An investigation of network security management methods

Shamila Anuranga Ratnayake
Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/theses_hons

Part of the Information Security Commons

Recommended Citation
https://ro.ecu.edu.au/theses_hons/1260

This Thesis is posted at Research Online.
https://ro.ecu.edu.au/theses_hons/1260
Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.

- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author’s moral rights contained in Part IX of the Copyright Act 1968 (Cth).

- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
AN INVESTIGATION OF NETWORK SECURITY MANAGEMENT METHODS

By
Shamila Anuranga Ratnayake

This thesis is presented in fulfilment of the requirements for the degree of Bachelor of Science Honours (Computer Science)

Faculty of Computing, Health and Science
Edith Cowan University

December 2005
USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.
ABSTRACT

Network Management (NM) is concerned with reducing complexity and managing cost. The traditional NM tools and techniques are based on the Open System Interconnection (OSI) NM model. However, several drawbacks have been identified when managing a network using traditional NM tools (Sarkar & Verma, 2001).

Network security is a major issue when managing a network. Even though the technology assists to reduce security risks, unless properly managed, the security measures may not do the job as expected.

The State Model (SM) diagram is a new method, which may assists in managing the network. This new method may provide functionality not currently offered by current NM tools. Furthermore it may be possible to integrate the SM with NM tools. SM diagrams integrate relevant output from devices with protocol finite state information by means of tables. The diagrams are modular and hierarchical thereby providing top down decomposition by means of levelling. Furthermore, their modular, hierarchical characteristics allow technical detail to be introduced in an integrated and controlled manner.

The State Model Diagrams were evaluated as a network management tool by twenty participants. The results clearly demonstrated that these diagrams could be of value not only as a NM tool but also as a tool for network security management.
DECLARATION

I certify that this thesis does not, to the best of my knowledge and belief:

(i) incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education.

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material.

I also grant permission for the Library at Edith Cowan University to make duplicate copies of my thesis as required.

Signature: 

Date: 05/1/2006
ACKNOWLEDGEMENTS

Thank you most of all to my supervisor, Dr. S. P. Maj for his commitment of time, guidance and for being patient and understanding. I would also like to thank my lecturer Mrs. Barbara Combes and Mr. Bao Tran for their guidance and support throughout. Without their support I would not have come this far. I would also like to thank both of my parents, my father, Mr H. Ratnayake and my mother, Mrs. V Ratnayake, for their hard work that sent me to Australia and made this possible. Last but not least, I would like to extend my thanks to my loving girlfriend, Miss P. Peiris, for being my sleepless companion all this time. To everyone else that I forgot to mention, thank you.
# TABLE OF CONTENTS

**USE OF THESIS** ....................................................................................................................................... II

**ABSTRACT** ............................................................................................................................................... III

**ACKNOWLEDGEMENTS** ...................................................................................................................... V

**1.0 INTRODUCTION** ................................................................................................................................ 1

1.1 **BACKGROUND TO THE STUDY** ................................................................................................. 1
1.2 **PURPOSE OF THE STUDY** ............................................................................................................. 3
1.3 **HYPOTHESIS** ................................................................................................................................. 4
1.4 **RESEARCH QUESTIONS** ................................................................................................................... 4

**2.0 LITERATURE REVIEW** .................................................................................................................... 5

2.1 **GENERAL LITERATURE** ................................................................................................................ 5

**3.0 THEORETICAL FRAMEWORK** ..................................................................................................... 18

3.1 **IDENTIFICATION OF VARIABLES IMPACTING ON THE HYPOTHESIS** ........................................ 18
3.2 **TARGETED POPULATION** .............................................................................................................. 18

**4.0 MATERIALS AND METHODS OF INVESTIGATION** .................................................................... 19

4.1 **DESCRIPTION OF MATERIALS TO BE EMPLOYED** ................................................................... 19
4.2 **DESIGN AND PROCEDURE OF THE STUDY** .............................................................................. 19
4.3 **DATA COLLECTION** ...................................................................................................................... 36
4.4 **ETHICAL CONSIDERATION** .......................................................................................................... 36

**5.0 RESEARCH FINDINGS** .................................................................................................................. 37

5.1 **AN EVALUATION OF STATE MODEL DIAGRAMS** ..................................................................... 37
5.2 **FURTHER RESEARCH** .................................................................................................................... 41
5.3 **LIMITATION OF THE STUDY** ....................................................................................................... 41

**6.0 CONCLUSION** ................................................................................................................................ 42

**7.0 REFERENCES** ................................................................................................................................... 43

**APPENDIX A** ........................................................................................................................................ 46

**APPENDIX B** ........................................................................................................................................ 51

**APPENDIX C** ........................................................................................................................................ 56
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A Typical Network Management Architecture</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>OSI systems management overview</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Router State Model (RIP)</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>Switch State Model</td>
<td>15</td>
</tr>
<tr>
<td>5</td>
<td>Wireless Access Point State Model</td>
<td>16</td>
</tr>
<tr>
<td>6</td>
<td>PIX Firewall State Model</td>
<td>17</td>
</tr>
<tr>
<td>7</td>
<td>Experiment 1 with single Internetworking device (firewall)</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>Experiment 2 with multiple Internetworking devices (router, firewall)</td>
<td>20</td>
</tr>
<tr>
<td>9</td>
<td>Experiment 3 with multiple Internetworking devices (router, firewall and switch)</td>
<td>21</td>
</tr>
<tr>
<td>10</td>
<td>Experiment 4 with multiple Internetworking devices (router, firewall, switch, access point)</td>
<td>21</td>
</tr>
<tr>
<td>11</td>
<td>Experiment 5 with multiple Internetworking devices in the LAN</td>
<td>21</td>
</tr>
<tr>
<td>12</td>
<td>Network management evaluation procedures</td>
<td>22</td>
</tr>
<tr>
<td>13</td>
<td>Evaluating the effectiveness of NM using the SM and Ciscoworks</td>
<td>22</td>
</tr>
</tbody>
</table>
1.0 INTRODUCTION

1.1 Background to the study

Network Management

Deri, L. (1996, para 1) states that, “The increasing complexity and heterogeneity of modern networks has pushed industry and research towards a single and consistent way of managing networks”. In general, network management is a service that employs a wide variety of software and hardware products to assist network system administrators in monitoring and maintaining networks. Due to heavy demands for quick and efficient telecommunication services, active telephone network management first began in the mid-1920s with the establishment of regional Traffic Control Bureaus in Chicago, Cleveland and New York. These bureaus served as clearinghouses for all information affecting traffic over their portion of the network. Staff implemented management plans for coping with unusual calling patterns, weather, damaged lines or other emergency situations. The structure of these early network management systems have influenced current computer network management (AT&T., 2005).

Most network management architectures use the same basic structure and set of relationships (Figure-1). Computer systems and other network devices run software that enable them to send alerts when they recognize problems. When receiving these alerts, management entities are programmed to react by executing one, several, or a group of actions, including operator notification, event logging, system shutdown, and automatic attempts at system repair (Cisco Systems, 2002).

Figure 1: A Typical Network Management Architecture Maintains Many Relationships. (Cisco Systems, 2002, p. 2)
However, many organizations did not take NM seriously until the development of computer networks in the early 1980s. In 1998, a group of telecommunication vendors combined to come to an agreement on simplified specifications that could speed up the implementation of Open System Interconnection (OSI) management standards and reduce the difficulty involved in the NM of computer networks (Raman, 1998).

**Network Security**

Network security is the protection of networks and their services from unauthorized modification, destruction, or admission (Information Assurance Division, 2004). Protection methods help to stop unauthorized users from accessing any part of the network system. It guarantees that a network performs its critical functions correctly.

According to Bose, (cited in 3COM Corporation, 2005, para. 5):

> Security must permeate the entire network, not just at key points -- which tends to leave much of the network and its various points of connection unguarded and untouched. Furthermore, key points of vulnerability and threats that have multiple means of propagation require an integrated response from more than one type of security technology, in essence requiring a multi-layered protection.

Clearly, multiple layers of protection across the whole network are essential if the integrity of the network is to be protected. Furthermore, according to Brahce, (cited in Kammerer, 2005, para 16) "Security is really a balance of security versus access". The challenge is to manage the correct level of security and access.

In current network security management, a common mistake is to assume that protection is just a matter of having the right security products and infrastructure. According to Stoller (2005, para. 3),

> The marketing literature that goes along with the firewalls, anti-virus software and VPNs (virtual private networks) certainly give the impression that once the product is installed, all will be well. But the real challenges lurking beneath the surface are people issues, not technology issues.

Even though the technology assists to reduce security risks, unless properly managed, the security software may not do the job as expected. Therefore the only safe solution is to ensure that employees maintain and manage network security properly. This can be done by ensuring the security devices are configured properly, ongoing monitoring of the network and patches are consistently installed and updated (Stoller, 2005).
State Model Diagrams

The State Model (SM) diagrams were designed to provide network students with a conceptual model to maximize their understanding of the network. There is evidence that it can also be used for managing security firewalls (Maj & Kohli, 2004). Work to date indicates that it is diagrammatic, allowing network administrators to have a complete picture of the network and to view the physical as well as logical network topologies. The model employs multiple views, and hence provides a hierarchical top down decomposition, thereby controlling technical detail. This new SM diagrams may integrate with NM tools, therefore network administrators may have a better understanding of networking devices and view of the network. Hence, SM may lead to efficient NM.

1.2 Purpose of the study

Network management software gives centralized control of the network components to the network administrator which helps to increase the physical control of the network. Managing a network through traditional NM tools is generally automatic and not defensive. The problems are rectified and the network manager only becomes aware of the problem after seeing the effect on a specific service. By this time half the damage is already done (Sarkar & Verma, 2001).

Biswas (cited in Sarkar & Verma, 2001, para. 5) says "The biggest drawback of several NM solutions available on the market is that while most tools support a good breadth of devices, they lack the depth to which they can manage or monitor a device". Since more applications are being implemented over networks, each with their own unique requirements from the network, the devices have to be modified to perform optimally in demanding and critical environments. In order to use the same tools all over the network, network administrators require tools that give them depth of management.

According to Maj, Murphy and Kohli (2004), many network administrators use the Command Line Interface (CLI) to manage their network devices. In order to determine device (router etc) states a number of different CLI commands must be used. The complexity of the CLI affects the learning phase for novices, resulting in a lack of ability to use it to manage most of the network devices (Maj & Kohli, 2004). With a good network and system analyser, network administrators may know exactly what traffic is on the network and precisely how the applications and systems are used. A good network and system analyser allows managers and operators to visualise and
respond to service availability trends in real time. This research will investigate whether the State Model diagrams can use for successful NM.

1.3 Hypothesis

State Model diagrams assist in network security management and lead to more comprehensive network management.

1.4 Research Questions

1. What are the relative strengths and weaknesses of current network management tools?

2. Does the State Model diagram assist in network security management to simplify the complexity of the networks and as a result leads to more efficient network management?

3. Can the State model be integrated into a vendor based system to simplify network management?
2.0 LITERATURE REVIEW

2.1 General literature

*Network Management*

In order to guarantee sufficient levels of performance and reliability, computer and communication systems require increasingly more complicated management strategies. IT departments are under increasing pressure when the network is at risk from outside threats such as viruses or software audits (Novell Releases ZENworks 7, 2005).

The rapid expansion of net-based business communications is driving larger amounts of different types of traffic over increasingly complex enterprise infrastructures. Unfortunately, NM budgets are not increasing at a rate that is comparative with this increase in traffic or the challenge of managing these more complex network environments. Also there are not enough skilled people available to solve current NM problems (Liebmann, 2000). Hence, the deployments of efficient NM tools are more critical than ever.

The monitoring tools can be simple or complicated. However, they are all likely to be simple to access and use. When there is a bad network link, there is no time to spend on complex analysis or complicated tools when the major concern is to get the systems back on line quickly (Cohen, 2002).

