

Kumaraguru College of Technology
Department of Computer Science and Engineering
Coimbatore-641 006



ISO 9001:2000
Certified

MULTIPLEXING A LAN

Project work done at

**GLOBAL SOFTWARE Pvt. Ltd.
CHENNAI.**

P-1079

PROJECT REPORT

Submitted in partial fulfilment of the
Requirements for the award of the degree of
Master of Science in Applied Science

Software Engineering

Bharathiar University, Coimbatore.

Submitted by

SAKTHIVEL.S.M
Reg.No-0037S0100

INTERNAL GUIDE

Mrs. S. Devaki, BE., MS.,
Dept of Computer science & Engineering,
Kumaraguru College of Technology,
Coimbatore.

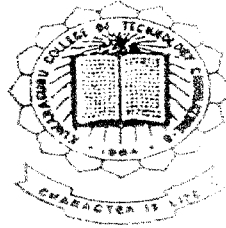
EXTERNAL GUIDE

Mr. Aravind prabhu,
GLOBAL SOFTWARE Pvt. Ltd,
Chennai.

CERTIFICATE

CERTIFICATE

Department of Computer Science and Engineering
Kumaraguru College of Technology
Coimbatore – 641 006



This is to certify that the project work entitled

"MULTIPLEXING A LAN"

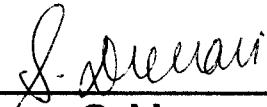
has been submitted by

Mr. S.M. Sakthivel

(Reg.No: 0037S0100)

In partial fulfillment of the award of the degree of
Master of Science in Applied Science – Software Engineering of
Bharathiar University, Coimbatore

During the academic year 2003-2004

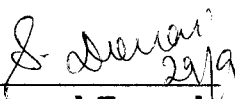


Guide



Head of the Department

Certified that we examined the candidate in the Project Work Viva
Voce Examination held on 29.9.2003.



Internal Examiner



External Examiner

22/10

16/09/03

CERTIFICATE

This is to certify that Mr.sakthivel . S. M. of IV th year Msc
(S/w Engineering) student of Kumaraguru college of
Techonology,Coimbatore, has done his project on "Multiplexing
A LAN" under my guidance during June 2003 to September
2003. We find his project satisfactory

J. Selvamuthukumar

J. Selvamuthukumar
(Deputy – Manager Training)

Aravind Prabh


Aravind Prabhu
(Project Guide)

DECLARATION

DECLARATION

I hereby declare that the project entitled “ *MULTIPLEXING A LAN* ” submitted to **GLOBAL SOFTWARE (p) Ltd , Chennai** in partial fulfillment of the requirements for the award of the degree of Master of Science (Applied Science) Software Engineering, is a record of original work done by me, under the supervision and guidance of **Mr. Aravind Prabhu., GLOBAL SOFTWARE (p) Ltd , Chennai .**

Date:


Signature of the Student

S.M.SAKTHIVEL

Reg No- 0037S0100

ACKNOWLEDGEMENT

ACKNOWLEDGEMENT

I deem it a great pleasure to place my deep sense of gratitude and indebtedness to, **Dr. K. K. Padmanaban, B.Sc.(Engg.), M.Tech., Ph.D., Principal**, Kumaraguru College of Technology for giving me the opportunity to undertake the project work.

I am grateful to, **Dr. S. Thangasamy, Ph.D., Professor and Head of the Department**, Kumaraguru College of Technology, for giving me this golden opportunity to carry out my project work successfully.

My sincere thanks are offered to **Mrs. Devaki, BE, MS.**, for the encouragement and support bestowed on me as my Project Guide. I am very much indebted to her for the suggestions and guidance extended in successfully completing the project.

I thank all my faculties whose diligent efforts have led me to complete the project successfully. I owe my deepest gratitude to **Mr. Selva Muthu Kumar** GLOBAL SOFTWARE LIMITED, for rendering me permission to carry out my project work in the esteemed concern.

My sincere thanks to **Mr. Aravind prabhu**, GLOBAL SOFTWARE LIMITED, my project guide for his valuable guidance, timely suggestions and constant assistance in time of need.

I wish to express my sincere thanks to the people who have contributed a lot towards the successful completion of this project work.

SYNOPSIS

SYNOPSIS

The project “Multiplexing a LAN” deals with windows 2000 networking and implementation. An Office Environment of the latest trends needs to have quiet interesting challenges & features. Those Features have to be considered all along way from planning, designing, Implementation and Training. In this project we have an Ideal Office and proceed the same in all the phases of Networking i.e. Planning, Implementation, Maintenance and Supporting using windows 2000 & its components.

The project mainly deals with the networking, so our challenge is to shifting the machines at employees Interest. Participating network wherever thy inside the office building. Connectivity between the branch office and the corporate office. All the Employees want their Quota of Hard disk storage/usage. The main challenge is to provide security in all stages.

