

AN ACCESS CONTROL FOR KUKTEM WIRED LAN
(AC-Spot)

SIVAGANASAN S/O RAMALINGAN

A thesis submitted in fulfillment of the
requirements for the award of the degree of
Bachelor of Computer Science (Computer Systems & Network)

Faculty of Computer Systems & Software Engineering
University College of Engineering and Technology Malaysia

PERPUSTAKAAN KOLEJ UNIVERSITI KEJURUTERAAN & TEKNOLOGI MALAYSIA	
No. Perolehan	No. Panggilan
021227	TK S105.875
Tarikh	.157
31 JAN 2007	SS8 2006 re T.lect

NOVEMBER, 2006

ABSTRACT

Nowadays internet networks has become widespread technology and emerging as one information technology which connects to each other although in a different location or no matter how long as the connection of the network. There are many benefits that internet networks offer not such connecting people around the world or just about business matters but it is also beneficial in studying and learning is the reason why internet networks are so essential in universities environment. The current KUKTEM Wired LAN shows that the network considered not fully secure because there is no authentication mechanism provided. Due to this matter KUKTEM Wired LAN can be accessed by any outsiders or unauthorized parties easily by plug-in the UTP cable direct to face port. Since all users gain access to internet through KUKTEM Wired LAN, due to this the speed of internet connection decreased and network become traffic. So to overcome this kind of problem, the system needs to change to more sophisticated and secure system. Thus, this Wired LAN System (AC-Spot) was developed specifically for KUKTEM users. This system not only control access the internet by users but it become helpful to administrator ICT of KUKTEM in order to identify the person, time and IP Addresses of the users who browsing the internet. This Wired LAN System is easy to use because the architecture of the system is user-friendly. This system proved that, it is more efficient and secure compare to existing system. Application of this system developed by using PHP(Hypertext Preprocessor), JavaScript, HTML(Hypertext Markup Language) and Microsoft Office Access. Generally hoped that, this system become more secure and efficient in KUKTEM internet networks compare to current existing system.

ABSTRAK

Dalam era teknologi hari ini, rangkaian internet semakin pesat berkembang dan muncul sebagai salah satu alat komunikasi untuk menghubungkan setiap computer samada rangkaian internet dalam negara mahupun rangkaian internet luar negara. Rangkaian internet boleh dihubungkan kepada sesiapa sahaja, berkenaan dengan business, pendidikan dan pembelajaran melalui melayari internet. Sebenarnya rangkaian internet ini membawa banyak kebaikan kepada semua lapisan masyarakat terutamanya kepada para pelajar dalam menimba ilmu baru. Rangkaian internet juga memainkan peranan penting dalam urusan perniagaan secara global. Kini Rangkaian internet telah diperkenalkan hampir seluruh universiti. KUKTEM merupakan salah sebuah universiti yang mempunyai rangkaian internet yang serba moden. Walaupun KUKTEM memiliki rangkaian internet yang canggih, tetapi rangkaian internet masih belum selamat digunakan. Ini kerana rangkaian internet KUKTEM tidak memiliki mekanisme pengesahan dan mudah dimasuki oleh orang luar dengan hanya memasang kabel UTP kepada face port. Ini akan menyebabkan kelajuan rangkaian internet akan menjadi kurang dan sesak. Oleh yang demikian, Wired LAN System (AC-Spot) ini dibangunkan berdasarkan persekitaran KUKTEM yang amat diperlukan. Ia bukan sahaja dapat membantu mengawasi pihak yang tertentu sahaja melayari internet malah dapat digunakan oleh pentadbir ICT untuk mengenal pasti siapa, bila dan alamat IP bagi mereka yang melayari internet. Sistem ini juga mudah digunakan berdasarkan pembangunannya yang mesra pengguna. Sistem ini terbukti lebih berkesan dan selamat berbanding dengan sistem yang sedia ada. Aplikasi ini telah dibangunkan dengan menggunakan perisian PHP(HypertextPreprocessor), JavaScript, HTML(Hypertext Markup Language) dan Microsoft Office Access. Secara amnya, system ini akan dijangka menjadi sebuah sistem yang akan meningkatkan lagi keselamatan rangkaian internet di KUKTEM dan lebih berkesan berbanding sistem yang sedia ada.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	TITLE PAGE	i
	STUDENT'S DECLARATION	ii
	SUPERVISOR'S DECLARATION	iii
	DEDICATION	iv
	ACKNOWLEDGMENT	v
	ABSTRACT	vi
	ABSTRAK	vii
	TABLE OF CONTENTS	viii
	LIST OF TABLES	xiii
	LIST OF FIGURES	xiv
	LIST OF TERMINOLOGY	xvi
	LIST OF APPENDICES	xviii
1	INTRODUCTION	1
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Objectives	3
	1.4 Scopes	3
	1.5 Project Importance	3
	1.6 Report Organization	4

