

**Contents**

<b>Contents.....</b>	<b>1</b>
Task 1.....	6
1. Introduction .....	6
1.1. Different Addressing Modes.....	6
1.1.1. DNS.....	6
1.1.1.1. DNS Hierarchy/ Domain Name Space .....	7
1.1.1.2. Second level Domains and Subdomains .....	7
1.1.2. Active Directory.....	7
1.1.2.1. Benefits of Active directory.....	8
1.1.3. IP Addressing .....	9
1.1.3.1. Static IP .....	9
Benefits and drawback of Static IP .....	9
1.1.3.2. Dynamic IP [DHCP] .....	9
Benefits and drawback of Dynamic IP .....	9
1.2. ROLES of Address .....	10
1.2.1. Resource Management .....	10
1.2.2. Security of Resources .....	10
1.3. Summary.....	10
1.4. References.....	11
Task 2.....	12
2. Introduction .....	12
2.1. Servers supporting networking infrastructure management .....	12
2.1.1. DHCP Server .....	12
2.1.2. Print Server.....	13
2.1.3. File Server.....	13
2.2. Router.....	14

2.2.1.	Manageable Router.....	14
2.2.2.	Non-Manageable Router.....	14
2.3.	Printer.....	14
2.4.	Switches .....	15
2.4.1.	Unmanageable Switches.....	16
2.4.2.	Manageable Switches .....	16
2.5.	Firewall .....	16
2.5.1.	Hardware Firewall .....	16
2.5.2.	Software Firewall .....	17
2.5.3.	TMG (thread management gateway).....	17
2.6.	Access Modes .....	17
2.6.1.	Wireless access point.....	17
2.6.2.	Cabled Access.....	18
2.7.	Network Design Mode.....	18
2.7.1.	Workgroup Computers Network .....	18
2.7.2.	Domain Base Network.....	19
2.8.	Summary.....	19
2.9.	References.....	20
Task 3.....		20
3.	Introduction .....	21
3.1.	User Rights management .....	21
3.1.1.	NTFS permission.....	21
3.2.	User management and Strategy .....	22
3.3.	Access Limitation .....	22
3.3.1.	Logon Hour.....	22
3.3.2.	Group allocation Scheme.....	23
3.3.3.	OU management Strategy.....	24

3.3.4. Group policy management.....	24
3.4. Virtual Private Network.....	25
3.5. IP Security (IPsec) .....	25
3.6. Summary.....	26
Task 4.....	27
4. Introduction .....	27
4.1. Server Technologies.....	27
4.1.1. Domain controller (DC) .....	27
4.1.1.1. Benefits of DC .....	27
4.1.2. Read only domain controller (RODC) .....	28
4.1.3. Domain name system (DNS).....	28
4.1.4. Secondary DNS.....	29
4.1.4.1. Role of DNS in the Solution .....	29
4.1.5. Dynamic Host Configuration Protocol (DHCP) .....	29
4.1.6. Virtual private network (VPN) .....	29
4.1.6.1. Role in in solution.....	29
4.1.7. Routing and Remote Access Service (RRAS) .....	30
4.2. Network devices.....	30
4.2.1. Router .....	30
4.2.2. Switch .....	30
4.2.3. Printer .....	31
4.2.4. Access Point .....	31
4.2.5. Firewall.....	31
4.3. Network Components .....	31
4.3.1. IP-addressing .....	31
4.3.2. Sub netting.....	32
4.3.3. User.....	32

---

4.3.4.	Organizational Units and Groups .....	32
4.3.5.	Rights and Policies .....	32
4.4.	Design Solution.....	33
4.5.	Recommendations.....	35
4.6.	References.....	35
Task 5.....		36
5.	Introduction .....	36
5.1.	Addressing .....	36
5.1.1.	Identification of devices and resources .....	36
5.1.2.	Naming methodology .....	36
5.1.3.	Positive aspects.....	37
5.2.	Deployment.....	37
5.2.1.	Scalability .....	37
5.2.2.	Adaptability .....	38
5.2.3.	Commercial requirements.....	38
5.2.4.	Use of Technology.....	39
5.2.4.1.	Domain Based Network.....	39
5.2.4.2.	Internet .....	39
5.2.5.	Supportive of environments.....	39
5.2.6.	Change Management .....	39
5.3.	Summary.....	40
5.4.	References.....	40
Task 6.....		42
6.	Introduction .....	42
6.1.	Right and Security Requirements .....	42
6.1.1.	Access to Files and Directory .....	42
6.1.1.1.	Benefits .....	43

---

6.1.2.	Access to Printer .....	43
6.1.2.1.	Benefits .....	43
6.1.3.	Access to VPN .....	44
6.1.3.1.	Benefit .....	44
6.1.3.2.	Drawback .....	44
6.1.4.	Group Policies .....	44
6.1.4.1.	Benefits of Group policy in given environment .....	45
6.1.5.	Time Based Rules .....	45
6.2.	Evaluations Summary .....	46
6.3.	Recommendation .....	46
Task 8.....		47
7.	Introduction .....	47
7.1.	Critical Review .....	47
7.1.1.	Introduction: Existing System .....	47
7.1.2.	Body: Positive Aspects of Implemented system .....	47
7.1.3.	Limitations.....	48
7.2.	Testing of Implemented system .....	48
7.3.	Summary .....	56

**Task 1****Evaluate** current name resolution services. [1.1, M1]**1. Introduction**

Name resolution is described as conversion of a human readable name into address understood by machine or network, PCMAG (n.d.). In network infrastructure, components are given appropriate name to identify them. Components can be access via their name resolution. In this document some of the name resolution services such as DNS, active directory, IP addressing etc. is evaluated.

**1.1. Different Addressing Modes****1.1.1. DNS**

According to Beal (n.d.) DNS is short form of Domain Name System/Service which is used for translating domain name such as bank.prabhu.com into machine-readable IP address such as 10.10.10.1 as shown in figure 1 below. DNS itself serves as a database, similar to a phonebook in mobile that stores naming resolutions of hosts and their IP addresses. As domain names are alphabetic,

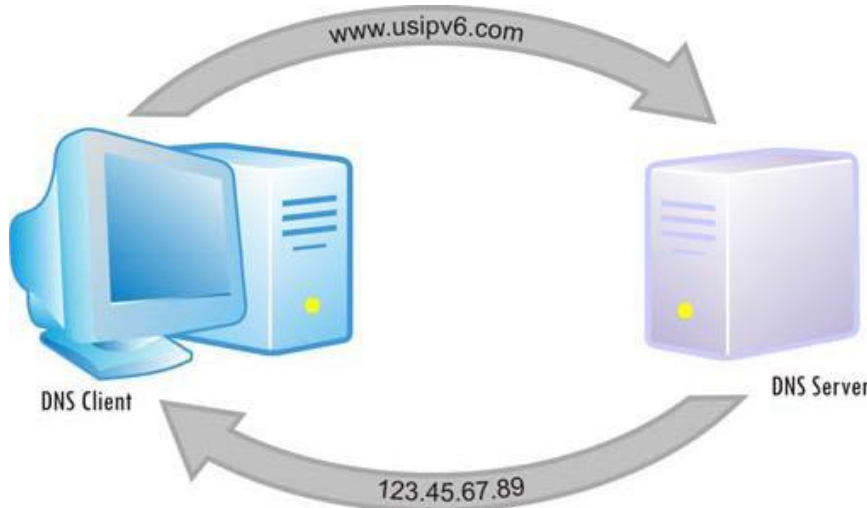


Figure 1 DNS Resource: <http://www.routercheck.com/wp-content/uploads/2014/03/dns-and-ipv6.jpg>

it is easier to remember than numeric IP addresses.

Users usually does not know the IP addresses of resources within the network, even if they do it is almost impossible to remember IP addresses of all resources. DNS makes life easier as it provides friendly name that are easy to remember. Without DNS, user will have to remember IP address for all webpages, computers to access them.

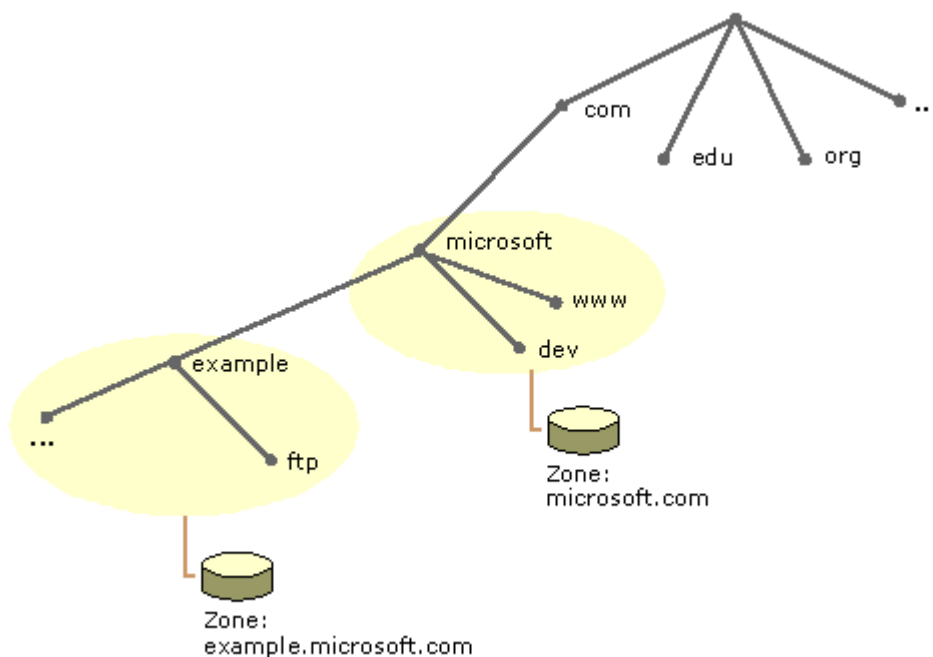
### 1.1.1.1. DNS Hierarchy/ Domain Name Space

A domain name is hierarchical series where each level is separated by dot “.” DNS Hierarchy has single domain at top are called root domain. Root domain is represented by dot “.” And below that proceeds top-level domain. Some of the top-level domains are listed here below.

Domain Name	Used For
.com	Commercial use
.edu	Educational use
.org	Organizational use
.mil	Military use

### 1.1.1.2. Second level Domains and Subdomains

Second level domains in DNS is used under top-level domain to represent individual organizations or entities. Similarly, subdomains is used under second-level domain to represent entities under that domain. Figure 2 show how domain and sub domain is used with top-level domain to represent two different system.



**Figure 2 Domain and Subdomain** Resource: <https://i-technet.sec-s-msoft.com/dynimg/IC195084.gif>

### 1.1.2. Active Directory

U-tools (n.d.) describes active directory as a database that stores all user accounts and password information of organization. Active directory also known as AD is used by system administrator to create and manage users, groups, organizational units, policies and user privileges.

Active directory database also stores information of computers and other resources within the domain network. Each resources within the network must have unique name resolution and IP address in order to be understood by active directory. To access these resources, user must authenticate to active directory.

#### 1.1.2.1. Benefits of Active directory

- **DNS integration:**

Active directory offers easy DNS integration which resolves resources IPs into user friendly names. This allows users to easily access network resources using name rather than IP address.

- **Centralized:**

AD offers centralized environment where user can access different network resources using user account created in AD. User does not have to create different user account for database server, web server, mail server.

- **Scalable:**

AD offers great scalability as administrator can create unlimited users, groups, organizational unit and add resources to system as long as the hardware can support them i.e. storage, RAM, processor. Additionally, AD allows to add additional domain to form forest.

- **Security**

Active Directory offers security as it can define access control to each attributes of each objects. Active directory can maintain user access, user rights and privileges, resources access etc.

- **Policy-based management**

Active directory can enforce policies to user, group and whole organization unit.



### 1.1.3. IP Addressing

According to paessler (n.d.), IP address allows system to understand each other in distributed environment. Each hosts in the network requires addresses that can describe network and unique host id. These 32 bits addresses (for IPv4, 128 bits for IPv6) as mentioned above has two identifiers, host and network. IP address is represented in 4 blocks of decimal numbers, each block is 4 octets.

For example, address 192.128.1.1 represents 32-bits binary number 11000000.10000000.00000001.00000001. But IPv6 IP is represented in Hexadecimal notation like, 3FFE:F200:0234:8123:AE00:BE12:3822:EF12. According to Beal (2010), IPv4 gives possible IP addresses around  $2^{32}$ , which is just over 4 billion addresses. Similarly, IPv6 gives around  $2^{128}$ .

32 bits IP address is classified into different classes such as Class A, Class B, Class C, Class D and Class E. Number of hosts and network varies based on their class.

Any resource in the network requires valid IP address in order to work properly. IP address can be assigned manually to the machine or can be assigned dynamically. Based on their assignment method IP is described as static IP and dynamic IP.

#### 1.1.3.1. Static IP

Static IP is assigned to a machine manually and then remains constant. Network resources such as printers, gateways, servers whose IP are required to be known and constant are assigned static IP.

#### Benefits and drawback of Static IP

One of the key benefits of static IP is it remains constant hence it can be used in VPN secure connect, game hosting, servers, IPLOCATION (n.d.). On the other hand, it also has some drawbacks such as security threats can rise as IP is always same. Assigning IP on large number of hosts manually can be less cost effective than dynamic IP.

#### 1.1.3.2. Dynamic IP [DHCP]

Dynamic IP is assigned to host machine dynamically using DHCP (Dynamic Host Control Protocol). IP in machines whose IP does not require to be constant are assigned dynamically. NOIP (n.d.) notes, Dynamic IPs change time to time. IP in Wi-Fi devices are often dynamic.

