) can be quantified. NetFlow examines several metrics, including bytes transferred, the activity of flows, transfer rates, and IP header fields. Dozens of applications have been created to interpret and display flow monitoring results from NetFlow, including both freeware and commercial utilities. The specific capabilities of the reporting software depend on its source, but higher quality reporting tools allow thorough graphical displays for complete comprehension of results. While NetFlow is a high-quality product, some drawbacks do exist; due to its numerous capabilities, the documentation for the product is likewise long and complex, making it difficult to fully appreciate and understand all that NetFlow can do. Cisco does include sample code segments and illustrations, mitigating the complexity, but still forcing users to go through many pages of text. Additionally, Cisco's products are not inexpensive; consequently, alternative flow monitoring tools might be worth considering, rather than large purchasing amounts of hardware, unless the network being monitored is of especially high value and importance.

An alternative, the product sFlow [sFlow], originally designed by InMon, is a commercial protocol that can handle high bandwidths (up to 100 Gbps and beyond) while still monitoring effectively. The goal of sFlow is to find data that can be interpreted to solve many types of network issues including congestion, usage accounting, identification of unauthorized activity, and capacity planning. The sFlow system works in the following fashion, as described by the website in a high-level manner: packets are randomly sampled at some relatively low level of probability. An sFlow agent obtains the header and other information from this packet to begin to form an sFlow datagram. Additional information is found and added to this datagram including forwarding information, user ID and interface counter values. This datagram is then sent to an sFlow Collector & Analyzer. This process continuously as long as desired at dozens of switches and routers. More details concerning the procedure can be found in RFC3176 [RFC3176]. Data obtained from sFlow can be analyzed by various software applications, which an administrator can select from by choosing whichever reports data in the optimal manner. One positive, albeit surprising, note, is that sFlow is licensed free of charge, even though it is a commercial product with many companies such as HP and Hitachi assisting in development. The costs of sFlow are entirely comprised of obtaining sFlow-enabled hardware and a utility to analyze the reported data. Consequently, for these commercial flow-monitoring protocols, it is best to examine the existing infrastructure, and only then make further decisiosn based upon its type and compatibility.

The following table provides a brief summary of flow monitoring tools.

	Cost	Download Size	Platform	Notable Informatiom
Argus	Free	~1 MB for all files	Linux, Mac OS X, Solaris	Output can be read in XML; however, output format somewhat complex

NetraMet	Free	~500 KB	Linux, Windows	Main project website unavailable; uses SRL for specification of filtering rules
NetFlow	Unspecified; costs dependent on hardware used	Unspecified	Interpreter utilities exist for all platforms	Requires interpreter for reading in and displaying results; basis of IETF flow standard. Operates on Cisco hardware
sFlow	Code is free; costs dependent on hardware used	Code, toolkit and free analyzer are ~2 MB	Linux, Solaris, Windows	Capability for monitoring high (100+ Gbps) bandwidths; significant information for developers provided

Table 2: Summary of Flow Monitoring Tools

Although flow monitoring will provide strong insights into a network's operation and performance, this examination can be continued on what can be considered a lower level. Packet capture and sniffing breaks the analysis down to the degree of packet examination, which will be seen to provide its own insights.

Back to Table of Contents

4.0 Packet Capture/Sniffing

While most aspects of NPM attempt to make broad statements concerning user activity or traffic patterns, packet capture and sniffing instead chooses to make its analysis by simply examining the contents of packets themselves. And while these utilities may gain notoriety for being of much assistance for computer attacks and data theft, they work equally well in analyzing the system to strengthen its defenses. Most of such tools are free, as public domain programs for packet capture generally perform as well as commercial products. Consequently, three free utilities will be examined, being Wireshark, tcpdump, and Snoop, with the lone industry product being Etherpeek. It is worth noting that although most NPM services do some level of packet capture, other monitoring systems generally concern themselves only with the analysis of aggregate results. Consequently, these more 'basic' products for sniffing merit examination, as they form the basis for many of the other facets of NPM.

4.1 Basis of Packet Capture/Sniffing

Given their ability to capture and analyze large numbers of individual packets, packet capture and sniffing utilities provide many opportunities for the network administrator. Unsecured versions of Telnet, HTTP, SNMP, FTP, and in fact hundreds of other protocols can be monitored with sniffing utilities such that every packet transmitted within the network is decoded and revealed. The physical operations of most packet capture software are quite similar for purposes of NPM, where packets are simply read off the wire. Additionally, since the sniffing within the network is benign, Ethernet switches within the network can be designed such that full forwarding and promiscuous listening are enabled, where packets are not unnecessarily kept from or encrypted by hosts.

Consequently, employee and computer activity is no longer some nebulous part of a flow; instead, if frequent accesses to some work-inappropriate website are made, the HTTP packets will reveal this usage. If a user is downloading files through FTP, squandering the company's resources, packets will reveal the specifics of this activity as well. One note about packet capture and sniffing is that they do not inherently provide intrusion detection. However, the experienced analyst or an interpreting program can examine packet logs to provide this capability, discovering that certain unexpected commands are being issued and unauthorized accesses are being attempted.