Tyminski (cited in Lais & Sarni, 2000) comments on NM:

> I figured out that to manage systems just for one of the data centres, you'd need to watch 18 separate consoles. An alarm could flash across the screen, and unless you happened to be watching that monitor at that moment, you'd miss it. (p. 8)

Hence, complexity and incompatibility are the foundation of most NM problems in modern corporate networks. The complexity is created when any hardware addition increases the points of potential network failure. Incompatibility occurs when IT hardware is not carefully inventoried and placed inappropriately and indelicately on the network. This scenario allows the administrator to see the status of all systems in real time and all on a single console (Lais & Sarni, 2000). However, building a flexible and dynamic NM platform upon which complicated management functions can guarantee uninterruptible, high-quality services is very difficult (Jingsha & Yi-Shang, 1995).
Kahani and Beadle point out that there are three basic approaches for NM systems; centralised, hierarchical and distributed. Most NM systems are centralised. Therefore, only a single management machine which is a single point of failure can collect the information and controls the entire network. If it fails, the entire network may collapse. If the management host does not fail, but a fault partitions the network, the other part of the network is left without any management functionality. In addition, a centralised system cannot easily be extended when the size or complexity of the network increase (Kahani & Beadle, 1997).

**Network Management Models**

Several NM models have been developed to date. Popular NM models are:

1. OSI Network Management
2. Telecommunications Management Networks
3. OMNiPoint theory
4. IT Infrastructure Library
5. Tasks—Frame of reference
6. DUnTe Management Model (Hemmen, 2000).

**OSI Network Management**

The International Organization for Standardization network management model, Open System Interconnection (OSI), is the primary means for understanding the major functions of NM systems. There are three basic components that comprise the elements of the management architecture to support a successful NM environment: a functional component, an information component and a communication component. The functional component describes the various activities to be performed in support of management. This component consists of five theoretical areas which facilitate rapid and consistent progress on each category in individual areas. These are configuration, fault, performance, security and accounting management. The information component explains how the management information is exchanged between the managing and managed systems. In order to enable successful transfer and interpretation of management information, the communication component addresses support infrastructure capabilities (Raman, 1998).
The traditional diagram that explains the manager and agent roles (Figure 2), presents a view that includes the three components mentioned above. The functional component is the alarm surveillance. The communication component is addressed by requests and responses, while the information component is represented by managed resources (Raman, 1998).

![Figure 2: OSI systems management overview.](Raman, 1998, p. 47).

However, Tanenbaum (cited in OSI Model, n.d.) argues that the OSI protocol is inappropriate because,

...the failure of the OSI suite to become popular was due to bad timing, bad technology, bad implementations, and bad politics. The timing was bad because the model was finished only after a significant amount of research time and money had been spent on the TCP/IP model. The technology is "bad" because the session and presentation layers are nearly empty, whereas the data link layer is overfilled. Early implementations were notoriously buggy and in the early days, OSI became synonymous with poor quality, whereas early implementations of TCP/IP were more reliable. Finally, the politics were bad because TCP/IP was closely associated with Unix, making it popular in academia, whereas OSI did not have this association. (para. 31)

**Telecommunications Management Networks (TMN).**

TMN is an important development in the telecommunication service providers' world. In large distributed telecommunications networks fault, configuration, accounting, performance, and security services are all significant elements of managing critical resources. The TMN concepts have been commonly implemented to manage networks ranging from high-speed fiber-optic networks to distributed cellular and satellite based wireless communication systems (Telecommunications Management Networks, n.d.).

In order to provide an organization with management services, TMN uses a five layer hierarchy of services. These layers include:
- Business Management
- Service Management
- Network Management
- Element Management

- Network Element (Telecommunications Management Networks, n.d.).

TMN describes the NM architecture in more detail than the OSI model. The NM architecture is expanded in the TMN model, where the OSI functional areas are used to define one of the four layers (Hemmen, 2000). However, the TMN model addresses the functions within a discipline, such as fault or configuration. Therefore, the TMN builds a stack of functions that can often be over-kill for a service provider. Furthermore, most Operational Support Systems (OSS’s) do not cleanly map to the TMN model, making the model even more of a burden on the development and deployment process. In addition further limitations of TMN are:

- Lacks the flexibility required for approaching iterative services.
- Not regarded the legacy which has provided the foundation for many Service Providers (Gillen, n.d.).

**OMNIPoint theory**

Open Management Interoperability Point (OMNIPoint) can be defined as “... a set of standards, implementation specifications, testing methods and tools, and object libraries that make possible the development of interoperable management systems and applications” (Hemmen, 2000, p. 303). It provides terms for the basic infrastructure to implement open management of networks. Further more OMNIPoint architecture is built by defining actions and their common relationships, which are essential for NM. However, OMNIPoint theory does not define the actual management applications themselves. Even though OMNIPoint defines the elements that must be implemented to achieve the effective exchange of management information, the detailed functions to be performed by particular management applications are not defined by OMNIPoint (Hemmen, 2000).
IT Infrastructure Library

According to Dubie (2002, para. 2), "The Information Technology Infrastructure Library (ITIL) is a set of rules for how to deliver information technology (IT) services more efficiently by improving management processes across IT departments that support networks, applications, databases and systems". ITIL describes IT infrastructure as the total technological components, the system and application software, the documentation and all the procedures that are essential to realise one or more IT services. Each of the processes and objects is described in a module and in each module a reference is made to other modules that are related to the process or object described by that module. The ITIL module ‘Network Services Management’ describes processes and their common relationships. Generally these processes and their common relationships are related to the infrastructure (IT). Hence, these processes can be used to define a design for NM (Hemmen, 2000).

However, limitations of ITIL are described as follows:

- Lack of management commitment; ITIL takes time and a lot of process change.
- Complexity; IT staff will get overwhelmed if break each ITIL process into large steps.
- Poor work instructions; ITIL gives guidance, but it doesn't tell how to actually do anything.
- Misdirected metrics; Need to measure quality, not just performance.
- Diminished momentum; Need to develop achievable goals that keep this in mind (Worthen, 2005).

Tasks—Frame of reference (T-FORce)

According to Hemmen (2000), T-FORce is defined as offering methods, models and techniques for managing information systems. This requires managing, controlling and maintaining implemented information systems. The following concepts are considered in the T-FORce model:

- Tasks, task areas, task fields.
- Levels of management.
Tasks can recognise processes and these tasks can be grouped to form a process. From a NM perspective the weakness of T-Force is that its primary focus is upon information systems rather than networks. Networks are defined as a part of an information system; therefore T-FORce model is only fairly applicable to NM. Hence, not all tasks that are considered in T-FORce model apply to NM (Hemmen, 2000).

**DÚneT Management Model**

The purpose of the DÚneT Management Model is to order the different network services and to describe service interfaces. This model describes the functions that are essential for data communications. The DÚneT Management Model is a layered model. In order to assist the understanding of a service that is essential to carry out the service in the layer above, each lower layer offers a service. Furthermore, in all layers a service provider can offer its own network services (Hemmen, 2000).

However, according to Terplan (1988), DÚneT model does not describe NM architecture, NM functions, NM instrumentation, Organisational components or Organisational approach.

In conclusion, Hemmen (2000) states that for the above described models:

None of the models are adequate to model evolving heterogeneous networks, due to the following definitions:

- None of the models presently available deal with the evolution of networks, but they cover heterogeneity. All vendors and users are aware of the necessity for open systems in which hardware and software can be connected and can interact. Evolution of the network and network services has received less attention. It is initiated by such driving forces as economics, Organizational and technical forces.

- The models described use a top-down approach only instead of a mixture of a top-down and a bottom-up approach. With the top-down approach is meant that architecture for NM is recognized, without considering the actual realization in detail of that architecture in practice. NM is described at an abstract level, where details are not recognized.

- The models are impracticable for managers at a strategic and tactical level. Those described were selected for their focus on the Organization of NM. Many other models exist which focus only on technical aspects of NM. The technical focus of those models implies the influence of the
operational level due to the professional knowledge that is required to perform NM. Due to a lack and deficiencies of present instruments in providing information for senior management, management is not able to control NM effectively. (p. 313)

The available models focus mainly on the technical aspects of NM that are part of the operational NM. Due to the huge investments and the strategic importance of the network and its services, decisions concerning the network and its services must be made by senior management. However, none of the above models, methods or techniques are available to assist managers with these decisions. Thereby it is necessary to invent models and provide methods to further develop effective NM (Hemmen, 2000).

Protocols for Network Management

The protocols used by the NM tools play a significant role in the management arena. The first detailed NM tool was the Simple Gateway Monitoring Protocol (SGMP), introduced in 1987. While SGMP can monitor gateways, still was not a general purpose tool. Simple Network Management Protocol (SNMP) came along a year later, but only for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. In 1993, SNMP was extended to use AppleTalk and Novell Inc.'s Internetwork Packet Exchange (IPX) protocols. However, SNMP is extremely difficult to implement and not very efficient. Even though SNMP is widely available and interoperable amongst a variety of network components, it wastes considerable bandwidth relaying unnecessary information (Kay, 2002).

In addition, the following are further limitations of SNMP.

- May not be suitable for management of truly large networks because of polling performance limitations.
- Not well suited for retrieving large amounts of data (entire routing table).
- Traps are unacknowledged (could be lost based on UDP/IP).
- Only trivial authentication in base protocol--better for monitoring than control.
- Only way to trigger an event is to set a variable (rather than having a remote procedure call like interface)
- Does not support manager-to-manager communications (Worcester Polytechnic Institute, 2004, para. 40).
While the OSI NM model addresses some of the above issues, but it is widely believed that size of the specification is too complicated and its full functionality has taken long time to implement (Worcester Polytechnic Institute, 2004).

Remote Network Monitoring (RMON) is another protocol that was used for NM. RMON is designed to collect information about the network itself. A single management station can monitor multiple segments through distributed monitoring. Then in the mid-1990s, the more powerful and secure Common Management Information Protocol (CMIP) was developed to replace SNMP (Kay, 2002). However, "The fact that CMIP uses 10 times the network overhead has meant that SNMP is still the major player in the industry" (Kay, 2002, p. 48).

Network Security Management

The best way to balance network security threats is to predict things before they occur and to expect the unexpected (Kammerer, 2005). Hence, according to Lynas (cited in Lawson, 2005, p. 45) "Spend absolutely every penny you need to on security but not a penny more". In order to manage the various firewalls, Intrusion Detection System (IDS) and other security devices, it is better to have security specialists because security occurs at a very specific location on the network and has a very specific function. Furthermore, the boundary of security is absorbent, and therefore, security needs to be applied at the application level, at the network level and at the storage level (Cummings, 2005).

According to Levine (2005), most companies are increasingly adopting wireless communications for their employees. Wireless options often may permit an avoidance of security policies, intentionally or unintentionally since most employees remain uneducated or undereducated about the possibilities of security violations. Therefore, according to Markovich (cited in Levine, 2005, p. 54) "Malware and hackers target WLANs (wireless local area networks) because they are the new low-hanging fruit of the IT world. It's relatively easy to exploit an open AP or divert a laptop to a hacker's wireless device".

While there are many types of wireless threats, some are exacerbated by improper employee use. Sometimes internal violations occur because employees knowingly compromise the network, they are careless or they simply do not understand how to keep transmissions secure. Increase employee awareness training and emphasize written
security policies are basic solutions to prevent security breaches in wireless networks (Levine, 2005).

In the professional IT environment not all threats are technical in nature. Physical security is as important as technological security. There are two general classifications of physical threats, malicious and non-malicious. Malicious threats include attempts to break into the network and non-malicious threats arise when a good person makes a mistake. However, both threats can be tackled with effective physical security (Gilmer, 2005).

There are several threats that may cause problems when connecting to the Internet. Some of these are port probes, viruses and worms, Denial of Service (DoS) attacks, Ping of Death (PoD) attacks, and Universal Datagram Protocol (UDP) flood attacks. Proper management knowledge is a key factor in fighting off these attacks, while well managed firewalls and routers can protect core networks (Gilmer, 2005).

Commercial systems which commonly use remote access are open to major security risks. Remote access puts responsive data on the outside of the company firewall usually on various movable devices that are difficult to control. In order to ensure a high security environment, companies need to have resources and processes, consistently and thoroughly in place, as well as much better security management methods (Stoller, 2005).

**State Model Diagrams**

According to Maj and Kohli (2004, p. 136-214) “Models are a means of controlling detail and complexity. Desirable model characteristics include; diagrammatic, self documenting, easy to use and hierarchical top down decomposition to control detail”. A good model, levels the processes by which complex systems can be progressively decomposed, whilst still maintaining essential links. Maj and Kohli (2004) proposed that internetworking devices (switches, routers etc) could be diagrammatically represented using a collection of tables called state model diagrams. These diagrams have been successfully used for teaching internetworking technology curriculum.

