A Summary of Network Traffic Monitoring and Analysis Techniques

Alisha Cecil , acecil19@yahoo.com

Abstract
As company intranets continue to grow it is increasingly important that network administrators are aware of and have a handle on the different types of traffic that is traversing their networks. Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so as to not bring network services to a stand still for extended periods of time. Numerous tools are available to help administrators with the monitoring and analysis of network traffic. This paper discusses router based monitoring techniques and non-router based monitoring techniques (passive versus active). It gives an overview of the three most widely used router based network monitoring tools available (SNMP, RMON, and Cisco Netflow), and provides information about two newer monitoring methods that use a combination of passive and active monitoring techniques (WREN and SCNM).

Keywords: NetFlow, network monitoring, network analysis, watching resources from edge of network, self configuring network monitor, active monitoring, passive monitoring

---

Table of Contents

1.0 Importance of Network Monitoring and Analysis

Network monitoring is a difficult and demanding task that is a vital part of a Network Administrators job. Network Administrators are constantly striving to maintain smooth operation of their networks. If a network were to be down even for a small period of time productivity within a company would decline, and in the case of public service departments the ability to provide essential services would be compromised. In order to be proactive rather than reactive, administrators need to monitor traffic movement and performance throughout the network and verify that security breeches do not occur within the network.

Back to Table of Contents

2.0 Monitoring and Analysis Techniques

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network." -Orebaugh, Angela. Two Monitoring Techniques are discussed in the following sections: Router Based and Non-Router Based. Monitoring functionalities that are built-into the routers themselves and do not require additional installation of hardware or software are referred to as Router Based techniques. Non-Router based techniques require additional hardware and software to be installed and provide greater flexibility. Both techniques are further discussed in the following paragraphs [UnivPenn02].

2.1 Router Based Monitoring Techniques

Router Based Monitoring Techniques are hard-coded into the routers and therefore offer little flexibility. A brief explanation of the most commonly used monitoring techniques is given below. Each technique has undergone years of development to become a standardized model.

2.1.1 Simple Network Monitoring Protocol (SNMP) RFC 1157

SNMP [Cisco5606] is an application layer protocol that is part of the TCP/IP protocol suite. It allows Administrators to manage network performance, find and solve network problems, and plan for network growth. It gathers traffic statistics through passive sensors that are implemented from router to end host. While two versions exist, SNMPv1 and SNMPv2, this section deals with SNMPv1. SNMPv2 builds upon SNMPv1 and offers enhancements, such as additional protocol operations. Standardization of yet another version of SNMP. SNMP Version 3 - (SNMPv3)is pending.

There are 3 key components to SNMP: Managed Devices, Agents, and Network Management Systems (NMSs). These are shown in Figure 1 below.

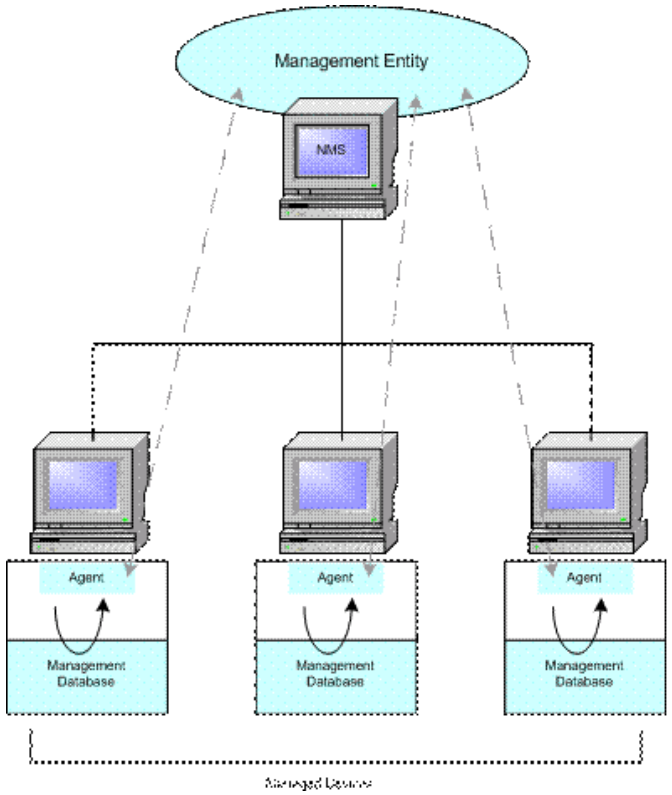

Figure 1: SNMP Components [Cisco5606]

The Managed Devices contain the SNMP Agent and can consist of routers, switches, hubs, pcs, printers, and items such as these. They are responsible for collecting information and making it available to the NMSs.

