# Lesson Module Status

- Slides – draft
- Properties - done
- Flashcards – not done
- 1st minute quiz –
- Web Calendar summary –
- Web book pages –
- Commands – done
- Howtos –
- Skills pacing -
- Lab – done
- Depot (VMs) – na

# Course history and credits

Jim Griffin

- Jim created the original version of this course
- Jim's site: http://cabrillo.edu/~jgriffin/

Rick Graziani

- Thanks to Rick Graziani for the use of some of his great network slides
- Rick's site: http://cabrillo.edu/~rgraziani/

Joe P.

Joe A.

Chuck

Kay

Lieven

Rich

Jesus

Josh

Joe B.

Chris H.

Edwin

Julio

Jack

Drew

Casady

Brynden

Ryan

Aaron

Edgar

Chris B.


www.cccconfer.org
dial-in: 888-886-3951
passcode: 439080

John

Junious

Robert

VMs for tonight

**(Revert, 384MB RAM and Power up)**

**Elrond Legolas William**



*Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit*

# Quiz

Please take out a blank piece of paper, switch off your monitor, close your books, put away your notes and answer these questions:

- To configure an NFS server, what file must be edited to specify the directories to be shared ?
- What is one way you might fix a “Stale NFS file handle” error?
- What URL would be used to browse to the local CUPS web-based configuration utility?

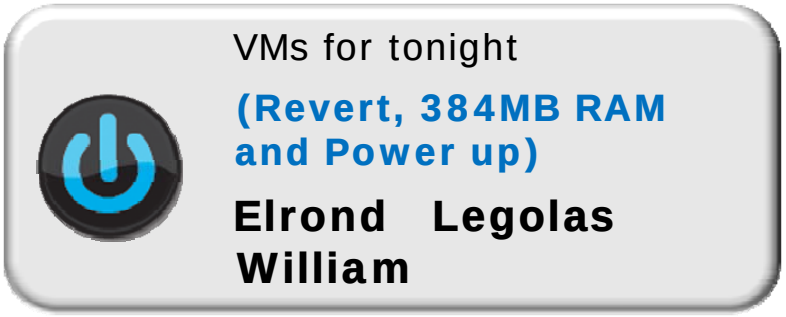
# Samba

| Objectives | Agenda |
| --- | --- |
| • Use SAMBA to browse directories on the Linux servers from a Windows machine. | • Quiz<br>• Questions on previous material<br>• Housekeeping<br>• Basic Windows Skills - IPs, /etc/hosts<br>• Warmup - William and Elrond configuration<br>• Samba<br>• Windows Shares (viewing, monitoring, browsing)<br>• Share browsing and access - from Windows<br>• Share browsing and access - from Linux<br>• Installing Samba<br>• SWAT<br>• Lab 8<br>• Wrap |

# Questions on previous material

# Questions?

- Previous lesson material
- Lab assignment
- Tests

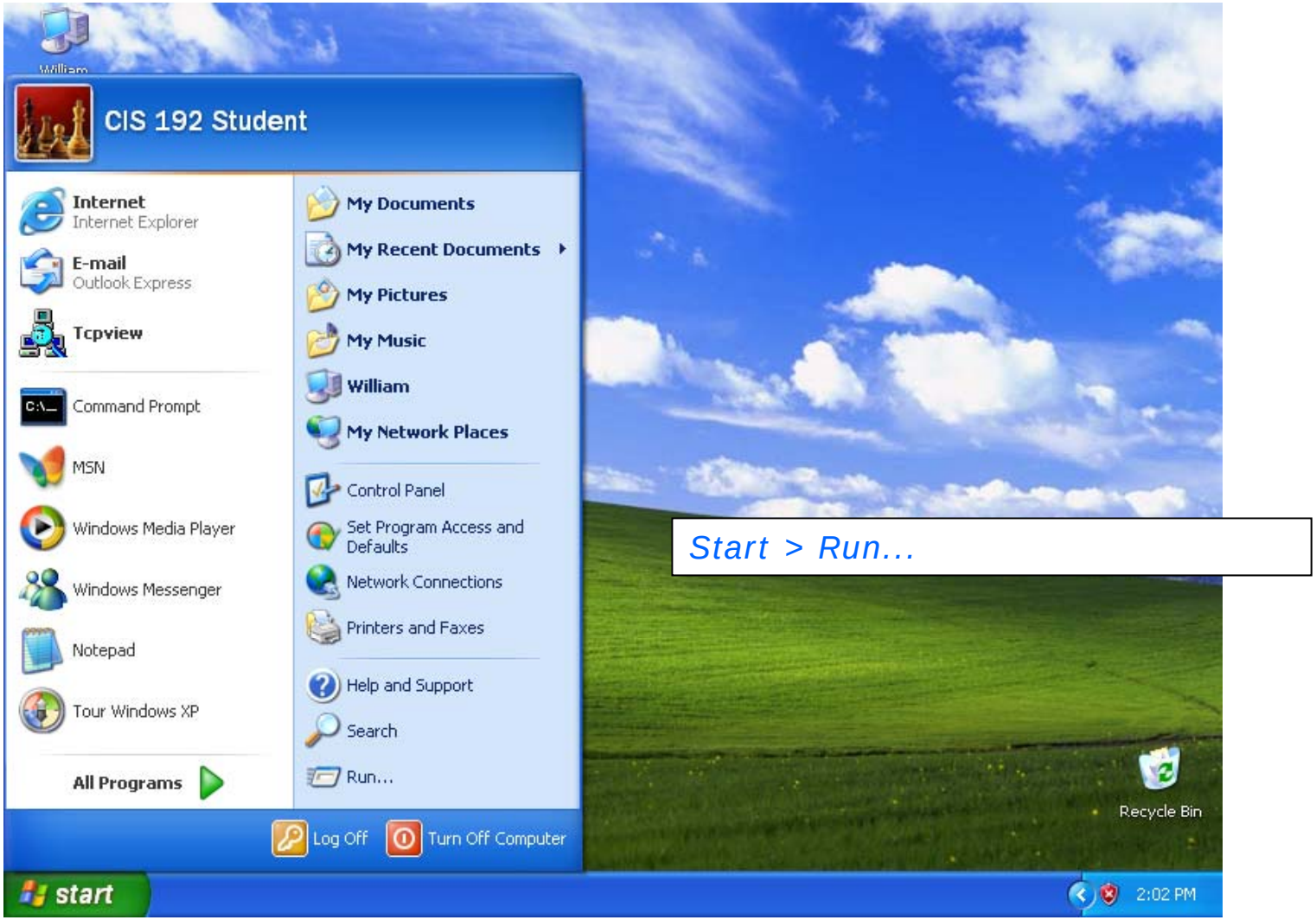


# Housekeeping

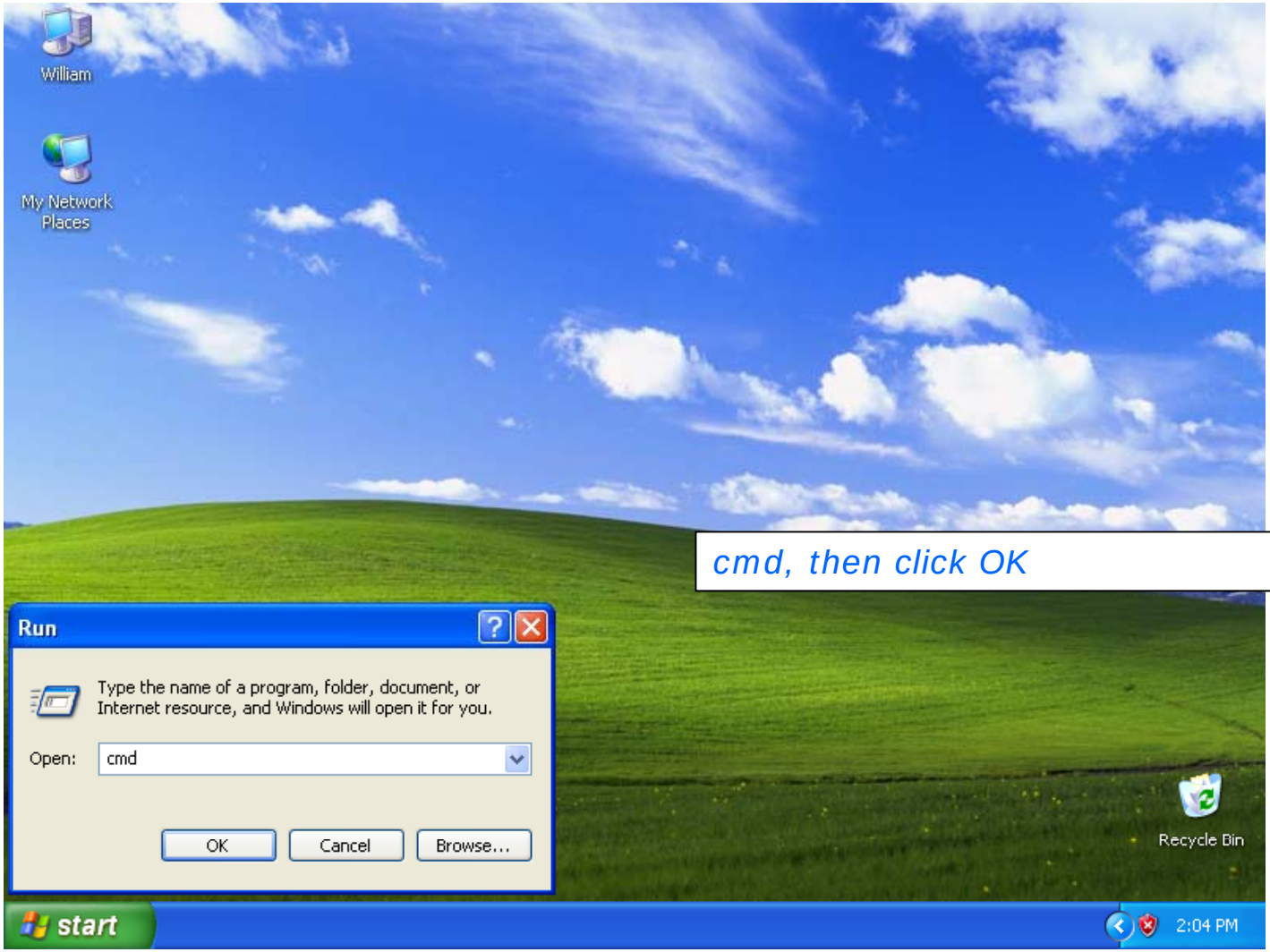
- No labs due today
- Fall schedule is available online
  http://cabrillo.edu/publications/schedule/fall2010schedule.pdf
- Preparing for the final exam
  - Organization and troubleshooting skills are essential
  - Know where to locate information quickly
  - *Tip:* Make you own personal crib sheet/web page
  - "Muscle memory" for basic commands
  - Practice makes perfect

# Windows Skills
# IP addresses

# Windows - Show the IP Address

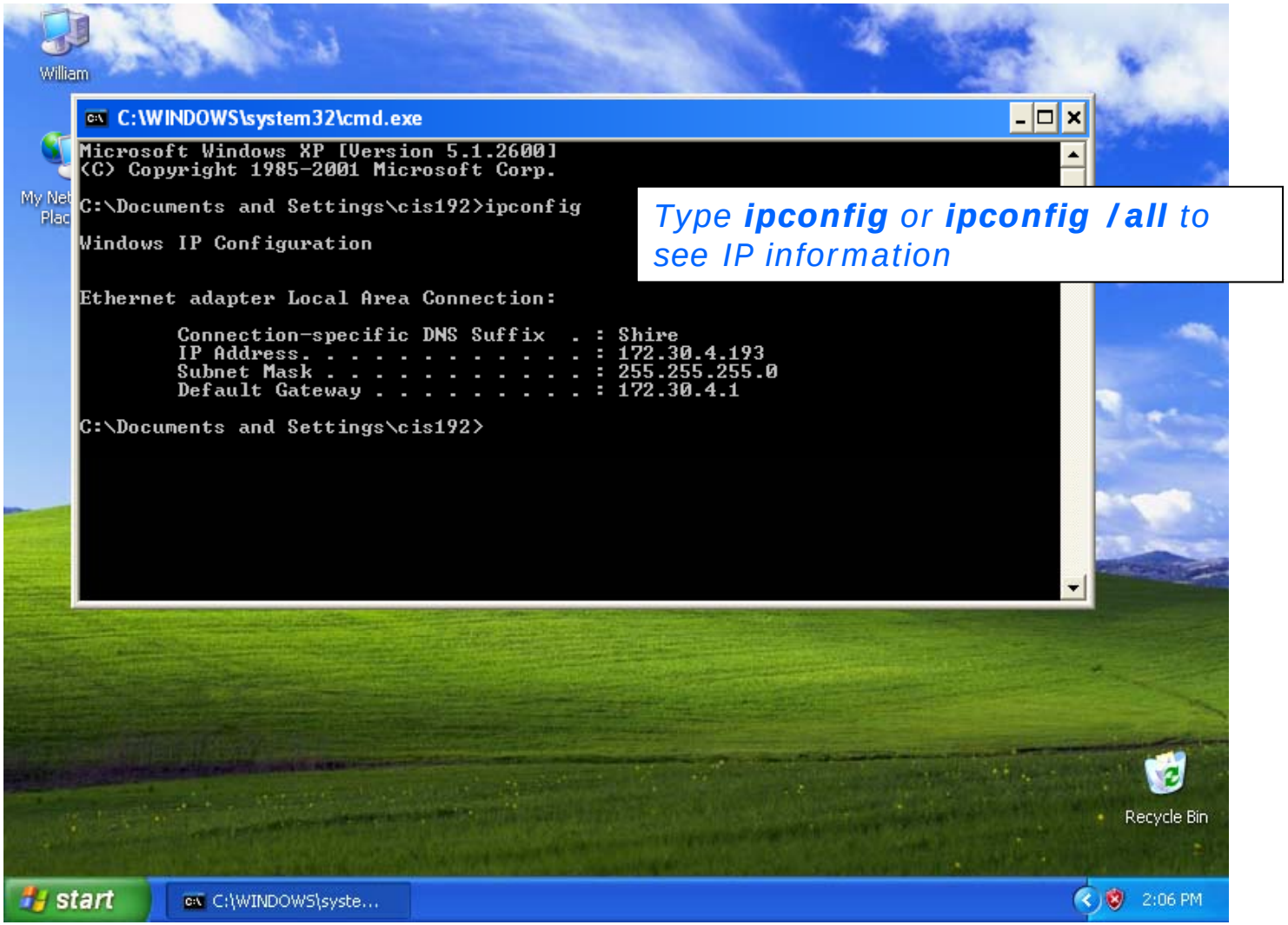


# Windows - Show the IP Address

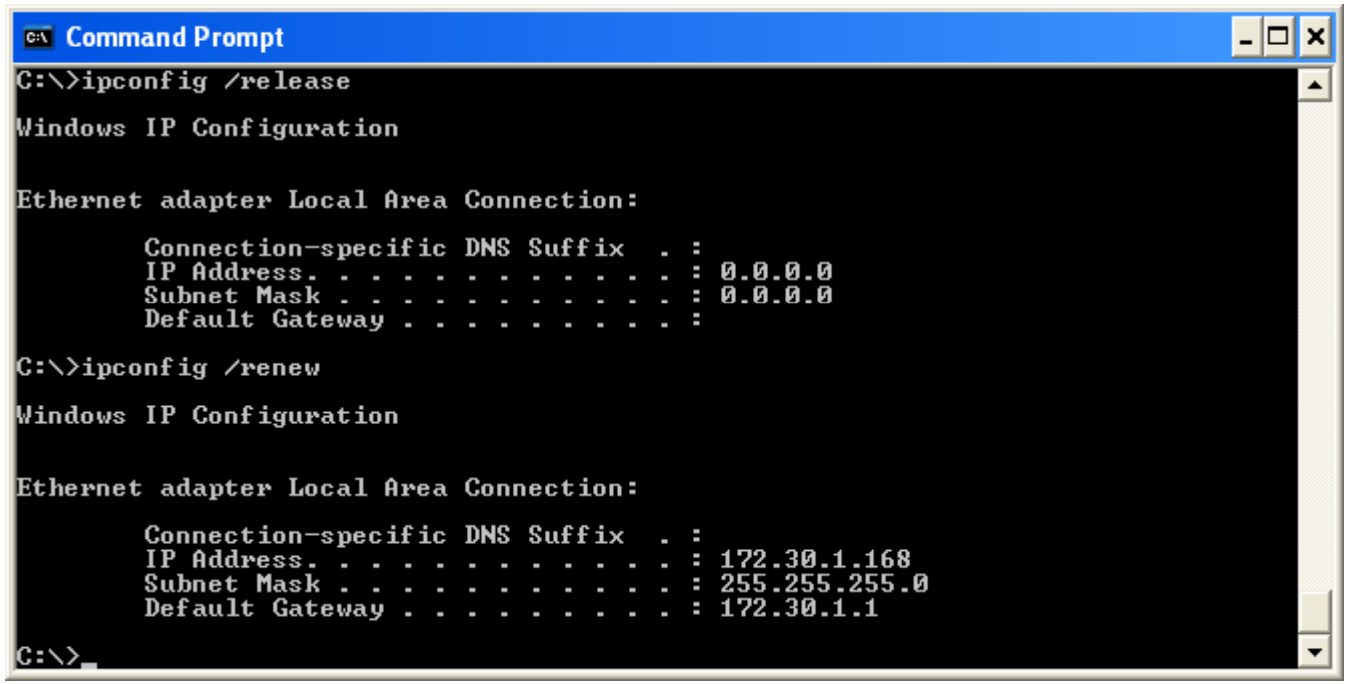



*cmd, then click OK*

# Windows - *Show the IP Address*



# Windows - Show the IP Address




*Use **ipconfig /release** to release the current IP addresses obtained using DHCP*

*Use **ipconfig /renew** to obtain a new IP address via DHCP*

# Windows – IP Addresses

To show IP address: **ipconfig**

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.30.1.168
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.30.1.1

C:\>
```

# Windows – IP Addresses

To show IP address and more: **ipconfig /all**

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : william
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : AMD PCNET Family PCI Ethernet Adapter
        Physical Address. . . . . . . . . : 08-00-27-D2-E9-40
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.30.1.168
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.30.1.1
        DHCP Server . . . . . . . . . . . : 172.30.1.1
        DNS Servers . . . . . . . . . . . : 207.62.187.53
        Lease Obtained. . . . . . . . . . : Thursday, April 29, 2010 7:50:50 AM
        Lease Expires . . . . . . . . . . : Thursday, April 29, 2010 1:50:50 PM
```

# Windows – IP Addresses

To release an IP address (back to DHCP): **ipconfig /release**

```
C:\>ipconfig /release

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\>
```

# Windows – IP Addresses

To obtain an IP address (from DHCP): **ipconfig /renew**

```
C:\>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.30.1.168
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.30.1.1

C:\>
```


- Start > Run... > cmd (click OK)
- Type **ipconfig**
- Type **ipconfig /all**
- Record William's IP address to use later