2	LITERATURE REVIEWS	5
2.1	Introduction	5
2.2	LAN Gateway	5
2.3	Implementation of LAN Gateway	6
2.4	Comparison with Current System	9
	2.4.1 Case Study-1: MODENAS	9
	2.4.2 Case Study-2: Pennsylvania Deke Kassabian University	9
2.5	Basic of AAA Framework	11
	2.5.1 Authentication	11
	2.5.2 Authorization	12
	2.5.3 Accounting	12
2.6	Network Address Translation	12
	2.6.1 Nat Operation	13
2.7	Proxies	15
	2.7.1 Benefits of Web Proxying	16
	2.7.2 Disadvantage of Web Proxying	16
2.8	IP Addresses	17
	2.8.1 Dynamic vs. Static IP Addresses	18
	2.8.2 IP version 4	19
	2.8.3 IP version 5	19
	2.8.4 IP version 6	19
2.9	Network Elements	20
	2.9.1 Avaya Stackable Ethernet Switch	20
	2.9.2 D-Link DFE-530TX+Fast Ethernet	21
2.10	Wired Network Architecture	22
	2.10.1 Network Architecture for Wired LAN	23
2.11	A propose system for an Access Control Wired LAN	24

3	METHODOLOGY	25
3.1	Introduction	25
3.2	Project Identification and Selection Level	26
3.3	Project Initiation and Planning Level	27
	3.3.1 Gantt Chart	27
	3.3.2 Technique	27
3.4	System Analysis	28
	3.4.1 Tools used in Access Control Wired LAN	28
	3.4.2 Hardware Requirements	29
	3.4.2.1 Ethernet LAN Networks	30
	3.4.2.2 Access Server	30
	3.4.2.3 Hub/Switches	31
	3.4.3 Software Requirements	31
	3.4.4 Use Case Diagram	33
3.5	System Design	35
	3.5.1 Project Design	35
	3.5.2 Interface Design	36
	3.5.2.1 User Login Form	37
	3.5.2.2 Change password Form	37
	3.5.2.3 User Information Form	38
	3.5.2.4 User Information Database	39
	3.5.2.5 System Interface	39
	3.5.2.6 User friendly	40
	3.5.2.7 Graphical Interface	40
	3.5.2.8 Color Combination	40
	3.5.2.9 Interface Security	41
	3.5.2.10Page layout	41
3.6	Implementation Level	41
	3.6.1 Databases	42