#### Benefits and drawback of Dynamic IP

Due to regular IP changes, it offers lesser security threat. IP address assigned to a computer can be assigned to another computer if first one goes offline. Dynamic IP is fast method to assign IPs to large number of machines.

Dynamic IP offers less reliable connection for gaming, VOIP, VPN as IP can change during connection.

## **1.2.ROLES of Address**

### **1.2.1. Resource Management**

In network system, resource management deploys and allocates organization's resources, Tenrox (n.d.). Resources can be printers or IP based host machines etc. Resource management includes, planning, and implementing configurations to ensure efficient resource sharing. Resource management first analyzes the requirements then helps the system to utilize network resources to achieve those requirements. For example, if an organization has one printer and HR department needs to access that printer, resource management can make printer available to that department.

Naming resolution helps users to access and manage network resources using names instead of IP address. For Example, user can access network printer using name like printer.company1.com instead of using IP associated with printer. This makes accessing resources easier. Similarly, naming resolution helps management of other resources like IP based cameras, doors etc.

### **1.2.2. Security of Resources**

Network security is prevention of misuse and unauthorized access to resources within the network. Administrator can enhance resource security by controlling access to those resources. Name resolution allows administrators to specify a computer by name rather than IP address. For example, Computer with IP address 10.10.10.100 can be referred as accountcomputer1.prabhu.com. Here, accountcomputer1 is name of machine and prabhu.com is domain. Admin can limit access to network resource based on machine name. For example, HRComputer1 cannot user printer1 which is installed specifically for account section. Such security of resources will result less business disruption and higher productivity.

## **1.3.Summary**

This document evaluated various addressing modes and name resolution services, requirement and benefits of such services. Addressing allows system to identify a resource. Name resolution is basically process of providing machine a human friendly name instead of number based IP address. Various technologies such as DNS, Active Directory, IP address etc. plays roles in name resolution process. Name resolution technologies has huge impact on any networking environment as it allows accessing resources using name instead of IP address. Administrator can distribute resources to users based using sources names and enforce securities on them.

#### 1.4. References

- Beal, V. (n.d.) DNS - Domain Name System [Online] Available: <http://www.webopedia.com/TERM/D/DNS.html> Accessed [10/2/2015]
- Beal, V. (n.d.) what is The Difference between IPv6 and IPv4? [Online] Available: [http://www.webopedia.com/DidYouKnow/Internet/ipv6\\_ipv4\\_difference.html](http://www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html) Accessed [10/1/2015]
- IPLOCATION (n.d.) what is the difference between a static and dynamic IP address? [Online] Available: <https://www.iplocation.net/static-vs-dynamic-ip-address> Accessed [10/4/2015]
- NOIP (n.d.) what is a Dynamic IP Address? [Online] Available: <http://www.noip.com/support/knowledgebase/what-is-a-dynamic-ip-address/> Accessed [10/4/2015]
- Paessler (n.d.) a short introduction to IP Addresses [Online] Available: <https://www.paessler.com/support/kb/questions/50> Accessed [10/4/2015]
- PCMAG (n.d.) name-resolution [Online] Available: <http://www.pcmag.com/encyclopedia/term/47598/name-resolution> Accessed [10/2/2015]
- Tenrox (n.d.) resource-management [Online] Available: <http://www.tenrox.com/glossary/resource-management/> Accessed [10/4/2015]
- U-tools (n.d.) what is Active Directory? [Online] Available: <https://u-tools.com/help/WhatIsAd.asp> Accessed [10/2/2015]

## **Task 2**

**Discuss** the technologies that support network infrastructure. [1.2]

### **2. Introduction**

To enable a network connection within an organization, number of hardware and software are required. These hardware and software resources are described as network infrastructure. According to Technopedia (n.d.) these network infrastructures are interconnected with each other to enable communication. This communication can be internal, external or both. Some of the network infrastructures includes, routers, switches, networked computer, firewall etc. This document discusses several technologies that supports network infrastructure.

### **2.1. Servers supporting networking infrastructure management**

Network infrastructure are managed through servers. There are several types of servers, each manages different aspect of a network infrastructure. Some of the servers are discussed below here.

#### **2.1.1. DHCP Server**

Dynamic host configuration protocol also referred as DHCP enabled server automatically assigns a valid IP address to client computers and other TCP/IP based infrastructures. Client devices must not have static IP assigned in order to receive IP from server automatically. According to Microsoft (n.d.) a DHCP server can be configured to distribute additional IPs that allows these clients to connect with DNS server, WINS server and Routers.

The core advantage of having a DHCP server is no manual IP configuration for each client machine is required. For a large network this can save large amount of time. Additionally it eliminates chance of duplicate IP among client devices.

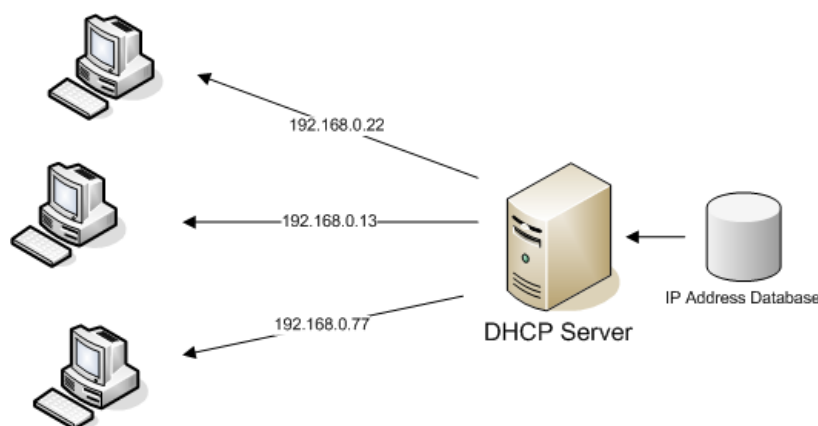


Figure 3 DHCP server (assigning IP to clients automatically) Source: Chris Sanders (2007)

### 2.1.2. Print Server

Print Server is a computer with print server enabled or a dedicated printer server device that allows computers in network access to network printer. Print server is used for managing one or more than one printers. Printer security, pooling, queue management, printer driver sharing etc. are configured through print server.

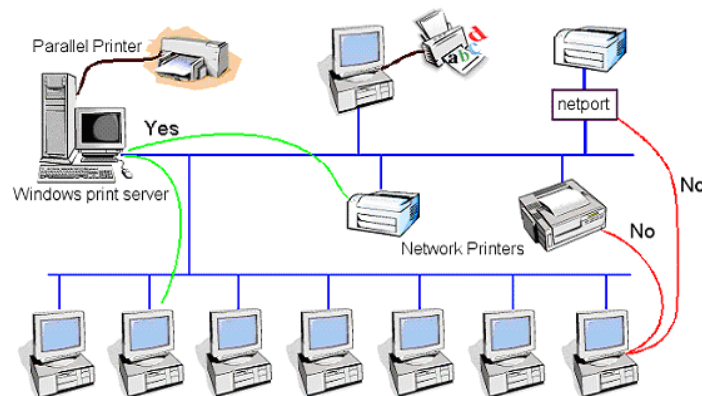


Figure 4 Print Server with Dedicated computer (Source: [www.papercut.com](http://www.papercut.com))

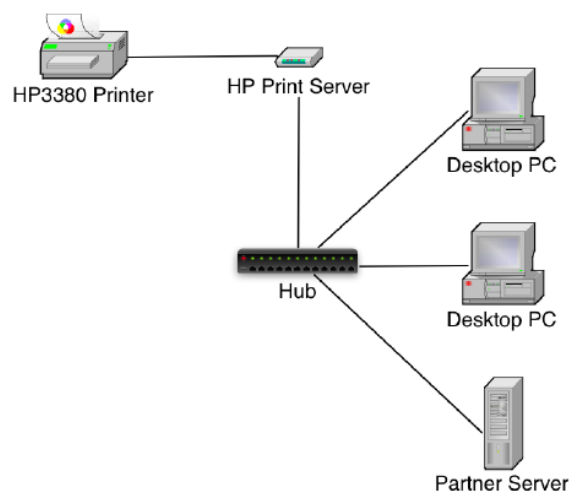


Figure 5 Print Server with Dedicated Print server device Source: [learn.pcc.com](http://learn.pcc.com)

### 2.1.3. File Server

File server is networked computer whose main purpose is to provide storage media to computers within the network. The main advantage of file server is any user within network can store file in file server and other user can access them. Rouse (2005) wrote, file server is used for sharing/transferring data without using any external device such as pen drive or DVD.

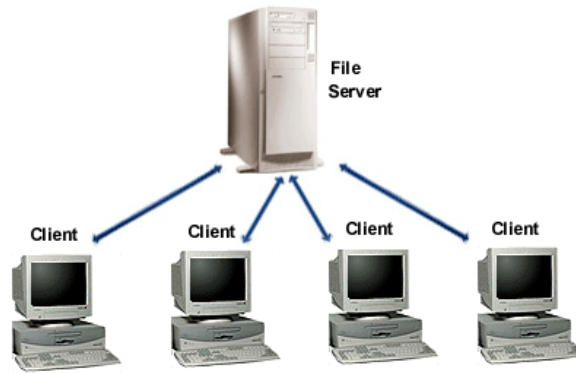


Figure 6 File server enabled network infrastructure (Source: dewassoc.com)

## **2.2.Router**

In simplest words, routers are physical device (sometimes software) that connects two different network. It is used for forwarding data package between networks. Unlike other network devices such as switch, router can analyze the data package to be transferred (COMPUTERHOPE, n.d.). Routers have capability to change the way data is packaged before transferring them to different network.

### **2.2.1. Manageable Router**

In manageable router, user can highly configure the router as per requirement. User can enforce security policy such as access control, firewall, routing protocols etc. Cisco, Juniper are some manufacturers producing highly manageable routers.

### **2.2.2. Non-Manageable Router**

In non-manageable router very limited configuration can be made. Firmware in router offers limited setting for user.

## **2.3.Printer**

Printer is an electronic machine that prints data from computer into paper. There are two types of network printing available based on how it is managed in network infrastructure.

### **2.3.1. Network Computer with Shared Printer**

In this type of Network Printing client connects to printer through host computer (printer server).

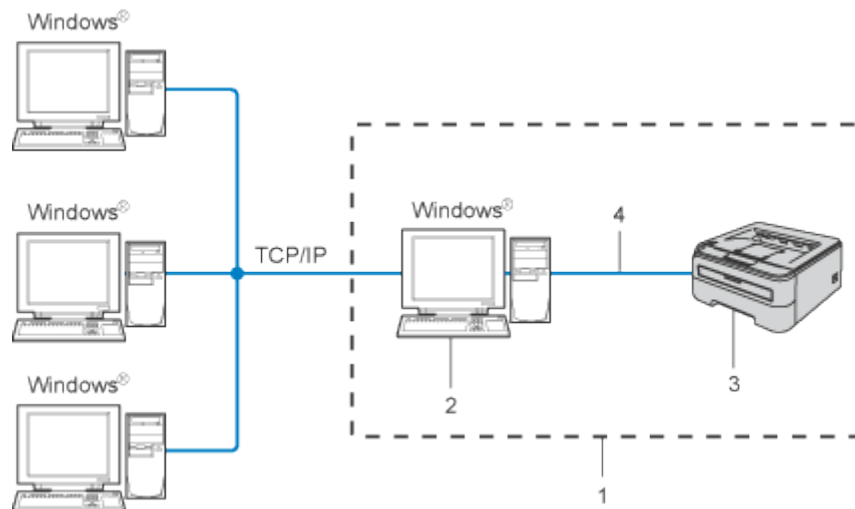


Figure 7 Network Printing through Host computer (source: uvm.com)

### 2.3.2. Network Printer with Dedicated IP

This type of network printer has their own IP address and are directly connected the network. Other computers uses Printer's IP address to access them.

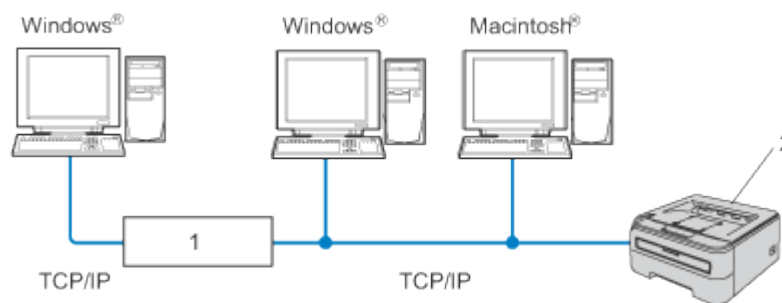


Figure 8 Network Printing using IP printer (source: uvm.com)

## 2.4. Switches

Switch is a device which is used for connecting computers and other IP based wired devices into a single network (LAN). According to cisco (n.d.) a switch works as a manager, enabling networked devices to communicate to each other efficiently. There are two types of switch available based on the way they are managed.

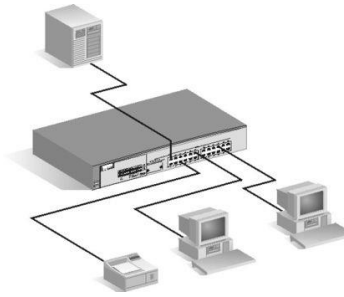


Figure 9 Computers and devices connected to single LAN using SWITCH (source: hp.com)

#### 2.4.1. Unmanageable Switches

An unmanageable switch are basically plug and play device with no configuration functionality. Computers and other devices are just need to be plugged into switch to be joined in same LAN. These type of switch as no additional application and can be useful for home or very small office as it cost much lesser than manageable switches.