# Windows Skills /etc/hosts

# Windows – Modifying /etc/hosts

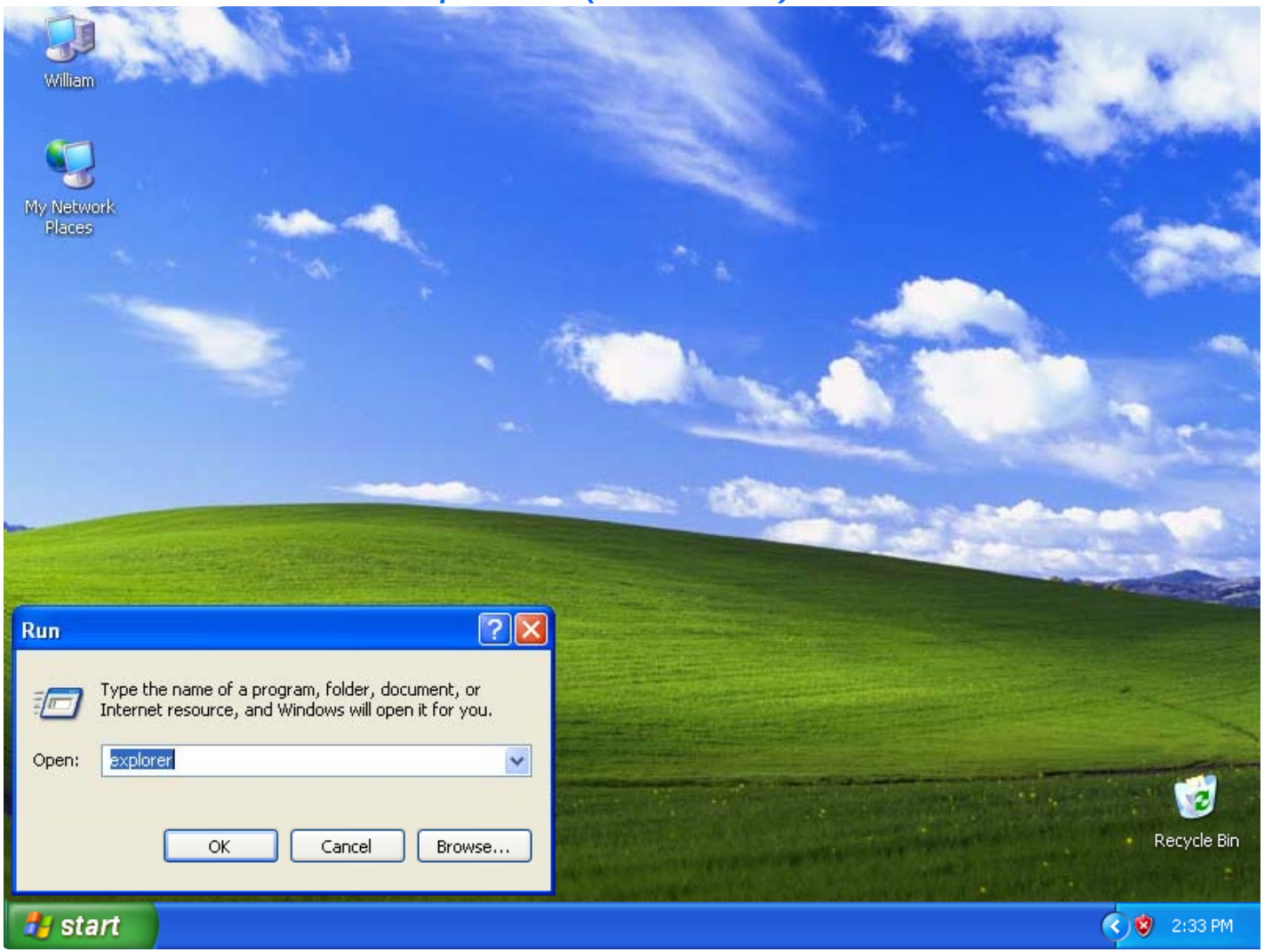
*Start*

# Windows – Modifying /etc/hosts

*Start > Run...*

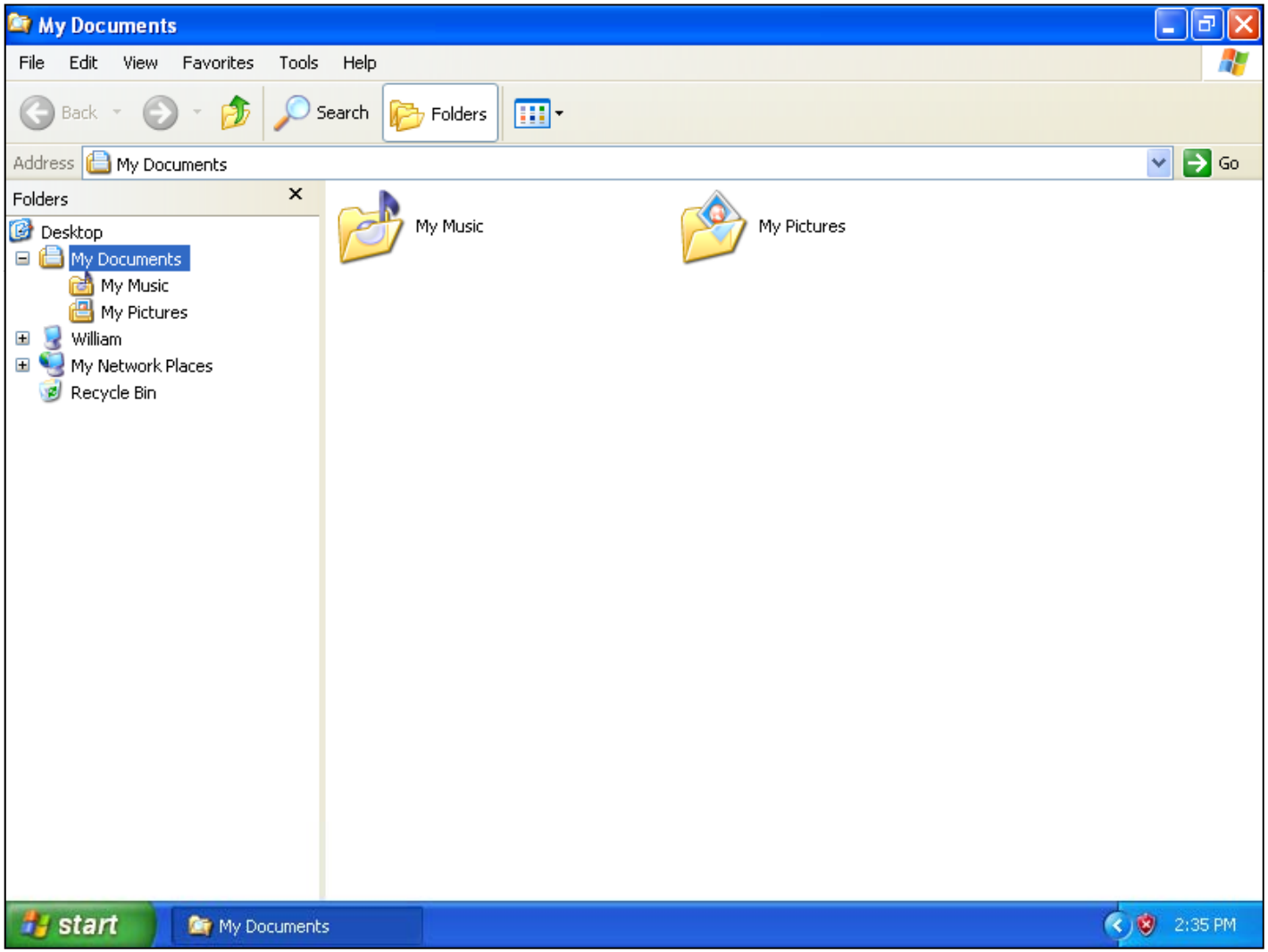
# Windows – *Modifying /etc/hosts*

*Start > Run... > explorer (Click OK)*



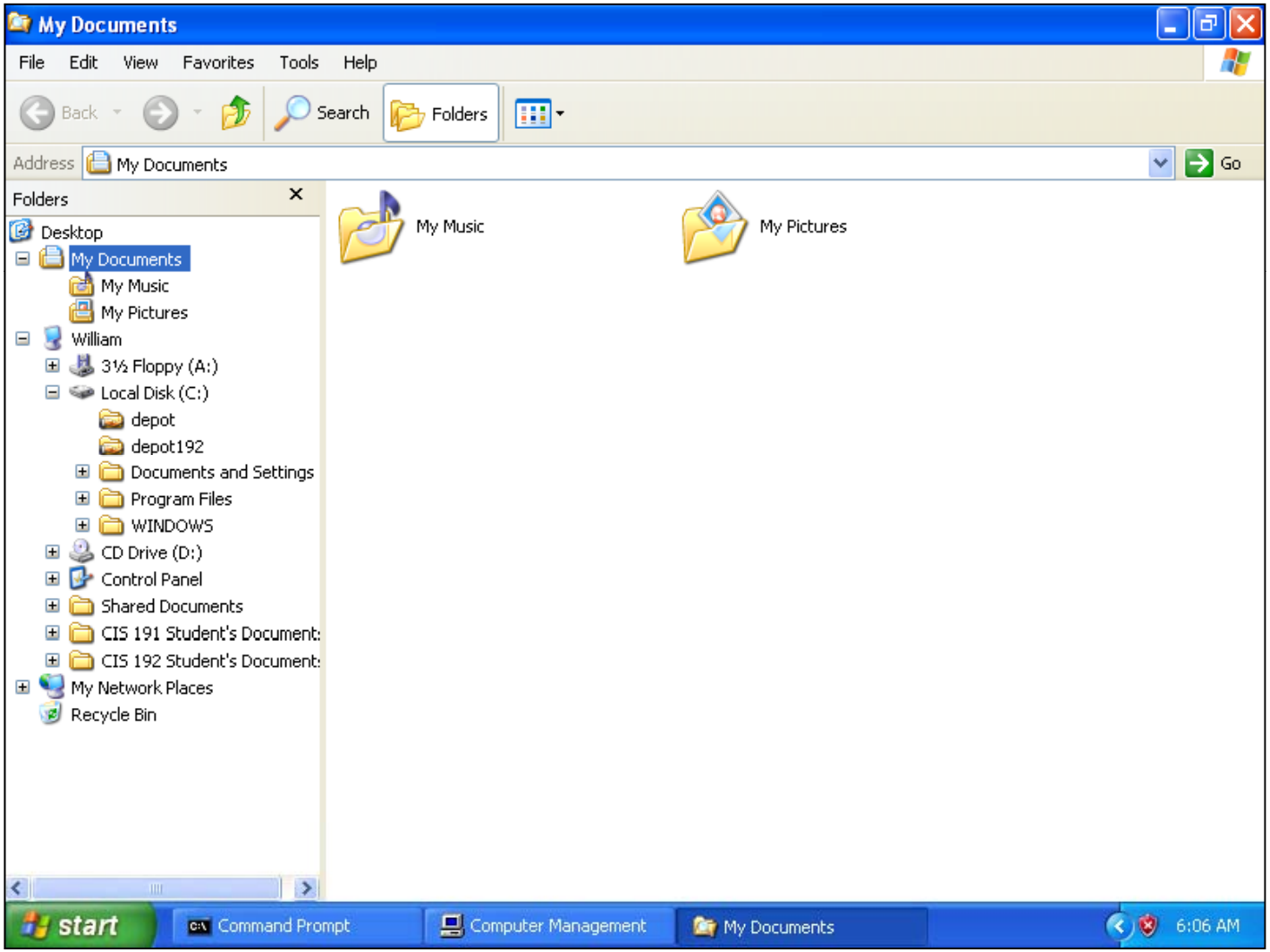
# Windows – Modifying /etc/hosts

*Expand William (MY Computer) on left panel*



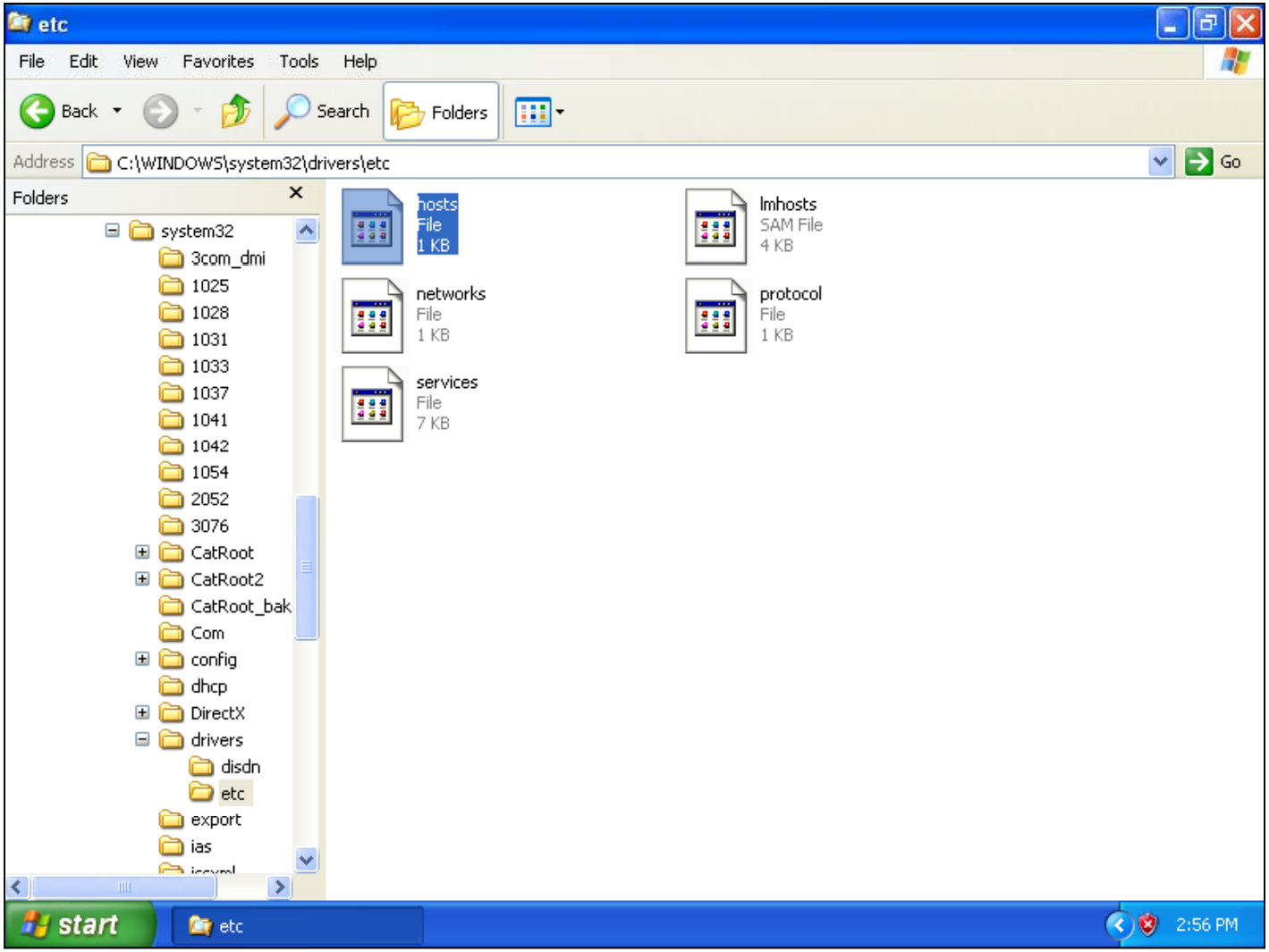
# Windows – *Modifying /etc/hosts*

*Navigate to C:\WINDOWS\system32\drivers\etc\hosts*



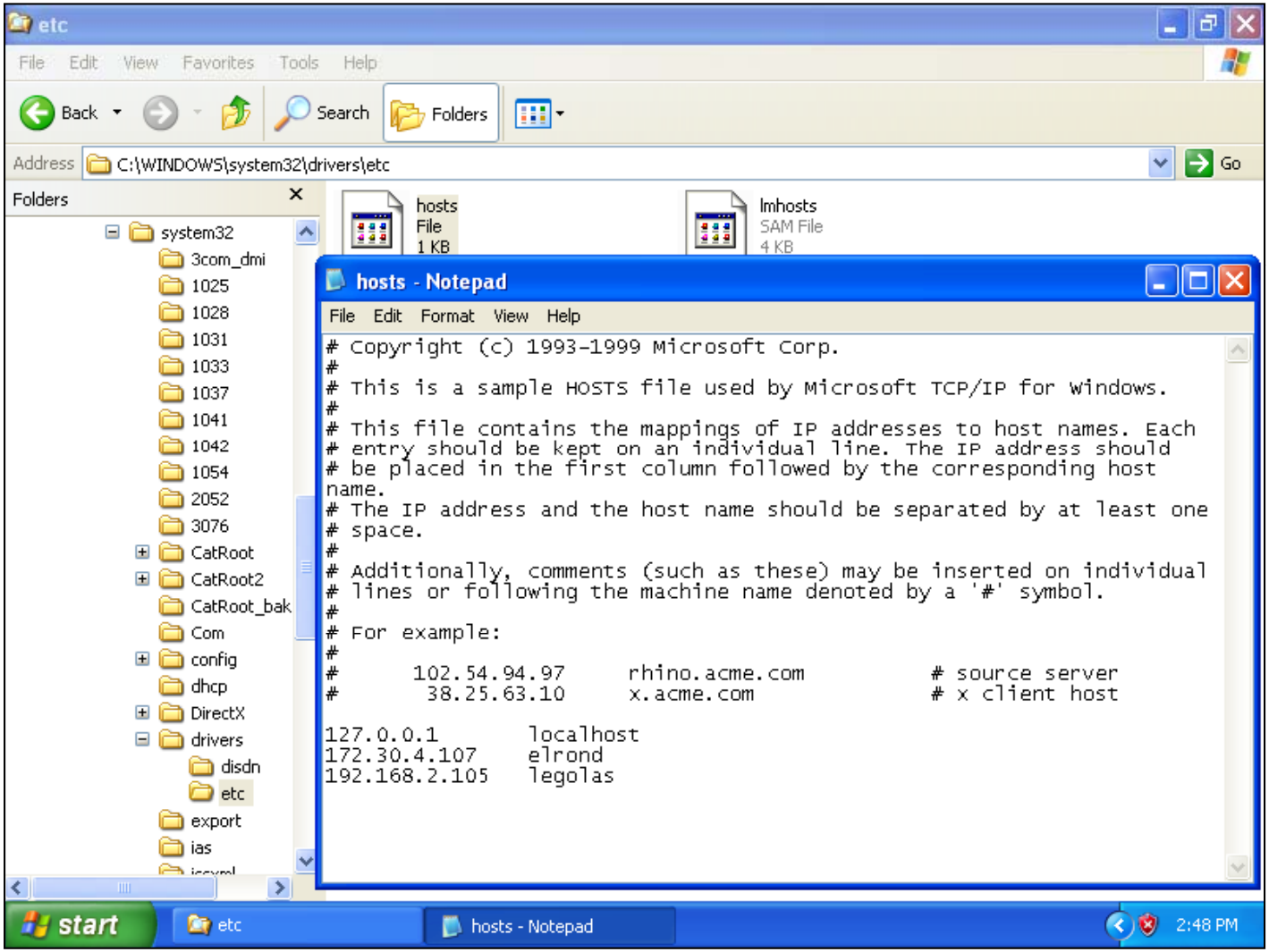
# Windows – Modifying /etc/hosts

*Navigate to C:\WINDOWS\system32\drivers\etc\hosts*

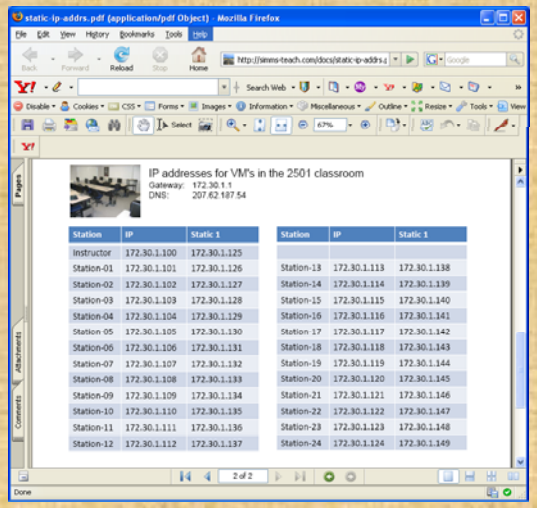


# Windows – Modifying /etc/hosts

*Edit C:\WINDOWS\system32\drivers\etc\hosts*



**William**




```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
172.30.N.1XX    elrond
```

- Lookup up the static IP address (based on your station number) to use Elrond with:

  http://simms-teach.com/docs/static-ip-addrs.pdf

- Add Elrond to C:\WINDOWS\system32\drivers\etc\hosts on William.

# Windows Skills
# Static Routes

# Windows – Static Routes

*With Windows there is an example showing how to make a static route in the online help*

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cis192>route ?

Manipulates network routing tables.

ROUTE [-f] [-p] [command [destination]
                  [MASK netmask]  [gateway] [METRIC metric]  [IF interface]
```

*< snipped >*

```
Examples:

    > route PRINT
    > route ADD 157.0.0.0 MASK 255.0.0.0  157.55.80.1 METRIC 3 IF 2
           destination^      ^mask      ^gateway     metric^    ^
                                                       Interface^
      If IF is not given, it tries to find the best interface for a given
      gateway.
    > route PRINT
    > route PRINT 157*          .... Only prints those matching 157*
    > route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

      CHANGE is used to modify gateway and/or metric only.
    > route PRINT
    > route DELETE 157.0.0.0
    > route PRINT
```

*< snipped >*

# Windows – Static Routes

To show routing table use: **route PRINT**

```
C:\>route PRINT
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...08 00 27 d2 e9 40 ...... AMD PCNET Family PCI Ethernet Adapter - Packet S
cheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.30.1.1    172.30.1.168       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
       172.30.1.0    255.255.255.0     172.30.1.168    172.30.1.168       20
     172.30.1.168  255.255.255.255        127.0.0.1       127.0.0.1       20
   172.30.255.255  255.255.255.255     172.30.1.168    172.30.1.168       20
        224.0.0.0        240.0.0.0     172.30.1.168    172.30.1.168       20
  255.255.255.255  255.255.255.255     172.30.1.168    172.30.1.168       1
Default Gateway:        172.30.1.1
===========================================================================
Persistent Routes:
  None

C:\>
```

# Windows – Static Routes

To add a route use: **route add** *address* **mask** *gateway*

```
C:\>route add 192.168.2.0 mask 255.255.255.0 172.30.1.200

C:\Documents and Settings\cis192>route PRINT
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...08 00 27 d2 e9 40 ...... AMD PCNET Family PCI Ethernet Adapter - Packet S
cheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.30.1.1    172.30.1.168       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
       172.30.1.0    255.255.255.0     172.30.1.168    172.30.1.168       20
     172.30.1.168  255.255.255.255        127.0.0.1       127.0.0.1       20
   172.30.255.255  255.255.255.255     172.30.1.168    172.30.1.168       20
      192.168.2.0    255.255.255.0     172.30.1.200    172.30.1.168        1
        224.0.0.0        240.0.0.0     172.30.1.168    172.30.1.168       20
  255.255.255.255  255.255.255.255     172.30.1.168    172.30.1.168       1
Default Gateway:        172.30.1.1
===========================================================================
Persistent Routes:
  None

C:\>
```

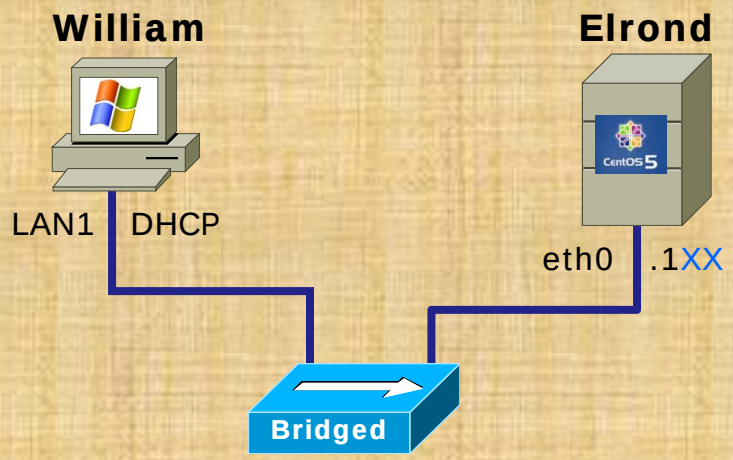
# Windows – Static Routes

To delete a route use: **route delete** *address* **mask** *gateway*

```
C:\>route delete 192.168.2.0 mask 255.255.255.0 172.30.1.200

C:\Documents and Settings\cis192>route PRINT
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...08 00 27 d2 e9 40 ...... AMD PCNET Family PCI Ethernet Adapter - Packet S
cheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.30.1.1    172.30.1.168       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
       172.30.1.0    255.255.255.0     172.30.1.168    172.30.1.168       20
     172.30.1.168  255.255.255.255        127.0.0.1       127.0.0.1       20
   172.30.255.255  255.255.255.255     172.30.1.168    172.30.1.168       20
        224.0.0.0        240.0.0.0     172.30.1.168    172.30.1.168       20
  255.255.255.255  255.255.255.255     172.30.1.168    172.30.1.168       1
Default Gateway:        172.30.1.1
===========================================================================
Persistent Routes:
  None

C:\>
```

# Warmup

# Warmup




- Cable as shown
- Configure NICs
  - IP
  - netmask
  - broadcast
- Configure /etc/hosts on Elrond with William's IP address
- Test:
  - On Elrond: **ping william**
  - On Elrond: **ping google.com**
  - On William: **ping elrond**

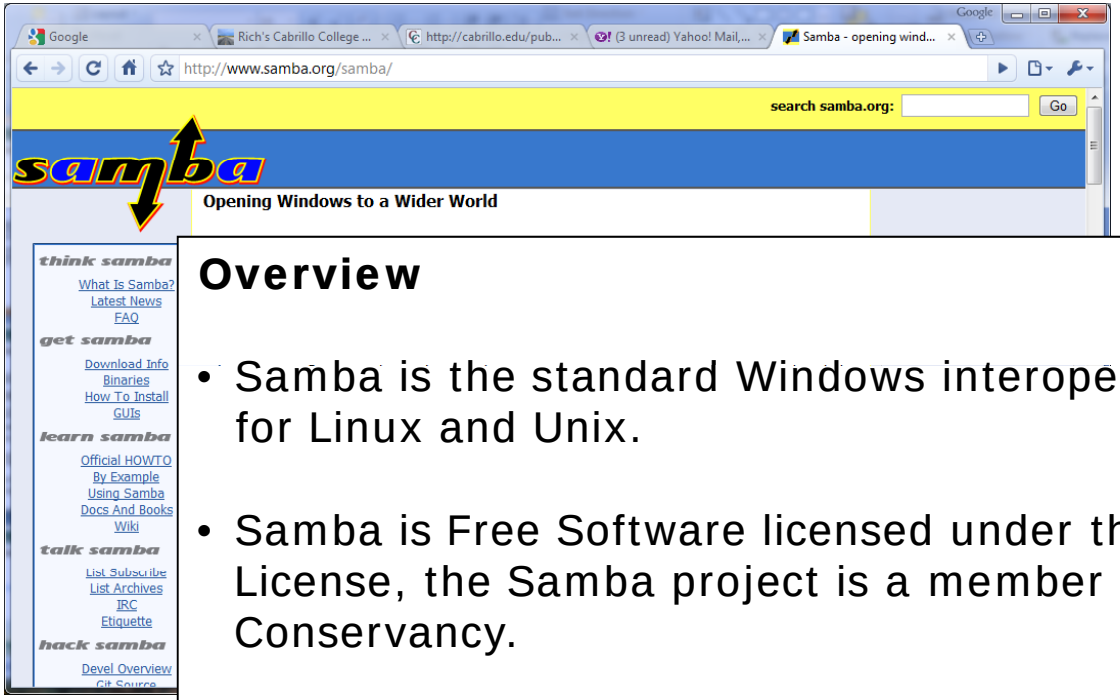
.1XX is based on your station number and the IP Table
N=1 for the classroom and N=4 for the CIS lab or CTC

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=172.30.N.1XX
NETMASK=255.255.255.0

# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
ONBOOT=no
BOOTPROTO=none
```

```
# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=elrond.shire
GATEWAY=172.30.N.1

# cat /etc/resolv.conf
nameserver 207.62.187.53

# service network restart
```

# Samba

# Samba




*http://samba.org/*

## Overview

- Samba is the standard Windows interoperability suite of programs for Linux and Unix.
- Samba is Free Software licensed under the GNU General Public License, the Samba project is a member of the Software Freedom Conservancy.
- Since 1992, Samba has provided secure, stable and fast file and print services for all clients using the SMB/CIFS protocol, such as all versions of DOS and Windows, OS/2, Linux and many others.
- Samba is an important component to seamlessly integrate Linux/Unix Servers and Desktops into Active Directory environments using the winbind daemon

# Samba

**Overview**

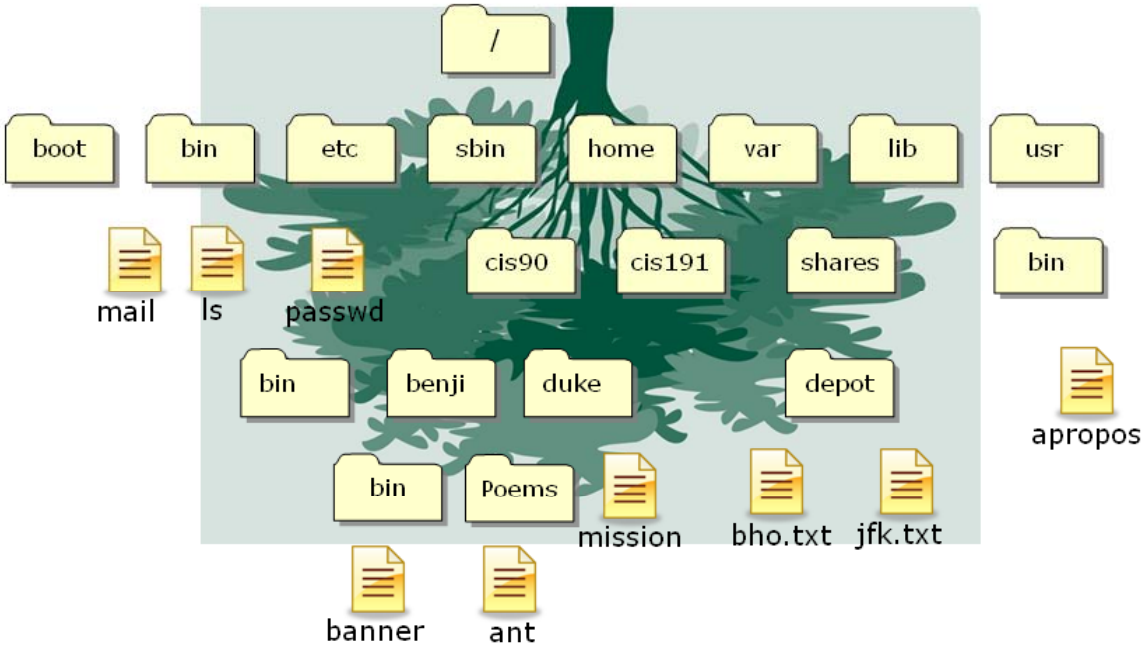
Enables a UNIX/Linux computer to be a Windows File and Print server that interoperates with Windows computers for common file and printer sharing.

- Andrew Tridgell, an Australian, is the original author. He wanted to mount disk space from a Unix server on his DOS PC!
- SMBServer name was already taken, so Andrew used grep -i '^s.*m.*b' /usr/share/dict/words and chose Samba
- Based on the CIFS (Common Internet File System) protocol. The CIFS name was introduced by Microsoft. CIFS is based on SMB (Server Message Block) protocol.
- SMB's history goes back to early days of PC's, DOS, NetBIOS and NetBEUI.
- NFS exported directories can only be used by other UNIX/Linux systems. Samba shared directories can be used by both UNIX/Linux and Windows systems.

# Samba


**Elrond**

*Here is a Linux server and its UNIX File Tree*

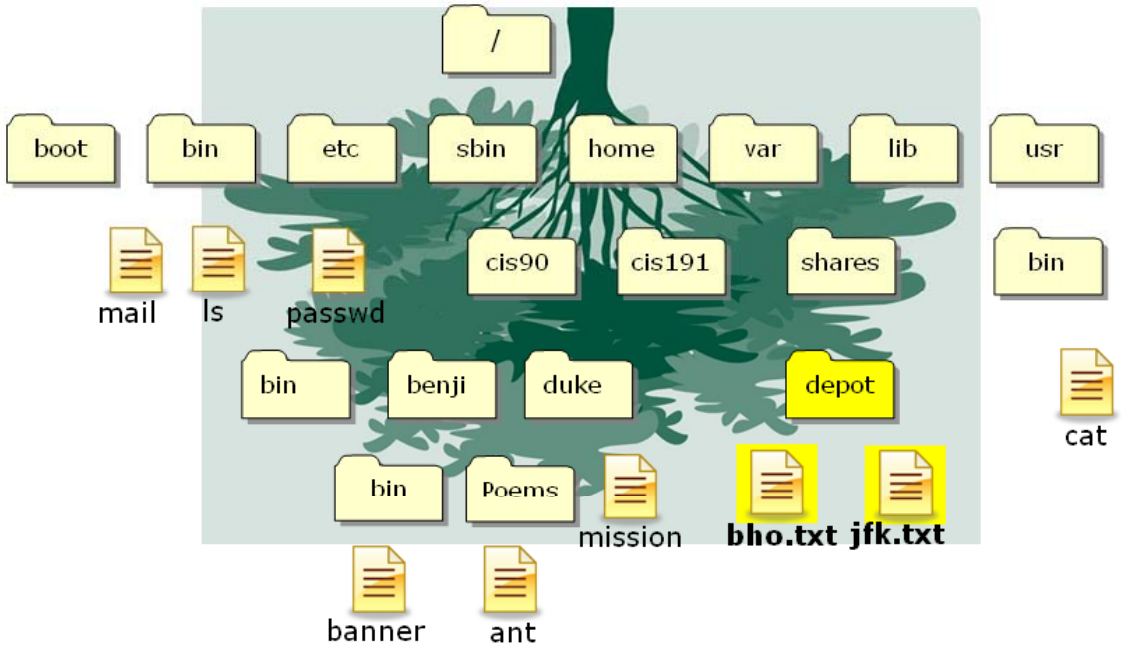


# Samba

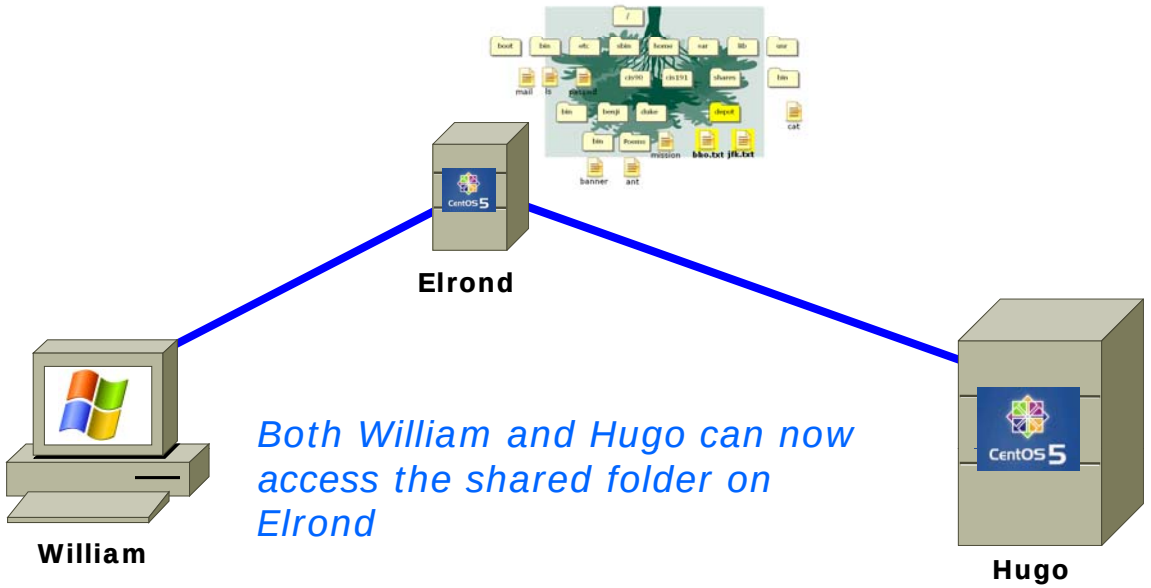

**Elrond**

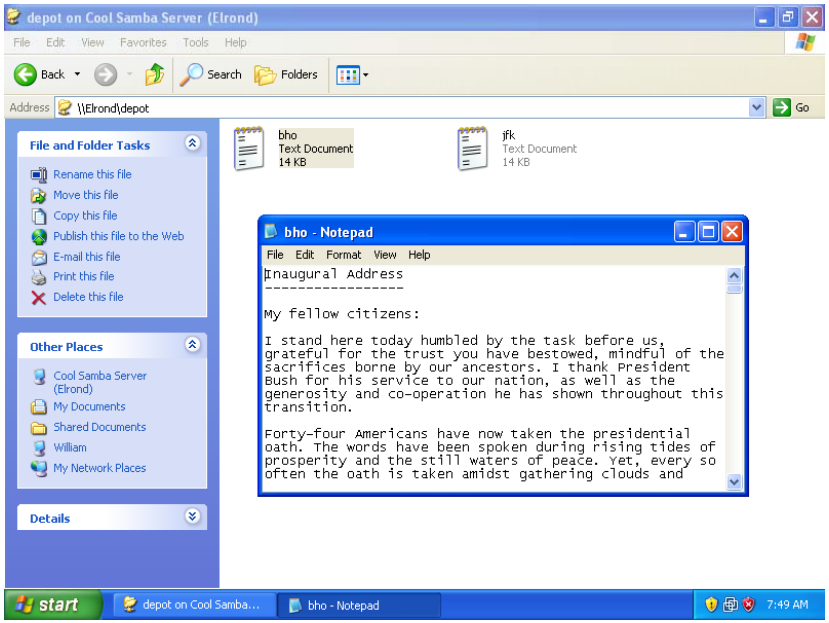
*To make a share, add the following lines to* ***/etc/samba/smb.conf*** *creates a shared directory on Elrond (and do a few other things)*

```
[depot]
        comment = Public files on Elrond
        path = /var/shares/depot
        read only = yes
        guest ok = yes
```



# Samba




```
[root@hugo ~]# mount //elrond/depot /mnt
Password:
[root@hugo ~]# ls /mnt
bho.txt  jfk.txt
[root@hugo ~]# cd /mnt
[root@hugo mnt]# cat bho.txt
Inaugural Address
-----------------

My fellow citizens:

I stand here today humbled by the task
before us, grateful for the trust you
have bestowed, mindful of the sacrifices
```


www.samba.org

**Packages**

```
[root@elrond ~]# rpm -qa | grep samba
samba-3.0.28-1.el5_2.1
samba-common-3.0.28-1.el5_2.1
samba-client-3.0.28-1.el5_2.1
```

**Firewall Ports Used**

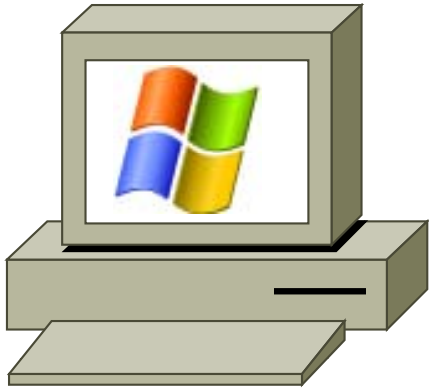
137/udp # NetBIOS Name Service
138/udp # NetBIOS Datagram Service
139/tcp # NetBIOS Session Service
445/tcp # Microsoft Directory Service

**Services**

```
[root@elrond ~]# service smb start
Starting SMB services:                                     [  OK  ]
Starting NMB services:                                     [  OK  ]

[root@elrond ~]# service smb status
smbd (pid 17212 17207) is running...
nmbd (pid 17210) is running...

[root@elrond ~]# chkconfig smb on
```

**Configuration**

```
[root@elrond ~]# ls /etc/samba/smb.conf
/etc/samba/smb.conf
```



# Windows Shares

# Windows Shares

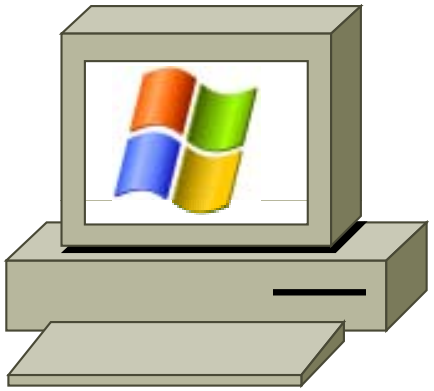
**Overview**:

- Files and printers can be shared on Windows over the network.
- **Simple File Sharing** must be disabled on the **Folder Options** dialog box to allow basic share permissions (Read, Change, Full Control) to be set.
- Shares are configured using the **Properties** dialog box for folders.
    - Use the **Sharing tab** to configure the share.
    - Note, the **Security tab** sets NTFS permissions which are different.
- Both share permissions and NTFS permissions are applied for accessing any file over the network.
- Use **MMC (Computer Management)** to monitor share usage

# Windows Shares

**Windows Share Permissions**:

- **Read** – Allows browsing file and folder names (including subfolders), reading files and executing programs.
- **Change** – Includes all Read permissions plus can add, delete and modify folders and files.
- **Full Control** - Includes all read and Change permissions plus can change permissions.