3.6.2	Server Configuration	43
3.6.3	Testing	44
3.6.4	Context Diagram of Wired LAN	45
3.6.5	A Data Flow Diagram of Wired LAN	45
3.6.6	Wired LAN Process flow	46
4	RESULT AND DISCUSSION	47
4.1	Introduction	47
4.2	Results	47
4.2.1	User Login	48
4.2.2	Redirect Page	49
4.2.3	Default Home Page	50
4.2.4	Invalid Login Page	51
4.2.5	Change Password Form	51
4.2.6	Succeed Password Change Page	52
4.2.7	Invalid User ID Page	53
4.2.8	Invalid Old Password Pages	54
4.2.9	Invalid New Password Page	56
4.2.10	Invalid Confirm Password Page	57
4.2.11	Wired LAN Infobox	58
4.2.12	User Disconnect	58
4.2.13	Wired LAN Disconnect User	59
4.2.14	One User Per Login	60
4.2.15	User Log Information	61
4.3	Discussion	62
4.4	Constraints	64

4.5	Further Research	64
5	CONCLUSION	65
	REFERENCES	67
	APPENDIX A (Gantt chart)	70
	APPENDIX B (Data Materials)	71
	APPENDIX C (User Manual)	72
	APPENDIX D (Photos)	73

LIST OF TABLES

TABLE NO	TITLE	PAGE
3.1	User Information	42

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
2.1	Packet-Internet Gateway	6
2.2	Diagram of hardware setup	8
2.3	The location of NAT	13
2.4	A simple Wired LANs Network Architecture	23
3.1	System Development Life Cycle for Wired LAN	26
3.2	Use Case Diagram of (AC-Spot) System	34
3.3	Sequence Diagram Login (User)	34
3.4	Overall System Design	36
3.5	Login Form	37
3.6	Change Password Form	38
3.7	User Information Form	38
3.8	User Information Database	39
3.9	Complete Diagram of Wired LAN system (AC-Spot)	44
3.10	Chart of the access control Wired LAN (AC-Spot)	
	Process flow	44
3.11	Context Diagram of Wired LAN (AC-Spot)	45
3.12	Data Flow Diagram of Wired LAN (AC-Spot)	45
4.1	Login page for user	48
4.2	Redirect page with inbox	49
4.3	Default Home Page	50
4.4	Invalid Login Page	51
4.5	Change Password Form	52
4.6	Succeed Password Change Page	53

4.7	Invalid User ID Page	54
4.8	Old Password Cannot Be Empty	55
4.9	Old Password Does Not Match	55
4.10	New Password Cannot Be Empty	56
4.11	Confirm Password Does Not Match	57
4.12	Wired LAN Infobox	58
4.13	User Disconnect	59
4.14	Wired LAN Disconnect user	60
4.15	One User Per Login	61
4.16	User Log Information	62

LIST OF TERMINOLOGIES

- DHCP - Dynamic Host Configuration Protocol
- DNS - Domain Name Service. It is an internet service that translates human-readable names (*like yahoo.com*) into IP addresses
- DOMAIN - A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the *IP address*.
- FTP - File Transfer Protocol
- GATEWAY - Computer that allows communications between networks one network with another.
- HTML - Hypertext Markup Language
- HTTP - Hypertext Transfer Protocol
- ICS - Internet Connection Sharing. It allows one PC on the networks to operate as an internet gateway for the other computers on the LAN
- IP - Internet Protocol
- ISP - Internet Service Provider

KUKTEM	-	Kolej Universiti Kejuruteraan & Teknologi Malaysia
LAN	-	Local Area Network
MAC	-	Media Access Control
NETWORK	-	A network is a series of points or nodes interconnected by Communication cables
PHP	-	Hypertext Preprocessor
PRIVATE	-	Private Network Interface Card(NIC). The network interface card that connects to the visitor-based network (Switch/Hub)
PUBLIC	-	Public Network Interface Card(NIC). The network interface card that connects to the public internet
SDLC	-	System Development Life Cycle
SERVER	-	A computer or device on a network that manages network Resources
SQL	-	Simple Query Language
TCP	-	Transmission Control Protocol
URL	-	Uniform Resource Locator
UTP	-	Unshielded Twisted Pair

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Gantt chart	70
B	Data Materials	71
C	User Manual For Admin/Server and Client	72
D	Photos	73