Packet capture and sniffing have nearly infinite uses, and consequently it is appropriate to identify its scope as equally limitless. As noted before, hundreds of protocols can be examined and the usage of these revealed. Therefore, possible uses are left to the individual needs of the administrator, where specific packet analyzers obtain, store and display the data in a comprehensible format.

4.2 Public Domain Packet Capture/Sniffing Tools

The first public domain tool discussed for packet capture is Wireshark [Wireshark], originally developed by Gerald Combs. It is formerly and perhaps more commonly known as Ethereal, but current product development operates under the name Wireshark for legal reasons. Regardless of its name, it is one of the best and most commonly used protocol analyzers on the Internet, with support for most major platforms, and incorporating the ability to output packet results in almost any format desired. Wireshark can capture packets off the network and use a variety of filters to discriminate between packets based upon protocol, destination, source, or any other packet-specific criteria desired. However, as is common with such high-quality sniffer utilities, a large amount of disk space is required, especially with high-speed links; a saturated 1 Gbps link can create gigabytes worth of data within a minute. As bandwidth rates have increased, disk storage costs have decreased; therefore, hard disk space may not be a significant issue unless bandwidth and utilization are especially high. Additionally, while Wireshark may be complex, the provided documentation is a significant benefit, providing pictorial examples of operation. One final note concerning Wireshark is that it is frequently updated; consequently, it is wise to occasionally check the Wireshark website and newsgroups to see if bugs have been found with the current version.

Another free utility for packet capture is tcpdump [tcpdump], developed by the aptly named Tcpdump team. This product also operates on most operating systems, although sometimes indirectly; for Windows systems, a separate, yet virtually identical port entitled Windump was created. Tcpdump operates as a command-line program, where the user inputs filtering rules, packet capture is executed, and then logs of results can be output to a separate file. Given that raw data from tcpdump is quite difficult to read, various freeware utilities have been created to read in tcpdump output for graphical display. One issue with tcpdump is that filtering rules may initially appear quite cryptic; however, the manual files provide several examples of realistic rules, as well as describing all commonly used terms. Another issue is that tcpdump has difficulty with some commands concerning IPv6 packets; consequently, IPv6 users should use Wireshark or at least note that some functionality may be disabled. One final concern is that attackers have been able to send corrupt packets that crash tcpdump; although patches have been released to fix such issues once found, it cannot be guaranteed that more of these vulnerabilities do not exist.

A final free tool for packet capturing is Snoop; however, it only bears brief mentioning, as its functionality is virtually identical to that of tcpdump. Its main difference is that it is included with the Sun/Solaris Unix operating system. Snoop output files may be viewable by the same utilities that can read tcpdump files; however, even if not, programs such as Wireshark can transform Snoop files into the appropriate format.

4.3 Commercial Packet Capture / Sniffing Tools

While tools such as Ethereal and tcpdump may be sufficient for most administrators, a commercial product such as Wildpackets's Etherpeek SE [EtherPeek SE] combined with their PacketGrabber [PacketGrabber] utility, may better serve more complex networks. EtherPeek SE is part of the larger EtherPeek program family, which can analyze networks containing multiple platforms and protocols. EtherPeek SE adds substantial functionality over public domain tools, permitting the creation and monitoring of multiple capture sessions from PacketGrabber simultaneously. Additionally, filtering rules are significantly easier to implement than in previously discussed products, as administrators simply have to click on types of traffic to filter, and these selections can be combined with basic Boolean operators for more specific rules. Furthermore, EtherPeek SE has graphical tools built in to display more comprehensible information about the packets captured, such that additional programs are not necessary for output translation. Alarms and triggers are also available within this program; instead of needing to respond to results retroactively, as with Wireshark, specified activities will be immediately identified and the appropriate employees can be alerted. This is all combined into one superior user interface that provides on-demand information to an administrator. However, two major drawbacks exist, one of which being cost; while the previously discussed tools are provided free of charge, Etherpeek SE alone costs $895, with support hundreds of dollars extra, and the costs of PacketGrabber and the rest of EtherPeek similarly high. Additionally, EtherPeek SE is only available for Windows systems. Consequently, although EtherPeek will serve most administrators well, it is not the right product for all.

The following table provides a brief summary of packet capture/sniffing tools.