CONTENTS	PAGE NO
1. INTRODUCTION	
1.1 Project Overview	2
1.2 Organization Profile	5
2. SYSTEM STUDY	
2.1 Existing System.....	9
2.2 Proposed System.....	11
2.3 Requirements of a new System.....	12
2.4 User Characteristics.....	12
3. REQUIREMENT SPECIFICATIONS	
3.1 Functional Requirements.....	14
3.2 Non-Functional Requirements.....	15
Interface Requirements.....	15
4. SYSTEM DESCRIPTION.....	17
5. NETWORK DESIGN	
5.1 Existing System.....	24
5.2 New System.....	25
6. CONFIGURATION	
6.1 DHCP Configuration.....	27
6.2 DNS Configuration.....	30
6.3 WINS configuration.....	31
6.4 RRAS configuration.....	33

7. TESTING & IMPLEMENTATION	
7.1 Problems Faced.....	38
7.2 Lessons Learnt.....	38
8. FUTURE ENHANCEMENT	40
9. BIBLIOGRAPHY.....	42
10 APPENDIXES.....	43

INTRODUCTION

1. INTRODUCTION

1.1 OVERVIEW OF THE PROJECT:

The project deals with planning and designing office LAN using windows 2000 components and then testing and monitoring the network by use of the software.

The project mainly deals naming and numbering the machine .connectivity between the branch office and corporate office, internet sharing, remote access is using the components provided by windows 2000 server/advanced server.

Scope of the Project:

While analyzing the scope of the network design, the main reference is given to the CISCO proprietary model to specify the types of functionality the new network design must address.

In addition to this, the following terms also define the scope of the network and project.

SEGMENT: A single network based on a particular layer protocol. It may include hubs, repeaters & multi station-access units.

LAN: A set of bridged or switched segments usually based on a particular layer-2 protocol. It may have one or more layer-3 protocols associated with it.

REMOTE ACCESS: Dial in/dial out solutions which are either analog or digital.

WAN: A geographical dispersed network including point-point, frame relay and other long distance connections.

VPN: The Routing and Remote Access service in Windows 2000 Server provides virtual private network (VPN) services for remote access and router-to-router VPN connections by using either the Point-to-Point Tunneling Protocol (PPTP) or the Layer Two Tunneling Protocol (L2TP) with Internet Protocol security (IPSec).

WINS: Windows Internet Name Service (WINS) provides a dynamic replicated database service that can register and resolve NetBIOS names to IP addresses used on your network.

1.2 ORGANIZATION PROFILE:

Global software limited (GSL) is promoted by an industrial group in the IT area. It is a technology focused multinational company that focuses on contemporary ESM solutions anchored by quality.

With a world class research and development center for operating systems, databases, networks and enterprise security, GSL provides ESM solutions from min-size to large organizations, portals and ISPs.

The company has offices in US, UK, Singapore, Mauritius and India with 150 experienced ESM professionals. It is backed by core technology teams with 100+ many years of experience in systems software and networking technologies.

Global Software Ltd, India, is a backend system integration company, focusing on enterprise systems management,(ESM).The company has excellent resources to offer the entire range of backend systems integration services in IT with specialization in the following areas.

- ¢ Managed services.
- ¢ Operating system services
- ¢ Network services
- ¢ ESM solution consulting

Our company is unique with 100% certified, thoroughly experienced, highly qualified professionals offering tangible, scalable ESM solutions to achieve increase in service deliverables: sound knowledge and vast experience to handle heterogeneous complexity of multiple systems.

With its unique competency center Globe's competency center-hardware and software global continually update the competency center in line with market changes. The ESM competency in center in Chennai is a true world -class infrastructure with state-of -the-art equipments. The company has high-speed links to internet and to all its world wide offices. The links can be extended to the client's location for off shore support/remote management there by providing cost effective solutions.

GSL is an IBM/Tivoli business partner, Microsoft certified solution provider and authorized parametric testing center.

Hardware:

The following are the wide range of hardware available at GLOBAL in India.

- " IBM S/390 Enterprise Server
- " IBM RS/6000 SSP @ Enterprise Server with SAN
- " Sun Enterprise Server -3500 Series
- " IBM Infinity 5500 Servers
- " CISCO Routers and Switches

Software:

The software platform includes:

- " Operating Systems: IBM OS/390, IBM AIX, Sun Solaris, HP-UX, True Unix and Windows NT
- " Database Management: IBM DB2, IBM UDB, Oracle, Sybase, SQL
- " Storage Management: IBM ADSM/TSM, Veritas, Legato And Solstice Disk Suite
- " System Management: IBM Tivoli, CA Unicenter TNG, BMC Patrol
- " Network Management: IBM Net view CISCO Works 2000 and HP-view

SYSTEM STUDY

2. SYSTEM STUDY

2.1 EXISTING SYSTEM:

Head Office	totally contains
Department	number of hosts
Human Resource	6
Administration	150
Finance & Marketing	30
Server systems	5

In the existing system hubs are used for connectivity between the departments. Hubs are connected to a backbone cable. Network is a star topology.

Drawbacks of the existing Network:

- ¢ This network is not having any of the latest Standards

- ¢ Security becomes a challenging issue when connecting to the branch office & Internet.

- ¢ Internet Access to all the desktops is not effectively monitored & rationed.
The existing network is based on a star topology, when hubs fail, that particular sub network will go flat.

- ¢ The server is mainly configured with the windows NT Operating Systems.

- ¢ The Client operating systems includes windows 95 & windows 98 , so stability becomes a challenge

2.2 PROPOSED SYSTEM / NETWORK:

Windows 2000 Operating System is the best of the currently available from the Microsoft family of products. As Microsoft is famous for its easiness & Convenient Nature, we decide to go for this windows 2000 network.

