

Networking Monitoring and Management Solution for Networking and Computing Solutions

By

Mark Gaynor

Submitted to:
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Engineering Technology

University of Cincinnati
College of Applied Science

March 2004

Monitoring/Management for the Johnson & Johnson Midwest Region

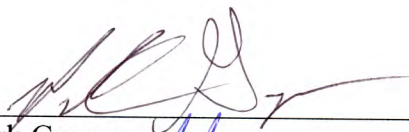
By

Mark Gaynor

Submitted to
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements
for
the Degree of Bachelor of Science
in Information Engineering Technology

© Copyright 2004 Mark Gaynor

The author grants to the Information Engineering Technology Program permission
to reproduce and distribute copies of this document in whole or in part.



Mark Gaynor

3/8/04

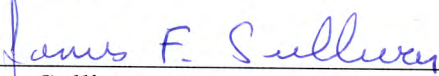
Date



Mark Stockman

3/8/04

Date



James Sullivan

8 March, 2004

Date

Table of Contents

Section	Page
Table of Contents	i.
List of Figures	iii.
Abstract	iv.
1. Statement of the Problem	1
2. Description of the Solution	1
2.1 User Profiles	2
2.2 Project Design	4
3. Objectives of the Project	4
4. Design and Development	4
4.1 Timeline	
4.1.1 Senior Design I	5
4.1.2 Senior Design II	6
4.1.3 Senior Design III	6
4.2 Budget	6
4.2.1 Budget for Solution	6
4.2.2 Other Associated Figures	7
4.3 Software	7
4.3.1 Ciscoworks 2000	7
4.3.2 Netscout	7
4.3.3 MRTG	8
4.3.4 Windows OS	8
4.4 Hardware	9
4.4.1 Ciscoworks 2000	9
4.4.2 Netscout	9
4.4.3 MRTG	10
4.4.4 Windows OS	10
4.5 Security	10
4.6 Testing Procedure	11
5. Proof of Design	11
5.1 Solution to monitor the network usage on multiple devices.	11
5.2 Setup a historical tracking system	14
5.3 Implement Cisco works 2000	17
5.4 Install NAM Blade in Cincinnati	20
5.5 Setup all routers and other devices	23
6. Conclusions and Recommendations	24
6.1 Conclusions	24
6.2 Recommendations	25

7. References

List of Figures

Figure Number	Page
Figure 1. System Layout of Cincinnati Local Area Network	3
Figure 2. Basic Timeline from start to finish of the Senior Design Sequence	5
Figure 3. The budget used to purchase all software and hardware for the solution	6
Figure 4. Hardware Requirements of the Ciscoworks/MRTG/Netscout Server	10
Figure 5. Configuring the Netscout to work with the NAM	11
Figure 6. Configuring Data Capture	13
Figure 7. Analyzing the Packets	14
Figure 8. Navigation for Core A Historical Data	15
Figure 9. Thirty-minute bandwidth chart for ports 1/1 and 2/1	16
Figure 10. Historical tracking of the RNC for daily, monthly and yearly data	17
Figure 11. Seed Devices (Cisco Catalyst 6509's)	18
Figure 12. User Tracking.	19
Figure 13. Cisco View	20
Figure 14. Telnet to the Core A router	21
Figure 15. Telnet to the Core A switch	21
Figure 16. Session to the NAM Blade	22
Figure 17. NAM Configuration	22
Figure 18. NAM GUI	23

Network Monitoring and Management Solution for Networking and Computing Services

Networking and Computing Services (NCS) asked me to build a monitoring and management solution for Johnson & Johnson's Midwest regional network. The old process for managing the network consisted of standard telnet sessions from a console window. NCS had only a high-level network monitoring software known as Network Health. Network Health does not have the ability to measure specifics on the network, but only overall bites in and out. I decided to use three separate software packages to offer NCS the flexibility it needed. The first piece of software I used was called Multi Router Traffic Grapher (MRTG.) MRTG allows NCS to view its core switching router on a port level as opposed to monitoring the entire device in one graph. The second piece of software I used is Ciscoworks 2000. Ciscoworks is a management solution for companies that use Cisco hardware in their networks. This software has eliminated telnet sessions and gives the administrators a central place to go for all configuration needs on the network. Finally I chose Netscout/Ngenius. This software with Network Analysis Module Blades installed on the core switching routers, gives NCS the ability to view packets on the network based on IP, segment, and protocol. These three pieces together give NCS the tool that it had been lacking when trying to monitor/manage Johnson & Johnson's Midwest regional network.

Networking Monitoring and Management Solution for Networking and Computing Solutions

1. Statement of the problem

Networks have changed the face of business. A network outage can prevent a company from conducting daily business activities. In a perfect environment a network would not have outages and the end user would never be affected. This unfortunately is not the case.

The ability to prevent these outages is essential to being a successful network administrator. Many different aspects of the computer environment can cause these outages. Software, hardware, and physical breakdowns are all some of the areas that can cause a network to fail. Preventing these outages through the network administrator's efforts alone is far from efficient. There are multiple software packages accompanied by hardware upgrades that allow the administrator to more effectively do his/her job. At the same time these software packages cannot replace the network administrator.

The problem with these software packages is cost. They generally require hardware upgrades. They are not for a small to medium company without a full time Information Management department. These packages are for companies with a considerable amount of money in their network, that handle large amounts of network traffic on a daily basis.

2. Description of the Solution

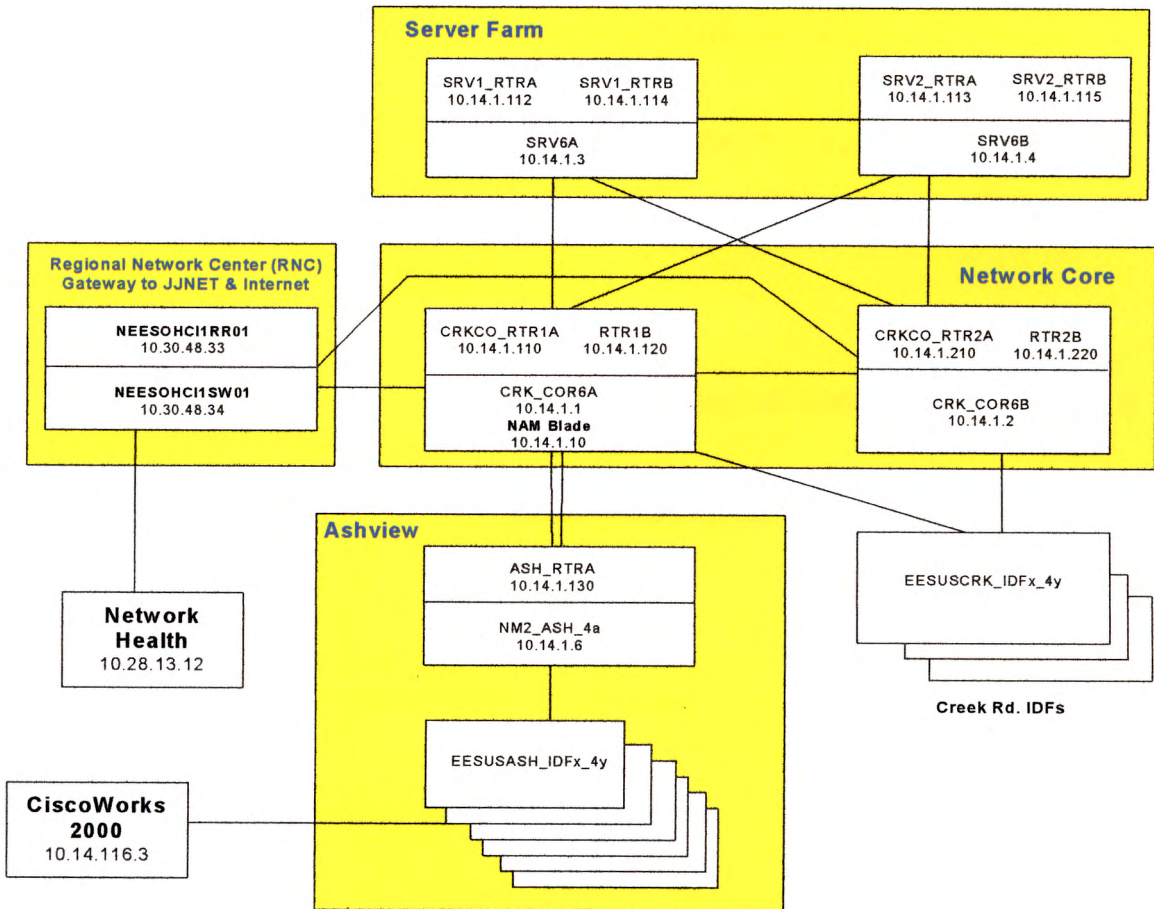
With the dynamic needs of Johnson and Johnson's Networking and Computing Services (NCS) one software package will not perform all necessary tasks that NCS requires. One software package does not have the capability for real-time monitoring and management. This is why I have chosen two separate software packages. The two I chose are Ciscoworks and Multi Router Traffic Grapher (MRTG.) These two pieces of software with Network Analysis Module (NAM) blades will allow me to provide NCS with a complete monitoring/management solution.

