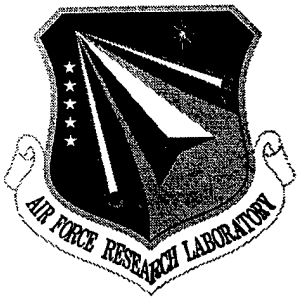
AFRL-IF-RS-TR-2001-106
Final Technical Report
June 2001




# MULTI DOMAIN NETWORK MANAGEMENTS (MDNM) PARTICIPATION IN JOINT EXPEDITIONARY FORCE EXPERIMENT (JEFX) AT LANGLEY AIR FORCE BASE

**BAE Systems**

**Adam Hovak**

*APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.*

**AIR FORCE RESEARCH LABORATORY**
**INFORMATION DIRECTORATE**
**ROME RESEARCH SITE**
**ROME, NEW YORK**

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2001-106 has been reviewed and is approved for publication.

APPROVED: 

SCOTT SHYNE
Project Engineer

FOR THE DIRECTOR: 

WARREN H. DEBANY, Technical Advisor
Information Gird Division
Information Directorate

If your address has changed or if you wish to be removed from the Air Force Research Laboratory Rome Research Site mailing list, or if the addressee is no longer employed by your organization, please notify AFRL/IFGA, 525 Brooks Road, Rome, NY 13441-4505. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

| REPORT DOCUMENTATION PAGE | Form Approved OMB No. 0704-0188 |
|---|---|



| 1. AGENCY USE ONLY *(Leave blank)* | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | JUNE 2001 | Final Jan 99 - Sep 01 |

**4. TITLE AND SUBTITLE**
MULTI DOMAIN NETWORK MANAGEMENTS (MDNM) PARTICIPATION IN JOINT EXPEDITIONARY FORCE EXPERIMENT (JEFX) AT LANGLEY AIR FORCE BASE

**5. FUNDING NUMBERS**
C - F30602-00-C-0210
PE - 63789F
PR - 233G
TA - 02
WU - 02

**6. AUTHOR(S)**
Adam Hovak

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
BAE Systems
Synectics Corporation
111 East Chestnut Street
Rome New York 13440

**8. PERFORMING ORGANIZATION REPORT NUMBER**
N/A

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
Air Force Research Laboratory/IFGA
525 Brooks Road
Rome New York 13441-4505

**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
AFRL-IF-RS-TR-2001-106

**11. SUPPLEMENTARY NOTES**
Air Force Research Laboratory Project Engineer: Scott S. Shyne/IFGA/(315) 330-4819

**12a. DISTRIBUTION AVAILABILITY STATEMENT**
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

**12b. DISTRIBUTION CODE**

**13. ABSTRACT** *(Maximum 200 words)*

This report describes the Multi Domain Network Management (MDNM) project, the MDNM development team and the Joint Expeditionary Force Experiment (JEFX). The MDNM project provides a network manager with the ability to view multiple domains in one Network Common Operational Picture (NCOP). Each domain interfaces with the NCOP through this boundary device. It is a controlled interface that sits between a low Network Management Station (NMS) and the NCOP. The NCOP uses Simple Network Management Protocol (SNMP) to query the Management Information Base (MIB) data of the low network manager. These MIB data contain up-to-date information about the resources that they manage. The data found at the low NMS is replicated and placed into the NCOP's data base. These data contain status information of the systems managed by the low NMS. The JEFX is designed to assess Air Force operations in a simulated war-fighting environment. JEFX also helps promote Expeditionary Aerospace Force, the Air Force's new concept of operations. EAF allows a uniquely tailored force to be used in a specific operation by taking pieces of each division and deploying them individually. The MDNM team attended JEFX to demonstrate the project's capabilities in a realistic test environment.

| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| Network Management, Boundary Device, Joint Expeditionary Force Experiment, JEFX | 20 |
| | 16. PRICE CODE |

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | UL |

# TABLE OF CONTENTS



## List of Tables



## List of Exhibits

# 1.0 INTRODUCTION

The Multi Domain Network Management (MDNM) engineering team participated in the Joint Expeditionary Force Experiment (JEFX) at Langley Air Force Base in Virginia. This paper describes the MDNM project, the MDNM development team and their respective duties, JEFX, testing performed at JEFX, user feedback, experimental code development, and users' quotes.