Functionally wise the windows 2000 server & windows 2000 Advance Server operating systems are more robust & Secure than the windows Nt Networks.

The Scalability is also the best when, we want to support the symmetric multiprocessing systems (with more cpu's)

The Domain Controllers are much more stable because, Here, these domain Controllers are using the workgroup sort of model w.r.t the windows Nt's client-server model.

Here, we selected to go for the

1. Single Domain Model with a single Name space, Consists of two Domain Controllers for supporting the entire client Operating Systems.
2. DNS & DHCP integrated with our existing Domain Name Space.
3. WINS for the older version of windows.
4. RAS Supported for the Branch office Connectivity
5. NAT for the internet Connection Sharing purpose.

The Client Operating systems are selected as the windows 2000 Professional Operating Systems.

2.3 REQUIREMENTS FOR THE PROPOSED SYSTEM

When we upgrade for the windows 2000 server environment. We will reach the maximum benefits. For connecting to the branch office we can make use of the VPN Network. The Latest Security Protocols like l2tp & IPSec can be implemented nicely on the windows 2000 environment.

2.4 USER CHARACTERISTICS

The End-user will feel that, the network is in good speed & Compatible. Because of the Roaming Profile implemented in our network, he will be able to get the same desktop as he expects from any of the machines. The Internet access from any of the Computers can be done & is also in good speed. The connecting procedure for the remote office is simple & easy to use.

Operating System Constraints:

When connecting to internet access, The Nat has to be implemented in the Cisco devices. When expanding to various sites, we do want to have some good wan connectivity. This operating system needs to be updated with the latest security patches every now and then. The service pack releases & the windows Updates has to be done periodically.

REQUIREMENT **SPCIFICATIONS**

3. REQUIREMENTS SPECIFICATION

3.1 FUNCTIONAL REQUIREMENT

Hardware specification:

PROCESSOR : INTEL PENTIUM III 733 MHZ

RAM : 64 MB

FDD : 1.44 MB

HARD DISK : 20 GB

MONITOR : 14"COLOUR MONITOR

KEY BOARD : 101/102 KEYS

For the Client Operating System called as “Windows 2000 Professional”

PROCESSOR : INTEL PENTIUM III 733 MHZ

RAM : 128 MB

FDD : 1.44 MB

HARD DISK : 20 GB

MONITOR : 14"COLOUR MONITOR

KEY BOARD : 101/102 KEYS

USB PORTS : for modems

For the Server Operating System called as “Windows 2000 Server /
Advanced Server”

Software Specification:

OPERATING SYSTEM : Ms WINDOWS 2000 Professional & Server/Advanced
Server.

MS- Office packages for all the Client Operating Systems.

Any of the Customized Software's as needed for the organization.

3.2 Non Functional Requirements:

Interface Requirements:

Network interface card

Modems:

DAX -56K

Dlink-56K

Cables:

Cat -10 base 2

Cat -10 base 5

Fast Ethernet -100 base 5

SYSTEM DESCRIPTION

4. SYSTEM DESCRIPTION

MODULES:

- ¢ System Analysis

- ¢ Network Design

- ¢ Configuration

- ¢ Testing & Maintenance

Analysis:

This module involves analysis of existing network. Based on the results of this analysis phase new network is built such that it has less traffic than the existing network. The disadvantages that are indicated by the analysis phase will pave way to analyze and arrange the new network. Analysis phase also considers cost factors of the old network.

Network Design:

This phase involves designing of the new network which has less traffic when compared to the old network. Network is designed such that there is a provision for extending the network as desired without affecting the network

traffic, so the final network is one which has effective traffic management mechanism for every department in the company.

Configuration:

In this phase network devices like the dhcp,rras,dns,wins and the Nat are configured and their startup configuration coding are written in their memory in order to enable them at startup.

DHCP configuration

Every switch has unique configuration screen, so as per the requirement of the different dhcp the configuration is made.

DNS configuration

The Domain Name System (DNS) is an Internet and TCP/IP standard name service. The DNS service enables client computers on your network to register and resolve DNS domain names. These names are used to find and access resources offered by other computers on your network or other networks, such as the Internet. It has unique configuration screen

WINS configuration

Windows 2000 Server provides WINS, which enables the server computer to act as a NetBIOS name server and register and resolve names for WINS-enabled client computers on your network as described in the NetBIOS over TCP/IP standards.

Router and Remote access configuration

All routers follow the same method of configuration. Only commands with respect to certain serial/Ethernet interfaces may change as per the requirement of the routers.

Testing and Maintenance:

This Module Performs the maintenance of the entire new network based on the traffic show by the network monitoring software.

Testing of the entire network is performed by using the router's and switches built-in commands. In testing there are provisions available in the network monitoring

Software to test whether a particular host is in connection with this system or not and test the gateway of the host.

Windows 2000 Servers:

Windows 2000 Advanced Server includes all the new features of Windows 2000 Server, and in addition offers enhanced memory support, support for additional processors, and clustering. Enhanced memory and processor support means your server applications can run faster, providing better response for users on the network. Now Clustering includes multiple clustering technologies: Network Load Balancing clusters and server clusters. You can set up these clustering technologies to work together to provide scalability and high availability for network applications.