The Agents contain software that have knowledge of management information and translates this information into a form compatible with SNMP. They are located on a managed device.

The NMSs execute applications that monitor and control the managed devices. Processing and memory resources that are needed for network management are provided by the NMSs. A minimum of one NMS must exist on any managed network. SNMP can act solely as a NMS or an agent, or can perform the duties of both. There are four basic commands used by SNMP NMS to monitor and control the managed devices: read, write, trap, and traversal operations. The read command examines the variables that are kept by the managed devices. The write command changes the values of the variables stored by the managed devices. Traversal operations look to find out what variables a managed devices supports and gathers information from the supported variable tables.The trap command is used by the managed devices to report the occurrence of certain events to the NMS.

SNMP uses four protocol operations in order to operate: Get, GetNext, Set, and Trap. The Get command is used when the NMS issues a request for information to managed devices. The SNMPv1 message (request) that is sent consists of a message header and a Protocol Data Unit (PDU). The PDU of the message contains the information that is needed to successfully complete a request

that will either retrieve information from the agent or set a value within the agent. The managed devices use the SNMP agents located on them to retrieve the needed information, and then respond to the NMS with an answer to the request. If the agent does not have any information in regards to the request, it does not return anything. The GetNext command will then retrieve the value of the next object instance. It is also possible for the NMS to send a request (Set operation) that sets the values of items within the agents. When an agent needs to inform the NMS of an event, it will use the Trap operation.

As discussed, SNMP is an Application Layer protocol that uses passive sensors to help administrators monitor network traffic and performance. Although SNMP can be a helpful tool to Network Administrators it does create a vulnerability to security threats because it lacks any authentication capabilities. It is unlike Remote Monitoring (RMON) that is discussed in the following section in that RMON monitors at the Network Layer and below, rather than at the Application Layer.

2.1.2 Remote Monitoring (RMON) RFC 1757

RMON [Cisco5506] enables various network monitors and console systems to exchange network-monitoring data. It is an extension of the SNMP Management Information Database (MIB). Unlike SNMP that must send out a request for information, RMON is able to set alarms that will monitor the network based on certain criteria. RMON allows Administrators to manage local networks as well as remote sites from one central location. It monitors at the Network Layer and below. RMON has 2 versions RMON and RMON2 this paper only deals with RMON. RMON2 allows for monitoring of packets on all network layers. It focuses on IP traffic and application level traffic.

While there are 3 key components to the SNMP monitoring environment there are only 2 in the RMON environment. They are shown in Figure 2 below.

