SECTION – 2

Operating System & Networking Lab

Session 1 : Network Configuration

Ex 1: Run the following commands and write the use of each command.-

Answer :

Ipconfig

C:\Documents and Settings\Administrator>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.227.1.81
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 10.227.1.1

ping

C:\Documents and Settings\Administrator>ping
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list

telnet

Microsoft (R) Windows 2000 (TM) Version 5.00 (Build 2195)
Welcome to Microsoft Telnet Client
Telnet Client Build 5.00.99206.1
Escape Character is 'CTRL+]'
Microsoft Telnet>

diskperf

C:\Documents and Settings\Administrator>diskperf
1 Physical Disk Performance counters on this system are currently set to start At boot.

netdiag

C:\Documents and Settings\Administrator>netdiag
'netdiag' is not recognized as an internal or external command,
operable program or batch file.

netstat

C:\Documents and Settings\Administrator>netstat
Active Connections
Proto Local Address Foreign Address State
TCP Amb:1208 72.20.27.115:8080 SYN_SENT
TCP Amb:2380 105.173.200.246:microsoft-ds SYN_SENT
TCP Amb:2381 17.43.237.130:microsoft-ds SYN_SENT

pathping

C:\Documents and Settings\Administrator>pathping
Usage: pathping [-n] [-h maximum_hops] [-g host-list] [-p period]
[-q num_queries] [-w timeout] [-t] [-R] [-r] target_name

ftp

C:\Documents and Settings\Administrator>ftp
ftp>

sfc

C:\Documents and Settings\Administrator>sfc
Microsoft(R) Windows 2000 Windows File Checker Version 5.00
(C) 1999 Microsoft Corp. All rights reserved
Scans all protected system files and replaces incorrect versions with correct Microsoft versions.
SFC [/SCANNOW] [/SCANONCE] [/SCANBOOT] [/CANCEL] [/ENABLE] [/PURGECACHE]
[/CACHE SIZE=x] [/QUIET]

nbtstat

C:\Documents and Settings\Administrator>nbtstat
Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP).

rcp

C:\Documents and Settings\Administrator>rcp
Copies files to and from computer running the RCP service.

lpr

C:\Documents and Settings\Administrator>lpr
Sends a print job to a network printer Usage: lpr -S server -P printer [-C class] [-J job] [-o option] [-x]
[-d]

filename

tracert

C:\Documents and Settings\Administrator>tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

nslookup

C:\Documents and Settings\Administrator>nslookup
*** Default servers are not available
Default Server: UnKnown
Address: 127.0.0.1

route

C:\Documents and Settings\Administrator>route
Manipulates network routing tables.

lpq

C:\Documents and Settings\Administrator>lpq
Displays the state of a remote lpd queue.
Usage: lpq -Sserver -Pprinter [-l]

net session

C:\Documents and Settings\Administrator>net session
There are no entries in the list.

drivers

C:\Documents and Settings\Administrator>drivers
'drivers' is not recognized as an internal or external command, operable program or batch file.

nettime

C:\Documents and Settings\Administrator>nettime
'nettime' is not recognized as an internal or external command, operable program or batch file.

rsh

C:\Documents and Settings\Administrator>rsh
Runs commands on remote hosts running the RSH service.
RSH host [-l username] [-n] command
host Specifies the remote host on which to run command.

chkdsk

C:\Documents and Settings\Administrator>chkdsk
The type of the file system is FAT32.
Volume HCL created 22/08/2002 5:53 PM
Volume Serial Number is 3A51-1906
Windows is verifying files and folders...
File and folder verification is complete.
Windows has checked the file system and found no problem.
39,058,992 KB total disk space.
1,287,888 KB in 734 hidden files.
53,440 KB in 3,223 folders.
22,328,464 KB in 67,626 files.
15,389,184 KB are available.
16,384 bytes in each allocation unit.
2,441,187 total allocation units on disk.
961,824 allocation units available on disk.

hostname

C:\Documents and Settings\Administrator>hostname Amb

net account

C:\Documents and Settings\Administrator>net account
The syntax of this command is:
NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP | HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION | SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW]

Ex 2: Use **arp** command to find your Ethernet physical address.

