IT Network Lab Upgrade

By

William H Weed

Submitted to
The Faculty of the Information Engineering Technology Program
In Partial Fulfillment of the Requirements for
The Degree of Bachelor of Science
In Information Engineering Technology

University of Cincinnati
College of Applied Science

December 2006

IT Network Lab Upgrade

By

William H Weed

Submitted to
The Faculty of the Information Engineering Technology Program
In Partial Fulfillment of the Requirements
For
The Degree of Bachelor of Science
In Information Engineering Technology

William H Weed	Date 12/13/06
Professor Mark Stockman, Faculty Advisor	Date 12/14/06
Dr. Hazem Said, Department Head	Date 12/14/06

Acknowledgements

I would like to give thanks to Professor Mark Stockman for his patience during the completion of this project. I would also like to give thanks to Professors John Nyland and Russ McMahon for suggesting the idea for the project. I would also like to give thanks to the numerous people who supported me in this effort. The list is long.

Table of Contents

Table of Contents

List of Figures

Abstract

The Network Computer Lab is an "isolated" computer network environment behind a firewall that provides educational services for the faculty and students in the Information Technology program at the University of Cincinnati. The users of the lab are able to create and test computer systems configurations with various network services on a live network, or virtually, without disrupting the production network of the University of Cincinnati while still maintaining connection to outside services. The lab was designed and built using "Best Practices" for a medium-sized business network and the underlying infrastructure services.

The lab environment allows for the exploration of network and computer services from individual workstation systems management to domain level enterprise management. Investigation of heterogeneous integration of disparate systems is encouraged within this environment. All levels of student expertise in information technology may be serviced by the Network Computer Lab.

The lab was designed and built with the expectations of growth in information technology. Future needs and considerations will be accommodated by the baseline design of the lab using current "Best Practices". The model design of this laboratory virtual environment may be exported to other educational disciplines.

IT Network Lab Upgrade

1. Statement of the Problem

The Department if Information Technology at the College of Applied Science, University of Cincinnati maintains and utilizes a Network Computer Lab in the Science Building on the Victory Parkway campus. The room is used to demonstrate and instruct students in the design and operation of systems administration and network administration in the field of information technology. The majority of work performed in the lab is done virtually through the use of emulation software. System and network emulation software allows multiple virtual instances to be created on a single computer in order to simulate enterprise network services and functionality.

The lab was initially set up as a temporary accommodation in room Science 302 and "patched" together with available equipment. The faculty and staff of the department would like the room upgraded to reflect "Best Practices" for a medium sized network infrastructure in design and operation (4). The hardware and software capabilities of the systems and physical network need to be dealt with to assure current and future use in the course work presented in the lab.

It is a desire of the faculty and staff to have this classroom built as a model for future classroom design for other courses (4, 7). Currently, nine information technology courses with multiple sections are taught using this room. Discussions have already occurred with the thoughts of adding other courses to the lab's work load (7). Conceivably, courses outside the information technology program could make use of this classroom design and functionality.

2. Description of the Solution

The Network Computer Lab provides students the opportunity to learn the design and operation of systems administration and network administration on a live computer network that is safe to other computers and services on the network. It is a laboratory computer network "isolated" from the University of Cincinnati's main computer network behind a firewall and proxy server to protect the UC network from undesirable experiments in the laboratory environment while giving the students access to necessary UC network services and the Internet.

Students are able to create Virtual Machine instances on computer workstations simulating enterprise network nodes and services that are fully functional on a live network. Students are exposed to various operating systems and network services, and their functionality in an enterprise network.

The Network Computer Lab is modeled and built from personal knowledge, professional consultation, and in part from the Microsoft Solutions for Small and Medium Business: Medium IT Solution Series guide (2). The Solution Series guide is a tested "Best Practices" guide for the design, development, and deployment of a core network infrastructure. Figure 1 (next page) displays a logical network diagram of the Network Computer Lab.

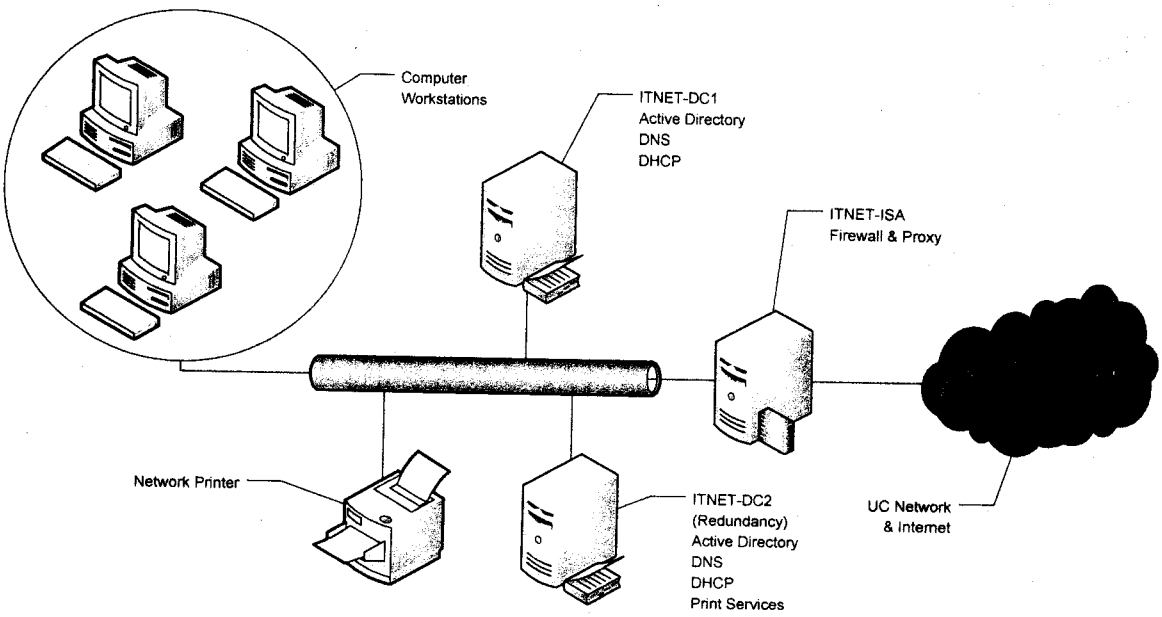

Figure 1. Science 302 Logical Network Diagram

2.1 User Profiles

This project will be implemented with three types of users in mind. The types of users will be System Administrators of the solution, Faculty Administrators, and Student Users who will benefit the most from the solution.

System Administrators will be responsible for maintaining the implemented solution. They must have working knowledge of the operating systems involved. They must have knowledge of user and resource administration within a networked domain structure involving the operating systems and technologies involved.

Faculty Administrators will have fewer rights and permissions to administer the domain environment, but will have administrator privileges on the workstations of the domain. Domain administration privileges will be limited to account management capabilities.

Student Users will be the primary users of the project solution. Their knowledge may be limited to logon procedures for the operating systems involved and network resource usage.

2.2 Design Protocols

The Network Computer Lab has been designed to allow faculty and students a wide range of latitude in their experimentation. Network connections and services are provided to give newer students the required services needed to accomplish their tasks in a virtual machine environment, while providing the more advanced students the freedom to create their own service solutions. The network services built for the infrastructure are primarily in place for the authentication and authorization of the isolated physical network services but some services may be over-ridden in a student's virtual machine implementation.