2.1 User Profiles

There are four different groups who need access to this solution. Some users will have access to each aspect of the solution and others will have access to only specific areas.

- A. The WAN Network Administrator is located in Dallas Texas. He is ultimately responsible for the entire network. He supervises all core upgrades, frame relay upgrades, and any kind of physical upgrades. All network design and configuration at a WAN level is mainly performed by the WAN administrator. He supports the LANs at multiple sites. LAN network administrators work in support him locally. The WAN network administrator has a Cisco Certified Internetwork Expert. This individual has complete access to the solution, including administrative functions.
- B. The LAN Network Administrators are the first individuals who will be working with my network monitoring solution. There is an administrator at Cincinnati, Albuquerque, and Juarez. These are the LAN administrators responsible for on site support for the LANs. They also support the WAN administrator for hardware/physical changes that need to be made. Each one of these users has a Cisco Certified Network Associate certification or better. LAN administrators have complete access to the solution.
- C. Management needs to access to the networking solution for the monitoring tools. They need to be able to make business related decisions based upon the information provided by the software. Upgrades and changes are partially be dictated by the software. All administrators answer to management. The LAN administrators answer one manager based in Cincinnati. The WAN administrator answers to a manager based in New Jersey. The managers generally have a technical background with either a bachelor in Information Systems or another similar degree. Management have complete access to all monitoring aspects of the solution.
- D. Miscellaneous members of the Data Team may need access from time to time. This includes co-ops, associates, and possibly IBM contractors. These individuals would have read access to view the network in its current state, but more then likely would not have write access. The Midwest Regional Manager would dictate this decision. Access will be granted on a case-by-case basis. Depending on who the user is, his/her role within the company, and what the situation calls for will dictate how much access he/she is given.

EES Cincinnati LAN High Level View



EES LAN Overview Ver 9.0
T. Cheung
R. Braidich
Mark Gaynor
November 7th, 2003

Figure 1. System Layout of Cincinnati Local Area Network

2.2 Project Design

Networking is the primary focus of my project, as a result of the need at Johnson and Johnson for networking monitoring and management. Working with Cisco switches and routers, Windows servers, and security is what makes this project as focused as it is. Additionally I have been tasked with building a Windows Server to house the Ciscoworks software.

The second focus of my project is web development. I built an introductory HTML page to help users navigate between the different aspects of my solution.

3. Objectives of the Project

- Solution to monitor the network usage on multiple devices. All must be real time.
- Setup a historical tracking system for bandwidth across designated ports.
- Implement Ciscoworks 2000 across the Midwest region WAN and LAN allowing network administrators to manage the network via the web.
- Install NAM blades in Cincinnati.
- Setup all routers and other devices to interact with Ciscoworks and MRTG

4. Design and Development

This section will cover the timeline of tasks and the schedule, budget, all software used, the hardware involved, and security.

4.1 Timeline

This section includes all progress of my project from Senior Design I through Senior Design III. There were a number of scares with the hardware issues, and a number of hurdles to overcome.

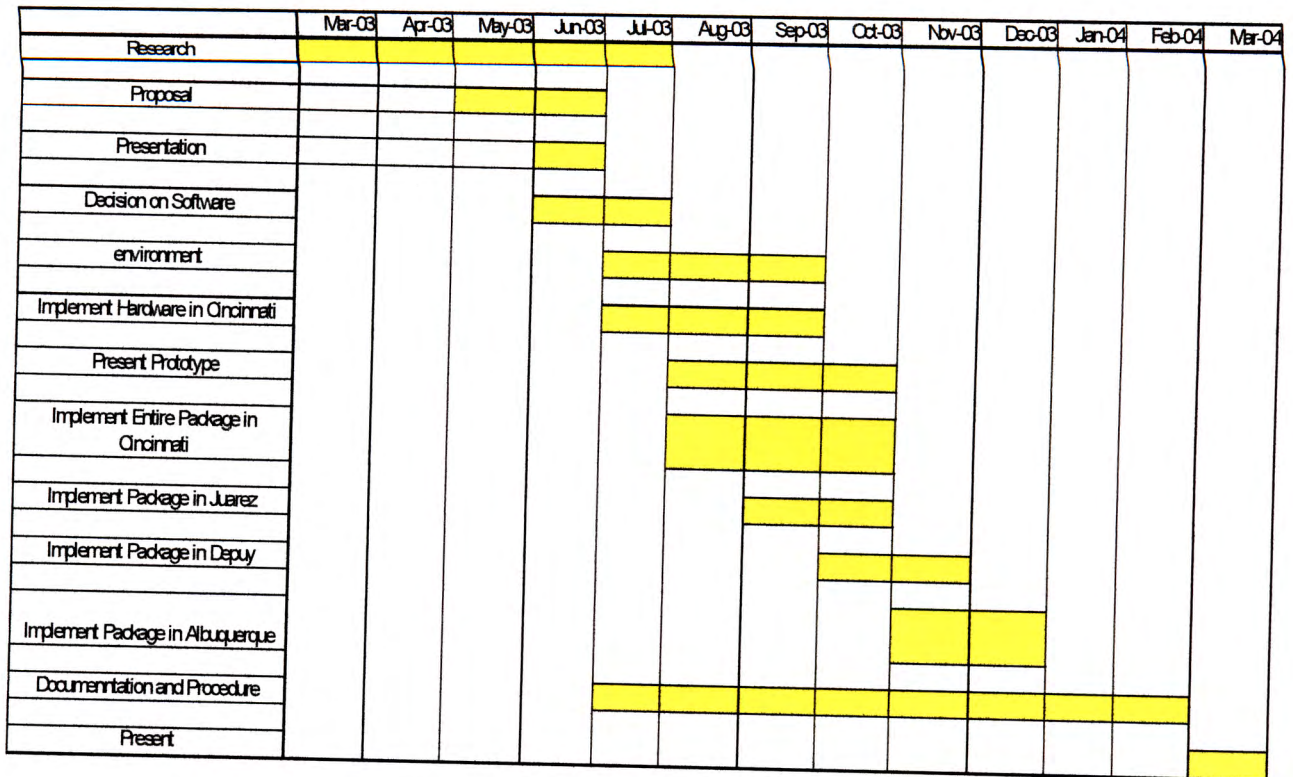


Figure 2. Timeline

4.1.1 Senior Design I

Weeks 1 – 4

- Gather possibilities for project
- Research

Weeks 5 – 8

- Decision on project
- Research

Weeks 9 - 11

- Prepare presentation
- Present decision on Networking Monitoring/Management Solution

4.1.2 Senior Design II

Weeks 1 – 7

- Decide on Software

- Configure MRTG and Setup

Weeks 8 – 11

- Install Ciscoworks 2000
- Setup For Cincinnati
- Purchase NAM Blades
- Installation of NAM Blades in Cincinnati
- Prototype presentation
- Turn in Design Freeze

Fall September – December

- Finish installation throughout the WAN
- Configure Ciscoworks for entire WAN
- Setup MRTG websites for all necessary Devices

4.1.3 Senior Design III

- Documentation for Maintenance
- User Guide
- Final Draft
- Present to Faculty/NCS Data Team

4.2 Budget

This section covers the budget used to build the solution. The overall hardware used for the solution but already owned and used by Johnson & Johnson is also included.