Answer :

arp

C:\Documents and Settings\Administrator>arp
Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
Example:

> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.

Ex 3: Modify the routing table using **ipxroute.**

Answer :

C:\Documents and Settings\Administrator>ipxroute
NWLink IPX Routing and Source Routing Control Program v2.00
Unable to open transport \Device\NwlnkIpx.

Ex 4: View the TCP/IP settings.

Answer :

Show tcp/ip
netsh>show mode tcp/ip
online

Ex 5: Configure interfaces.

Answer :

Configure interfaces:
netsh>set
The following commands are available:
Commands in this context:
set machine - Sets the current machine on which to operate.
set mode - Sets the current mode to online or offline.
netsh>set interface
The following command was not found: set interface.
netsh>set mode interface
'mode' is not an acceptable value for 'interface'.
The parameter is incorrect.
netsh>set mode
Usage: set mode [mode=] { online | offline }
Parameters:
Tag Value
mode - One of the following values:
online: Commit changes immediately
offline: Delay commit until explicitly requested
Remarks:
Sets the current mode to online or offline.
netsh>set machine

Session 2 : Linux / Unix Operating System

Ex 11: First try to execute the following commands on your operating system and write down the results and use of each command.

Answer :

Ls aa ab abc agm rajesh biju sem2
Pwd home\sem
Ls –x a1 a2 a.c agm a.out desktop frmstat.ui install.log
Ls –al drwxr-x- - 33 root root 4096 oct 2 10:12 .
drwx—xr-x 33 root root 6 oct 2 10:42 a1
-rw-r- -r-- 33 root root 5 oct 2 12:30 a2
-rwxr-x— 33 root root 4 oct 2 12:45 a.c

Ex 13: Make your own subdirectories called uni and linu in your home directory, Made? Ok, now delete the subdirectory called uni.

Answer :

Mkdir uni
Mkdir linu
Rmdir linu

Ex 14: Create a file called ignou.txt that contains the words "hello I am student of IGNOU". Now copy this file and paste to other director. Copied? Can you move the file also from one directory to another?

Answer :

Cat > ignou.txt
Cp ignou.txt \ab\a.txt
Mv ignou.txt \linu

Ex 15: In the previous question you have a file ignou.txt; change its permission to rwxrwxr-x. You can try different possibilities to changes in its permissions. One possibility may be rwxr-xr-x permissions. Find out what are the different commands available that can be used to change the permissions of a file/files.

Answer :

Chmod a+x ignou.txt
Chmod g-w ignou.txt
Chmod o-w ignou.txt

Ex 19: Change your password and write down the restrictions for given password.

Answer :

Passwd
Enter new password:
Re enter new password:
Restrictions to password
1.different from previous password
2.Have atleast 6 characters
3.Are not common words found in dictionary

Session 3 : Linux / Unix Operating System

Ex 21: Find the files (with full path) in your home directory those name are starting with the character 's' and redirect the output into a file redirecting.txt and if you receive any error message on execution of the command redirect into errors.txt.

Answer : **Ls –l s* >redirecting.txt**

Ex 22: Execute sleep 25 in the foreground, suspend it with Ctrl-z and then put it into the background with bg. show all process running in background, bring any process back into the foreground with fg. Repeat the same exercise using kill to terminate the process and use & for sending into background. (You need to see different options of the kill command)

Answer : **Sleep 25 –s**

Ex 24: Write a shell script, which returns the PID of a process and accept the name of the process.

Answer :

Ps e | grep init
Echo $a | cut –f1 –d " "

Ex 25: Use ping to find the round-trip delay to www.ignou.ac.in

Answer : Use ping to find the round-trip delay to www.ignou.ac.in
Ping "www.ignou.ac.in"

Ex 26: Send a message to all users which are online. Make provision so that you can send messages to other users but others cannot. Use talk to send messages.