Network Load Balancing clusters provide high scalability and availability for TCP/IP-based services and applications by combining up to 32 servers running Windows 2000 Advanced Server into a single cluster. The Network Load

Balancing service provides a foundation for Network Load Balancing clusters .work Load Balancing clusters can also provide load balancing for servers running COM+ applications .Server clusters provide high availability for applications through the failover of resources on servers running Windows 2000 Advanced Server. The Cluster service provides a foundation for server clusters. It is easy to maintaining the users and groups account

SYSTEM ANALYSIS

This network is not having any of the latest Standards. Security becomes a challenging issue when connecting to the branch office & Internet. Internet Access to all the desktops is not effectively monitored & rationed. The existing network is based on a star topology, when hubs fail, that particular sub network will go flat. The server is mainly configured with the windows NT Operating Systems. The Client operating systems includes windows 95 & windows 98 , so stability becomes a challenge

Windows 2000 Operating System is the best of the currently available from the Microsoft family of products. As Microsoft is famous for its easiness & Convenient Nature, we decide to go for this windows 2000 network

Functionally wise the windows 2000 server & windows 2000 Advance Server operating systems are more robust & Secure than the windows Nt Networks.

The Scalability is also the best when, we want to support the symmetric multiprocessing systems (with more cpu's)

The Domain Controllers are much more stable because, Here, these domain Controllers are using the workgroup sort of model w.r.to the windows NT's client-server model.

Here, we selected to go for the

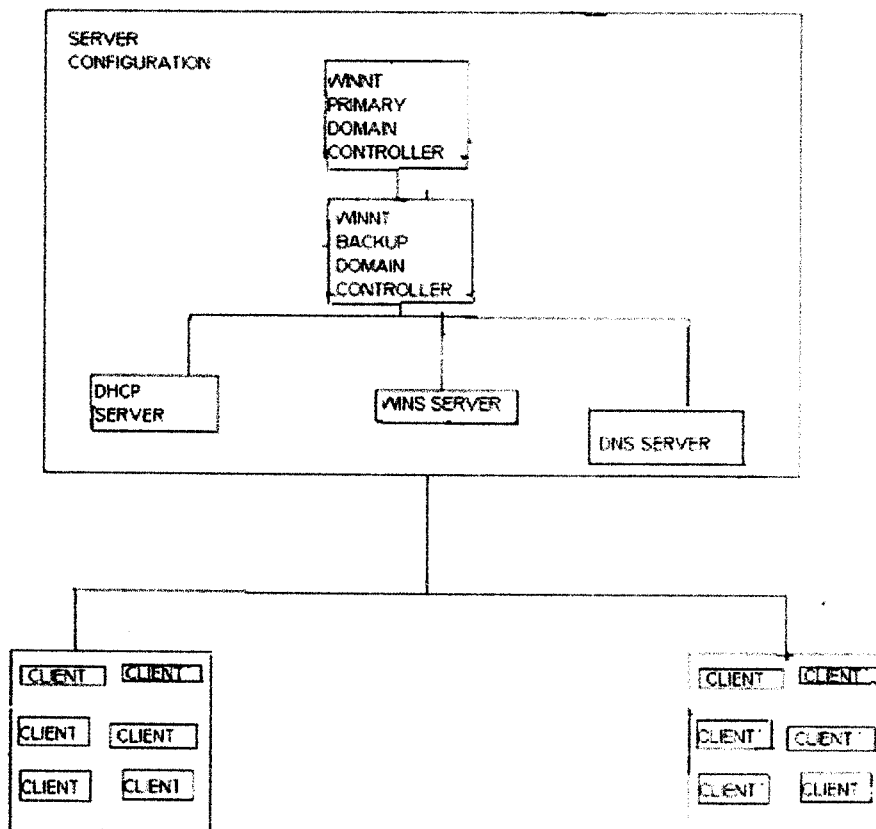
1. Single Domain Model with a single Name space, Consists of two Domains
2. Controllers for supporting all the client Operating Systems.
3. DNS & DHCP integrated with our existing Domain Name Space.

4. WINS for the older version of windows.
5. RAS Supported for the Branch office Connectivity
6. NAT for the internet Connection Sharing purpose.