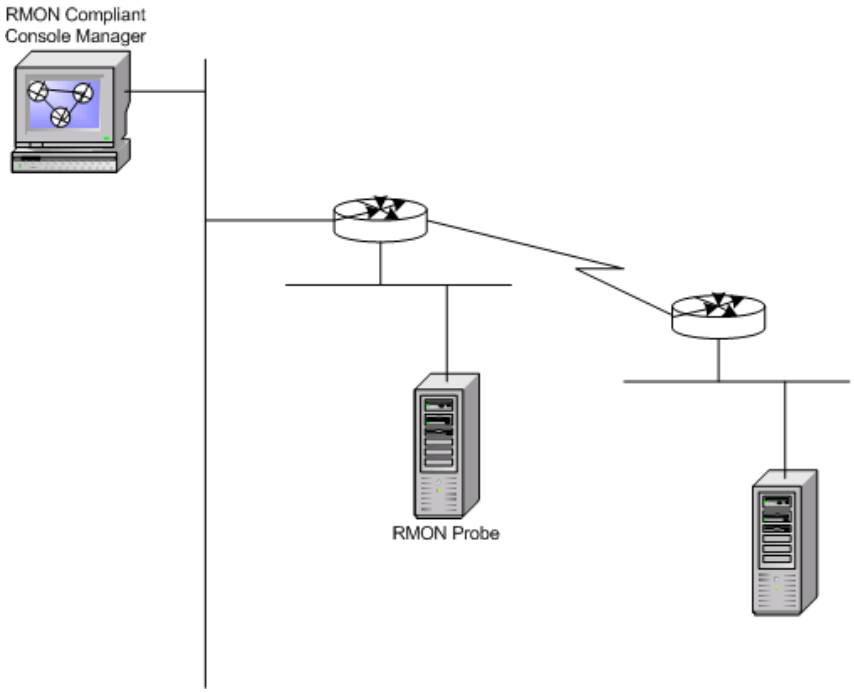

Figure 2: RMON Components [Cisco5506]

The 2 components of RMON are the probe also known as the agent or monitor, and the client also know as the management station. Not unlike SNMP the RMON probe or agent gathers and stores the network information. The probe is embedded software on the network hardware, such as routers and switches. The probe can also run on a pc. The probes must be put on each different LAN or WAN segment as they only are able to see traffic that flows through only their link, and are unaware of outside links. The Client is usually a management station that communicates with the probe using SNMP to obtain and correlate the RMON Data.

RMON [RMON] uses 9 different monitoring groups to obtain information about the network.

- Statistics - stats measured by the probe for each monitored interface on this device
- History - records periodic statistical samples from a network and store for retrieval
- Alarm - periodically takes statistic samples and compares them with a set of thresholds for event generation
- Host - contains statistics associated with each host discovered on the network
- HostTopN - prepares tables that describe top hosts
- Filters - enable packets to be matched by a filter equation for capturing events
- Packet capture - captures packets after they flow through the channel

- Events - controls generation and notification of events from a device
- Token ring - supports token ring

As stated above RMON, builds upon the SNMP protocol. Although traffic monitoring can be performed with these techniques, analysis of the information provided by SNMP and RMON takes a little extra work. Netflow, which is discussed in the next section, works well with many analysis software packages to help make the job of administrators a little easier.

2.1.3 Netflow RFC 3954

Netflow [Cisco06] is a feature that was introduced on Cisco routers that give the ability to collect IP network traffic as it enters an interface. By analyzing the data that is provided by Netflow a network administrator can determine things such as the source and destination of the traffic, class of service, and the cause of congestion. Netflow consists of three components: flow caching, FlowCollector, and Data Analyzer. Figure 3 shows the Netflow Infrastructure. Each component shown in the figure is explained in the following paragraphs.

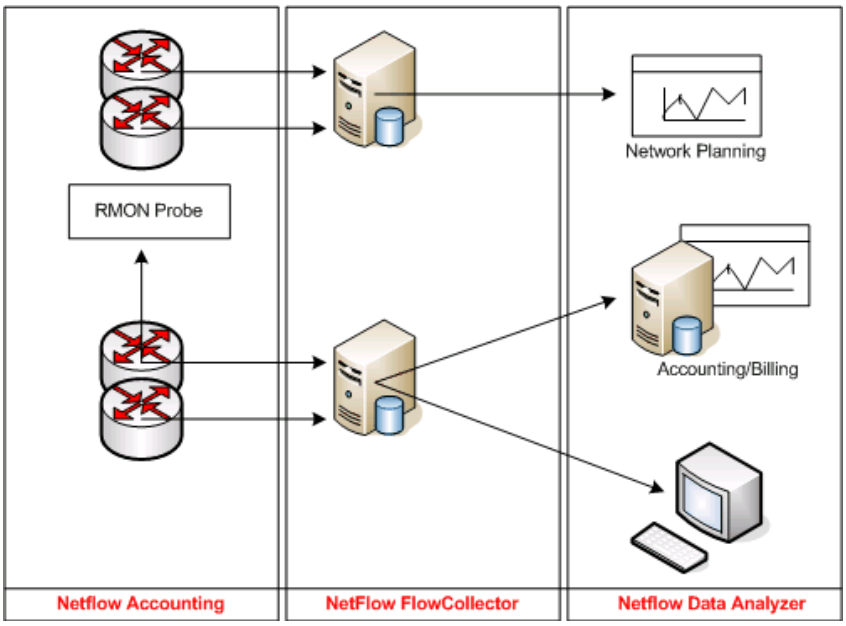

Figure 3: Netflow Infrastructure [Cisco06]

The flow caching analyzes [NetFlow06]and collects the IP data flows that enter an interface and prepares the data for exportation.