The physical network is a star network connected internally to two Gigabit switches providing the backbone of the network. Thirty-four data jacks are hardwired to two patch panels connected to the switches through patch cables. These provide network access for 25 workstations and 3 servers, and allows for future infrastructure expansion. This internal network is connected to the University of Cincinnati's network and the Internet through a firewall and proxy server connected to one outside line. The wiring standards follow the guidelines set by the Telecommunications Industry Association in the documents TIA/EIA-568-B.1 and TIA/EIA-568-B.2 (8, 9).

The internal network is based on a Class B subnet with the range of 172.16.0.1 to 172.16.7.254. The subnet mask for this implementation is 255.255.248.0 which allows up

to 2048 IP addresses. The gateway address for this subnet is 172.16.0.1 and is the internal network address for the firewall.

The fully qualified domain name for the network is DITNET.CAS.UC.EDU. The infrastructure network is built on a Microsoft Windows Server 2003, Standard Edition Active Directory domain. Workstations have the Microsoft Windows XP, Professional Edition operating system installed. All current service packs, updates, and patches are applied to the operating systems and applications on the servers and workstations.

The naming convention for all computer nodes is preceded with ITNET-. An infrastructure server is followed by a 2 or 3 letter descriptor for the service it provides plus an identifying digit for multiple servers of the same service; i.e. ITNET-DC2 is the second domain controller on the network. Workstations are followed by a two digit number except for the teaching station which is followed by "TS"; i.e. ITNET-03.

This implementation of the medium IT solution uses three servers: two domain controllers for redundant network services and one firewall and proxy server. A centralized file server for network storage would have been used, but the cost and performance issues did not justify the inclusion for the proposed uses on this network. All servers and workstations are configured with at least two hard drive partitions: a SYSTEM partition and a DATA partition. The SYSTEM partition primarily holds the operating system and installed applications. The DATA partition holds user data and shared data.

The primary domain controller (ITNET-DC1) provides authentication and authorization services for the network. It has a static IP address of 172.16.0.2. It provides Domain Naming Service (DNS) lookup for the internal network and forwards external

lookup requests to the University of Cincinnati's DNS server. It also provides Dynamic Host Configuration Protocol (DHCP) services for dynamic IP address assignments to requesting nodes on the internal network. The range of addresses in its pool for dynamic assignment is from 172.16.1.0 to 172.16.4.255.

The secondary domain controller (ITNET-DC2) is a redundant backup to the primary server in case of failure or scheduled downtime. It has a static IP address of 172.16.0.3. It also provides DNS and DHCP services for the network. The DHCP service pool for this server is from 172.16.5.0 to 172.16.7.254, so that it doesn't conflict with the primary server pool. This server also provides print network services.

The firewall and proxy server (ITNET-ISA) operates the Microsoft Internet Security and Acceleration Server 2004 (ISA). It has a static IP address internally of 172.16.0.1 and a dynamic IP address to the University of Cincinnati's network. It is configured for application layer filtering, intrusion detection and Web caching. Firewall Policies set for this server are listed in Appendix A.

The organizational unit (OU) structure for Active Directory is laid out in Figure 2 (next page). Group Policy Objects provide security and operational settings specific to objects with the organizational units like Folder Redirection.

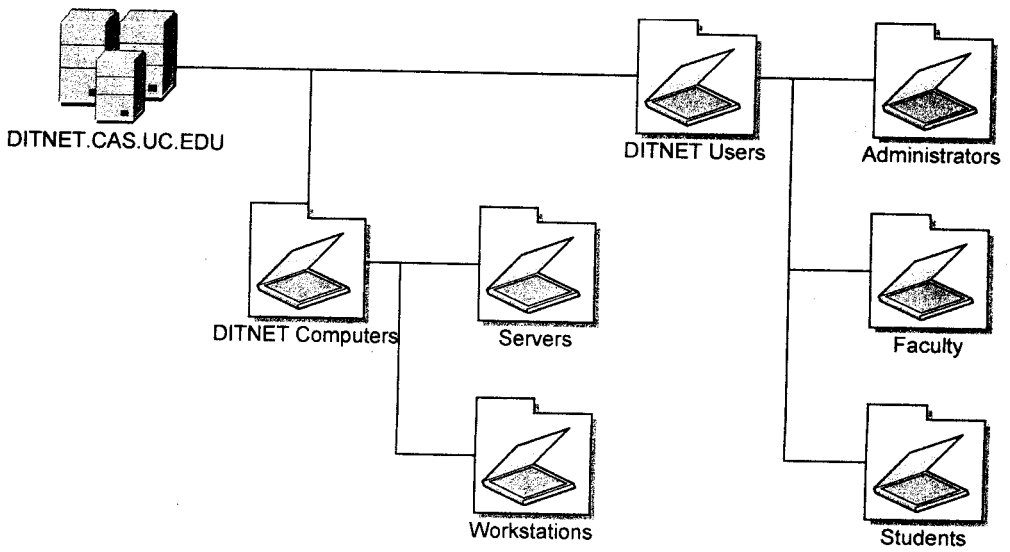

Figure 2. Active Directory Organizational Diagram

3. Objectives of the project

The objective of this project is to upgrade the core infrastructure of the Network Computer Lab in Science 302 using "Best Practices" for a medium sized network and remove the temporary conditions of the wired network in the lab. The objective of this project will be addressed by the services necessary to obtain the objective. The following services required for the objective are listed by infrastructure areas:

Physical Network

- Provide a permanent wired network with connection to the Internet.

Network Services

- Provide redundant DNS name resolution.
- Provide redundant DHCP assignment of IP addresses and client configuration.

Directory Services

- Provide authentication and authorization access of network services through the use of a directory listing.

Secured Internet Connectivity

- Provide firewall security of the internal network and prevent the external network from undesirable internal network traffic.

File Services

- Provide file management of user data.

4. Design and Development

The design and development of this project was done using Microsoft Virtual PC 2004 on a PC computer with a 3.2 GHz processor and 2 GB of RAM. The network connections for the virtual machine instances were local to the virtual application with the exception of the external ISA server connection. The external network connection was connected directly to the University of Cincinnati's network to simulate a live network connection.

Deployment of the project was done during down time for the Network Computer Lab, primarily in between quarters but also between class times.

4.1. Budget

This budget includes all the components that would be necessary to replace the equipment in the Network Computer Lab. This was done to estimate the cost of building this lab as a template. Some of the existing equipment could be re-used. The estimated total for the project would be $50715.70. The budget listing is in Appendix G.

4.2. Timeline

This project was completed by phases, the Proposal, the Design Freeze, and the Final Product. Much of the installation work was accomplished during the down-time of the lab, in between classes and quarters. The limited available time for installation was eased by prepping the replacement infrastructure servers off-line.

The Proposal phase included the following:

- Define the requirements of the Network Computer Lab infrastructure.
- Research the solutions to upgrading the Network Computer Lab infrastructure.
- Provide the required course documentation and proposal to upgrade the Network Computer Lab infrastructure.

The Design Freeze phase included the following:

- Develop and build a test environment for the proposed services of the Network Computer Lab infrastructure.
- Complete testing of the proposed services to verify functionality.
- Provide required course documentation and Design Freeze.
- Demonstrate the prototype network services from the test environment.
- Begin the replacement physical network wiring upgrade of the Network Computer Lab.