#### 2.4.2. Manageable Switches

Manageable switches are configurable according to need hence provides flexibility than unmanaged switches. These types of switches has functionality such as monitoring and managing locally and remotely, increased security level etc.

### 2.5. Firewall

Firewall is a system that can be software and hardware or both and controls the incoming and outgoing network traffic. Firewall is frequently used for preventing unauthorized access to network from user of another network generally internet.

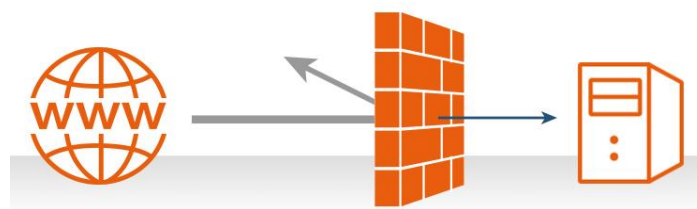


Figure 10basic concept of Firewall system (Source: sanketrjain.com)

#### 2.5.1. Hardware Firewall

Hardware firewall can be found as dedicated firewall hardware as well as integrated with modern broadband routers. Most hardware firewall can effectively protect the network attacker. Both type of hardware firewall, one that requires very few configuration and other requires complex configuration



are available in market. Figure 9 shows hardware firewall manufactured by cisco. Some of the other popular manufacturer of such type of firewall are ZyXEL, SonicWALL, and Netgear etc.



Figure 11 Hardware Firewall from CISCO (source: [www.vology.com](http://www.vology.com))

### 2.5.2. Software Firewall

Like other firewall software firewall's main purpose is to block unauthorized access to network. Software firewall is installed and runs on system hence it requires system resource and can affect system performance. Though according to Beal (2010) a good firewall generally takes small amount of resources and runs on background. Some of the popular software firewalls are from sygate, nortan, zone alarm etc.

### 2.5.3. TMG (thread management gateway)

Microsoft Forefront Thread Management Gateway (2010) also known as TMG is a firewall that provides outbound and limited inbound protection. It has features such as antimalware protection and application layer intelligence. Some of the features of TMG 2010 state by GUL (2012) are:

- Secure Routing
- Email Filtering
- Package Filtering
- Secured VPN
- Malware Protection

## 2.6. Access Modes

### 2.6.1. Wireless access point

Wireless access point is used to connect a wireless local area network (WLAN) with another WLAN or fixed wired LAN. It is a point that transmits and receives wireless radio signal hence also referred as a transceiver. Mitchel (n.d.) writes WAPs are commonly used for supporting public internet hotspots. Modern WAP devices supports up to 255 clients compared on 20 clients in old models. Enterprises uses WAP to increase their Wi-Fi zone and number of client supported.

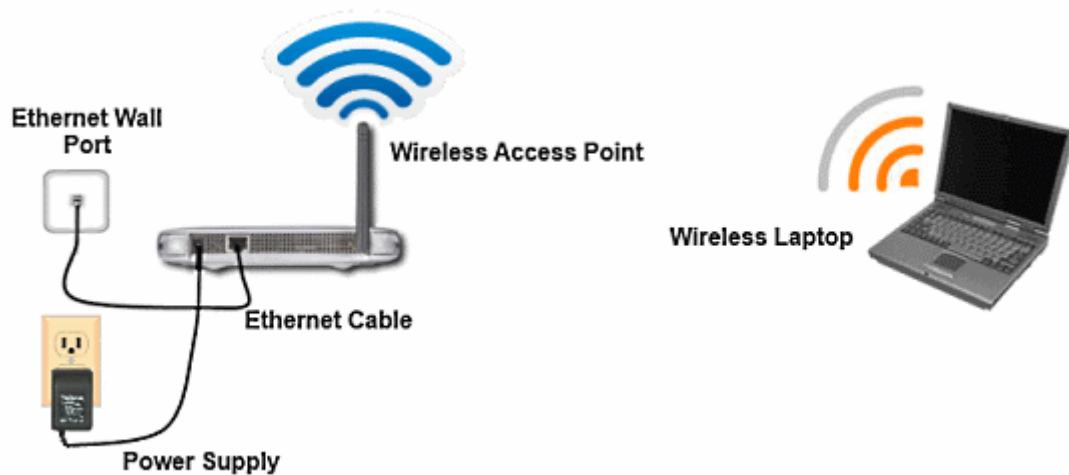


Figure 12 Connection using Wireless Access Point (WAP) |Source: oakdome.com

### 2.6.2. Cabled Access

Cable access allows connecting to resources and establishing networking environment using cables. Cable has always been helping information technology being a medium to transport information data. Be it television, telephone or other information system, cable has been used. In computer networking, cable is used for cable accessing computers and other resources. Ethernet cable allows computer to access resources and internet through router and switches. There are various type of cable available in market for networking purposes. These cables are manufactured varying data transportation speed, ranging from MB/s to GB/s. Cat 5, 5e, and Cat 6 are some of the popular cable models used in current market.

## 2.7. Network Design Mode

### 2.7.1. Workgroup Computers Network

Basically, workgroup based network is a collection of computers of same LAN. To establish such network, each computer should share similar workgroup name and IP subnet. This network allows resources sharing and all computers act as peers. Hence, this network is also referred to as peer-to-peer network. Some of the features of workgroup based network are discussed below.

- Network has no superior computer, one computer cannot control another controller.
- A computer can share its resources, allowing other computers to access those resources.
- Owner of the shared resources can set security configuration to limit access to the resource.
- Workgroup is not password protected technology hence anyone can join the workgroup using name and IP address of same subnet.

- User cannot use computer using user account information of another computer.

### 2.7.2. Domain Base Network

A server, central location which shares resources and manage them and other clients joins network to access to resources is known as domain based network. Unlike, workgroup based network, domain network has dedicated computer that centrally manages resource access and user accounts. Database that stores user account information in domain server is known as active directory and domain server is known as domain controller. Various technologies discussed in this document such as print server, file server etc. are maintained centrally via domain computer. Some of the core feature of domain based network environment is discussed below.

- As user account information is stored centrally, user can use different computer within the network, provided that administrator has granter user to do so.
- Computer need to go through authentication to join a domain.
- Admin can enforce various access based security policies.
- Client computer has very limited configuration ability as they are bound by policies enforced by administrator.

### 2.8.Summary

Various technologies that supports network infrastructure has been thoroughly discussed in this document. Server technologies such as DHCP, file server, printer server helps network to establish and manager resource sharing. DHCP offers faster dynamic IP distribution. Whereas file and printer server allows effective and secure file and printer sharing. Technologies such as cables, wireless access point, switch and router allows to establish networking environment.

This document also discussed technologies that helps to secure network environment. Firewall technology prevent suspicious activity in the network. At last, various network design technologies such as domain and peer to peer networking and their features were discussed. Which concluded that workgroup based network is suitable for scenario where security is not top priority and domain based network is suitable for any network where there are large number of users, resource security is top priority.

## **2.9.References**

- COMPUTERHOPE (n.d.) *Router* [Online] Available:  
<http://www.computerhope.com/jargon/r/router.htm> Accessed [10/7/2015]
- Beal, V. (2010) *the Differences and Features of Hardware and Software Firewalls* [Online] Available:  
[http://www.webopedia.com/DidYouKnow/Hardware\\_Software/firewall\\_types.asp](http://www.webopedia.com/DidYouKnow/Hardware_Software/firewall_types.asp)
- Cisco (n.d.) *what is a Network Switch vs. a Router?* [Online] Available:  
[http://www.cisco.com/cisco/web/solutions/small\\_business/resource\\_center/articles/connect\\_employees\\_and\\_offices/what\\_is\\_a\\_network\\_switch/index.html](http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html) Accessed [10/7/2015]
- GUL (2010) *Introduction to TMG 2010* [Online] Available:  
<http://www.trainingtech.net/introduction-to-tmg-2010/> Accessed [10/7/2015]
- Microsoft (n.d.) *DHCP Server* [Online] Available: <https://technet.microsoft.com/en-us/windowsserver/dd448608.aspx>
- Mitchel (n.d.) *access point* [Online] Available:  
[http://compnetworking.about.com/cs/wireless/g/bldef\\_ap.htm](http://compnetworking.about.com/cs/wireless/g/bldef_ap.htm) Accessed [10/7/2015]
- Rouse (2005) *file-server* [Online] Available:  
<http://searchnetworking.techtarget.com/definition/file-server> Accessed [10/6/2015]
- Technopedia (n.d.) *Network Infrastructure* [Online] Available:  
<http://www.techopedia.com/definition/16955/network-infrastructure> Accessed [10/6/2015]

## **Task 3**

**Discuss** security of resources available in network infrastructure management. [1.3]

### 3. Introduction

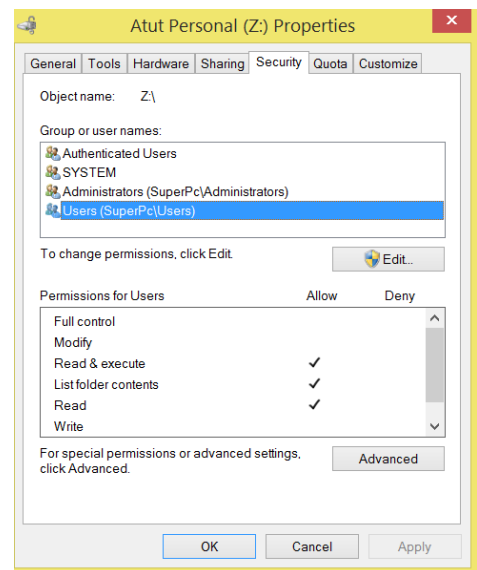
In network infrastructure management, security of resources is very important. Availability and accessibility to the resources must be controlled. In this document, such mechanism within infrastructure to manage resource security is discussed. It includes user right management, access limitation, IPsec, OU management and group policy etc.

#### 3.1. User Rights management

##### 3.1.1. NTFS permission

NTFS is file system regular file system for Windows NT or later operating system. Drives formatted with NT file system (NTFS), allows NTFS permission feature which allows or grant permission to user/groups to access file, folder or entire drive. Such permission determines user's access limitations.

Based on type of permission user or group has different level of accessibility on a file/folder. For example a user may have permission to read a file but s/he may not be able to modify it. Here is the full list of basic permission level that NTFS permission supports. Each permission type comes with allow or deny column.



Permission Type	Description
<b>Full Control</b>	User/Group has full control over directory. They can create, modify or delete the directory/file.
<b>Modify</b>	User/Group has permission to read and write the file. They can modify the content. This permission allows to create, modify and delete files within directory.
<b>Read and Execute</b>	For directory, user/group can read and executes files within the directory but cannot delete or modify files.
<b>Read</b>	This permission allows user/group to read file but cannot create new file within the directory as well as cannot modify them.
<b>Write</b>	This permission allows to create new file or folder within the directory but does not allow executing existing files.

NTFS permission offers control over resources on system. It provides entry level security to resources. Other advantage of this feature is it support both local and networked system.

### **3.2. User management and Strategy**

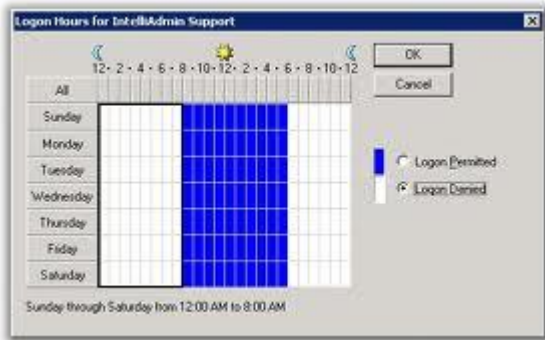
Users in network infrastructure are managed through user account. User account allows user to access the system. Each user account has their own username and password. For the security of system, users should not share same account as different account has different set of rights and permissions. After user is logged into the system, based on the permission rules user is allowed or denied access to domain resources.

Active Directory Users and Comput			
<div> <div> <div>+</div> <div>Saved Queries</div> </div> <div> <div>-</div> <div>www.bankprabhu.org</div> <div> <div>+</div> <div>Builtin</div> <div>+</div> <div>Computers</div> <div>+</div> <div>Domain Controllers</div> <div>+</div> <div>ForeignSecurityPrincipals</div> <div>+</div> <div>Managed Service Accounts</div> <div> <div>Users</div> </div> </div> </div> </div>			
Name	Type	Description	
Administrator	User	Built-in account for admini...	
Allowed ROD...	Security Group ...	Members in this group can...	
Cert Publishers	Security Group ...	Members of this group are...	
Denied ROD...	Security Group ...	Members in this group can...	
DnsAdmins	Security Group ...	DNS Administrators Group	
DnsUpdatePr...	Security Group ...	DNS clients who are permi...	
Domain Admins	Security Group ...	Designated administrators...	
Domain Com...	Security Group ...	All workstations and serve...	
Domain Cont...	Security Group ...	All domain controllers in th...	
Domain Guests	Security Group ...	All domain guests	
Domain Users	Security Group ...	All domain users	
Enterprise A...	Security Group ...	Designated administrators...	
Enterprise R...	Security Group ...	Members of this group are...	
Group Policy ...	Security Group ...	Members in this group can...	
Guest	User	Built-in account for guest ...	
RAS and IAS ...	Security Group ...	Servers in this group can ...	
Read-only D...	Security Group ...	Members of this group are...	
Schema Admins	Security Group ...	Designated administrators...	