4.2.1 Budget for Solution

Device	Cost	Location	Number	Total
NAM Blade	18,000	Cincinnati	2	36000
NAM Blade	18,000	Juarez	2	36000
NAM Blade	18,000	Albuquerque	1	18000
Software License (upgrade)	700	Cincinnati	1	700
Windows Box for Ciscoworks		Cincinnati	1	675
			Total	\$91,375

Figure 3. Budget

4.2.2 Other Associated Figures

- Cincinnati and Juarez has \$1.6 million of networking equipment including that in the regional network center.
- Juarez has \$660,000 in hardware.
- Albuquerque has \$660,000 in hardware.

4.3 Software

This section covers all software I used to build the solution for Johnson and Johnson. There were multiple parts I had to use when I thought I would only use two.

4.3.1 Ciscoworks 2000

Ciscoworks 2000 is a software package sold by Cisco that allows its users to both monitor and manage LAN and WAN technologies. This software allows users to utilize a Graphical User Interface to configure Cisco equipment such as routers and switches. The software comes with four modules. These modules each come with different capabilities. Some of which allow the user to manage the network and track hardware. Other uses are: tracking Cisco help desk cases, asset management, Virtual Private Network monitoring, and security on the software itself.

The software package allows Network administrators to access and manage the network without having to remote into each individual switch. All network management can be performed in a central location through a Web browser.

4.3.2 Netscout

Netscout/Ngenius is the fifth module of the Ciscoworks solution package. This application is setup to capture traffic sent to it from either probes or NAM blades setup on the network. The abilities of the software are directly related to how the NAM and switches are configured. With the correct hardware in place Netscout can sniff for specific protocols, IP's, or packets based on size. The software is useless without the

associated hardware, in this case the NAM blades. The NAM blades allow the administrators to monitor specific Protocols such as AOL, Real Audio, or SMTP. The administrator can then use Netscout to view the packets that are captured by the NAM blade.

4.3.3 Multi Router Traffic Grapher (MRTG)

MRTG is a software package, which is free to the public. It offers the ability to watch bandwidth utilization on specific devices. It is built with Perl, and the user must build the configuration files. Depending on configuration it runs on each segment of the network in five-minute intervals. NCS has been concerned with monitoring specific ports on its core devices. These devices are 6509 series switching routers. They are what support the entire network. MRTG allows the user to monitor each port and its bites both in and out.

4.3.4 Windows Operating System

Although the Ciscoworks 2000 software is designed to run on a server, the cost kept NCS from purchasing another server. I encountered numerous issues with trying to install Ciscoworks on an application server. We have two development servers, and due to multiple port conflicts and a lot of hours on the phone with Cisco I was unable to get the software running correctly. When I built a high-powered desktop and used Windows Professional 2000 I had no problems at all. This also gave me the ability to build manage my own box. This allowed me to make changes to the server without involving the server-farm administrators.

I was forced to install Internet Information Services on this box due to the needs of MRTG. MRTG requires IIS to host its pages. MRTG uses web pages to show its data, but without IIS I could not host them so NCS could utilize the charts.

4.4 Hardware

This section covers what I used to build my solution and house my software. I went through multiple iterations of hardware, but ended up settling on a high-powered desktop.

4.4.1 NAM Blade

Network Access Module (NAM) blades are modules that plug into the back of routers. They allow for monitoring specific devices across the network. These modules can record data real time and send it to a server somewhere on the network for library of historical data. This data can be filtered according to the administrators needs. The administrator can specify both destination and host addresses. The NAM blades also allow for protocol monitoring while reporting IP and MAC addresses. The blades themselves are an actual card that must be installed on a Cisco 6509 or some other high end switching router.

4.4.2 Cisco Catalyst 6509 Router

Cisco's Catalyst 6509 is the core of Johnson & Johnson's network. These devices handle all traffic coming into and out of the network. NAM blades are installed on them to allow for monitoring of the Network. Ciscoworks interfaces with them for network management and actual configuration on the 6509 itself.

4.4.3 Cisco Switches

A host of Cisco switches are used in Johnson and Johnson networks. Most are either a Cisco 4006 or a Cisco 3548 devices. These devices are scaleable allowing for expansion as users are added. Each one is "Trunked" back to a port on the Catalyst 6509's through a one-gig fiber cable. Additionally they interface with Ciscoworks 2000 allowing the administrator to manage the network without having to telnet or session around the network.

4.4.4 Desktop

The desktop in choice is an IBM desktop with Windows 2000. The requirements of this box were specified by Cisco. Cisco required certain Processor, RAM, Swap Space, and Available drive space of the desktop (4.)

System Requirements

Requirement Type	Entire LAN Bundle
Processor	Ultra 60MP
Memory (RAM)	512 MB
Swap space1	1 GB
Available drive space	6 GB and space for software management files

Figure 4. Hardware Requirements of the Ciscoworks/MRTG/Netscout Server

4.5 Security

Security is handled through different means. The Ciscoworks Software has user authentication already built into the software. I have created access lists based upon the needs of the user base. Network Health is currently hosted on a URL within Johnson & Johnson's intranet. The URL of the navigation page is distributed to those individuals

who have reason to view the page. It is not necessary to use an access list to prevent other users from accessing the site. The information is not confidential. Only giving out the URL to specific individuals is more than enough security.

4.6 Testing Procedure

Various people throughout the development of the solution preformed testing. I gave all users access to each aspect of the solution as it was implemented. They were allowed to use it as much as they wanted and in anyway. I addressed issues as they were found.

5. Proof of Design

This section will cover the proof of my design and go into detail of how all my deliverables were met.

5.1 Solution to monitor the network usage on multiple devices. All must be real time.

The Netscout/Ngenius software allowed me to add this ability to my solution. The software actually receives packets forwarded from the NAM blades and allows them to be arranged so they may be viewed for real time data.

The data available can be sorted, filtered, and saved into a CSV file so the data captured can be easily interpreted. The first step was configuring the Netscout to work with the NAM blade. Figure 5. shows the GUI used to set up the NAM.

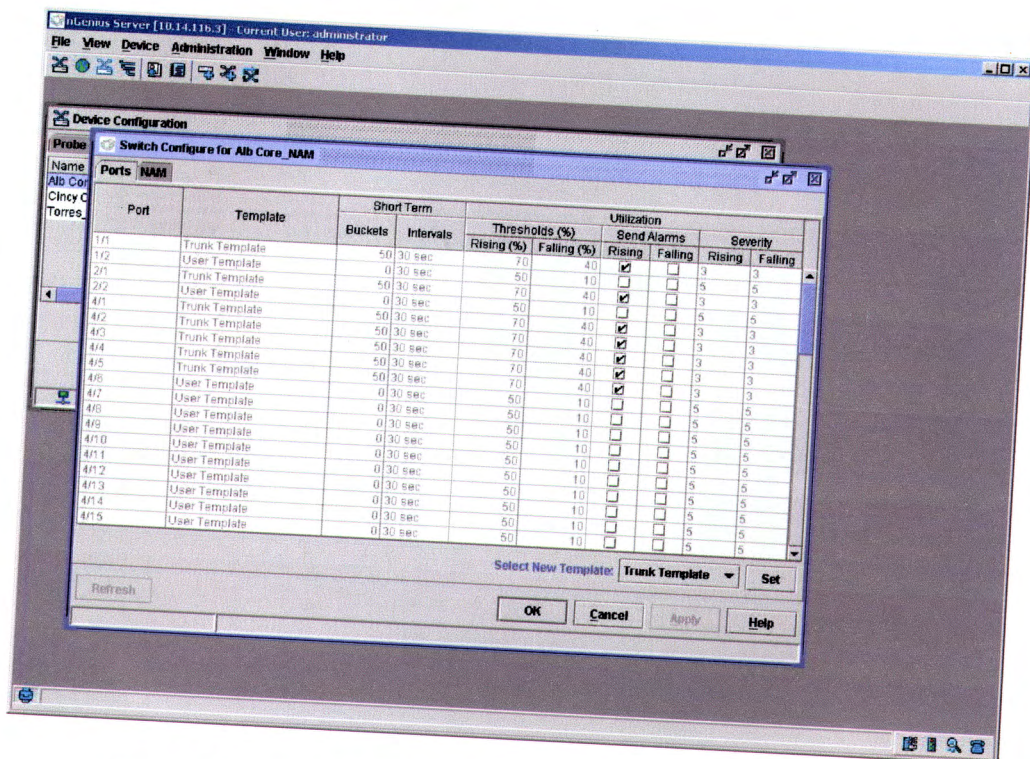


Figure 5. Configuring the Netscout to Work with the NAM

The next step to using Netscout and the NAM is configuring for specific protocols. In the instance in Figure 6. I used AOL Instant Messenger for my example. I used the NAM blade located in Cincinnati to capture the data, the IP address entered in the "Source" was mine (10.14.116.162,) and the protocol chosen was AIM.