# Viewing Share Configuration

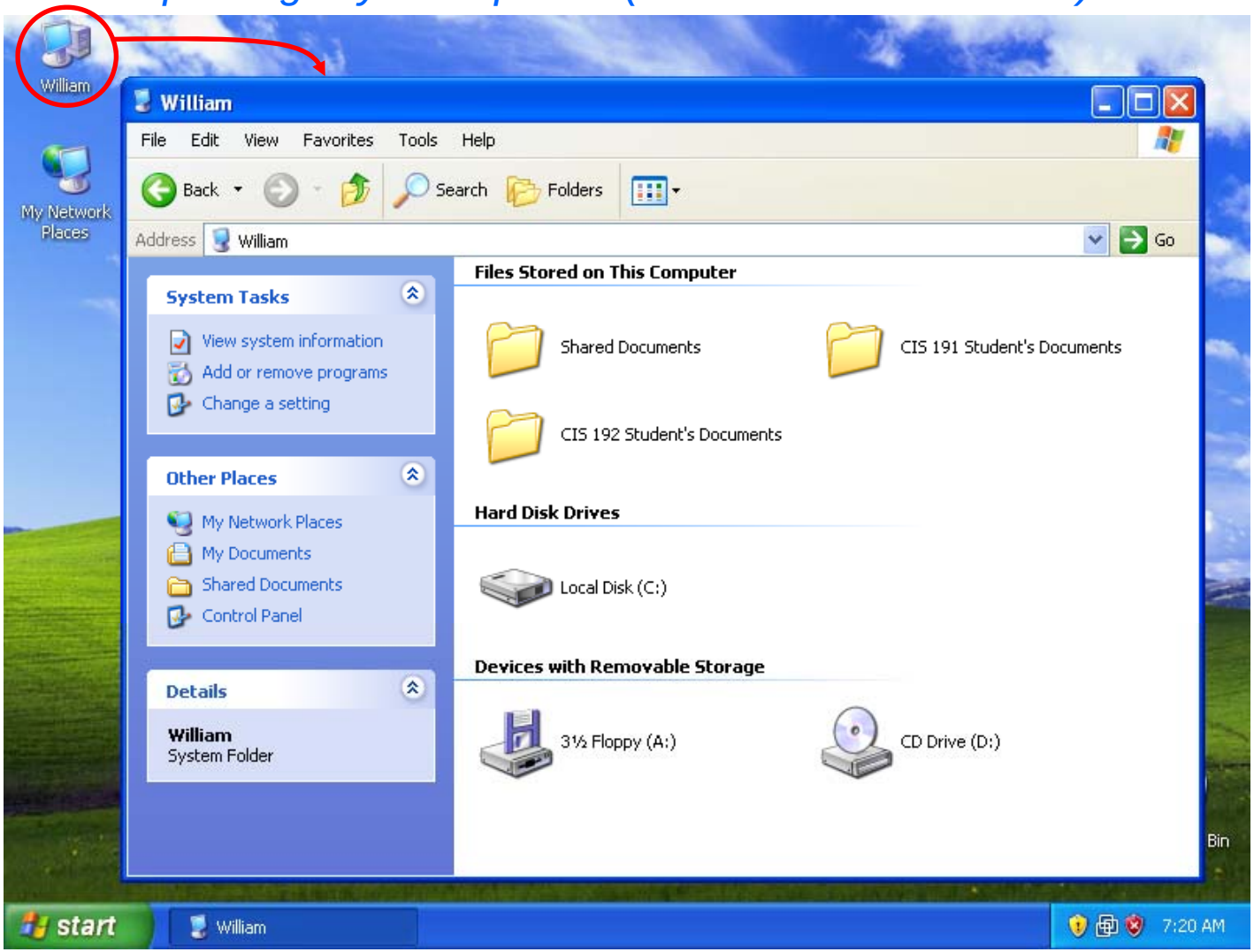
## Windows Shares

**The next series of slides walkthrough how to view share configurations on Windows**

*Note that this is only one of many ways to do this*

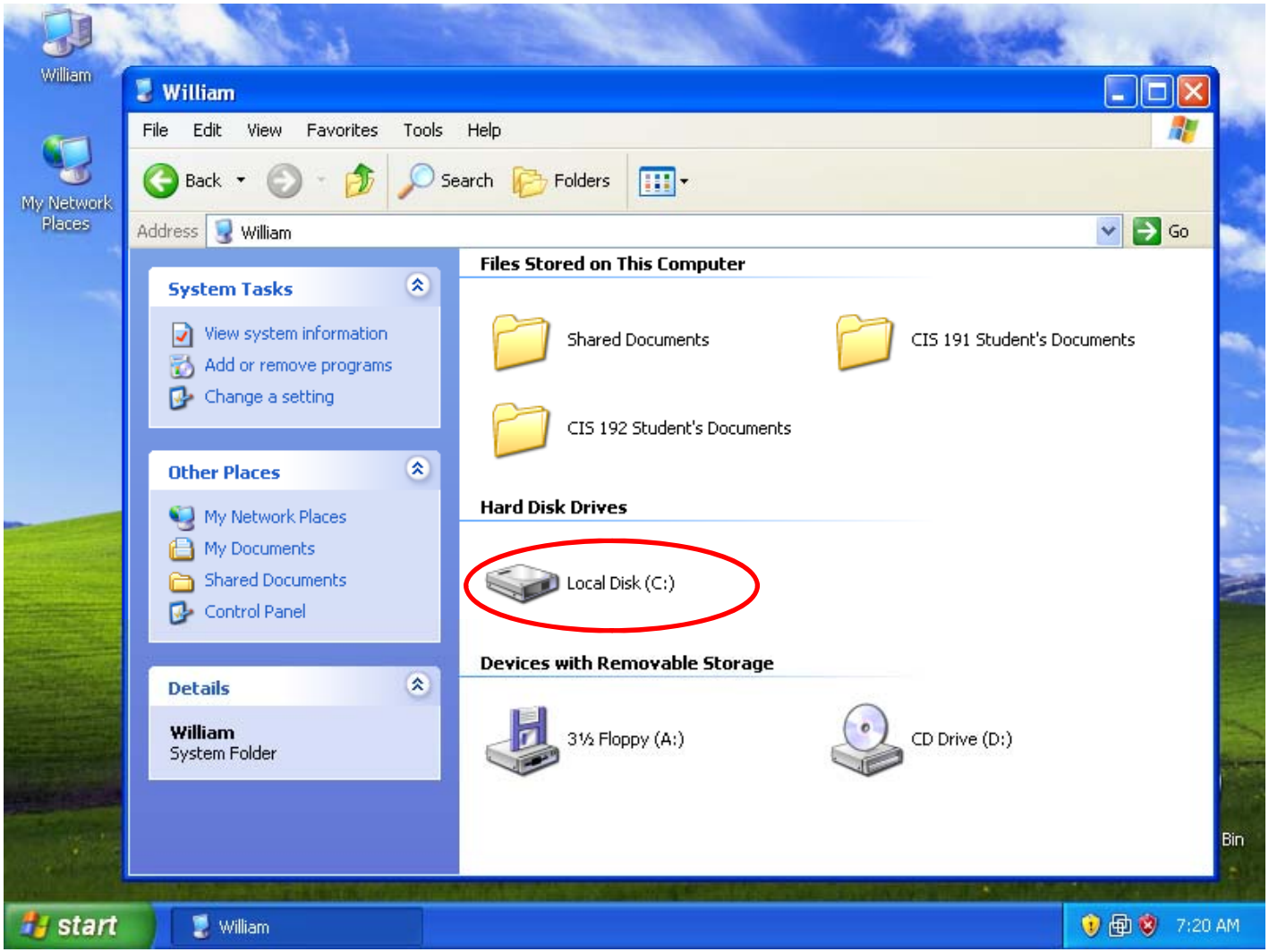
# Windows Shares – *viewing share configurations*

*After opening My Computer (labeled William here)*



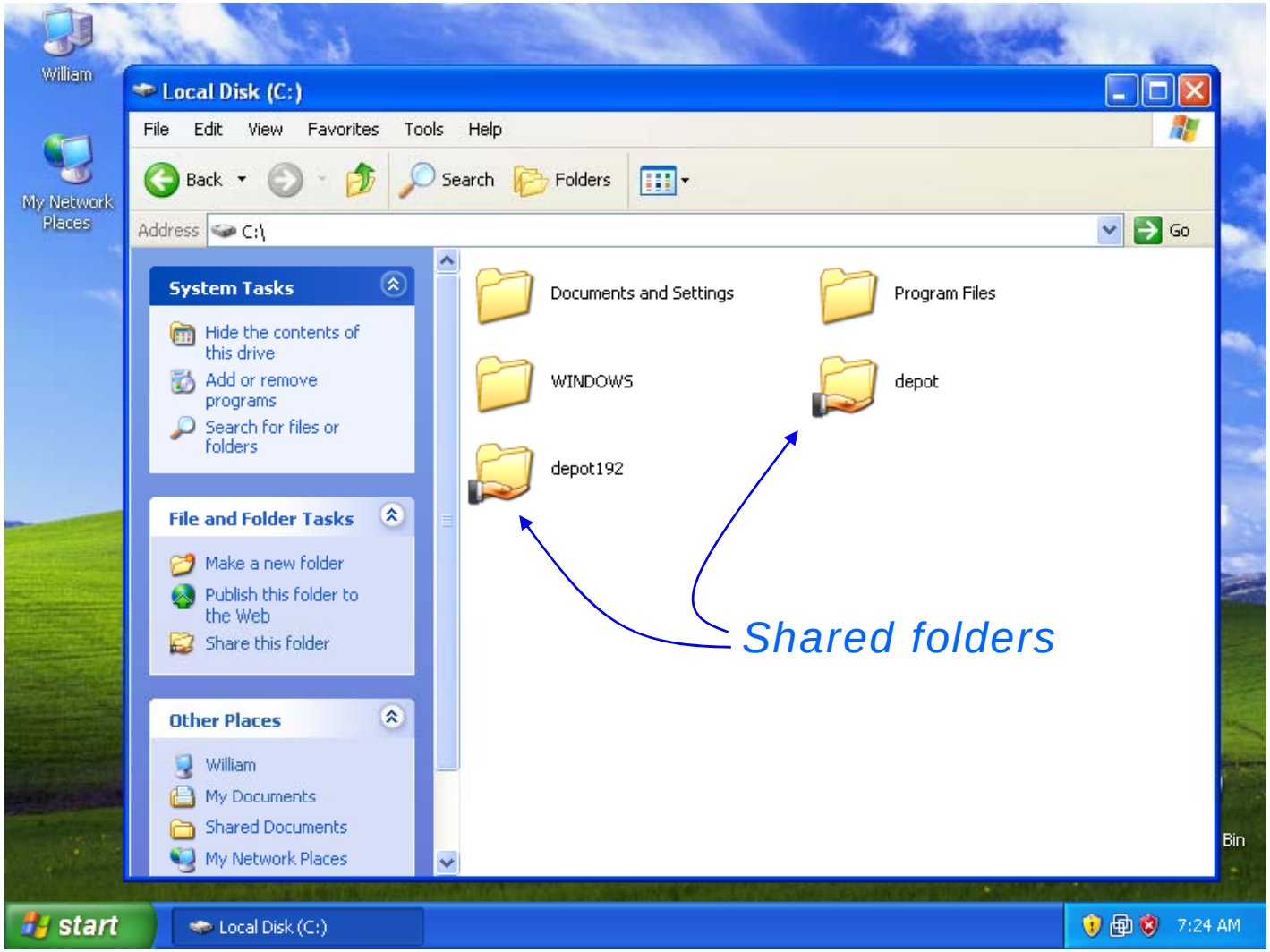
# Windows Shares – *viewing share configurations*

*Next, open the C: drive*



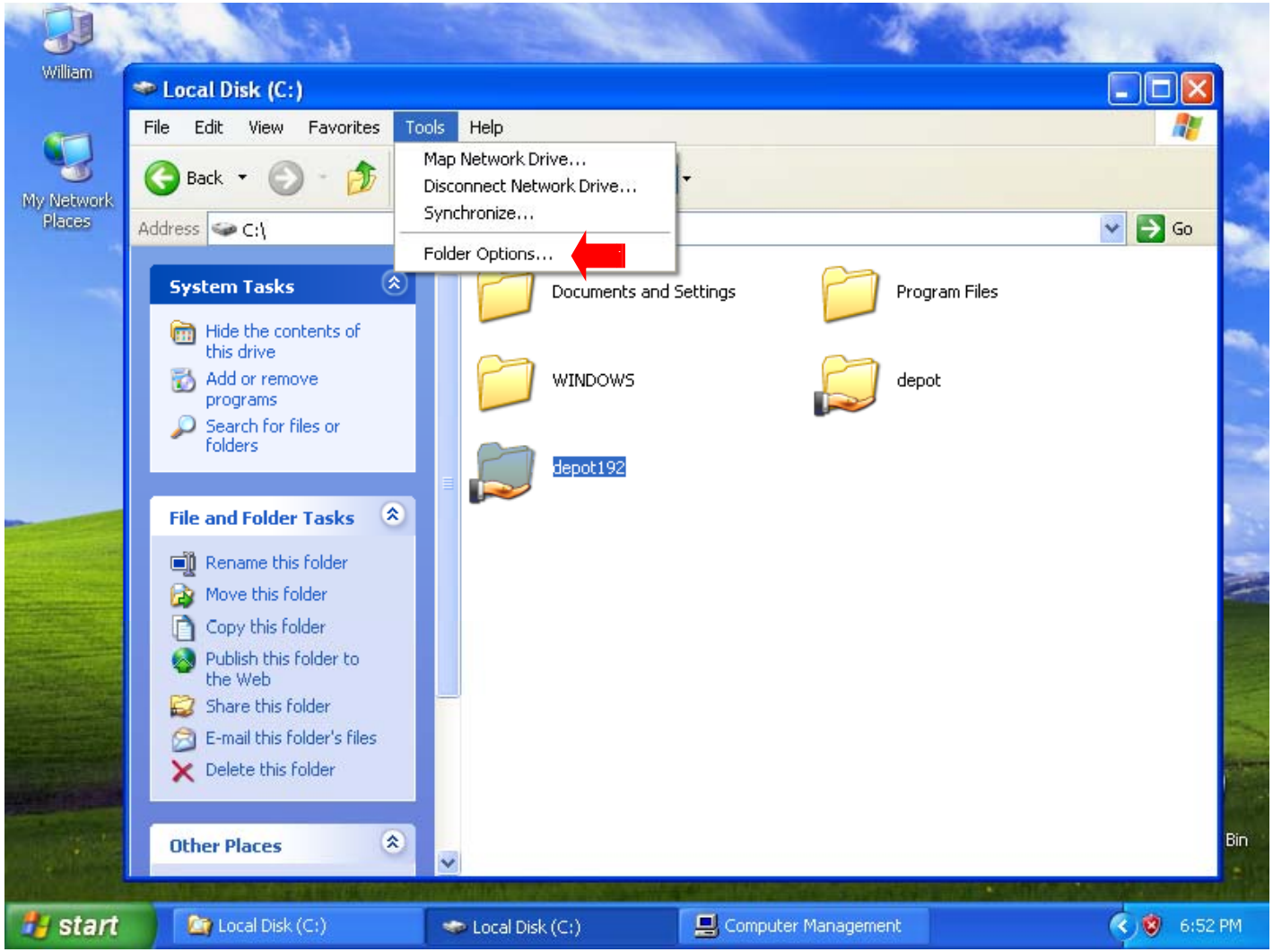
# Windows Shares – *viewing share configurations*

*Shared folders indicated with an open hand*



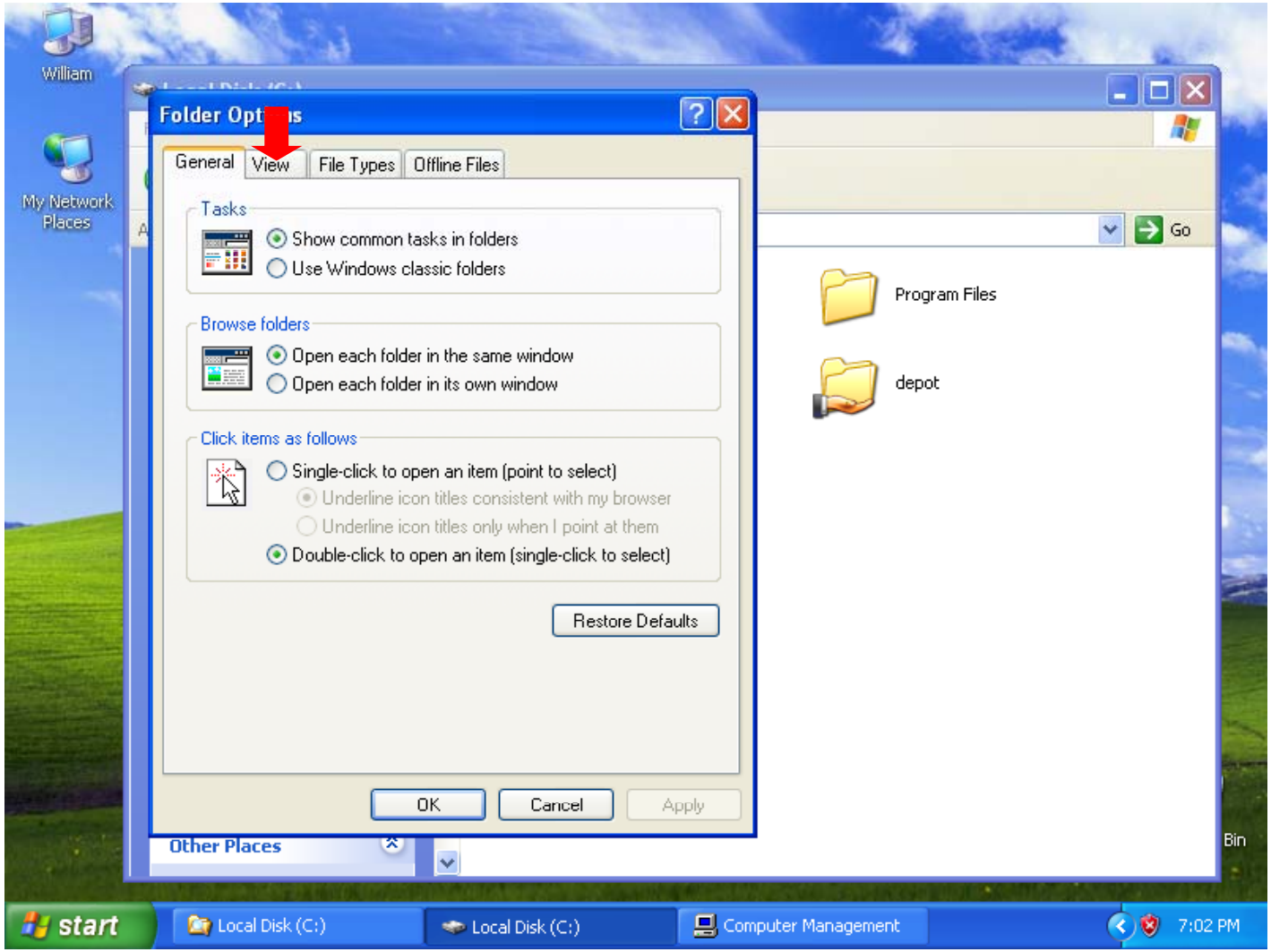
# Windows Shares – *viewing share configurations*

*Pull down Tools menu and select Folder Options*



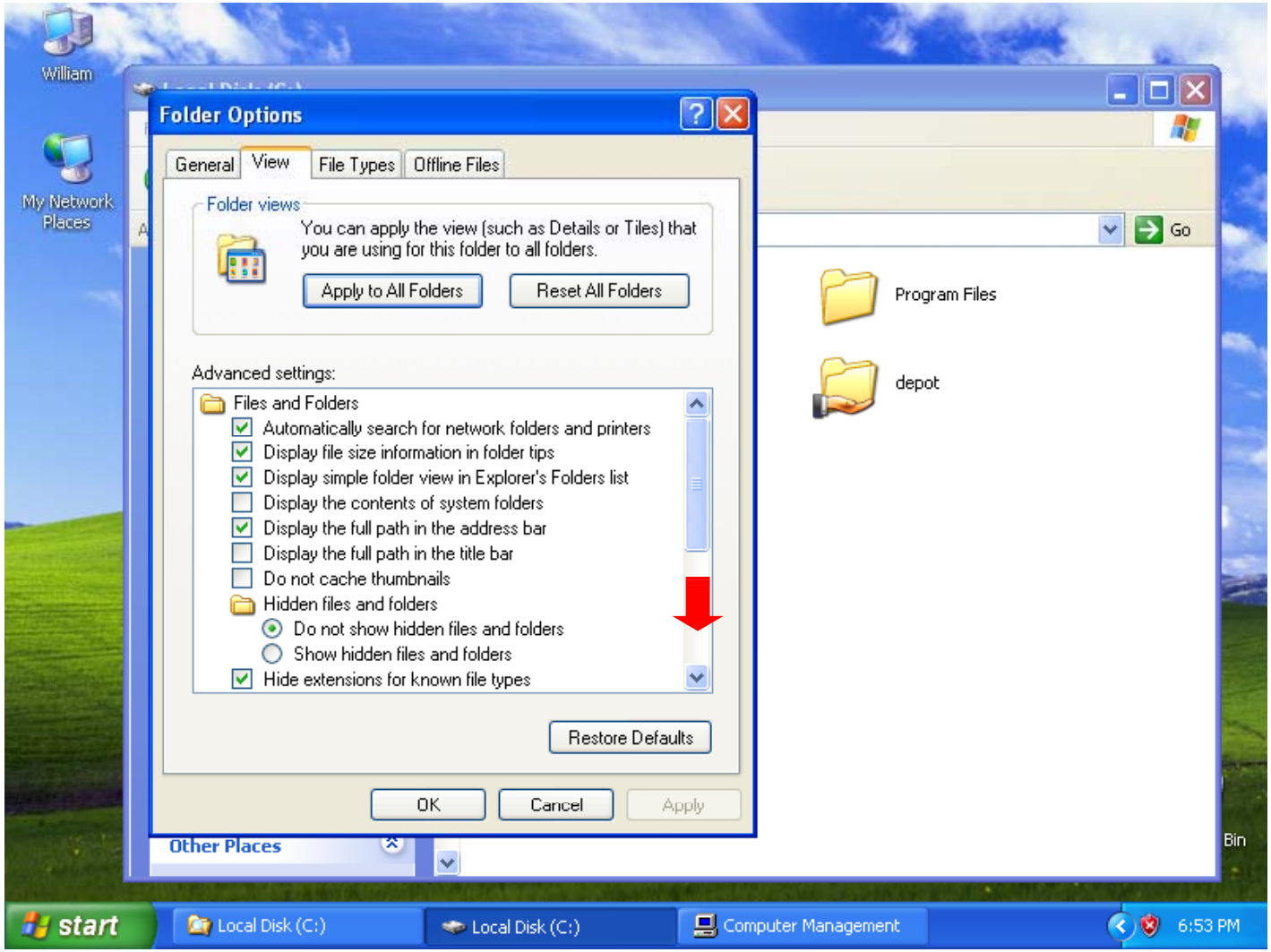
# Windows Shares – *viewing share configurations*

## *Select View tab on Folder Options dialog box*



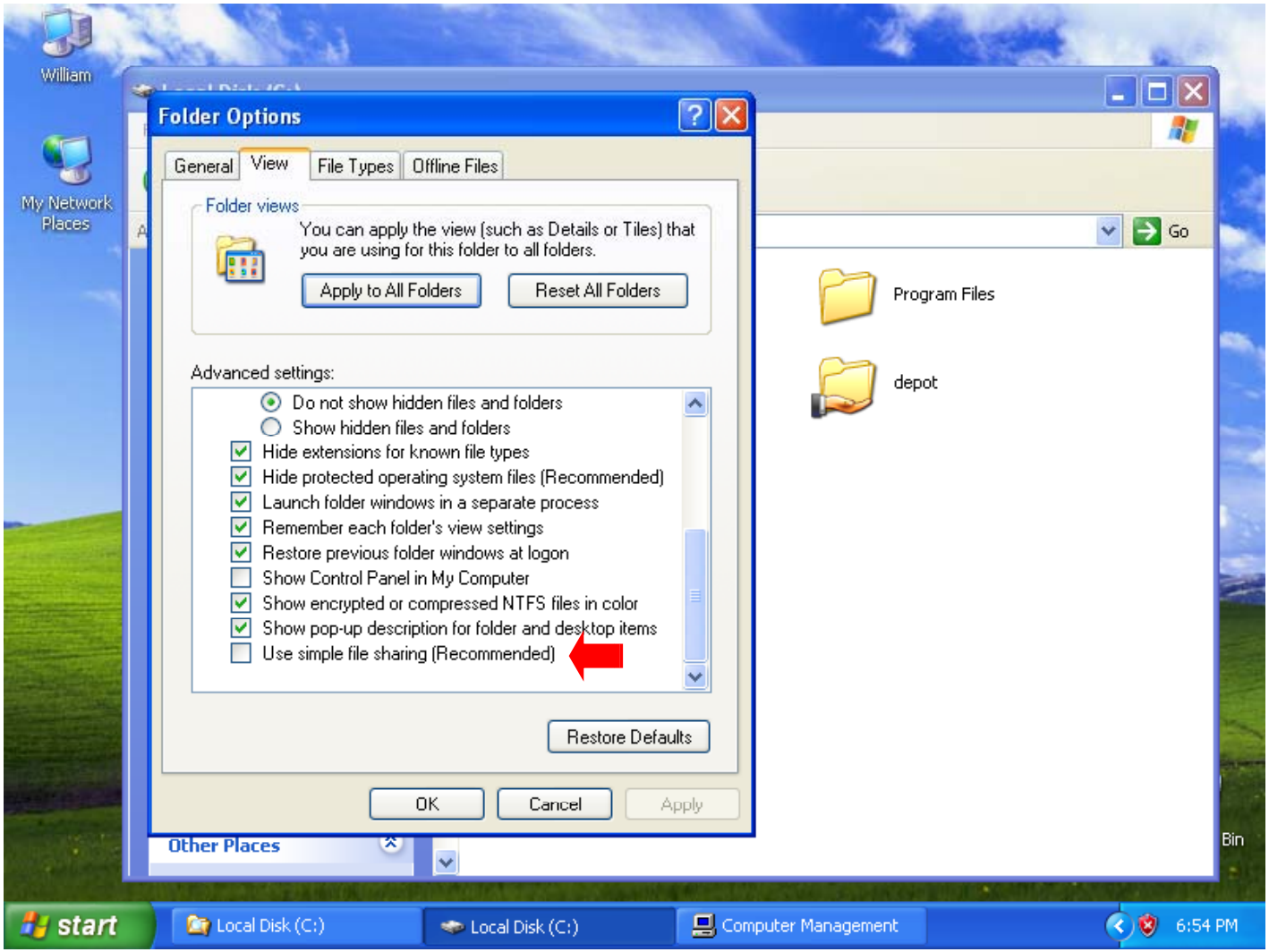
# Windows Shares – *viewing share configurations*

*Scroll down to the last Advanced setting*



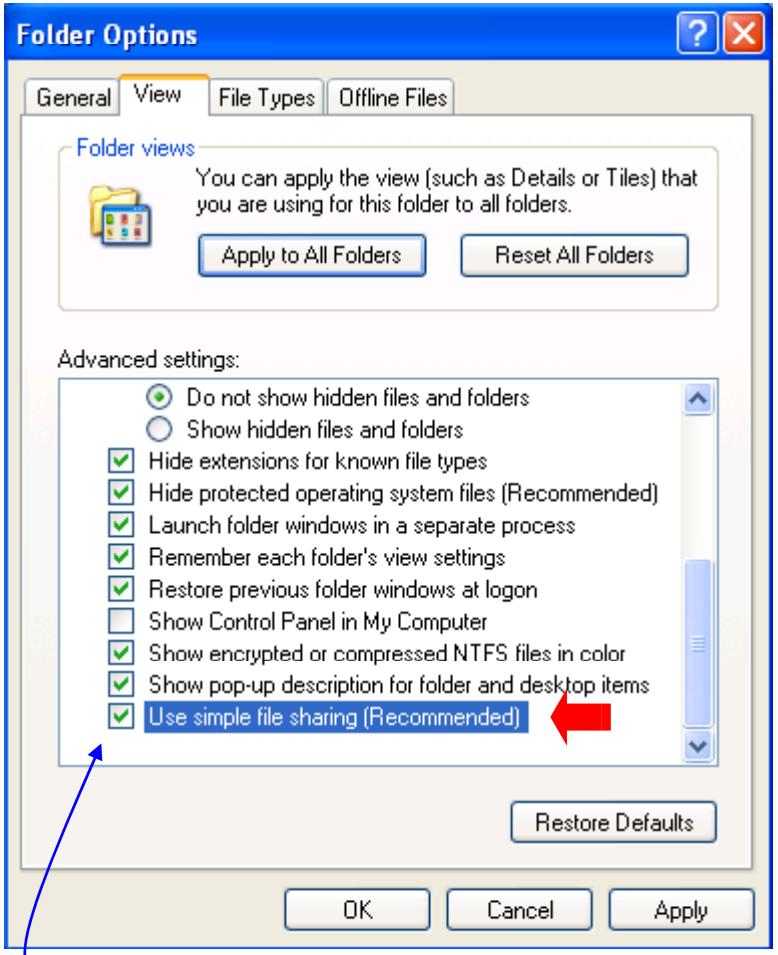
# Windows Shares – *viewing share configurations*