The following information can be obtained from Netflow packets: [NetflowAbout06]

- Source and Destination addresses
- Input and Output interface numbers
- Source and Destination port numbers
- Layer 4 protocol
- Number of packets in the flow
- Total Bytes in the flow
- Time stamp in the flow
- Source and Destination autonomous system (AS) number
- TCP_Flag and Type of Service (ToS)

The first packet of a flow through the standard switching path is processed to create the cache. Packets with similar flow characteristics are used to create a flow record which is kept in the cache for all active flows. The flow record tracks the packets and bytes per flow. The cache information is then periodically exported to the Flow Collector.

The Flow Collector [NetFlow06] is responsible for the data collection, filtering, and storage. It contains a history of the flow information that was switched within the interface. Data volume reduction is also done by the Flow Collector through selective filtering and aggregation.

Data Analyzer [NetFlow06] is then responsible for presentation of the data. As shown in the figure the data collected can be used for various purposes other than network monitoring such as network planning and accounting and billing.

The advantage of Netflow over other monitoring methods such as SNMP and RMON is that there are numerous traffic analysis software packages (data analyzers) that exist to pull the data from Netflow packets and present it in a more user friendly way.

By using a tool such as Netflow Analyzer [NetflowWhitePaper05] (just one tool that is available for analyzing Netflow packets) the information above can be pulled out of the Netflow packets to create charts and usage graphs that an Administrator can study to maintain an understanding of their network. The biggest benefit of using Netflow in combination with one of the available Analysis packages is that numerous different graphs detailing network activity can be created on the spur of the moment.

2.2 Non-Router Based Techniques

Although non-router based techniques are still limited in there abilities they do offer more flexibility than the router based techniques. These techniques are classified as either active or passive.

2.2.1 Active Monitoring

Active monitoring [Active06] transmits probes into the network to collect measurements between at least two endpoints in the network. Active measurement systems deal with metrics such as:

- Availability
- Routes
- Packet Delay
- Packet Reordering
- Packet Loss
- Packet Inter-arrival Jitter
- Bandwidth Measurements (Capacity, Achievable Throughputs)

Commonly used tools such as ping, which measures delay and loss of packets, and traceroute which helps determine topology of the network, are examples of basic active measurement tools. They both send ICMP packets (probes) to a designated host and wait for the host to respond back to the sender. Figure 4 is an example of the ping command that uses active measurements by sending an Echo Request from the source host through the network to a specified destination. The destination then sends an Echo Response back to the source it received the request from.

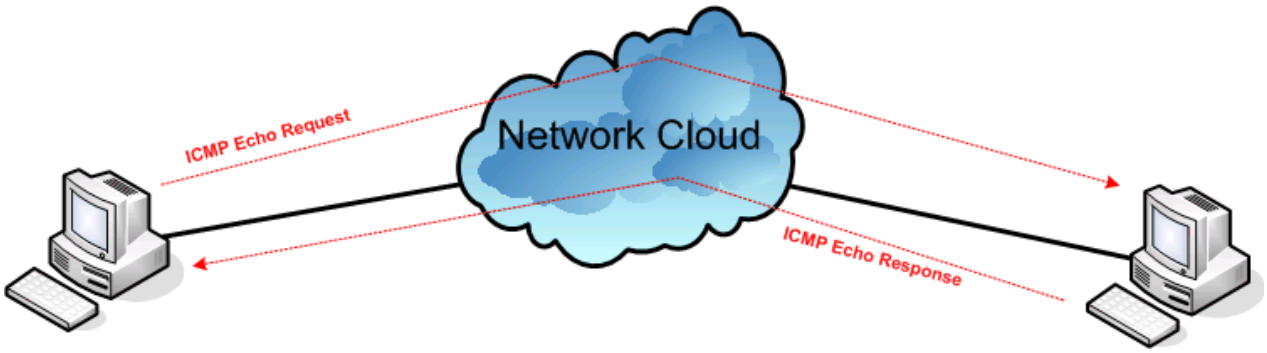

Figure 4: ICMP ping command (Active Measurement)

Not only can a person collect the metrics above from active measurements, one can also determine the network topology. Another common example of an active measurement tool is iperf. Iperf is a tool that measures TCP and UDP bandwidth performance. It reports bandwidth, delay jitter, and loss.