The Final Product phase included the following:

- Build and install the replacement infrastructure servers on the re-wired network.
- Join the workstations to the new network domain.

- Remove the "temporary" wired network and pre-existing infrastructure servers.
- Provide required course documentation and demonstrate the final product solution for the Network Computer Lab.

5. Proof of Design

This section will present diagrams, and screen shots of the services configured and in use for the solution to this project.

5.1. Physical Network

In hind sight, I should have taken a "before" photograph as a comparison for the temporary condition of the physical network in the Network Computer Lab. The following room layout diagram, Figure 3 (next page), displays the improved conditions of the lab and the location of the data jacks, switches, servers and workstations. Working operation of the physical network will be shown in succeeding screen shots.

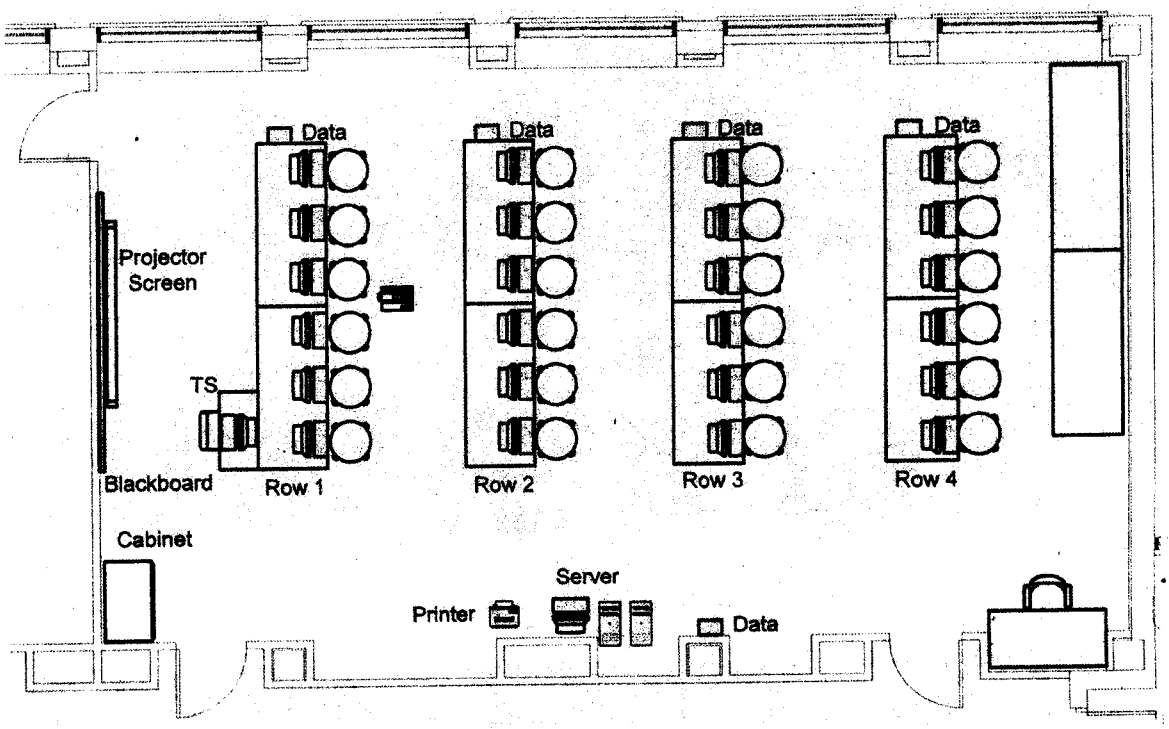

Figure 3. Science 302 Room Layout

5.2 Network Services

The following set of screen shots (next page) show the redundant fail-over functionality for the DNS and DHCP services is operational. Figure 4 is a screen shot taken from workstation ITNET-01 receiving an IP address from the domain controller ITNET-DC1 with ITNET-DC2 shut down. Figure 5 is a screen shot from the same workstation showing DNS name resolution being performed from the DNS service on ITNET-DC1.