CHAPTER 1

INTRODUCTION

1.1 Project Background

Wired LAN technologies are the main communication medium and widely in most of the companies. The early research showed that Wired LAN connection is implemented in most industries were becoming popular and normally used in large office building and enterprise network. Although the Wired LAN is a traditional infrastructure method but it gives the functionality more flexible, reliable and concern on speed of internet connection. The same approach that is Wired LAN connection were used in KUKTEM campus which assist in various related computer applications such as electronic transactions and electronic learning (E-learning) environments are become more energetic and powerful. Generally the KUKTEM campus network deploying this Wired LAN communications in most fields which are involved by most IT Managers, Engineers and technical staff in this project.

Although the KUKTEM Wired network covers many area such are laboratories, around the campus, buildings, hostel and offices but have no specific access control device to prevent the network usage from unauthorized parties through the internet. Currently there is no effective way to stop the network using by outsiders. The outsiders and unauthorized parties can easily access the internet once there plugging into the network. Meanwhile the current existing system also is not secure because it will affect the KUKTEM users when they are on the network where unauthorized parties, and not

authenticate method make easily access to intranet and internet. Hence a reliable system is needed to control access for KUKTEM Wired LAN. Therefore, a prototype, system Access Control Wired LAN (AC-Spot) is developed in order control access by allowing KUKTEM users only. The main purpose to develop this prototype system is specifically used for KUKTEM staffs, students and authorized parties.

1.2 Problem Statement

Problems cannot be avoid if do not understand the types of problems that occur to the current system. In this section the will be explained the problems which faced by current system in details.

The main problem of KUKTEM internetworking is that, it does not have an authentication feature in network access, so the outsiders or unauthorized parties can easily gain access to KUKTEM Wired LAN by direct plugging into the network. Apart from access to the KUKTEM Wired LAN, the system of access control also unable to address the type of users which gain access to the internet. Due to this, there is no special requirement implied to the users such authentication rules.

Due to this disadvantage, it will result the KUKTEM Wired LAN network become more traffic and slow due to many users whether right parties or outsiders parties gain access to the network. Besides that, the outsiders or unauthorized parties can sabotage the KUKTEM Wired LAN such as hack the network and can load traffic into the network. By this way the Wired LAN network become no more secure mechanism since all type of users can access to the internet. Besides that, the network becomes unstable and not consistent.

1.3 Objective

The objectives of this project as follows:

- i) To control the Wired LAN users by implementing authentication method through a login page before access the internet.
- ii) To develop a prototype of an access control for Wired LAN network systems.

1.4 Scopes

Below are the project's scopes:

- i) Develop an access control for KUKTEM Wired LAN network with implement login authentication method.
- ii) HTML, PHP and JavaScript are used to develop coding for this prototype.
- iii) Microsoft Access is used for data management system.
- iv) This prototype is develop according to authentication method to display and store users' information such Username, IP, MAC, Login time and URL tracking.

1.5 Project Importance

By using with this new system, the KUKTEM Wired LAN can be protected from unauthorized parties from accessing the internet. Further more, the new system can addressing the type of websites frequently visited by users.

This Wired LAN system developed mainly for control users to enter the KUKTEM network. Only right persons are allowed such as KUKTEM students, staffs and authorize parties to gain access to the internet otherwise it will restricted.

1.6 Report Organization

This thesis organized into 5 main chapters which consist of chapter 1 (Introduction), chapter 2(Literature Review), chapter 3(Methodology), chapter 4(Result and Discussion) and chapter 5(Conclusion).

Chapter 1 explains about the project background of the system, and identifies the current system problems. Thus an objectives and scopes of the system were drawn in order to develop a new system which is more secure, reliable and sophisticated.

In chapter 2 the background information of the system that related to development of the project is studied and discussed. Review on some network equipments are conducted such as LAN gateway, basic of AAA, NAT, proxies, IP addresses and Wired LAN architecture.