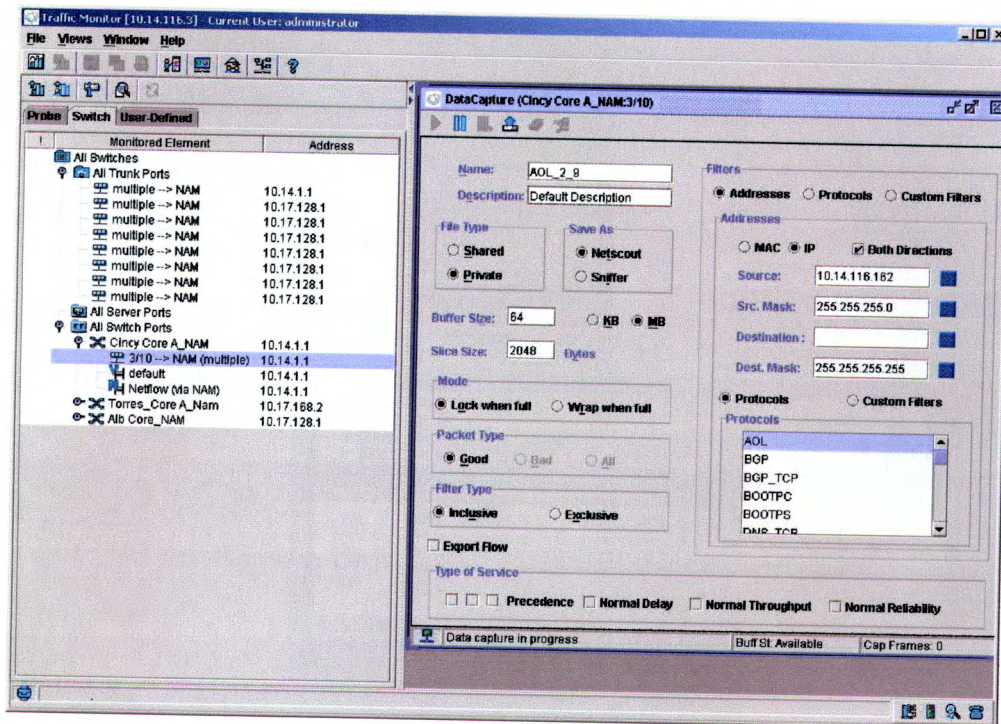


Figure 6. Configuring Data Capture

The final step after allowing the NAM to capture data is to upload the buffer and analyze the packets received. The buffer is uploaded to the server, and Netscout just uses the PC of the user to act as a terminal. Figure 7. shows a number of packets captured, all of which are from a client on the LAN using AOL Instant Messenger.

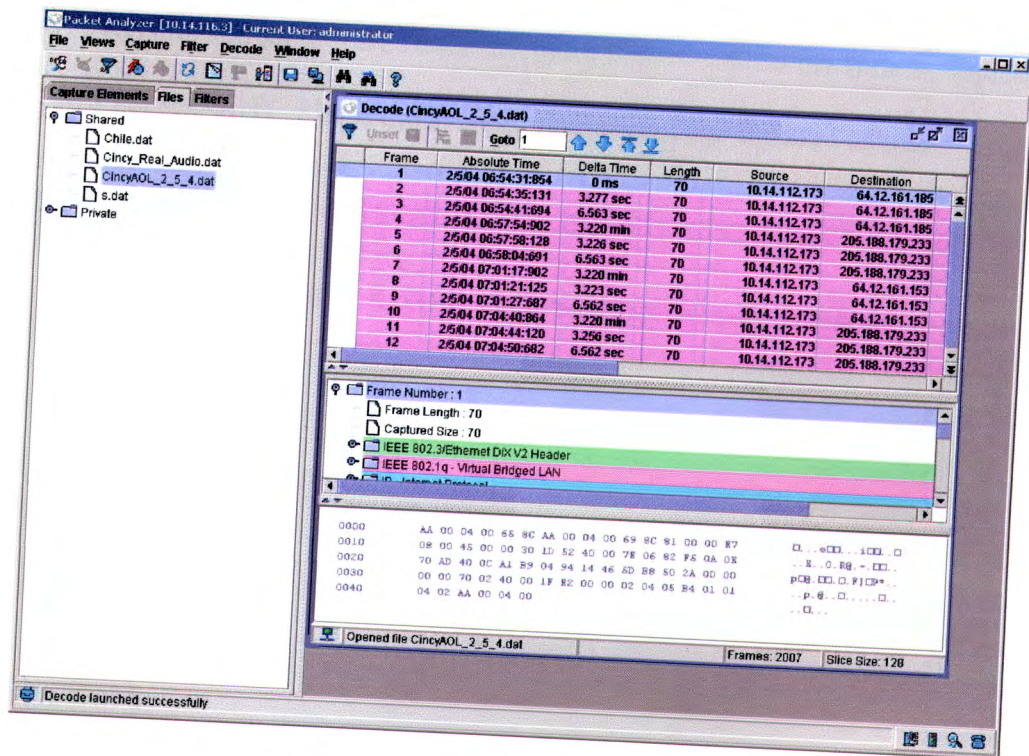


Figure 7. Analyzing the Packets

This shows packets with a destination, source, and time with a specific protocol.

This feature has allows NCS to find users on the network who are using AOL, Real streaming audio, and another of other protocols that present security and bandwidth concerns.

5.2 Setup a historical tracking system for bandwidth across designated ports.

I agreed to setup a tracking system for NCS across key ports on the Core A Catalyst 6509. This tracking keeps track of the utilization of bites in and bites out. Upon some research I spoke with a coworker who had heard of the Multi Router Traffic Grapher, which was open source and based on Perl. My boss was excited to hear open source and since Perl was free as well he was on board. I built the configuration files per specific ports he requested. These ports are on the Core A. The Regional Network

Center (RNC) link shown at the bottom of Figure 8 is the link to the Internet and what is called “J&J net” (WAN). I built the HTML navigation page for ease of use.

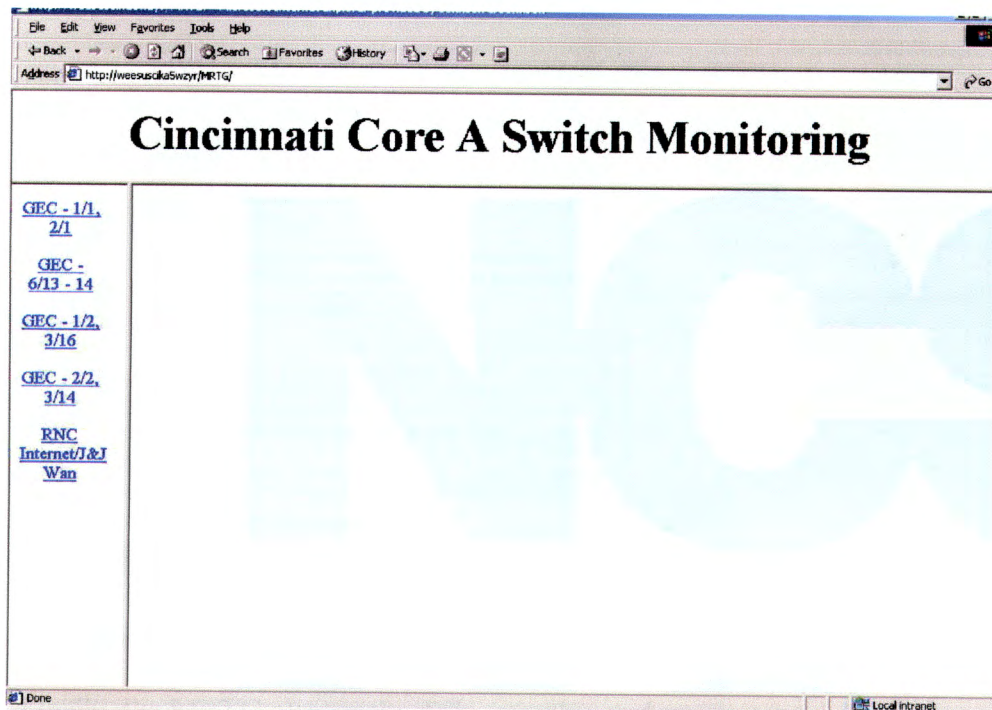


Figure 8. Navigation for Core A Historical Data

Figure 9. shows the thirty-minute utilization of ports 1/1 and 2/1. These ports are Trunk to Core Switch B. Core switch B is a redundant switch set up for support of the server core, Internet, and WAN connection. The green fill in the chart shows the bites in. The blue line on top represents the bites out. The Maximum amount of bites for that period is given under the chart along with the average and “current.” Current is not exactly accurate since one cannot physically watch the chart change.