Answer : **Mesg n**

Ex 28: Send a mail to yourself, and include ignou.txt inside the mail. Read the mail you have sent to yourself. Save the piece of message and file into some folder. Reply to yourself.

Answer :

Mail root(user 1) ->
Mail amb(user 2)

Ex 30: Use the ls command and grep to display all names starting with "s".

Answer : **Ls|grep[^s]**

Session 4 : System Administrator Using Unix & Linux

Ex 33: Delete the user, which just now you have added.

Answer : **Deluser abc**

Ex 38: Write a message to inform all users that "they should shut down their machine after completing the lab exercises".

Answer : **Wall "they should shut down their machine after completing the lab exercise"**

Session 5 : Windows 2000 : Introduction to Networking

Ex 42: Add different users and groups. Also configure their permissions.

Answer :

To add a new user to the computer

1. Open Users and Passwords in Control Panel.
2. Click **Add**.
3. Follow the instructions on the screen.

Notes

· You must be logged on as an administrator or a member of the Administrators group to use Users and Passwords.

· To open a Control Panel item, click **Start**, point to **Settings**, click **Control Panel**, and then double-click the appropriate icon.

· If the computer is part of a domain, **Add New User** gives an existing domain user permission to use the computer. If the computer is not part of a domain, **Add New User** creates a new local user.

· If the computer is part of a domain, you can only add existing domain users with Users and Passwords. To add a new local user, click the **Advanced** tab and then click the **Advanced** button. In Local Users and Groups, click **Users**, click **Action**, and then click **Create User**.

· You should not add a new user to the Administrators group unless the user will perform only administrative tasks. For more information, see Related Topics.

Types of access permissions for shares

The following types of access permissions can be applied to shared folders.

Read

Read permission allows:

o Viewing file names and subfolder names.
o Traversing to subfolders.
o Viewing data in files.
o Running program files.

Change

Change permission allows all Read permissions, plus:

o Adding files and subfolders.
o Changing data in files.
o Deleting subfolders and files.

Full Control

Full Control is the default permission applied to any new shares you create.
It allows all Read and Change permissions, plus:

o Changing permissions (NTFS files and folders only).
o Taking ownership (NTFS files and folders only).

Note

When a folder is shared, the default is to grant Full Access permissions to the Everyone group.

Ex 42 (ii): **Exercise** Install and configure a local printer

Answer :

1. Go to Settings, Printers, and start the add printer wizard.
2. Select Local Printer and Click next
3. Select the Printer Port. Say LPT1.
4. Select The Printer Manufacturer and Model.
5. Name the printer and Set to share the Printer if it has to be available in the Network.
6. After giving Location command and Print the test page. If all are ok, Finalise the setting and complete the wizard.

Ex 43: Connect and configure your computer with a Local Network Printer.

Answer :

To connect to a printer on a network

1. Open Printers.
2. Double-click **Add Printer** to start the Add Printer wizard, and then click **Next**.
3. Click **Network printer**, and then click **Next**.

4. Connect to the desired printer by:
o Searching for it in the Active Directory.
o Typing its name using the following format, or clicking **Next** to locate the printer on the network:
o Typing its URL using the following format:
5. Follow the instructions on the screen to finish connecting to the network printer.

Notes

- To open Printers, click **Start**, point to **Settings**, and then click **Printers**.
- If you are not logged on to a Windows 2000 domain running Active Directory, the option to **Find a printer in the Directory** will not be available.
- Connecting to a printer using its URL allows you to connect to printers across the Internet providing you have permission to use that printer.
- If you cannot connect to your printer using the general URL format above, please see your printer's documentation or contact your network administrator.
- You can also connect to a printer by dragging the printer from the Printers folder on the print server and dropping it into your Printers folder, or by simply right-clicking the icon and then clicking **Connect**.
- After you have connected to a shared printer on the network, you can use it as if it were attached to your computer.

Ex 45: Create a Hierarchical Directory Tree.