# 2.0 THE MDNM PROJECT

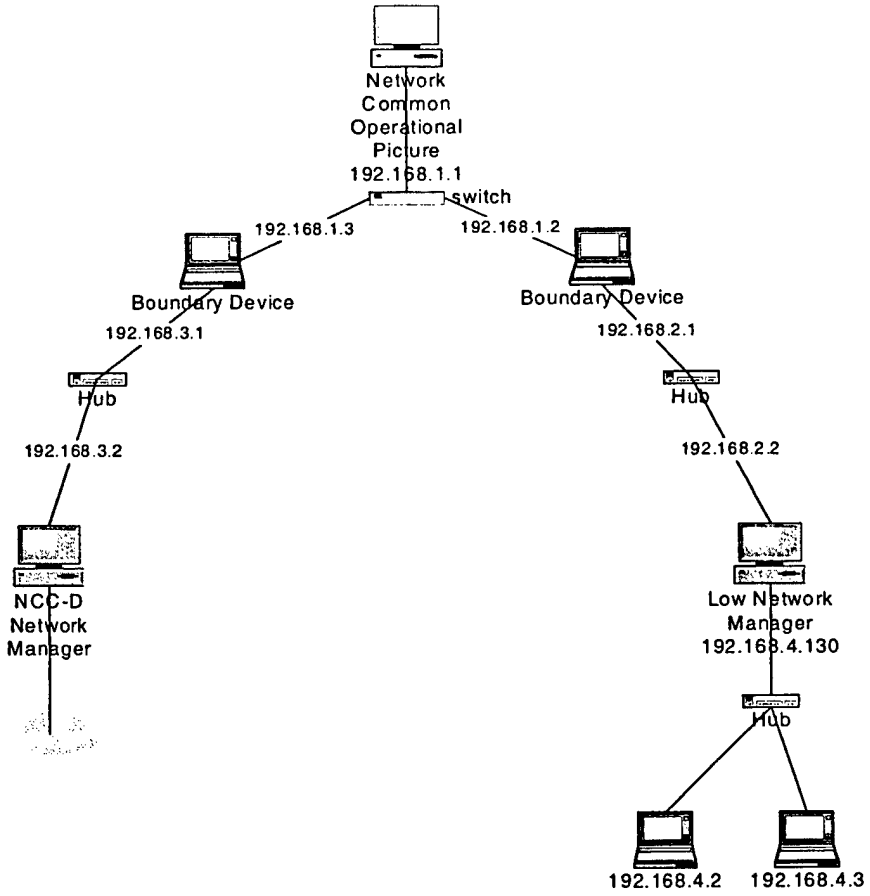
The MDNM project provides a network manager with the ability to view multiple domains in one network common operational picture (NCOP). Each domain interfaces with the NCOP through this boundary device. It is a controlled interface that sits between a low Network Management Station (NMS) and the NCOP (see Exhibit 1).

This architecture works as follows. The NCOP uses Simple Network Management Protocol (SNMP) to query the Management Information Base (MIB) data of the low network manager. These MIB data contain up-to-date information about the resources that they manage. The data found at the low NMS is replicated and placed into the NCOP's data base. These data contain status information of the systems managed by the low NMS.

A unique design of the boundary device is the ability to span Multi Level Security (MLS) domains. This is permissible because of our careful evaluation of each packet that tries to pass through it. When a packet arrives at the boundary device it is first met by the firewall. The firewall allows or denies the packet depending on origin, destination, and protocol. For instance, if a user on the NCOP wanted to telnet to the low NMS, the firewall configuration on the boundary device wouldn't allow this to occur because it only allows SNMP and ICMP.

The second stage of the boundary device is the proxy. The proxy is code that was developed by ARCA Systems. This code takes each individual packet, verifies that the SNMP command is allowed and then repackages the packet to ensure anonymity as well as command integrity. Anonymity is important so that the low NMS is not given any information about the NCOP. Command integrity is tested to ensure the validity of the command being sent based on the rules configured in /etc/SnmpProxy.cfg. For example, an SNMP Getrequest is denied from the low NMS to the NCOP but a Getrequest is allowed from the NCOP to the low NMS. Flow control is set this way because the NCOP holds information from multiple domains, which cannot be exchanged among the low domains.