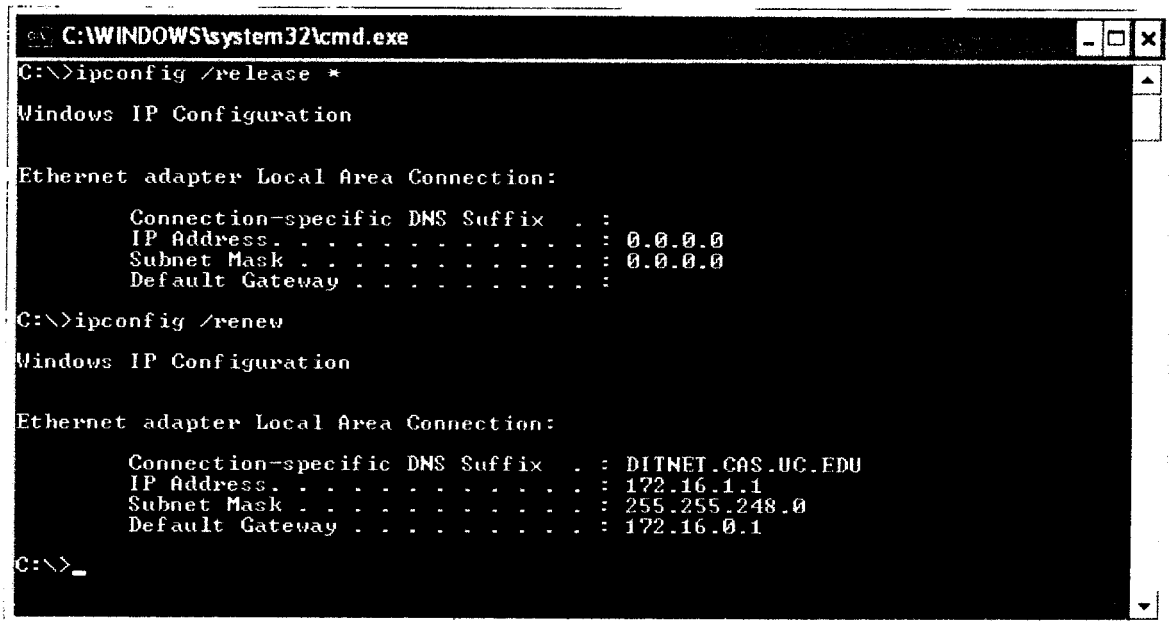

Figure 4. IP Address from ITNET-DC1

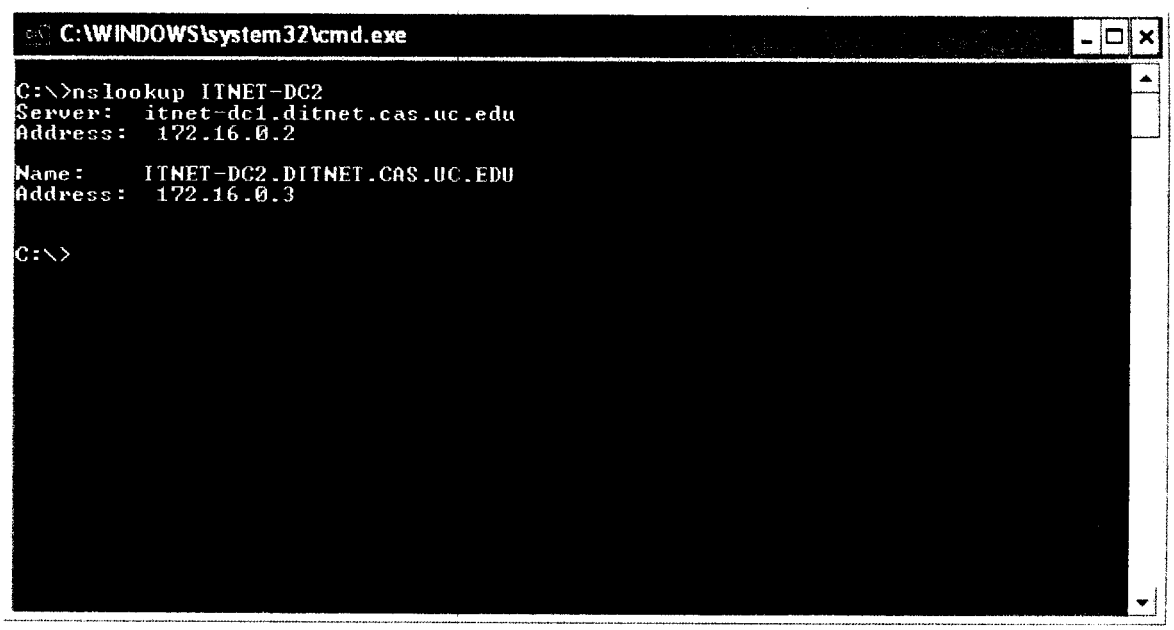

Figure 5. DNS Name Resolution from ITNET-DC1

With domain controller ITNET-DC2 operating and ITNET-DC1 shut down, the following figures provide a comparison for the redundancy of the network services provided to ITNET-01. Figure 6 shows ITNET-01 receiving an IP address from the IP address pool provided by ITNET-DC2. Figure 7 shows the DNS name resolution from

the DNS service on ITNET-DC2 handling another lookup after failing to contact ITNET-DC1.

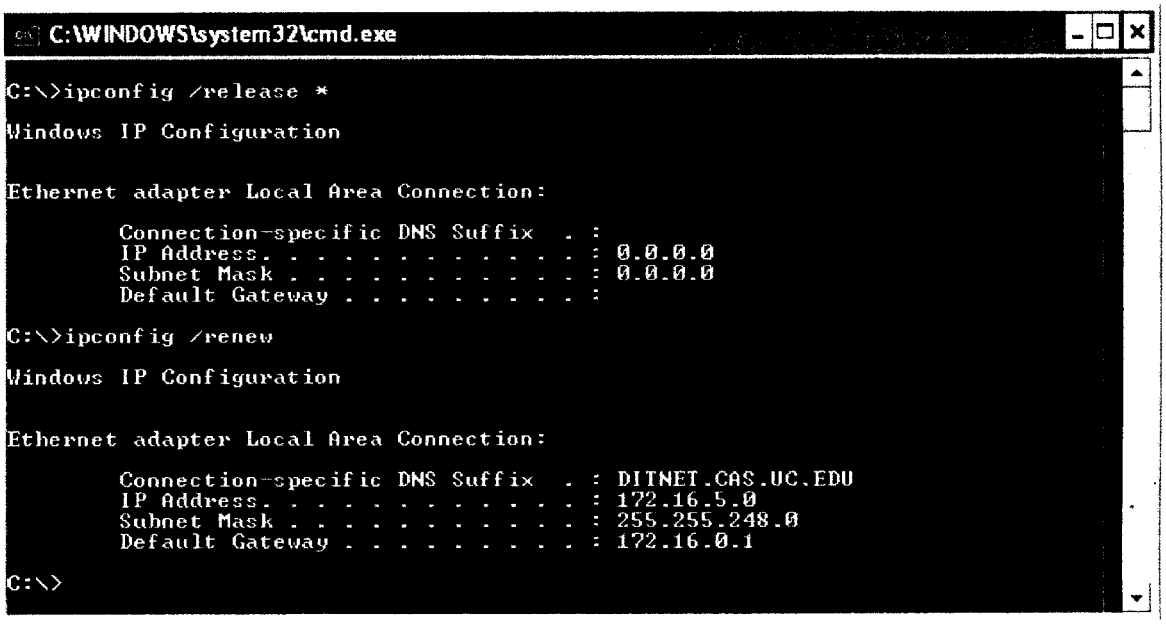

Figure 6. IP Address from ITNET-DC2

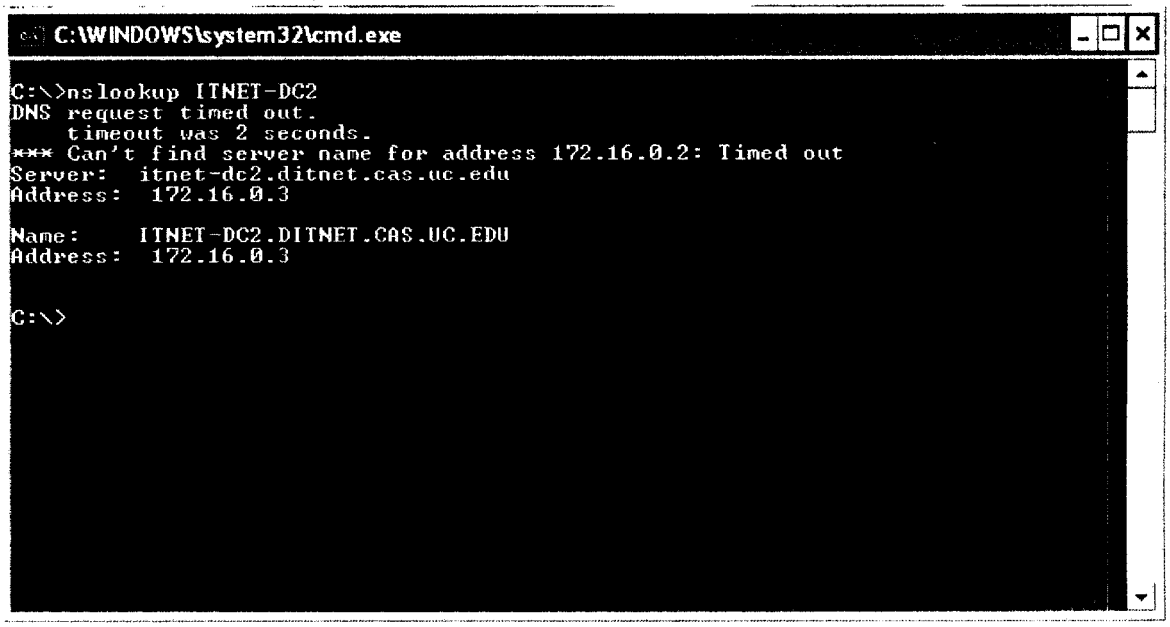

Figure 7. DNS Name Resolution from ITNET-DC2

5.3 Directory Services

The following screen shot is of the Active Directory Users and Computers management console. It shows a partial view of the Active Directory objects added to the DITNET domain. The Group Policy Objects policies for the domain and Organizational Units are listed in the appendices B through F.