## *Disable simple file sharing (remove the check)*

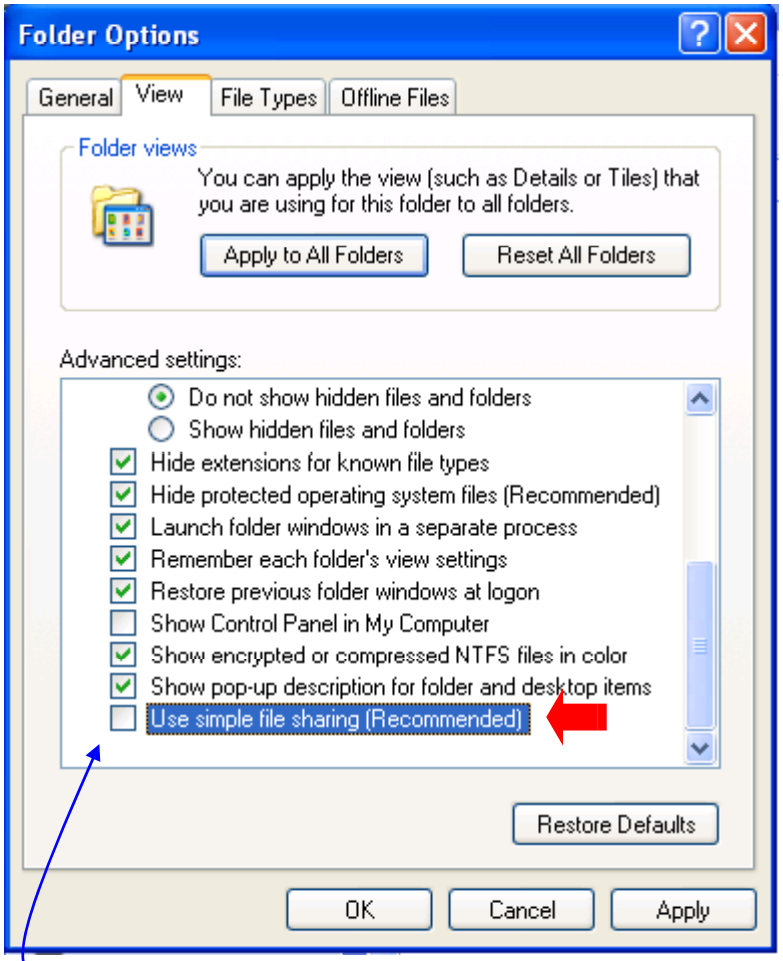


# Windows Shares – *viewing share configurations*

*Select View Tab on Folder Options dialog box*



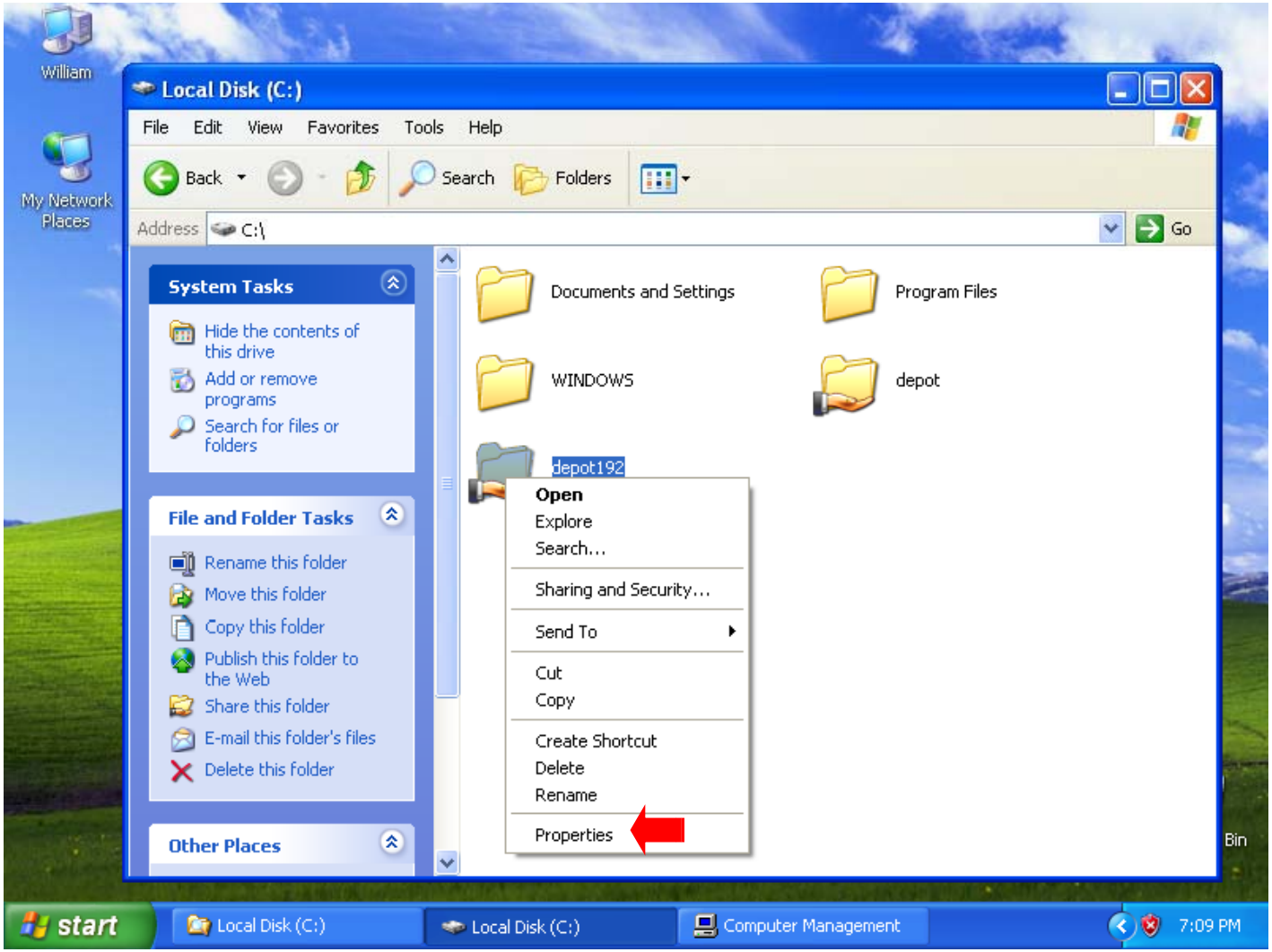

*Simple file sharing **enabled***




*Simple file sharing **disabled***

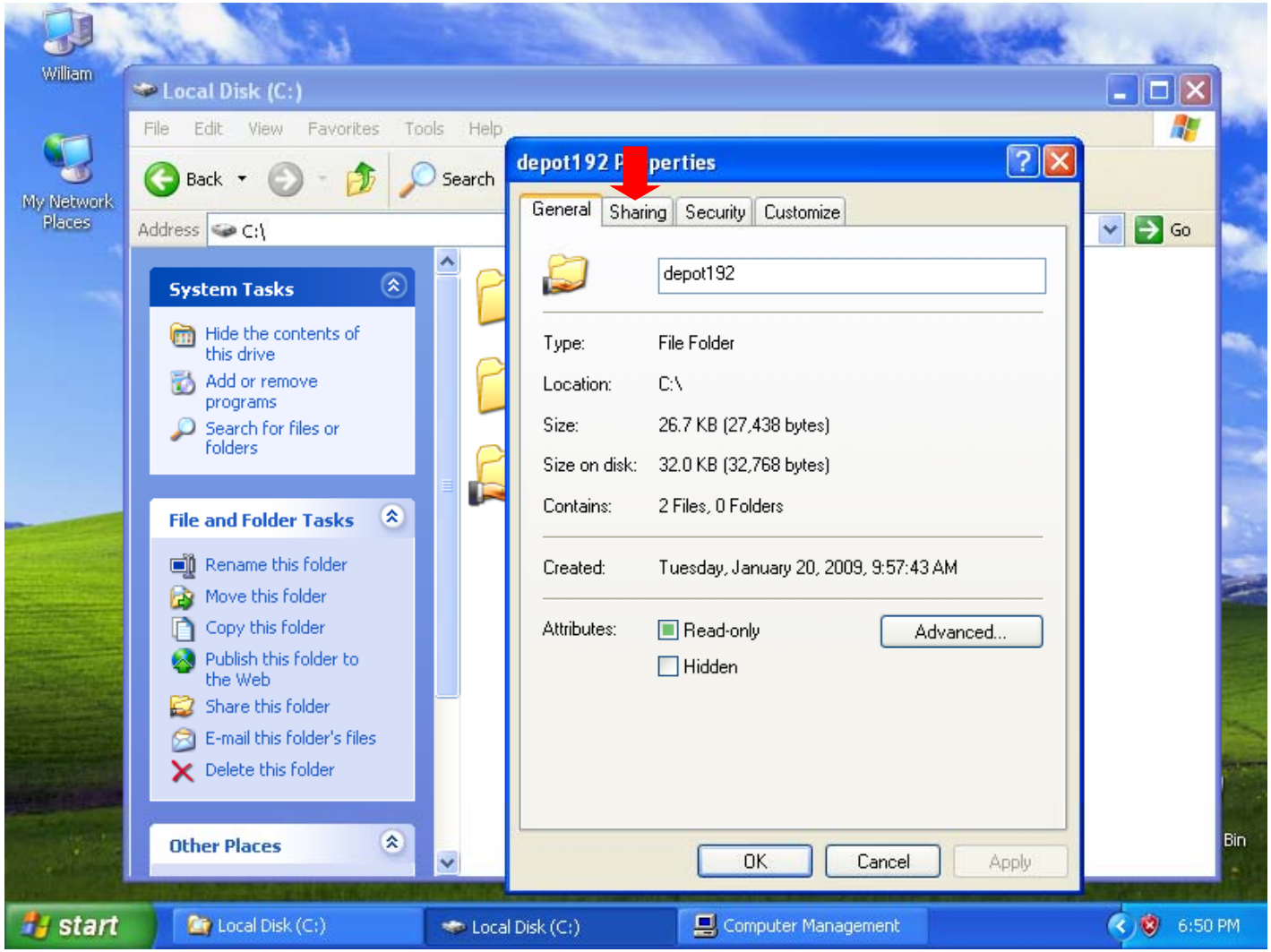
# Windows Shares – *viewing share configurations*

*For any folder, right click and select properties*



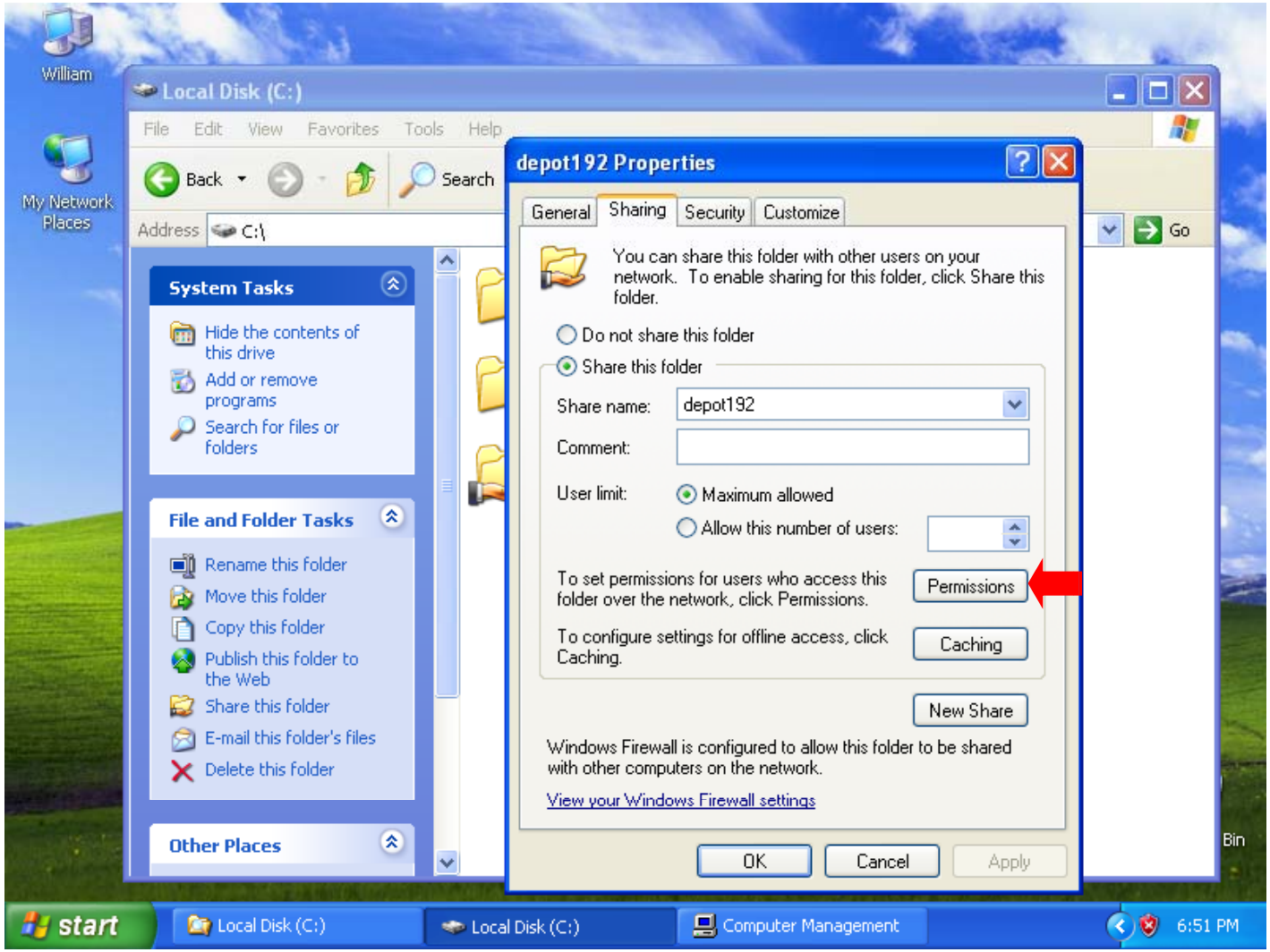
# Windows Shares – *viewing share configurations*

*Select the Sharing tab*



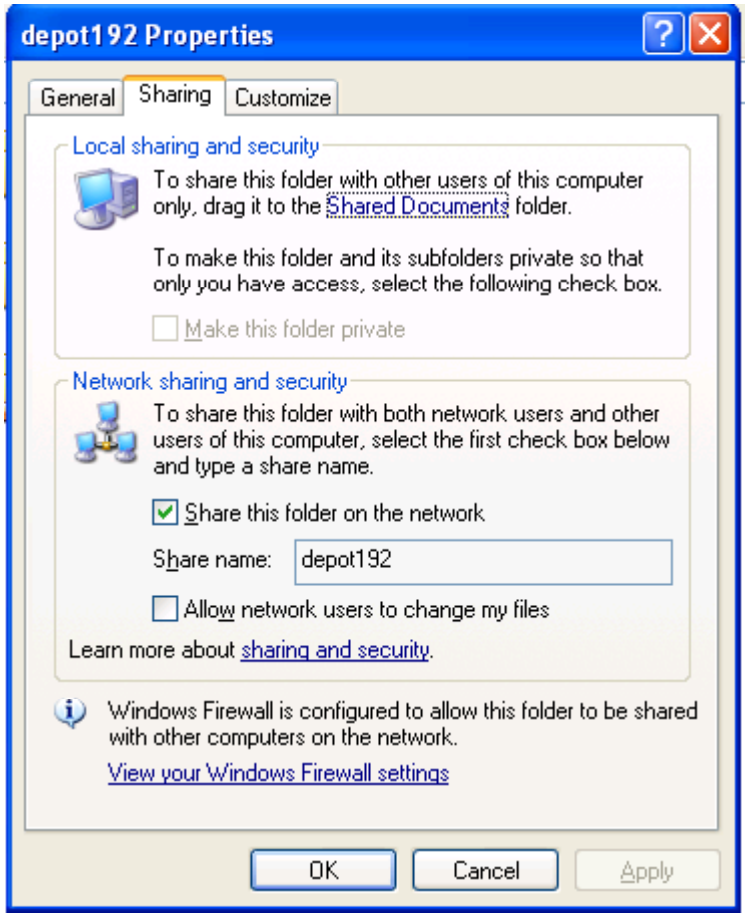
# Windows Shares – *viewing share configurations*

*Click on the Permissions button*

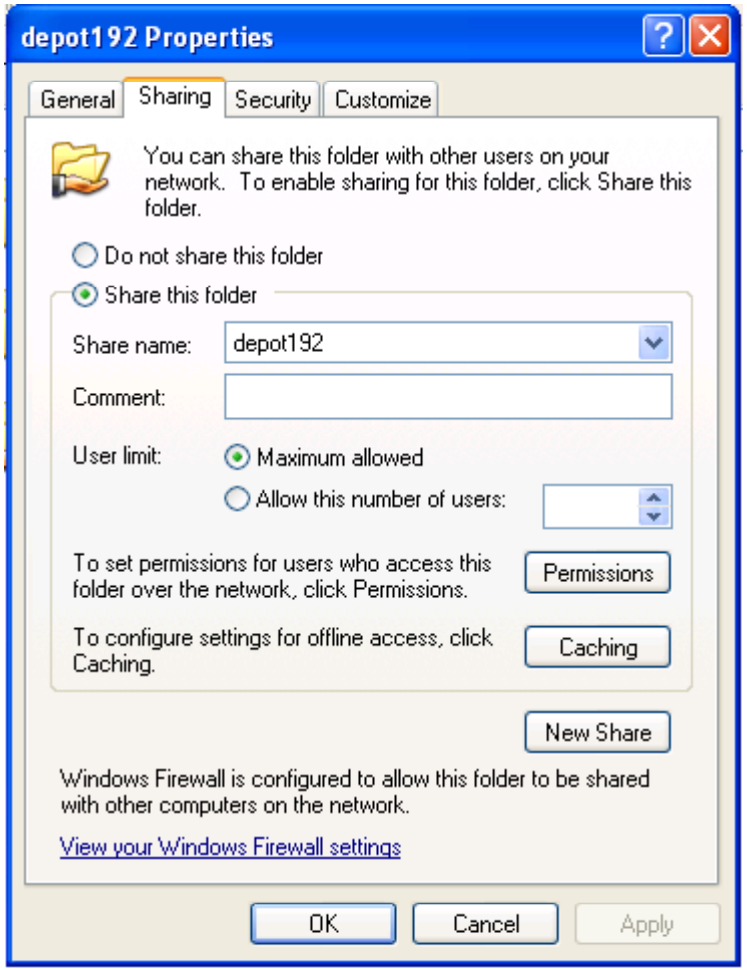


# Windows Shares – *viewing share configurations*

## *Simple file sharing*



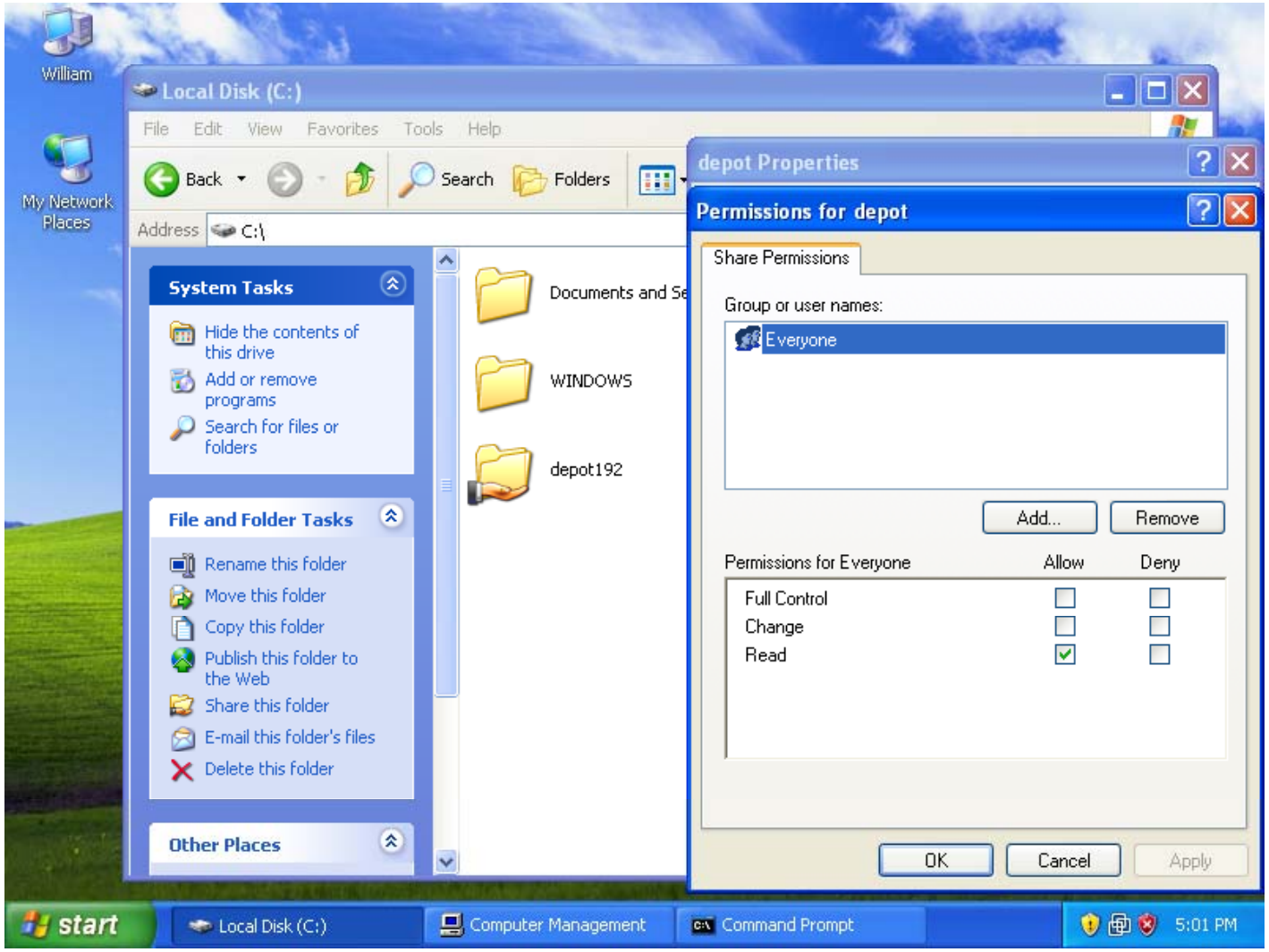

## *Simple file sharing disabled*




*Note: Permissions button and Security tab have been added*

# Windows Shares – *viewing share configurations*

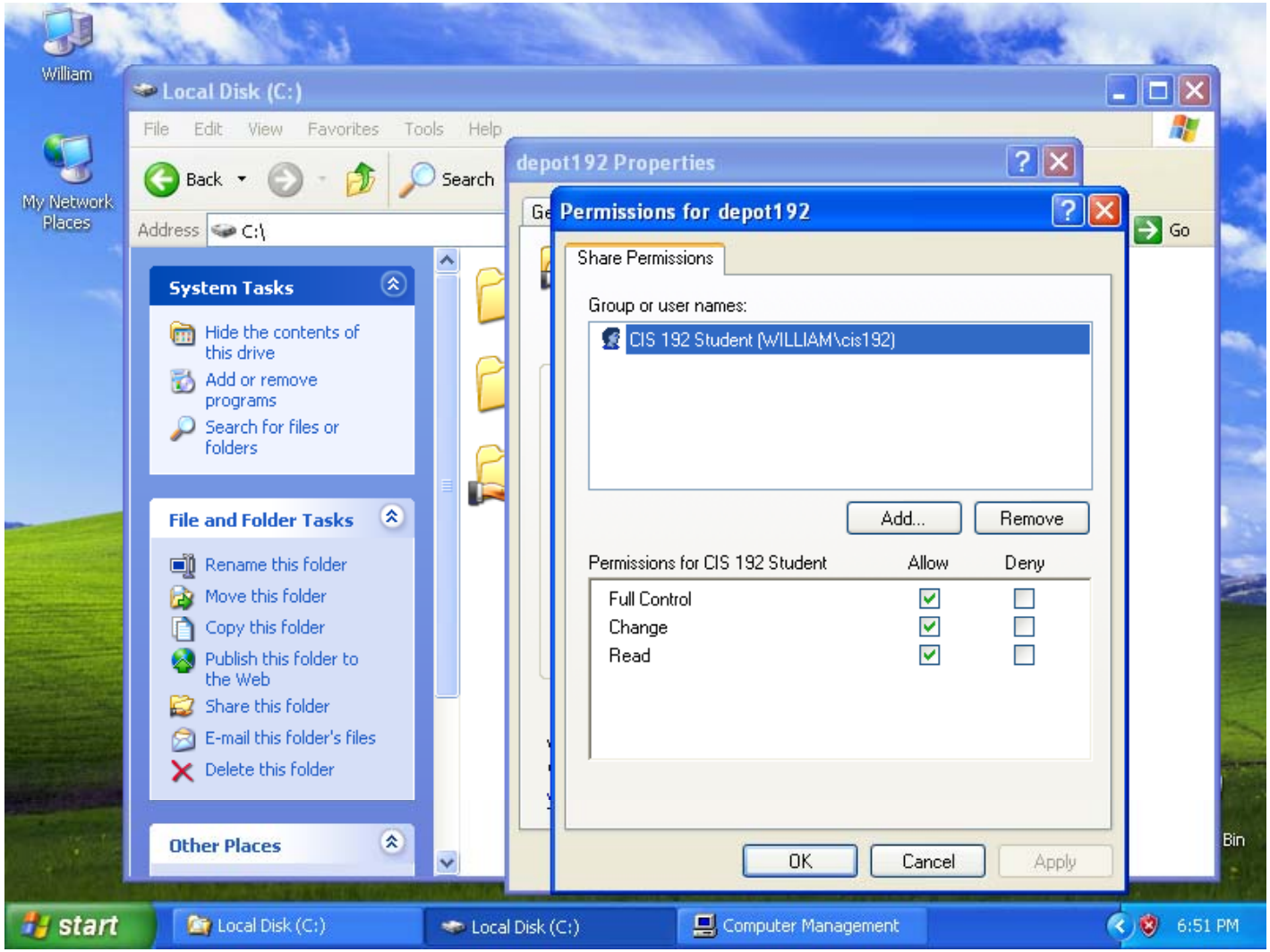
*Share permissions on \\william\depot*




*Read permissions for everyone*

# Windows Shares – *viewing share configurations*

*Share permissions on \\william\depot192*



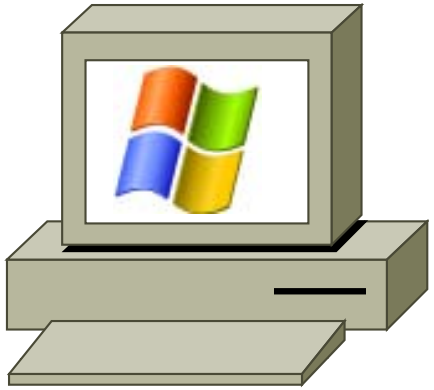

*cis192 has full control over this share.*

*cis191 has no permissions specified*

Examine the shares on William:

- Verify that Everyone has Read permission on the Depot share
- Verify that cis191 has no permissions for the depot192 share.
- Verify that cis192 has Full Control, Change and Read permissions on the depot192 share.
- Can you give cis192 Full Control and remove (uncheck) Change and Read permissions? What would the UI police say about this?