**Exhibit 1. The Original MDNM Architecture**




## 3.0 THE MDNM TEAM

The MDNM team is an integrated team composed of representatives from AFRL, BAE SYSTEMS, and ARCA Systems. Mr. Scott Shyne of the Air Force Research Laboratory Distributed Information Systems Division (AFRL/IFGA) manages this advanced technology demonstration (ATD) and is supported by Messrs. Joe Riolo and Adam Hovak of BAE SYSTEMS and Messrs. Ken Seiss and Herb Markle of ARCA Systems.

Mr. Seiss is the developer for the MDNM project. Mr. Markle is the system architect. He also provides design assistance to Mr. Seiss and tests the code. Both Mr. Riolo and Mr. Hovak provide independent integration and testing of the boundary device as well as system and network administration functions. The team has had great success working together.

# 4.0 JOINT EXPEDITIONARY FORCE EXPERIMENT (JEFX)

The JEFX is designed to assess Air Force operations in a simulated war-fighting environment. JEFX also helps promote Expeditionary Aerospace Force (EAF), the Air Force's new concept of operations. EAF allows a uniquely tailored force to be used in a specific operation by taking pieces of each division and deploying them individually. As an example, this selective deployment could be done in lieu of deploying the entire 9th Air Force. The MDNM team attended JEFX to demonstrate the project's capabilities in a realistic test environment. A description of our demonstration is provided below.

The MDNM team was given a live SIPRnet feed from the Network Command Center Deployed (NCC-D) at Langley Air Force Base. The SIPRnet is a secret network to which the team was given access specifically for managing the 1,050 JEFX-related nodes. The boundary devices acted as controlled interfaces between the NCOP, and both the SIPRnet and the team's model of the NIPRnet. The NIPRnet is an Air Force unclassified network. A model of it was used since the boundary device is not accredited and therefore did not permit spanning of multiple security domains. The team's demonstration provided an NCOP of both the JEFX SIPRnet and the modeled NIPRnet domains. This showed how both domains could be easily managed from one workstation.

JEFX was held at various military installations across the United States. The main Air Force bases were Nellis in Nevada, Hurlburt in Florida, and Langley in Virginia. The air exercises took place at Nellis; the main operations took place at Hurlburt with Langley acting as a backup to Hurlburt. The MDNM team was stationed in the NOSC at Langley.

# 5.0 TESTING

Testing is an essential part in developing a project. On the MDNM project, functionality as well as security is tested. Functional testing is done to prove the MDNM accomplishes the goals it has been designed to accomplish. Security testing is done to expose vulnerabilities in the boundary device.

## 5.1 FUNCTIONAL TESTING

The team performed numerous functional tests at Langley Air Force Base.

### 5.1.1 TIMING TESTS

For each timing test the team gathered 12 synchronization times, discarded the high and low times, and averaged the 10 best.

In the first timing test the team tested the time it took for the NCOP to synchronize with a low NMS managing 250 nodes. The tests concluded that synchronization takes an average of 52.7 seconds to complete. During this synchronization, the Central Processing Unit (CPU) of the low NMS peeks at approximately 80%.

The second test consisted of a synchronization experiment between the NCOP and a low NMS managing 1,033 nodes. The team concluded that synchronization takes an average of 180.7 seconds.

The third timing test consisted of 1,054 nodes. In this test it was found that it took an average of 185.1 seconds for the NCOP to synchronize with the low NMS. The team also noted that the CPU utilization on the boundary device was at approximately 57% while running x-windows and 27% while not running x-windows.

### 5.1.2 COMMAND TESTING

The third test was an exhaustive test whereby all SNMP commands were systematically tested.

The MDNM team created a program to ease the functionality testing process of the boundary device. The primary interface was written in tcl/tk and is called **snmptester.ui.tcl.** It works by accessing the SNMP utilities provided with HP Openview. A screenshot of snmptester.ui.tcl is shown below in Exhibit 2.

One command was tested fully while all other commands were turned off. The flow control is managed by /etc/SnmpProxy.cfg. This file was edited in order to test the boundary device. It is broken into two sections and each section is divided into two columns. The sections are High to Low traffic and Low to High traffic. The first column lists the available SNMP commands and the second column allows or denies the flow of that particular SNMP command. An example of /etc/SnmpProxy.cfg is shown below.