### **3.3. Access Limitation**

#### **3.3.1. Logon Hour**

Assigning logon hour ensures that user can only log into the system during specified days and hours. This is a great resources security mean to prevent unnecessary use of resources. For example, administrator can set logon hour of 10:00 am to 17:00 pm to an employee user. This way they cannot login the system after office hour to use the resources.



### 3.3.2. Group allocation Scheme

Groups are used to manage user account and assign same permission to a set of user at once. If same permission rule is needed to be applied to several users it can consume lots of time. Instead, permissions can be assigned to group of user hence rule is applied to all users within that group.

For example, if we want all the students have access denied to printer, instead of applying this rule to every student user accounts one by one, we can achieve this by taking all the student user accounts to Student user group and then applying the rule to the group. Now all the student will have access denied to the printer. By this way group scheme can be used to secure resources within the network infrastructure. Furthermore, there are two types of groups and three types of group scopes.

Group Types	
<b>Security</b>	This type of group can be used to control the access to resources within the system.
<b>Distribution</b>	This type of group cannot be used for access controlling. This group is just administrative group and are not security enabled.
Group Scope	
<b>Universal</b>	This type of scope can contain user and group from any domain within the same forest.
<b>Global</b>	This type of scope can contain user and group from same domain. But it itself can be member of universal and domain local group of any domain or global group of same domain.
<b>Domain Local group</b>	This type of scope can contain user, universal and global group of any domain within the forest and domain local group from same domain. This group can be member of other domain local group within same domain.

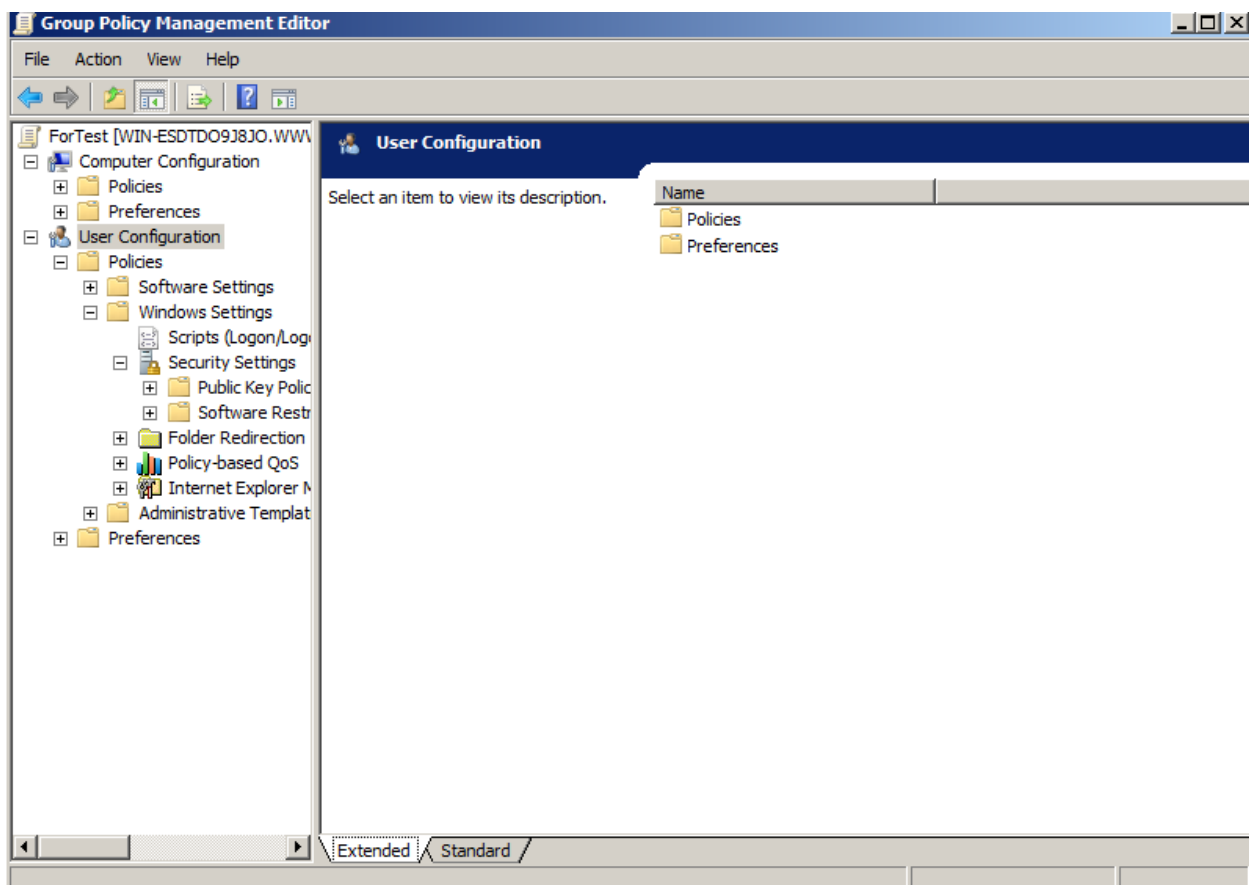
### 3.3.3. OU management Strategy

Organizational Units (OU) is a great method to keep the system controlled and organized. OU can contain other OU, users, groups and computers. Account permissions and group policy can be applied to OU to apply the permission rule to all groups and users within the OU. OU helps to maintain the security of the resources it cleans and organizes the system. OU is created to achieve business requirement and give administrators flexibility and control.

### 3.3.4. Group policy management.

Group policy is a tool used to enforce policies to users, groups and organizational units. It's an efficient way to maintain security of resources of infrastructure as only administrators are allowed to create and modify the policy.

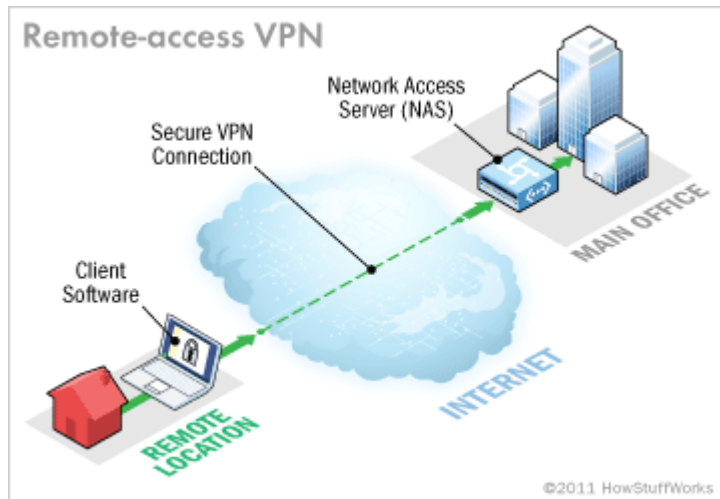
First of all group policy object (GPO) is created using Group Policy Management Console (GPMC). Then created GPO is linked with groups, OU, user accounts on which policies are to be applied. Then Group policy Management editor (GPME) allows administrator to change policy settings in GPO. All the policies specified in GPO are applied to all linked users.





### **3.4.Virtual Private Network**

Virtual Private Network (VPN) is a method to remotely and securely connect to other network via use of public network such as internet Remote access VPN is a very common VPN service to access home or office network remotely.



**Figure 13**<http://compsci2014.wikispaces.com/file/view/vpn-1.gif/376151146/vpn-1.gif>

VPN ensures data is protected from hackers by creating tunnel between VPN parties and encrypting the data. Transmitted data remains unchanged and only authentic parties are allowed to communicate. This way no other party can have access to network infrastructure. This enhances the resource security. In addition to this, Admin can set group policy or user privilege to VPN user to limit their accessibility within the resources.

### **3.5.IP Security (IPsec)**

As the use of internet grew, need of its security grew over the time. As the solution to this problem a protocol was introduced which could provide security at IP layer so that all the higher level at TCP/IP could take advantage of it. This IP protocol ensures secure packet exchange at IP layer. It is achieved by encrypting the information contained in IP datagrams through encapsulating. IPsec is a great method to provide security to resources within network infrastructure.

For example, most of the financial corporation commonly use IPsec to secure their customers financial and personal information. If IPsec is not used in such system like VPN, data can be intercepted and modified. IPsec is used to provide secure network and prevent Dos attack, Data pilfering, Credential theft and Data corruption.

### **3.6.Summary**

This document discussed various features and technologies available to secure the resources in the network. First of all, domain network environment provides user management feature. Which allows administrator to create and maintain user or groups according to requirement. Administrator can enforce policies and permission rules to those user and group. Now these group and user are bound by the policies and can only perform activities that are allowed by administrator. This is itself great mean of resource security.

File access permission maintains user access to file and directory. Similarly, time access rule limits user's access based on time. User can only access the network within specified period by administrator. Other mean of securing resources is VPN connection. VPN allows user to connect to domain remotely using public but secure path. Path is encrypted and data is securely transmitted and received.

## **Task 4**

**Design** a network infrastructure for a given networked environment [2.1, M2]

### **4. Introduction**

Prabhu bank, a renowned financial institution has over 90 branches and is still growing though out the nation. Prabhu bank is covering 32 districts but there is no central network management. Each branches has their own workgroup based system. Now it plans to upgrades its IT infrastructure. To design network environment for the bank, various server technologies are taken into consideration. IP distribution, various security policies are also identified for the network infrastructure design.

#### **4.1. Server Technologies**

##### **4.1.1. Domain controller (DC)**

Domain Controller is a server that controls hosts accessing the domain resources. It provides authentication service within the network. Active directory service in domain server stores information about user accounts, groups, organizational unit (OU) and enforces security policies within the domain network. User computer usage username and password stored in active directory to join the domain network. User can use any computer within the network to access the domain using username and password. After logged in, user can access to different resources based on privileges and rights assigned to that user account.

According to Hoffman (N.D) network administrators can modify group policy from domain controller to enforce security policy to each member machine within the system. This policy overrides the local policy of each system. Administrator can set time access, user rights and privilege etc. to secure the domain resources such as databases, printers, internet etc. Computers in domain network are under fully control of domain controller and are allowed to change very few things.

##### **4.1.1.1. Benefits of DC**

The core benefit of domain controller is it provides security to the network resources. It manages all user account and security policies. It maintains a list of who can access the network. Domain controller provides secure platform for other network services such as email server, secure VPN, Remote desktop connection etc.

##### **4.1.1.2. Role of DC in the Solution**

In the above scenario of designing network for Prabhu Bank, Domain controller plays fundamental role. When a computer is part of a domain network, DC is in control of everything. There are large

number of computer in the bank network considering all the branches hence domain controller can centrally manage all computers and maintain network security. DC can centrally enforce privileges to user groups/OU and allow access to network resources.

#### **4.1.2. Read only domain controller (RODC)**

Read only domain controller (RODC) is read only replica of domain network database. Client cannot write changes in RODC and it provides normal active directory services but exception of account password information, SERVERBRAIN (2013). Additionally RODC allows to create Read-Only DNS which is one directional copy of DNS.

##### **4.1.2.1.Role of RODC in the Solution**

Connection between branch office and central office can break any time such as natural disaster, power failure, or problem in ISP network etc. In cases branch office still needs to up and running and here is where RODC is useful. RODC would replicate the main DC and helps to establish the domain network in absence of main DC. Additionally RODC can be used as security layer in bank as changes made by attackers in RODC is not saved in Domain. Other role of RODC in branch is to install Read-only DNS to provide DNS even in case of network failure with main DNS.

#### **4.1.3. Domain name system (DNS)**

Domain name system (DNS) server provides service that converts machine friendly IP address of hosts to human friendly names and vice-versa. Such name resolutions are not case sensitive and makes possible for user to connect with different resources in network using names rather than complex IP addresses. A fully qualified domain name consists of host's name and domain name such as, account.prabhubank.com.

##### **4.1.3.1.Role of DNS in the Solution**

In the designed solution for the bank, DNS has an important role. There is going to be large number of computers with in the network. To access all those computer remotely user need to know their IP address. It is very difficult to remember large number of IP addresses. Hence DNS server will provide user friendly name for each computer within the network. This will allow admin to remotely access the host computer using FQDN (fully qualified domain name).

#### **4.1.4. Secondary DNS**

Like RODC to DC, Secondary DNS is read only copy of DNS server. It is only read only replica means DNS records cannot be written to it directly. It handles DNS queries from users when primary DNS server is down.

##### **4.1.4.1.Role of DNS in the Solution**

Designed solution has secondary DNS server in each of the branches. This ensures host machines can connect with other resources within the domain using name instead of IP address even in the scenario of DNS server failure.

#### **4.1.5. Dynamic Host Configuration Protocol (DHCP)**

A DHCP server is service provider that automatically assign IP addresses to hosts that joins the network. Additionally, DHCP can assign DNS address, subnet mask along with IP address to hosts. This service reduces the effort requires to manually configure all devices to make them able to connect to the system. Hosts with DHCP client enabled, can automatically request DHCP server to assign setting configured in DHCP. When configuring a large network manually, there is always chance of assigning same IP address to two or more host devices. This cause problem in the network. Using DHCP to assign IP address eliminates this issue.

##### **4.1.5.1.Role of DHCP in the Solution**

As stated above, manually assigning IP to large number of hosts can take long time and can cause problem if same IP gets assigned to multiple hosts. In current scenario there is large number of host within the system. DHCP server can be used to assign IP to host computer dynamically.

#### **4.1.6. Virtual private network (VPN)**

VPN server allows to connect to remote network via Public network yet using secure path. Branch office network uses VPN connection to connect with main office and ensure information remains safe. VPN connection encrypts information before sending and only authentic receiver can decrypt them.