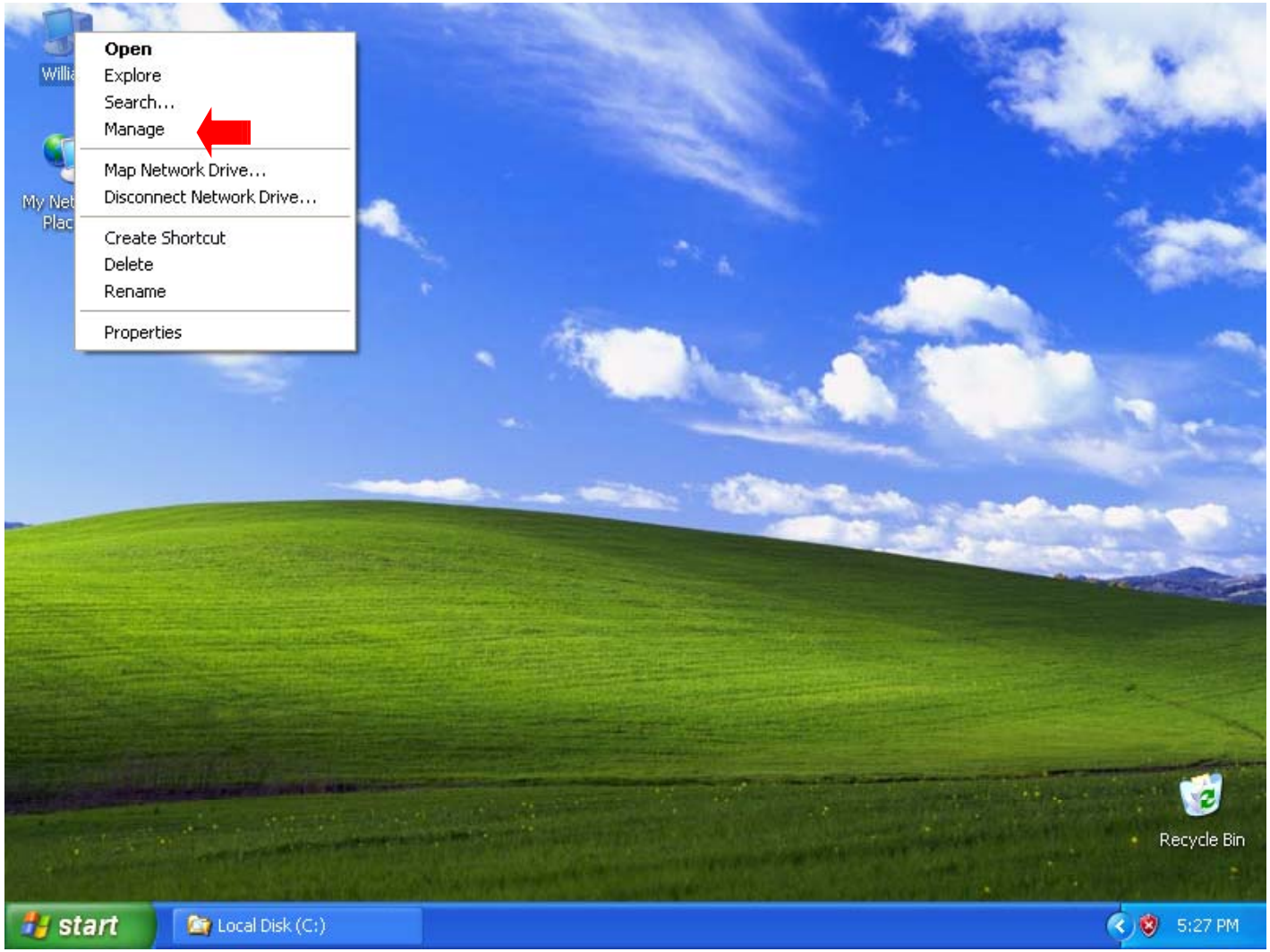
**William**



# Monitoring Shares

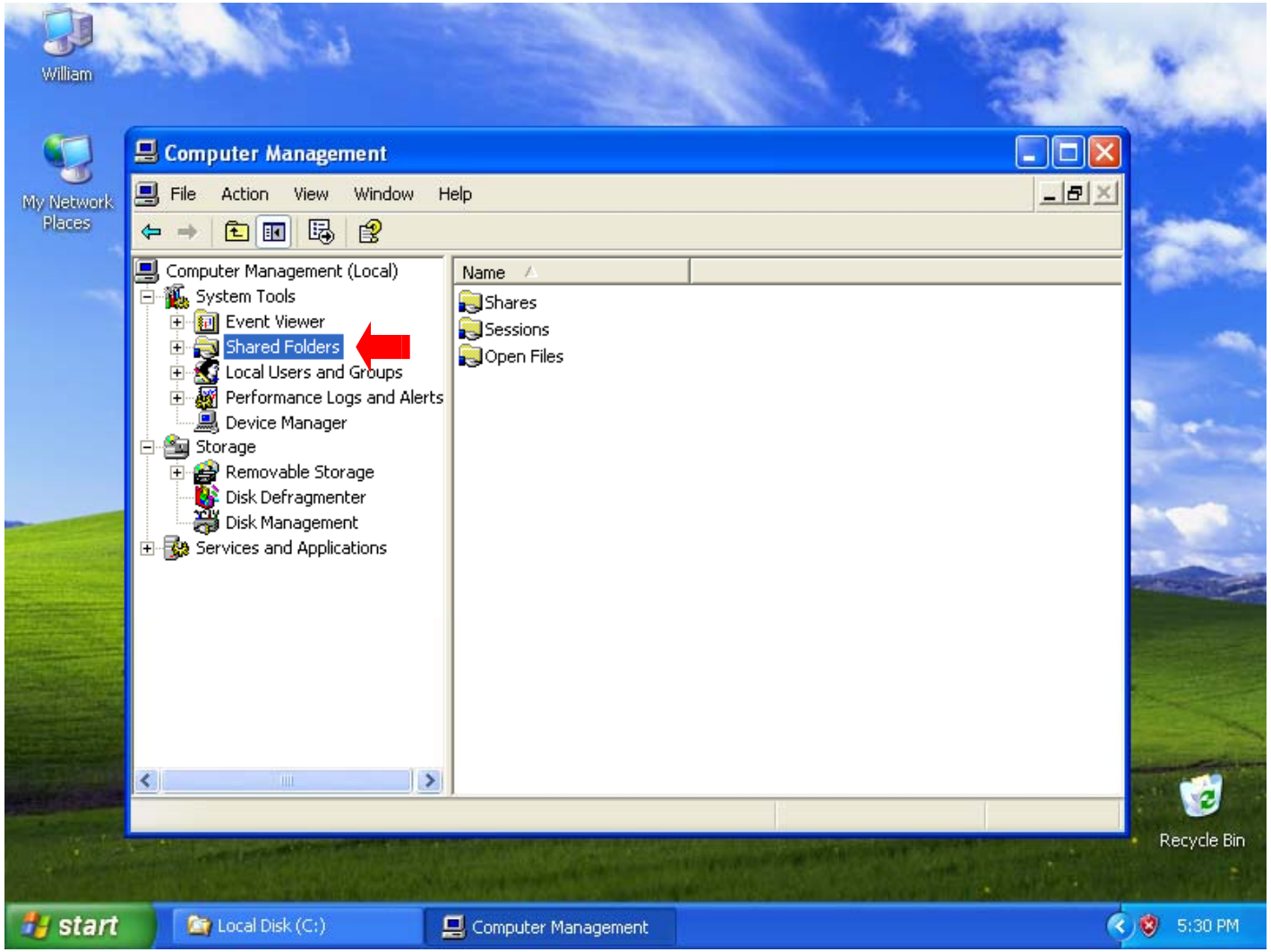
# Windows Shares – *monitoring shares*

*Right click on My Computer (William here) and select Manage*



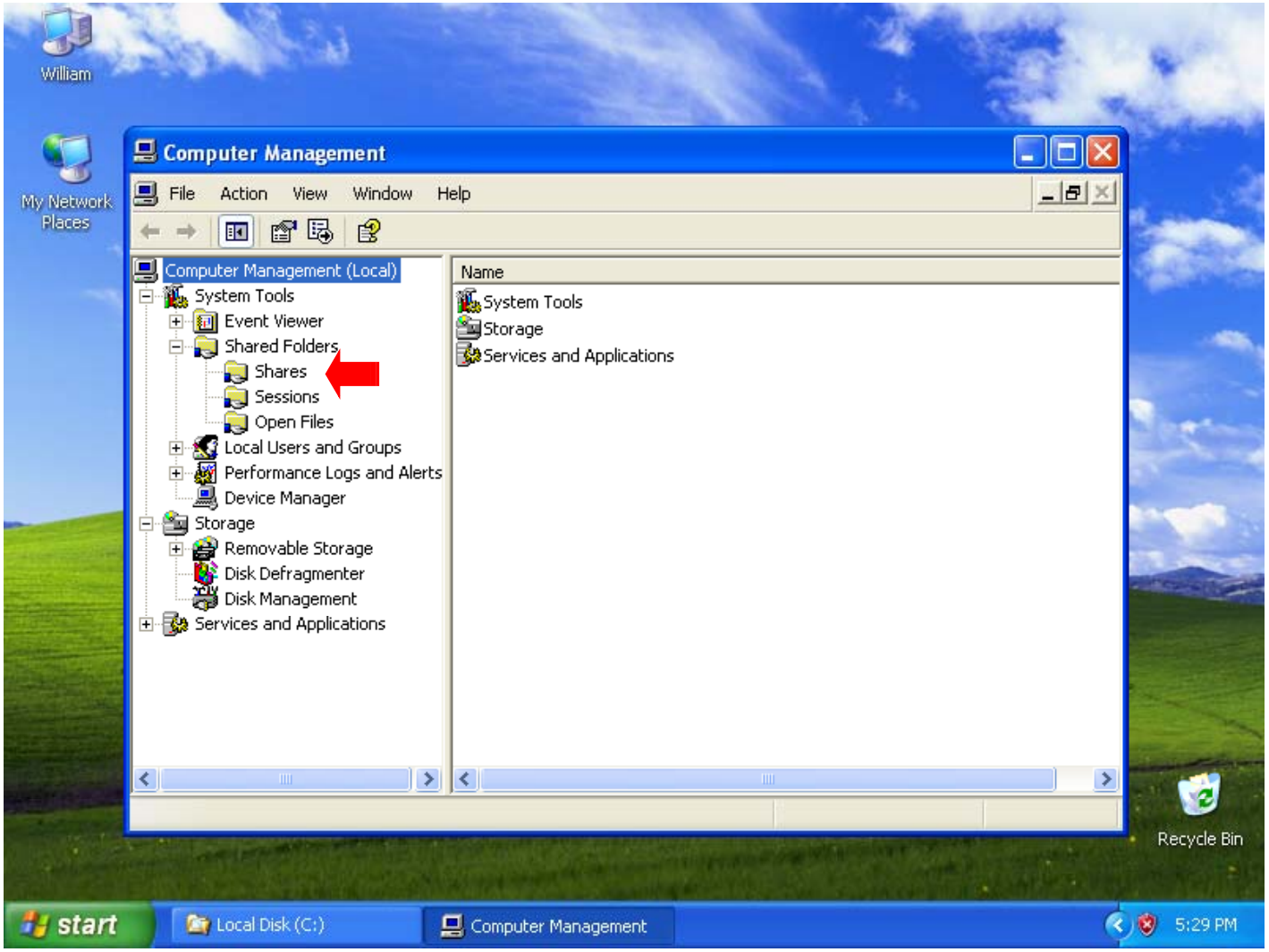
# Windows Shares – *monitoring shares*

*Expand (click on +) Shared Folders on left panel*



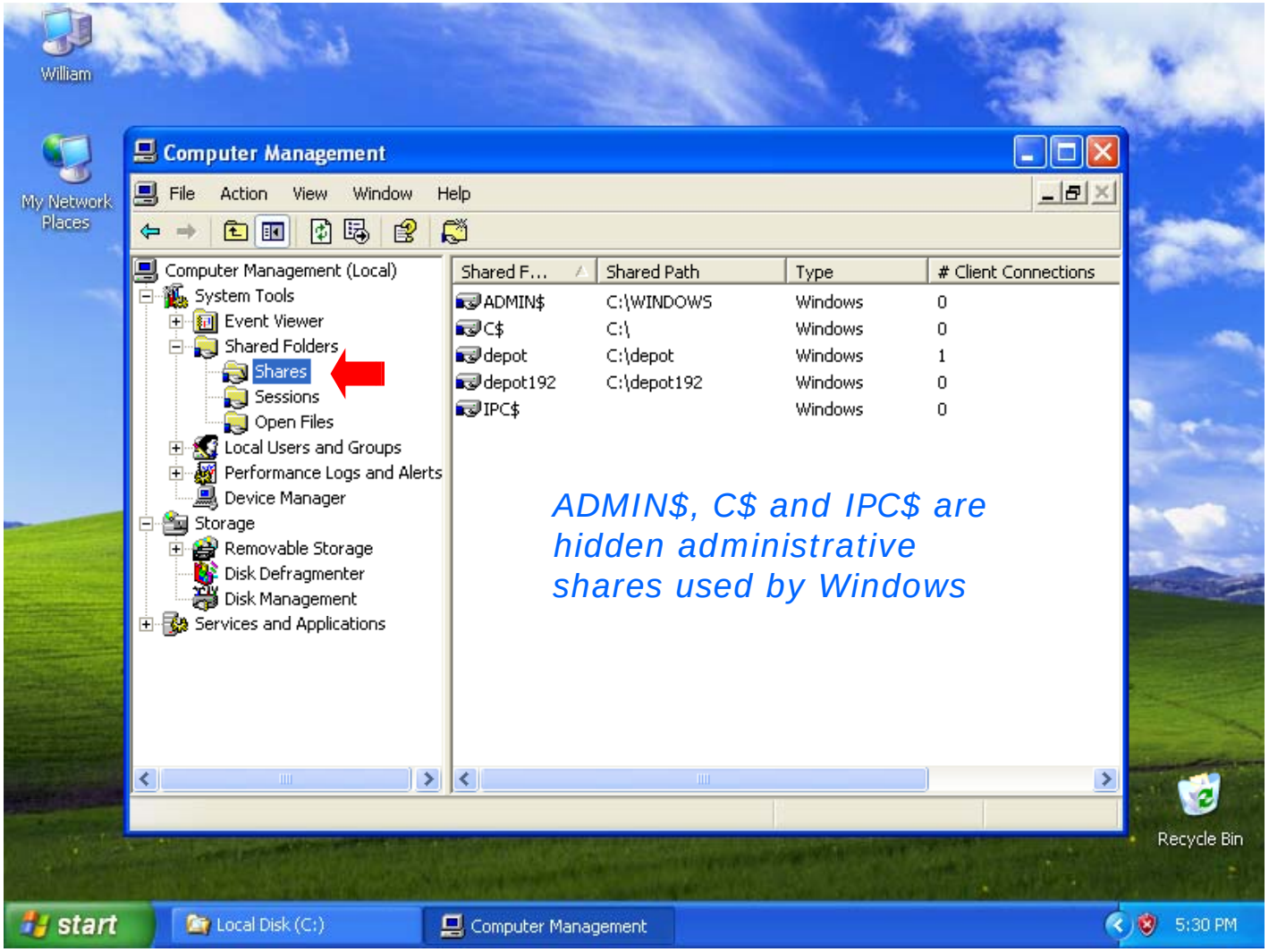
# Windows Shares – *monitoring shares*

*Select Shares on left panel to see available shares*



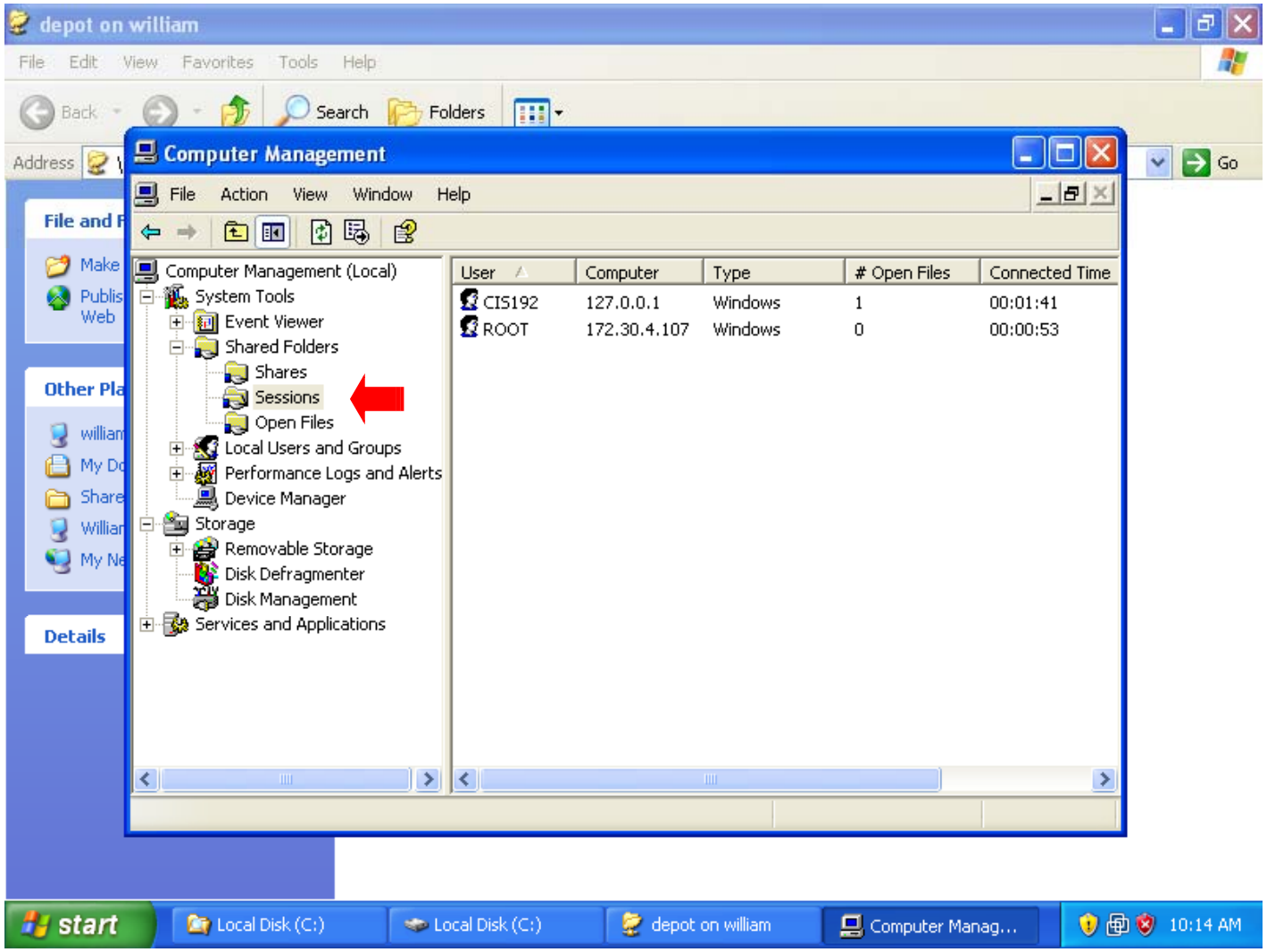
# Windows Shares – *monitoring shares*

*Shares will show all available shares*



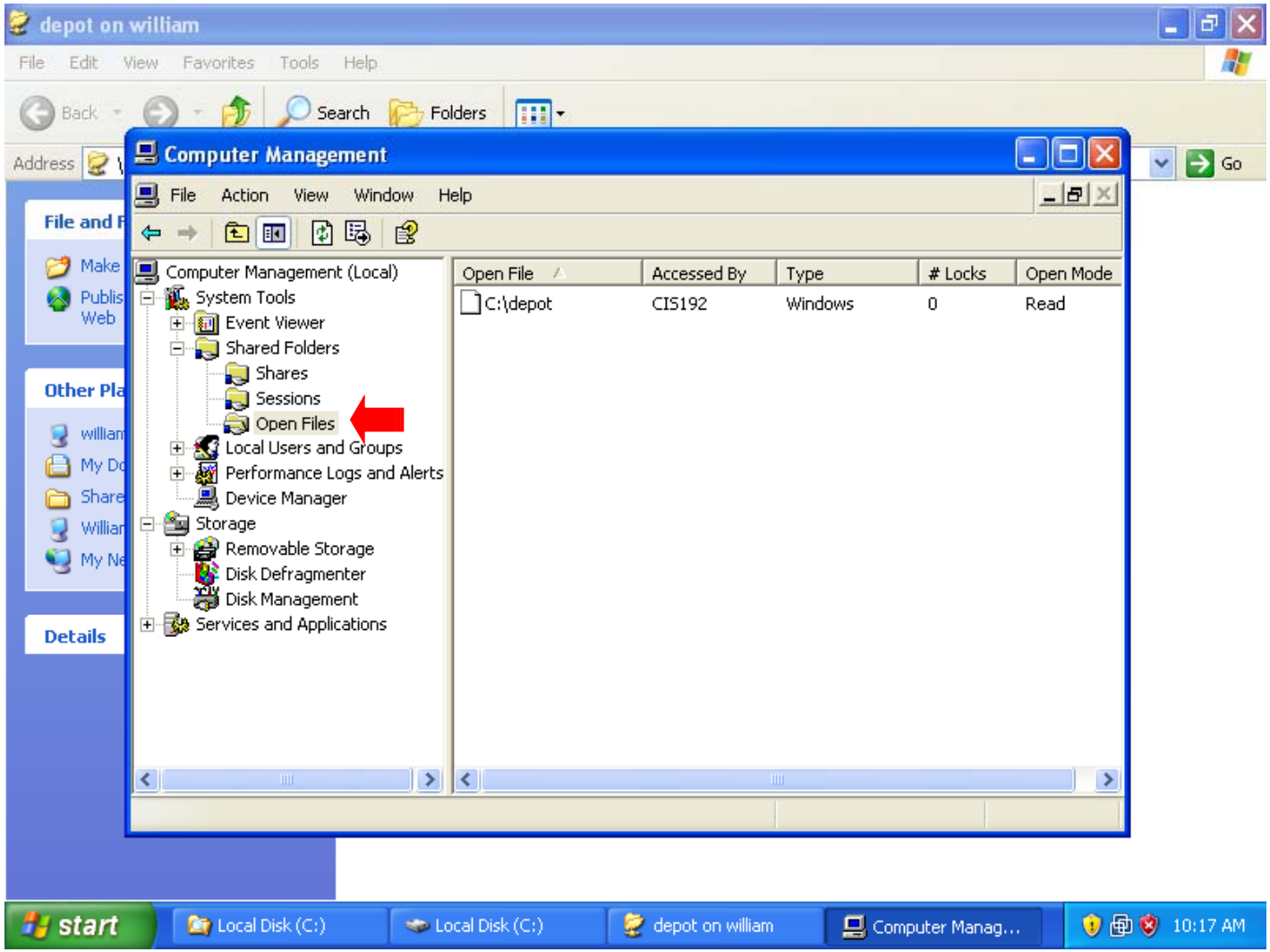
# Windows Shares – *monitoring shares*

*Sessions will show users accessing the shares*



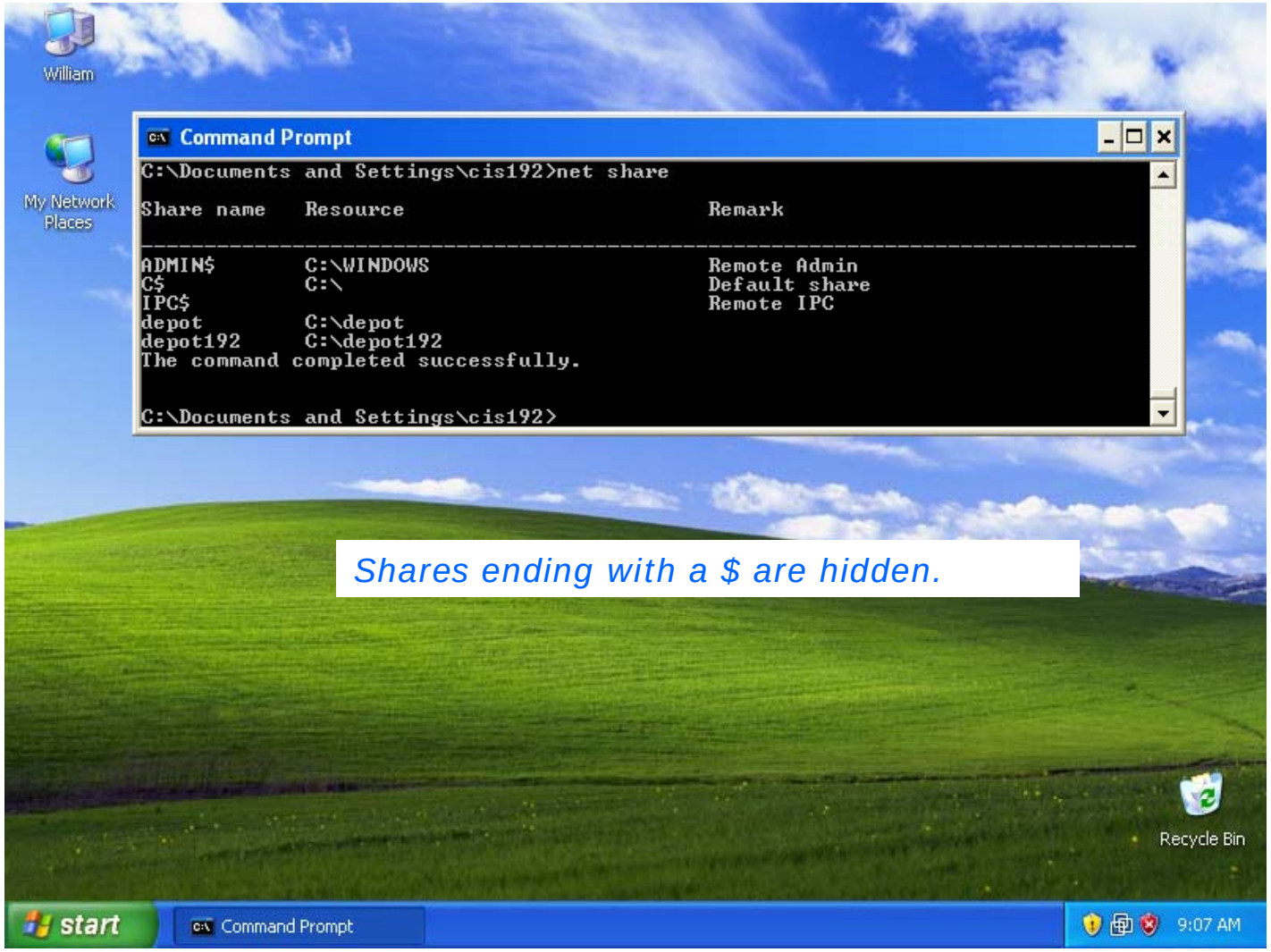
# Windows Shares – *monitoring shares*

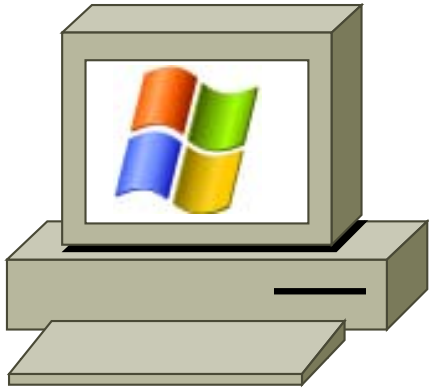
*Open Files will show files being accessed (for Windows Users)*