	Cost	Download Size	Platform	Notable Information
Wireshark	Free	~15 MB	Windows, Linux, Solaris, BSD	Highly effective capturing and filtering abilities; supports and identifies hundreds of protocols
tcpdump	Free	~ 1 MB for all necessary files	Linux; Windows port also available	Not fully compliant with some IPv6 packets; output needs alternative software for effective analysis
Snoop	Free	Included with OS	Solaris	Virtually identical to tcpdump
Etherpeek	$895/year for Etherpeek SE, $300/year for support	10 GB disk space, 512 MB RAM required (minimum)	Windows	Flexible definition of rules; superior user interface with on-demand alert system

Table 3: Summary of Packet Capture / Sniffing Tools

Packet capture and sniffing provides the basis for all sorts of analysis, as well as providing substantial information on its own. However, the network may be inherently flawed, in a manner that packet examination will not reveal. Path and bandwidth analysis, as discussed within the next section, can reveal poor topologies and crippling bottlenecks within a network.

Back to Table of Contents

5.0 Path / Bandwidth Analysis

In previous sections discussing NPM, it has been a common trend to focus on packets from standard traffic patterns and their individual or aggregate impact on the network. However, this does not have to be the case; with path and bandwidth analysis, the focus can be concerning what happens to sample test packets, and what their route and transit times indicate.

As public domain path and bandwidth analysis tools are significantly simpler than and perform similarly to corresponding commercial utilities, all the programs discussed for this task are free. Three tools examined are Pathchar, Pathload, and Pathrate, all similarly named yet entirely different products. Additionally, many research papers exist on this topic, including 'A Practical Approach to Available Bandwidth Estimation' and 'pathChirp: Efficient Available Bandwidth Estimation for Network Paths', both of which will be briefly evaluated.

5.1 Basis of Path / Bandwidth Analysis

Within a network, even the most seemingly inconsequential links can become network-crippling bottlenecks. As loose routing is common, packets may be directed in ways entirely unexpected, leading to an underprovisioned link quickly becoming one of the most highly traveled. Path analysis can be used to detect such issues, by finding the hops where the most significant delays occur. While unexpected delays may result from other causes than poor topology, discovering them through path analysis is still preferable to leaving them unfixed, even if their direct cause is not always apparent.

When providing service to customers or clients, bandwidth analysis is necessary to determine whether sufficient bandwidth capabilities exist. One of the most critical examples of this is streaming video; if the network cannot sustain data transfer above a certain threshold, the client's viewing experience will be significantly disrupted. Additionally, determining the available bandwidth can identify some of the same issues as path analysis, such as congestion within certain links. Although in some cases there may be no other solution other than to purchase extra servers, this analysis will assist in determining precisely how much more bandwidth is needed in such cases. One further use for bandwidth analysis is to reveal overprovisioning - if a network consistently has high bandwidth availability, therefore having low utilization, the number and operation of servers can safely be scaled down.

5.2 Public Domain Tools for Path / Bandwidth Analysis

The first tool examined is pathchar [pathchar], developed by Van Jacobson of the Network Research Group. Although developed back in 1997, pathchar remains relevant for modern use due to its underlying principles. Its main goal is enhance traceroute such that more information is obtained and returned to the user. During execution, pathchar sends and tracks a specified number of packets with a variety of sizes to a destination, returning the bandwidth, propagation delay, round-trip time, and queuing delay for each hop based upon the average values obtained by the packets. While this program will provide a significant amount of path and bandwidth information to the user, it does have its drawbacks. One issue is that it does not correctly analyze paths that respond significantly differently to packets of different sizes. Additionally, the utility requires customization in almost a trial-and-error method to determine appropriate sample sizes for each network. Furthermore, it is currently not maintained or updated; while this product may provide basic information adequately, it should not be the full extent of path and bandwidth analysis performed.

Another utility for bandwidth analysis is Pathload [Pathload], created by Constantine Dovrolis and Manish Jain. This program calculates the available bandwidth on a path, as defined by the amount of traffic that a source can generate without disrupting the other data transfers on the links. This tool is based upon one central principle: if a stream of UDP packets is sent at a rate that exceeds the available bandwidth, packet delays will increase along that transmission path. However, if the available bandwidth is not met, then these delays will have no discernible trend. Pathload uses this knowledge by sending differing sizes of test streams to approximate the available bandwidth. This can be done successively to bound the range of bandwidth values with a very high degree of precision. However, one major issue exists: if the normal traffic has non-trivial changes in intensity over time, Pathload's bounding may be inaccurate or may not converge. Although the results obtained from Pathload may be interesting and useful for stable networks, unless bandwidth variation is consistently quite low, they cannot be reliably used for predictive analysis.

A tool of somewhat similar ability is entitled Pathrate [Pathrate], created by the above Constantine Dovrolis, as well as Parameswaran Ramanathan and David Moore. But while Pathload concerned itself with what bandwidth was free and available, Pathrate finds the bottleneck/maximum possible bandwidth of a path. Restarting this, calculations are made to determine the highest bandwidth possible, rather than the current bandwidth available, as that would be a task for Pathload. Pathrate sends a long packet train consisting of dozens of groups of packets of different sizes, in order to obtain a large sampling of data concerning operational bandwidth. This data is taken and averaged to give a relatively narrow bounding of path capacity, quantified by a returned coefficient of variation. Although the statistical techniques used within this paper are valid, the range of path bandwidths can only be stated with a high degree of reliability, not absolute certainty; therefore, it would be prudent to run Pathrate multiple times before attempting to send at a rate near the specified maximum.