Methodology is in chapter 3 which discuss the method that used throughout the project and defined as a guideline in development of the system. During development and implementing of the system some phases take into consideration such as project planning and requirement analysis, system design, implementation and testing.

In chapter 4 the result and discussion are presented in well manner, besides that, it shows the output of the new prototype system after the implementation. The strengths and limitations of the system are discussed as well as with the further research technique to enhance the prototype system.

Final chapter 5 explains about the conclusion of the new Wired LAN system and its future expectations.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Through this chapter the process of developing a prototype of an access control for Wired LAN system was conducted by doing research, study existing systems of access control network, study on wired technologies and survey on hotspot. Several types of software and hardware are discuss such are LAN gateway and implementation,AAA policies, Network Address Translation(NAT),IP address, Ethernet switch, Ethernet Adapter, Wired Network and Wired LAN network topology.

2.2 LAN Gateway

A network gateway is an internetworking system, a system that joins two or more networks together. A system that provided access between two or more networks. Gateways are typically used to connect networks that are dissimilar. A network gateway can be implemented completely in software, completely in hardware, or as a combination of the two (Warren Toomey VK1XWT, 1994). Depending on their implementation, network gateways can operate at any level of the OSI model from application protocols to low-level signaling. Gateway is also communication device/program which passes data between networks having similar functions but dissimilar implementations. Because a

network gateway by definition appears at the edge of a network, related functionality like fire walling tends to be installed on the network gateway.

2.3 Implementation of LAN Gateway

A packet Internet gateway obviously must be able to communicate to both the Internet, and the amateurs in its local area. Therefore, it must have at least two interfaces, one to the Internet, and another one to the amateur community. This is shown in Figure 2.1.