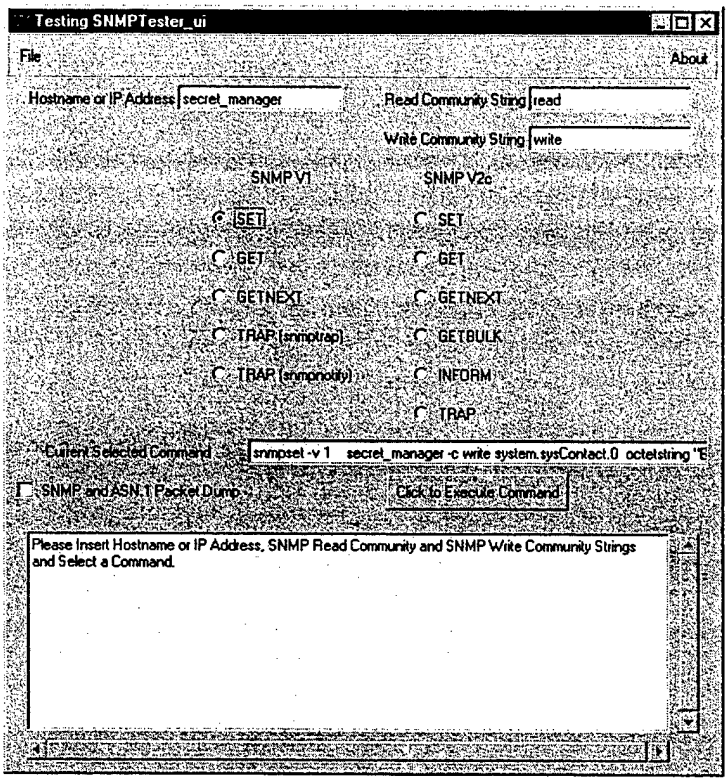
```
/* code snippet
SNMP v1         allow
SNMP v2         allow

H2Lset allow

L2Hset denied
L2Hget          denied

*/ end of code snippet
```

## Exhibit 2. Screen Shot of snmptester.ui.tcl




The testing continued until all commands were exhausted. Table 1 shows an example of the desired test results for a correctly configured boundary device.

## Table 1. Rules for a Correctly Configured Boundary Device

| COMMAND | DESCRIPTION | HIGH TO LOW | LOW TO HIGH |
|---|---|---|---|
| Set | Assigns a value to a variable | Conditionally permitted | Not permitted |
| Get | Returns value of variable(s) | Permitted | Not permitted |
| GetNext | Returns a value list of variables | Permitted | Not permitted |
| GetBulk | Returns a number of variables | Permitted | Not permitted |
| Inform | Transmits unsolicited information | Not permitted | Not permitted (Investigating) |
| Trap | Transmits unsolicited information | Not permitted | Permitted |
| Responses | Responses to commands | Not permitted | Permitted |

Documentation is very important when creating test scenarios. The documentation included:

- The test being performed.
- The current configuration of the network, particularly the switches in /etc/SnmpProxy.cfg.
- The expected results.
- The actual results (i.e., does the proxy accomplish the required functionality for network management?).

The functional testing proved to be fairly successful. The team performed 16 tests of which only 2 failed. All commands were allowed through the boundary device except for SNMP traps. SNMP version 1 traps did not go through the boundary device regardless of the configuration of the boundary device. This information was passed to Mr. Seiss and he is currently addressing the issue.

### 5.1.3 SECURITY TESTING

During the security test plan the boundary device was bombarded with some of the most current intrusion tools found on the Internet.

The testing began with an evaluation of the functionality of the available software and its usefulness for hacking the boundary device. The tools chosen by the team were Ethereal, Strobe, Vetescan, and Ostronet. After testing each tool for ease of use and number of incorporated tools, the team chose Ostronet because it was easy to use as well as purposeful to the testing. Ostronet is a collection of Internet tools that provides a domain scanner, port scanner, Ping and Traceroute features, host address-to-name and name-to-address resolution, detailed output, Whois and Ph clients, and a finger utility.

### 5.1.4 PENETRATION TESTING

In the first test the team utilized the Scan Wizard featured in the Ostronet tools package. The Scan Wizard is a port scanner used to detect the boundary device. The scanner was assigned a subnet of 192.168.2.*; however, the scanner did not detect the boundary device in this test.

In the second test, the port scanner was used again to test all ports on the boundary device. After a thorough scan of the boundary device, no ports were shown to be open.

# 6.0 USER FEEDBACK

During the JEFX exercise the team interacted with many users in the NOSC at Langley Air Force Base. The users dealt with network management software everyday, managing both the unclassified NIPRnet and the secret network SIPRnet. The support team at Langley used programs like What's Up Gold and HP Openview to manage their networks. One strong complaint about their software was that it was either too difficult to use or it was too general.