The problem that exists with active monitoring is that introducing probes into the network can be an interference to the normal traffic on the network. [UnivPenn02] Often times the active probes are treated differently than normal traffic as well, which causes the validity of the information provided from these probes to be questioned.

As a result of the information detailed above, active monitoring is very rarely implemented as a stand-alone method of monitoring as a good deal of overhead is introduced. On the other hand passive monitoring does not introduce much if any overhead into the network.

2.2.2 Passive Monitoring

Passive monitoring [Curtis00] unlike active monitoring does not inject traffic into the network or modify the traffic that is already on the network. Also unlike active monitoring, passive monitoring collects information about only one point in the network that is

being measured rather than between two endpoints as active monitoring measures. Figure 5 shows the setup of a passive monitoring system where the monitor is placed on a single link between two endpoints and monitors traffic as it passes along the link.

Figure 5: Passive Monitoring Setup

Passive measurements deal with information such as: Traffic and protocol mixes Accurate bit or packet rates Packet timing and inter-arrival timing

Passive monitoring can be achieved with the assistance of any packet sniffing program.

Although passive monitoring does not have the overhead that active monitoring has, it has its own set of downfalls. [UnivPenn02] With passive monitoring, measurements can only be analyzed off-line and not as they are collected. This creates another problem with processing the huge data sets that are collected.

As one can see passive monitoring my be better than active monitoring in that overhead data is not added into the network but post-processing time can take a large amount of time. This is why a combination of the two monitoring methods seems to be the route to go.

2.2.3 Combinational Monitoring

After reading the sections above one can safely come to the conclusion that a combination of active and passive monitoring is better than using one or the other. Combinational techniques utilize the best aspects of both passive and active monitoring environments. Two newly introduced combinational monitoring techniques are described below. Watching Resources from the Edge of the Network (WREN) and Self-Configuring Network Monitor (SCNM).

2.2.3.1 Watching Resources from the Edge of the Network (WREN)

WREN [LowekampZangrilli04] uses a combination of active and passive monitoring techniques by actively monitoring when traffic is low and passively monitoring during high traffic times. It monitors traffic at both the source and destination end host which allows for more accurate measurements. WREN uses packet traces from existing application traffic to measure the available bandwidth. WREN is split into two levels, the kernel level packet trace facility and the user level trace analyzer.

The kernel level packet trace facility is responsible for capturing the information associated with incoming and outgoing packet. Figure 6 lists the information that is gathered for each packet. A buffer was added to the Web100 kernel to collect these characteristics. Access to the buffer is through 2 system calls. One call starts the trace and provides the information needed to conduct it while another call retrieves the trace from the kernel.

Incoming Packets				Outgoing Packets			
timestamp	seq #	ack #	TCP cwnd	timestamp	seq #	ack #	data size

Figure 6: Information collected by WREN kernel level packet trace [LowekampZangrilli04]

The packet trace facility is able to coordinate measurements between the different machines. One machine will trigger the other machine by setting a flag in the header of outgoing packets to start tracing the same range of packets that it is tracing. The other machine will in turn trace all packets that it sees with the same header flag set. This coordination ensures that the information about the same packets is stored at each end of the connection regardless of what happens in between.

The user level trace analyzer is the other level in the WREN environment. It is the component that begins any packet traces and collects and processes the data returned from the kernel level trace facility. By design the user-level components are not required to read the information from the packet trace facility at all times. It can be analyzed immediately after the trace is completed to make runtime decisions or stored for future analysis.

When traffic is low, WREN will actively introduce traffic into the network in order to maintain a continuous flow of measurements. After numerous studies, it was found that WREN produced the same measurements in congested and un-congested environments.

In the current implementation of WREN users are not constrained to capturing only the traces that were initiated by them. Although

any user is able to trace another users application traffic they are restricted to the information that can be obtained from another users trace. They are only able to get the sequence and acknowledgement numbers but not the actual data segments of the packets.