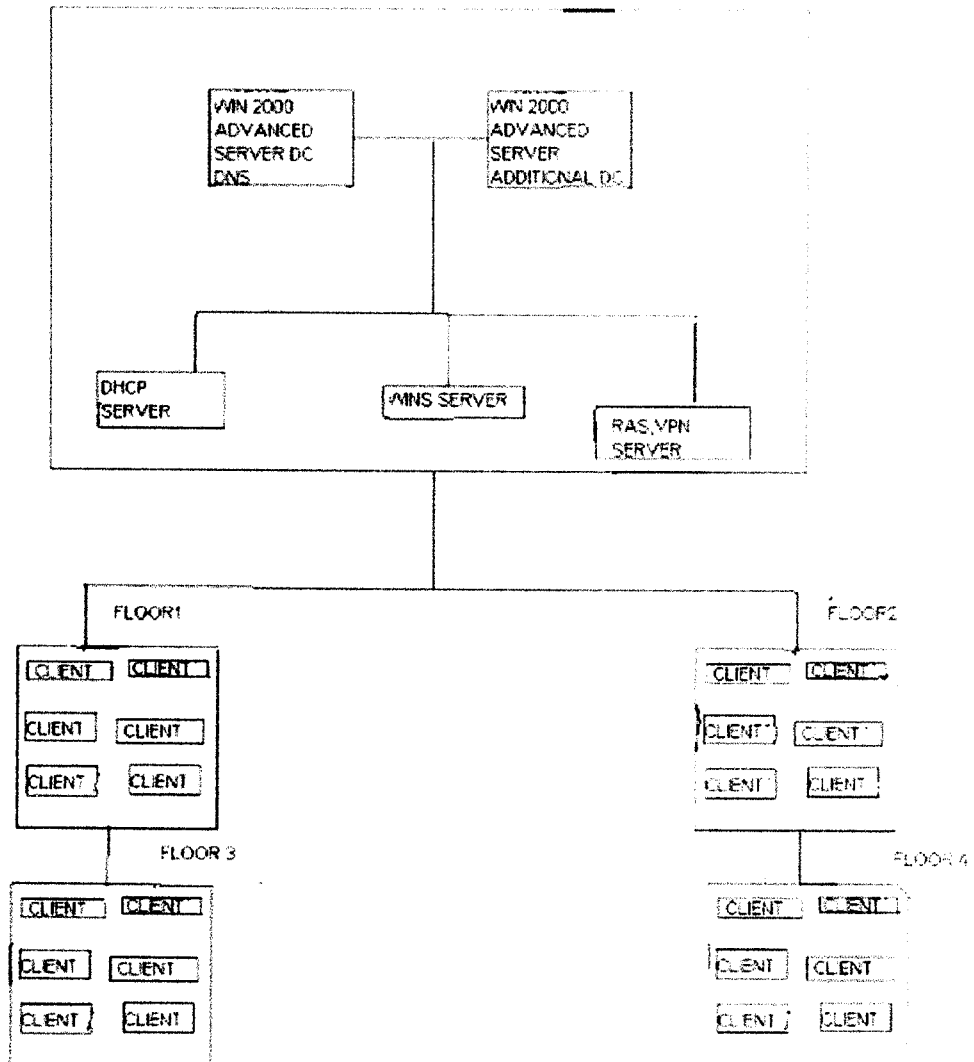
NETWORK DESIGN

5. NETWORK DESIGN

5.1 NETWORK DESIGN -EXISTING SYSTEM



5.2 NETWORK DESIGN -NEW SYSTEM



CONFIGURATION

6. CONFIGURATION

6.1 DHCP CONFIGURATION:

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard designed to reduce the complexity of administering address configurations by using a server computer to centrally manage IP addresses and other related configuration details used on your network. Windows 2000 Server provides the DHCP service, which enables the server computer to perform as a DHCP server and configure DHCP-enabled client computers on your network as described in the current DHCP draft standard.

SCOPE:

A scope is the full consecutive range of possible IP addresses for a network. Scopes typically define a single physical subnet on our network to which DHCP services are offered. Scopes also provide the primary way for the server to manage distribution and assignment of IP addresses and any related configuration parameters to clients on the network.

SUPERSCOPE

A *super scope* is an administrative grouping of scopes that can be used to support multiple logical IP subnets on the same physical subnet. Super scopes only contain a list of *member scopes* or *child scopes* that can be activated together. Super scopes are not used to configure other details about scope usage. For configuring most properties used within a super scope.

EXCLUSION RANGE

An *exclusion range* is a limited sequence of IP addresses within a scope, excluded from DHCP service offerings. Exclusion ranges assure that any addresses in these ranges are not offered by the server to DHCP clients on our network.

ADDRESS LEASE

A *lease* is a length of time that a DHCP server specifies, during which a client computer can use an assigned IP address. When a lease is made to a client, the lease is *active*. Before the lease expires, the client typically needs to renew its address lease assignment with the server. A lease becomes *inactive* when it expires or is deleted at the server. The duration for a lease determines when it will expire and how often the client needs to renew it with the server.

OPTION TYPE

Option types are other client configuration parameters a DHCP server can assign when serving leases to DHCP clients. For example, some commonly used options include IP addresses for default gateways (routers), WINS servers, and DNS servers. Typically, these option types are enabled and configured for each scope. The DHCP console also permits you to configure default option types that are used by all scopes added and configured at the server. Most options are predefined through RFC 2132, but you can use the DHCP console to define and add custom option types if needed.

OPTION CLASSES

An *options class* is a way for the server to further manage option types provided to clients. When an options class is added to the server, clients of that class can be provided class-specific option types for their configuration. For Windows 2000, client computers can also specify a class ID when communicating with the server. For earlier DHCP clients that do not support the class ID process, the server can be configured with default classes to use instead when placing clients in a class. Options classes can be of two types: vendor classes and user classes.

6.2 DNS CONFIGURATION:

The Domain Name System (DNS) is an Internet and TCP/IP standard name service. The DNS service enables client computers on your network to register and resolve DNS domain names. These names are used to find and access resources offered by other computers on your network or other networks, such as the Internet. DNS is an abbreviation for Domain Name System, a system for naming computers and network services that is organized into a hierarchy of domains. DNS naming is used in TCP/IP networks, such as the Internet, to locate computers and services through user-friendly names. When a user enters a DNS name in an application, DNS services can resolve the name to other information associated with the name, such as an IP address. After you install a DNS server, you can use the DNS console to perform these basic administrative server tasks:

1. Performing initial configuration of a new DNS server.
2. Connecting to and managing a local DNS server on the same computer, or remote DNS servers on other computers.
3. Adding and removing forward and reverse lookup zones as needed.
4. Adding, removing, and updating resource records in zones.
5. Modifying how zones are stored and replicated between servers.
6. Modifying how servers process queries and handle dynamic updates.
7. Modifying security for specific zones or resource records.