Answer : **Create a Hierarchical Directory Tree**

A hierarchical representation of the folders, files, disk drives, and other resources connected to a computer or network. For example, Windows Explorer uses a tree view to display the resources that are attached to a computer or a network.

Ex 46: Share any folder available in your directory, also configure its share permissions for different users.

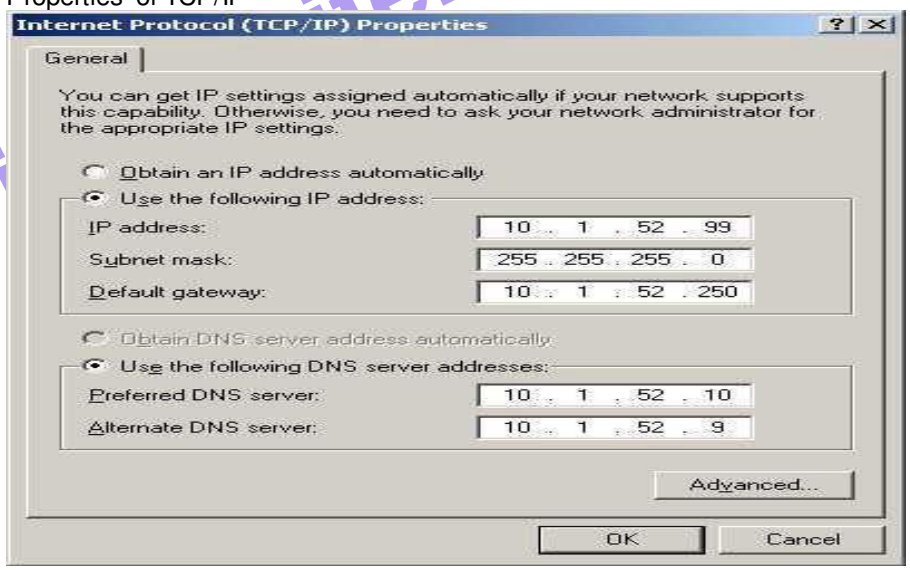
Answer : **Share and Share Permissions.**

I create a folder test uder c:\temp directry and set permissions as follows.
Take Properties of Local Area Connction

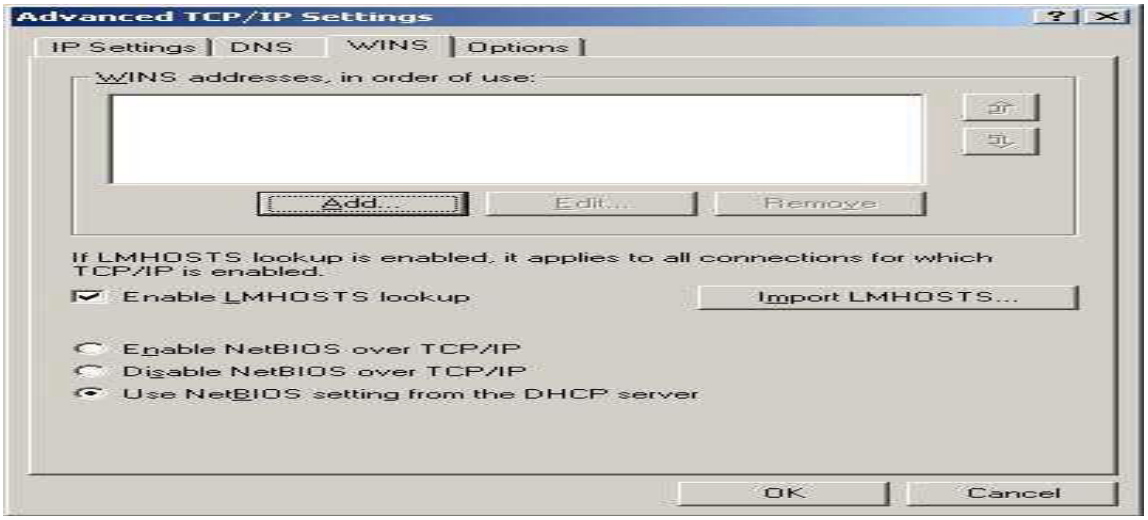
Ex 47: Install and Configure TCP/IP.