As a pedagogical tool the state diagrams explicitly incorporate the TCP/IP and OSI stacks (Figure 3), however for experienced administrators they may be removed.
The modular nature of the diagrams provides a top down decomposition by means of levelling. According to Maj, Kohli and Fetherston (2005):

One of the most important features of these diagrams is the ability to construct a variety of different levels according to the level of abstraction required. This means that the initial (level 0) diagram can be consulted to obtain a high level overview of device interconnectivity i.e. what switches and routers are connected together. When details of a specific device are needed, then greater technical complexity for that specific device can be obtained. Obviously, the different levels of diagram are consistent. The diagrams may be decomposed to the level that is meaningful for the purpose that the diagram is required.

This may be illustrated by a router OSI layer 1 line status (carrier detect table). For the purposes of NM, it is not appropriate to decompose this further - the interface is either up or down. Furthermore, a simple routing protocol e.g. RIP may be represented by a level 3 routing table (Figure 3). Significantly, this same basic state model used for a router running RIP may be also be used for other more complex routing protocol such as Enhanced Interior Routing Protocol (EIGRP).
According to Maj, Kohli and Fetherston (2005):

It is possible, using the switch state model, to implement protocols that include: basic switch operation (address learning, forwarding/filtering), Spanning Tree, Virtual LAN’s (VLANs), trunking, VLAN Trunking Protocol (VTP) and Etherchannelling.

Figure 4: Switch State Model. (Maj, Kohli and Fetherston, 2005, p. 2)

Significantly, hyperlinks may be used to navigate between not only different devices but also different tables in the same device.

According to Maj, Ratnayake & Tran (2005) state model diagrams of a wireless Access Point and a PIX firewall were developed. The wireless Access Point (AP) state model (Figure 5) consists of an association table, radio interface table and cable interface (Ethernet) table. The association table provides IP to MAC address associations. The radio interface table allows identification of the radio interface (e.g. 802.11a, 5GHz), the SSID and authentication parameters.

Stateful packet filters combine the best of packet filtering and proxy filtering technologies. Stateful packet filters maintain complete session state information for each session. Each time an IP connection is established (inbound or outbound), the
information is logged in a stateful session flow table. For this research study, a Private Internet exchange (PIX) stateful packet filter (firewall) was used. PIX firewalls employed dedicated hardware (ensuring high performance) and use the Adaptive Security Algorithm (ASA) for stateful connection control. The ASA uses the concept of security levels – security level 100 being the highest and is assigned to an inside interface. Security level 0 is the lowest and is assigned to an outside interface. PIX devices may have more than two interfaces, in which case these may be assigned different levels of security.

![Diagram of PIX state model with AP1200-1 MAC IP Device Narre Parent State table and interface details: dot11radio1 SSID Group2 Authentication Open Channel Frequency 40 (5200MHz) Interface Ethernet 0 IP MAC]

**Figure 5:** Wireless Access Point State Model.

(Maj, S. P., Ratnayake, S. A., & Tran, B., 2005, p. 3)

High (inside) to low (outside) security may be enabled by two different methods – static or dynamic translation. Dynamic translation employs a global address pool and Network Address Translation (NAT). The PIX firewall state model diagram (Figure 6) shows a static translation. However, it is possible to also model dynamic translation. This PIX state model diagram incorporates the Address Resolution Protocol (ARP), route and interface tables. It also includes the Xlate table that provides the local to global IP address translation and the “conn” table identifies the two end devices being connected.
Figure 6: PIX Firewall State Model.
(Maj, S. P., Ratnayake, S. A., & Tran, B., 2005, p. 4)
3.0 THEORETICAL FRAMEWORK

3.1 Identification of Variables Impacting on the Hypothesis

In order to avoid errors, repetitive measurements have been taken and the results were based on practical experiments. The experiments data that collected relied upon the responses of the software and hardware in the network and research data that collected relied upon the responses from research participants.

3.2 Targeted Population

- Network managers and administrators searching for ways to minimize costs and complexity when managing the network.
4.0 MATERIALS AND METHODS OF INVESTIGATION

4.1 Description of Materials to be employed

The following equipment was used for the research investigation:

- Ciscoworks 2000 NM application
- Computers: Intel Pentium IV machines with 512 MB of RAM
- Operating systems: Windows XP, Windows 2003 advanced server and Red hat Linux 9.0 operating systems
- Routers: Cisco 2600 series routers, running IOS version 12.2
- Switches (Layer 2): Catalyst 2950 wire-speed 24 ports Fast Ethernet switches, running IOS version 21.1
- Switches (Layer 3): Catalyst 3550 multi-layer switches with 24-port 10/100 switch and GBIC-based Gigabit Ethernet ports will be use to experiment with multicasting, running IOS version 21.1
- Pix firewall: Pix 515e with 3 interfaces supporting VPN and 3DES encryption.
- Wireless Client Adapter: Aironet 802.11a/b/g wireless PCI adapter.
- Intel Pro 10/100 Mbps network interface cards.

The School of Computer and Information Science at Edith Cowan University had all the equipment to perform the investigation. The network equipment in the labs was up-to-date and standardised for both education and commercial environments. Therefore this investigation provided valuable information about the network environment.

4.2 Design and Procedure of the Study

This investigation involved examining the results provided by the NM application. A direct measurement method was used for this investigation because it was application specific (Ori, 2002).
Stallings (1993) stated that NM can be measured in 2 steps:

Step 1: Network monitoring – a read function, concerned with observing and analyzing status and behaviors of the configurations and its components.

Step 2: Network control – a write function, concerned with altering parameters of various components in the network.

In order to achieve accurate measurements, multiple network configurations implemented for the evaluation. The experiments were conducted only in a Local Area Network (LAN) environment. The initial investigation involved examining simple network configurations which was used afterwards as a baseline. Afterwards, the baseline used to assess more complex network configurations. The experimental configurations are as follows:

**LAN Configurations**

(Refer to Appendix C for the configuration commands)

*Figure 7: Experiment 1, baseline experiment with single Internetworking device (firewall).*

*Figure 8: Experiment 2 with multiple Internetworking devices (router, firewall)*
**Figure 9:** Experiment 3 with multiple Internetworking devices (router, firewall and switch)

**Figure 10:** Experiment 4 with multiple Internetworking devices (router, firewall, switch, access point)

**Figure 11:** Experiment 5 with multiple Internetworking devices in the LAN.
In order to achieve maximum accuracy and reliability, the evaluation compared and contrasted based on the three parameters as in Figure 12.

1. State Model: Managing the network using the SM.
2. Automate: Use CiscoWorks to evaluate NM.

Figure 12: Network management evaluation procedures

Figure 13: Evaluating the effectiveness of NM using the SM and CiscoWorks
State Model for Experiment 1.
State model 2.1 for experiment 2
### Router

<table>
<thead>
<tr>
<th>C</th>
<th>IP</th>
<th>A/M</th>
<th>IP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>192.168.3.0</td>
<td></td>
<td></td>
<td>Fa0/1</td>
</tr>
<tr>
<td>C</td>
<td>192.168.4.0</td>
<td></td>
<td></td>
<td>Fa0/0</td>
</tr>
</tbody>
</table>

### IP address, MAC address, Interface

<table>
<thead>
<tr>
<th>IP address</th>
<th>MAC address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.3.99</td>
<td>0012.d96f.db58</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>192.168.3.98</td>
<td>0012.d96f.db58</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>192.168.3.2</td>
<td>0012.d96f.db58</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>192.168.3.1</td>
<td>0012.01ae.7461</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>192.168.4.1</td>
<td>0002.5573.0867</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>192.168.4.2</td>
<td>0012.01ae.7460</td>
<td>Fa0/0</td>
</tr>
</tbody>
</table>

### Port, IP address

<table>
<thead>
<tr>
<th>Port</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>192.168.3.1</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>192.168.4.2</td>
</tr>
</tbody>
</table>

### Port, MAC address

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>0012.01ae.7461</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>0012.01ae.7460</td>
</tr>
</tbody>
</table>

### PIX Firewall

- **IP address**: 192.168.3.0
- **IP address**: 192.168.4.0

### Device: PC2

<table>
<thead>
<tr>
<th>Device</th>
<th>IP</th>
<th>Gateway</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC2</td>
<td>192.168.4.1/24</td>
<td>192.168.4.2</td>
<td>0002.5573.1167</td>
</tr>
</tbody>
</table>

**State Model 2.2 for Experiment 2.**
### ARP

<table>
<thead>
<tr>
<th>Interface</th>
<th>Inside</th>
<th>Dmz</th>
<th>Outside</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>192.168.2.1</td>
<td>192.168.1.1</td>
<td>192.168.3.1</td>
</tr>
<tr>
<td>MAC</td>
<td>000e.30e2.c760</td>
<td>0002.557a.8125</td>
<td>0002.5573.0b48</td>
</tr>
</tbody>
</table>

### NAT

<table>
<thead>
<tr>
<th>nameif</th>
<th>Inside</th>
<th>Dmz</th>
<th>SNM</th>
<th>Max conn</th>
<th>Emb-limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat-id</td>
<td>1</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>real-ip</td>
<td>192.168.4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNM</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Xlate

<table>
<thead>
<tr>
<th>global</th>
<th>local</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.3.99</td>
<td>192.168.4.1</td>
</tr>
<tr>
<td>192.168.3.98</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>192.168.1.99</td>
<td>192.168.4.1</td>
</tr>
</tbody>
</table>

### Route

<table>
<thead>
<tr>
<th>Interface</th>
<th>inside</th>
<th>Dmz</th>
<th>outside</th>
<th>inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ip</td>
<td>192.168.2.0</td>
<td>192.168.1.0</td>
<td>192.168.3.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Snm</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Ip</td>
<td>192.168.2.2</td>
<td>192.168.1.2</td>
<td>192.168.3.2</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>Metric</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Connect</td>
<td>Connect</td>
<td>Connect</td>
<td>Connect</td>
<td>Other</td>
</tr>
<tr>
<td>type</td>
<td>static</td>
<td>static</td>
<td>static</td>
<td>static</td>
</tr>
</tbody>
</table>

### Static

| Inside   | 192.168.4.1 |
| Outside  | 192.168.3.99 |
| Inside   | 192.168.4.1 |
| dmz      | 192.168.1.99 |
| dmz      | 192.168.1.1 |
| Outside  | 192.168.3.98 |

### CiscoWorks Server

<table>
<thead>
<tr>
<th>Interface</th>
<th>Cable NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>192.168.4.1</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.4.2</td>
</tr>
<tr>
<td>MAC</td>
<td>0002.5573.0840</td>
</tr>
</tbody>
</table>

### ACL

<table>
<thead>
<tr>
<th>Interface</th>
<th>e0</th>
<th>e1</th>
<th>e2</th>
<th>e3</th>
</tr>
</thead>
<tbody>
<tr>
<td>nameif</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>outside</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Security</td>
<td>0</td>
<td>100</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>IP</td>
<td>192.168.3.2</td>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
</tr>
<tr>
<td>A-group</td>
<td>ACLIN</td>
<td>ACLIN2</td>
<td>ACLIN</td>
<td>ACLIN2</td>
</tr>
<tr>
<td>In/out</td>
<td>in</td>
<td>in</td>
<td>in</td>
<td>in</td>
</tr>
<tr>
<td>MAC</td>
<td>0012.d96f.db4d</td>
<td>0012.d96f.db4d</td>
<td>0012.d96f.db4d</td>
<td>0012.d96f.db4d</td>
</tr>
</tbody>
</table>

### Interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>e0</th>
<th>e1</th>
<th>e2</th>
</tr>
</thead>
<tbody>
<tr>
<td>nameif</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>outside</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Security</td>
<td>0</td>
<td>100</td>
<td>50</td>
</tr>
<tr>
<td>IP</td>
<td>192.168.3.2</td>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
</tr>
<tr>
<td>A-group</td>
<td>ACLIN</td>
<td>ACLIN2</td>
<td>ACLIN</td>
</tr>
<tr>
<td>In/out</td>
<td>in</td>
<td>in</td>
<td>in</td>
</tr>
<tr>
<td>MAC</td>
<td>0012.d96f.db4d</td>
<td>0012.d96f.db4d</td>
<td>0012.d96f.db4d</td>
</tr>
</tbody>
</table>