In summary, WREN is a very useful tool that utilizes the benefits of both active and passive monitoring. Although it is in its early stages WREN can provide Administrators with a valuable resource in the monitoring and analyzing their network. Self Configuring Network Monitor (SCNM) is another tool that uses both active and passive monitoring techniques.

2.2.3.2 Self Configuring Network Monitor (SCNM)

SCNM [Agarwal03] is a monitoring tool that uses a combination of active and passive measurements to collect information at layer 3 ingress and egress routers and at other significant points within the network being monitored. The SCNM environment consists of both hardware and software components.

The hardware is installed at critical points in the network. It is responsible for passively collecting the packet headers. The software runs on the endpoints of the network. Figure 7 below shows the software components of the SCNM environment.

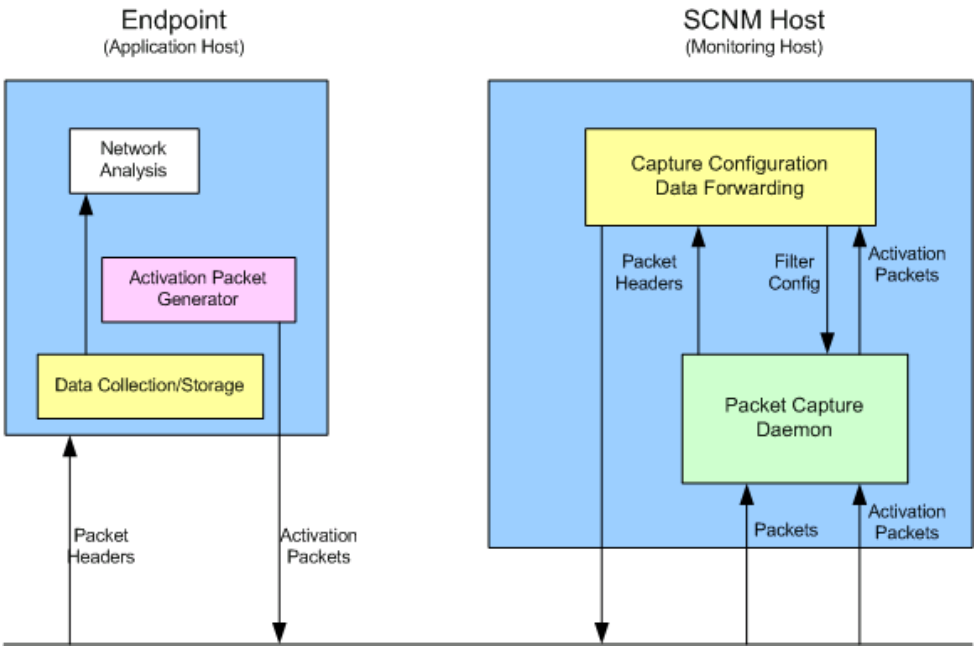

Figure 7: SCNM Software Components [Agarwal03]

The software is responsible for creating and sending the activation packets that are used to start the monitoring of the network. A user will send an activation packet out into the network containing the details about the packets they want to monitor and gather. The user does not need to know the location of the SCNM hosts due to the fact that all hosts listen for packets. Based on the information that is within the activation packet a filter is set up within a data collection daemon that is also running on an endpoint. The network and transport layer headers of packets that correspond to the filter are collected. The filter will automatically time out after a specified amount of time unless it receives another application packet. The packet capture daemon which runs on the SCNM host uses a tcpdump like packet capture program in order to receive requests and to record the traffic that corresponds to the requests.

When a problem is detected by the passive monitoring tools, traffic can be generated using the active tools, allowing one to collect additional data to further study the problem. By having these monitors deployed at every router along the path, we can study only the section of network that seems to be having the problem. [Tierney04].

SCNM [Agarwal03] is intended to be installed and used mainly by network administrators; however average users can use a subset of its functionality. Although average users are capable of using part of the SCNM monitoring environment they are only allowed to monitor their own data.

In conclusion, SCNM is another combinational monitoring tool that utilizes both active and passive monitoring to help administrators monitor and analyze their networks.

