NETWORK ISSUES IN KUKTEM AND SOLUTIONS : DOMAIN

KHAIRUL AFHAM BIN SANI

A report submitted in partial fulfilment
of the requirements for the award
of the degree of
Bachelor of Computer Technology (Computer Systems and Network)

Faculty of Computer System & Software Engineering
University College of Engineering & Technology Malaysia

MARCH, 2005

ABSTRACT

Nowadays, networking has become widespread technology and emerging as one (1) of methods that can connect each of us no matter where you are as long as there has a connection of the network. One (1) way is implementing "Domain" that featured in Windows Server for controlling access of network. Two(2) elements have been identified to take a concern are performance and security. This domain is an alternative way to ease in managing users within an organization. The domain functioned as a controller over the other workstation, which only domain controller will affect through an attack such as viruses that could give benefits to administrator for fixing the problem. The project consists of project requiremnet and analysis,design, experiment and testing phase. The project had been implemented using four (4) Pc as a mini-network environment within FSKKP lab. Two (2) domains are created to show that different domain can be connected each another. After several testing, the Domain project are ready to be bring into our real world because it does not neglect the performance and security terms

ABSTRAK

Pada era siber ini, tidak dapat dinafikan rangkaian ataupun lebih dikenali dengan istilah "network" telah menjadi teknologi yang pesat berkembang dan muncul sebagai salah satu (1) kaedah yang dapat menghubungkan setiap individu tidak kira di mana berada melainkan tiadanya rangkaian di tempat tersebut. Dua (2) elemen iaitu prestasi dan keselamatan harus diambil kira dalam setiap implementasi rangkaian. Satu (1) cara yang sesuai ialah menggunakan "Domain" yang ditawarkan di dalam Windows Server untuk mengawal akses di dalam rangkaian di KUKTEM. Doman bertindak sebagai pengawal dalam keseluruhan rangkaian di mana sekiranya terdapat sebarang masalah atau gangguan hanya ditumpukan kepada pengawal itu sahaja. Projek ini terdiri daripada empat (4) fasa,iaitu keperluan projeck dan analisis, mereka, implementasi dan pengujian. Projek ini mengunakan empat (4) Pc di dalam makmal FSKKP. Dua (2) domain telah dibina bagi menunjukkan bahawa ia dapat dirangkaikan satu sama lain. Setelah menjalani beberapa pengujian didapati Domain ini bersedia untuk diaplikasi dalam dunia sebenar.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF TERMINOLOGY

Network	In information technology, a network is a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks. The most common topology or general configurations of networks include the bus, star, Token Ring, and mesh topologies. Networks can also be characterized in terms of spatial distance as local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs).
Bandwidth	In computer networks, bandwidth is often used as a synonym for data transfer rate - the amount of data that can be carried from one point to another in a given time period (usually a second). This kind of bandwidth is usually expressed in bits (of data) per second (bps). Occasionally, it's expressed as bytes per second (Bps). A modem that works at 57,600 bps has twice the bandwidth of a modem that works at 28,800 bps. In general, a link with a high bandwidth is one that may be able to carry enough information to sustain the succession of images in a video presentation.
WLAN	The WLAN supports network communication over short distances using radio or infrared signals instead of traditional network cabling. WLANs often extend an existing wired local area network.
Wi-Fi	The term Wi-Fi refers a group of industry standards for wireless communication including 802.11b and 802.11g.

SSID	Service set identifier .To communicate with each other, all wireless devices on a WLAN must employ the same SSID
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*. All devices sharing a common part of the IP address are said to be in the same domain.
Packet	A piece of a message transmitted over a packet-switching network. See under packet switching. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called *datagrams.*
MAC Address	Short for Media Access Control address, a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sublayers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.
Server	A computer or device on a network that manages network resources. For example,a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.

Authentication	The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
Ethernet	A local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet supports data rates of 1 gigabit (1,000 megabits) per second.
VPN	(pronounced as separate letters) Short for virtual private network, a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
Switches	In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol.

LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

Network has become an essential part in every part of our life because it can connect each of us without caring about the geography or even the distances. This project reviewed the networking in Kolej Universiti Kejuruteraan Teknologi Malaysia or known as KUKTEM.

Security and performance are the two areas that have to be concerned because of the freedom that networking offers to users can create chances to attacker or intruder access organization such as KUKTEM. KUKTEM has using Gigabit Ethernet and also eleven (11)Mbps wireless through 2.4 GHz. These criteria have been taken heavily to create efficiency in controlling and managing the network within any organization.

Network has evolved from day to day. Even each of transaction is now changing just by using an internet through networking. Performance is defined as amounts to how fast and how far the network is working for the users. For example, how fast does information move to and from personal computer or even to laptop by downloading music easily from the Internet or transfer a file from one computer to another without experiencing a noticeable delay. Other than security, performance is one of the criteria that must be considered for all the time within network.

1.1 Problem Statements

The difficulty of controlling and managing users had been identified as weakness because it can make the network here can be access to anyone. Any users here can be using the network here without an authentication before using the network.

The increasing users within KUKTEM environment each year does make sense to an administrator due to it would make the performance and security degrade. This can happens as not all users are well knowledgeable of maintaining their own personal computer (PC) or laptop that can threaten over this organization.

1.2 Objectives

There is one (1) objective that has been recognized in making this project. Below is the project's objective:

i. To prove domain as an alternative way in controlling network in terms of performance and security.

1.3 Scopes

Below are the project's scopes in making the objectives accomplish:

i. Wired network KUKTEM labs as case study.

ii. Used four (4) computers that installed Windows Advanced Server 2000 operating system.

CHAPTER 2

LITERATURE REVIEWS

The project reviewed the network performance and security within network in KUKTEM. Security of wired network must be considered to implement within the organization but recently the threats over the wired and so far wireless network has given much problem in any organization that implement this technology.

KUKTEM is implementing wired (Gigabit Ethernet) and wireless to support network usage in the hostel. "Wayne Lewis (2003) has stated the familiarity of Ethernet such as easy upgradeable (scalability), support quality of services (QoS) and last but not least is higher bandwidth offered is the reason why Gigabit Ethernet has given an influence to the current network technologies."

2.1 Network Problem in KUKTEM

KUKTEM has implementing eleven (11) Mbps wireless network in their hostel starting at year 2002 and combining with Gigabit Ethernet within staffs' building. The increasing students each year slowly influenced in decreasing the performance because it doe s make sense, the more users also meaning that the more difficult had to deal to maintain the network and to control their usage.

The networking service that has been provided currently gives the problem users are mainly from low connection speed. "There are also several probable causes for the problem such as network congestion, lower rate transmissions, or client configuration issues (Mike Montemurro 2003)."

Second problems that have been identified are the authentication through accessing the network. All users have the same privilege except the administrator and this makes sense for intruder using this chance to penetrate the network because the network itself does not has an authentication to anyone who want to access the network Make it worst fact is that wireless devices that have been deployed within KUKTEM are dangerous to all organizations. "Intruders and hackers will use an anything as a launch pad to break into to an organization's corporate backbone and compromise the integrity of financial data, customer information or even trade secrets. No longer should the security of wireless networks be a peripheral thought (Anil Khatod, 2004)."

2.2 Network Solutions

There are many new technologies out there can be used in enhancing the security and performance of network in KUKTEM. Below are the solutions that have interconnected through the project.

2.2.1 Domain Overview

A domain is Microsoft's terminology for a grouping of NT servers and other LAN manager servers. The key thing to remember about a domain is that administrator can treat a domain of servers as a single unit for management and security purposes. Systems are added to a domain by assigning the domain name to a new system during installation or from an NT server, which is a Backup Domain Controller (BDC) or a Primary Domain Controller (PDC) in the domain.