Answer : **Install and Configure TCP/IP**

Properties of TCP/IP



Enter Ip address, Subnet Mask, Default Gateway, and DNS Server entries.
Add WINS server Entries and Complete the Settings.



Ex 48: Install a caching DNS server and find out how it reduces the network traffic.

Answer : **Install a caching DNS server and find out how it reduces the network traffic**

Windows 2000 authentication is implemented in two steps: an interactive logon process and a network

authentication process. Typically, the same set of credentials is used by the interactive logon process and the network authentication process. If your credentials differ, you are prompted to provide Windows domain credentials each time you access a network resource. You can avoid this by logging on to your computer using your Windows domain name, your Windows domain user name, and Windows domain password before you try to connect to a network resource. If you log on without being connected to the network, Windows 2000 recognizes the information from a previous successful logon. You receive the message "Windows cannot connect to a server to confirm your logon settings. You have been logged on using previously stored account information." When you connect to your network, the cached credentials are passed to your Windows 2000 domain and you are able to access network resources without having to provide a password again. Limiting the number of protocols on your computer enhances network performance and reduces network traffic.

Ex 50: Implement delegated zones for a Domain Name Server.

Answer : **Implement delegated zones for a Doman Name server**

In the Macintosh environment, a logical grouping that simplifies browsing the network for resources, such as servers and printers. It is similar to a domain in Windows 2000 Server networking. In a DNS (Domain Name System) database, a zone is a sub tree of the DNS database that is administered as a single separate entity, a DNS server. This administrative unit can consist of a single domain or a domain with subdomains. A DNS zone administrator sets up one or more name servers for the zone.

Session 6 : Windows 2000 : Server Management

Ex 51-60: Install and Configure Windows 2000 Client & server.

Answer : **Configuring Windows client as VPN client**

VPN Client is an application that runs on a Microsoft® Windows®-based PC, a Sun ultraSPARC workstations, a Linux desktop, or a Macintosh (Mac) personal computer that meets the system requirements stated in the next section. In this document, the term "PC" applies generically to all these computers, unless specified otherwise. The VPN Client on a remote PC, communicating with a Cisco VPN device at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user. This secure connection is a Virtual Private Network (VPN).

System Requirements

To install the VPN Client on *any* system, you need–CD-ROM drive (if you are installing from CD-ROM) – Administrator privileges •The following table indicates the system requirements to install the VPN Client on each of the supported platforms.

Computer Operating System Requirements

Computer with a Pentium®- class processor or greater

•Microsoft® Windows® 98 or Windows 98 (second edition)

•Windows ME

•Windows NT® 4.0 (with Service Pack 6, or higher)

•Windows 2000

•Windows XP

•Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
•50 MB hard disk space.
•RAM:
–32 MB for Windows 98
–64 MB for Windows NT and Windows ME
–64 MB for Windows 2000 (128 MB recommended)
–128 MB for Windows XP (256 MB recommended) Computer with and Intel x86 processor
RedHat Version 6.2 or later Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later

Note

The VPN Client does not support SMP (multiprocessor) or 64-bit processor kernels.
•32 MB Ram
•50 MB hard disk space Sun UltraSPARC computer
32-bit or 64-bit Solaris kernel OS Version 2.6 or later
• 32 MB Ram
• 50 MB hard disk space
Macintosh computer
Mac OS X, Version 10.2.0 or later
50 MB hard disk space

The VPN Client supports the following Cisco VPN devices:
•Cisco VPN 3000 Concentrator Series, Version 3.0 and later.
•Cisco PIX Firewall, Version 6.2.2(122) or Version 6.3(1).
•isco IOS Routers, Version 12.2(8)T and later
If you are using Internet Explorer, use version 5.0, Service Pack 2 or higher.