##### **4.1.6.1.Role in in solution**

VPN server in the designed system is used to ensure secure connection from main office to branch office. Deploying VPN allows remote hosts to access network resources. This design deploys site to site VPN connection to connect two whole network i.e. main office, branch office securely.

#### **4.1.7. Routing and Remote Access Service (RRAS)**

RRAS is short form of Routing and Remote Access service which provides a user access to an internal network remotely. RRAS provides several connectivity technology options such as VPN through public IP, through ISP or through dial-up service. According to technopedia (N.D), RRAS allows user to connect remote server directly or connect two different remote server using site to site connection. After the connection is made, it functions like locally/physically connected network infrastructure. Additionally, RRAS is provides IP routing service allowing the server to work as LAN router.

##### **4.1.7.1.Role of RRAS in the Solution**

As stated above, proposed network design solution is going to use VPN connection to enable secure connectivity between branch office and head office. RRAS would allow VPN connection through either ISP or public IP.

#### **4.2.Network devices**

##### **4.2.1. Router**

Routers are hardware device (on occasion software) that connects two different network. In NCIB network, routers are required for connecting bank with its branches through internet. Designed network uses highly configurable cisco 2951 router. Here are some of the features of cisco 2951 router that makes it suitable for designed solution, Cisco (N.D):

- Enhanced Security
  - Hardware acceleration for VPN encryption
  - Integrated threat control using firewall protection
- Enhanced Easy VPN
- High Performance

##### **4.2.2. Switch**

Switch used for linking computers and other IP based resources into a single network (LAN). In NCIB, switch is used for connecting various servers, client computers and printers in single network. For switch, designed network uses manageable Cisco Catalyst 2960-Plus Series Switches WS-C2960+24PC-L Switch which has some features that makes this switch suitable for the solution(Cisco, N.D.):

- 24 Ethernet port that is suitable for head office network and branch office network
- Allows stacking of switches

- Smart Operations tool
- Energy friendly
- Highly Secure

#### 4.2.3. Printer

Any IP based wired/wireless printer that can satisfy bank's business requirement would be suitable for the solution. Printer can be selected based on performance.

#### 4.2.4. Access Point

Designed solution has Access points that would allow wireless device to connect with wired network. Connected user can access to network resources. Access point can also be used to increase the number of clients supported computer in bank network if additional switch is required as AP is less expensive than switch.

Cisco Aironet 2700 Series AP is used in design as it is designed for small and medium sized network.

#### 4.2.5. Firewall

Firewall is security module which prevents unauthorized access to network by controlling incoming and outgoing traffic. Both hardware and software type of firewall is available. High quality hardware firewall can be used in current scenario such as cisco firewall, juniper firewall.

### **4.3. Network Components**

#### 4.3.1. IP-addressing

Designed solution uses static IP distribution method to set IP address on client computers and dynamic IP distribution method to set IP addresses in server computers within the network. This solution is based on IPv4 classless IP address. Table below shows how IP address is distributed.

<b>Head Office</b>		
<b>Machine</b>	<b>IP Address (Range)</b>	<b>Subnet Mask</b>
Domain Controller	10.10.10.1	255.255.255.224
DNS	10.10.10.2	255.255.255. 224
VPN	10.10.10.3 (Adapter 1) 192.168.1.1 (Adapter 2)	255.255.255. 224
DHCP	10.10.10.5	255.255.255. 224
Print Server	10.10.10.6	255.255.255. 224

RODNS	10.10.10.7	255.255.255. 224
HR	10.10.10.33-10.10.10.62	255.255.255. 224
IT	10.10.10.65-10.10.10.94	255.255.255. 224
Sales	10.10.10.97-10.10.10.126	255.255.255. 224
Finance	10.10.10.129-10.10.10.158	255.255.255. 224
<b>Branch Office</b>		
<b>Machine</b>	<b>IP Address (Range)</b>	<b>Subnet Mask</b>
RODC	192.168.1.5	255.255.255. 224
VPN	10.10.10.101 (Adapter 1) 192.168.1.2 (Adapter 2)	255.255.255. 224
Read-Only DNS	192.168.1.3	255.255.255. 224
Printer	192.168.1.11	255.255.255. 224

#### 4.3.2. Sub netting

Sub net is short form of sub network and as the name suggest, it is process of making smaller network from larger network. By dividing large IP address into smaller group, it limits broadcast from slowing down the network. Hence, to satisfy the business requirement and enhance network performance 255.255.255.224 subnet mask has been used in designed network.

#### 4.3.3. User

Necessary user accounts will be created and maintained in active directory.

#### 4.3.4. Organizational Units and Groups

OU/Group	IP Distribution	Subnet Mask
HR	192.168.1.33-192.68.1.62	255.255.255. 224
IT	192.168.1.65-192.68.1.94	255.255.255. 224
Sales/Marketing	192.168.1.97-192.68.1.126	255.255.255. 224
Finance	192.168.1.129-192.68.1.158	255.255.255. 224

#### 4.3.5. Rights and Policies

OU/Group	Rule	Description
Marketing	Logon Time	Set Logon hour to ensure user can only access system during specified hours.



	Logon Script	Run scripts to install necessary applications required by user.
	Access Right	Grant access to necessary resources and prevent accessing unnecessary information.
HR	Logon Time	Set Logon hour to ensure user can only access system during specified hours.
	Logon Script	Run scripts to install necessary applications required by user.
	Access Right	Grant access to necessary resources and prevent accessing unnecessary information.
IT	Logon Time	Set Logon hour to ensure user can only access system during specified hours.
	Logon Script	Run scripts to install necessary applications required by user.
	Access Right	Grant access to necessary resources and prevent accessing unnecessary information.
Sales	Logon Time	Set Logon hour to ensure user can only access system during specified hours.
	Logon Script	Run scripts to install necessary applications required by user.
	Access Right	Grant access to necessary resources and prevent accessing unnecessary information.
Finance	Logon Time	Set Logon hour to ensure user can only access system during specified hours.
	Logon Script	Run scripts to install necessary applications required by user.
	Access Right	<ul style="list-style-type: none"> <li>• Grant access to necessary resources and prevent accessing unnecessary information.</li> <li>• Prevent access to internet</li> </ul>

#### **4.4.Design Solution**

Network design for the solution is drawn here below in another page.



#### **4.5.Recommendations**

This document designed network infrastructure for Prabhu bank by identifying and utilizing required server and security technologies. Use of technologies and devices used in network has been accessed and demonstrated the reason behind selection. Now, after designing network infrastructure, it is necessary to practice right methods to implement the design. It is always nice to prepare system development plan for designing and implementing a system. Additionally, it is always a good practice to keep interaction with Prabhu bank to understand change in requirements. And finally, testing design in virtual system is nice practice before implementing design into real word.

#### **4.6.References**

- Cisco (N.D) *Cisco 2900 Series Integrated Services Routers* [Online] Available: <http://www.cisco.com/c/en/us/products/routers/2900-series-integrated-services-routers-isr/index.html> Accessed [10/16/2015]
- Cisco, N.D.) *Cisco Catalyst 2960-X Series Switches* [Online] Available: <http://www.cisco.com/c/en/us/products/switches/catalyst-2960-x-series-switches/index.html> Accessed [10/16/2015]
- Hoffman, C. (n.d.) *what is a Windows Domain and How Does It Affect My PC* [Online] Available: <http://www.howtogeek.com/194069/what-is-a-windows-domain-and-how-does-it-affect-my-pc/> Accessed [10/16/2015]
- SERVERBRAIN (2013) *upgrading-2003-to-2008* [Online] Available: <http://www.serverbrain.org/upgrading-2003-to-2008/its-features.html> Accessed [10/16/2015]
- Technopedia (N.D) *Routing and Remote Access Service (RRAS)* [Online] Available: <https://www.techopedia.com/definition/3424/routing-and-remote-access-service-rras> Accessed [10/16/2015]

**Task 5**

**Evaluate** addressing and deployment solutions for a given networked environment. [2.2, D1]

**5. Introduction**

To implement designed network infrastructure plan proper addressing and deployment technologies and components are required to be collaborated. This document evaluates addressing solution as well as deployment solution for designed network.

**5.1. Addressing****5.1.1. Identification of devices and resources**

Given network design consists of various devices and resources. In order to access those resources, network needs to be able to identify them. Each device needs to have unique identification so that user can access them without causing any conflicts in system. Just like we need email address to send email to specific person, network use unique identifier to send data to specific computer, Crawford (n.d.). In most network these days including proposed network design uses TCP/IP protocol as communication standard. In this protocol IP address is used as unique identifier.

Given network design has allocated unique IP addresses to its devices and resources so that it can be identified. Specific resource can be accessed using IP address given that user has required rights and privilege. For example, printer in branch office is given IP address of 192.168.1.11. Other computers with in the same LAN can access this resources using given IP address. Similarly, IP address is used for identifying other devices and resources to manage network.

Given network uses both static IP address as well as static IP address. Server computers such as DC, printers, VPN etc. are given static IP which does not changes automatically. And client computers are given dynamic IP address.

**5.1.2. Naming methodology**

Instead of using only IP address to identify resource and device within the network, user friendly name can also be used. For this IP address of specific device needs to be translated into name so that device can be identified using that name. With this technology, resources with in network can be identified and accessed using friendly names instead of IP addresses.

To translate IP address to name and name to IP address, given network design has DNS server system. With DNS server network has fast name conversion and resources are given user friendly names that

are easier to remember. For example, a device in network has IP address of 10.10.10.10. To access same device user can use FQDN of client1.bank.prabhu.com.

#### 5.1.3. Positive aspects

1. For effective and consistent performance, server computers are given static IP.
2. In given network, IP addresses are properly distributed to client devices and resources dynamically using DHCP server.
3. With help of DNS server, resources in the network can be access using both IP address or corresponding name.

### 5.2.Deployment

Various aspects of network environments such as scalability, adaptability, used technologies and devices, supportive of environments are need to studied and analyzed in order to evaluate deployment for given network.

#### 5.2.1. Scalability

Scalability of network defines ability to handle growth in amounts of resources and services. It is very important aspect of any network design. Scalability allows system to add more resources without any sacrifice in performance. Scalability of a system can be studied using various elements such as number of users, computers, branch, GPO allowed etc.

##### A. **Number of users**

Prabhu bank has around 250 total numbers of user accounts including administrator over all 90 branches. This number can be increased over years as bank would have more employees and users which will require individual user accounts for them. Current active directory environment supports large number of user accounts creation.

##### B. **Number of resources**

With growth of business, organization will have more computers and other resources like printers. Given network environment has capability to support additional resources. Network infrastructure such as wires, switches etc. in current environment allows increase or reduce number of resources.

### **C. Number of Branch**

Current network system is designed to support 90 branches including ATM centers. System can support additional number of branches with help of more ADC and child DCs. Branch office can connect to main office using VPN tunnel for secure connection.

### **D. Number of GPO applied**

Group policy object is enforced to users, groups, OUs to apply rules. Scalability in number of GPO means number of policy object that can be applied to user or group. Windows server supports up to 999 group policy object in a user. This means administrator has ability to increase number of GPO applied for any specific user or group as required.

#### **5.2.2. Adaptability**

Adaptability in network infrastructure describes environmental capability to support changes in services. It describes how much a system can adapt if new service is introduced or existing system is replaced or removed. For example, given network environment has read only DNS servers which means naming system can still be working if connection to main DNS server is broken. System is able to adapt according to requirement. Main office can connect to its branch offices using dial up connection if necessary. But this option is less secure and effective.

Similarly, network design is capable of adapting to new services such as email service, application services etc. Additionally, use of read only domain controller ensures user can still access the domain in branch offices if connection to main DC is broken.

#### **5.2.3. Commercial requirements**

Prabhu bank organizational has various commercial requirements that are need to be considered while designing and deploying networking environments. Evaluation of development needs to be based on these requirements. Below are some of the commercial requirements of Prabhu bank.

- a. Fast Services
- b. Extended coverage with VPN
- c. Security
- d. Central Data Management

Proper use of domain based network, security policies and VPN tunneling services in the proposed design allows to achieve above requirements. Bank network should be able to provide fast and secure service. Central domain computer allows to manage whole network centrally.

#### 5.2.4. Use of Technology

Various technologies are used while deploying given network environment. Study of such technologies in the system will help the evaluation of deployment all together.

##### 5.2.4.1. Domain Based Network

Given network environment is designed in domain based technology. Network has at least one dedicated computer as domain controller. Active directory in DC stores user accounts that allows user to use different computer. User account for VPN, DNS, Print Server, DHCP server are manage centrally. Here are some benefits of using domain based network for given environment.

1. User accounts and groups are managed centrally
2. Various permission rules and access policies are enforced to secure bank network.
3. VPN and DNS service is supported by Domain controller.
4. As client computer has very limited ability, less security threats composed.

##### 5.2.4.2. Internet

Internet is global network system that interconnects millions of computers. There are billions of user of Internet mainly use Internet for mailing, gaining information, chatting etc. Designed network uses Internet to connect with its remote branches. Through VPN connection branch offices are able to connect with main office securely. Once connected, they work as if they are connected locally.

#### 5.2.5. Supportive of environments

Prabhu bank has existing workgroup based network. This network mainly has windows based computers and has windows 7 or later operating system installed. Given environment is designed to support windows based system as it has Microsoft windows server as domain controller. Existing computers from workgroup can be reused in domain network. This will reduce deployment cost and will be effective solution.