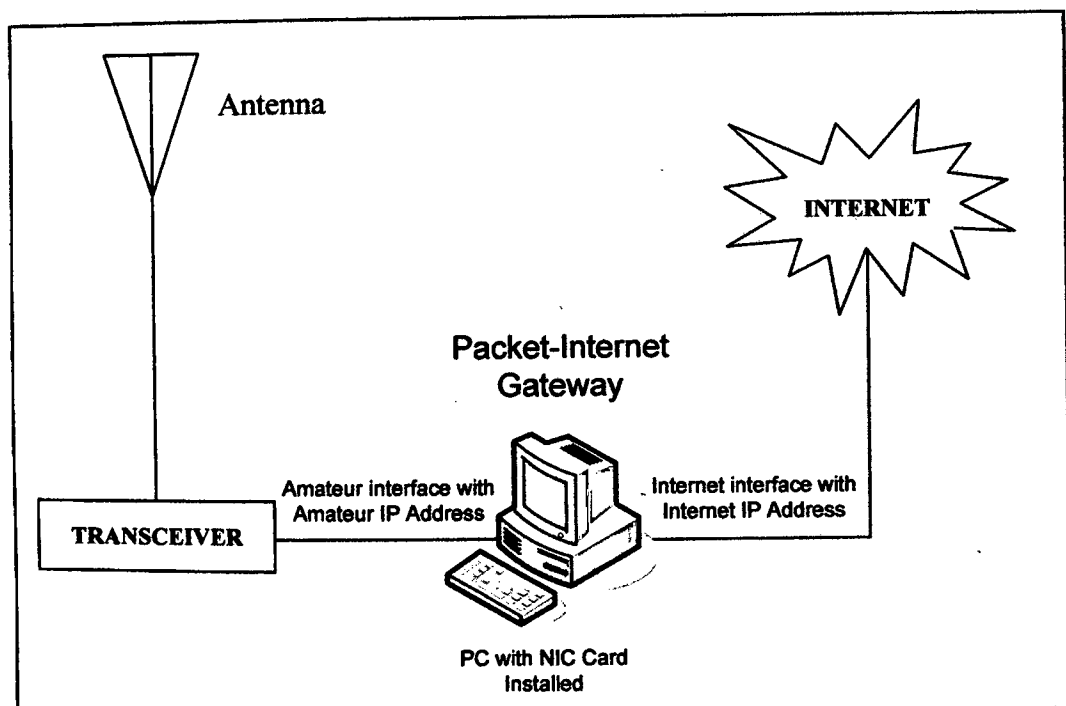


Figure 2.1: Packet-Internet Gateway

/

The gateway is a machine that runs the software that enables it to perform its function. For gateway performance, it is advisable to recommend a computer with at least the performance of a 20MHz IBM AT, A 386SX or DX of course would be better. For file transfer or mail access, a hard disk is needed. Each interface must have a unique IP address, so that both the local amateurs and the other gateways can communicate with it.

The Internet interface's address is assigned by the AARNet/Internet administrator (W.Bauerfeld, 1987) of the institution, and the amateur radio interface's address is assigned by the local amateur IP administrator. Each interface must also have the appropriate hardware needed for it to communicate with its destination. On the amateur radio side, a Terminal Node Controller, a transceiver and an antenna convert the packets from the gateway into radio transmissions that can be received by amateur stations.

On the Internet side, there are two(2) main options an Ethernet card connects the gateway to the local area network, which is part of the AARNet/Internet, or a serial line connects the gateway to another machine in the institution which is on the local area network, and hence is part of the AARNet/Internet. The serial line can run either the SLIP or PPP protocol to communicate with the other machine. That completes the overview of the hardware setup of the gateway.

The gateway and other hardware must be reliable, and be readily available to the maintenance of the gateway to fix unforeseen problems. The gateway must be placed in a physical position to suit both its connection to the AARNet/Internet, and to the TNC/transceiver. The transceiver and antenna must be in a position to satisfy both the needs of the local amateur community. If using Ethernet, the gateway's position must allow it to be physically connected to the local area network.

At an elementary level, the gateway works as follows. Messages are broken up into packets when they are sent over the Internet. When the gateway receives a packet on one interface, it checks the destination IP address in the packet, and according to its table of routes, it retransmits that packet on the interface that will send the packet to its destination.

Even though the global amateur community has been allocated a block of valid Internet addresses, none of the Internet machines in the world know how to send packets to these addresses. The easiest solution would be to advertise the routes to these addresses to all internet machines. The same application is going to apply in access control (AC-Spot) system which requires 2 network interface cards (NIC) or 1 network interface card and 1 Wi-fi Adapter that are Public Network Interface and Private Network interface card also known Amateur IP Address. The following in Figure 2.2 shows that a diagram of hardware setup