Installation Notes

The following files are included in this release:
vpnclient-win-msi-4.6.00.0049-k9.zip Windows client MSI installer
vpnclient-win-is-4.6.00.0045-k9.zip Windows client IS installer
vpnclient-darwin-4.6.00.0045-GUI-k9.dmg Mac OS X installer
vpnclient-linux-4.6.00.0045-k9.tar.gz Linux package
vpnclient-solaris-4.6.00.0045-k9.tar.Z Solaris package
vpn3000-4.1.6.bin VPN 30xx Concentrator code
vpn3005-4.1.6.bin VPN 3005 Concentrator code
update-4.6.00.0045.zip VPN Client AutoUpdate package
Because of platform differences, the installation instructions for Windows and non-Windows platforms also differ.
The following notes are important for users who are upgrading to Windows XP and users who want to downgrade to an earlier version of the VPN Client software.
Installation Notes - Windows Platforms
Release 4.6 includes the following installation considerations for Windows users:
Installing the VPN Client Software Using InstallShield Installing the VPN Client software on Windows NT, Windows 2000, or Windows XP with InstallShield requires Administrator privileges. If you do not have Administrator privileges, you must have someone who has Administrator privileges install the product for you.

Note

The VPN Client Installer does not allow installations from a network drive (CSCeb43490).
Installing the VPN Client Software Using the MSI Installer
If you are using the MSI installer, you must have Windows NT-based products such as Windows NT 4.0 (with SP6), Windows 2000, or Windows XP.
Installing with MSI also requires Administrator privileges.
When installing the Windows MSI installation package, the user must manually uninstall the previous VPN Client if it is older than version 4.6. The version 4.6 MSI installer does not detect older versions, and the installer will attempt to install before aborting gracefully. Once a version 4.6 MSI package has been installed, future client versions will be able to detect the existing version 4.6 installation and automatically begin the uninstallation process.
VPN Client Installation Using Windows Installer (MSI) Requires Windows NT SP6 When you attempt to install the VPN Client using MSI install (vpnclient_en.exe) on NT SP3, SP4, or SP5, the error messages do not indicate
that the VPN Client cannot be installed on those operating systems because they are unsupported. Once the errors occur, no other messages are displayed and the installation is aborted.

When you attempt to run vpnclient_en.exe on Windows NT SP3, SP4, or SP5 you see the following messages:
"Cannot find the file instmsiw.exe (or one of its components). Make sure the path and filename are correct and that all the required libraries are available."
-then-
"Cannot find the file MSIEXEC (or one of its components). Make sure the path and filename are correct and that all the required libraries are available."
The Windows Installer (MSI) can be installed only on NT SP6, so the error messages you see using earlier service packs are due to an MSI incompatibility (CSCdy05049).
Installation Notes - Solaris Platforms
The following sections describe actions you must take when installing the VPN Client on a Solaris platform.
Uninstall an Older VPN Client If Present on a Solaris Platform If you have a previous version of the VPN Client running under Solaris, you *must* uninstall the older VPN Client before installing a new VPN Client.
You are not required to uninstall an old VPN Client, if one is present, *before* installing a new VPN Client for Linux or Mac OS X. Disable the ipfilter Firewall Kernel Module Before Installing the VPN Client on a Solaris Platform
If have an IP firewall installed on your workstation, the reboot after installation of the VPN Client takes an inordinate amount of time. This is caused by a conflict between the vpnclient kernel module cipsec and the ipfilter firewall module. To work around this issue, disable the ipfilter firewall kernel module before you install the VPN Client (CSCdw27781).
Using the VPN Client
•To use the VPN Client, you need –Direct network connection (cable or DSL modem and network adapter/interface card), or –Internal or external modem, and
•To connect using a digital certificate for authentication, you need a digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:
–Baltimore Technologies (www.baltimoretechnologies.com)
–Entrust Technologies (www.entrust.com)
– Netscape (www.netscape.com)
–Verisign, Inc. (www.verisign.com)
–Microsoft Certificate Services
— Windows 2000
–A digital certificate stored on a smart card. The VPN Client supports smart cards via the MS CAPI Interface.