Domains are really neat because all the servers in the domain share the same user account and security database. Users log in to the domain once and have access to resources throughout the domain. This access makes using and managing a domain much simpler than a network that has several individual servers. There are no multiple servers to manage account and security databases for and no myriad of server names for users to remember.

Domains also segregate the workstations in a network when a user browses the network for file or print resources. All servers and workstations in a domain appear intended under the domain in a browse list.

2.2.1.1 Primary domain controller

The key to the successful implementation of the domain concept is the organization of the servers in the domain. NT servers use one (1) server in each domain to serve as the Primary Domain Controller (PDC). The PDC maintains the master copy of the account and security database. "Currently only NT servers can serve as PDCs, because they are the only servers that fully support trusted domains and other features of the NT server network (Spencer and Goncalves, 1998)."

The PDC is the system that makes all changes to the account and security database. NT server allows administrator to manage the account and security database easily with user manager for domains. User manager for domains allows the administrator to choose which domain to manage by selecting the domain from a list. User manager for domains automatically updates the database on the PDC as changes are made.

In addition to the PDC, any organizations that want to implement this technology should have at least one Backup Domain Controllers (BDC) per domain. "If the PDC becomes unavailable, a BDC can be promoted to primary domain and domain continues to function (Spencer and Goncalves, 1998)". The user account and

security database is copied from the PDC every five minutes to all BDCs in the domain. All other NT server BDCs in the network ask the PDC if any changes to the database have been made. Changes are then sent to each NT server BDC in the network. The entire database is not sent, only changes are sent.

The PDC is a very busy system because of all the tasks that it performs, the larger the network, the busier the PDC. The PDC validates most of the network log-on requests, performing replication of the SAM database, maintaining the browse list for domain resources and attending to other tasks related to the domain.

2.2.1.2 Backup Domain Controllers

Every NT server BDC in a domain can serve as a backup to the PDC by maintaining a copy of the domain database. Any NT server BDC can be promoted to the PDC with the assurance that domain database is no more than five (5) minutes out of date.

The NT server BDC in a domain also improves the performance of the network. Each NT server BDC can process a log-on request by any workstation in the domain. "This capability stated by Spencer and Goncalves (1998) drastically improves the performance of the domain when a large number of users log on the domain at one (1) time for an example in KUKTEM environment, while office hour period."

2.2.1.3 Company that deployed the Domain

Pacific Life is one (1) of North America's most successful financial services companies. Founded in 1868, the company saw explosive growth in the 1990s. Today, Pacific Life provides its corporate and individual customers with an array of

insurance, annuity, asset management, and diversified financial services. The company manages more than $335 billion in assets, and is the largest domiciled California life insurance company and the fourteenth (14th) provider of insurance services in the United States. Pacific Life is the flagship insurance company of Pacific Mutual Holding Company. Below are the details about this company and the affiliates related:

Corporate Headquarters: Newport Beach, CA
Employees: 3,600
Selected Subsidiaries and Affiliates:
Pacific Financial Products, Newport Beach, CA
Mutual Service Corporation, West Palm Beach, FL
M.L. Stern, Beverly Hills, CA
Associated Financial Group, Los Angeles, CA
United Planners, Scottsdale, AZ
Aviation Capital Group, Newport Beach, CA

Pacific Life's implementation of the Windows 2000 platform and the Active Directory service is an excellent example of a successful planning and implementation strategy developed and executed by a lead business unit on behalf of the parent company. By taking the lead on behalf of the enterprise, the Life Insurance division of Pacific Life was able to meet its needs and adopt Active Directory well ahead of its sister business units. "The Life Division's careful design and implementation strategy made it easy for other units to integrate their businesses into the company's enterprise architecture (Microsoft, 2003).