What's Up Gold is a network management program that shows generic network infrastructure. It only monitors specific switches and routers at critical throughput points in the network. The support group at the NOSC stated that What's Up Gold could detect a problem, but that it could not identify the problem. HP Openview had to be used since this program has the ability to show which individual node has the problem. The support staff at the NOSC told us that HP Openview is difficult to use because it provides a very complicated picture.

The support staff enjoyed the team's centralized view of the network and called it a "good idea." One member of the staff even asked why this idea took so long to be presented.

Another member of the staff mentioned that, "this capability is even more relevant now that 3-dimensional networking is available. 3-D networks allow multiple virtual LANs on the same network. This can allow different security domains to travel over the same infrastructure." For example, the JEFX Network infrastructure was classified as secret but with encryption, unclassified data could be sent over it. Therefore if a network administrator has both networks correlated on the same display it would be easier to pinpoint a network hardware problem.

## 6.1 SUGGESTIONS

Along with praise comes criticism. The team was lucky in that it received constructive criticism from actual network managers at JEFX. They said that a network common operational picture was very useful as long as some extra ideas were incorporated. They suggested adding a drill-down capability, allowing the NCOP the ability to query specific system information from individual nodes. Adding a drill-down capability would facilitate the gathering of useful information such as system contact, system description, and system location. This information could then be used in debugging problems.

# 7.0 EXPERIMENTAL CODE DEVELOPMENT

The user feedback the MDNM team received from the support staff in the NOSC at Langley led to a new idea, which was to use the test network side of the MDNM demonstration to try out new code. This new code would be created during JEFX and it would provide the capabilities suggested by the NOSC support staff.

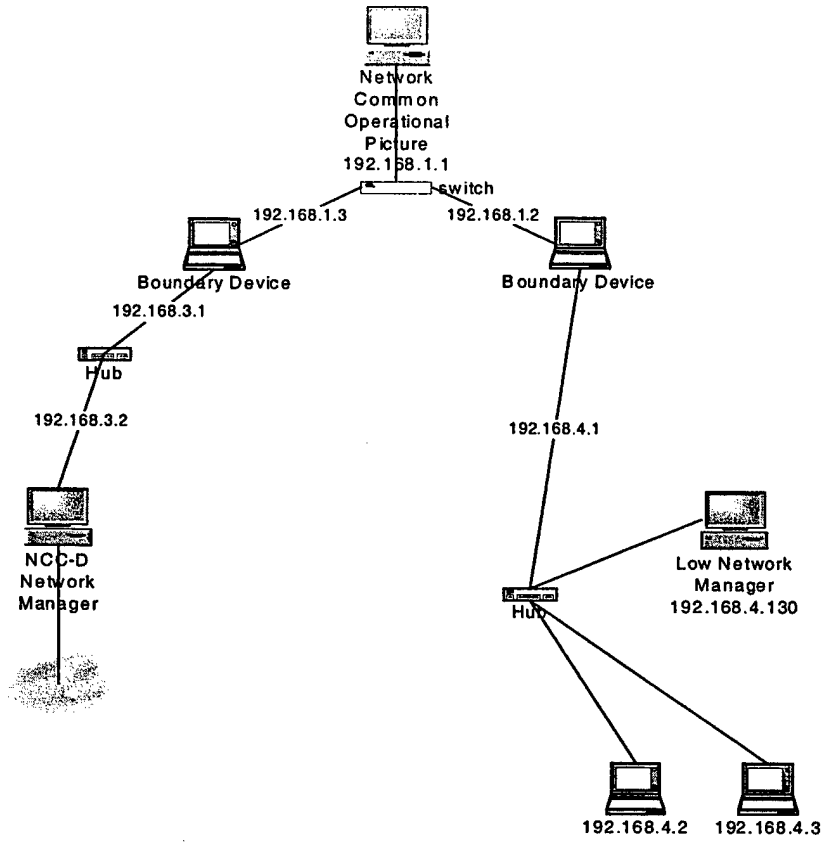
When Mr. Seiss arrived at the JEFX demonstration he was met with the challenge of creating new code to accommodate the suggestions of the NOSC support staff. The plan was to design a second proxy to run on the controlled interface. This second proxy would facilitate a drill-down capability to the NCOP, i.e., the NCOP would be able to query specific system information from individual nodes.