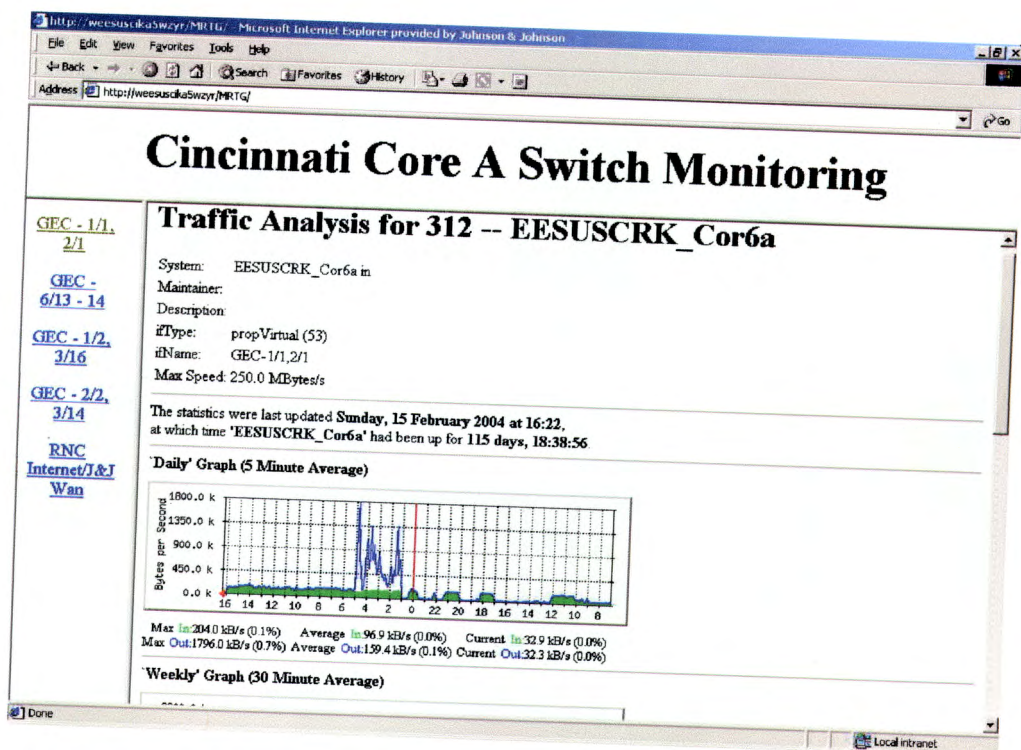


Figure 9. Thirty-minute Bandwidth Chart for Ports 1/1 and 2/1

Finally, the MRTG also tracks daily, monthly and yearly usage. This allows NCS to examine the charts and check for trends. This is something that was lacking prior to this solution. A port would get overworked and need a redundant connection, but the network administrator and management had no way of knowing. Figure 10. shows the RNC connection to the Internet and to the WAN. This is the exact same page (except for different ports) as shown in Figure 9. except it shows historical tracking instead of the 30-minute chart.

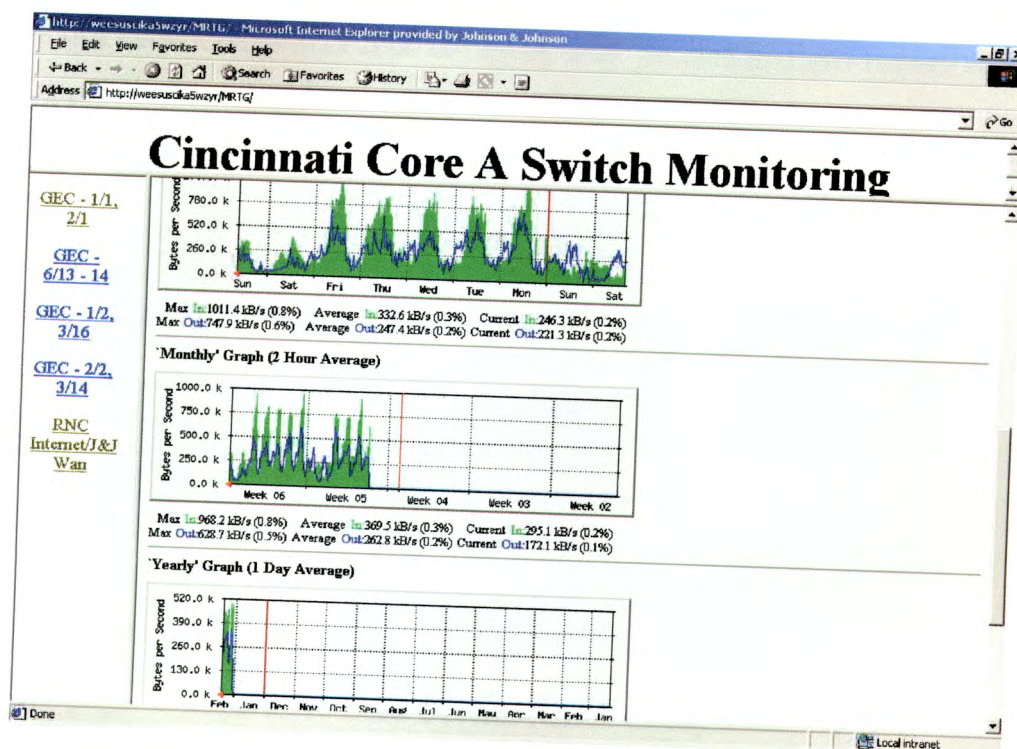


Figure 10. Historical Tracking of the RNC for Daily, Monthly and Yearly Data

5.3 Implement Ciscoworks 2000.

Ciscoworks 2000 is powerful in two respects. It allows both monitoring and management of the network. My decision to use it was driven by the fact that Johnson & Johnson already had a license for it, although NCS had to pay for its specific use for the Midwest region. I had to do a number of things to correctly configure the software. The hardware devices throughout the network had to be configured. These configurations including: setting up community and Simple Network Management Protocol (SNMP) strings. The "code" (Operating System) on those devices had to be upgraded as well. Finally seed devices had to be specified so that Ciscoworks could reach across the network to discover all nodes on the LAN and WAN. There are also a number of unforeseen port conflicts that I ran into. These ports had to be changed to open ports on the desktop. Figure 11. shows the configuration of the seed devices. These are the

devices that allow Ciscoworks 2000 to “spider web” out and find new regions of the LAN/WAN.

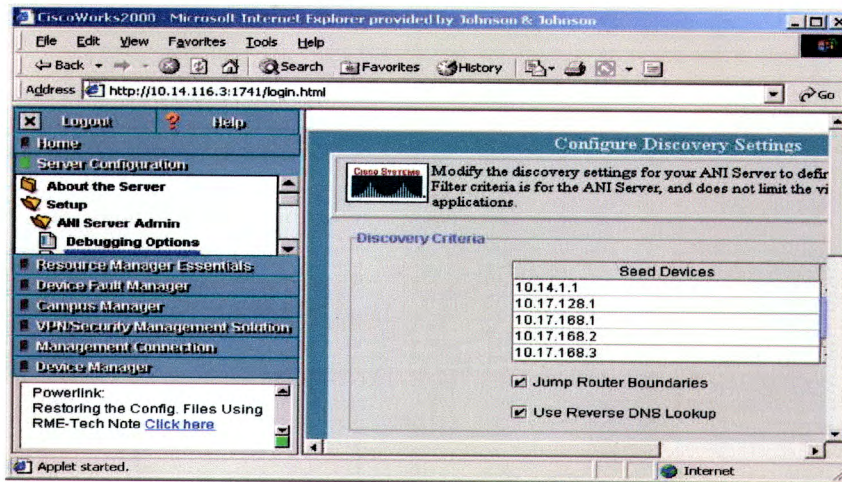


Figure 11. Seed Devices (Cisco Catalyst 6509's)

Ciscoworks 2000's ability to monitor the network goes not just to its own devices, but also to all other devices on the network. This was part of my reasoning for choosing this software. This gave the NCS staff the ability to quickly find devices on the network, both from a physical and logical location. Figure 12. shows part of the list from “User Tracking.” User Tracking allows the user to find devices on the network, their MAC address, IP, device they are on.