Two research proposals concerning path and bandwidth analysis merit mention. The first of these is A Practical Approach to Available Bandwidth Estimation (ABwE) [Navratil03], which attempts to calculate available bandwidth on a path. However, instead of the methods used by Pathload, ABwE operates by sending pairs of packets together several times, and interpreting the delay results to classify the network and determine bandwidth. However, while this paper claims a product exists based upon the paper, it does not appear to be readily available for download. Another paper proposes pathChirp [Ribiero03], which functions similarly to the previous utilities. pathChirp sends successive groups of packets, each of which increases in the number of probes per group. By sending these packets, pathChirp is able to observe packet interarrival times and then averages results in order to bound the minimum and maximum possible bandwidth, as done within Pathrate. Although pathChirp is available for download, it is not as customer-friendly as might be preferred; it is only available in Unix, and does not have documentation on the product website.

The following table provides a brief summary of path and bandwidth analysis tools.

	Cost	Download Size	Platform	Notable Informatiom
pathchar	Free	~100 KB	Linux, Solaris, NetBSD	Developed by the creator of traceroute as an enhancement; somewhat outdated
Pathload	Free	67 KB	Linux	Analyzes available bandwidth on a path; can determine this to high degree of precision
Pathrate	Free	65 KB	Linux	Determines maximum possible bandwidth of a path through sending of packet trains
pathChirp	Free	~350 KB for all files	Linux	Similar to Pathrate; uses packet interarrival times to determine maximum bandwidth

Table 4: Summary of Path / Bandwidth Analysis Tools

Path and bandwidth estimation, as well as the previous methods described, all help to analyze and discover large amounts of data concerning networks. However, it must be considered whether these tools are sufficient in a world whether the number of wired networks is decreasing, giving way to wireless networks. While many of the programs previously described might work without modification, others do not port so well. Consequently, the following section discusses NPM in the wireless environment.

Back to Table of Contents

6.0 Wireless Network Monitoring

The previous topics have concerned themselves primarily with wired networks, or simply networks in general. However, as mobility becomes the primary issue of Internet evolution, wireless networks merit consideration for specific examination, due to their inherent challenges and security risks. Two free tools for Wireless LAN monitoring that will be discussed are NetStumbler and Kismet, while two commercial tools to be examined are CommView and the Orion Wireless Network Monitor.

6.1 Basis of Wireless Network Monitoring

For network administrators, wireless networks require an entirely new set of tools, as previous solutions will prove inadequate in least in some regard. There will be no wires to sniff and read packets off of, and no physically contiguous block of hosts that can be examined or isolated. Additionally, security becomes an immense concern; while encryption may be easier to achieve with the large bandwidth capabilities of wired networks, wireless networks must deal with lower data rates, being forced to decide between security and efficiency, as attackers are much more capable of intercepting packets. Consequently, wireless network monitoring is necessary to determine if any rogue hosts and access points are attempting to establish themselves within or nearby the company network. Additionally, it can be examined whether users are ordering themselves in an appropriate manner; while wireless networking may allow for systems to be spread further geographically, outlying users may be receiving only a weak signal and may therefore encounter performance issues.

While wireless network monitoring does required new tools, it incorporates many of the same reasons for monitoring as described within other sections. Packet sniffing still provides significant insight into the operations of users, and may in fact be of higher use within wireless networks; if the administrator can easily sniff and decode passwords and sensitive information transmitted within the network, it is quite likely that an attacker can and will do the same. Monitoring the application usage of users is similarly of great importance; active wireless users are at higher risk of attack as compared to wired users behind firewalls and network address translation (NAT), and consequently detecting any vulnerable programs on wireless machines is critical. The security issues with wireless networking lead its motivations and impact its analysis substantially.

6.2 Public Domain Wireless Network Monitoring Tools

One free tool for wireless network analysis is NetStumbler [NetStumbler]. This program allows an administrator to scan wireless networks for appropriate coverage, discovering interference, determining antenna direction, or to detect unauthorized nodes and access points. This is accomplished through active scanning, the process of sending probes out every second and reporting the responses. However, many issues exist with NetStumbler. One problem is that it only operates on modern Windows operating systems; consequently, this tool will be unusable by many. Additionally, some wireless networking cards are incompatible with NetStumbler. Passive scanning is also unimplemented. Therefore, this tool is not for the company wanting guaranteed monitoring of all traffic in all methods, but may still be sufficient for the bulk of users not using exotic network cards. One final negative note is that given the current iteration number of this product (0.4.0), a final version of NetStumbler cannot be expected in the near future, and hence reliability is somewhat low.