#### 5.2.6. Change Management

Change management is approach to deal with various changes occurred in the organization. In other word it is ability to adapt to change in the environment. Prabhu bank needs to plan change management to ensure network sustainability. To improve security and performance of the system, various changes

needs to be made in the system. Change can be made on services, servers, devices etc. For Prabhu bank following changes are recommended:

- System should use IPsec policy to ensure data encryption between server and client communication
- IIS server should be installed to run banking application over web throughout the network
- To ensure Physical security, organization should implement suitable security system

Employees of the bank are trained to use workgroup based network. Moving to domain based network can create complications and hence can cause negative impact on productivity of the bank. To deal with such threats, following change management plans can be implemented.

- Running training program to aware staff about Domain network and its advantages over workgroup based network would motivate staff to learn domain based network.
- Running domain based network training for staff would help staff learn new system

### **5.3.Summary**

Addressing and Deployment for given environment is evaluated in this document. In addressing section, technologies used for identifying resources and devices in network are evaluated. Current system uses IP addressing to identify devices in the network. Use of DNS Server allows IP to name conversion. This means resources can be identified and access using both IP address and their human friendly names.

Deployment of the network environment is evaluated based on various criteria. Scalability evaluates changes in size of network supported by environment and adaptability evaluates ability to deal with service changes in environment. Evaluation shows given network design has ability to adapt to size and service changes. Furthermore, this document evaluated various technologies and required change management plan required to successfully deploy given network design environment.

### **5.4.References**

Crawford, S (n.d.) <http://computer.howstuffworks.com/internet/basics/question549.htm>





## Task 6

**Evaluate** the rights and security requirements for a given networked environment. [2.3, D3]

### 6. Introduction

Implementation of necessary rights and security measurement is very important phase during deployment of any network infrastructure environment. Often people forget to give necessary focus to analyze and evaluate required components leaving them vulnerable to various security threats. Such threats includes data loss, data theft, viruses etc. To eradicate such security threats in the network, analyst must evaluate security measurements. This includes identifying right and security policies for the network. This document further identifies and evaluates right and security requirements for the proposed network environment.

### 6.1.Right and Security Requirements

#### 6.1.1. Access to Files and Directory

It is necessary to manage security of file and directory. It is procedure to define what a user can do with particular document. In network environment of bank it is must to control user access to critical information. User of one department must not have access to documents of other documents. Similarly, general users should not be able to modify shared information.

In given network environment, administrative group or user account have full control shared files and folders. Whereas, some directory or file gives only partial permission to some users or groups. Only administrator user are able to modify permission rules. For example, figure 1 demonstrate how finance user has only read permission on shared folder. In this account tries to access and modify files from this particular shared directory, he/she will be denied as shown in figure 2 below.

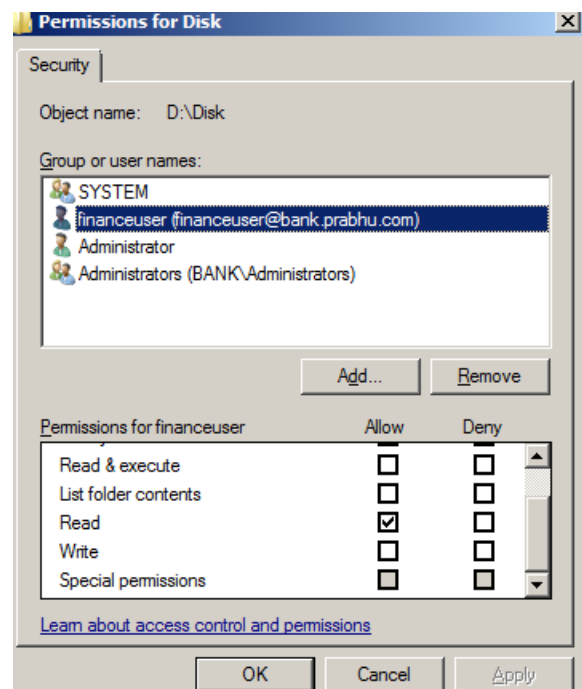
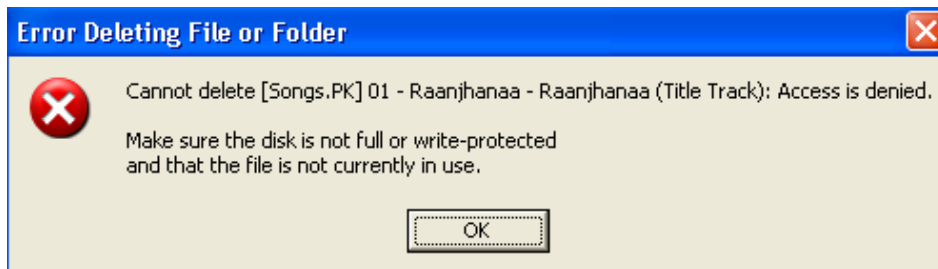


Figure 14 Permission for directory



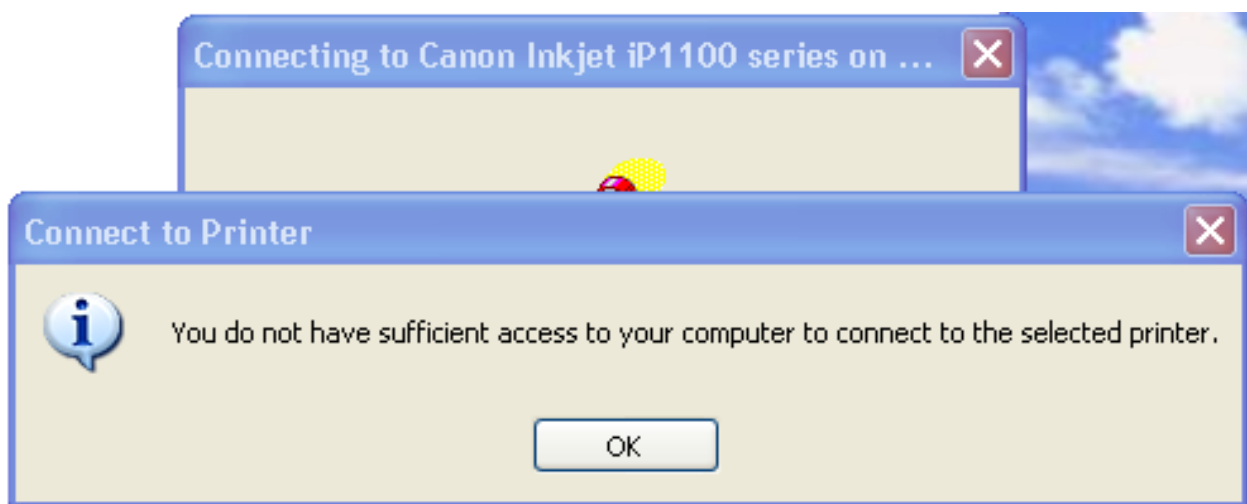
**Figure 15** Access denied to file or folder

#### 6.1.1.1. Benefits

This functionality of enforcing permission rules in files and directory allows administrator to limit user access to critical information. It forbids user to perform activities on information that are not meant to be accessed. It helps preventing disasters like data loss and data theft.

#### 6.1.2. Access to Printer

Separate printer for each division of bank is installed in network. Allowing users to access all printer in network can complicate things as he/she can accidentally send print request to wrong printer. In designed network environment printer server is used for maintaining printer access. Different groups in active directory is granted access to separate printer in network. In the printer setting specific time is configured to allow using printer.



**Figure 16** Printer access permission denied

#### 6.1.2.1. Benefits

Main benefit of enforcing printer access rules is to protect printer from being misuse. It forbids users who does not supposed to use printer from accessing the printer. It also prevents unnecessary

complications like users sending print command to wrong printer. In addition, user of time control in printer setting prevents use of printer during off hour.

### 6.1.3. Access to VPN

In given environment, VPN is used for connecting branch office with main office. It is must to secure VPN connection as it uses public path and somebody can modify the data in between. To secure VPN access both access to VPN service and VPN connection need to be secured. Current network environment allows administrator to create user with remote access ability. This allows user to access domain server remotely using VPN. Only users with remote access permission are allowed to connect through VPN.

#### 6.1.3.1. Benefit

As only user with remote access ability are allowed to connect via VPN, it enhances security of resources. Not all users from active directory are able to connect through VPN. It means administrators can allow remote access to certain user who is outside work area and needs connection to domain network. Or administrator can create VPN user for each branch so that they can connect branch with main office.

#### 6.1.3.2. Drawback

Even though VPN is secure connection method, it requires remote access policy to enhance security of connection. Given network environment has not implemented remote access policy to secure VPN connection. For that VPN server needs to have network policy server (NPS) and needs to be configured as RADIUS client. VPN tunneling protocol L2TP/IPsec should be defined as protocol for designed environment. This provides data authentication, data integrity and data confidentiality.

### 6.1.4. Group Policies

Group policy is feature that allows enforcing configuration to users and groups through domain controller. It allows administrator to run configurations based on requirements to users. In windows server 2008 group policy is enabled through group policy object (GPO). Group policy enables user or computer based configuration that means configuration done in GPO is applied to corresponding user/group or computer. Such configuration includes hiding run menu, internet setting, wallpaper setting, control panel hiding etc.

In given environment, various policies needs to be applied to users. For example, General users should not have access to control panel. This prevents general user changing computer configuration. Table below here lists some of the identified policy requirements for the given environment.

Target User/Group/Computer	Policy	Description
Account	<ul style="list-style-type: none"> <li>• Run script to open accounting software</li> <li>• Prevent internet access</li> <li>• Disable command prompt</li> <li>• Set allow lockdown</li> <li>• Max password age</li> </ul>	When user with account of account group gets logged in, script would automatically executes. Policy would disable command prompt so user cannot run batch file. If any suspicious login attempt occurs, account will be locked down. And user will have to change password at regular basis. (30 days)
All general groups	Remove Run menu Disable command prompt	Prevents general users from accessing run menu

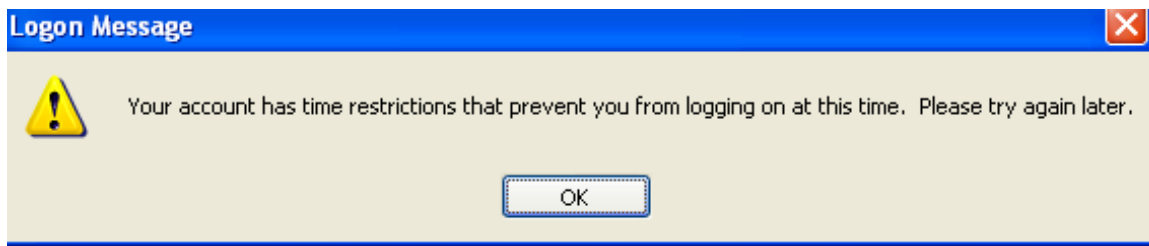
#### 6.1.4.1. Benefits of Group policy in given environment

- Client user has very limited configuration ability this means they are not allowed to install new software in the system that may potentially affect the performance of the system
- Users cannot install or run scripts means less threat of viruses and worms
- Administrator can enforce above listed policies and other policies to all domain user based on requirements
- User cannot modify network configuration that can harm the environment
- Resources security are greatly improved.
- Prevents suspicious login attempts
- Prevents Internet access which can improve productivity

#### 6.1.5. Time Based Rules

It is essential to configure security setting also based on time. Employees from day shift should not be able to login to system during night hour and vice versa. For this administrator needs to configure login hour for the user. Similarly, printers can also have time based security configuration. This forbids user from using the printer during specified time zone in configuration.

In the given environment day shift users are disabled to login during night shift. Printer time setting is also configured.



**Figure 17**system preventing login access outside logon hour

### **6.2.Evaluations Summary**

This document successfully identified and evaluated right and security requirement for the given environment. Proposed network environment has designed various right and security policies to secure the network. Such polices includes access policies, group policies and time based policies. This document evaluated how various security requirements are imposed by the network and how those requirements can be satisfied. Even though basic security requirement has been addressed within the network, for a critical network environment like bank, extensive approaches needs to be taken. Recommendation for optimizing security for the environment is given below.

### **6.3.Recommendation**

Following approaches can be taken into consideration while enhancing security of the system. Providing physical Access is always essential for any network environment. Especially for critical network, physical security is crucial. Resources, server rooms, routers, switches must be physically secured in order to optimize security of network environment itself.

It is always good practice to keep upgrading system with latest security updates, apply necessary security patches. This helps to identify and eliminate security vulnerabilities of the system. And finally, conducting awareness program for staff would improve security of the system.

**Task 8**

Critically review and test the implemented system and evaluate system and user assurance of the implemented system. [4.1, 4.2, M3]

**7. Introduction**

Testing and evaluation of critical review of implemented network infrastructure system is crucial phase. This phase helps to study strengths and weaknesses of the network and identify possible improvements. Testing phase can find misconfigurations and helps to eliminate them to achieve business requirements and optimal service quality. This document is critical review and testing documentation for implemented system. Furthermore, it also evaluates the system and user assurance.

**7.1.Critical Review****7.1.1. Introduction: Existing System**

There are several problems in existing workgroup based network system. As there is no central connection, Main office has very less control over branch office network and cannot remotely monitor the system. Each branch has their own database system hence client has to create multiple accounts for different branches which means client cannot save money in one branch and withdraw from another.

Additionally, security policies are very poor due to workgroup based network and for a sensitive institute like bank, network security level needs to be really high.