### State Model 3.1 for Experiment 3

26
### MAC Address Table

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC address</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0002.5573.0340</td>
<td>DYNAMIC</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>1</td>
<td>000c.30e2.c761</td>
<td>DYNAMIC</td>
<td>Fa0/2</td>
</tr>
</tbody>
</table>

### Interface LP

- **Fa0/1**: Up
- **Fa0/2**: Up

### Interface LS

- **Fa0/1**: Up
- **Fa0/2**: Up

### Device

- **CiscoWorks Server**
- **IP**: 192.168.4.1
- **MAC**: 0002.5573.0840

---

### State model 3.2 for Experiment 3

**PIX Firewall**

---

### Router

<table>
<thead>
<tr>
<th>C</th>
<th>IP</th>
<th>A/M</th>
<th>IP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>192.168.4.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S</td>
<td>192.168.1.0</td>
<td>1/0</td>
<td>192.168.2.2</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>C</td>
<td>192.168.2.0</td>
<td></td>
<td></td>
<td>Fa0/0</td>
</tr>
<tr>
<td>S</td>
<td>192.168.3.0</td>
<td>1/0</td>
<td>192.168.2.2</td>
<td></td>
</tr>
</tbody>
</table>

### IP address

<table>
<thead>
<tr>
<th>IP address</th>
<th>MAC address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.2</td>
<td>0012.d96f.db4d</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>192.168.2.1</td>
<td>000c.30e2.c760</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>192.168.4.1</td>
<td>0002.5573.0840</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>192.168.4.2</td>
<td>000c.30e2.c761</td>
<td>Fa0/1</td>
</tr>
</tbody>
</table>

### Port IP address

- **Fa0/1**: 192.168.4.2
- **Fa0/0**: 192.168.2.1
### Layer 3: Network

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP address</th>
<th>SNM</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC</td>
<td>192.168.4.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

### Layer 2: Datalink

<table>
<thead>
<tr>
<th>Interface</th>
<th>Wireless NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>ML13.134-AP4</td>
</tr>
<tr>
<td>Network</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>AP auth</td>
<td>Open</td>
</tr>
<tr>
<td>MAC</td>
<td>0040.96a6.7d64</td>
</tr>
</tbody>
</table>

### Layer 1: Physical

<table>
<thead>
<tr>
<th>NIC</th>
<th>802.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power level</td>
<td>20mW</td>
</tr>
<tr>
<td>Channel</td>
<td>40 (5200MHz)</td>
</tr>
<tr>
<td>Data rate</td>
<td>Auto</td>
</tr>
<tr>
<td>Power save mode</td>
<td>Constantly Awake Mode (CAM)</td>
</tr>
</tbody>
</table>

### AP1200-1

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>Device</th>
<th>Name</th>
<th>Parent</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>000b.5f55.3972</td>
<td>192.168.4.10</td>
<td>AP</td>
<td>AP4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Interface

<table>
<thead>
<tr>
<th>SSID</th>
<th>dot11radio1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Open</td>
</tr>
<tr>
<td>Channel Frequency</td>
<td>40 (5200MHz)</td>
</tr>
<tr>
<td>MAC address</td>
<td>000b.46ca.61c5</td>
</tr>
<tr>
<td>Bridge-group</td>
<td>1</td>
</tr>
</tbody>
</table>

### MAC & IP

- **PC2**
  - IP: 192.168.3.1
  - MAC: 0002.5573.1167

- **PC1**
  - IP: 192.168.1.1
  - MAC: 0002.5573.b7f2

### Network Infrastructure

- AP authentication: Open
- MAC: 0040.96a6.7d64

### Diagram

- **AP1200-1** connected to **Switch** via **Fa0/1**
- **Switch** connected to **Router** via **Fa0/1**
- **Switch** connected to **PC1** via **Fa0/2**
- **Router** connected to **PIX Firewall** via **Fa0/0**

**State Model 4.1 for Experiment 4**
State Model 4.2 for Experiment 4
MAC Address Table

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC address</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0040.96a6.7d64</td>
<td>DYNAMIC</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>1</td>
<td>000c.309e.6481</td>
<td>DYNAMIC</td>
<td>Fa0/2</td>
</tr>
</tbody>
</table>

Switch

<table>
<thead>
<tr>
<th>Interface</th>
<th>LP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>Up</td>
</tr>
<tr>
<td>Fa0/2</td>
<td>Up</td>
</tr>
</tbody>
</table>

Port

<table>
<thead>
<tr>
<th>Port</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>192.168.4.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>000c.309e.6481</td>
</tr>
</tbody>
</table>

Router

<table>
<thead>
<tr>
<th>C</th>
<th>IP</th>
<th>A/M</th>
<th>IP</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>192.168.4.0</td>
<td></td>
<td></td>
<td>Fa0/1</td>
</tr>
<tr>
<td>S</td>
<td>192.168.1.0</td>
<td>1/0</td>
<td>192.168.2.2</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>C</td>
<td>192.168.2.0</td>
<td></td>
<td></td>
<td>Fa0/0</td>
</tr>
<tr>
<td>S</td>
<td>192.168.3.0</td>
<td>1/0</td>
<td>192.168.2.2</td>
<td>Fa0/0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP address</th>
<th>MAC address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.2</td>
<td>0012.d96f.db47</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>192.168.2.1</td>
<td>000c.309e.6480</td>
<td>Fa0/0</td>
</tr>
<tr>
<td>192.168.4.1</td>
<td>0040.96a5.7d64</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>192.168.4.2</td>
<td>000c.309e.6481</td>
<td>Fa0/1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>192.168.4.2</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>192.168.2.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td>000c.309e.6481</td>
</tr>
<tr>
<td>Fa0/0</td>
<td>000c.309e.6480</td>
</tr>
</tbody>
</table>

State Model 4.3 for Experiment 4
Layer 3: Network
- **Interface**: NIC
- **IP address**: 192.168.1.1
- **SNM**: 255.255.255.0

Layer 2: Datalink
- **Interface**: Wireless NIC
- **SSID**: ML13.134-AP5
- **Network**: Infrastructure
- **AP authentication**: Open
- **MAC**: 0002.5573.b7f2

Layer 1: Physical
- **NIC**: 802.11a
- **Power level**: 20mW
- **Channel Frequency**: 40 (5200MHz)
- **Data rate**: Auto
- **Power save mode**: Constantly Awake Mode (CAM)

Access Point 1
- **MAC**: 0013.1a32.97eb
- **IP**: 192.168.1.10
- **Device**: AP
- **Name**: AP5

<table>
<thead>
<tr>
<th>Interface</th>
<th>Device</th>
<th>Name</th>
<th>Parent</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot11radio1</td>
<td>IP</td>
<td>IP</td>
<td>IP</td>
<td>CAM</td>
</tr>
<tr>
<td>ML13.134-AP5</td>
<td>MAC</td>
<td>MAC</td>
<td>B-G</td>
<td></td>
</tr>
<tr>
<td>0011.20ee.d2bd</td>
<td>Bridge-group</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

State Model 5.1 for Experiment 5
State Model 5.2 for Experiment 5
PC 4

Layer 3: Network

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP address</th>
<th>SNM</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC</td>
<td>192.168.5.2</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

Layer 2: Datalink

<table>
<thead>
<tr>
<th>Interface</th>
<th>Wireless NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>ML13.134-AP4</td>
</tr>
<tr>
<td>Network</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>AP authentication</td>
<td>Open</td>
</tr>
<tr>
<td>MAC</td>
<td>0002.5573.b23a</td>
</tr>
</tbody>
</table>

Layer 1: Physical

<table>
<thead>
<tr>
<th>NIC</th>
<th>802.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power level</td>
<td>20mW</td>
</tr>
<tr>
<td>Channel Frequency</td>
<td>40 (5200MHz)</td>
</tr>
<tr>
<td>Data rate</td>
<td>Auto</td>
</tr>
<tr>
<td>Power save mode</td>
<td>Constantly Awake Mode (CAM)</td>
</tr>
</tbody>
</table>

Access Point 2

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>Device</th>
<th>Name</th>
<th>Parent</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>000b.5f55.3972</td>
<td>192.168.5.10</td>
<td>AP</td>
<td>AP4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>dot11radio1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>ML13.134-AP4</td>
</tr>
<tr>
<td>Authentication</td>
<td>Open</td>
</tr>
<tr>
<td>Channel Frequency</td>
<td>40 (5200MHz)</td>
</tr>
<tr>
<td>MAC address</td>
<td>000b.46ca.61c5</td>
</tr>
<tr>
<td>Bridge-group</td>
<td>1</td>
</tr>
</tbody>
</table>

Interface Ethernet 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Ethernet 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td></td>
</tr>
<tr>
<td>B-G</td>
<td></td>
</tr>
</tbody>
</table>

CiscoWorks Server

<table>
<thead>
<tr>
<th>Interface</th>
<th>Cable NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>192.168.5.1</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.5.3</td>
</tr>
<tr>
<td>MAC</td>
<td>0002.5573.2024</td>
</tr>
</tbody>
</table>

Switch 2

Fa0/3

State Model 5.4 for Experiment 5
State Model 5.5 for Experiment 5
### PIX Firewall 2

<table>
<thead>
<tr>
<th>ARP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td><strong>Inside</strong></td>
</tr>
<tr>
<td>IP</td>
<td>192.168.5.1</td>
</tr>
<tr>
<td>MAC</td>
<td>0002.5573.2024</td>
</tr>
</tbody>
</table>

### Route

<table>
<thead>
<tr>
<th>Interface</th>
<th>inside</th>
<th>outside</th>
<th>outside</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ip</td>
<td>192.168.5.0</td>
<td>192.168.4.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Smm</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Ip</td>
<td>192.168.5.3</td>
<td>192.168.4.1</td>
<td>192.168.4.2</td>
</tr>
<tr>
<td>Metric</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>type</td>
<td>static</td>
<td>static</td>
<td>static</td>
</tr>
<tr>
<td></td>
<td>Connect</td>
<td>Connect</td>
<td>Other</td>
</tr>
</tbody>
</table>

### Static

- Inside: 192.168.5.1
- Outside: 192.168.4.99
- Inside: 192.168.5.2
- Outside: 192.168.4.98

### ACL

<table>
<thead>
<tr>
<th>Name</th>
<th>ACLIN</th>
<th>ACLIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit/Deny</td>
<td>Permit</td>
<td>Permit</td>
</tr>
<tr>
<td>Protocol</td>
<td>Tcp</td>
<td>ICMP</td>
</tr>
<tr>
<td>Source</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Destination</td>
<td>192.168.4.98</td>
<td>192.168.4.99</td>
</tr>
<tr>
<td>Parameters</td>
<td>Eq www</td>
<td>Echo-reply</td>
</tr>
</tbody>
</table>

### CiscoWorks Server

- Interface | Cable NIC
- IP        | 192.168.5.1
- Gateway   | 192.168.5.3
- MAC       | 0002.5573.2024

### State Model 5.6 for Experiment 5
4.3 Data Collection

After above experiments were implemented, a questionnaire (refer to Appendix A) was given to selected network experts and network students to evaluate State Model diagrams with Ciscoworks and CLI. Also was data collected by face to face interview with network experts to provide more in depth data (refer to Appendix B). Feedbacks on the effectiveness of managing the network evaluated.

4.4 Ethical Considerations

Participants were informed in writing that all original records would be stored in a locked room at Edith Cowan University and that the anonymity of the participants was guaranteed. A permission form signed by every participant prior to participate in the study. The interviewees were notified that their voices will be recorded only for study purposes. Participants were quite at ease during the study and enjoyed being part of the study.
5.0 RESEARCH FINDINGS

5.1 An Evaluation of State Model Diagrams

Based on the experimental networks, twenty participants experienced in networking were asked to evaluate the following NM tools:

- State model diagrams (paper based only)
- Ciscoworks for Windows
- Command Line Interface

The participants were given a short introduction to the state model diagrams and provided with the opportunity to manage the network using these tools. They were then asked to complete a questionnaire and participate in interviews to obtain details about their work experience. The questionnaire and interview also included a number of questions most of which were based on the Likert scale (SA, A, D, SD, U) and the opportunity to provide any comments.