User Tracking (admin@ANSERVER4.1.WUESUSLIKASWZVR) - Microsoft Internet Explorer provided by Johnson & Johnson

UserName	MACAddress	HostName	IPAddress	Subnet	DeviceName	Device	Port	PortName	PortState	VTPDomain	VLAN	VLANType	LastSeen
297	00-00-85-0...	eesusclic33...	10.14.2...	10.14.21.0	10.14.1.142	10.14.1.142	294		static	EESUS	VLAN0001	ethernet	2004/02/15 14:09:33
298	00-00-85-0...	eesusclic33...	10.14.2...	10.14.21.0	10.14.1.142	10.14.1.142	513		static	EESUS	VLAN0142	ethernet	2004/02/15 14:10:4
299	00-00-85-0...	eesusclic33...	10.14.2...	10.14.21.0	10.14.1.142	10.14.1.142	514		static	EESUS	VLAN0142	ethernet	2004/02/15 14:14:4
300	00-00-85-0...	eesusclic33...	10.14.2...	10.14.21.0	10.14.1.142	10.14.1.142	418		static	EESUS	VLAN0142	ethernet	2004/02/15 14:10:1
301	00-00-85-0...	eesusclic22...	10.14.1...	10.14.12.0	10.14.1.72	10.14.1.72	518		static	EESUS	VLAN0072	ethernet	2004/02/15 14:18:1
302	00-02-a5-8...	eesusclicpn...	10.14.1...	10.14.127.0	10.14.1.3	10.14.1.3	912		static	EESUS	VLAN0205	ethernet	2004/02/15 14:23:4
303	00-02-a5-8...	eesusclicpn...	10.14.1...	10.14.127.0	10.14.1.3	10.14.1.3	989		static	EESUS	VLAN0205	ethernet	2004/02/15 14:08:4
304	00-02-a5-8...	eesusclicps0...	10.14.1...	10.14.127.0	10.14.1.3	10.14.1.3	7119	Eesus...	static	EESUS	VLAN0205	ethernet	2004/02/15 14:09:2
305	00-02-a5-8...	eesusclicps0...	10.14.1...	10.14.127.0	10.14.1.3	10.14.1.3	7110	Eesus...	static	EESUS	VLAN0205	ethernet	2004/02/15 14:09:2
306	00-50-8b-8...	eesusclicfx0...	10.14.1...	10.14.128.0	10.14.1.3	10.14.1.3	448	eesus...	static	EESUS	VLAN0207	ethernet	2004/02/15 14:09:2
307	00-50-8b-8...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	844	Eesus...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:22:4
308	00-08-02-5...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	834	Eesus...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:13:0
309	00-02-a5-4...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	834	Eesus...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:08:4
310	00-08-02-5...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	848	Excha...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:20:4
311	00-02-a5-4...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	831	Eesus...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:20:3
312	00-08-02-5...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	835	Eesus...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:11:4
313	00-02-a5-4...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	832	Excha...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:06:4
314	00-08-02-5...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	845	Eesus...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:06:4
315	00-08-02-5...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	841	EESU...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:13:3
316	00-02-a5-4...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	838	Eesus...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:13:3
317	00-02-a5-4...	eesusclicfx...	10.14.1...	10.14.130.0	10.14.1.1	10.14.1.1	847	Excha...	static	EESUS	VLAN0210	ethernet	2004/02/15 14:10:4
318	00-10-4b-8...	eesusclicsm...	10.14.1...	10.14.124.0	10.14.1.4	10.14.1.4	63		static	EESUS	VLAN0210	ethernet	2004/02/15 14:11:4
319	00-0b-cd-9...	eesusclicart...	10.14.1...	10.14.124.0	10.14.1.4	10.14.1.4	47	eesus...	static	EESUS	VLAN0202	ethernet	2004/02/15 14:07:3
320	00-0b-cd-9...	eesusclicart...	10.14.1...	10.14.124.0	10.14.1.4	10.14.1.4	46	eesus...	static	EESUS	VLAN0202	ethernet	2004/02/15 14:12:2
321	00-0b-cd-9...	eesusclicart...	10.14.1...	10.14.124.0	10.14.1.4	10.14.1.4	45	eesus...	static	EESUS	VLAN0202	ethernet	2004/02/15 14:06:4
322	00-0b-cd-9...	eesusclicart...	10.14.1...	10.14.124.0	10.14.1.4	10.14.1.4	44	eesus...	static	EESUS	VLAN0202	ethernet	2004/02/15 14:10:1
323	00-e0-61-2...	eesusclicic1...	10.14.2...	10.14.21.0	10.14.1.142	10.14.1.142	247		static	EESUS	VLAN0142	ethernet	2004/02/15 14:17:1
324	00-0b-cd-9...	eesusclicap...	10.14.1...	10.14.127.0	10.14.1.3	10.14.1.3	435	eesus...	static	EESUS	VLAN0205	ethernet	2004/02/15 14:21:4
325	00-0b-cd-9...	eesusclicap...	10.14.1...	10.14.127.0	10.14.1.3	10.14.1.3	441	eesus...	static	EESUS	VLAN0205	ethernet	2004/02/15 14:09:1
326	00-0b-cd-9...	eesusclicap...	10.14.1...	10.14.127.0	10.14.1.4	10.14.1.4	645	eesus...	static	EESUS	VLAN0205	ethernet	2004/02/15 14:18:1
327	00-0b-cd-9...	eesusclicap...	10.14.1...	10.14.127.0	10.14.1.4	10.14.1.4	643	eesus...	static	EESUS	VLAN0205	ethernet	2004/02/15 14:05:3
328	00-0b-cd-9...	eesusclic2w...	10.14.1...	10.14.126.0	10.14.1.3	10.14.1.3	922		static	EESUS	VLAN0204	ethernet	2004/02/15 14:19:3
329	00-08-02-8...	eesusclic2w...	10.14.1...	10.14.124.0	10.14.1.4	10.14.1.4	818	EESU...	static	EESUS	VLAN0202	ethernet	2004/02/15 14:09:1
330	00-0b-cd-9...	eesusclic2k...	10.14.1...	10.14.126.0	10.14.1.3	10.14.1.3	920		static	EESUS	VLAN0204	ethernet	2004/02/15 14:23:4
331	00-a0-16-35...	eesusap13...	10.17.1...	10.17.168.0	EESMKJRSW...	10.17.168.10	Fa0/2		static	EESMX	default	ethernet	2004/02/15 14:05:3
332	00-01-e8-9...	eesusalrain...	10.17.1...	10.17.131.0	EESUSALB...	10.17.128.9	347		static	EESUSALB	VLAN0004	ethernet	2004/02/15 14:23:3
333	00-02-a5-8...	eesusalsm...	10.17.1...	10.17.137.0	EESUSALB...	10.17.128.2	745	Win2k...	static	EESUSALB	VLAN0401	ethernet	2004/02/15 14:20:1
334	00-02-a5-8...	eesusalsm...	10.17.1...	10.17.137.0	EESUSALB...	10.17.128.2	738	EESU...	static	EESUSALB	VLAN0401	ethernet	2004/02/15 14:07:1

4

Fetches 3533 row(s) in 7 second(s).

idle

Figure 12. User Tracking

The final piece of Ciscoworks 2000 that makes it so valuable is its ability to manage hardware on the network. Figure 13. shows the back of a Cisco Catalyst 4006 switch. This view shows the switch as if one was physically looking at the back of the device. The green ports represent a port with a device currently live, while the tan ones do not have a device plugged in. The drop down box shows all devices that Cisco View can utilize.