Another public domain utility for examining a wireless network is Kismet [Kismet], developed by Mike Kershaw. This functions as an alternative to NetStumbler, running on Linux, BSD, Mac OS X and Win32 systems. Kismet exhibits high functionality, allowing for data to be logged in standard Wireshark/tcpdump-compatible formats, while also able to interpret data in order to display graphical representations of network topology and a detailed identification of access points and clients. With these abilities, Kismet can be used not only as a tool to analyze the existing network, but also for intrusion detection. Unfortunately, with all of the abilities permitted, the setup time for this program is relatively high, which decreases ease of use. Extra utilities must be downloaded and specific program configurations must be made to permit successful operation. As with NetStumbler, some wireless cards are not supported. However, in spite of its complexity, Kismet appears superior as a free wireless network monitoring tool for both its flexibility and functionality.

6.3 Commercial Wireless Network Monitoring Tools

As mobile computing continues to increase, expenditures on products facilitating a secure, reliable wireless environment seem less frivolous. For larger company networks, one wireless network monitoring utility is CommView [CommView] by TamoSoft. CommView intercepts all wireless traffic, and reports detailed results to a console. This data can easier be sorted, filtered, and analyzed through a clear, easy to use user interface. Additionally, CommView is designed to dynamically report and alert specified users if designed unexpected or suspicious activity occurs. One ability that TamoSoft cites as extraordinary is CommView's ability to decrypt both WEP and WPA packets. Given that WEP is falling increasingly out of favor due to its vulnerability to attacks, this is a critical ability. TamoSoft's thirty-day free trial of this product permits users to test these features and discover CommView's superiority to free tools.

Another commercial utility is the Orion Wireless Network Monitor [Orion] from SolarWinds. Orion is designed for particularly high-end networks, providing superlative interface and capabilities as well as user support. While the specific abilities are similar in name to products such as CommView, the functions are enhanced, with further graphical modeling and analysis possible. Custom accounts can be created, such that one administrator account is not forced to be responsible for all issues, and access controls can be enabled for users of different authority levels or in different locations. However, this all comes with requirements and costs; Orion can only operate on recent Windows machines, and has significantly higher price as compared to other wireless network monitoring products. A trial version is provided, and this is very much recommended for testing before purchasing the full Orion product.

The following table provides a brief summary of wireless network monitoring tools.

	Cost	Download Size	Platform	Notable Informatiom
NetStumbler	Free	1.3 MB	Windows	Only implements active scanning; incompatible with some wireless cards
Kismet	Free	~1 MB	Linux, Mac, Solaris	High complexity; high functionality for inputting/outputting data

CommView	$199 to $499; 30-day free trial	Unspecified size; 128 MB RAM required	Windows	Can handle both WEP and WPA-encrypted packets; provides graphic reports and permits remote access
Orion	$2495; trial version available	10-20 GB disk space, 256 MB-1 GB RAM	Windows	Superior reporting and interpretation of data; allows custom user access levels

Table 5: Summary of Wireless Network Monitoring Tools

While wireless networking may be the future, it is not currently and may never be the standard of business use. Additionally, while these individual fields and previously discussed tools each accomplish specific tasks, in some cases a monolithic platform may be desired to aggregate all monitoring objectives and abilities into one source. This is the philosophy behind Network Monitoring Platforms, as discussed within the following section.

Back to Table of Contents

7.0 Network Monitoring Platforms

Where price is not an issue, commercial products can be used in order to cover most network bases simultaneously. For networks that have especially high value and use, these Network Monitoring Platforms (NMPs) may be the optimal solution. These NMPs are generally commercial programs with higher costs, with four of such being VitalSuite, NimBUS, Ciscoworks and NetCool.

7.1 Basis of Network Monitoring Platforms

Although the whole is generally thought to be more than the sum of its parts, this maxim will not hold true for network administrators implementing a multifaceted monitoring scheme comprised of several different programs created by different organizations. Packet sniffers cannot be guaranteed to output data in a format readable by the other tools, and while translation utilities exist, these simply add to overall complexity and waste time. Perhaps more critically, programs may be redundant and may unnecessarily consume resources by each attempting to gather the same data. Alternatively, using a large number of monitoring programs may simply add an aggregate CPU overhead such that the network performance monitoring programs themselves may be the ones degrading performance. With NMPs, all aspects of the platform are designed to work together, such that efficiency and performance are increased.

Even if such issues are not considered, integrated NMPs are preferable for their reliability. Established companies such as Lucent and Cisco have created effective, high-quality software, and can be trusted to release products that will not include egregious exploits and will not covertly pass on sensitive company information. The same cannot necessarily be said for free utilities that are maintained by a small group of individuals releasing unfinished builds. Furthermore, these NMPs come with user support and comprehensive documentation; the inexperienced network administrator can be assisted through carefully reading product notes, or directly contacting dedicated support personnel of the vendor. A more accurate adage concerning NPM would be that one gets what one pays for; for NMPs, although costs will be high, quality will be assured.