Question 1

Does the state model provide an easy way to understand the relationship between the devices of a network?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
<th>Do not know</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Question 2

The state model allows network administrators to have a better view of the entire network than other methods/models.

<table>
<thead>
<tr>
<th>SA</th>
<th>A</th>
<th>D</th>
<th>SD</th>
<th>U</th>
</tr>
</thead>
<tbody>
<tr>
<td>30%</td>
<td>65%</td>
<td></td>
<td></td>
<td>5%</td>
</tr>
</tbody>
</table>

Question 3

The state model cannot be used to manage complex networks.

<table>
<thead>
<tr>
<th>SA</th>
<th>A</th>
<th>D</th>
<th>SD</th>
<th>U</th>
</tr>
</thead>
<tbody>
<tr>
<td>30%</td>
<td>60%</td>
<td>5%</td>
<td></td>
<td>5%</td>
</tr>
</tbody>
</table>
Question 4

The integration of the state model with Ciscoworks simplifies the complexity of the network.

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>D</th>
<th>SD</th>
<th>U</th>
</tr>
</thead>
<tbody>
<tr>
<td>40%</td>
<td>40%</td>
<td></td>
<td></td>
<td>20%</td>
</tr>
</tbody>
</table>

Question 5

The state model does NOT assist efficient NM.

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>D</th>
<th>SD</th>
<th>U</th>
</tr>
</thead>
<tbody>
<tr>
<td>70%</td>
<td>30%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Question 6

The state model assists in network security management as a tool and as a result leads to more successful NM.

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>D</th>
<th>SD</th>
<th>U</th>
</tr>
</thead>
<tbody>
<tr>
<td>20%</td>
<td>70%</td>
<td>5%</td>
<td></td>
<td>5%</td>
</tr>
</tbody>
</table>

Question 7

I would NOT use the state model to manage my network.

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>D</th>
<th>SD</th>
<th>U</th>
</tr>
</thead>
<tbody>
<tr>
<td>5%</td>
<td>50%</td>
<td>40%</td>
<td></td>
<td>5%</td>
</tr>
</tbody>
</table>

All the responses to the request for any comments were recorded and are as follows:

Participant 1

“Yes, state diagrams provide a clear, concise view of a network configuration which helps identify any security issues”.

Participant 2

“Because the state model show you all the information in one go it would allow a better understanding of the network which in turn provides better security”.

39
Participant 3

“I have not previously seen a state model in my studies. I think it could have been useful if I had been exposed to it earlier. In the last unit I am studying called network troubleshooting, I think it provides an additional mechanism not only to troubleshoot but to be able to manage the security risks. I think the appropriate niche for this type of model will be in software where this information could be juxta positioned with statistics or breach attempts and intrusions whereby alters could be provided in these instances”.

Participant 4

“State model gives a clear picture of each item/component and its configuration values. This model could be developed or further developed which can lead to a view/idea about each component. Saves time when it comes to working out network issues. Rather than using the command line method to view configuration values. Disadvantages are manual/paper based system can be damaged or lost”.

Participant 5

“State model provides a layman’s view where it is simple and easy to understand the network”.

Participant 6

“Yes, this will help to identify any bugs in the design”.

Participant 7

“State model provides clear understanding and creates a clear picture about the network. It will help to identify any bugs or faulty points in the network. I strongly believe this approach will lead to a world class product”.

Participant 8

“Easy to understand the structure of the network and information flow through the separate interfaces which strongly helps to understand security needs”.

Participant 9

“State model gives a clear overview of the entire network including IP addresses, MAC addresses and all other relevant information. It helps a lot to understand the security needs of the system, and exact interfaces to put all ACLs”.
Participant 10

“State model manages the network well but it does not address the security issues”.

Participant 11

“State model is useful to efficiently manage the complexity of networks”.

Participant 12

“State model is very good method of understanding the entire network but if the network becomes complex it will be very cumbersome or difficult to understand the state model and hence the network”.

Participant 13

“State Model diagrams provide clear picture of the entire network. That will help to identify any faulty points in the network. I strongly believe this method provides an efficient network security management”.

Participant 14

“This State Model is good for getting a good view of the network. However, further develop need”.

Participant 15

“State Model might help to identify security if logs showing success of authorised traffic and unauthorised attempts are identified regardless of success or other status. However, looks feasible, would need to be confirmed with logged attempts to degrade or bypass security”.

Participant 16

“State Model clearly shows what sort of security permissions have given to the network”.

Participant 17

“State Model might help to identify security risk by inserting extra fields to cover things like authentication methods, access list settings etc”.

Participant 18

“Yes, State Model shows all information as a map rather than documentation. It is focus on the key points of the network”.
Participant 19

"For a secure network we need understand how it works. SM is a map we can look at to understand rather than read. SM is extremely helpful for beginners because it identifies all the necessary information that beginner wants to learn. Further development need to manage complex network”.

Participant 20

“SM brings out the major points and less complex. Showing Access Control List (ACL) information is very helpful. SM has a potential value and very useful edition to other network management tools. So it is important but would not relay only to the State Model, combination with Ciscoworks give better network management. It is a additional tool rather than a tool”.

This is only a limited study based on a simple LAN with only twenty participants. However, the results are consistent. Of the twenty participants only one had reservations about the using the state model as a NM tool.

5.2 Further Research

In this study, the state model diagrams were paper based. A hyperlink implementation is currently being developed. This will allow users to more easily navigate between different devices and include or exclude detail as needed. A more extensive study involving a more complex network and more interviewees is currently being planned.

5.3 Limitation of the Study

This study was not based upon the NM tools or vendor specific NM tools. However, the author aware of the number of NM tools on the market and interoperability issues. The primary objectives of the research were to investigate the efficiency of NM tools and the integration of the State Model diagrams with Ciscoworks and its effectiveness for security and effective NM.
6.0 CONCLUSION

There are numerous NM tools available on the market, but complexities increased when they are used to manage or monitor a device. Even though various NM models and methods were introduced to reduce complexity, many studies indicate that this is in fact, not the case. Network security is a critical issue of modern NM. Even though the technology assists to reduce security risks, poor NM may mean that the network is insecure. Therefore the only safe solution is ensuring employees have the skills and understanding to maintain and manage network devices and security properly.

Most of the NM devices use CLI which requires a good understanding and experience of the device to manage it. Lack of understanding reduces the likelihood of successful NM even if the right NM model or method is used. The SM approach includes implementation details derived from CLI commands, hence it is possible to easily verify and validate device operations. The research results clearly demonstrated that these models are diagrammatic and easy to use. Hence, using these models to document a network it is relatively easy to understand the purpose and structure of the devices. The state models employ leveling and hence provide hierarchical top down decomposition thereby controlling technical detail. This leads to more efficient NM. An evaluation of state model diagrams as a NM tool clearly demonstrated that it provided documentation, functionality not found in either the Command Line Interface or a standard NM tool. It also provided that the State model can integrated into a vendor based system to simplify network management. Finally new, diagrammatic State Model diagrams are very useful for secure NM environment.
7.0 REFERENCES


12 November 2005,

Information Letter for the Questionnaire

Dear Participant,

This letter is an invitation to consider participating in a study of an investigation of Network Security Management Methods which I am conducting as a part of my Bachelor of Science Honours (Computer Science) degree in the School of Communication, Health and Science at Edith Cowan University, under the supervision of Associate Professor Dr Paul Maj. I would like to provide you with more information about this project and what your involvement would result in if you decide to take part.

Network Management (NM) is concerned with reducing complexity and managing cost. The traditional NM tools and techniques are based on the Open System Interconnection (OSI) NM model. However, several drawbacks have been identified when managing a network using traditional NM tools. Network security is a major issue when managing a network. Even though the technology assists to reduce security risks, unless properly managed, the security measures may not do the job as expected. In order to manage the network easily, network administrators must have a good knowledge of the network devices and their operation. Though, most Internetworking devices are generally based on the Command-Line Interface (CLI). The complexity of the CLI affects the learning phase, which may result in the lack of ability to manage the device.

State Model (SM) is a new method, which may assist in managing the network. This new method may provide functionality not currently offered by current NM tools. Furthermore, it may be possible to integrate the SM with NM tools. The benefit of the State model is that it gives us the complete picture of the network, another word, it is diagrammatic, allowing us to view the physical as well as the logical topologies.

The main aim of the research is to find out whether the State model assists in network security management to simplify the complexity of the networks and as a result leads to more successful network management.

Taking part in this study is voluntary. The questionnaire will be conducted in the Cisco Internetworking laboratory, room 13.134, at Mount Lawley campus. The questionnaire may take approximately 30 minutes. You have the right not to answer any of the questions. I promise you will not find this questionnaire as difficult. Furthermore, you may decide to withdraw from this study at any time.

All information you provide is completely confidential. Your name will not appear in any thesis or report resulting from this study, however, with your permission, anonymous quotations may be used. Data collected during this study will be kept for a minimum of 5 years and no one can gain access to the information except myself and my supervisor Dr. S. P. Maj. There are no known or anticipated risks to you as a...
participant in this study. You will have the opportunity to reflect on your own learning by participating to this study. Also your responses may provide useful information to the network managers and administrators searching for ways to minimize costs and complexity when managing the network. Also may helpful to the students on networking courses.

If you have any questions regarding this research or would like further information to help you in reaching a decision about participation, please do not hesitate to contact me on [redacted] or my email [redacted] You can also contact my supervisor, Associate Professor Dr Paul Maj on [redacted] or alternatively you can email him on p.maj@ecu.edu.au. Further, if you have any concerns or complaints about the research project and wish to talk to an independent person, you may contact:

Research Ethics Officer  
Human Research Ethics Officer  
Edith Cowan University  
100 Joondalup Drive  
JOONDALUP WA 6027  
Phone: (08) 6304 2170  
Email: research.ethics@ecu.edu.au

If you would like to participate, please sign the Informed Consent Document and return it to me. Your cooperation will be greatly appreciated.

Yours sincerely,

Shamila Ratnayake.
Informed Consent Document

I have read the information presented in the information letter for the study of an investigation of Network Security Management Methods being conducted by Mr. Shamila Ratnayake of School of Communication, Health and Science at Edith Cowan University. I have had the opportunity to ask any questions related to this study, to receive satisfactory answers to my questions, and any additional details I wanted.

I am aware that I have the option of allowing the information from the questionnaire may be included in the thesis and/or publications to come from this research, with the understanding that the quotations will be anonymous.

I was informed that all information I provide is completely confidential and I may withdraw my consent at any time without penalty by advising the researcher.

I was informed that if I have any comments or concerns resulting from my participation in this study, I may contact either project supervisor on [email protected] email p.maj@ecu.edu.au or office of Ethics Research at Edith Cowan University on (08) 6304 2170, email research.ethics@ecu.edu.au.

I, ___________________________ freely do agree/ do not agree to participate in this project.

I do agree/ do not agree to the use of anonymous quotations in any thesis or publication that comes from this research.

__________________________  ___/___/_____
Participant’s Signature      Date

__________________________  ___/___/_____
Investigator’s Signature     Date
Questionnaire: Network Security Management Methods

01) What is your job title? Circle one.
   a) Network Expert
   b) Network Student
   c) Other; Please specify ____________________________

02) Do you have experience in network management area? Circle one.
   a) Yes
   b) No (Please skip questions 03 and 04. Go directly to question 05)

If Yes: How many years of experience do you have? __________________

03) Which methods/models/tools you use to manage your network? eg. Cisco Works

__________________________________________

04) What methods do you use to identify security risks in your network?

__________________________________________

(Please skip question 05. Go directly to question 06)

05) Which kind of experience do you have in the networking field?

__________________________________________

06) Does the State Model provide an easy way to understand the relationships between the devices of the network? Circle one.
   a) Yes
   b) No
   c) Do not know

If Yes: Do you think State Model approach helps to identify any security risk?

__________________________________________

Below each of the statements presented below, please indicate whether you Strongly Agree (SA), Agree (A), Disagree (D), Strongly Disagree (SD), or are Undecided (U).