During the last few days of the exercise, an Alpha version of the second proxy was created. This proxy allowed the NCOP to query one node on the test network. The second proxy only allowed the NCOP to query one node because there were some troubles involving Access Control Lists (ACL). The Alpha version of the code was used to enhance the MDNM demonstration. The second proxy was run on the boundary device controlling the information exchange between the NCOP and the test network.

The second proxy, proxy2, was designed for a purpose different from that of the original proxy. In order for proxy2 to work the architecture of the demo needed to be changed (see Exhibit 3).

As seen in Exhibit 3, the boundary device is now connected directly to the lower domain. While this architecture allows the NCOP the ability to query individual hosts, it is also much more of a security risk. Adding the boundary device to the local domain allows the hosts direct access to it, and there is always a potential security threat if a user can access a boundary device.

**Exhibit 3. New Multi Domain Network Management Architecture**




## 8.0 CONCLUSION OF JEFX

Upon the completion of JEFX, the MDNM team was met with a few challenges involving the removal of the demonstration hardware from the NOSC so it could be returned to AFRL. Since the equipment was connected to the secret network SIPRnet, the systems had to be declassified. Declassification involved "wiping clean" all the machines.

About two days before the exercise ended, the team began the tedious process of cleaning the hard disks. The team soon discovered that Langley support staff were not familiar with declassifying machines. In fact, they had no software suitable for this purpose.

A few phone calls were made to Air Force Research Lab (AFRL) asking for assistance. The site had two applications that could be used to declassify machines, UniShred Pro and Norton Wipe. The software was shipped overnight to the security manager at Langley. Once the team received the software, the first step was to start UniShred pro on each of the Sun boxes. It was not as

easy, however, to declassify the Intel platforms. The program, Norton Wipe, was limited to wiping only 2 gigabyte partitions. In order to declassify the machines, the 2 20-gigabyte drives had to be broken up into 10 partitions each. The other 2 hard drives were only 4 gigabytes and were broken up into 2 partitions each. After all the partitions had been created the team ran into one more problem: someone had to physically start each partition format every 90 minutes. This left the team with the inconvenience of manning the declassification process throughout the night. After a few scheduling discussions, a plan was decided and, by morning, all the hard drives were completely wiped.

The last task required before the team could leave the NOSC was the certification of the machine declassification. Lt. Warne was enlisted to supervise the removal of the SECRET stickers from the machines. Sgt. Porter checked out our equipment and the team headed home.

## 9.0 LESSONS LEARNED

JEFX was a very useful experiment in which to participate with the Multi Domain Network Management project. The team was afforded the chance to test the product in a real-world situation and receive user feedback. JEFX was structured such that the software could be tested in between demonstrations and new code created to reflect the user feedback received by the team. Having actual support staff give real-time input led the team to new development ideas as well as modifications to make the user's job a little easier.

## 10.0 IMPORTANT QUOTES

Throughout the two weeks at JEFX the team gave demonstrations to users as well as their supervisors. After the overwhelmingly positive feedback, it is useful to record the users' thoughts pertaining to the MDNM project.

*"This type of system would give me the capability to know specifically what systems within both SIPRnet and NIPRnet were operational from one workstation."* Captain Hugh St. Martin

*"What took so long? Why didn't somebody think of this earlier?"* Captain Matthew Gebhardt

*"This fine grain control may significantly enhance firewall capability at the base and MAJCOM level."* Captain Travis Ross.

*"The correlation capability provided by this system would give us a much better understanding of the potential relationships of individual network events occurring within different security domains."* Tech Sergeant Terrence Bruce

*"I hope you're planning to participate in JEFX '02 as a Cat I or Cat II. I believe your program is providing a critical capability to the Air Force Network Operations Personnel."* Lieutenant Colonel Gordon Mann

## 11.0 GLOSSARY

| | |
|---|---|
| AFRL | Air Force Research Laboratory |
| CPU | Central Processing Unit |
| ICMP | Internet Control Message Protocol |
| JEFX | Joint Expeditionary Force Experiment |
| MDNM | Multi Domain Network Management |
| MIB | Management Information Base |
| NCOP | Network Common Operational Picture |
| NIPRnet | An unclassified Internet Protocol Routing Network |
| NMS | Network Management Station |
| NOSC | Network Operations Security Center |
| SIPRnet | A Secret Internet Protocol Routing Network |
| SNMP | Simple Network Management Protocol |