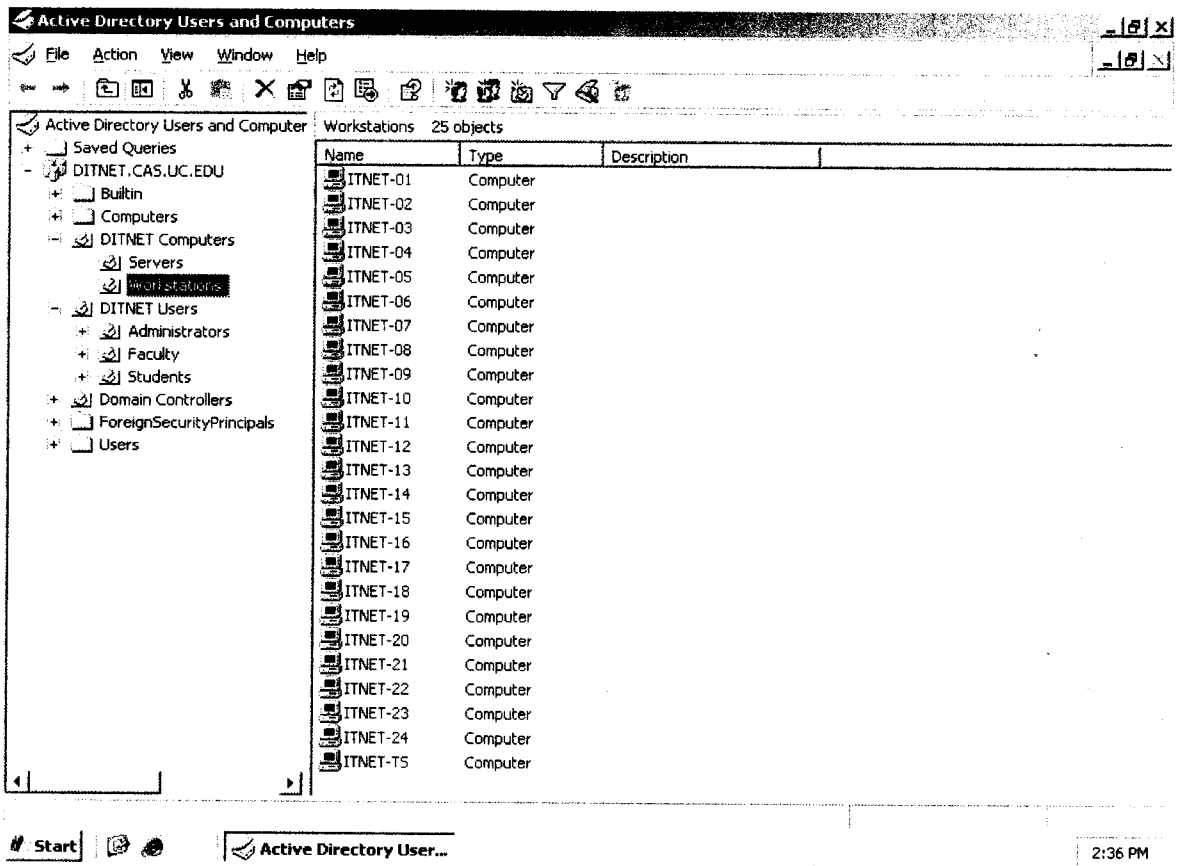

Figure 8. Active Directory Domain Objects

5.4 Secured Internet Connectivity

Connections from the internal network must pass through the firewall which filters network traffic into and from both the internal and external network. Figure 9 (next page) shows a mapped drive to the 'UCFileSpace' service on the University of

Cincinnati's network from the workstation ITNET-01. This indicates that network services outside the internal network are accessible.

The primary reason for implementing the firewall was to block DHCP services from getting onto the university's network and disrupting services there. Proof that this solution works is explained in the testing section later in this document.

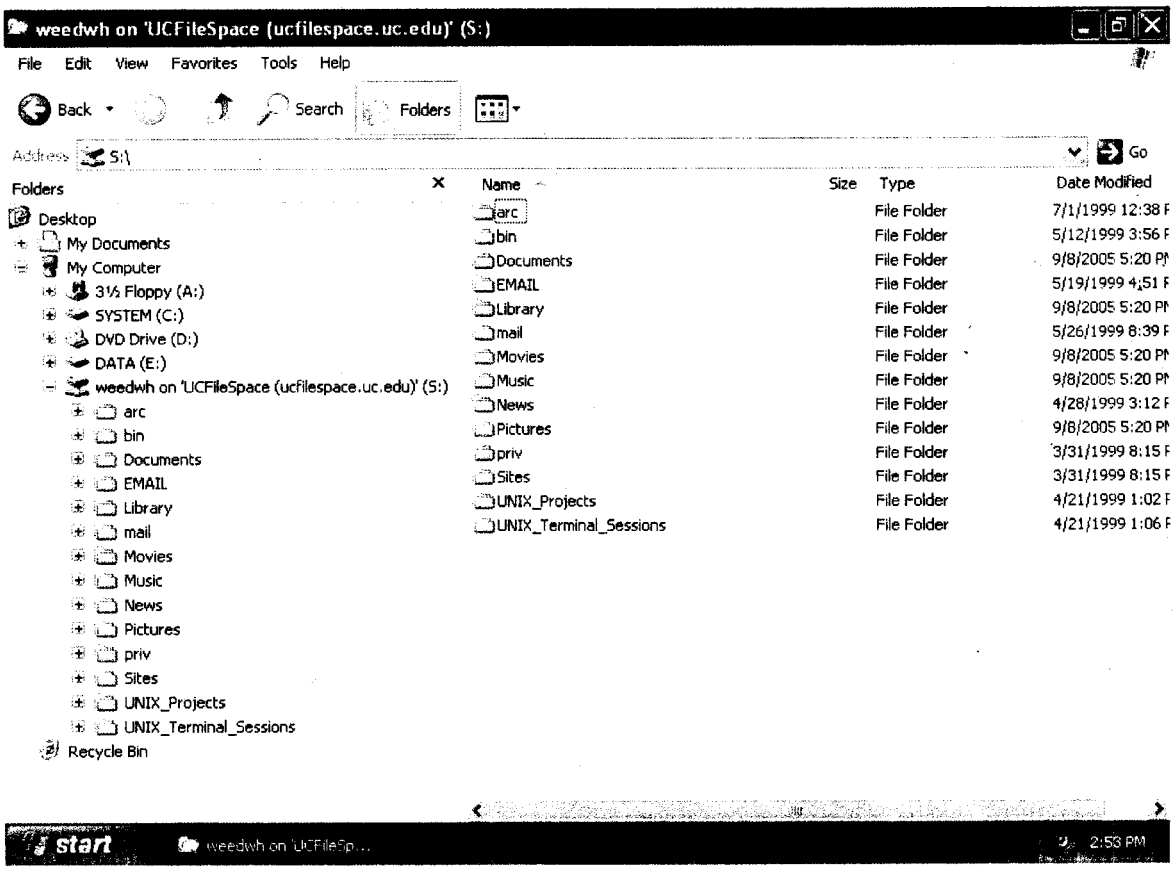

Figure 9. 'UCFileSpace' Mapped Drive

5.5 File Services

The large user data files (5-10 GB) created with the virtual emulation software necessitated local storage on the workstations. The performance issues of storing these files on a network share prevented the use of network storage. The user files still needed to be secure for each domain user and easily accessible to them performance wise. I

chose to use Folder Redirection policies from a Group Policy Object within Active Directory. These policies redirected the user's 'My Documents' folder to the local DATA drive on the workstation at which the user is logged on. The down side of this solution is that the user's data is saved to a specific workstation. The following figure shows a user's data files redirected to the local DATA drive.