07) The State Model allows network administrators to have a better view of the entire network than other methods/models.
   SA A D SD U

08) The State Model cannot be used to manage complex networks.
   SA A D SD U
09) The integration of the State Model with the CiscoWorks makes the complexity of the network easier to understand.

SA   A   D   SD   U

10) The State Model does not provide efficient network management.

SA   A   D   SD   U

11) The State Model assists in network security management as a tool and as a result leads to more successful network management.

SA   A   D   SD   U

12) I would not use the State Model to manage my network.

SA   A   D   SD   U

13) Comments:

_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

Thank you very much for your help.
12 November 2005,

Information Letter for the Interview

Dear Participant,

This letter is an invitation to consider participating in a study of an investigation of Network Security Management Methods which I am conducting as a part of my Bachelor of Science Honours (Computer Science) degree in the School of Communication, Health and Science at Edith Cowan University, under the supervision of Associate Professor Dr Paul Maj. I would like to provide you with more information about this project and what your involvement would result in if you decide to take part.

Network Management (NM) is concerned with reducing complexity and managing cost. The traditional NM tools and techniques are based on the Open System Interconnection (OSI) NM model. However, several drawbacks have been identified when managing a network using traditional NM tools. Network security is a major issue when managing a network. Even though the technology assists to reduce security risks, unless properly managed, the security measures may not do the job as expected. In order to manage the network easily, network administrators must have a good knowledge of the network devices and their operation. Though, most Internetworking devices are generally based on the Command-Line Interface (CLI). The complexity of the CLI affects the learning phase, which may result in the lack of ability to manage the device.

State Model (SM) is a new method, which may assist in managing the network. This new method may provide functionality not currently offered by current NM tools. Furthermore it may be possible to integrate the SM with NM tools. The benefit of the State model is that it give us the complete picture of the network, another word, it is diagrammatic, allowing us to view the physical as well as the logical topologies.

The main aim of the research is to find out whether the State model assists in network security management to simplify the complexity of the networks and as a result leads to more successful network management.

Taking part in this study is voluntary. The interview will be conduct in the Cisco Internetworking laboratory, room 13.134, at Mount Lawley campus. The interview may take about 30 minutes. You have the right not to answer any of the interview questions. Furthermore, you may decide to withdraw from this study at any time.

With your permission, I will tape-record your conversation to assist my collection of data for analysis later. All information you provide is completely confidential. Your name will not appear in any thesis or report resulting from this study, however, with your permission anonymous quotations may be used. Data collected during this study will be kept for a minimum of 5 years and no one can gain access to the information except my self and my supervisor Dr. S. P. Maj. There are no known or anticipated risks.
to you as a participant in this study. You will have the opportunity to reflect on your own learning by participating in this study. Also your responses may provide useful information to the network managers and administrators searching for ways to minimize costs and complexity when managing the network. Also may helpful to the students on networking courses.

If you have any questions regarding this research or would like further information to help you in reaching a decision about participation, please do not hesitate to contact me on [redacted] or my email [redacted]. You can also contact my supervisor, Associate Professor Dr Paul Maj on [redacted] or alternatively you can email him on p.maj@ecu.edu.au. Further, if you have any concerns or complaints about the research project and wish to talk to an independent person, you may contact:

Research Ethics Officer
Human Research Ethics Officer
Edith Cowan University
100 Joondalup Drive
JOONDALUP WA 6027
Phone: (08) 6304 2170
Email: research.ethics@ecu.edu.au

If you would like to participate, please sign the Informed Consent Document and return it to me. Your cooperation will be greatly appreciated.

Yours sincerely,

Shamila Ratnayake.
Informed Consent Document

I have read the information presented in the information letter for the study of an investigation of Network Security Management Methods being conducted by Mr Shamila Ratnayake of School of Communication, Health and Science at Edith Cowan University. I have had the opportunity to ask any questions related to this study, to receive satisfactory answers to my questions, and any additional details I wanted.

I am aware that I have the option of allowing my interview to be tape-recorded and the information from the interview may be included in the thesis and/or publications to come from this research, with the understanding that the quotations will be anonymous.

I was informed that all information I provide is completely confidential and I may withdraw my consent at any time without penalty by advising the researcher.

I was informed that if I have any comments or concerns resulting from my participation in this study, I may contact either project supervisor or office of Ethics Research at Edith Cowan University on (08) 6304 2170, email research.ethics@ecu.edu.au.

I, ____________________________ freely do agree/ do not agree to participate in this project.

I do agree/ do not agree to have my interview tape-recorded.

I do agree/ do not agree to the use of anonymous quotations in any thesis or publication that comes from this research.

_________________________________   __/__/____
Participant’s Signature            Date

_________________________________   __/__/____
Investigator’s Signature           Date
Interview Questions: Network Security Management Methods

01) What is your job title?
   a) Network Expert
   b) Network Student
   c) Other; Please specify __________________________

02) Do you have experience in network management area?
   c) Yes
   d) No (Please skip questions 03, 04, 05, 06 and 07. Go directly to question 08)

   If Yes: How many years of experience do you have? __________________________

03) Which methods/ models/ tools you use to manage your network? eg. CiscoWorks

04) How often you use these tools in your day to day work?

05) Areas in which you use these tools? e.g. connectivity issues, availability, change configuration etc.

06) Do you use the tools for reporting to management or fault finding?

07) What are the issues with current network management tools? eg. Product specific or generic

(Please skip question 08. Go directly to question 09)

08) Which kind of experience do you have in the networking field?

09) Does the State Model provide an easy way to understand the relationships between the devices of the network?
   d) Yes
   e) No
   f) Do not know

   If Yes: Do you think State Model approach helps to identify any security risk?
Below each of the statements presented below, please indicate whether you Strongly Agree (SA), Agree (A), Disagree (D), Strongly Disagree (SD), or are Undecided (U).

10) The State Model allows network administrators to have a better view of the entire network than other methods/models.

   SA  A  D  SD  U

11) The State Model cannot be used to manage complex networks.

   SA  A  D  SD  U

12) The integration of the State Model with the CiscoWorks makes the complexity of the network easier to understand.

   SA  A  D  SD  U

13) The State Model does not provide efficient network management.

   SA  A  D  SD  U

14) The State Model assists in network security management as a tool and as a result leads to more successful network management.

   SA  A  D  SD  U

15) I would not use the State Model to manage my network.

   SA  A  D  SD  U

16) Comments:

   __________________________________________
   __________________________________________
   __________________________________________
   __________________________________________
   __________________________________________

   Thank you very much for your help.
Experiment 1

CiscoWorks server:

C: \Documents and Settings \Administrator> ipconfig /all
Windows IP Configuration
   Physical Address: 00-02-55-7A-6F-D3
   IP Address: 192.168.1.1
   Subnet Mask: 255.255.255.0
   Default Gateway: 192.168.1.2

PC 1:

C: \Documents and Settings \Administrator> ipconfig /all
Windows IP Configuration
   Physical Address: 00-02-55-73-B2-3A
   IP Address: 192.168.2.1
   Subnet Mask: 255.255.255.0
   Default Gateway: 192.168.2.2

PC 2:

C: \Documents and Settings \Administrator> ipconfig /all
Windows IP Configuration
   Physical Address: 00-02-55-73-08-24
   IP Address: 192.168.3.1
   Subnet Mask: 255.255.255.0
   Default Gateway: 192.168.3.2

PIX Firewall:

PIX(config)# show run
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50

ip address outside 192.168.3.2 255.255.255.0
ip address inside 192.168.1.2 255.255.255.0
ip address dmz 192.168.2.2 255.255.255.0

static (inside,outside) 192.168.3.99 192.168.1.1 netmask 255.255.255.0
static (inside,dmz) 192.168.2.99 192.168.1.1 netmask 255.255.255.0
static (dmz,outside) 192.168.3.98 192.168.2.1 netmask 255.255.255.0

snmp-server host inside 192.168.1.1
snmp-server community public
snmp-server enable traps
end

PIX(config)# show int el
interface ethernet1 "inside" is up, line protocol is up
   Hardware is 82559 ethernet, address is 0012.d96f.db47
   IP address 192.168.1.2, subnet mask 255.255.255.0
PIX1(config)# show int e2
interface ethernet2 "dmz" is up, line protocol is up
    Hardware is i82559 ethernet, address is 000e.0c66.6bdb
    IP address 192.168.2.2, subnet mask 255.255.255.0

PIX1(config)# show int e0
interface ethernet0 "outside" is up, line protocol is up
    Hardware is i82559 ethernet, address is 0012.d96f.db46
    IP address 192.168.3.2, subnet mask 255.255.255.0

PIX1(config)# show route
    inside 192.168.1.0 255.255.255.0 192.168.1.2 1 CONNECT static
dmz 192.168.2.0 255.255.255.0 192.168.2.2 1 CONNECT static
outside 192.168.3.0 255.255.255.0 192.168.3.2 1 CONNECT static

PIX1(config)# show arp
    outside 192.168.3.1 0002.5573.1167
    inside 192.168.1.1 0002.557a.6fd3
    dmz 192.168.2.1 0002.5573.b7f2

PIX1(config)# show xlate
    3 in use, 3 most used
    Global 192.168.2.99 Local 192.168.1.1
    Global 192.168.3.99 Local 192.168.1.1
    Global 192.168.3.98 Local 192.168.2.1

PIX1(config)# show conn
    1 in use, 1 most used
    TCP out 192.168.3.1:80 in 192.168.2.1:1325 idle 0:00:31 Bytes 1253
    flags UIO

PIX1(config)# show static
    static (inside, outside) 192.168.3.99 192.168.1.1 netmask 255.255.255.0 0 0
    static (inside, dmz) 192.168.2.99 192.168.1.1 netmask 255.255.255.255 0 0
    static (dmz, outside) 192.168.3.98 192.168.2.1 netmask 255.255.255.255 0 0

Experiment 2

CiscoWorks Server:

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
    Physical Address. . . . . . . . . : 00-02-55-7A-1C-39
    IP Address. . . . . . . . . . . . : 192.168.1.1
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . : 192.168.1.2

PC 1:

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
    Physical Address. . . . . . . . . : 00-02-55-73-06-49
    IP Address. . . . . . . . . . . . : 192.168.2.1
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . : 192.168.2.2
PC 2:
C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
 Physical Address: 00-02-55-73-08-67
 IP Address: 192.168.2.1
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.2.2

PIX Firewall:
PIX(config)# show run
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50

access-list ACLIN permit tcp any host 192.168.3.99 eq www
access-list ACLIN permit tcp any host 192.168.3.98 eq www
access-list ACLIN permit icmp any any echo
access-list ACLIN permit icmp any host 192.168.3.99 echo-reply
access-list ACLIN permit icmp any host 192.168.3.98 echo-reply
access-list ACLIN2 permit tcp any any
access-list ACLIN2 permit icmp any any echo
access-list ACLIN2 permit icmp any host 192.168.1.99 echo-reply
access-list ACLIN2 permit icmp any any echo-reply

ip address outside 192.168.3.2 255.255.255.0
ip address inside 192.168.2.2 255.255.255.0
ip address dmz 192.168.1.2 255.255.255.0

global (outside) 1 192.168.3.10-192.168.3.20 netmask 255.255.255.0

global (dmz) 1 192.168.1.10-192.168.1.20 netmask 255.255.255.0

nat (inside) 1 192.168.2.0 255.255.255.0 0 0

static (dmz,outside) 192.168.3.98 192.168.1.1 netmask 255.255.255.255 0 0
static (inside,dmz) 192.168.1.99 192.168.2.1 netmask 255.255.255.255 0 0
static (inside,outside) 192.168.3.99 192.168.2.1 netmask 255.255.255.255 0 0

access-group ACLIN in interface outside
access-group ACLIN2 in interface dmz
route outside 0.0.0.0 0.0.0.0 192.168.3.1 1

snmp-server host inside 192.168.1.1
snmp-server community public
snmp-server enable traps
end

PIX(config)# show int el
interface ethernet1 "inside" is up, line protocol is up
 Hardware is i82559 ethernet, address is 0012.d96f.db47
 IP address 192.168.2.2, subnet mask 255.255.255.0