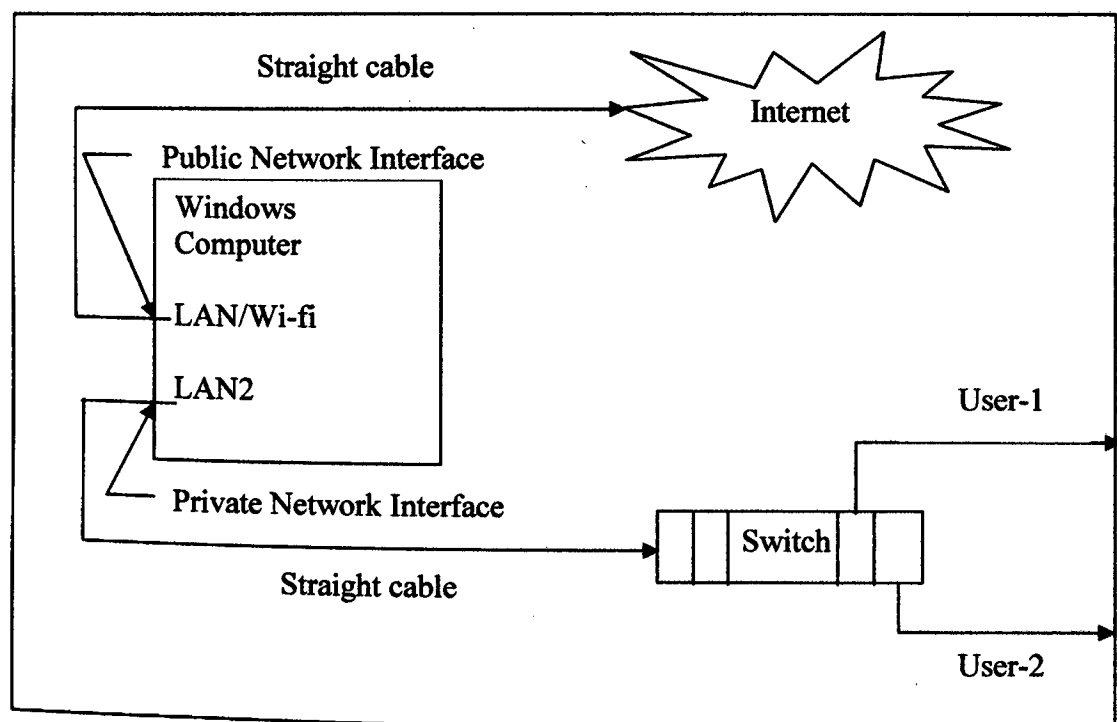


Figure 2.2: Diagram of hardware setup

2.4 Comparison with Current System

2.4.1 Case Study 1: MODENAS

At Motosikal & Enjin Nasional Sdn.Bhd (MODENAS) environment, the company deployed Wired LAN technology which requests the users to enter username and password in order to login the network. By this way, this makes the MODENAS users can safely access the internet. Moreover, the MODENAS Company implemented this kind of access control method to limit users. Only allowed authorized parties to borrowing the internet and prevent the network usage from unauthorized people through the internet. For time being the MODENAS's network using authentication mechanism in order to allow right parties are verified and gain access to the internet. Although the MODENAS network imply authentication login page for users in term of security but the network still has some less security feature. The MODENAS network can be access by anyone if the authorized party forgot to logout and also don't have security feature like connection idle timeout.

2.4.2 Case Study 2: Pennsylvania Deke Kassabian University

Pennsylvania Deke Kassabian University (Deke Kassabian,, 1997) has established some wired networks to limit access based on network hardware addresses or even usernames and passwords. These access controls have generally been used to limit access to a community of users or to support a number of broad information security initiatives. Below are some of these approaches and technologies are discuss regard to the prospects for performing not only access control, but also advanced policy-based networking, following below there are some approaches used to performing access control in Pennsylvania Deke Kassabian University.

i) Network Login

The function of network login is to authenticated network users to access for networks, allowing for subsequent Authorization and Accounting. For example ISC Network Engineering is considering a variety of approaches to network login, including 802.1x port based authentication, (Deke Kassabian,, 1997) Ethernet switch-specific control, and web-intercept authenticating gateways. This term is used in Wired LAN system to make the users are authenticate before browsing the internet.

ii) Network Authorization

The network authorization enables the users or their machine being authenticated to the network first, then a decision on whether service should be provided or not considered. Once the users are successfully authenticated, (Deke Kassabian,, 1997) they can allow to accessing the internet. The access control decisions would then need to be enforced by an element of network infrastructure, such as a switch, a router, an authenticating gateway, or a tunnel endpoint. The same approach use in (AC-Spot) system.

iii) Address Association

Address Association means the address associate to particular websites with known as an IP address. All the web sites address is refer to the IP address. Thus an IP address becomes identification for every websites. Moreover it associating a specific person (such as through the use of a PennName) with a PennNet IP address, for a given moment in time. The activity will generally have only an Internet Protocol address (IP address) as the identifying information. Translating this IP address to the name of a person is not trivial (Deke Kassabian,, 1997), as different people and different computers may be associated with a given IP address at different times. So the usage of address association is implemented in (AC-Spot) system in order captured the IP address which visited by users.