6.3 WINS CONFIGURATION:

Windows Internet Name Service (WINS) provides a dynamic replicated database service that can register and resolve NetBIOS names to IP addresses used on your network. Windows 2000 Server provides WINS, which enables the server computer to act as a NetBIOS name server and register and resolve names for WINS-enabled client computers on our network as described in the NetBIOS over TCP/IP standards.

IP SECURITY:

IPSec policies can be applied to local computers, domain members, domains, organizational units, or any Group Policy object in Active Directory. Our organization's IPSec policies should be based on your organization's written guidelines for secure operations. Policies may store multiple security actions, called *rules*, so that one policy may be applied to multiple computers.

Internet Protocol Security Policy Management

Internet Protocol Security Policy Management is used to create and configure IPSec policies through the Microsoft Management Console (MMC). It can manage policy centrally (for Active Directory clients), manage policy locally (the computer on which you are running the snap-in), or manage policy remotely for a computer or domain.

You must add the snap-in to the MMC. A wizard guides you through the correct snap-in configuration. The customized console can then be saved so that it is available to you again at any time.

- IPsec policies that are applied to domain policy will override the local, active IPsec policy when that computer is a member of the domain.
- IPsec policies that are assigned to organizational units in Active Directory will override domain level policy for any members of that organization unit, and the lowest-level organizational unit IPsec policy will override IPsec policy for
- higher-level organizational units for any members of that organizational unit, not merge with them.
- Assigning policies at the highest possible level provides the greatest breadth of effect with the least amount of administrative effort.
- IPsec policy will remain active even after the Group Policy object to which it is assigned has been deleted. You must unassign the IPsec policy before you delete the policy object. If you delete the policy objects and keep the policy assigned, the IPsec Policy Agent will assume it simply cannot find the policy and use a cached copy.
- Backup and restore of Group Policy in Active Directory must also include IPsec policies to ensure consistency.

The IPsec Policy Agent only checks Active Directory for updates to the *active* or *assigned* IPsec policy. If *new* IPsec policies have been created in Active

Directory, or an IPSec policy has been changed and assigned to a client computer, the Winlogon service will discover these changes during its next polling cycle for Group Policy changes, it will notify the IPSec Policy Agent, and then the changes will be applied to the client computer.

6.4 ROUTING AND REMOTE ACCESS

ROUTING

Microsoft Windows 2000 Server routing provides multi protocol LAN-to-LAN, LAN-to-WAN, virtual private network (VPN), and network address translation (NAT) routing services. Windows 2000 Server routing is intended for use by system administrators who are already familiar with routing protocols and services, and routable protocols such as TCP/IP, IPX, and AppleTalk. An advantage of the Routing and Remote Access service is integration with the Windows 2000 Server operating system. The Routing and Remote Access service delivers many cost-saving features and works with a wide variety of hardware platforms and hundreds of network adapters. The Routing and Remote Access service is extensible with application programming interfaces (APIs) that developers can use to create custom networking solutions and those new vendors can use to participate in the growing business of open internetworking.

REMOTE ACCESS

The remote access feature of Microsoft Windows 2000 Server enables remote or mobile workers who use dial-up communication links to access corporate networks as if they were directly connected. Remote access also provides virtual private network (VPN) services so that users can access corporate networks over the Internet. Windows 2000 Server remote access, part of the integrated Routing and Remote Access service, connects remote or mobile workers to organization networks. Remote users can work as if their computers are physically connected to the network.

Users run remote access software and initiate a connection to the remote access server. The remote access server, which is a computer running Windows 2000 Server and the Routing and Remote Access service, authenticates users and services sessions until terminated by the user or network administrator. All services typically available to a LAN-connected user (including file and print sharing, Web server access, and messaging) are enabled by means of the remote access connection.

TESTING AND IMPLEMENTATION



7. TESTING AND IMPLEMENTATION

TESTING:

The system entitled "Network Monitoring" has been thoroughly tested and found to have successfully passed all the tests. The system has been tested with every kind of data. The sequence flow of data has been altered and checked for. In case of extremity error messages has been generated.

The system has been tested for efficiency and has been found satisfactory. It has been implemented in parallel with the existing system and found to perform in a superior manner in both terms of speed and efficiency. In this system all the activities have to be very reliable and the system should have a high degree of accuracy, so efficient and effective working of this system is a must and this is checked using the following tests.

Unit testing:

Verification effort on the smallest unit of software design-module is termed as unit testing.

- ¢ Test cases are given for testing against requirements of the unit being tested. Test cases for path or branch coverage.
- ¢ Test cases for data-flow.

Validation testing:

It can be defined in many ways, but a simple definition is that validation succeeds when the software functions in the manner that is expected by the customer. This is achieved by a series of tests that demonstrates conformity with requirements. After validation tests have been conducted one of the following conditions exists.

- € The function or performance characteristics confirm that it is as expected.
- € The validation from the specification is uncovered and a deficiency created.