7.2 Commercial Network Monitoring Platforms

The first commercial NMP examined is VitalSuite [VitalSuite] by Lucent Technologies. VitalSuite is designed to handle monitoring of up to hundreds of different devices in an automated manner. In fact, up to ten million total objects can be monitored at a time. Dynamic charts and statistics are constantly updated in order to find network congestion and failures before they significantly impact the company. VitalSuite improves data collection through efficient importation of device information; consequently, hardware elements can be identified by more than just a generic title. A variety of configurations are supported, as well as the latest protocols, enhancing flexibility. Additionally, system requirements are not excessively prohibitive; any Windows 2000 or newer operating system is supported, as well as Sun Solaris platforms. One issue, however, is that Lucent's site is undergoing renovation as of the time of this paper, causing some links to be missing their targets, including some relevant VitalSuite documentation. The price for this NMP is also left somewhat unclear; administrators desiring further information on VitalSuite would be advised to contact Lucent directly concerning the product status.

Another commercial NMP is NimBUS [NimBUS] from Nimsoft. Although this is not a well-known company, the product is still excellent, providing detailed monitoring capabilities, even for global networks. NimBUS includes the common scope of abilities for NMPs, including monitoring access periods and response times for devices and applications, performing traffic analysis, gathering SNMP statistics, and providing extensive graphical display possibilities. Extensive documentation is available, although users must register on the Nimsoft website to access these files. Additionally, the price for the software and the system requirements are not clearly stated. While NimBUS advertises its flexibility in its ability to be deployed at multiple points throughout the network, and it is stated that it will work on Windows-based hosts, its compatibility with other operating systems is unclear. However, a trial download of NimBUS is provided, allowing for administrators to determine whether this product will be acceptable for their domain. This is highly encouraged, as for all that is provided on the product website, real-world testing can provided practical responses to previously answered questions about NimBUS.

A well-known NMP is Cisco's Ciscoworks [Ciscoworks]. While one might expect this NMP to be monolithic, it is actually composed of several pieces that can be applied to specific areas. Ciscoworks includes solutions for Wireless LANs, VPNs, and quality of service analysis, with even a specific subsection designed for serving smaller companies. This wide range of products cannot be described within this paper, but the basic LAN Management Solution (LMS) bears brief examination, as it may be the most commonly used for wired networks. LMS further delineates the LAN into layers, such that devices, flows, hosts and links can all be analyzed effectively by appropriate subsystems. Up to 1500 devices can be monitored simultaneously, providing real-time results concerning performance. LMS is only available for Solaris and Windows systems, and requires high-end hardware; for Windows systems, a 2.8 GHz machine with between 2-8 GB of RAM is required for the main host, with all clients needing 512 MB of memory for LMS applications. Consequently, networks with low-end machines may be unable to use Ciscoworks products such as this or may encounter performance issues. The Ciscoworks family is broad, as well as expensive; it is advised to do significant research into the products supported in addition to contacting Cisco directly to determine which tools would be best for any specific company.

A final NMP is NetCool [NetCool] by IBM and Micromuse. Micromuse states their goals from a very business-oriented perspective, attempting to discover where extra resources are needed most and how service-level agreements can be followed as closely as possible. Four main modules are included within NetCool; the first of these is DataLoad, which polls SNMP devices and reads data files. DataChannel collects and analyze data, processing it for display within seconds. DataMart acts as a storage utility for both old and new data as well as network policies. Finally, DataView aids in providing an exceptional user interface, able to deliver reports within seconds. With this modular design, each step of the monitoring process can easily be identified and defined, creating an overall system that is both flexible and comprehensive. Although the recent merger of IBM and Micromuse might seem to inhibit development, IBM's resources have instead allowed for a multimedia demo to be created for NetCool. However, it does appear that NetCool may be in the process of being combined with a similar product titled Tivoli; potential users are advised to check for news updates concerning the service. As no trial version of NetCool is available, contacting IBM concerning the current status of the project and its cost is very much recommended.

The following table provides a brief summary of network monitoring platforms.

	Cost	Download Size	Platform	Notable Informatiom
VitalSuite	$35,000+ [Nance06]	Minimal	Windows, Solaris	Lucent/Alcatel merger causes product website issues; can poll and monitor up to 10 million devices
NimBUS	$10,000+ [Biggs05], Trial Version Available	Unspecified	Windows	Extensive documentation; some information unavailable; high quality monitoring and display capabilities
Ciscoworks	$9,000 - $20,000 for LMS [Windows Marketplace]	2-8 GB of RAM for server, 512 MB RAM for clients	Windows, Solaris	High-quality, well known product; allows simultaneously monitoring of diverse devices; many products available depending on specific needs
NetCool	$75,000+ [MM_SLM]	Unspecified	Windows, Solaris, Linux	Uses multiple modules to split tasks into definable pieces; very business oriented; can read data and deliver dynamic reports within seconds

Table 6: Summary of Network Monitoring Platforms

While these commercial NMPs may represent the pinnacle of NPM, they do come at a price. For many networks, the individual public domain NPM tools may suffice, especially where reliability is high. However, when considering which products to obtain, and considering the seemingly high costs of NMPs, network administrators must ask themselves two questions: what will happen to the business if the network fails, and tools are not in place to determine the solution? Similarly, how will it reflect on the administrator when it is discovered that utilities could easily have been installed to detect and control damage? As such failures are generally catastrophic both economically and professionally, this question drives researchers to improve NPM principles and develop new products.