# Windows Shares – *viewing share configurations*

## *Using the command line to view local shares*

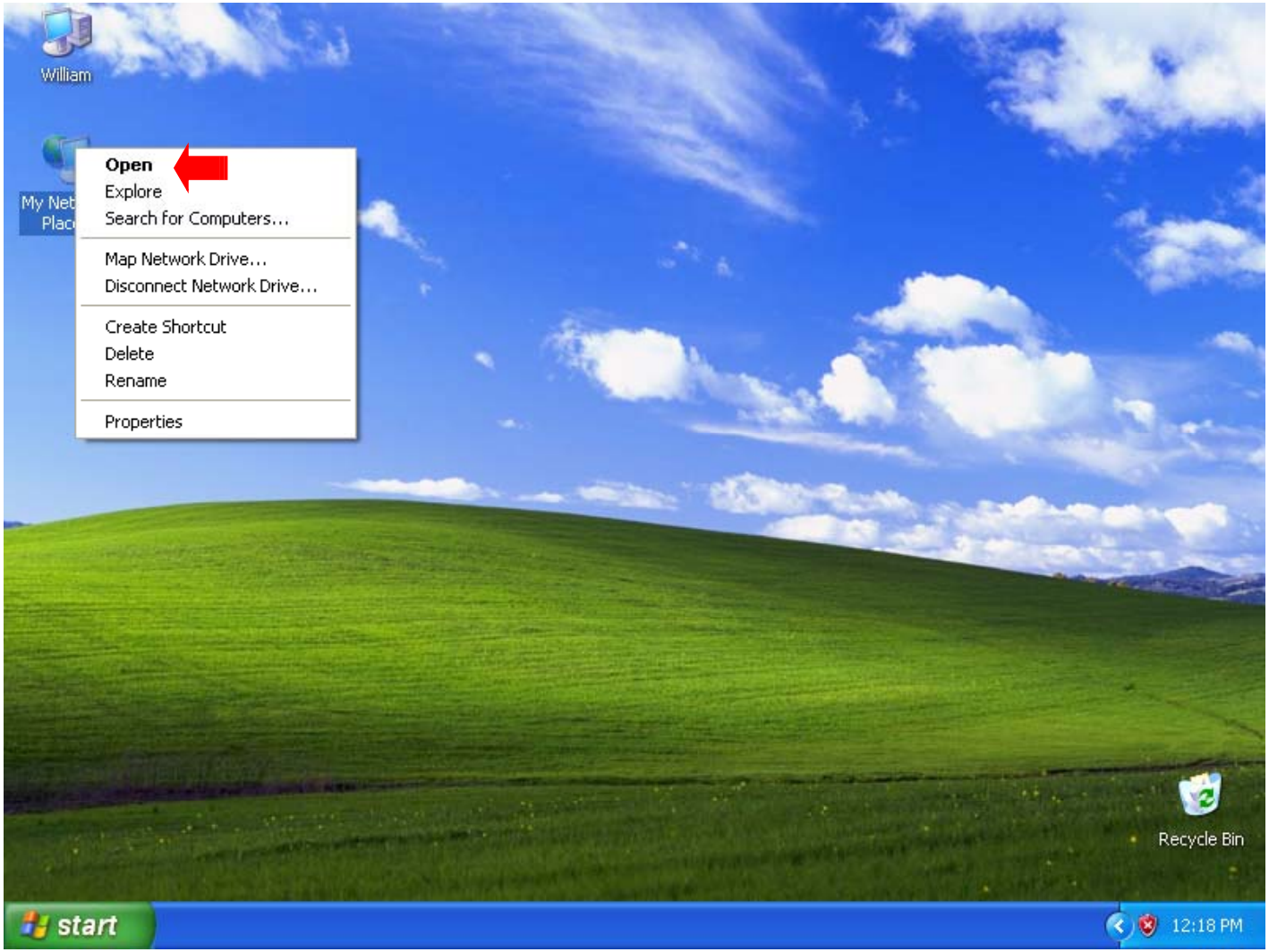




# Browsing Shares

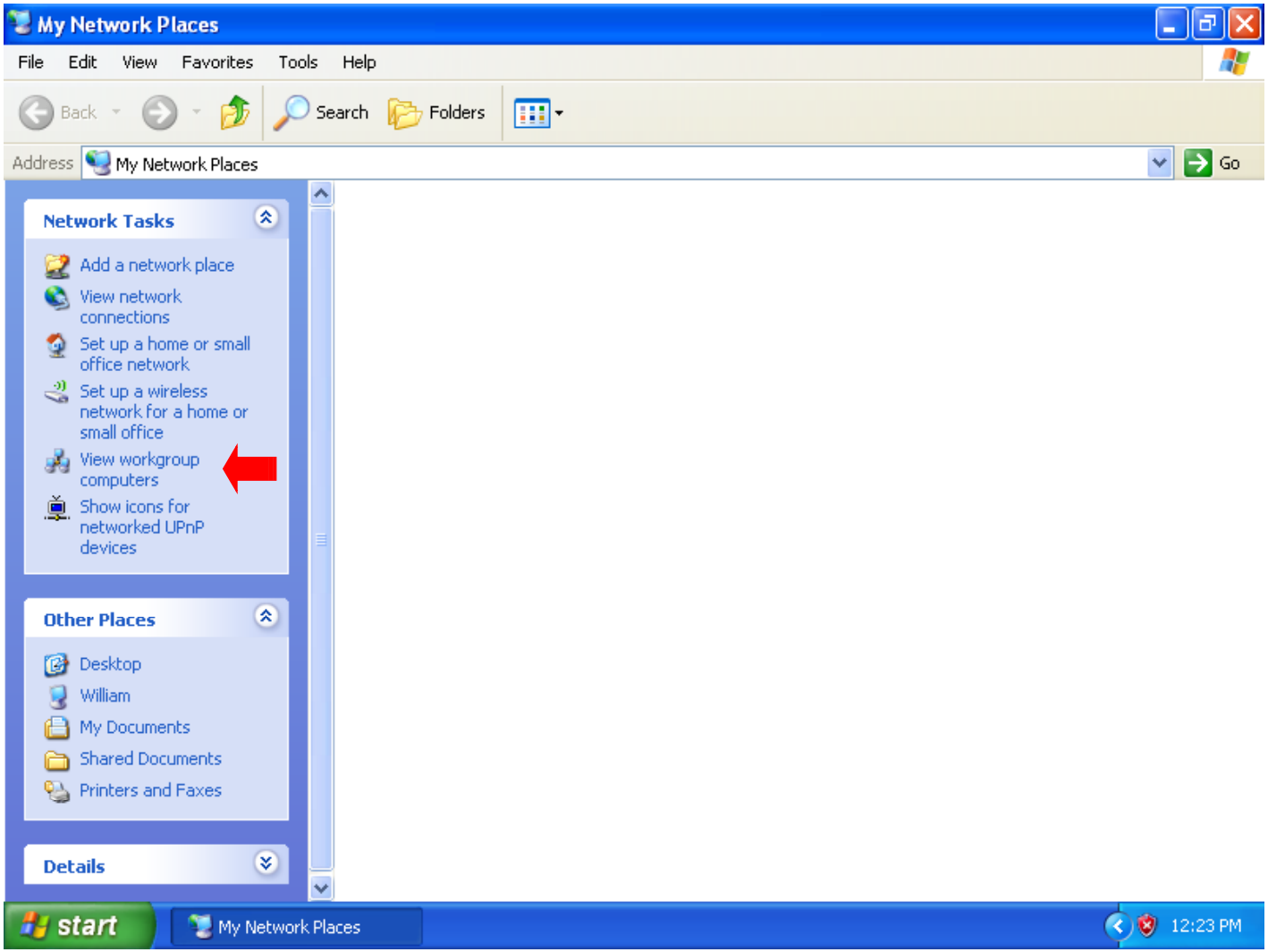
# Windows Shares – *browsing shares*

## *Open My Network Places icon on desktop*



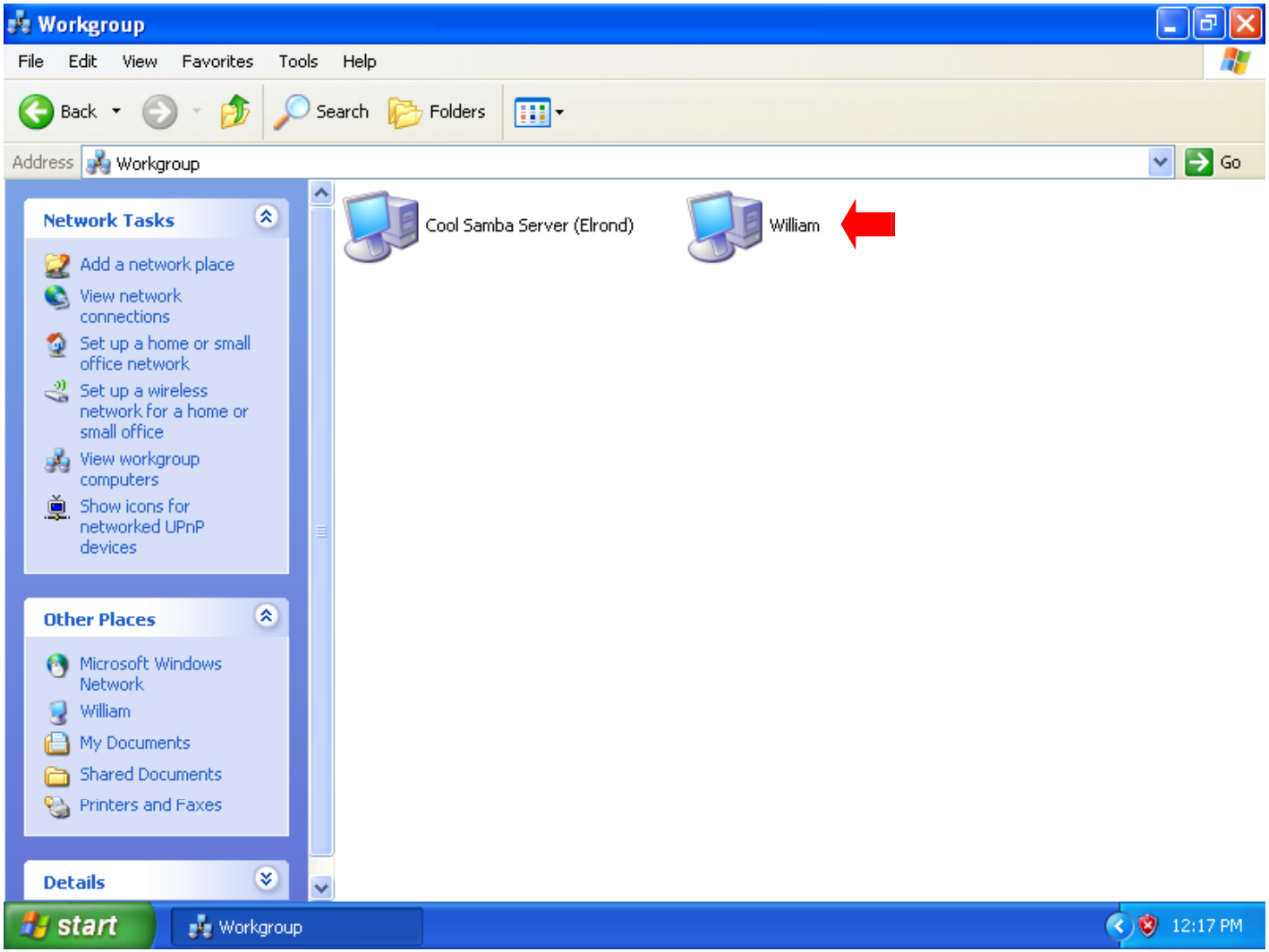
# Windows Shares – *browsing shares*

*Click on View workgroup computers*



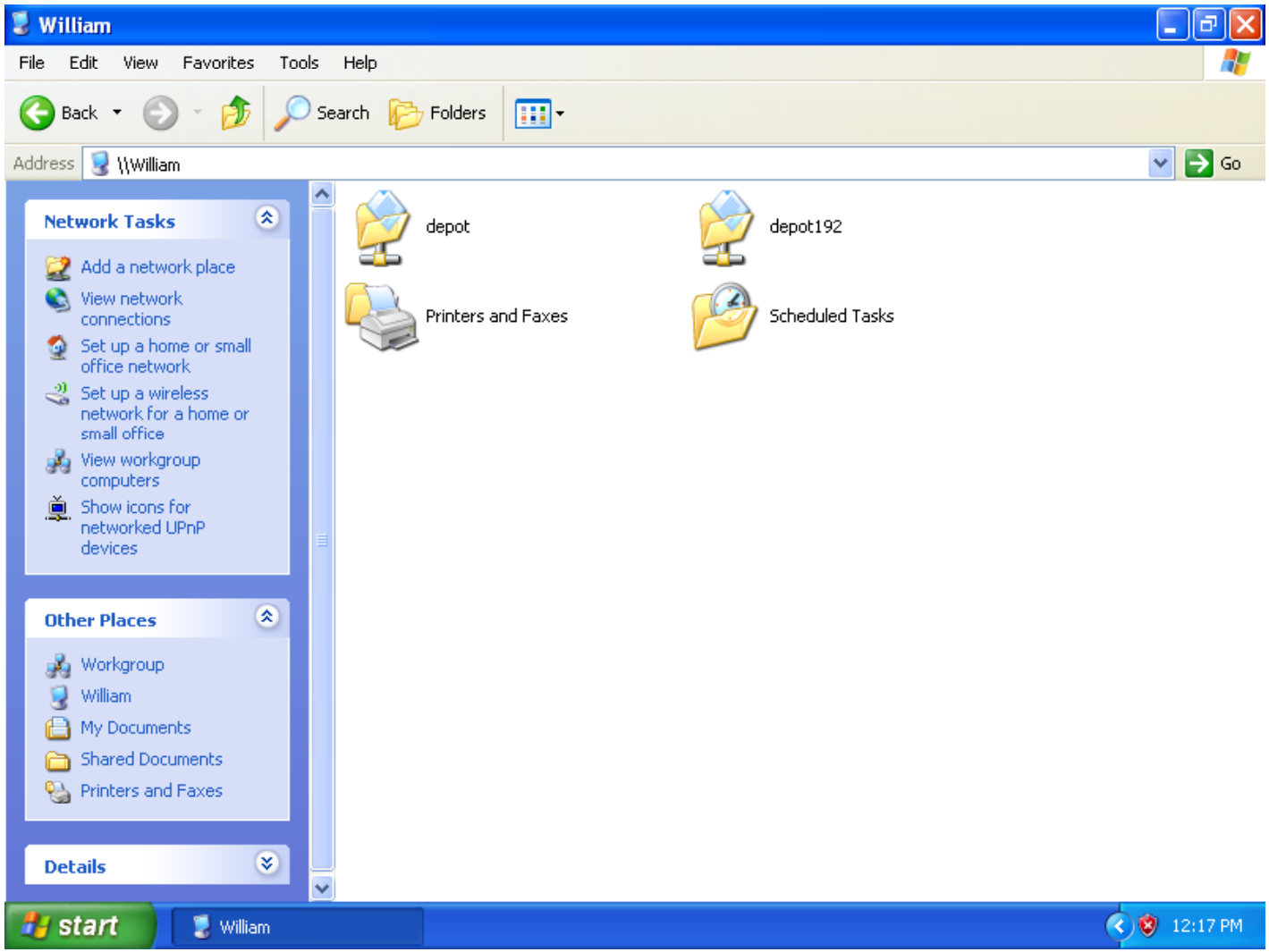
# Windows Shares – *browsing shares*

## *Open William*



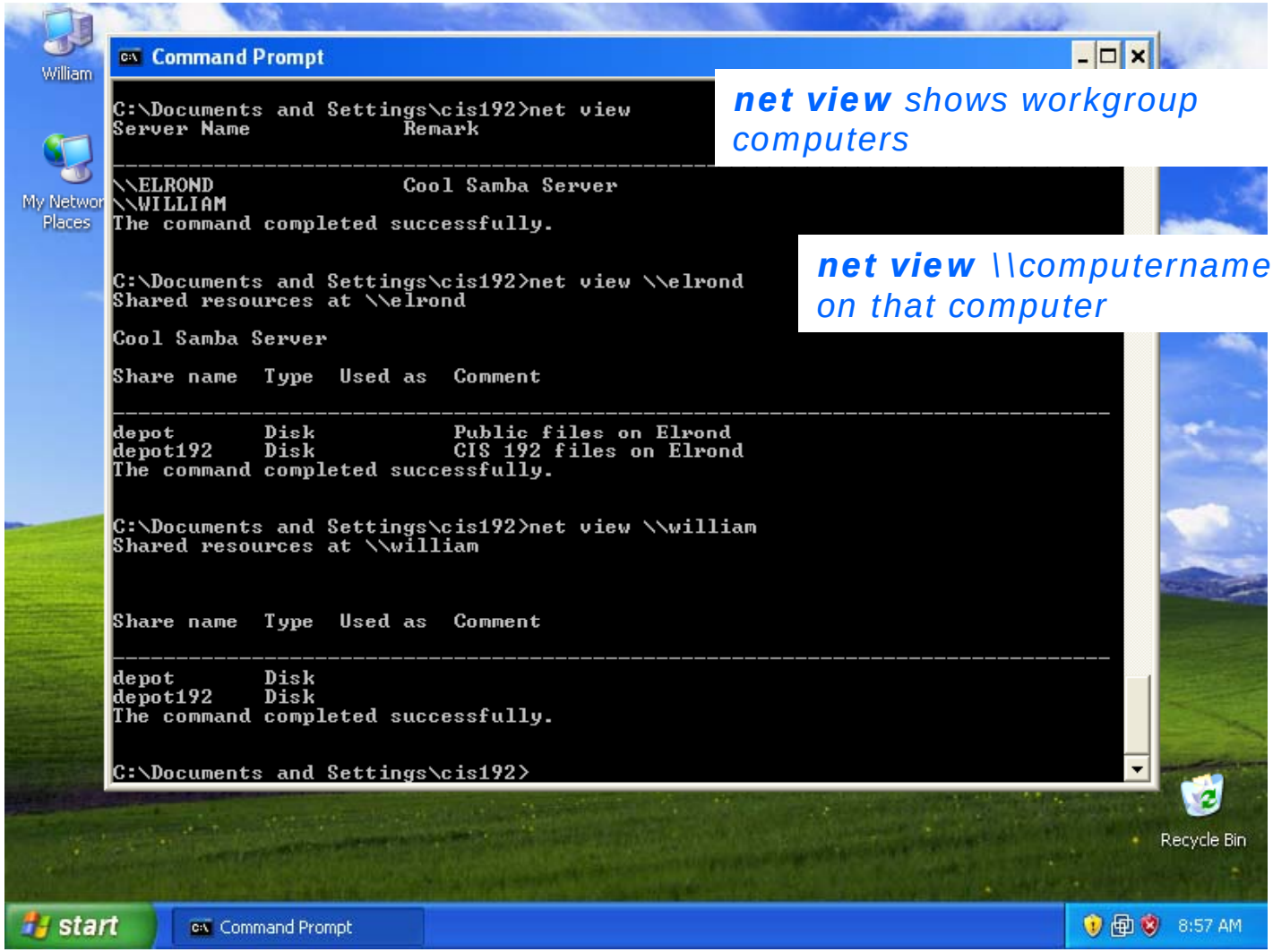
# Windows Shares – *browsing shares*

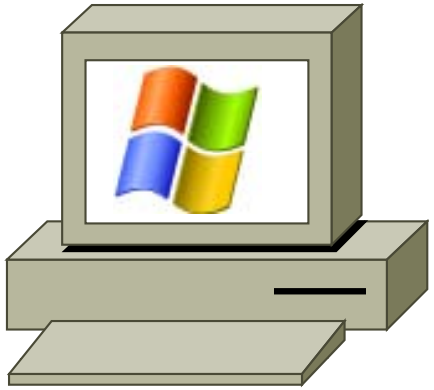
*The depot and depot192 shares on William are displayed*



# Windows Shares – *browsing shares*

## *Browsing from the Windows command line*

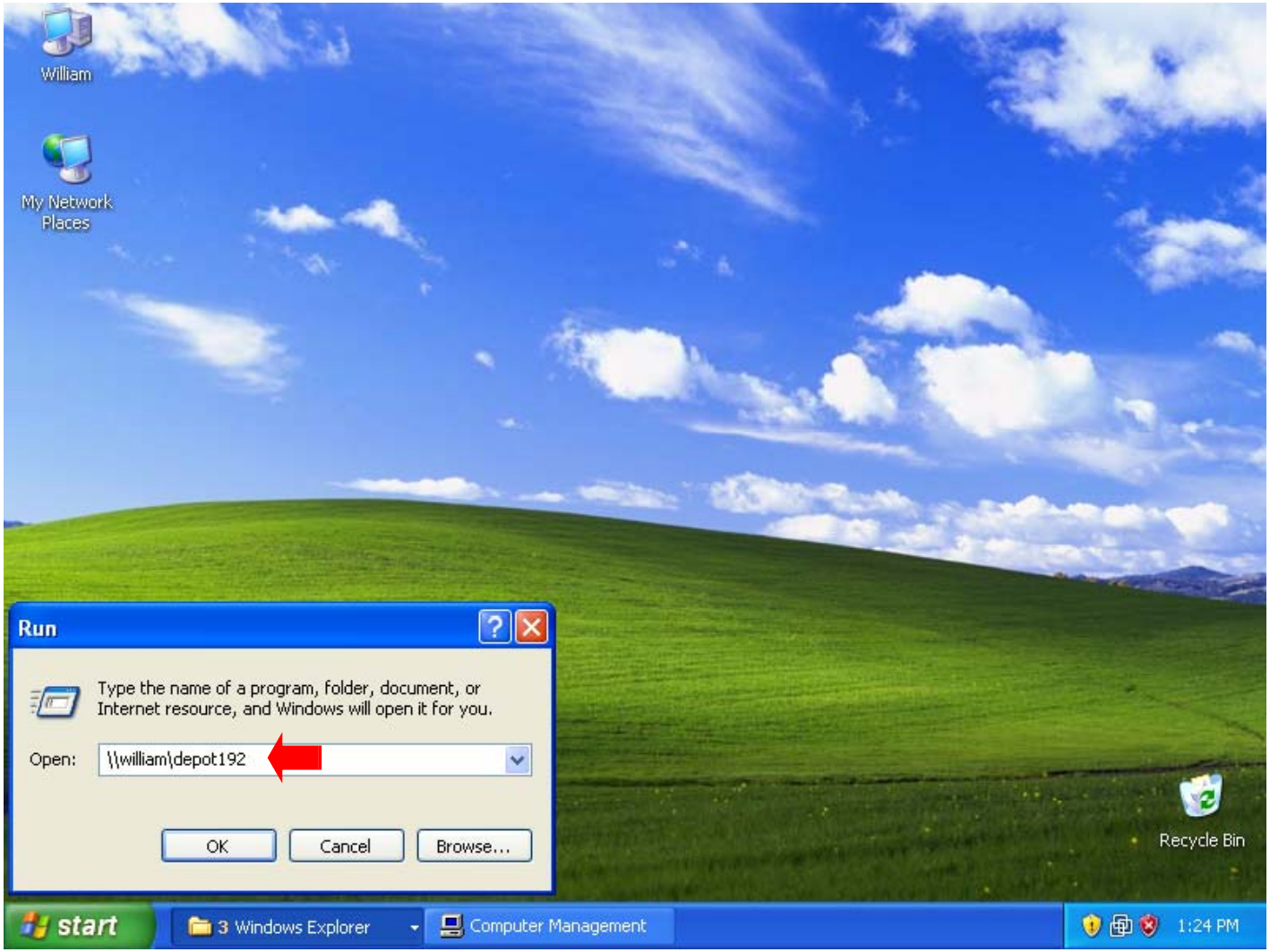




# Successful Share Access

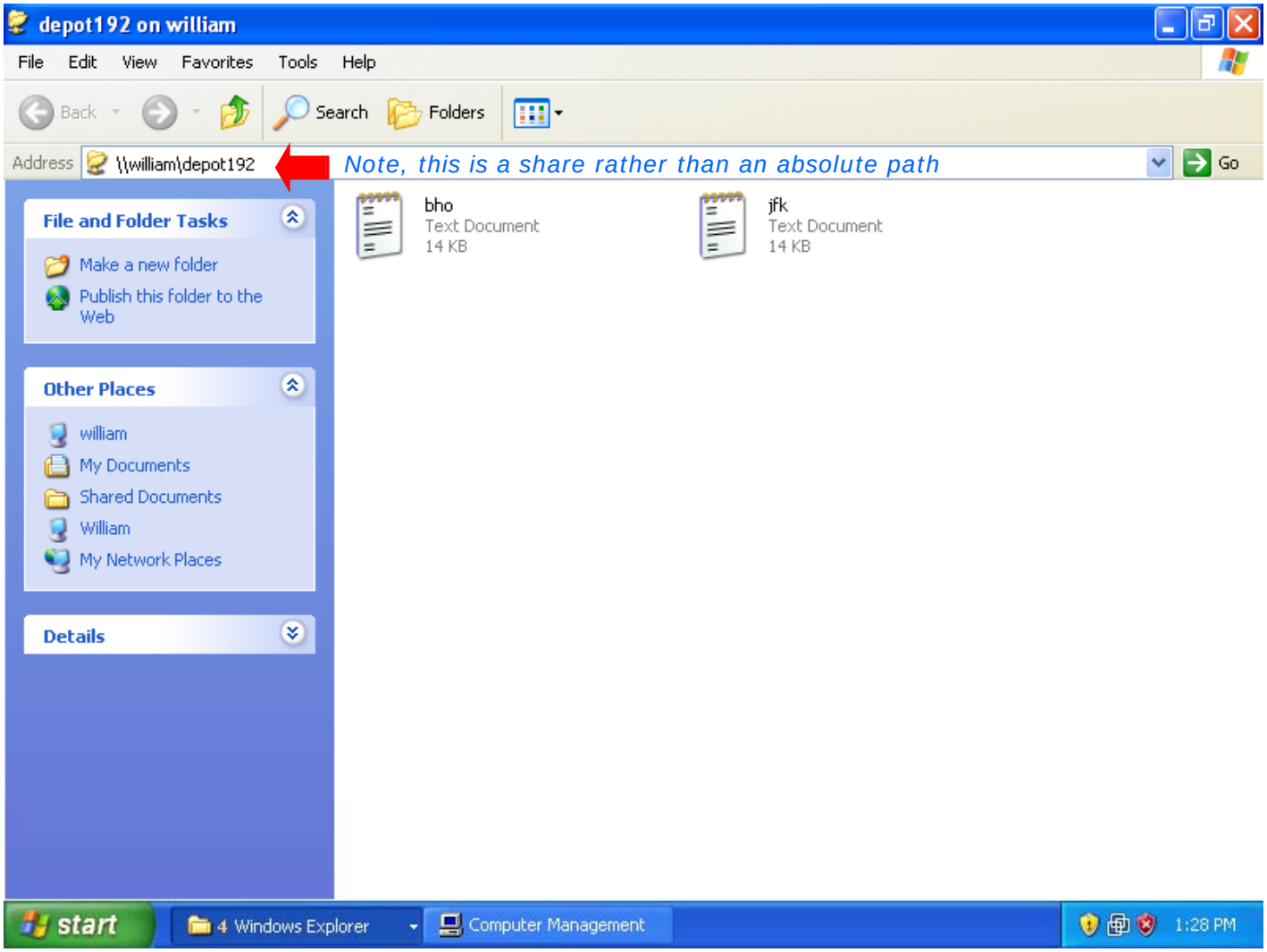
# Windows Shares – *accessing shares*

*As cis192, Start > Run... > \\hostname\sharename*



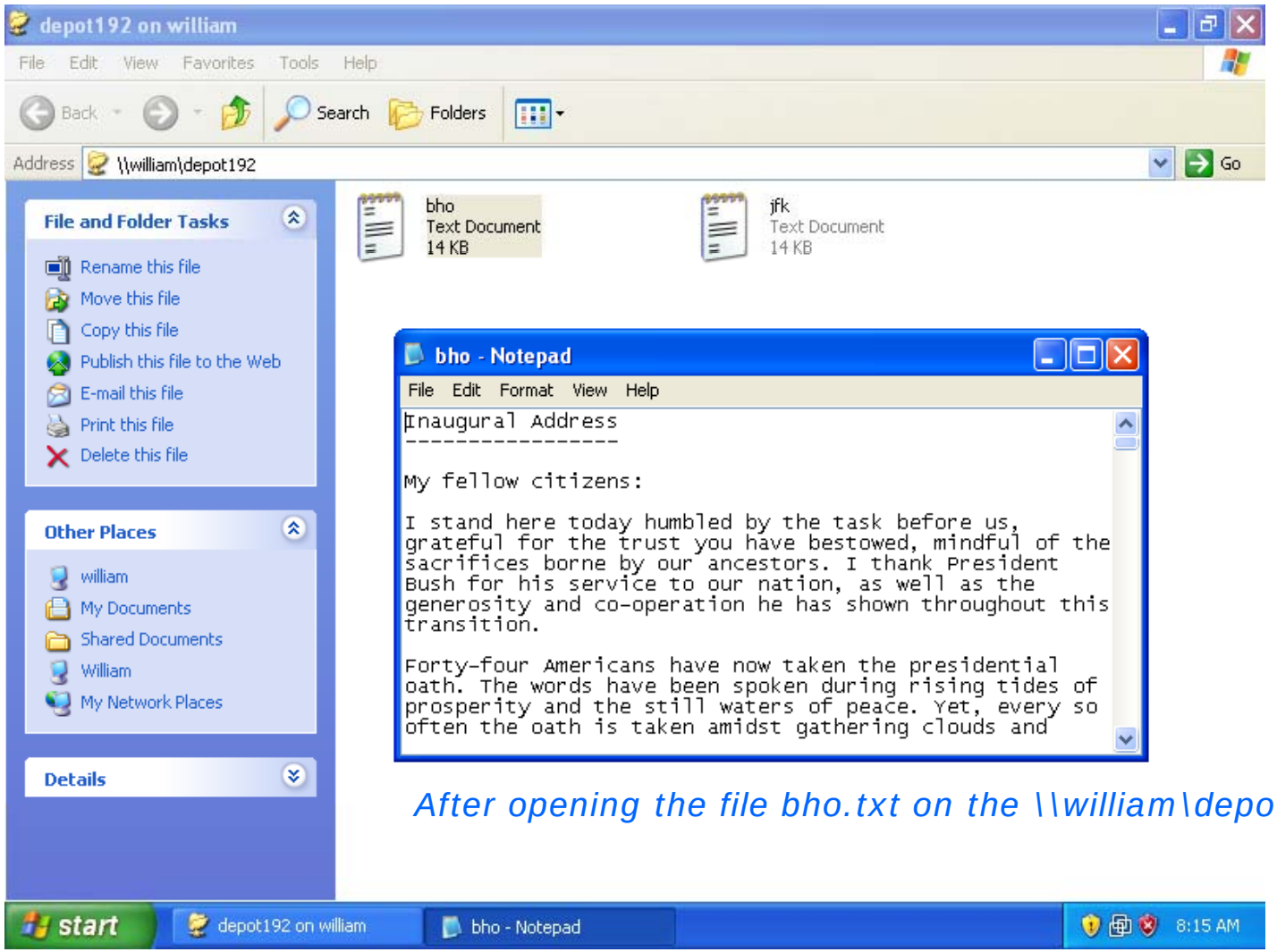
# Windows Shares – *accessing shares*

*As cis192, view the files on the depot192 share*

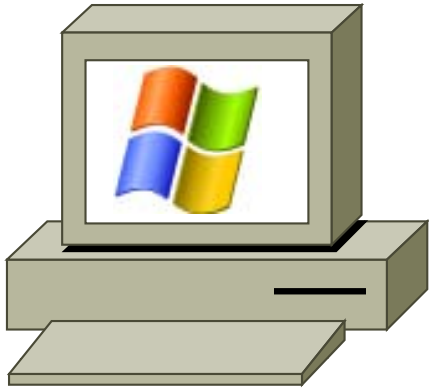


# Windows Shares – *accessing shares*

*As cis192, open the files on the depot192 share*



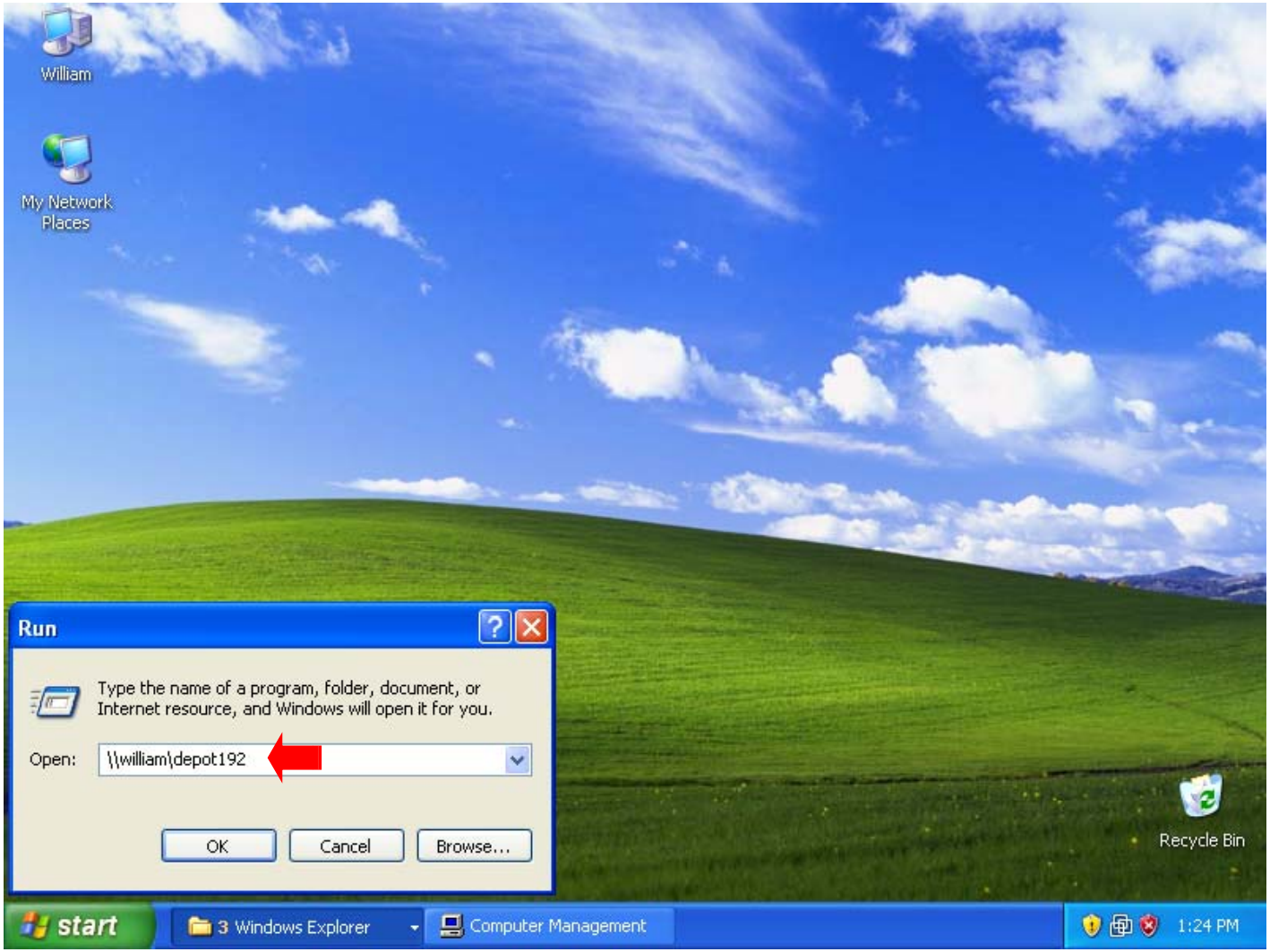

*After opening the file bho.txt on the \\william\depot192 share*



# Failed Share Access

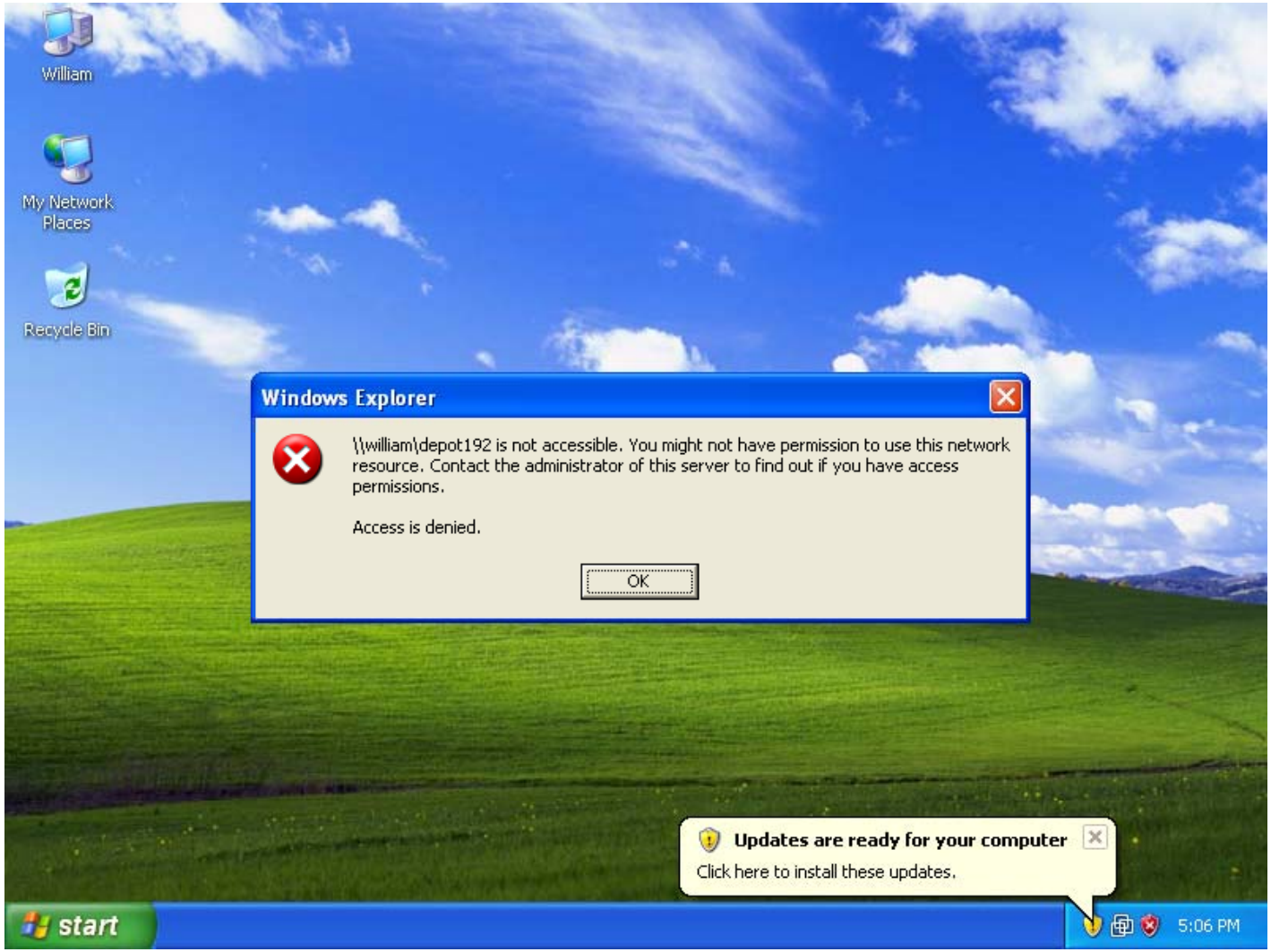
# Windows Shares – *accessing shares*

*Switch to the cis191 user and try again*



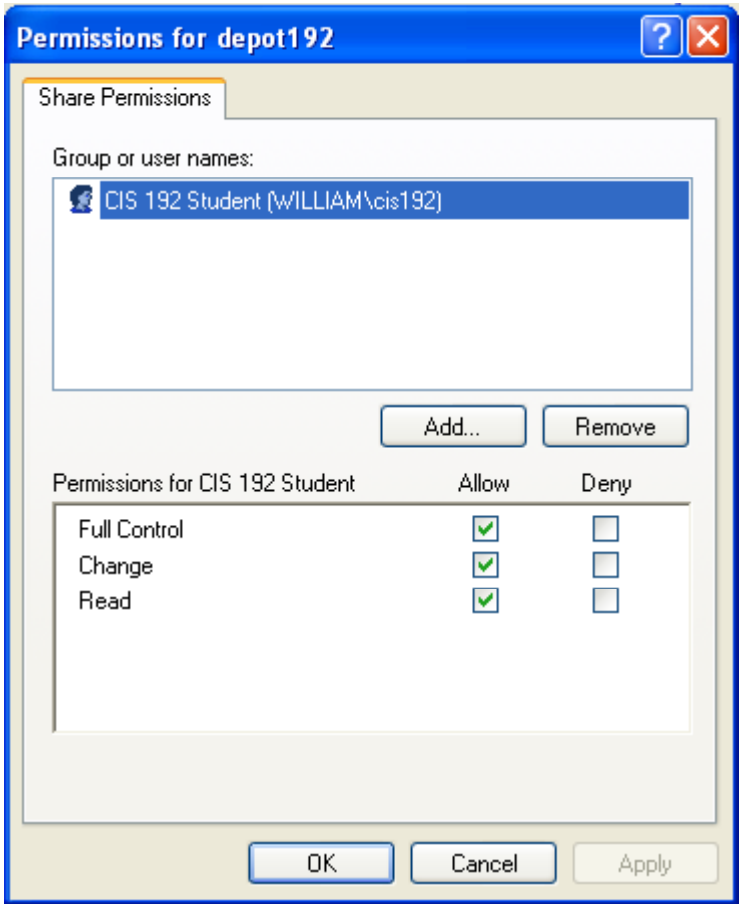
# Windows Shares – *viewing share configurations*

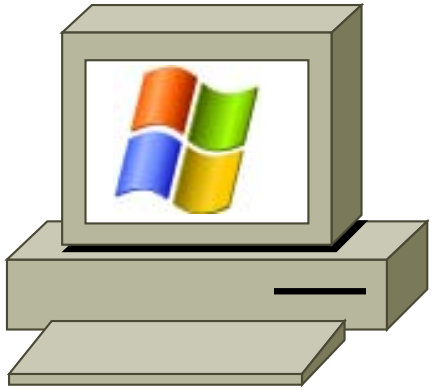
*Note cis191 user cannot access the \\william\depot192 share*