Deviation or errors discovered at this stage are corrected prior to the completion of the project with the help of the user by negotiating to establish a method for resolving deficiencies. Thus the proposed system has been tested by using validation testing and is found to be working satisfactorily.

IMPLEMENTATION:

7.1 Problems Faced:

- € Manually assigning the ip address
- € Format of the dhcp table information was vague.
- € Hop count and broadcast count determination was difficult.

7.2 Lessons Learnt:

- € DHCP information from the router is read by the usage of commands.
- € Hop count and broadcast count determination for a WAN node could be calculated by counting the counts of each LAN and by summing them up.

FUTURE ENHANCEMENT

8. FUTURE ENHANCEMENT

Plans:

- Usage of protocols like DHCP can be implemented.
- ISDN backup can be used for failure.
- New clients can be easily added.
- Network can be easily expanded.
- MAC address can be easily modified.

BIBLIOGRAPHY

BOOKS

- Dino Esposito, **MS Press book - II nd Edition**, Addison – Wesley pub. co., Year 1994
- Matthew Gibbs , **Network Infrastructure** , BPB Publications , Year 1998
- Russell Jones , **Network Associate Study Guide** , Shroff Publishers & Distributors , Year 1999
- Richard Anderson , **Microsoft Win 2000 Networking** , Shroff Publishers & Distributors Pvt. Ltd , Year 1996

WEBSITES

www.microsoft.com

www.Networkstudy.com

9. BIBLIOGRAPHY

References:

Books:

MS PRESS BOOK- Microsoft Systems Inc

NETWORK INFRASTRUCTURE- Microsoft Systems Inc.

NETWORK ASSOCIATE STUDY GUIDE

CCNA VIRTUAL LAB EDITION

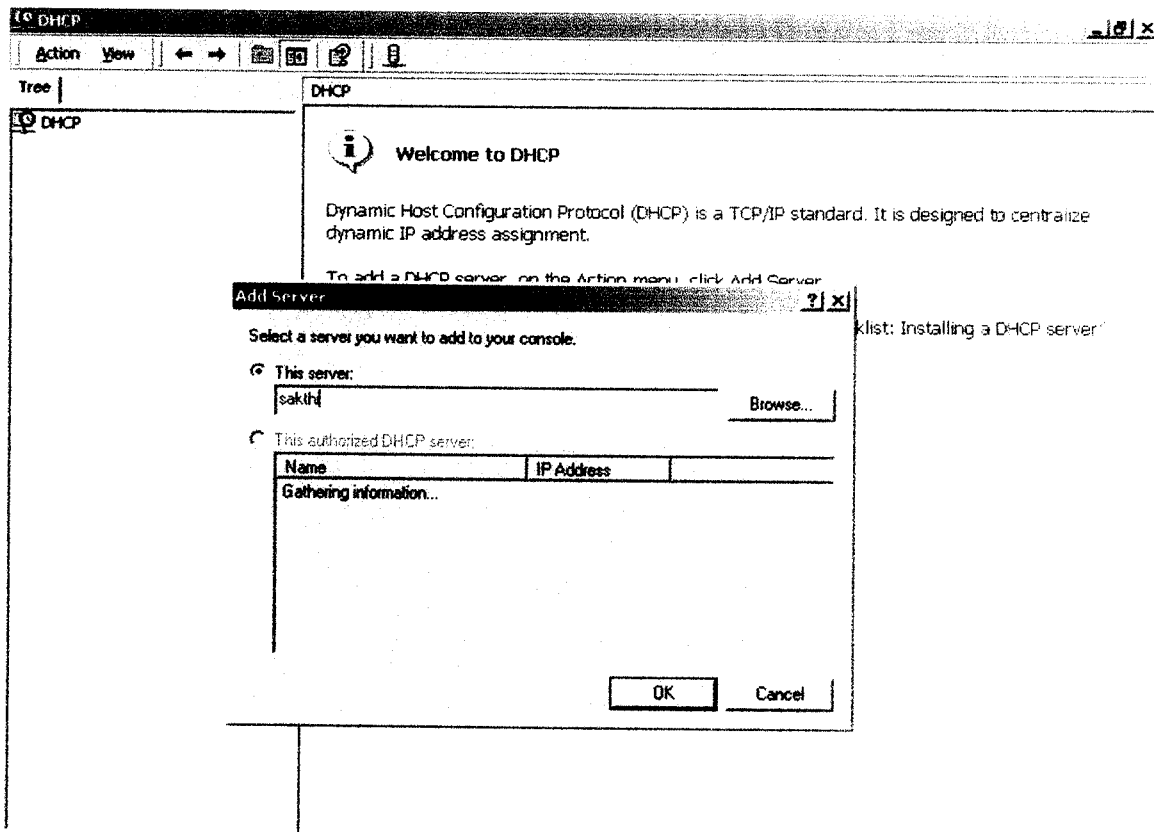
IMPLEMENT AND ADMINISTER SECURITY IN WINDOWS-2000

MICROSOFT WIN 2000 NETWORKING CERTIFICATION

Website:

www.microsoft.com

APPENDIX



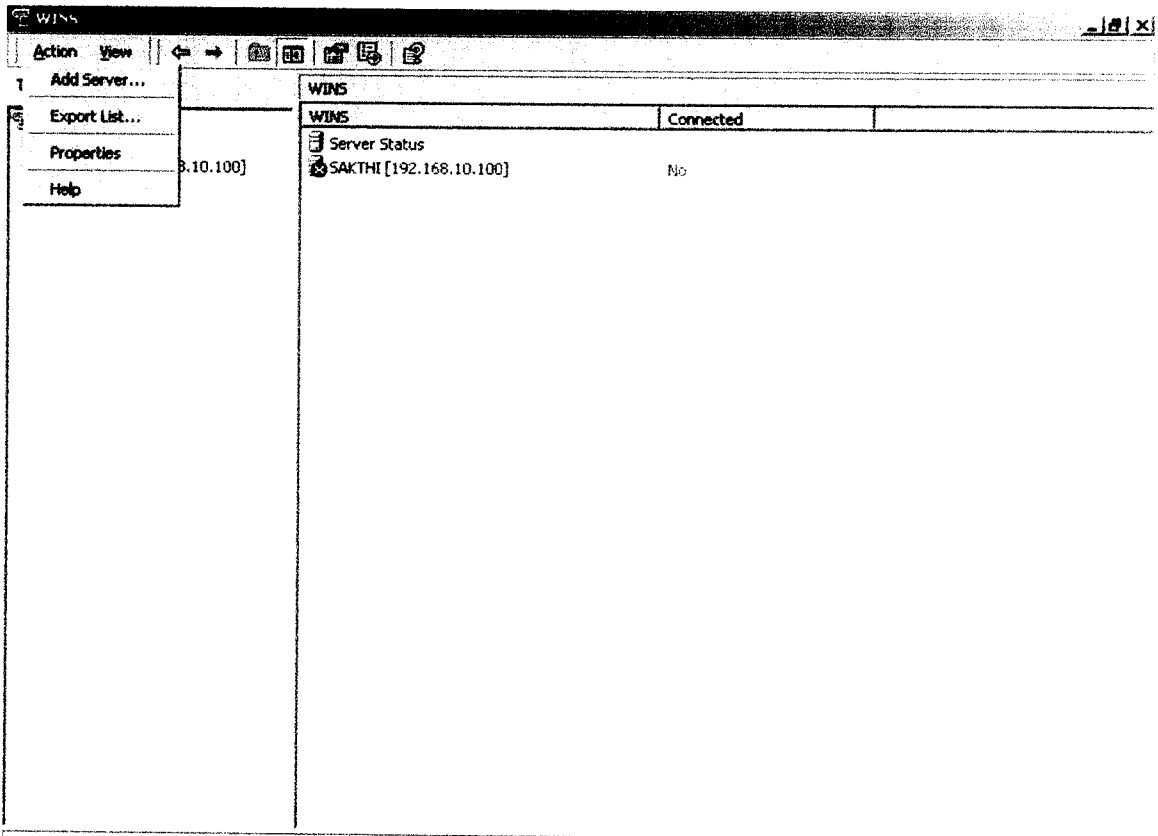
Domain Security Policy

Action View

Tree

- Windows Settings
 - Security Settings
 - Account Policies
 - Password Polik
 - Account Lock
 - Kerberos Polik
 - Local Policies
 - Event Log
 - Restricted Groups
 - System Services
 - Registry
 - File System
 - Public Key Policies
 - Encrypted Dal
 - Automatic Cer
 - Trusted Root
 - Enterprise Tru
 - IP Security Policies

Name /	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No



Routing and Remote Access

Action View

Tree

- Routing and Remote Access
 - Server Status
 - SAKTHI (local)
 - Routing Interfaces
 - Ports
 - Remote Access Client:
 - IP Routing
 - Remote Access Policie
 - Remote Access Loggri

Name	Device	Comment	Status
WAN Miniport (PPTP) (VPN2-4)	VPN		Inactive
WAN Miniport (PPTP) (VPN2-3)	VPN		Inactive
WAN Miniport (PPTP) (VPN2-2)	VPN		Inactive
WAN Miniport (PPTP) (VPN2-1)	VPN		Inactive
WAN Miniport (PPTP) (VPN2-0)	VPN		Inactive
WAN Miniport (L2TP) (VPN1-4)	VPN		Inactive
WAN Miniport (L2TP) (VPN1-3)	VPN		Inactive
WAN Miniport (L2TP) (VPN1-2)	VPN		Inactive
WAN Miniport (L2TP) (VPN1-1)	VPN		Inactive
WAN Miniport (L2TP) (VPN1-0)	VPN		Inactive
Direct Parallel (LPT1)	PARALLEL		Inactive

Routing and Remote Access

Action View

Tree

- Routing and Remote Access
 - Server Status
 - SAKTHI (local)
 - Routing Interfaces
 - Ports
 - Remote Access Client:
 - IP Routing
 - Remote Access Policies
 - Remote Access Logging

Remote Access Policies

Name	Order
Allow access if dial-in permission is enabled	1

Add Remote Access Policy

Policy Name
Specify a friendly name for the policy.

A Remote Access Policy is a set of actions which can be applied to a group of users meeting certain conditions.

Analogous to rules you can apply to incoming mail in an e-mail application, you can specify a set of conditions that must be matched for the Remote Access Policy to apply. You can then specify actions to be taken when the conditions are met.

Policy friendly name:
win

< Back Next > Car