PIX(config)# show int eg
interface ethernet0 "outside" is up, line protocol is up
 Hardware is i82559 ethernet, address is 0012.d96f.db46
 IP address 192.168.3.2, subnet mask 255.255.255.0
PIX(config) # show route
outside 0.0.0.0 0.0.0.0 192.168.3.1 1 OTHER static
dmz 192.168.1.0 255.255.255.0 192.168.1.2 1 CONNECT static
inside 192.168.2.0 255.255.255.0 192.168.2.2 1 CONNECT static
outside 192.168.3.0 255.255.255.0 192.168.3.2 1 CONNECT static
PIX(config) # show xlate
3 in use, 3 most used
Global 192.168.3.99 Local 192.168.2.1
Global 192.168.3.98 Local 192.168.1.1
Global 192.168.1.99 Local 192.168.2.1
PIX(config) # show arp
outside 192.168.3.1 000c.309e.6481
inside 192.168.2.1 0002.5573.b7f2
dmz 192.168.1.1 0002.557a.6fd3
PIX(config) # show conn
1 in use, 6 most used
TCP out 192.168.4.1:80 in 192.168.1.1:1895 idle 0:02:18 Bytes 1253
flags UO
PIX(config) # show static
static (dmz, outside) 192.168.3.98 192.168.1.1 netmask 255.255.255.255 0 0
static (inside, dmz) 192.168.1.99 192.168.2.1 netmask 255.255.255.255 0 0
static (inside, outside) 192.168.3.99 192.168.2.1 netmask 255.255.255.255 0 0
PIX(config) # show global
global (outside) 1 192.168.3.10-192.168.3.20 netmask 255.255.255.0
global (dmz) 1 192.168.1.10-192.168.1.20 netmask 255.255.255.0
PIX(config) # show nat
nat (inside) 1 192.168.2.0 255.255.255.0 0 0
PIX(config) # show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 1024)
alert-interval 300
access-list ACLIN; 5 elements
access-list ACLIN line 1 permit tcp any host 192.168.3.99 eq www
(hitcnt=7)
access-list ACLIN line 2 permit tcp any host 192.168.3.98 eq www
(hitcnt=7)
access-list ACLIN line 3 permit icmp any any echo (hitcnt=213)
access-list ACLIN line 4 permit icmp any host 192.168.3.99 echo-reply
(hitcnt=16)
access-list ACLIN line 5 permit icmp any host 192.168.3.98 echo-reply
(hitcnt=12)
access-list ACLIN2; 4 elements
access-list ACLIN2 line 1 permit tcp any any (hitcnt=15)
access-list ACLIN2 line 2 permit icmp any any echo (hitcnt=109)
access-list ACLIN2 line 3 permit icmp any host 192.168.1.99 echo-reply
(hitcnt=28)
access-list ACLIN2 line 4 permit icmp any any echo-reply (hitcnt=8)
PIX(config) # show access-group
access-group ACLIN in interface outside
access-group ACLIN2 in interface dmz
Router:

Router#show int fa0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is AmdFE, address is 000c.309e.6481 (bia 000c.309e.6481)
  Internet address is 192.168.3.1/24

Router#show int fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.309e.6480 (bia 000c.309e.6480)
  Internet address is 192.168.4.2/24

Router#show run
Building configuration...
hostname Router
interface FastEthernet0/0
  ip address 192.168.4.2 255.255.255.0
interface FastEthernet0/1
  ip address 192.168.3.1 255.255.255.0
router rip
  network 192.168.3.0
  network 192.168.4.0
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps tty
end

Router#show ip route
C  192.168.4.0/24 is directly connected, FastEthernet0/0
C  192.168.3.0/24 is directly connected, FastEthernet0/1

Router#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.3.99 106 0012.d96f.db46 ARPA
FastEthernet0/1
Internet 192.168.3.98 105 0012.d96f.db46 ARPA
FastEthernet0/1
Internet 192.168.3.2 7 0012.d96f.db46 ARPA
FastEthernet0/1
Internet 192.168.3.1 0 000c.309e.6481 ARPA
FastEthernet0/1
Internet 192.168.4.1 7 0002.5573.1167 ARPA
FastEthernet0/0
Internet 192.168.4.2 0 000c.309e.6480 ARPA
FastEthernet0/0
Router#

Experiment 3:

CiscoWorks Server:

C:\Documents and Settings\Administrator>spconfig /all
Windows IP Configuration
  Physical Address: 00-40-96-A6-7D-64
  IP Address: 192.168.4.1
  Subnet Mask: 255.255.255.0
  Default Gateway: 192.168.4.2
PC 1:

C:\Documents and Settings\Administrator> ipconfig /all
Windows IP Configuration
Physical Address: 00-02-55-7A-81-25
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.2

PC 2:

C:\Documents and Settings\Administrator> ipconfig /all
Windows IP Configuration
Physical Address: 00-02-55-73-0B-48
IP Address: 192.168.3.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.3.2

PIX Firewall: (**Same configurations for the Experiment 4**)

PIX(config)# show run
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
access-list ACLIN permit tcp any host 192.168.3.99 eq www
access-list ACLIN permit tcp any host 192.168.3.98 eq www
access-list ACLIN permit icmp any any echo
access-list ACLIN permit icmp any host 192.168.3.99 echo-reply
access-list ACLIN permit icmp any host 192.168.3.98 echo-reply
access-list ACLIN2 permit tcp any any eq WWW
access-list ACLIN2 permit icmp any any echo-reply eq WWW
access-list ACLIN2 permit icmp any any echo
access-list ACLIN2 permit icmp any host 192.168.1.99 echo-reply
access-list ACLIN2 permit icmp any any echo-reply
ip address outside 192.168.3.2 255.255.255.0
ip address inside 192.168.2.2 255.255.255.0
ip address dmz 192.168.1.2 255.255.255.0

global (outside) 1 192.168.3.10-192.168.3.20 netmask 255.255.255.0
global (dmz) 1 192.168.1.10-192.168.1.20 netmask 255.255.255.0

nat (inside) 1 192.168.4.0 255.255.255.0 0 0
static (dmz, outside) 192.168.3.98 192.168.1.1 netmask 255.255.255.255 0 0
static (inside, dmz) 192.168.1.99 192.168.4.1 netmask 255.255.255.255 0 0
static (inside, outside) 192.168.3.99 192.168.4.1 netmask 255.255.255.255 0 0

access-group ACLIN in interface outside
access-group ACLIN2 in interface dmz
route inside 0.0.0.0 0.0.0.0 192.168.2.1 1

snmp-server host inside 192.168.4.1
snmp-server community public
snmp-server enable traps
end
PIX(config)# show route
inside 0.0.0.0 0.0.0.0 192.168.2.1 1 OTHER static
dmz 192.168.1.0 255.255.255.0 192.168.1.2 1 CONNECT static
inside 192.168.2.0 255.255.255.0 192.168.2.2 1 CONNECT static
outside 192.168.3.0 255.255.255.0 192.168.3.2 1 CONNECT static

PIX(config)# show int e1
interface ethernet1 "inside" is up, line protocol is up
Hardware is i82559 ethernet, address is 0012.d96f.db47
IP address 192.168.2.2, subnet mask 255.255.255.0

PIX(config)# show int e2
interface ethernet2 "dmz" is up, line protocol is up
Hardware is i82559 ethernet, address is 000e.0c66.6bdb
IP address 192.168.1.2, subnet mask 255.255.255.0

PIX(config)# show int e0
interface ethernet0 "outside" is up, line protocol is up
Hardware is i82559 ethernet, address is 0012.d96f.db46
IP address 192.168.3.2, subnet mask 255.255.255.0

PIX(config)# show xlate
3 in use, 5 most used
Global 192.168.3.99 Local 192.168.4.1
Global 192.168.3.98 Local 192.168.1.1
Global 192.168.1.99 Local 192.168.4.1

PIX(config)# show arp
outside 192.168.3.1 0002.5573.1167
inside 192.168.2.1 000c.309e.6480
dmz 192.168.1.1 0002.5573.b7f2

PIX(config)# show static
static (dmz,outside) 192.168.3.98 192.168.1.1 netmask 255.255.255.255 0 0
static (inside,dmz) 192.168.1.99 192.168.4.1 netmask 255.255.255.255 0 0
static (inside,outside) 192.168.3.99 192.168.4.1 netmask 255.255.255.255 0 0

PIX(config)# show global
global (outside) 1 192.168.3.10-192.168.3.20 netmask 255.255.255.0
global (dmz) 1 192.168.1.10-192.168.1.20 netmask 255.255.255.0

PIX(config)# show nat
nat (inside) 1 192.168.4.0 255.255.255.0 0 0

PIX(config)# show conn
2 in use, 6 most used
TCP out 192.168.1.1:1381 in 192.168.4.1:80 idle 0:00:19 Bytes 1255
flags UIOB
TCP out 192.168.3.1:80 in 192.168.1.1:1382 idle 0:00:11 Bytes 1253
flags UIO

Router: (**Same configurations for the Experiment 4**)

Router#show int fa0/1
FastEthernet0/1 is up, line protocol is up
Hardware is AmdFE, address is 000c.309e.6481 (bia 000c.309e.6481)
Internet address is 192.168.4.2/24

Router#show int fa0/0
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 000c.309e.6480 (bia 000c.309e.6480)
Internet address is 192.168.2.1/24

Router#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.2.2 5 0012.d96f.db47 ARPA
FastEthernet0/0
Internet 192.168.2.1 - 000c.309e.6480 ARPA
FastEthernet0/0
Internet 192.168.4.1 5 0002.557a.6fd3 ARPA
FastEthernet0/1
Internet 192.168.4.2 - 000c.309e.6481 ARPA
FastEthernet0/1

Router#show ip route
Codes: C - connected, S - static,
C 192.168.4.0/24 is directly connected, FastEthernet0/1
S 192.168.1.0/24 [1/0] via 192.168.2.2
C 192.168.2.0/24 is directly connected, FastEthernet0/0
S 192.168.3.0/24 [1/0] via 192.168.2.2

Router#show run
Building configuration...
hostname Router
interface FastEthernet0/0
  ip address 192.168.2.1 255.255.255.0
interface FastEthernet0/1
  ip address 192.168.4.2 255.255.255.0
  ip classless
  ip route 192.168.1.0 255.255.255.0 192.168.2.2
  ip route 192.168.3.0 255.255.255.0 192.168.2.2
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps tty
end

Switch: (**Same configurations for the Experiment 4**)

Switch_B#show mac-address-table dynamic
Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0002.557a.6fd3</td>
<td>DYNAMIC</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>1</td>
<td>000c.309e.6481</td>
<td>DYNAMIC</td>
<td>Fa0/2</td>
</tr>
</tbody>
</table>

Total Mac Addresses for this criterion: 2

Switch_B#show int fa0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000c.30df.a281 (bia 000c.30df.a281)

Switch_B#show int fa0/2
FastEthernet0/2 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000c.30df.a282 (bia 000c.30df.a282)
Switch_B#show run
hostname Switch_B

interface Vlan1
 ip address 192.168.4.12 255.255.255.0

snmp-server community public RO
snmp-server community private RW

end

Experiment 4:

CiscoWorks Server:

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
 Physical Address: 00-40-96-A6-7D-64
 IP Address: 192.168.4.1
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.4.2

PC 1:

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
 Physical Address: 00-02-55-73-B7-F2
 IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.1.2

PC 2:

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
 Physical Address: 00-02-55-73-11-67
 IP Address: 192.168.3.1
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.3.2

Access Point:

ap#show run
Building configuration...
version 12.2

hostname ap

interface Dot11Radio1

 ssid ML13.134-AP4
 authentication open
guest-mode

interface BV11
 ip address 192.168.4.10 255.255.255.0

ip radius source-interface BV11
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps tty

end
ap#show int bvi 1
BVII is up, line protocol is up
   Hardware is BVI, address is 000b.5f55.3972 (bia 000b.46ca.61c5)
   Internet address is 192.168.4.10/24

ap#show int dot11Radio 1
Dot11Radio1 is up, line protocol is up
   Hardware is 802.11A Radio, address is 000b.46ca.61c5 (bia 000b.46ca.61c5)

**Experiment 5:**

**PC 1:**

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
   Physical Address. . . . . . : 00-02-55-73-B7-F2
   IP Address. . . . . . . : 192.168.1.1
   Subnet Mask . . . . . . : 255.255.255.0
   Default Gateway . . . . : 192.168.1.2