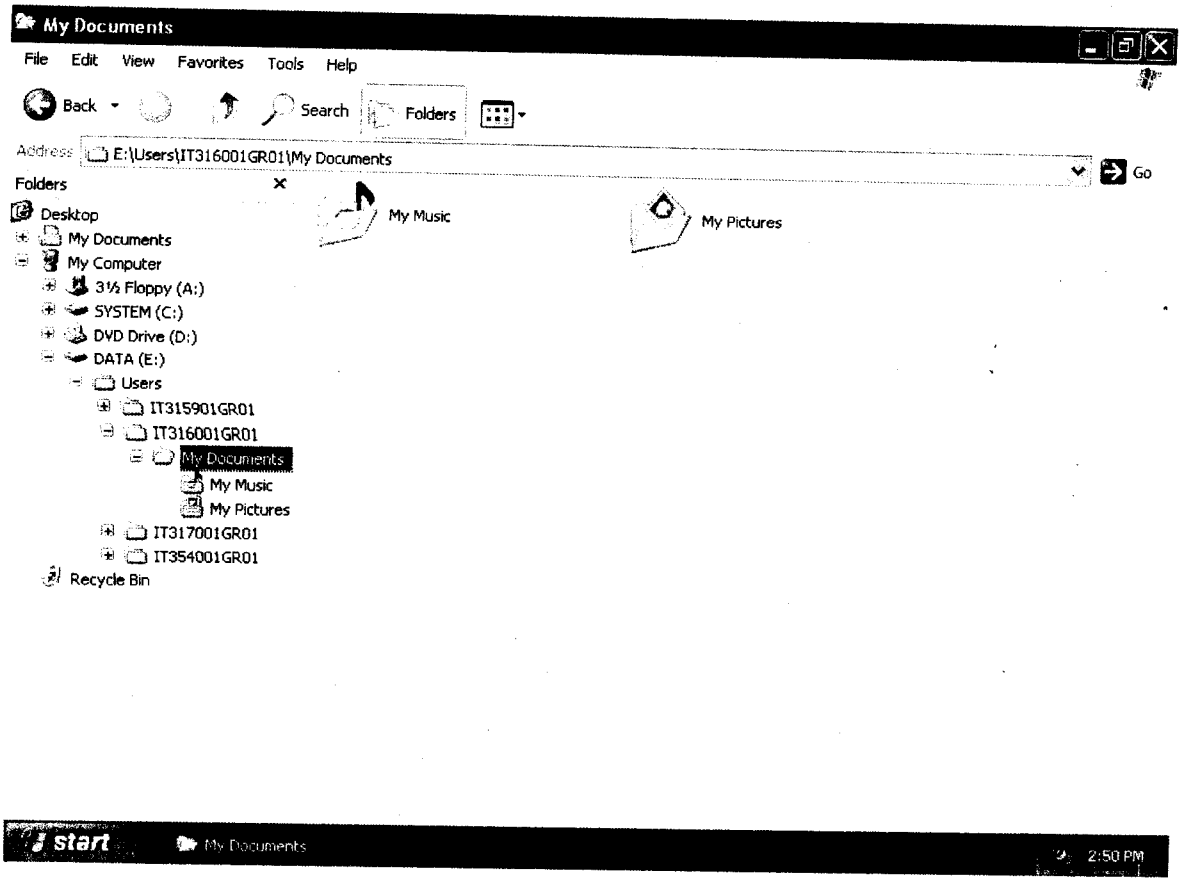

Figure 10. User Data Folder Redirection

6. Testing

Testing for this project was done to verify the functionality of the configuration settings connectivity of the physical network and the services provided by the base infrastructure. Testing was performed during the development stage to determine the proper configuration settings necessary. During the build and implementation phase of

the project, testing was carried out to verify the final functionality of the project by repeating the tests performed in the development stage.

Ethereal is a "sniffer" application used to monitor network traffic. It was used to determine the appropriate ports and network protocols that need to be available through the firewall particularly for the non-published attributes of 'UCFileSpace' and VMware server. Monitoring the attempted connections to these network services with Ethereal showed the network protocols and ports that are required to be open for the services. These "sniffed" responses were added to the firewall filters of the ISA server. Successful connections to 'UCFileSpace' and the VMware server showed that the correct ports and protocols were added.

Ethereal was used also to verify the prevention of DHCP traffic from the Network Computer Lab getting on to the university's network. This was accomplished by sniffing traffic from the "external" side of the firewall and monitoring the IP address acquisition of another workstation external to the isolated network. The only DHCP service responding to the IP address of the workstation request came from the official University of Cincinnati's DHCP service server.

As shown earlier, the redundancy and fail-over functions of domain controllers and the infrastructure services they provide were tested by shutting down one server at a time. The assigned DHCP address and the cached DNS entries on the workstation had to be cleared each time for a valid test to occur. The workstation was shut down and cold booted in between server shut downs in order to test the authentication and authorization of the workstation and user to the Active Directory copy on each server. The workstation

shutdown was done to remove any cached account information stored in memory on the workstation and provided by the Active Directory.

The physical wire network was tested using a Fluke MicroScanner Pro wire map tester. This tester shows that proper wire mapping connections are implemented according to the TIA/EIA-568 standards. It was able to indicate miss-configured mappings and open connections.

7. Conclusions and recommendations

The design and implementation of a computer network is a customized operation to the requirements of the users of the system. Using "Best Practices" in this endeavor assists in the standardization of the services provided. This aids the management requirements of the Systems Administrator, and provides for future expansion of the network infrastructure. The Network Computer Lab was designed and built to aid in a student's learning of the technologies in Information Technology. The concept of the lab to produce multiple and variable systems virtually for comparison and study may be ported to specific applications in other fields.

The high cost of network storage and its performance limitation prevented the installation of this type of service for this project. A future consideration for the Network Computer Lab, cost allowing, would be the implementation of network storage for the creation of central backups of the workstation DATA drives. This would provide a limited backup/restore capability for the lab allowing a student's work to be saved to a second device in case of hardware failure of the workstation the student uses.

A second consideration for the future of this lab would be the joining of this domain with a parent domain. This would allow user accounts of the parent domain to logon onto the workstations of the Network computer Lab using a single account.

Appendix A.
Firewall Policies

Name	Action	Protocols	Port	From	To
Time Service	Allow	NTP	UDP - 123	Internal Domain Controllers	External
UCFileSpace	Allow	NetBios Datagram NetBios Name Service NetBios Session SMB	UDP - 138 UDP - 137 TCP - 139 TCP - 443	All Protected Networks	External
Network Utilities	Allow	ICMP Information Request ICMP Timestamp Ping		All Protected Networks	All Networks
DNS Forwarder	Allow	DNS	TCP, UDP - 53	Internal Domain Controllers	External
DNS Internal	Allow	DNS DNS Server	TCP, UDP - 53 TCP, UDP - 53	All Protected Networks	All Networks
Telnet Traffic	Allow	Rlogin SSH Telnet Telnet Server	TCP - 513 TCP - 22 TCP - 23 TCP - 23	All Networks	All Networks
VMware Virtual Server	Allow	"user defined"	TCP - 902, 5900	All Networks	All Networks
Web Traffic	Allow	FTP HTTP HTTPS	TCP - 21 TCP - 80 TCP - 443	All Protected Networks	All Networks

Appendix B.
Default Domain Policy

Linked to the DITNET.CAS.UC.EDU container.