**7.1.2. Body: Positive Aspects of Implemented system**

Network Infrastructure system for Prabhu bank is designed to solve business requirements. This system utilizes various technologies and services that support network infrastructures. To abandon Workgroup based network and problems caused by such network, new implemented system is domain based network. It has domain controller with active directory installed, a technology essential for domain network. Domain controller stores user account information, groups, organizational unit's information in active directory. Additionally, domain controller enforces policies, helps other server technologies, and helps to utilize network resources.

Implemented network design uses DHCP that can distribute IPs to clients dynamically. Other server technologies in system have their own benefits. DNS server in network resolves IP address to text based friendly name, allowing access to resources using friendly names instead of IP address. Printer server allows to manage various printers and accessibility to those printers. Network is designed to use VPN technology to connect main office with branch offices. This connection is made through VPN tunnel which is a very secure way of connecting two offices. For the security of network resources, various

rights and rules are implemented. IPs are properly sub netted according to requirements, this enhance both network security and performance.

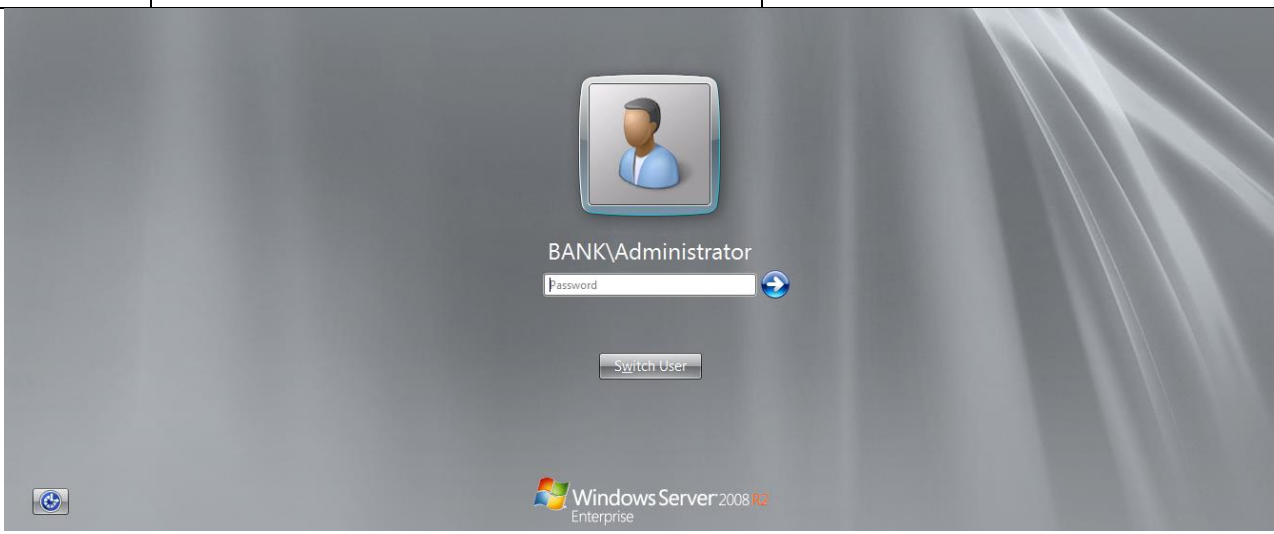
At last, network design uses highly manageable switches and routers which allows to customize the configuration according to requirements. Use of proper hardware based firewall enhances security of network.

### 7.1.3. Limitations

Even through this network design is able to satisfy business requirements, it also has some limitations. Network security policy is not implemented for VPN service at VPN server. This forbids VPN connection with optimal security. Additionally, this system does not have Mail Servers and Application Server which limits networks functionality. If bank decides to run its own mailing system and run server based business application, network would require these servers.

### 7.2. Testing of Implemented system

Designed network environment for Prabhu bank is implemented. Before running banking service through this network it is necessary to thoroughly test the system to find any inaccuracy in the system. This document now tests various components of implement system. Test result will be analyzed to identify if server technologies utilized in network are functioning right or not. If any problem found it will be recorded in log for maintenance.

<b>What was tested: <i>Domain Controller Configuration</i></b>		<b>Date: 10/17/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>
1.	Should allow login to BANK domain	Allowed to login to domain
		



2.	System properties should show domain as bank.prabhu.com	Properties showed domain as bank.prabhu.com
----	---	---

## System

Processor: Intel(R) Core(TM) i3-2310M CPU @ 2.10GHz 2.10 GHz  
 Installed memory (RAM): 512 MB (511 MB usable)  
 System type: 64-bit Operating System  
 Pen and Touch: No Pen or Touch Input is available for this Display

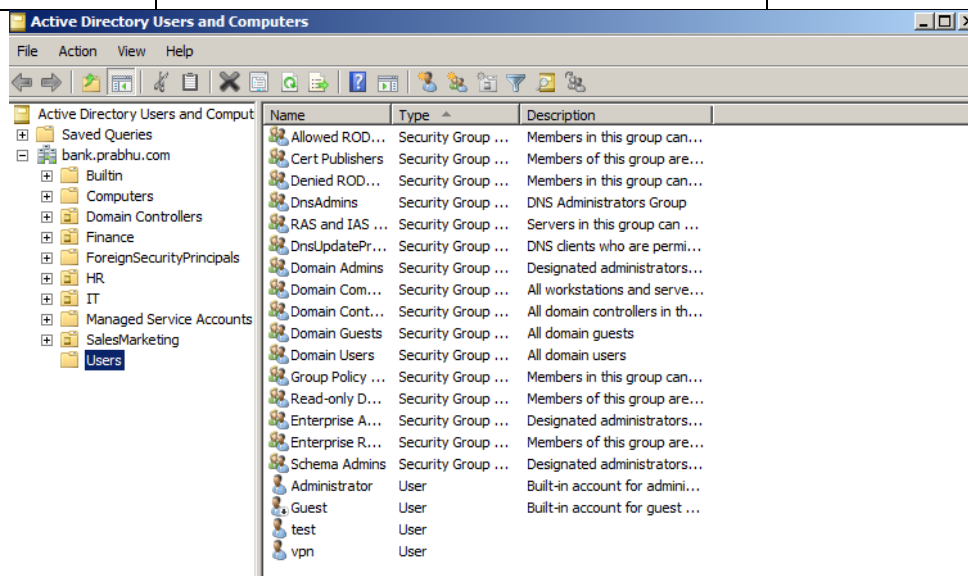
## Computer name, domain, and workgroup settings

Computer name: WIN-ESD938JO  
 Full computer name: WIN-ESD938JO.bank.prabhu.com  
 Computer description:  
 Domain: bank.prabhu.com


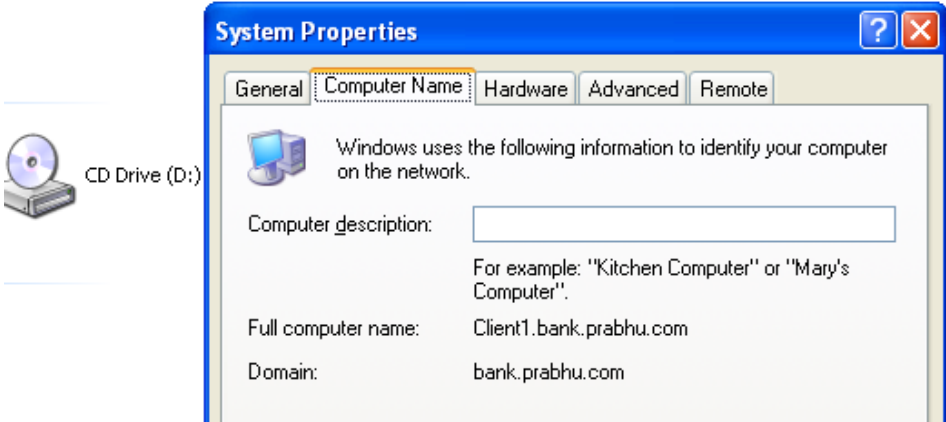
## Windows activation

Windows is activated  
 Product ID: 00486-OEM-8400691-20006

3.	Active directory users and computers (DSA.MSC) should show all groups, user, computers, OUs of domain	DSA.MSC displayed existing users, groups, OUs of domain and allowed to create and maintain new user accounts
----	---	--

**Analysis:**

Test of **Domain Controller Configuration** showed positive results. All result delivered expected output. Admin was allowed to access domain system, properties showed right domain name and DC has active directory installed correctly. This means domain controller is configured correctly.

<b>What was tested: DC Member configuration</b>		<b>Date: 10/17/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>
1.	Member should able to login to domain network	Member successfully logged into domain
		
2.	System properties should show domain as bank.prabhu.com	Domain of member is showing as bank.prabhu.com
		
<p><b>Analysis:</b></p> <p>Test of <b>Domain Controller member Configuration</b> showed positive results. All result delivered expected output. Member was allowed to access domain system, properties showed right domain. This means domain controller member is configured correctly.</p>		
<b>What was tested: DNS SERVER Configuration</b>		<b>Date: 10/17/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>
1.	NSLOOKUP tool should show IP address and FQDN of the network	Showed FQDN of DC and corresponding IP address

**Administrator: Command Prompt - NSLOOKUP**

```
C:\>NSLOOKUP
Default Server:  win-esdtdo9j8jo.bank.prabhu.com
Address:  10.10.10.1
> _
```

- |    |   |  |
|----|---|--|
| 2. | Should allow to ping other resources using both IP and corresponding text-based friendly name | Supported pinging client computer using name and IP. |
|----|---|--|

**Administrator: Command Prompt**

```
C:\>ping client1.bank.prabhu.com

Pinging client1.bank.prabhu.com [10.10.10.10] with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Administrator: Command Prompt**

```
C:\>ping 10.10.10.10

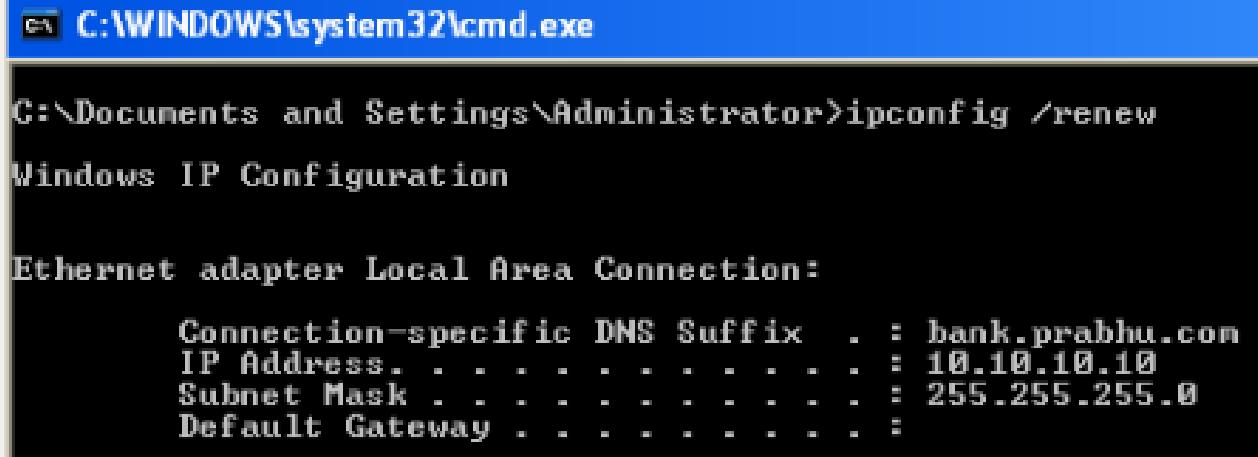
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time=2ms TTL=128
Reply from 10.10.10.10: bytes=32 time=2ms TTL=128
Reply from 10.10.10.10: bytes=32 time=3ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

**Analysis:**

Test of DNS showed positive results. All result delivered expected output. Both IP address and name could be used for accessing the resources. It showed successful IP to name conversion. Hence, it shows DNS configuration is correct in developed system.