Back to Table of Contents

8.0 Conclusion

With today's on-demand world, high network performance is no longer some secondary, idealistic goal. Instead, it is a multifaceted part of network administration that cannot be ignored. In this paper, several different aspects of Network Performance Monitoring have been discussed, with multiple proposed tools for each topic; the solution no longer simply has to be to obtain more bandwidth or to upgrade the servers every time a problem is found. While one does not need to frivolously go and buy every service, when NPM is adequately addressed, the customer's experience will be significantly improved, with persistent, unsolvable errors becoming a thing of past.

Back to Table of Contents

9.0 References and Acronyms

Note Concerning References

Much information has been obtained from these product websites, and hence they are cited. In some cases, this information was obtained from documentation and pages linked from the product homepage; for brevity of the following list, and an easier experience browsing references, citations are generally made only for the main site. Detailed technical information is generally available with minimal browsing.

Project Refernece List

[Azoff06] Michael Azoff. "Technology Audit: IT Management". Butler Group analytical paper on recent Compuware version. May 2006. http://www.compuware.nl/perskamer/pdf/Compuware-Vantage_9.9.pdf. *Analytical paper discussing Vantage.*

[Biggs05] Margie Biggs. "Web Site Sleuths". FCW.com comparative article on monitoring solutions. March 14, 2005 issue. http://www.fcw.com/article88255. *Article discusses and compares different monitoring utilities.*

[MM_SLM] Unsigned; Enterprise Management Associates. "Micromuse Service Level Management Buyer's Guide - 2nd Edition". Product summary and cost analysis document. 2004. http://www.micromuse.com/downloads/pdf_lit/Micromuse_SLM_Brief_ema_jan2003.pdf. *Detailed guide for potential buyers of NetCool.*

[Nance06] Barry Nance. "Lucent Clear Winner in Network and Application Performance Management Software Test". NetworkWorld Custom Media article comparing various products. September 2006. http://www.networkworldpartners.com/lucent/Bakeoff4.pdf. *Article discusses and compares different application monitoring utilities.*

[RFC2723] Natalie Brownlee. "SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups". Official RFC Document, October 1999. http://www.ietf.org/rfc/rfc2723.txt. *RFC discussing process used in NetraMet.*

[RFC3176] P. Phaal, S. Panchen and N. McKee. "InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks". Official RFC Document, September 2001. http://www.rfc-editor.org/rfc/rfc3176.txt. *RFC discussing processes used in sFlow.*

[Sticky] Unsigned. "Tool info: AppMonitor". Brief description of AppMonitor. October 13, 2005. http://stickyminds.com/sitewide.asp?Function=edetail&ObjectType=TOOL&ObjectId=1688. *Brief examination of the AppMonitor tool including pricing.*

[WindowsMarketplace] Unsigned; Microsoft Corporation. "Product details for CiscoWorks LAN Management Solution Large Enterprise Package - (v. 2.6) - license". Official Microsoft Product Vending website. http://www.windowsmarketplace.com/details.aspx?view=info&itemid=3138552. *Microsoft site providing commercial products; link is to specific page indicating cost of LMS.*

Product Reference List

[AppMonitor] Webmetrics. "Application Monitoring and Web Transaction Monitoring". Official Commercial Product Website. http://www.webmetrics.com/applicationmonitoring.html. *Company website for Application Monitoring product.*

[Argus] QoSient, LLC. "Argus - Home". Official Product Website. http://www.qosient.com/argus/. *Company website for Flow Monitoring product.*

[CiscoWorks] Cisco Systems. "CiscoWorks". Official Commercial Product Website. http://www.cisco.com/warp/public/cc/pd/wr2k/index.shtml. *Company website for Network Monitoring Platform.*

[CommView] TamoSoft. "Wireless Network Analyzer and Monitor - CommView for WiFi". Official Commercial Product Website. http://www.tamos.com/products/commwifi/. *Company website for Wireless Network Monitoring product.*

[EtherPeek SE] WildPackets. "WildPackets - EtherPeek SE - Overview". Official Commercial Product Website. http://www.wildpackets.com/products/etherpeek/etherpeek_se/overview. *Company website for Packet Capture / Sniffing tool.*