Default Domain Policy

General

Details

Domain	DITNET.CAS.UC.EDU
Owner	DITNET\Domain Admins
User Revisions	1 (AD), 1 (sysvol)
Computer Revisions	1 (AD), 1 (sysvol)
Unique ID	{9B40000D-DCB6-4464-8DA7-CD82B3EED4D8}
GPO Status	User settings disabled

Links

Location	Enforced	Link Status	Path
DITNET	No	Enabled	DITNET.CAS.UC.EDU

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

WMI Filtering

WMI Filter Name	None
Description	*Not applicable*

Delegation

These groups and users have the specified permission for this GPO

Name	*Allowed Permissions*	*Inherited*
DITNET\Domain Admins	*Edit settings, delete, modify security*	*No*
DITNET\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered

Maximum password age	42 days
Minimum password age	2 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	50 invalid logon attempts
Reset account lockout counter after	30 minutes

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/User Rights Assignment

Policy	Setting
Add workstations to domain	BUILTIN\Administrators

Restricted Groups

Group	Members	Member of
BUILTIN\Backup Operators		

Public Key Policies/Autoenrollment Settings

Policy	Setting
Enroll certificates automatically	Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled
Update certificates that use certificate templates	Disabled

Public Key Policies/Encrypting File System Properties

Policy	Setting
Allow users to encrypt files using Encrypting File System (EFS)	Enabled

Certificates

Issued To	Issued By	Expiration Date	Intended

			Purposes
Administrator	Administrator	5/15/2007 8:43:40 PM	File Recovery

For additional information about individual settings, launch Group Policy Object Editor.

Public Key Policies/Trusted Root Certification Authorities Properties

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

User Configuration (Disabled)

Windows Settings

Remote Installation Services

Client Installation Wizard options

Policy	Setting
Custom Setup	Disabled
Restart Setup	Disabled
Tools	Disabled

Appendix C.
Default Domain Controllers Policy

Linked to the Domain Controllers Organizational Unit.

Default Domain Controllers Policy

General

Details

Domain	DITNET.CAS.UC.EDU
Owner	DITNET\Domain Admins
User Revisions	0 (AD), 0 (sysvol)
Computer Revisions	1 (AD), 1 (sysvol)
Unique ID	{6AC1786C-016F-11D2-945F-00C04fB984F9}
GPO Status	Enabled

Links

Location	Enforced	Link Status	Path
Domain Controllers	No	Enabled	DITNET.CAS.UC.EDU/Domain Controllers

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

WMI Filtering

WMI Filter Name	None
Description	Not applicable

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
DITNET\Domain Admins	Edit settings, delete, modify security	No
DITNET\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Windows Settings

Security Settings

Local Policies/Audit Policy

Policy	Setting

Audit account logon events	Success
Audit account management	Success
Audit directory service access	Success
Audit logon events	Success
Audit object access	No auditing
Audit policy change	Success
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success

Local Policies/User Rights Assignment

Policy	**Setting**
Access this computer from the network	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Act as part of the operating system	
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	BUILTIN\Administrators, NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Allow log on locally	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Account Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Back up files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Bypass traverse checking	BUILTIN\Pre-Windows 2000 Compatible Access, NT AUTHORITY\Authenticated Users, BUILTIN\Administrators, Everyone
Change the system time	BUILTIN\Server Operators, BUILTIN\Administrators, NT AUTHORITY\LOCAL SERVICE
Create a pagefile	BUILTIN\Administrators
Create a token object	
Create permanent shared objects	
Debug programs	BUILTIN\Administrators
Deny access to this computer from the network	DITNET\SUPPORT_388945a0

Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	DITNET\SUPPORT_388945a0
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Server Operators, BUILTIN\Administrators
Generate security audits	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Print Operators, BUILTIN\Administrators
Lock pages in memory	
Log on as a batch job	DITNET\SUPPORT_388945a0, NT AUTHORITY\LOCAL SERVICE
Log on as a service	NT AUTHORITY\NETWORK SERVICE
Manage auditing and security log	BUILTIN\Administrators
Modify firmware environment values	BUILTIN\Administrators
Profile single process	BUILTIN\Administrators
Profile system performance	BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Restore files and directories	BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Shut down the system	BUILTIN\Print Operators, BUILTIN\Server Operators, BUILTIN\Backup Operators, BUILTIN\Administrators
Synchronize directory service data	
Take ownership of files or other objects	BUILTIN\Administrators

Local Policies/Security Options
Domain Controller

Policy	Setting
Domain controller: LDAP server signing requirements	None

Domain Member

Policy	Setting
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled

Microsoft Network Server

Policy	Setting
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled

Network Security

Policy	Setting
Network security: LAN Manager authentication level	Send NTLM response only

User Configuration (Enabled)

No settings defined.

Appendix D.
Default Administrators Policy

Linked to the Administrators Organizational Unit under the DITNET Users Organizational Unit.

Default Administrators Policy

General

Details

Domain	DITNET.CAS.UC.EDU
Owner	DITNET\Domain Admins
User Revisions	3 (AD), 3 (sysvol)
Computer Revisions	0 (AD), 0 (sysvol)
Unique ID	{ECD0F962-79A8-48A5-8FFB-B5F2C5790A83}
GPO Status	Computer settings disabled

Links

Location	Enforced	Link Status	Path
Administrators	No	Enabled	DITNET.CAS.UC.EDU/DITNET Users/Administrators

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

WMI Filtering

WMI Filter Name	None
Description	Not applicable

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
DITNET\Domain Admins	Edit settings, delete, modify security	No
DITNET\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Disabled)

No settings defined.

User Configuration (Enabled)

Windows Settings

Folder Redirection

Application Data
Setting: Basic (Redirect everyone's folder to the same location)
Path: \\ITNET-TS\Users\Administrators\%USERNAME%\Application Data
Options

Grant user exclusive rights to Application Data	Enabled
Move the contents of Application Data to the new location	Enabled
Policy Removal Behavior	Leave contents

Desktop
Setting: Basic (Redirect everyone's folder to the same location)
Path: \\ITNET-TS\Users\Administrators\%USERNAME%\Desktop
Options

Grant user exclusive rights to Desktop	Enabled
Move the contents of Desktop to the new location	Enabled
Policy Removal Behavior	Leave contents

My Documents
Setting: Basic (Redirect everyone's folder to the same location)
Path: \\ITNET-TS\Users\Administrators\%USERNAME%\My Documents
Options

Grant user exclusive rights to My Documents	Enabled
Move the contents of My Documents to the new location	Enabled
Policy Removal Behavior	Leave contents

Appendix E.
Default Faculty Policy

Linked to the Faculty Organizational Unit under the DITNET Users Organizational Unit.

Default Faculty Policy

General
Details

Domain	DITNET.CAS.UC.EDU
Owner	DITNET\Domain Admins
User Revisions	3 (AD), 3 (sysvol)
Computer Revisions	0 (AD), 0 (sysvol)
Unique ID	{6424587D-3E85-4CF0-A98C-87B4B4FDA591}
GPO Status	Computer settings disabled

Links

Location	Enforced	Link Status	Path
Faculty	No	Enabled	DITNET.CAS.UC.EDU/DITNET Users/Faculty

This list only includes links in the domain of the GPO.

Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

WMI Filtering

WMI Filter Name	None
Description	Not applicable

Delegation
These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
DITNET\Domain Admins	Edit settings, delete, modify security	No
DITNET\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Disabled)
No settings defined.
User Configuration (Enabled)
Windows Settings
Folder Redirection
Application Data
Setting: Basic (Redirect everyone's folder to the same location)

Path: \\ITNET-TS\Users\Faculty\%USERNAME%\Application Data
Options

Grant user exclusive rights to Application Data	Enabled
Move the contents of Application Data to the new location	Enabled
Policy Removal Behavior	Leave contents

Desktop
Setting: Basic (Redirect everyone's folder to the same location)
Path: \\ITNET-TS\Users\Faculty\%USERNAME%\Desktop
Options

Grant user exclusive rights to Desktop	Enabled
Move the contents of Desktop to the new location	Enabled
Policy Removal Behavior	Leave contents

My Documents
Setting: Basic (Redirect everyone's folder to the same location)
Path: \\ITNET-TS\Users\Faculty\%USERNAME%\My Documents
Options

Grant user exclusive rights to My Documents	Enabled
Move the contents of My Documents to the new location	Enabled
Policy Removal Behavior	Leave contents

Appendix F.
Default Student Policy

Linked to the Students Organizational Unit under the DITNET Users Organizational Unit.

Default Student Policy

General
Details

Domain	DITNET.CAS.UC.EDU
Owner	DITNET\Domain Admins
User Revisions	36 (AD), 36 (sysvol)
Computer Revisions	0 (AD), 0 (sysvol)
Unique ID	{BCF9B777-82DA-4EBF-AD84-E3F1BBA232FD}
GPO Status	Computer settings disabled

Links

Location	Enforced	Link Status	Path
Students	No	Enabled	DITNET.CAS.UC.EDU/DITNET Users/Students

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

WMI Filtering

WMI Filter Name	None
Description	Not applicable

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
DITNET\Domain Admins	Edit settings, delete, modify security	No
DITNET\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Disabled)
No settings defined.
User Configuration (Enabled)
Windows Settings
Security Settings

Public Key Policies/Autoenrollment Settings

Policy	Setting
Enroll certificates automatically	Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled
Update certificates that use certificate templates	Disabled

Folder Redirection
My Documents
Setting: Basic (Redirect everyone's folder to the same location)
Path: E:\Users\%USERNAME%\My Documents
Options

Grant user exclusive rights to My Documents	Enabled
Move the contents of My Documents to the new location	Enabled
Policy Removal Behavior	Leave contents

Administrative Templates
Control Panel

Policy	Setting
Prohibit access to the Control Panel	Enabled

Control Panel/Display

Policy	Setting
Remove Display in Control Panel	Enabled

Desktop

Policy	Setting
Don't save settings at exit	Enabled
Hide My Network Places icon on desktop	Enabled
Prohibit adjusting desktop toolbars	Enabled
Remove Properties from the My Computer context menu	Enabled
Remove Properties from the My Documents context menu	Enabled
Remove the Desktop Cleanup Wizard	Enabled

Network/Network Connections

Policy	Setting
Prohibit access to properties of components of a LAN connection	Enabled

Start Menu and Taskbar

Policy	Setting
Lock the Taskbar	Enabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Remove and prevent access to the Shut Down command	Enabled
Remove Drag-and-drop context menus on the Start Menu	Enabled

Remove links and access to Windows Update	Enabled
Remove My Music icon from Start Menu	Enabled
Remove My Network Places icon from Start Menu	Enabled
Remove My Pictures icon from Start Menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove Search menu from Start Menu	Enabled

System

Policy	**Setting**
Prevent access to the command prompt	Enabled
Disable the command prompt script processing also?	No

System/Ctrl+Alt+Del Options

Policy	**Setting**
Remove Lock Computer	Enabled

Windows Components/Microsoft Management Console/Restricted/Permitted snap-ins

Policy	**Setting**
Computer Management	Enabled
Disk Management	Enabled
Local Users and Groups	Disabled

Windows Components/Windows Explorer

Policy	**Setting**
Remove Security tab	Enabled

Appendix G
Budget

Physical Network Hardware

2ea.	CAT 5e UTP Cable - 1000'	$62.27	$124.54
34 ea.	CAT 5e Data Jack	$4.36	$148.24
4 ea.	4 port Face Plate	$1.85	$7.40
3 ea.	6 port Face Plate	$1.85	$5.55
6 ea.	Single Channel Cable Raceway	$11.94	$71.64
1 ea.	Three Channel Cable Raceway	$24.14	$24.14
6 ea.	Mounting Box for Wall Plate	$2.57	$15.42
2 ea.	CAT 5e 24 port Patch Panel	$76.32	$152.64
1 ea.	Hinged Wall Mount Bracket	$29.40	$29.40
2 ea.	24 port Gigabit Ethernet Switch	$406.43	$812.86
1 ea.	CAT 5e RJ-45 Modular Connectors - 100 pcs.	$25.25	$25.25
			$1,417.08

Computer Hardware

25 ea.	Workstation Computer 3.2 GHz Processor 2 GB RAM 40 GB HDD 160 GB HDD Microsoft Windows XP - Professional	$1,381.00	$34,525.00
26 ea.	15 inch LCD Monitor	$167.91	$4,365.66
3 ea.	Server Computer 3.0 GHz Processor 2 GB RAM 73 GB HDD 73 GB HDD Microsoft Windows Server 2003 - Standard	$3,275.00	$9,825.00
1 ea.	KVM Switch 4 port with Cables	$69.81	$69.81
14 ea.	Surge Protectors	$14.00	$196.00
			$48,981.47

Software

3 ea.	Microsoft Windows Server 2003 - Standard	Server installed
25 ea.	Microsoft Windows XP - Professional	Workstation installed
1 ea.	Microsoft Internet Security and Acceleration Server 2004	$317.15
1 ea.	Microsoft Virtual PC 2004	Free download
1 ea.	Ethereal v0.10.14	Free download
		$317.15

References

1. Allen, Robbie. *Active Directory Cookbook for Windows Server 2003 and Windows 2000.* O'Reilly. 2003.
2. *Microsoft Solutions for Small & Medium Business: Medium IT Solution Series – Medium Business Solution for Core Infrastructure.* Microsoft Corporation. 2005.
3. *Microsoft Solutions for Small & Medium Business: Medium IT Solution Series – Medium Business Solution for Management and Security using Active Directory Group Policy.* Microsoft Corporation. 2005.
4. Nyland, John. Assistant Professor. Department of Information Technology, OMI College of Applied Science, University of Cincinnati. Personal interview. September 24, 2005.
5. Peterson, Larry L. Davie, Bruce S. *Computer Networks: A Systems Approach.* Morgan Kaufmann Publishers. 2003
6. Ruest, Nelson. Ruest, Danielle. *Windows Server 2003: Best Practices for Enterprise Deployments.* McGraw-Hill/Osborne. 2003.
7. Stockman, Mark. Assistant Professor. Department of Information Technology, OMI College of Applied Science, University of Cincinnati. Personal interview. September 24, 2004.
8. *TIA/EIA-568-B.1.* Telecommunications Industry Association. May 2001.
9. *TIA/EIA-568-B.2.* Telecommunications Industry Association. May 2001.