Eventually, the company hopes that the Internet will be a vehicle for direct training and a variety of other offerings. For now, however, the Division provides much of its support through a field organization of over thirty (30) remote offices to provide those agents with support and training services. The Division has been challenged with a variety of security, control, and cost challenges in order to support those field offices.

From a security perspective, the Division needed to support its workers whether they were at a field office, at a client, or located inside headquarters. At the same time, many of the documents involved in the Life Insurance business are highly sensitive and must be secured against unwarranted access. "The Division's architecture needed to set access permissions based on roles, on which the users were not where they were located. From an administrative cost and control basis, the Division's IT team had to track and support a wide variety of resources and users by centralizing some functions, simplifying others and delegating administrative control over still others (Microsoft, 2003)."

2.2.1.4 Reasons on why the company deployed Domain

"The Life Division committed to Active Directory and directory services architecture for number reasons (Microsoft, 2003):"

i. Security

As a practical matter the Life Division wanted to ensure remote access while providing better security. Spread out in offices across the country, the Life Division was interested in providing for a broad, consistent mechanism for determining identities and managing the distributed resources found across Pacific Life's global network. The Division felt that a directory services architecture that was tightly integrated with the management and security functions of the operating system would be better able to guarantee the integrity of the network and the privacy of its users and files.

ii. Cost Effective

The company needed to cut costs. The Division felt that an enterprise architecture centered on directory services would help administrators define and maintain the infrastructure, improve administration and enhance the user experience, and do so at a supportable cost. They saw Active Directory as both a robust repository for information about

network-based elements such as applications, printers, and workers. More importantly they saw it as a consistent way to identify, secure, and manage those resources; as an architecture that would allow those resources to work together as intended and which could do so at a reasonable cost.

iii. Future Planning

In addition, the Division felt that, operationally directory services were an essential element of the functionality of the enterprise environment. Further, they felt that the enterprise and desktop level systems should work together, smoothly and seamlessly, supported by a vendor committed to supporting those systems into the future.

iv. Ease Administration

Pacific Life agents and internal staffers routinely exchange important personal and financial information about their clients as part of their service process. The company wanted to take full advantage of security features in Windows 2000. Active Directory supports policy-based administration. Group policies can determine a user's access to directory objects and resources based on a set of group credentials. Administrators can define groups and security policies and deploy them across the domain or limit them to a specific set of users or individuals

2.2.1.5 Discussion on Deployment and Experimenting

The process of deploying the Domain is not just set up or configuration this or that, because it involved many details and aspect that should be taken. All aspect just should not be burdened to administrator alone. Hence, an organization which wants to deploy the Domain environment suggested establishing a team that consists of IT expertise and guidance from person who understand about Domain..

Pacific Life for an example had formed development team that broken to several teams that functioned differently. Table 2.1 showed the teams and participant for each team:

Table 2.1: Development team of Pacific Life Company

Team Roles	**Team Members**
Product Management	Brad Sherrell, Cameron Cosgrove
Program Management	Matt Hansberger, Darron Inman (MCS)
Development	Tom Lavoie
Directory Service Team	Tom Lavoie, Tim Knoop, John Russell, Steve Robinson, Brad Sherrell, Tim Huckaby
DNS Team	Frank Becera
Base OS Team	Steve Robinson, Russ Deer, Huy Phan, Tom Lavoie
Security Team	John Russell, Tom Lavoie, Matt Hansberger, Robin Fleming, Tim Huckaby
Network Team	John Russell, Frank Becera, Matt Hansberger
Applications Compatibility	Tim Knoop, David Wong, Robin, Jeff Craney, All Workgroup Mgrs., Wendy Davilla, Mike D, Dave Dear, Laura, Jason.
Test/QA	Tim Knoop, Russ Deer
Logistics,User & OperationsEducation	Jeff Craney
Operations Planning	Robin Fleming

(Microsoft, 2003)

There must have explanations on why the company had formed a team which consist many staff instead just assign to one (1) person. The processes of Domain deployment are risky, not an easy part and needs lots of work.