[Kismet] Mike Kershaw. "Kismet". Official Product Website. http://www.kismetwireless.net/. *Company website for Wireless Network Monitoring product.*

[MossHe] Volker Tanger. "WYAE - MoSSHe - Lightweight, secure server monitoring". Official Product Website for Weyland Yutani Arms & Equipment. http://www.wyae.de/software/mosshe/. *Website for Application Monitoring product.*

[Navratil03] Jiri Navratil and R. Les. Cottrell. "ABwE :A Practical Approach to Available Bandwidth Estimation". SLAC-PUB-9622, published at PAM 2003. http://moat.nlanr.net/PAM2003/PAM2003papers/3781.pdf. *Research paper concerning Path / Bandwidth analysis.*

[Netcool] Micromuse. "Products & Solutions: Netcool Suite Overview". Official Commercial Product Website. http://www.micromuse.com/products_sols/. *Company website for Network Monitoring Platform.*

[NetFlow] Cisco Systems. "Cisco IOS NetFlow". Official Commercial Product Website. http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html. *Company website for Flow Monitoring protocol.*

[NetraMet] Thomas Lindh, Nevil Brownlee. "Integrating Active Methods and Flow Meters - An Implementation Using NetraMet". Research paper presented at PAM2003 at San Diego in April 2003. http://www.caida.org/publications/papers/2003/netramet/ntm-oam-pam2003.pdf. *Research paper concerning Flow Monitoring product.*

[NetStumbler] Unsigned. "NetStumbler.com". Official Product Website. http://www.netstumbler.com. *Company website for Wireless Network Monitoring product.*

[NimBUS] Nimsoft. "Nimsoft - NimBUS for Network Monitoring". Official Commercial Product Website. http://www.nimsoft.com/solutions/network-monitoring/index.php. *Company website for Network Monitoring*

Platform.

[OpenSMART] Holger Schultheiss, Ulrich Herbst. "OpenSMART - The Open (Source|System) Monitoring and Reporting Tool". Official Product Website. http://opensmart.sourceforge.net/index.html. *Website for Application Monitoring product.*

[Orion] SolarWinds. "Wireless Network Monitor Solarwinds". Official Commercial Product Website. http://www.solarwinds.net/products/orion/wireless.aspx. *Company website for Network Monitoring Platform.*

[PacketGrabber] WildPackets. "WildPackets - PacketGrabber - Overview". Official Commercial Product Website. http://www.wildpackets.com/products/other_products/packetgrabber/overview. *Company website for Packet Capture / Sniffing utility.*

[pathchar] Van Jacobson. "pathchar - a tool to infer characteristics of Internet paths". Official Product Documentation. ftp://ftp.ee.lbl.gov/pathchar/msri-talk.pdf. *Document discussing Path Analysis tool.*

[Pathload] Constantine Dovrolis, Manish Jain. "Pathload". Official Product Website. http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/bw.html. *Website for Bandwidth Analysis tool.*

[Pathrate] Constantine Dovrolis, Ravi Prasad. "Pathrate". Official Product Website. http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/pathrate.html. *Website for Bandwidth Analysis tool.*

[Ribiero03] Vinay J. Ribeiro, Jiri Navratil, Les Cottrell, et al. "pathChirp: Efficient Available Bandwidth Estimation for Network Paths". Passive and Active Measurement Workshop. April 2003. http://moat.nlanr.net/PAM2003/PAM2003papers/3824.pdf. *Document discussing Bandwidth Analysis tool.*

[sFlow] Unsigned. "sFlow.org - Making the Network Visible". Official Commercial Product Website. http://www.sflow.org/index.php. *Company website for Flow Monitoring tool.*

[tcpdump] JWS. "TCPDUMP Public Repository". Official Product Website. http://www.tcpdump.org/. *Website for Packet Capture / Sniffing tool.*

[Vantage] Compuware. "Vantage - Compuware's complete application service management solution". Official Commercial Product Website. http://www.compuware.com/products/vantage. *Company website for Application Monitoring tool.*

[VitalSuite] Lucent Technologies. "Lucent - VitalSuite Performance Management Software for Enterprises". Official Commercial Product Website. http://www.lucent.com/. Note: direct link to product information unavaiable. *Company website for Network Monitoring Platform.*

[Wireshark] CACE Technologies. "Wireshark: The World's Most Popular Network Protocol Analyzer". Official Product Website. http://www.wireshark.org/. *Website for Packet Capture / Sniffing tool.*

Acronyms

CDN - Content Delivery Network
MIB - Management Informational Base
NAT - Network Address Translation
NMP - Network Monitoring Platform
NPM - Network Performance Monitoring
OS - Operating System

QoS - Quality of Service
RTFM - Realtime Traffic Flow Measurement
SRL - Simple Ruleset Language
VPN - Virtual Private Network
WEP - Wired Equivalent Privacy
WPA - Wi-Fi Protected Access

Back to Table of Contents

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

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