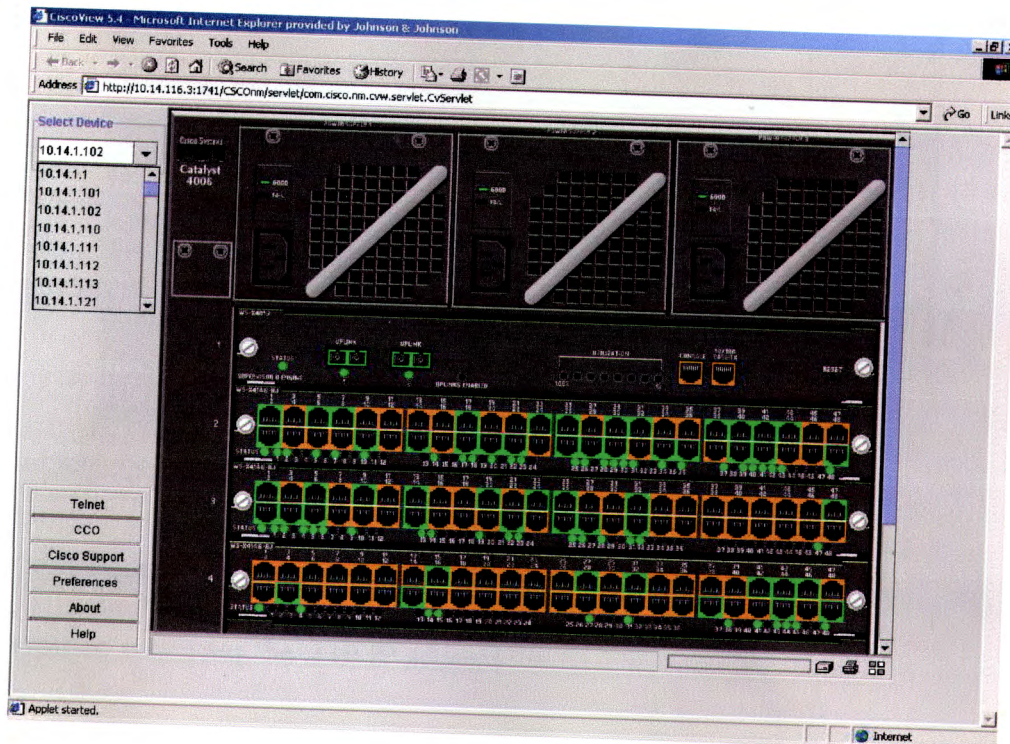


Figure 13. Cisco View

5.4 Install NAM Blade in Cincinnati

My group had a scheduled network outage in November of 2003 which I used to my advantage. To install a NAM Blade into a Catalyst 6509, the code on the switch must be upgraded, and the device must be powered down, then restarted. I was able to get the code upgraded, and make the necessary configuration changes on that Sunday. Figures 14., 15., 16., and 17. show the steps I have to take every time I need to log into the NAM Blade.

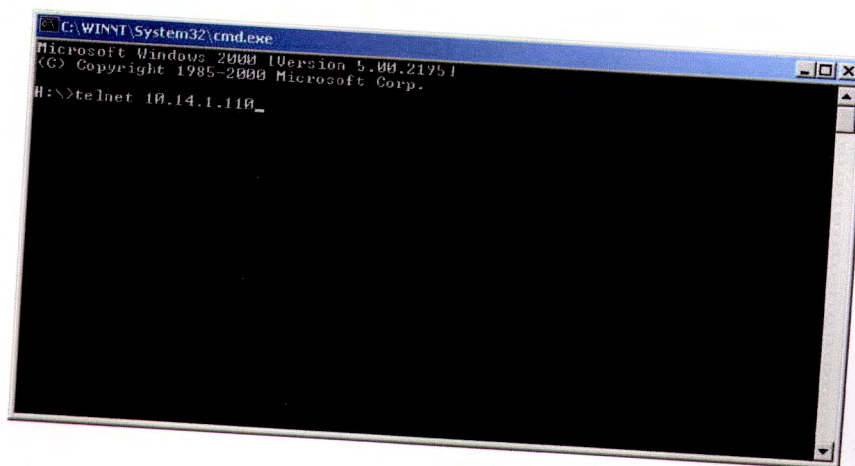


Figure 14. Telnet to the Core A router

To connect to the switch which houses the NAM blade, one must telnet first to the built in router, which has the .110 IP address.

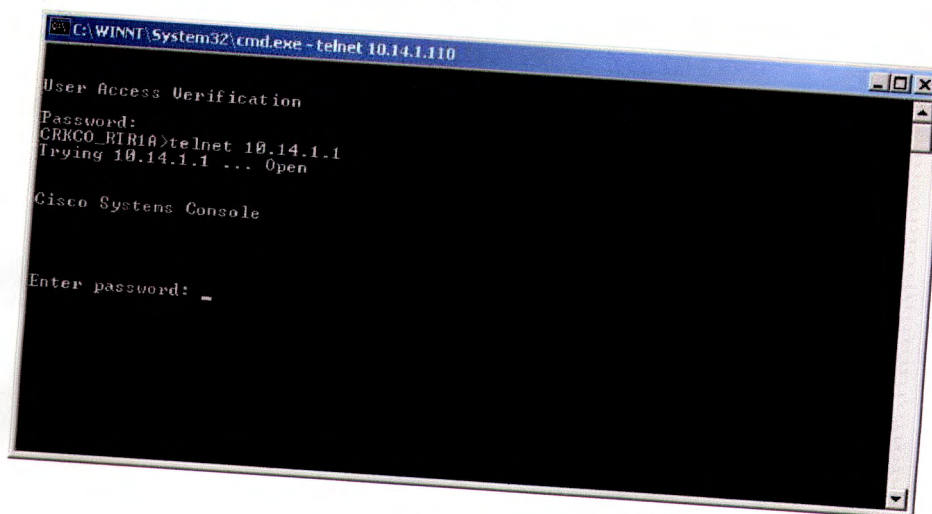
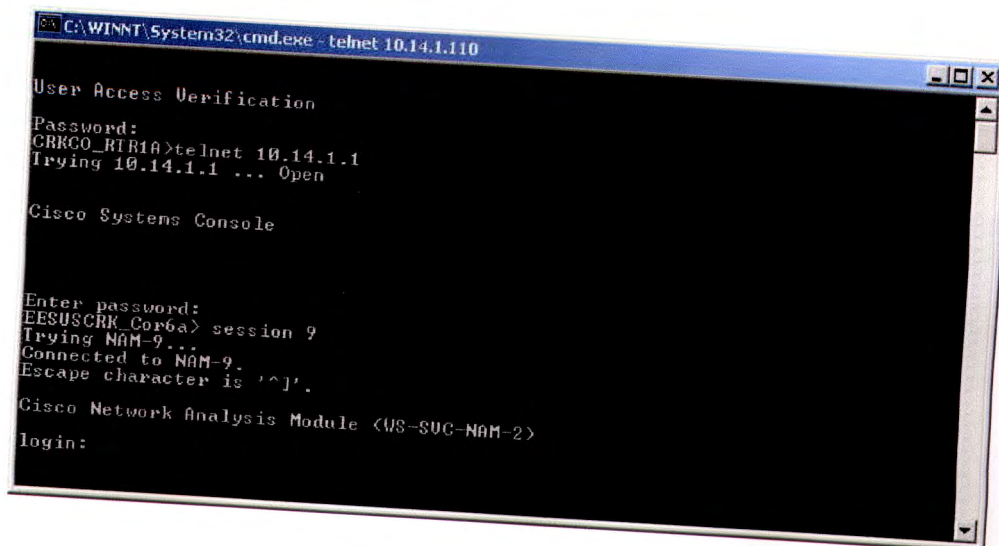