# Windows Shares – *viewing share configurations*

*Note cis191 user has no permissions to access the \\william\depot192 share*

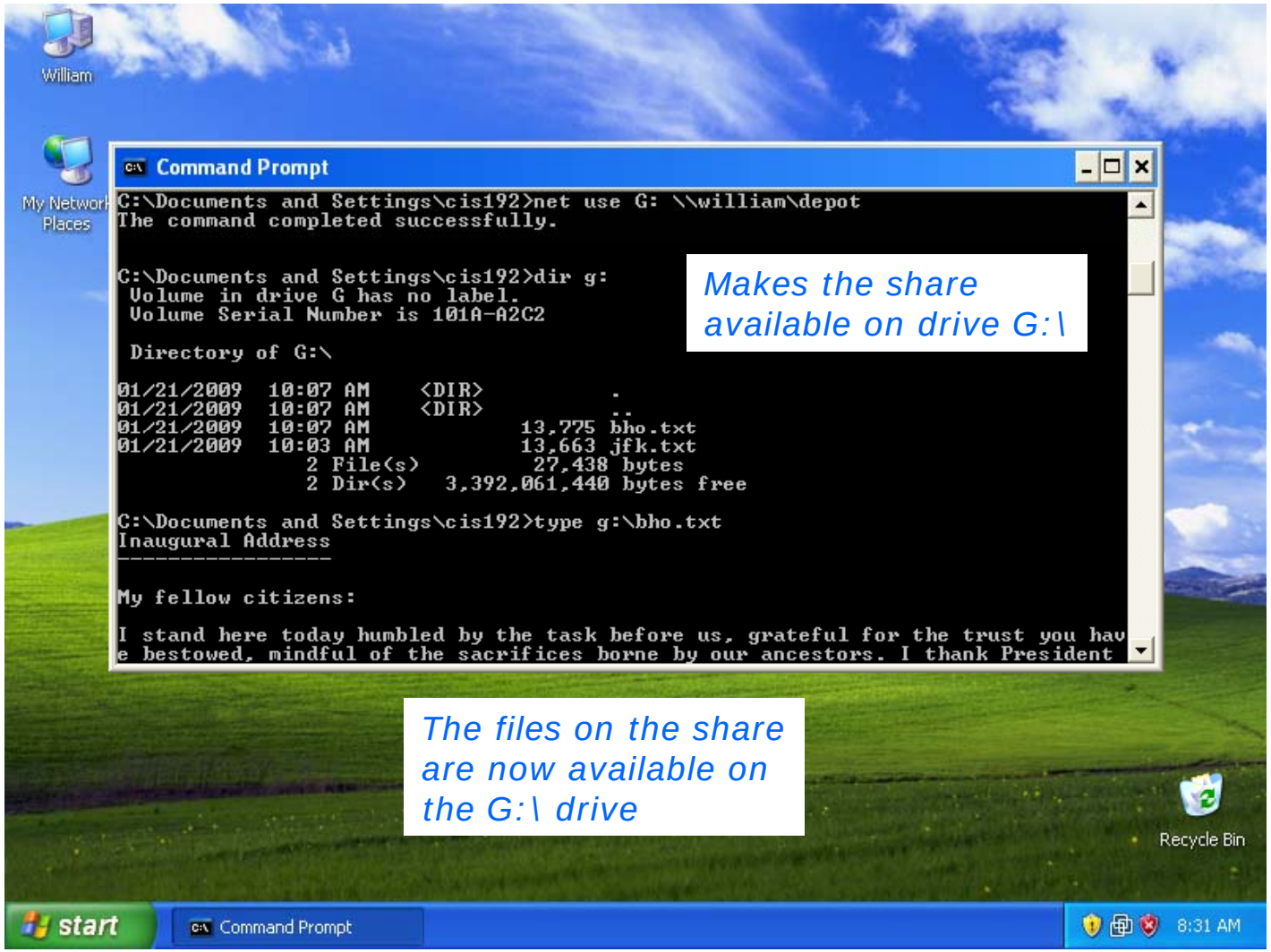




# Command Line Share Access

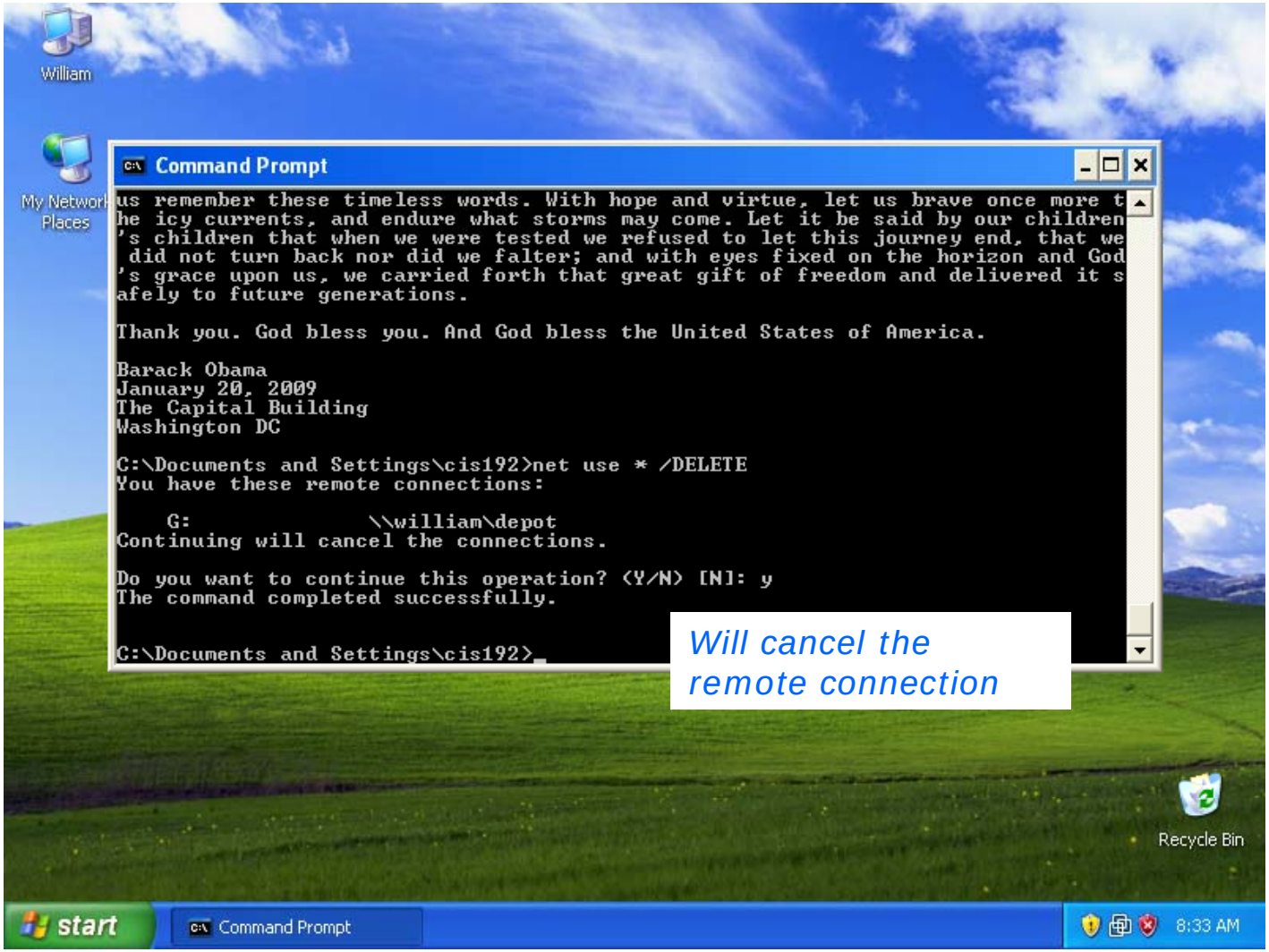
# Windows Shares – *accessing shares*

***net use drive: \\computername\share** command*



# Windows Shares – *accessing shares*

## *The **net use * /DELETE** command*




- Access both William shares from William:
  - GUI method
    - Start > Run... > \\william\depot
    - Open bho.txt file in notepad
  - DOS command method
    - **net use G: \\william\depot192**
    - View jfk.txt with **type jfk.txt**

- Run MMC/Computer Management
  - View Shares
  - View Sessions
  - View Open Files


# Browsing from Linux

# Browsing shares from Linux

```
[root@elrond ~]# smbtree
Password:
WORKGROUP
        \\WILLIAM
                \\WILLIAM\C$                    Default share
                \\WILLIAM\ADMIN$                Remote Admin
                \\WILLIAM\depot192
                \\WILLIAM\depot
                \\WILLIAM\IPC$                  Remote IPC
        \\ELROND                        Cool Samba Server
                \\ELROND\IPC$                   IPC Service (Cool Samba Server)
                \\ELROND\depot192               CIS 192 files on Elrond
                \\ELROND\depot                  Public files on Elrond
```

*This is equivalent to doing viewing a network neighborhood on Windows*

# Browsing shares from Linux

*Note: Password not needed to browse shares*

```
[root@elrond ~]# smbclient -L william
Password: <no password used>
Domain=[WILLIAM] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        depot           Disk
        depot192        Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
Domain=[WILLIAM] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

*The depot and depot192 shares are visible*

*Note, if you are browsing a Windows computer, you will see the hidden administrative shares IPC$, ADMIN$, and C$. Using the $ at the end of the share name makes it hidden.*

# Browsing shares from Linux

```
[root@elrond ~]# smbclient -L elrond
Password: <no password used>
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.28-1.el5_2.1]

        Sharename       Type      Comment
        ---------       ----      -------
        depot           Disk      Public files on Elrond
        depot192        Disk      CIS 192 files on Elrond
        IPC$            IPC       IPC Service (Cool Samba Server)
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.28-1.el5_2.1]

        Server               Comment
        ---------            -------
        ELROND               Cool Samba Server
        LEGOLAS              Cooler Samba Server
        WILLIAM

        Workgroup            Master
        ---------            -------
        WORKGROUP            WILLIAM
```

*Password not needed to browse shares*

*The depot and depot192 shares are visible*

*Note: Elrond must be first configured as a Samba server before you can do this!*


- Try using the **smbtree** command
- Browse the shares on William:
  **smbclient –L william**


# Accessing shares from Linux

# Accessing shares from Linux

```
[root@elrond ~]# mount -o user=cis191 //william/depot /mnt
Password:
[root@elrond ~]# ls /mnt
bho.txt  jfk.txt
[root@elrond ~]# head -5 /mnt/bho.txt

==> bho.txt <==
Inaugural Address
-----------------

My fellow citizens:


[root@elrond ~]# umount /mnt
```

# Accessing shares from Linux

```
[root@elrond ~]# mount -o user=cis191 //william/depot192 /mnt
Password:
mount error 20 = Not a directory
Refer to the mount.cifs(8) manual page (e.g.man mount.cifs)
```

*Error because cis191 does not have access to the depot192 share on William*

```
[root@elrond ~]# mount -o user=cis191 //william/badname /mnt
Password:
retrying with upper case share name
mount error 6 = No such device or address
Refer to the mount.cifs(8) manual page (e.g.man mount.cifs)
```

*Error because badname share on William does not exist*

# Accessing shares from Linux

*An FTP-like access method*

```
[root@elrond ~]# smbclient -U cis192 //william/depot192
Password:
Domain=[WILLIAM] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> help
?              altname        archive        blocksize      cancel
case_sensitive cd             chmod          chown          close
del            dir            du             exit           get
getfacl        hardlink       help           history        lcd
link           lock           lowercase      ls             mask
md             mget           mkdir          more           mput
newer          open           posix          posix_open     posix_mkdir
posix_rmdir    posix_unlink   print          prompt         put
pwd            q              queue          quit           rd
recurse        reget          rename         reput          rm
rmdir          showacls       setmode        stat           symlink
tar            tarmode        translate      unlock         volume
vuid           wdel           logon          listconnect    showconnect
!
smb: \> ls
  .                                   D        0  Tue Jan 20 12:55:11 2009
  ..                                  D        0  Tue Jan 20 12:55:11 2009
  bho.txt                             A    13775  Wed Jan 21 09:08:10 2009
  jfk.txt                             A    13663  Wed Jan 21 09:03:51 2009

                49073 blocks of size 131072. 25960 blocks available
smb: \> get jfk.txt
getting file \jfk.txt of size 13663 as jfk.txt (139.0 kb/s) (average 139.0 kb/s)
smb: \> exit
```


- Mount the depot share on William:
  **mount -o user=cis192 //william/depot /mnt**
- View the files on /mnt
  **head /mnt/***
- Unmount with **umount /mnt**
- Try the alternative FTP-like method
  **smbclient -U cis192 //william/depot192**
  **help**
  **ls**
  **get jfk.txt**
  **exit**


# Installing Samba Server

# Service Applications

**Steps to installing services**

1. Install software package using **yum**, **rpm** or build from source code
2. Customize service's configuration file
3. Modify the firewall to allow access to the service
4. Customize SELinux context settings to allow use
5. Start the service
6. Configure service to automatically start when system boots
7. Monitor and verify service is running
8. Troubleshoot as necessary
9. Monitor log files as appropriate
10. Configure additional security

# Installing Samba Server

**Step 1** *Install software*

```
[root@legolas ~]# rpm -qa | grep samba
samba-common-3.0.28-0.el5.8
samba-client-3.0.28-0.el5.8
[root@legolas ~]#
```

*At this point only the samba client and common modules are installed which allows access to other Samba servers.*

*The server package “samba” has not yet been installed.*

# Installing Samba Server

**Step 1** *Install software with yum*

```
[root@elrond ~]# yum install samba
base                      100% |=========================| 1.1 kB    00:00
updates                   100% |=========================|  951 B    00:00
addons                    100% |=========================|  951 B    00:00
extras                    100% |=========================| 1.1 kB    00:00
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package samba.i386 0:3.0.28-1.el5_2.1 set to be updated
--> Processing Dependency: samba-common = 3.0.28-1.el5_2.1 for package: samba
--> Running transaction check
--> Processing Dependency: samba-common = 3.0.28-0.el5.8 for package: samba-client
---> Package samba-common.i386 0:3.0.28-1.el5_2.1 set to be updated
--> Running transaction check
---> Package samba-client.i386 0:3.0.28-1.el5_2.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved
```

# Installing Samba Server

```
Dependencies Resolved

================================================================================
 Package                 Arch       Version           Repository        Size
================================================================================
Installing:
 samba                   i386       3.0.28-1.el5_2.1  updates            16 M
Updating:
 samba-common            i386       3.0.28-1.el5_2.1  updates           8.7 M
Updating for dependencies:
 samba-client            i386       3.0.28-1.el5_2.1  updates           4.9 M

Transaction Summary
================================================================================
Install      1 Package(s)
Update       2 Package(s)
Remove       0 Package(s)

Total download size: 30 M
Is this ok [y/N]:
```

# Installing Samba Server

```
Is this ok [y/N]: y
Downloading Packages:
(1/3): samba-client-3.0.2 100% |=========================| 4.9 MB    01:00
(2/3): samba-common-3.0.2 100% |=========================| 8.7 MB    01:44
(3/3): samba-3.0.28-1.el5 100% |=========================|  16 MB    02:53
warning: rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID e8562897
Importing GPG key 0xE8562897 "CentOS-5 Key (CentOS 5 Official Signing Key)
<centos-5-key@centos.org>" from http://mirror.centos.org/centos/RPM-GPG-KEY-
CentOS-5
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating  : samba-common                  ########################### [1/5]
  Installing: samba                         ########################### [2/5]
  Updating  : samba-client                  ########################### [3/5]
  Cleanup   : samba-common                  ########################### [4/5]
  Cleanup   : samba-client                  ########################### [5/5]

Installed: samba.i386 0:3.0.28-1.el5_2.1
Updated: samba-common.i386 0:3.0.28-1.el5_2.1
Dependency Updated: samba-client.i386 0:3.0.28-1.el5_2.1
Complete!
[root@elrond ~]#
```

# Installing Samba Server

**Step 1** *Or install software using rpm command (Centos 5.4)*

```
[root@elrond packages]# rpm -qa | grep samba
samba-common-3.0.33-3.14.el5
samba-client-3.0.33-3.14.el5
```

```
[root@elrond packages]# ls samba* perl*
perl-Convert-ASN1-0.20-1.1.noarch.rpm
samba-3.0.33-3.15.el5_4.1.i386.rpm
samba-client-3.0.33-3.15.el5_4.1.i386.rpm
samba-common-3.0.33-3.15.el5_4.1.i386.rpm
```

*RPMs needed to install Samba*

```
[root@elrond packages]# rpm -Uhv samba* perl*
Preparing...                ########################################### [100%]
   1:samba-common           ########################################### [ 25%]
   2:samba-client           ########################################### [ 50%]
   3:perl-Convert-ASN1      ########################################### [ 75%]
   4:samba                  ########################################### [100%]
```

*Updating Samba and installing the server package. Note the perl module is a dependency.*

# Installing Samba Server

```
[root@elrond shares]# rpm -qa | grep samba
samba-3.0.28-1.el5_2.1
samba-common-3.0.28-1.el5_2.1
samba-client-3.0.28-1.el5_2.1
```

*Server modules have been installed*

Note, you can use **yum** command to only download rpms (and not install them) with the downloadonly option. Useful for doing installations on systems with no Internet access.

**yum install yum-downloadonly**
**yum install samba --downloadonly**

*The downloaded rpms will be found in /var/cache/yum/*/packages*


- Check which samba packages have been installed on Elrond with **rpm –qa | grep samba**
- Install the samba server package on Elrond with **yum install samba** or appropriate **rpm** command
- Check again which samba packages have been installed on Elrond with **rpm –qa | grep samba**
- Use **rpm –qi** on any of the Samba packages to see what they do


# Make Shares


Make a sample file to share:

```
echo "We can do anything we want if we stick to it
long enough." - Helen Keller > /tmp/hk.txt
```

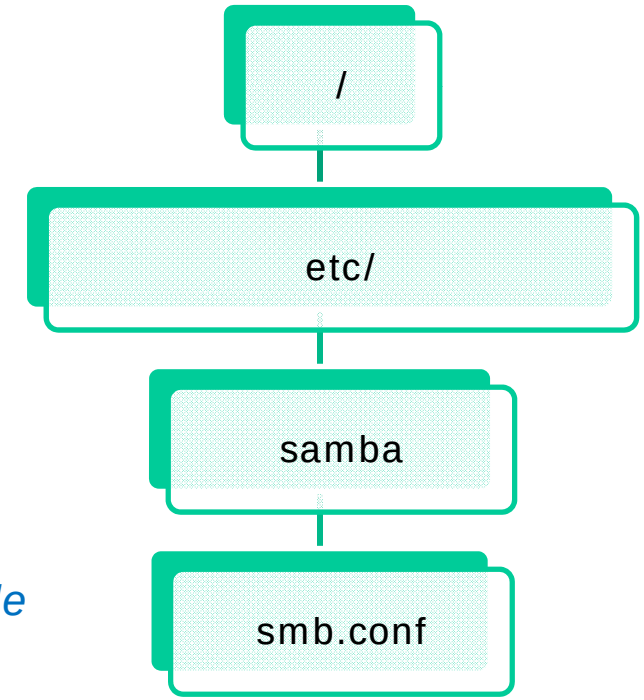
Make two directories to be shared in /var/shares:

```
cd /var
mkdir -p shares/depot  shares/depot192
cd shares
cp /tmp/hk.txt depot/
cp /tmp/hk.txt depot192/
chmod 755 *
chown -R cis192:users *
```

# smb.conf

# /etc/samba/smb.conf

**Step 2** *Customize the configuration files*




*main configuration file for Samba daemon*

# /etc/samba/smb.conf

**Step 2** *Customize the services configuration file*

## Changes we will make to smb.conf

- `workgroup = xxxxxxxx` — *Workgroup membership*
- `server string = xxxxxxxxx` — *Server description*
- `[xxxxxxxx]` — *Share specification*

## Finding smb.conf

```
[root@elrond var]# smbd -b | grep PRIVATE_DIR
   PRIVATE_DIR: /etc/samba

[root@elrond var]# ls -l /etc/samba/
total 52
-rw-r--r-- 1 root root    20 Jun 21  2008 lmhosts
-rw------- 1 root root  4096 Jan 21 11:04 passdb.tdb
-rw------- 1 root root  8192 Jan 21 11:04 secrets.tdb
-rw-r--r-- 1 root root 10006 Jan 21 14:38 smb.conf
-rw-r--r-- 1 root root    97 Jun 21  2008 smbusers
```

# /etc/samba/smb.conf

**Some share options**

- `path =` *Absolute path to share*
- `guest ok =` *Yes or no, for guest user access*
- `read only =` *Yes or no (default is yes)*
- `writeable =` *Yes or no (alternate way to specify)*
- `valid users =` *Limits users that can access this share*
- `browseable =` *Yes or no to appear in network neighborhood*
- `comment =` *Shown to users browsing share*
- `hosts allow =` *List of hostnames (e.g. localhost 192.168.2. 10.10.10.)*
- `hosts deny =` *List of hostnames (use ALL or 0.0.0.0/0 for all hosts)*

*Of course, there are many more options than this!*
*(use **man smb.conf** or Google)*

# /etc/samba/smb.conf

```
[root@legolas ~]# cat /etc/samba/smb.conf
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this example
#
# For a step to step guide on installing, configuring and using samba,
# read the Samba-HOWTO-Collection. This may be obtained from:
#  http://www.samba.org/samba/docs/Samba-HOWTO-Collection.pdf
#
# Many working examples of smb.conf files can be found in the
# Samba-Guide which is generated daily and can be downloaded from:
#  http://www.samba.org/samba/docs/Samba-Guide.pdf
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentry and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors.
#
```

*Good advice!*

# /etc/samba/smb.conf

```
#---------------
# SELINUX NOTES:
#
# If you want to use the useradd/groupadd family of binaries please run:
# setsebool -P samba_domain_controller on
#
# If you want to share home directories via samba please run:
# setsebool -P samba_enable_home_dirs on
#
# If you create a new directory you want to share you should mark it as
# "samba-share_t" so that selinux will let you write into it.
# Make sure not to do that on system directories as they may already have
# been marked with othe SELinux labels.
#
# Use ls -ldZ /path to see which context a directory has
#
# Set labels only on directories you created!
# To set a label use the following: chcon -t samba_share_t /path
#
# If you need to share a system created directory you can use one of the
# following (read-only/read-write):
# setsebool -P samba_export_all_ro on
# or
# setsebool -P samba_export_all_rw on
#
# If you want to run scripts (preexec/root prexec/print command/...) please
# put them into the /var/lib/samba/scripts directory so that smbd will be
# allowed to run them.
# Make sure you COPY them and not MOVE them so that the right SELinux context
# is applied, to check all is ok use restorecon -R -v /var/lib/samba/scripts
#
```

*Lab 8 will not work unless this is done*

*Lab 8 will not work unless this is done*

# /etc/samba/smb.conf

```
#======================= Global Settings =====================================

[global]

# ----------------------- Network Related Options -------------------------
#
# workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH
#
# server string is the equivalent of the NT Description field
#
# netbios name can be used to specify a server name not tied to the hostname
#
# Interfaces lets you configure Samba to use multiple interfaces
# If you have multiple network interfaces then you can list the ones
# you want to listen on (never omit localhost)
#
# Hosts Allow/Hosts Deny lets you restrict who can connect, and you can
# specifiy it as a per share option as well
#
        workgroup = MYGROUP
        server string = Samba Server Version %v

;       netbios name = MYSERVER

;       interfaces = lo eth0 192.168.12.2/24 192.168.13.2/24
;       hosts allow = 127. 192.168.12. 192.168.13.
```

***Modify to:***

*workgroup = WORKGROUP*

*server string = Cool Samba Server*

# /etc/samba/smb.conf

```
# ----------------------------- Logging Options -----------------------------
#
# Log File let you specify where to put logs and how to split them up.
#
# Max Log Size let you specify the max size log files should reach

        # logs split per machine
;       log file = /var/log/samba/%m.log
        # max 50KB per log file, then rotate
;       max log size = 50

# ----------------------- Standalone Server Options ------------------------
#
# Security can be set to user, share(deprecated) or server(deprecated)
#
# Backend to store user information in. New installations should
# use either tdbsam or ldapsam. smbpasswd is available for backwards
# compatibility. tdbsam requires no further configuration.

security = user
passdb backend = tdbsam
```

*Lab 8 will use a stand-alone server model*

*This is the default*

*Good choice for local servers and < 250 users. Use ldapsam for larger organizations*

*With tdbsam, the Samba account information will be stored in /etc/samba/passdb.tdb. Note: This file requires that account information is available from the /etc/passwd file.*

# /etc/samba/smb.conf

```
# ----------------------- Domain Members Options ------------------------
#
# Security must be set to domain or ads
#
# Use the realm option only with security = ads
# Specifies the Active Directory realm the host is part of
#
# Backend to store user information in. New installations should
# use either tdbsam or ldapsam. smbpasswd is available for backwards
# compatibility. tdbsam requires no further configuration.
#
# Use password server option only with security = server or if you can't
# use the DNS to locate Domain Controllers
# The argument list may include:
#   password server = My_PDC_Name [My_BDC_Name] [My_Next_BDC_Name]
# or to auto-locate the domain controller/s
#   password server = *


;       security = domain
;       passdb backend = tdbsam
;       realm = MY_REALM

;       password server = <NT-Server-Name>
```

*The Samba server can join a domain. Not using for Lab 8*

```
# ----------------------- Domain Controller Options ------------------------
#
# Security must be set to user for domain controllers
#
# Backend to store user information in. New installations should
# use either tdbsam or ldapsam. smbpasswd is available for backwards
# compatibility. tdbsam requires no further configuration.
#
# Domain Master specifies Samba to be the Domain Master Browser. This
# allows Samba to collate browse lists between subnets. Don't use this
# if you already have a Windows NT domain controller doing this job
#
# Domain Logons let Samba be a domain logon server for Windows workstations.
#
# Logon Scrpit let yuou specify a script to be run at login time on the client
# You need to provide it in a share called NETLOGON
#
# Logon Path let you specify where user profiles are stored (UNC path)
#
# Various scripts can be used on a domain controller or stand-alone
# machine to add or delete corresponding unix accounts
#
;       security = user
;       passdb backend = tdbsam

;       domain master = yes
;       domain logons = yes

        # the login script name depends on the machine name
;       logon script = %m.bat
        # the login script name depends on the unix user used
;       logon script = %u.bat
;       logon path = \\%L\Profiles\%u
        # disables profiles support by specifing an empty path
;       logon path =

;       add user script = /usr/sbin/useradd "%u" -n -g users
;       add group script = /usr/sbin/groupadd "%g"
;       add machine script = /usr/sbin/useradd -n -c "Workstation (%u)" -M -d /nohome -s /bin/false "%u"
;       delete user script = /usr/sbin/userdel "%u"
;       delete user from group script = /usr/sbin/userdel "%u" "%g"
;       delete group script = /usr/sbin/groupdel "%g"
```

*Samba can act as a domain controller. Not using this for Lab 8*

# /etc/samba/smb.conf

```
# ----------------------- Browser Control Options ----------------------------
#
# set local master to no if you don't want Samba to become a master
# browser on your network. Otherwise the normal election rules apply
#
# OS Level determines the precedence of this server in master browser
# elections. The default value should be reasonable
#
# Preferred Master causes Samba to force a local browser election on startup
# and gives it a slightly higher chance of winning the election
;       local master = no
;       os level = 33
;       preferred master = yes
```

*Browser control is about letting Windows and Samba servers appear in Network Neighborhood views. Only one master can be allowed on a domain or workgroup.*

# /etc/samba/smb.conf

```
#----------------------------- Name Resolution -------------------------------
# Windows Internet Name Serving Support Section:
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
#
# - WINS Support: Tells the NMBD component of Samba to enable it's WINS Server
#
# - WINS Server: Tells the NMBD components of Samba to be a WINS Client
#
# - WINS Proxy: Tells Samba to answer name resolution queries on
#   behalf of a non WINS capable client, for this to work there must be
#   at least one        WINS Server on the network. The default is NO.
#
# DNS Proxy - tells Samba whether or not to try to resolve NetBIOS names
# via DNS nslookups.