Back to Table of Contents

3.0 Summary

When choosing a particular tool to use for monitoring, an Admin must first decide if they would like to use a more proven system or a newer system. If the proven system is the direction that feels more comfortable, NetFlow is the most beneficial tool to use since a data analysis package can be used in conjunction with it to present the data in a user friendly environment; however if an Admin is willing to try out a newer system, a combinational monitoring approach such as WREN or SCNM is the best direction to proceed.

Being able to monitor and analyze networks is vital in the job of Network Administrators. They must strive to keep the networks they oversee in good health as to not disrupt productivity within a company and to not disrupt any essential public services. As summarized throughout this paper several router based and non-router based techniques are available to assist Network Administrators in the day to day monitoring and analysis of their networks. SNMP, RMON, and Cisco's NetFlow are a few of the router based techniques that are briefly reviewed. The non-router based techniques that were discussed were Active, Passive, and Combinational monitoring tools.

Back to Table of Contents

References

1. [Cisco5606] Cisco Systems, " Simple Network Management Protocol", Internetworking Technologies Handbook, Chpt 56, 1992--2006
   http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

2. [Cisco5506] Cisco Systems, "Remote Monitoring", Internetworking Technologies Handbook, Chpt 55, 1992--2006
   http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm

3. [LowekampZangrilli04] Lowekamp, Bruce B; Zangrilli, Marcia, "Using Passive Traces of Application Traffic in a network Monitoring system", IEEE Computer Society 2004
   http://portal.acm.org/citation.cfm?id=1033294

4. [Agarwal03] Agarwal, Deb; Gonzalez, Jose Maria; Jin, Goujun; Tierney, Brian, "An Infrastructure for Passive Network Monitoring of Application Data Streams", Proceedings of the 2003 Passive and Active Monitoring Workshop
   http://www.pam2003.org

5. [UnivPenn02] Anagnostakis, K.G.; Ioannidis, S. ; Miltchev, S. ; Greenwald, M. ; Smith, J.M. (University of Pennsylvania), "Efficient Packet Monitoring for Network Management" Proceedings of the 8th IEEE/IFIP Network Operations and Management Symposium (NOMS), 2002
   http://citeseer.ist.psu.edu/anagnostakis02efficient.html

6. [Tierney04] Tierney, Brian L, "Self-Configuring Network Monitor A High Performance Network Engineering Proposal: Network Measurement and Analysis", For the period June 1, 2001 - May 31, 2004
   http://dsd.lbl.gov/Net-Mon/SCNM-proposal.pdf

7. [NetflowWhitePaper05] "Traffic Analysis with Netflow WhitePaper", 2005
   http://manageengine.adventnet.com/products/netflow/Traffic_Analysis_with_Cisco_Netflow.pdf

8. [NetflowAbout06] "About Cisco Netflow", 2006
   http://manageengine.adventnet.com/products/netflow/cisco-netflow.html

9. [RMON] "RMON: Remote Monitoring MIBs (RMON1 and RMON2)"
   http://www.networkdictionary.com/protocols/rmon.php?PHPSESSID=677dddf6927ec036f62817f8c29dc5ea

10. [Active06] "Active Network Performance Measurement and Estimation" Nov. 14, 2006
    http://www.imse.cnm.es/fedemp/abet/index.html

11. [Curtis00] Curtis, James "Passive Measurement", Jan 17, 2000.
    http://wand.cs.waikato.ac.nz/old/wand/publications/jamie_420/final/node9.html

12. [Cisco06] Cisco IOS Netflow Data Sheet, 1992-2006
    http://www.cisco.com/en/US/products/ps6601/products_data_sheet0900aecd80173f71.html

13. [NetFlow06] NetFlow Services Solutions Guide, 1992-2006
http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html

Back to Table of Contents

Acronymns

AS	Autonomous System
ICMP	Internet Control Message Protocol
LAN	Local Area Network
MIB	Management Information Database
NMS	Network Management System
PDU	Protocol Data Unit
RMON	Remote Monitoring
SCNM	Self Configuring Network Monitor
SNMP	Simple Network Management Protocol
ToS	Type of Service
WAN	Wide Area Network
WREN	Watching Resources from the Edge of the Network

Back to Table of Contents

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