**PC 2:**

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
   Physical Address. . . . . . : 00-02-55-73-11-67
   IP Address. . . . . . . : 192.168.1.2
   Subnet Mask . . . . . . : 255.255.255.0
   Default Gateway . . . . : 192.168.1.3

**CiscoWorks Server:**

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
   Physical Address. . . . . . : 00-02-55-73-20-24
   IP Address. . . . . . . : 192.168.1.1
   Subnet Mask . . . . . . : 255.255.255.0
   Default Gateway . . . . : 192.168.1.3

**PC 4:**

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
   Physical Address. . . . . . : 00-02-55-73-B2-3A
   IP Address. . . . . . . : 192.168.1.2
   Subnet Mask . . . . . . : 255.255.255.0
   Default Gateway . . . . : 192.168.1.3

**AccessPoint 1:**

ap#show run
hostname ap

interface Dot11Radio1
   ssid ML13.134-AP5
   authentication open
guest-mode
interface BVII
   ip address 192.168.1.10 255.255.255.0
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps tty
end
BVIl is up, line protocol is up  
Hardware is BVI, address is 0013.1a32.97eb (bia 0011.20ee.d2bd)  
Internet address is 192.168.1.10/24

Dot11Radio1 is up, line protocol is up  
Hardware is 802.11A Radio, address is 0011.20ee.d2bd (bia 0011.20ee.d2bd)

Switch 1:

switch1# show mac-address-table  
Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0012.d96f.db47</td>
<td>DYNAMIC</td>
<td>Fa0/2</td>
</tr>
<tr>
<td>1</td>
<td>0013.1a32.97eb</td>
<td>DYNAMIC</td>
<td>Fa0/1</td>
</tr>
<tr>
<td>1</td>
<td>0040.96a6.7df2</td>
<td>DYNAMIC</td>
<td>Fa0/1</td>
</tr>
</tbody>
</table>

Total Mac Addresses for this criterion: 3

FastEthernet0/1 is up, line protocol is up  
Hardware is Fast Ethernet, address is 0009.b7c8.1841 (bia 0009.b7c8.1841)

PIX Firewall 1:

PIX1(config)# show run  
PIX Version 6.3(4)  
interface ethernet0 100full  
interface ethernet1 100full  
nameif ethernet0 outside security0  
nameif ethernet1 inside security100  
hostname PIX1

access-list ACLIN permit icmp any any echo  
access-list ACLIN permit icmp any host 192.168.2.99 echo-reply  
access-list ACLIN permit tcp any host 192.168.2.99 eq www  
access-list ACLIN permit icmp any host 192.168.2.98 echo-reply  
access-list ACLIN permit tcp any host 192.168.2.98 eq www

ip address outside 192.168.2.1 255.255.255.0  
ip address inside 192.168.1.3 255.255.255.0

static (inside,outside) 192.168.2.99 192.168.1.1 netmask  
255.255.255.255 0 0  
static (inside,outside) 192.168.2.98 192.168.1.2 netmask  
255.255.255.255 0 0
access-group ACLIN in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.2.2 1

snmp-server host inside 192.168.5.1
snmp-server community public
snmp-server enable traps
end

PIX1(config)# show route
outside 0.0.0.0 0.0.0.0 192.168.2.2 1 OTHER static
inside 192.168.1.0 255.255.255.0 192.168.1.3 1 CONNECT static
outside 192.168.2.0 255.255.255.0 192.168.2.1 1 CONNECT static

PIX1(config)# show conn
2 in use, 3 most used
TCP out 192.168.4.98:80 in 192.168.1.1:1053 idle 0:00:27 Bytes 1255 flags UIO
TCP out 192.168.4.99:80 in 192.168.1.1:1055 idle 0:00:06 Bytes 1255 flags UIO

PIX1(config)# show conn
2 in use, 3 most used
TCP out 192.168.4.99:80 in 192.168.1.2:1063 idle 0:00:19 Bytes 1255 flags UIO
TCP out 192.168.4.98:80 in 192.168.1.2:1065 idle 0:00:03 Bytes 1255 flags UIO

PIX1(config)# show xlate
2 in use, 2 most used
Global 192.168.2.99 Local 192.168.1.1
Global 192.168.2.98 Local 192.168.1.2

PIX1(config)# show arp
outside 192.168.2.2 0009.b765.29a0
inside 192.168.1.1 0002.5573.163c
inside 192.168.1.2 0002.557a.6e7e

PIX1(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 1024)
alert-interval 300
access-list ACLIN: 5 elements
access-list ACLIN line 1 permit icmp any any echo (hitcnt=29)
access-list ACLIN line 2 permit icmp any host 192.168.2.99 echo-reply (hitcnt=36)
access-list ACLIN line 3 permit tcp any host 192.168.2.99 eq www (hitcnt=1)
access-list ACLIN line 4 permit icmp any host 192.168.2.98 echo-reply (hitcnt=8)
access-list ACLIN line 5 permit tcp any host 192.168.2.98 eq www (hitcnt=1)

PIX1(config)# show static
static (inside,outside) 192.168.2.99 192.168.1.1 netmask 255.255.255.0
static (inside,outside) 192.168.2.98 192.168.1.2 netmask 255.255.255.0

PIX1(config)# show int et1
interface ethernet1 "inside" is up, line protocol is up
Hardware is 82559 ethernet, address is 0012.d96f.db47
IP address 192.168.1.3, subnet mask 255.255.255.0

68
PIX1(config)# show int e0
interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0012.d96f.db46
  IP address 192.168.2.1, subnet mask 255.255.255.0

Router 1:

router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

R  192.168.4.0/24 [120/1] via 192.168.3.2, 00:00:25, Serial0/0
C  192.168.2.0/24 is directly connected, FastEthernet0/0
C  192.168.3.0/24 is directly connected, Serial0/0

router1#show run
hostname router1

interface FastEthernet0/0
  ip address 192.168.3.1 255.255.255.0

interface FastEthernet0/1
  ip address 192.168.2.2 255.255.255.0

router rip
  network 192.168.2.0
  network 192.168.3.0

snmp-server community public RO
snmp-server community private RW
snmp-server enable traps tty
end

router1#show arp
Protocol Address      Age (min) Hardware Addr Type Interface
Internet 192.168.2.99 34 0012.d96f.db46 ARPA
FastEthernet0/1
Internet 192.168.2.2  - 000c.309e.6481 ARPA
FastEthernet0/1
Internet 192.168.3.2 34 000c.30e2.c620 ARPA
FastEthernet0/0
Internet 192.168.3.1  - 000c.309e.6480 ARPA
FastEthernet0/0
Internet 192.168.2.1 15 0012.d96f.db46 ARPA
FastEthernet0/1

router1#show int fa0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is AmdFE, address is 000c.309e.6481 (bia 000c.309e.6481)
  Internet address is 192.168.2.2/24

router1#show int fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.309e.6480 (bia 000c.309e.6480)
  Internet address is 192.168.3.1/24

Access Point 2:

ap#show run
Building configuration...
hostname ap

interface Dot11Radio1
ssid ML13.134-AP4
    authentication open
guest-mode
!
interface BVII
    ip address 192.168.4.10 255.255.255.0

ip radius source-interface BVII
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps tty
end

ap#show int bvi 1
BVII is up, line protocol is up
    Hardware is BVII, address is 000b.5f55.3972 (bia 000b.46ca.61c5)
    Internet address is 192.168.4.10/24

ap#show int dot11Radio 1
Dot11Radio1 is up, line protocol is up
    Hardware is 802.11A Radio, address is 000b.46ca.61c5 (bia 000b.46ca.61c5)

Switch 2:

switch2#show mac-address-table
Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0002.5573.2024</td>
<td>DYNAMIC</td>
<td>Fa0/3</td>
</tr>
<tr>
<td>1</td>
<td>0012.d96f.db39</td>
<td>DYNAMIC</td>
<td>Fa0/2</td>
</tr>
</tbody>
</table>

Total Mac Addresses for this criterion: 2

switch2#show int fa0/2
FastEthernet0/2 is up, line protocol is up
    Hardware is Fast Ethernet, address is 000c.30df.a282 (bia 000c.30df.a282)

switch2# show run
interface Vlan1
    ip address 192.168.5.11 255.255.255.0

snmp-server engineID local 800000090300000C30DFA281
snmp-server community public RO
snmp-server community private RW
end

PIX Firewall 2:

PIX2(config)# show route
    out 0.0.0.0 0.0.0.0 192.168.4.2 1 OTHER static
    out 192.168.4.0 255.255.255.0 192.168.4.1 1 CONNECT static
    inside 192.168.5.0 255.255.255.0 192.168.5.3 1 CONNECT static

PIX2(config)# show run
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full

nameif ethernet0 out security0
nameif ethernet1 ins inside security100
hostname PIX2

access-list ACLIN permit tcp any host 192.168.4.99 eq www
access-list ACLIN permit icmp any any echo
access-list ACLIN permit tcp any host 192.168.4.98 eq www
access-list ACLIN permit icmp any host 192.168.4.98 echo-reply

ip address out 192.168.4.1 255.255.255.0
ip address inside 192.168.5.3 255.255.255.0

static (inside,out) 192.168.4.99 192.168.5.1 netmask 255.255.255.255 0
static (inside,out) 192.168.4.98 192.168.5.2 netmask 255.255.255.255 0

access-group ACLIN in interface out
route out 0.0.0.0 0.0.0.0 192.168.4.2 1

snmp-server host inside 192.168.5.1
snmp-server community public
snmp-server enable traps
end

PIX2(config)# show conn
3 in use, 3 most used
TCP out 192.168.2.99:80 in 192.168.5.2:1048 idle 0:00:21 Bytes 1255
flags UIO
TCP out 192.168.2.98:80 in 192.168.5.1:1054 idle 0:00:56 Bytes 1255
flags UIO
TCP out 192.168.2.98:80 in 192.168.5.2:1050 idle 0:00:06 Bytes 1255
flags UIO

PIX2(config)# show xlate
2 in use, 2 most used
Global 192.168.4.99 Local 192.168.5.1
Global 192.168.4.98 Local 192.168.5.2

PIX2(config)# show arp
out 192.168.4.2 0009.b76f.ad60
inside 192.168.5.2 0002.5573.b23c
inside 192.168.5.1 0002.5573.098b

PIX2(config)# show static
static (inside,out) 192.168.4.99 192.168.5.1 netmask 255.255.255.255 0
static (inside,out) 192.168.4.98 192.168.5.2 netmask 255.255.255.255 0

PIX2(config)# show int el
interface ethernet1 "inside" is up, line protocol is up
   Hardware is i82559 ethernet, address is 0012.d96f.db39
   IP address 192.168.5.3, subnet mask 255.255.255.0

PIX2(config)# show int e0
interface ethernet0 "out" is up, line protocol is up
   Hardware is i82559 ethernet, address is 0012.d96f.db38
   IP address 192.168.4.1, subnet mask 255.255.255.0

71
**Router 2:**

```
router2#show run
hostname router2

interface FastEthernet0/0
ip address 192.168.3.2 255.255.255.0

interface FastEthernet0/1
ip address 192.168.4.2 255.255.255.0

router rip
network 192.168.3.0
network 192.168.4.0

snmp-server community public RO
snmp-server community private RW
snmp-server enable traps tty
end
```

```
router2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
C  192.168.4.0/24 is directly connected, FastEthernet0/0
R  192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:04, Serial0/1
C  192.168.3.0/24 is directly connected, Serial0/1
```

```
router2# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.4.99 26 0012.d96f.db38 ARPA
FastEthernet0/1
Internet 192.168.3.2 0 00c.30e2.c620 ARPA
FastEthernet0/0
Internet 192.168.3.1 38 00c.309e.6480 ARPA
FastEthernet0/0
Internet 192.168.4.1 12 0012.d96f.db38 ARPA
FastEthernet0/1
Internet 192.168.4.2 0 00c.30e2.c621 ARPA
FastEthernet0/1
```

```
router2#show int fa0/0
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 00c.30e2.c620 (bia 00c.30e2.c620)
Internet address is 192.168.3.2/24
```

```
router2#show int fa0/1
FastEthernet0/1 is up, line protocol is up
Hardware is AmdFE, address is 00c.30e2.c621 (bia 00c.30e2.c621)
Internet address is 192.168.4.2/24
```