Session 8 : Windows 2000 : Security

Ex 72: Protect client machine by using Internet Connection Firewall (ICF).

Answer : **Protect client machine by using Internet Connection Firewall(ICF)**

Windows 2000 includes a Firewall to protect your system against unwanted "visitors" from the Internet (but not controlling connections from your system to the Internet, for which you would need to install a Non-Microsoft Firewall, like ZoneAlarm), which is configured using the Properties of the modem-connection: (using the Firewall on a LAN connection will cause network access problems to your system)

In the properties of the Internet Connection : tab : Advanced.
make sure, that the checkmark is placed for the Internet Connection Firewall.
Using Settings, you can configure the firewall.
tab : Services
The list of programs, which could run on your system. By default, no access is allowed ***from*** the Internet ***to*** your system to any of these services.
Unless you need to grant such an access, do NOT activate any of these services.
tab: Security Logging
Allows to activate a log-file tab : ICMP
ICMP (Internet Control Message Protocol is part of TCP/IP, the most common use is the PING program to test a network connection.
By default, the firewall will NOT respond to any ICMP , incl. PING, from the Internet.
Advanced Setup:
In case you have the Internet Information Server (maybe including the FTP server) installed and you like to ***allow access from the Internet***, then you need to place the Check-marks (you are prompted to confirm the system allowed to be accessed) Activate ONLY the service, which people need to access from the Internet.
tab: ICMP To allow people on the Internet to test, that the connection is working to your system, you should allow incoming echo requests (PING-requests).
Warning: now your systems becomes also visible for all these "bad boys and girls", which probe all IP-addresses on the Internet and then try to find out which system they had found, and some of them may try to damage your system !

Ex 73: Configure TCP/IP packet filter.

Answer : **Configure TCP/IP packet filter**

1. Click **Start** , point to **Settings** , click **Control Panel** , and then double-click **Network and Dial-up Connections** .
2. Right-click the interface on which you want to configure inbound access control, and then click **Properties** .
3. In the **Components checked are used by this connection** box, click **Internet Protocol (TCP/IP)** , and then click **Properties** .
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Advanced** .
5. Click the **Options** tab.
6. Click **TCP/IP filtering** , and then click **Properties** .
7. Select the **Enable TCP/IP Filtering (All adapters)** check box. When you select this check box, you enable filtering for all adapters, but you configure the filters on a per-adapter basis. The same filters do not apply to all adapters.
8. There are three columns with the following labels:

TCP Ports
UDP Ports
IP Protocols

In each column, you must select either of the following options:
Permit All . If you want to permit all packets for TCP or UDP traffic, leave **Permit All** activated. **Permit Only** . If you want to allow only selected TCP or UDP traffic, click **Permit Only** , click **Add** , and then type the appropriate port in the **Add Filter** dialog box. If you want to block all UDP or TCP traffic, click **Permit Only** , but do not add any port numbers in the **UDP Ports** or **TCP Port** column. You cannot block UDP or TCP traffic by selecting **Permit Only** for **IP Protocols** and excluding IP protocols 6 and 17.
Note that you cannot block ICMP messages, even if you select **Permit Only** in the **IP Protocols** column and you do not include IP protocol 1.
TCP/IP Filtering can filter only inbound traffic. This feature does not affect outbound traffic or response ports that are created to accept responses from outbound requests. Use IPSec Policies or packet filtering if you require more control over outbound access.

Ex 75: Customize and configure IPsec policy and rules for transport mode on the local computer.