<b>What was tested: <i>DHCP IP Distribution Configuration</i></b>		<b>Date: 10/17/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>
1.	DHCP member should get IP address dynamically using IPCONFIG /Release and IPCONFIG /Renew	Client obtained dynamic IP from DHCP



```

C:\WINDOWS\system32\cmd.exe

G:\Documents and Settings\Administrator>ipconfig /renew

Windows IP Configuration

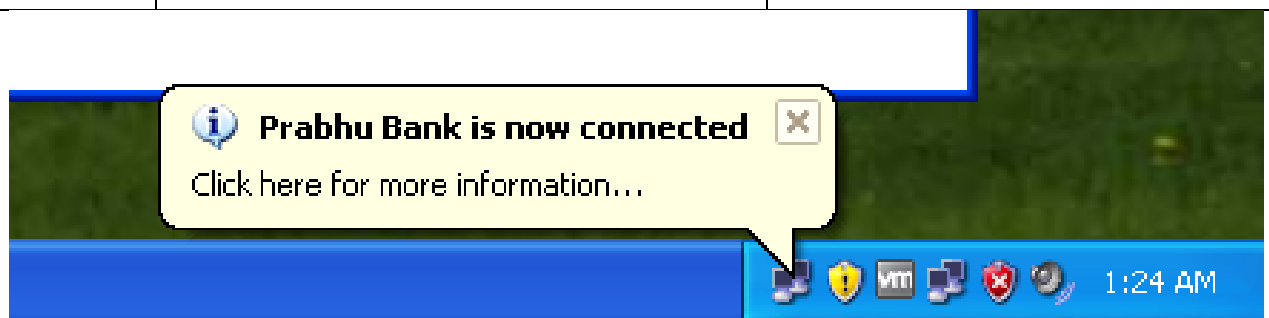
Ethernet adapter Local Area Connection:

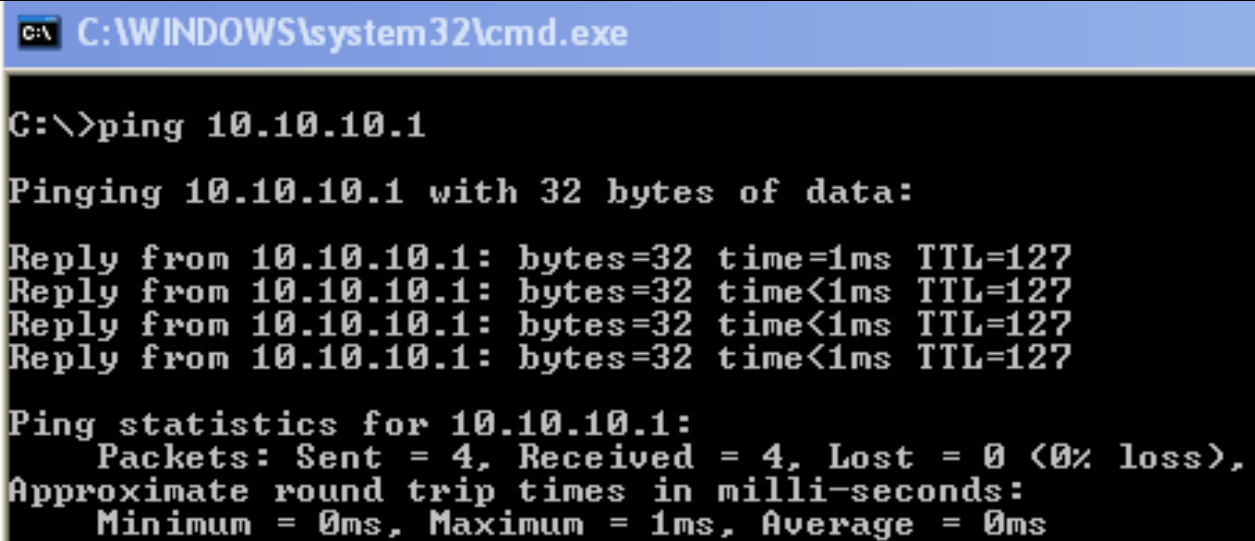
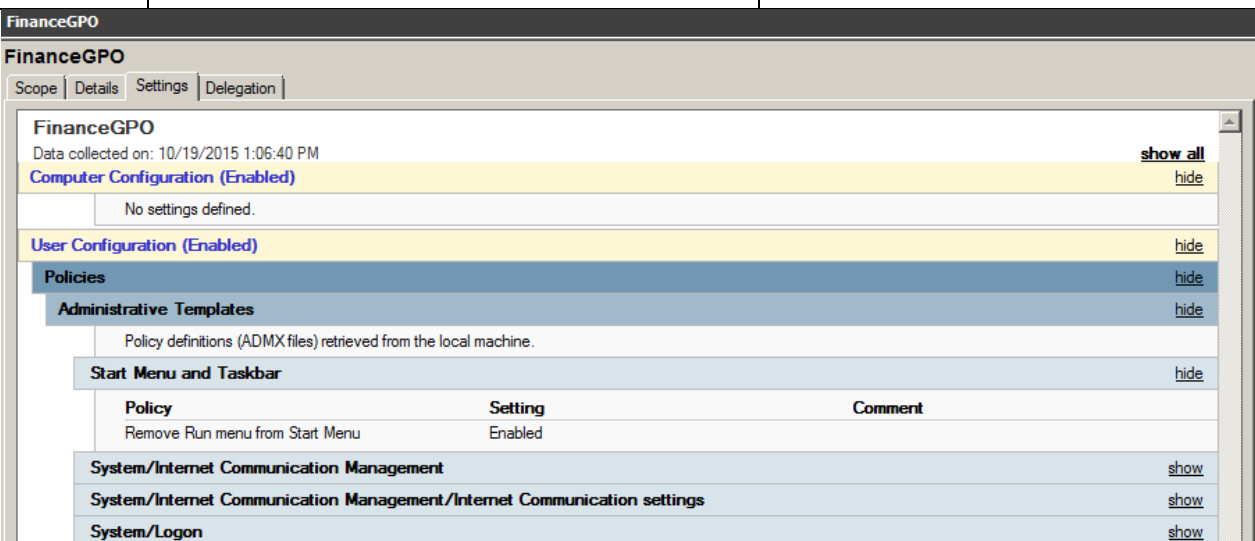
    Connection-specific DNS Suffix  . : bank.prabhu.com
    IP Address. . . . .               : 10.10.10.10
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         :
  
```

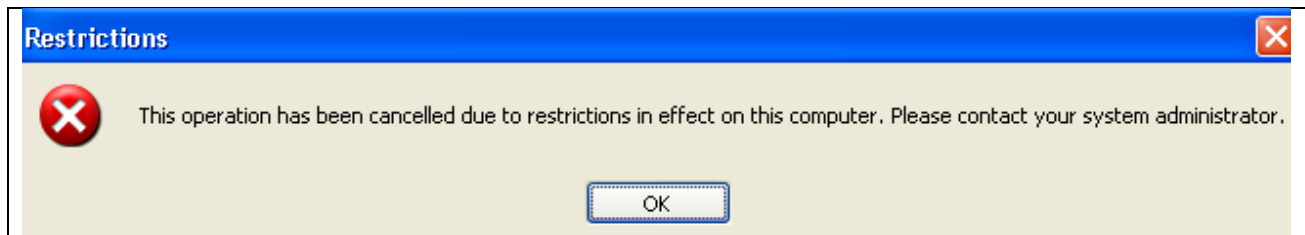
**Analysis:**

Test of **DHCP** showed positive results. Result delivered expected output. Client was able to run IPCONFIG /release and IPCONFIG /Renew command to obtain dynamic IP. This shows DHCP configuration is successful in the system.

<b>What was tested: <i>VPN Connection configuration</i></b>		<b>Date: 10/17/2015</b>
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>
1.	User should able to successfully connect to VPN SERVER remotely	Connected through VPN server Successfully

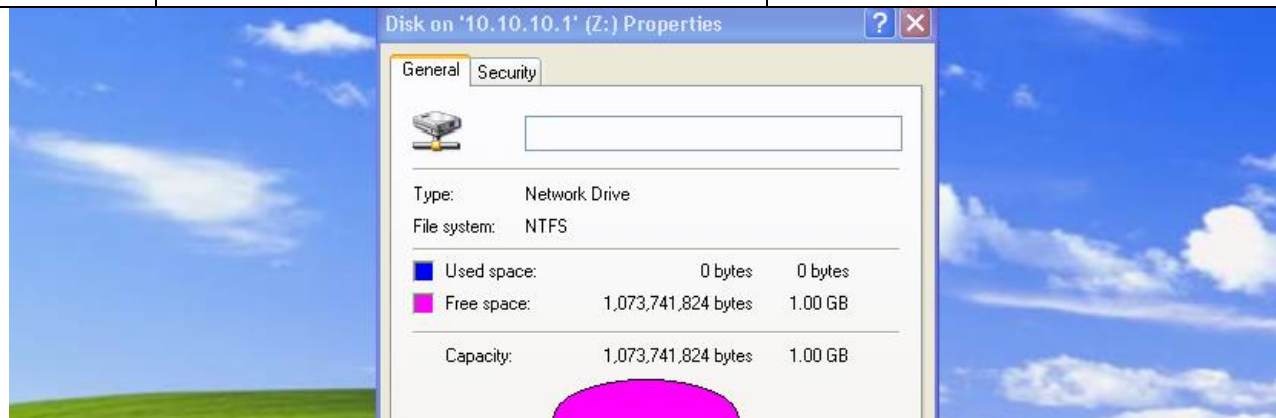


2.	Connected machine should able to ping Domain network	Successfully pinged DC						
 <pre> C:\&gt;ping 10.10.10.1  Pinging 10.10.10.1 with 32 bytes of data:  Reply from 10.10.10.1: bytes=32 time=1ms TTL=127 Reply from 10.10.10.1: bytes=32 time&lt;1ms TTL=127 Reply from 10.10.10.1: bytes=32 time&lt;1ms TTL=127 Reply from 10.10.10.1: bytes=32 time&lt;1ms TTL=127  Ping statistics for 10.10.10.1:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 1ms, Average = 0ms </pre>								
<b>Analysis:</b> Test of <b>VPN configuration</b> showed positive results. Result delivered expected output. Client was able to remotely connect to VPN server and ping the system. This shows VPN configuration is successful in the system.								
<b>What was tested: Policies Configuration</b>		<b>Date: 10/17/2015</b>						
<b>S.N.</b>	<b>Expected Output</b>	<b>Actual Output</b>						
1.	Group policy management should show all policies Enabled	Group policy management shows all policies						
 <p><b>FinanceGPO</b></p> <p>Scope   Details   Settings   Delegation</p> <p><b>FinanceGPO</b> Data collected on: 10/19/2015 1:06:40 PM</p> <p><b>Computer Configuration (Enabled)</b> <a href="#">show all</a> <a href="#">hide</a></p> <p>No settings defined.</p> <p><b>User Configuration (Enabled)</b> <a href="#">hide</a></p> <p><b>Policies</b> <a href="#">hide</a></p> <p><b>Administrative Templates</b> <a href="#">hide</a></p> <p>Policy definitions (ADMX files) retrieved from the local machine.</p> <p><b>Start Menu and Taskbar</b> <a href="#">hide</a></p> <table border="1"> <thead> <tr> <th>Policy</th> <th>Setting</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>Remove Run menu from Start Menu</td> <td>Enabled</td> <td></td> </tr> </tbody> </table> <p><b>System/Internet Communication Management</b> <a href="#">show</a></p> <p><b>System/Internet Communication Management/Internet Communication settings</b> <a href="#">show</a></p> <p><b>System/Logon</b> <a href="#">show</a></p>			Policy	Setting	Comment	Remove Run menu from Start Menu	Enabled	
Policy	Setting	Comment						
Remove Run menu from Start Menu	Enabled							
2.	Policy should enforce rule e.g. finance user should not have run menu	Finance user does not have run menu						

**Analysis:**

Test of **policy configuration** showed positive results. Result delivered expected output. Group policy management showed implemented group objects. Other test showed policy is configured correctly as policy enforced to user worked correctly.

What was tested: <i>Disk Quota Configuration</i>		Date: 10/18/2015
S.N.	Expected Output	Actual Output
1.	User should only have 1 GB of disk quota	Mapped network drive showed only 1 GB space

**Analysis:**

Test of **Disk Quota Configuration** showed positive results. Result delivered expected output. Properties of disk showed 1 GB size. This means disk quota is configured correctly.

What was tested: <i>Logon Hour Configuration</i>		Date: 10/18/2015
S.N.	Expected Output	Actual Output
1.	IT_DAY_GROUP member should only able to login within specific day time. (Monday-Friday)(8AM-5PM)	Display login error when tried to access after defined time in logon hour.

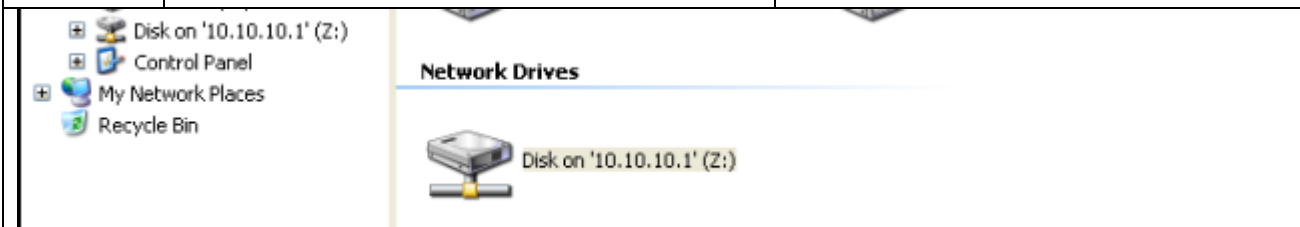
**Analysis:**

Test of **logon hour configuration** showed positive results. Result delivered expected output. User was unable to access system during denied time. This shows logon hour is configured correctly.

**What was tested:** *Map Network Configuration*

**Date:** 10/18/2015

S.N.	Expected Output	Actual Output
1.	Should able to Map network drive successfully.	Was able to map network drive.

**Analysis:**


Test of **network drive configuration** showed positive results. Result delivered expected output. User was able to map network drive successfully. This shows map drive configuration is correct.

**What was tested:** *NTFS Permission*

**Date:** 10/18/2015

S.N.	Expected Output	Actual Output
1.	Should throw error message while trying to delete document with no modify permission to the user	Threw error message and disallowed user from deleting the document

Error Deleting File or Folder

 Cannot delete [Songs.PK] 01 - Raanjhanaa - Raanjhanaa (Title Track): Access is denied.  
Make sure the disk is not full or write-protected  
and that the file is not currently in use.

OK

**Analysis:**

Test of **NTFS permission configuration** showed positive results. Result delivered expected output. User was not able to delete a document which gave only read permission to user. This shows NTFS configuration in system is successful.

### 7.3. Summary

This document completed planned test on proposed then implemented network environment for Prabhu Bank. Servers, services, policies from the network were verified through test process. Test was used for documenting all test results. To analyze the results, output from the test were analyzed with expected outputs. Test verifies the configuration of the network environment. Testing of the system assures the security of the system and its accessibility from clients. Shared resources will be utilized by clients to improve productivity of the system.