Figure 15. Telnet to the Core A switch



```
C:\WINNT\System32\cmd.exe - telnet 10.14.1.110

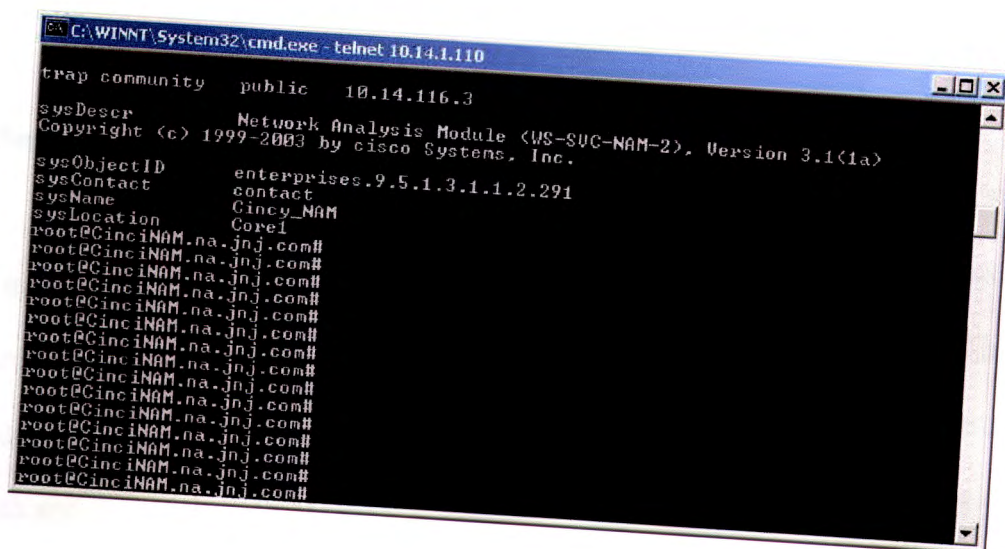
User Access Verification
Password:
CRKCO_RTR1A>telnet 10.14.1.1
Trying 10.14.1.1 ... Open

Cisco Systems Console

Enter password:
EESUSCRK_Cor6a> session 9
Trying NAM-9...
Connected to NAM-9.
Escape character is '^J'.
Cisco Network Analysis Module (WS-SUC-NAM-2)
login:
```

Figure 16. Session to the NAM Blade

Even though the NAM Blade is physically in the same case as both the Core A switch and Routers, they are logically separate. This is why it is required to “session” to the NAM Blade.



```
C:\WINNT\System32\cmd.exe - telnet 10.14.1.110

trap community public 10.14.116.3
sysDescr Network Analysis Module (WS-SUC-NAM-2), Version 3.1(1a)
Copyright (c) 1999-2003 by cisco Systems, Inc.
sysObjectID enterprises.9.5.1.3.1.1.2.291
sysContact contact
sysName Cincy_NAM
sysLocation Core1
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
root@Cincinnati.na.jnj.com#
```

Figure 17. NAM Configuration

For Security reasons I cannot show my entire configuration to the NAM Blade. This shows some of what I had to configure through the telnet sessions. Figure 18. shows the GUI that can be used once initial configuration is complete. The GUI on the NAM is

all but useless with the use of the Netscout software. The Netscout software allows for just about all functionality that the NAM Blade has to offer.

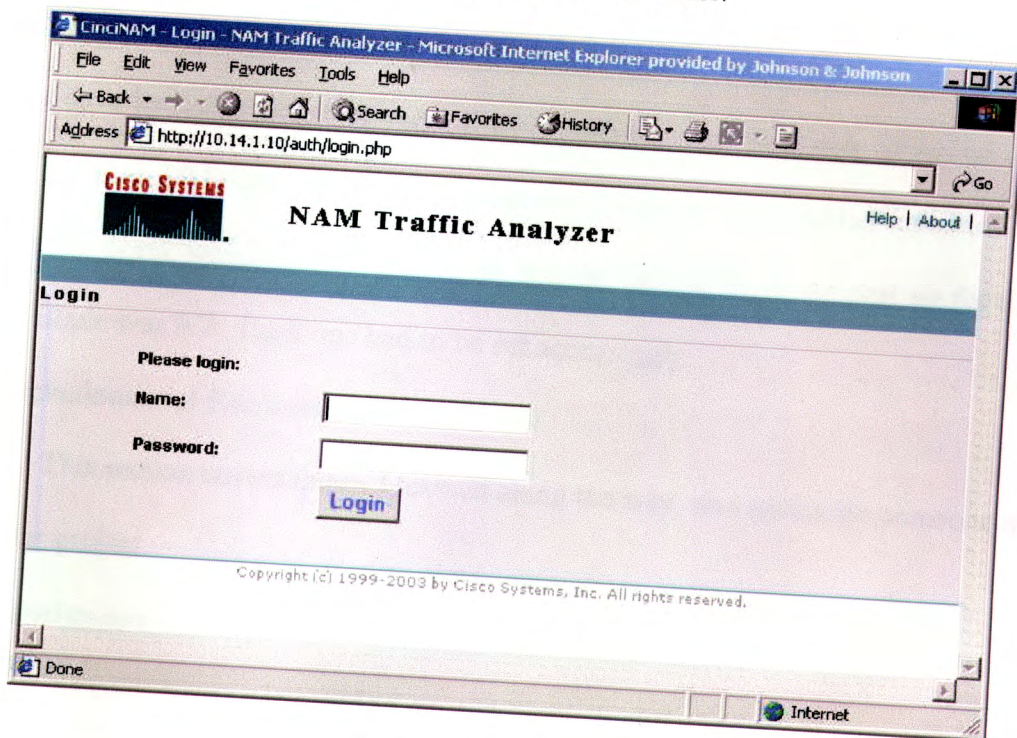


Figure 18. NAM GUI

5.5 Setup all routers and other devices to interact with Ciscoworks and MRTG.

The final piece for the solution was the configuration of all devices to function with my software selection. A number of devices had no SNMP scripts set up. I had to go through and find all devices that would not show up in Cisco View. I knew from asset records how many pieces of Cisco hardware were in the network. I then had to go through and find which ones were, and which ones were not in the network. Once I found which ones were not, I had to telnet to them and setup the SNMP scripts on each device.

I had a few other issues with some devices showing up, but they could not be managed or changed from the GUI within Ciscoworks. Each one of these turned out to

be an incorrect "Write" community string. When I set the community strings to match the ones I set within Ciscoworks the devices were then accessible.

All three NAM Blades were installed on a Catalyst 6509. Each of these devices did not have Switched Port Analyzer (SPAN) enabled. I had to enable SPAN on each 6509, and then SPAN ports per what I wanted to monitor. I also had to setup the SPAN destination ports, which was always the NAMs. In Cincinnati the port set for the NAM Blade was 9/7. Each one had to be set accordingly.

6 Conclusions and Recommendations

This section covers things I learned along the way, and advice for someone doing a similar project.

6.1 Conclusions

This project was proposed to me and I initially thought I could complete it by the end of the summer. Each time I got close I would run into either technical issues or bureaucratic issues. Three times I had to change devices that would house the solution. The first time I had the solution on an IBM desktop but I was told not to use a desktop and it went against Johnson & Johnson standards to have a desktop act as a server. When I tried to purchase a server I was forced to put the software first on a development/application server. I ran into SQL server on this server. After a number of emails with Cisco's tech support I found that Ciscoworks will not function correctly with SQL.

I was then forced to move the box to another development/application server only to find more port conflicts on it. The final solution was to purchase virtual servers, but

they would not come in until after I finished this project. I ended up putting the solution back on the original desktop.

Hardware seemed to be the recurring theme for my project. When I thought I was close to getting the NAM blades purchased I found out that the money that was allocated for their purchase was not in the budget. My project was at a standstill and I got the feeling that I would be searching for a new project. At the last minute, NCS' network administrator did some creative number crunching and found the money in the budget.

I ended up rather frustrated from all this because I almost could not finish this project multiple times. More than once I foresaw another six months of Senior Design so I could find a new project.

6.2 Recommendations

After working for a large company and doing a senior design project for them I found myself at its mercy. This was a warning I received from multiple faculty members. I would still recommend doing a Senior Design project for a large company, but ensure that money is allocated, and spend it immediately. Do not wait, because if the money is not spent, it is gone.

Finally, I worked closely with Cisco's technical support. When I started the project I did not have an ID of my own. I was constantly borrowing the network admin's and he would forward responses to me. When the announcement was made that the network admin was leaving I immediately got my own account. This meant I could log into Cisco's secure site, download patches on my own, and gain access to documentation. Had I not done this, I am not sure I would have completed the project in time. With my other duties at work it was not an issue waiting on the network admin to assist me, but

when I got my own I could focus more on my solution then some of my other duties. My recommendation is do not count on anyone else for anything on a Senior Design project.

7 References:

1. Braidich, Richard. Network Administrator (CCNP.)
2. Cisco. www.cisco.com , June 2003 – March 2004.
3. Troubleshooting Assistance Case (TAC.) www.cisco.com , June 2003 – March 2004.