Answer : **To create an IPSec Policy**

1. Using HQ-RES-WRK-01, in the left pane of the MMC Console, right-click IP Security Policies on Local Machine, and then click Create IP Security Policy. The IP Security Policy Wizard appears.
2. Click Next.
3. Type Partner as the name of your policy, and click Next.
4. Clear the Activate the default response rule check box, and then click Next.
5. Make sure the Edit Properties check box is selected (it is by default), and then click Finish.
6. In the Properties dialog box for the policy you have just created, ensure that Use Add Wizard check box in the lower-right corner is selected, and then click Add to start the Security Rule Wizard.
7. Click Next to proceed through the Security Rule Wizard, which you started at the end of the previous section.
8. Select This rule does not specify a tunnel, (selected by default) and then click Next.
9. Select the radio button for All network connections, (selected by default) and click Next.

Session 9 : Windows 2000 : Network Management

Ex 81: Create a Group Policy Object (GPO) and Console.

Answer : **Creation of Group Policy objects**

1. Open Active Directory Users and Computers.
2. In the console tree, click **Users**.
3. In the **Name** column in the details pane, double-click **Group Policy Creator Owners**.
4. In the **Group Policy Creator Owners Properties** dialog box, click the **Members** tab.
5. Click **Add**, and then double click the name of each user or security group to whom you want to delegate creation rights.
6. Click **OK** in the **Select Users, Contacts, or Computers** dialog box, and then click **OK** in the **Group Policy Creator Owners Properties** dialog box.

Notes

· To start Active Directory Users and Computers, open a Remote Desk Top connection to either a Windows 2000 domain controller or a member server that has Windows 2000 Administration Tools installed. You must log on to the server as a domain administrator in order to complete this procedure.

· By default, only domain administrators, enterprise administrators, Group Policy Creator Owners, and the operating system can create new Group Policy Objects. If the domain administrator wants a

Non administrator or a group to be able to create Group Policy objects, that user or group can be added to the Group Policy Creator Owners security group. When a user who is not an administrator, but who is a member of the Group Policy Creator Owners group, creates a Group Policy object, that user becomes the creator and owner of the Group Policy object; therefore, that user can edit the Group Policy object. Being a member of the Group Policy Creator Owners group gives the user full control of only those Group Policy objects that the user creates or those Group Policy objects that are explicitly delegated to that user. It does not give the non administrator user any additional rights over other Group Policy objects for the domain—these users are not granted rights over Group Policy objects that they did not create.

· When an administrator creates a Group Policy object, the Domain Administrators group becomes the Creator Owner of the Group Policy object.

· When you delegate this task to non administrators, also consider delegating the ability to manage the links for a specific organizational unit. The reason for this is that, by default, non administrators cannot manage links, and the inability to manage links prevents them from being able to use the Active Directory Users and Computers snap-in to create a Group Policy object.

Session 10 : Windows 2000 : Troubleshooting

Ex 94: Back up the recovery agent Encrypting File System (EFS) private key.

Answer : **Backup the recovery agent Encrypting File System9EFS) Private key:**

1. Use Backup or another backup tool to restore a user's backup version of the encrypted file or folder to the computer where your file recovery certificate and recovery key are located.
2. Open windows Explorer.
3. Right-click the file or folder and then click **Properties**.
4. On the **General** tab, click **Advanced**.
5. Clear the **Encrypt contents to secure data** check box.
6. Make a backup version of the decrypted file or folder and return the backup version to the user.

Notes

· To open Windows Explorer, click **Start**, point to **All Programs**, point to **Accessories**, and then click **Windows Explorer**.

· You can return the backup version of the decrypted file or folder to the user as an e-mail attachment, on a floppy disk, or on a network share.

· You can also physically transport the recovery agent's private key and certificate, import the private key and certificate, decrypt the file or folder, and then delete the imported private key and certificate. This procedure exposes the private key more than the procedure above but does not require any backup or restore operations or file transportation.

· If you are the recovery agent, use the **Export** command from Certificates in Microsoft Management Console (MMC) to export the file recovery certificate and private key to a floppy disk. Keep the floppy disk in a secure location. Then, if the file recovery certificate or private key on your computer is ever damaged or deleted, you can use the **Import** command from Certificates in MMC to replace the damaged or deleted certificate and private key with the ones you have backed up on the floppy disk.

· For more information about using Certificates in MMC, see Related Topics.