;       wins support = yes
;       wins server = w.x.y.z
;       wins proxy = yes

;       dns proxy = yes
```

*Not using for Lab 8.*

*We will just use /etc/hosts files.*

# /etc/samba/smb.conf

```
# ----------------------------- Printing Options -----------------------------
#
# Load Printers let you load automatically the list of printers rather
# than setting them up individually
#
# Cups Options let you pass the cups libs custom options, setting it to raw
# for example will let you use drivers on your Windows clients
#
# Printcap Name let you specify an alternative printcap file
#
# You can choose a non default printing system using the Printing option

        load printers = yes
        cups options = raw

;       printcap name = /etc/printcap
        #obtain list of printers automatically on SystemV
;       printcap name = lpstat
;       printing = cups
```

*Leave as is for Lab 8*

# /etc/samba/smb.conf

```
# ----------------------------- Filesystem Options -----------------------------
#
# The following options can be uncommented if the filesystem supports
# Extended Attributes and they are enabled (usually by the mount option
# user_xattr). Thess options will let the admin store the DOS attributes
# in an EA and make samba not mess with the permission bits.
#
# Note: these options can also be set just per share, setting them in global
# makes them the default for all shares

;       map archive = no
;       map hidden = no
;       map read only = no
;       map system = no
;       store dos attributes = yes
```

*Leave these options commented out for Lab 8*

# /etc/samba/smb.conf

```
#============================ Share Definitions ==============================

[homes]
        comment = Home Directories
        browseable = no
        writable = yes
;       valid users = %S
;       valid users = MYDOMAIN\%S

[printers]
        comment = All Printers
        path = /var/spool/samba
        browseable = no
        guest ok = no
        writable = no
        printable = yes

# Un-comment the following and create the netlogon directory for Domain Logons
;       [netlogon]
;       comment = Network Logon Service
;       path = /var/lib/samba/netlogon
;       guest ok = yes
;       writable = no
;       share modes = no
```

*The default will allow access to home directories*

# /etc/samba/smb.conf

```
#============================ Share Definitions ==============================


# Un-comment the following to provide a specific roving profile share
# the default is to use the user's home directory
;       [Profiles]
;       path = /var/lib/samba/profiles
;       browseable = no
;       guest ok = yes


# A publicly accessible directory, but read only, except for people in
# the "staff" group
;       [public]
;       comment = Public Stuff
;       path = /home/samba
;       public = yes
;       writable = yes
;       printable = no
;       write list = +staff
[root@legolas ~]#
```

*Leave these example shares commented out for Lab 8*

# /etc/samba/smb.conf

*Add these shares to the end of smb.conf*

```
[depot]
comment = Public files on Elrond
path = /var/shares/depot
read only = yes
guest ok = yes

[depot192]
comment = CIS 192 files on Elrond
path = /var/shares/depot192
valid users = cis192
writeable = yes
```

# testparm

```
[root@legolas shares]# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[depot]"
Processing section "[depot192]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

[global]
        server string = Cool Samba Server
        passdb backend = tdbsam
        cups options = raw

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[depot]
        comment = Public files on Elrond
        path = /var/shares/depot
        guest ok = Yes

[depot192]
        comment = CIS 192 files on Elrond
        path = /var/shares/depot192
        valid users = cis192
        read only = No
```

## testparm

*After making any changes to smb.conf, use **testparm** to validate*


- Validate smb.conf with **testparm** command
- Fix any errors found

# Create users and passwords

# Adding Users

*Add a normal user account to the system*

```
[root@elrond var]# useradd -c "CIS 191" -g users cis191
[root@elrond var]# passwd cis191
Changing password for user cis191.
New UNIX password:
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

# Adding Users

*Add Samba passwords*

```
[root@elrond var]# smbpasswd -a cis191
New SMB password:
Retype new SMB password:
Added user cis191.

[root@elrond var]# smbpasswd -a cis192
New SMB password:
Retype new SMB password:
Added user cis192.
```


- Verify cis192 user exists:
  **cat /etc/passwd | grep cis191**
- Create a cis191 user:
  **useradd –c "CIS 191" –g users cis191**
- Add a password for cis191:
  **passwd cis191**
- Configure Samba user passwords:
  **smbpasswd –a cis191**
  **smbpasswd –a cis192**

# Firewall

# Samba and the Firewall

**Step 3** *Modify the firewall*

**Firewall ports used for file and printer sharing**

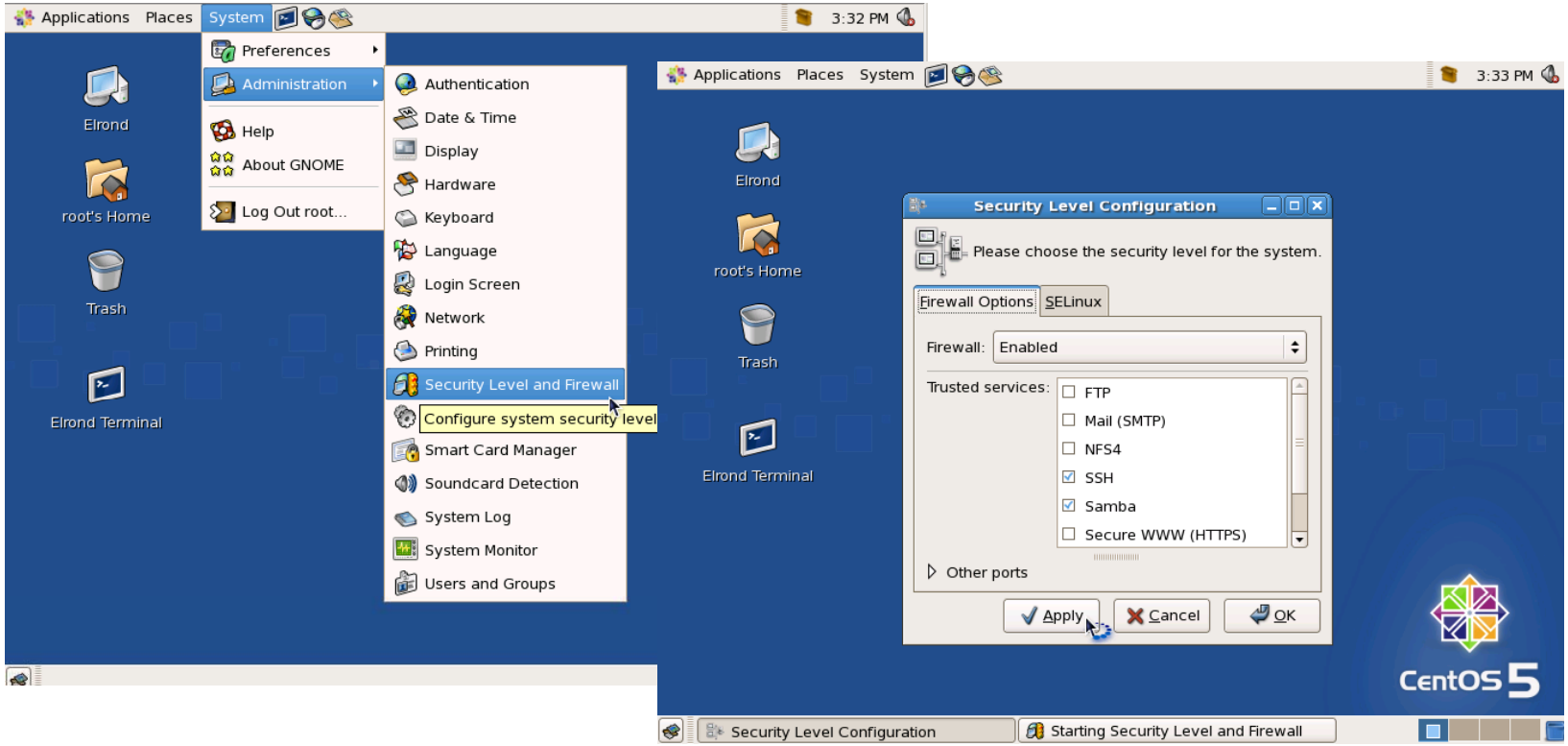
| | |
|---|---|
| UDP 137 | *NetBIOS Name Service* |
| UDP 138 | *NetBIOS Datagram Service* |
| TCP 139 | *NetBIOS Session Service* |
| TCP 445 | *Microsoft Directory Service* |
| | *(allows SMB to run over IP)* |

# Samba and the Firewall

## *With command line*

```
iptables -I RH-Firewall-1-INPUT 9 -p udp -m state --state NEW -m udp --dport 137 -j ACCEPT
iptables -I RH-Firewall-1-INPUT 9 -p udp -m state --state NEW -m udp --dport 138 -j ACCEPT
iptables -I RH-Firewall-1-INPUT 9 -p tcp -m state --state NEW -m tcp --dport 139 -j ACCEPT
iptables -I RH-Firewall-1-INPUT 9 -p tcp -m state --state NEW -m tcp --dport 445 -j ACCEPT
```

## *With GUI*



# Samba and the Firewall

```
[root@elrond ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:445
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:139
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           state NEW udp dpt:138
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           state NEW udp dpt:137
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
```

*udp/137*
*udp/138*
*tcp/139*
*tcp/445*
*are open now*

**Elrond**


- View the default firewall:
  **iptables -nL**

- Insert rules to open the Samba ports:

```
iptables -I RH-Firewall-1-INPUT 9 -p udp -m state --state NEW -m udp --dport 137 -j ACCEPT
iptables -I RH-Firewall-1-INPUT 9 -p udp -m state --state NEW -m udp --dport 138 -j ACCEPT
iptables -I RH-Firewall-1-INPUT 9 -p tcp -m state --state NEW -m tcp --dport 139 -j ACCEPT
iptables -I RH-Firewall-1-INPUT 9 -p tcp -m state --state NEW -m tcp --dport 445 -j ACCEPT
```

- View the default firewall:
  **iptables –nL**

- Save the firewall:
  **iptables-save > /etc/sysconfig/iptables**

# SELinux

# SELinux

**Step 4** *Configure SELinux*

## Overview

SELinux is like an internal firewall where you can define what subjects (users, programs) can access which objects (files, devices)

- Originally created by the NSA (National Security Agency)
- Based on the MAC (Mandatory Access Control) concept where administrators control all interactions between programs.
- Programs and users start with no rights. Any rights must be granted by the administrator as part of the security policy for the system.
- Standard UNIX permissions are checked first then SELinux rules are applied if necessary.

# SELinux

## Security Contexts

Security context have three components: a **user identity**, a **role**, and a **type** (also known as a domain).

```
[root@celebrian var]# ls -ldZ shares/
drwxr-xr-x  root root root:object_r:var_t                 shares/

[root@elrond var]# ls -lZ /usr/sbin/[sn]mbd
-rwxr-xr-x  root root system_u:object_r:nmbd_exec_t       /usr/sbin/nmbd
-rwxr-xr-x  root root system_u:object_r:smbd_exec_t       /usr/sbin/smbd

[root@elrond var]# id root
uid=0(root) gid=0(root)
  groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
  context=root:system_r:unconfined_t:SystemLow-SystemHigh
```

*A user identity is the SELinux user account*

*Types (use "_t" suffix) are the primary method used by SELinux to make authorization decisions.*

*A role (uses "_r" suffix) defines a set of permissions granted to a SELinux user.*

# /etc/samba/smb.conf

```
#--------------
# SELINUX NOTES:
#
# If you want to use the useradd/groupadd family of binaries please run:
# setsebool -P samba_domain_controller on
#
# If you want to share home directories via samba please run:
# setsebool -P samba_enable_home_dirs on
#
# If you create a new directory you want to share you should mark it as
# "samba-share_t" so that selinux will let you write into it.
# Make sure not to do that on system directories as they may already have
# been marked with othe SELinux labels.
#
# Use ls -ldZ /path to see which context a directory has
#
# Set labels only on directories you created!
# To set a label use the following: chcon -t samba_share_t /path
#
# If you need to share a system created directory you can use one of the
# following (read-only/read-write):
# setsebool -P samba_export_all_ro on
# or
# setsebool -P samba_export_all_rw on
#
# If you want to run scripts (preexec/root prexec/print command/...) please
# put them into the /var/lib/samba/scripts directory so that smbd will be
# allowed to run them.
# Make sure you COPY them and not MOVE them so that the right SELinux context
# is applied, to check all is ok use restorecon -R -v /var/lib/samba/scripts
#
```

*Lab 8 will not work unless this is done*

*Lab 8 will not work unless this is done*

# Samba and SELinux

Set permissive mode

```
[root@legolas ~]# setenforce permissive
[root@legolas ~]# getenforce
Permissive
```

Set enforcing mode

```
[root@legolas ~]# setenforce enforcing
[root@legolas ~]# getenforce
Enforcing
```

Show SELinux status

```
[root@legolas ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 21
Policy from config file:        targeted
```

*In Lab 8 we will configure Samba to work in enforcing mode*

# Samba and SELinux

*This share on Elrond can be accessed …*

```
[root@elrond var]# ls -ld shares/
drwxr-xr-x 4 root root 4096 Jan 21 13:23 shares/

[root@elrond var]# ls -ld shares/depot
drwxr-xr-x 2 cis192 users 4096 Apr 27 02:30 shares/depot

[root@elrond var]# ls -ld shares/depot/jfk.txt
-rw-r--r-- 1 root root 13663 Apr 27 02:30 shares/depot/jfk.txt
```

*This share on Celebrian cannot be accessed …*

```
[root@celebrian var]# ls -ld shares/
drwxr-xr-x 4 root root 4096 Apr 25 08:59 shares/

[root@celebrian var]# ls -ld shares/depot
drwxr-xr-x 2 cis192 users 4096 Apr 25 09:03 shares/depot

[root@celebrian var]# ls -ld shares/depot/jfk.txt
-rw-r--r-- 1 root root 13675 Apr 25 09:03 shares/depot/jfk.txt
```

*Can you see why? … I can't!*

# Samba and SELinux

*This works ...*

```
[root@elrond var]# ls -ldZ shares/
drwxr-xr-x  root root root:object_r:var_t                 shares/

[root@elrond var]# ls -ldZ shares/depot
drwxr-xr-x  cis192 users root:object_r:samba_share_t      shares/depot

[root@elrond var]# ls -ldZ shares/depot/jfk.txt
-rw-r--r--  root root root:object_r:samba_share_t      shares/depot/jfk.txt
```

*This does NOT work ...*

```
[root@celebrian var]# ls -ldZ shares/
drwxr-xr-x  root root root:object_r:var_t                 shares/

[root@celebrian var]# ls -ldZ shares/depot
drwxr-xr-x  cis192 users root:object_r:var_t              shares/depot

[root@celebrian var]# ls -ldZ shares/depot/jfk.txt
-rw-r--r--  root root root:object_r:var_t              shares/depot/jfk.txt
```

*Can you see why?*

# Samba and SELinux

*This works ...*

*Use the Z option to show SELinux info*

```
[root@elrond var]# ls -ldZ shares/
drwxr-xr-x  root root root:object_r:var_t                shares/

[root@elrond var]# ls -ldZ shares/depot
drwxr-xr-x  cis192 users root:object_r:samba_share_t     shares/depot

[root@elrond var]# ls -ldZ shares/depot/jfk.txt
-rw-r--r--  root root root:object_r:samba_share_t        shares/depot/jfk.txt
```

*This does NOT work ...*

```
[root@celebrian var]# ls -ldZ shares/
drwxr-xr-x  root root root:object_r:var_t                shares/

[root@celebrian var]# ls -ldZ shares/depot
drwxr-xr-x  cis192 users root:object_r:var_t             shares/depot

[root@celebrian var]# ls -ldZ shares/depot/jfk.txt
-rw-r--r--  root root root:object_r:var_t                shares/depot/jfk.txt
```

*Can you see why? ... I can!*

# Samba and SELinux

```
[root@elrond ~]# chcon -Rv -t samba_share_t /var/shares/*
context of /var/shares/depot retained as root:object_r:samba_share_t
context of /var/shares/depot/hk.txt retained as root:object_r:samba_share_t
context of /var/shares/depot192 retained as root:object_r:samba_share_t
context of /var/shares/depot192/hk.txt retained as root:object_r:samba_share_t
[root@elrond ~]#
```

*Note the use of the recursive and verbose options to make the change on all files in the directory and show what was changed*

# Samba and SELinux

```
[root@elrond bin]# setsebool -P samba_enable_home_dirs=1
[root@elrond bin]# getsebool samba_enable_home_dirs
samba_enable_home_dirs --> on
[root@elrond bin]#
```

*This SELinux boolean must be enabled to allow the sharing of home directories*

# Samba and SELinux

Set permissive mode

```
[root@legolas ~]# setenforce permissive
[root@legolas ~]# getenforce
Permissive
```

Set enforcing mode

```
[root@legolas ~]# setenforce enforcing
[root@legolas ~]# getenforce
Enforcing
```

Show SELinux status

```
[root@legolas ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 21
Policy from config file:        targeted
```

*In Lab 8 we will configure Samba to work in enforcing mode*


- Leave SELinux in the default Enforcing mode
- View the security contexts on the shares:
  **ls –lRZ /var/shares**
- Change the security context for the share directories and files
  **chcon -vR -t samba_share_t /var/shares/***
  **setsebool -P samba_enable_home_dirs=1**
- View the revised security contexts on the shares:
  **ls –lRZ /var/shares**

# start services

# Samba

**Step 5** *Start the service*

```
[root@elrond var]# service smb start
Starting SMB services:                                     [  OK  ]
Starting NMB services:                                     [  OK  ]
```

**Step 6** *Start the service automatically during system startup*

```
[root@elrond var]# chkconfig smb on
[root@elrond var]#
```

# Samba

**Step 7** *Monitor and verify service is running*

```
[root@elrond ~]# service smb status
smbd (pid  674) is running...
nmbd (pid  677) is running...
[root@elrond ~]#
```

# Samba

**Step 7** *Monitor and verify service is running*

```
[root@elrond var]# netstat –tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:139                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:815                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:445                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
[root@elrond ~]#
```

*Port 139 is used for NetBIOS sessions (file and print sharing)*
*Port 445 is used for Microsoft Active Directory Services and it enables SMB to run over IP*

# Samba

**Step 7** *Monitor and verify service is running*

```
[root@elrond var]# netstat –uln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 172.30.4.131:137           0.0.0.0:*
udp        0      0 192.168.2.1:137            0.0.0.0:*
udp        0      0 0.0.0.0:137                0.0.0.0:*
udp        0      0 172.30.4.131:138           0.0.0.0:*
udp        0      0 192.168.2.1:138            0.0.0.0:*
udp        0      0 0.0.0.0:138                0.0.0.0:*
udp        0      0 0.0.0.0:809                0.0.0.0:*
udp        0      0 0.0.0.0:812                0.0.0.0:*
udp        0      0 0.0.0.0:54213              0.0.0.0:*
udp        0      0 0.0.0.0:5353               0.0.0.0:*
udp        0      0 0.0.0.0:111                0.0.0.0:*
udp        0      0 0.0.0.0:631                0.0.0.0:*
udp        0      0 :::56616                   :::*
udp        0      0 :::5353                    :::*
[root@elrond ~]#
```

*UDP Port 138 is used for NetBIOS name service (file and print sharing)*
*UDP Port 139 is used for NetBIOS datagram service (file and print sharing)*

# Trouble Shooting

# Samba

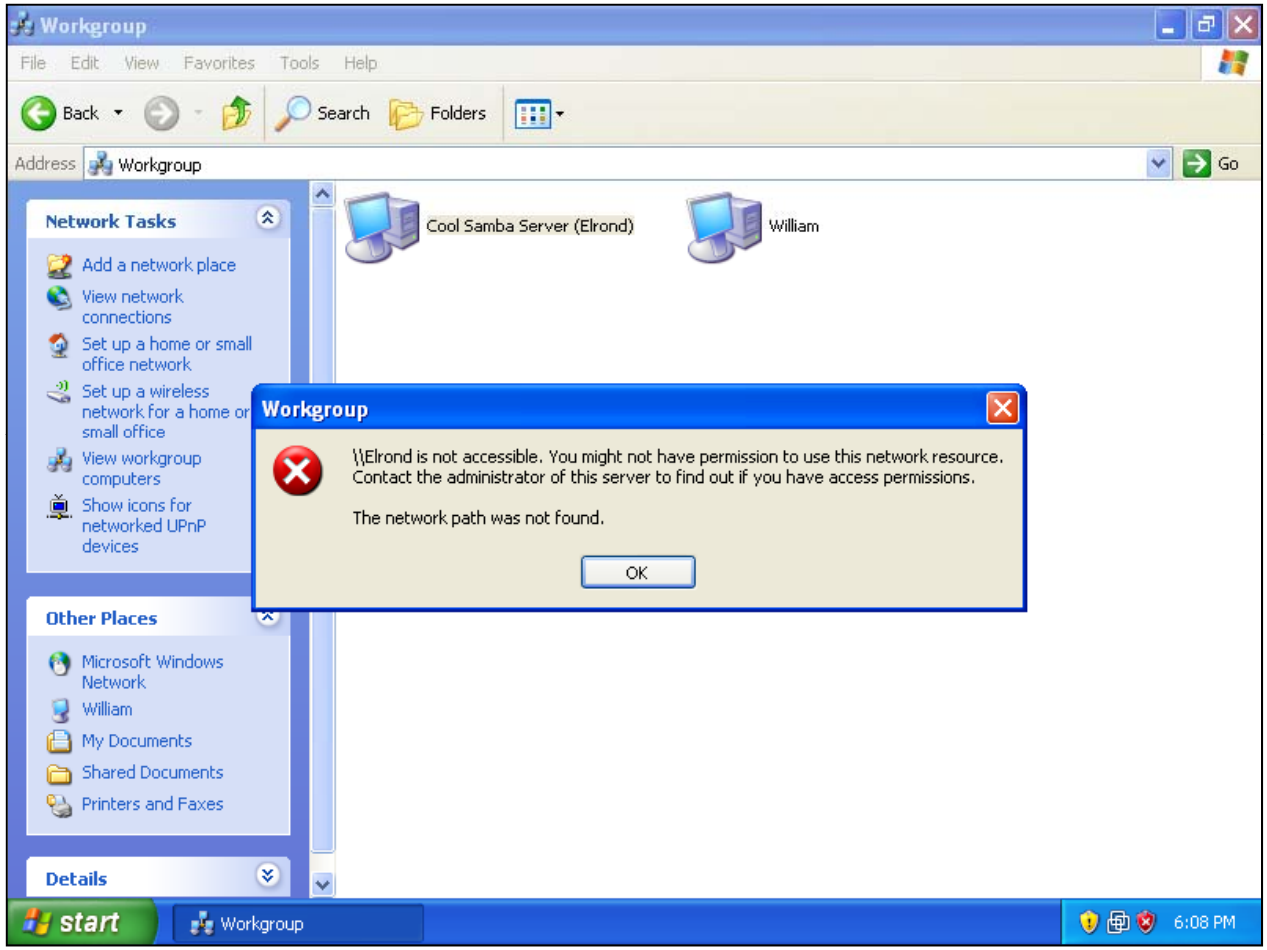
**Step 8** *Troubleshoot*

```
[root@elrond bin]# smbclient -L william100
Password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Sharename       Type      Comment
        ---------       ----      -------
cli rpc pipe open: cli nt create failed on pipe \srvsvc to machine william100.
Error was NT_STATUS_ACCESS_DENIED
Error returning browse list: NT_STATUS_ACCESS_DENIED
Anonymous login successful
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Server               Comment
        ---------            -------
        DV2000
        ELROND               Cool Samba Server
        WILLIAM100

        Workgroup            Master
        ---------            -------
        WORKGROUP            WILLIAM100
[root@elrond bin]#
```

Problem: Get error message above when trying to browse Samba Server.

Fix: specify a user (e.g. smbclient –L william100 –U cis192) and supply the password for that user when prompted.

## Step 8 *Troubleshoot*




Problem: Get error message above when trying to open Cool Samba Server.

Fix: Open firewall on Samba server to allow (ports 137/udp, 138/udp, 139/tcp, and 445/tcp)

# Samba

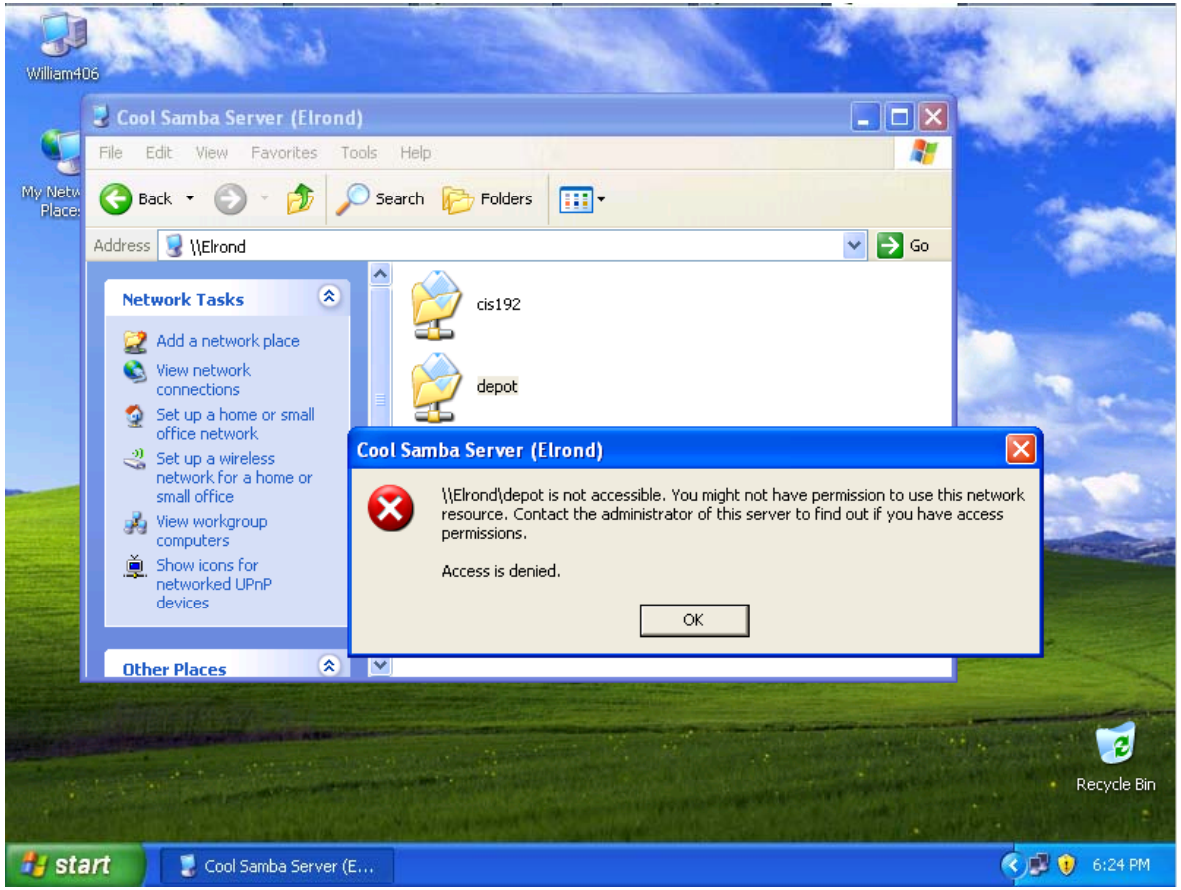
**Step 8** *Troubleshoot*

```
[root@legolas ~]# ping -c1 elrond
PING elrond (192.168.2.1) 56(84) bytes of data.
64 bytes from elrond (192.168.2.1): icmp_seq=1 ttl=64 time=2.10 ms

--- elrond ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.108/2.108/2.108/0.000 ms
[root@legolas ~]# smbclient -L elrond
Error connecting to 192.168.2.1 (No route to host)
Connection to elrond failed (Error NT_STATUS_HOST_UNREACHABLE)
[root@legolas ~]#
```

Problem: Get error message above when trying to browse Samba Server.

Fix: Open firewall on Samba server to allow (ports 137/udp, 138/udp, 139/tcp, and 445/tcp)

## Step 8 *Troubleshoot*




Problem: Get error message above when trying to open a share on Samba server

Fix: On Samba server, set the SELinux type on the shares with:

**chcon –R –t samba_share_t /var/shares/***

# Samba

**Step 8** *Troubleshoot*

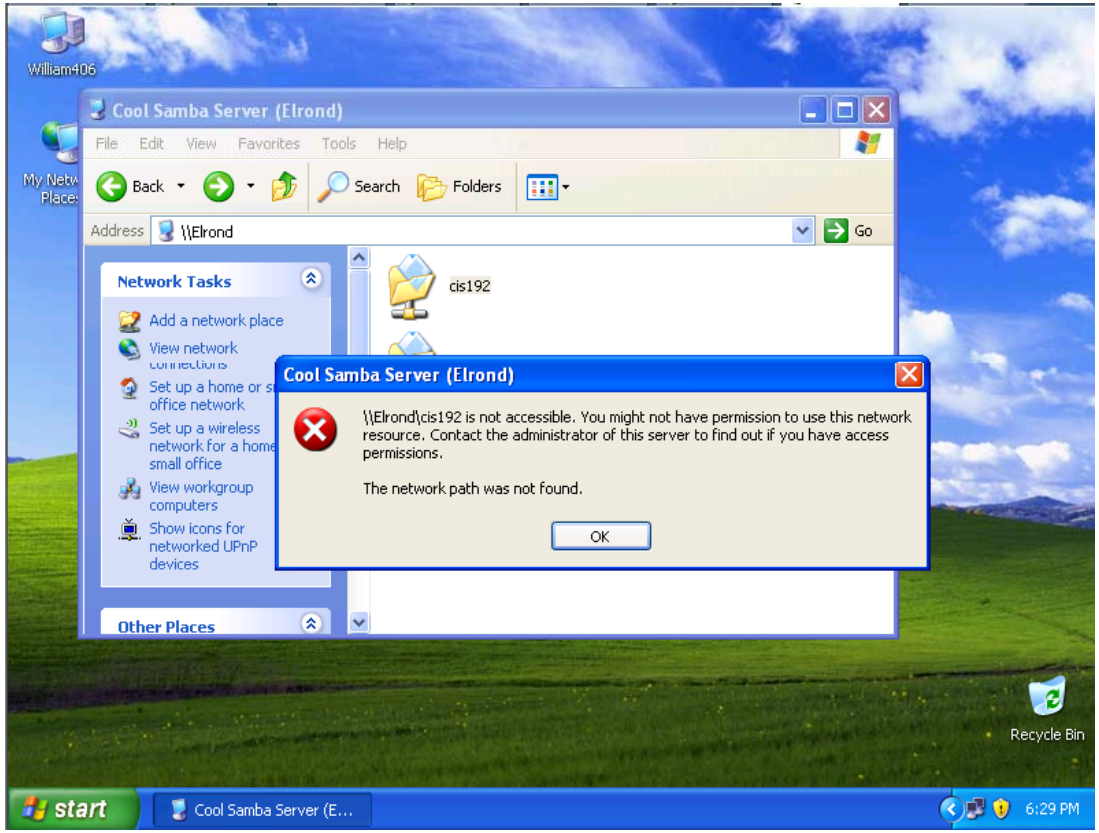
```
[root@legolas ~]# mount -o username=cis192 //elrond/depot /mnt
Password:
[root@legolas ~]# ls /mnt
ls: reading directory /mnt: Permission denied
[root@legolas ~]#
```

Problem: Get error message above when trying to open a share in /var/shares

Fix: On Samba server, set the SELinux type on the shares with:

**chcon –R –t samba_share_t /var/shares/***

## Step 8 *Troubleshoot*




Problem: Get error message above when trying to open home directory share on Samba server

Fix: Set the SELinux type with **setsebool -P samba_enable_home_dirs=1** to enable sharing home directories on the Samba server

# Samba

**Step 8** *Troubleshoot*

```
[root@legolas ~]# mount -o username=cis192 //elrond/cis192 /mnt
Password:
retrying with upper case share name
mount error 6 = No such device or address
Refer to the mount.cifs(8) manual page (e.g.man mount.cifs)
[root@legolas ~]#
```

Problem: Get error message above when trying to open home directory share on Samba server

Fix: Set the SELinux type with **setsebool -P samba_enable_home_dirs=1** to enable sharing home directories on the Samba server

# Samba

**Step 8** *Troubleshoot*

```
[root@legolas shares]# smbpasswd -a cis191
New SMB password:
Retype new SMB password:
tdbsam_open: Converting version 0 database to version 3.
account_policy_get: tdb_fetch_uint32 failed for field 1 (min password length), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 2 (password history), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 3 (user must logon to change password), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 4 (maximum password age), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 5 (minimum password age), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 6 (lockout duration), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 7 (reset count minutes), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 8 (bad lockout attempt), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 9 (disconnect time), returning 0
account_policy_get: tdb_fetch_uint32 failed for field 10 (refuse machine password change), returning 0
Added user cis191.
```

*Misleading messages that can happen the first time a new user is added. It still works and doesn't happen again.*

# Logs

# Samba

## Step 9 *Monitor log files*

```
[root@elrond ~]# tail -20 /var/log/messages
Apr 23 19:27:37 elrond nmbd[327]:
Apr 23 19:27:37 elrond nmbd[327]:   *****
Apr 23 20:14:39 elrond nmbd[327]: [2010/04/23 20:14:39, 0] nmbd/nmbd.c:terminate(58)
Apr 23 20:14:39 elrond nmbd[327]:   Got SIGTERM: going down...
Apr 23 20:16:39 elrond nmbd[626]: [2010/04/23 20:16:39, 0] nmbd/nmbd.c:terminate(58)
Apr 23 20:16:39 elrond nmbd[626]:   Got SIGTERM: going down...
Apr 23 20:18:45 elrond kernel:  CIFS VFS: cifs_read_super: get root inode failed
Apr 23 20:22:04 elrond kernel:  CIFS VFS: cifs_read_super: get root inode failed
Apr 23 20:22:22 elrond nmbd[677]: [2010/04/23 20:22:22, 0]
nmbd/nmbd_become_lmb.c:become_local_master_stage2(396)
Apr 23 20:22:22 elrond nmbd[677]:   *****
Apr 23 20:22:22 elrond nmbd[677]:
Apr 23 20:22:22 elrond nmbd[677]:   Samba name server ELROND is now a local master browser for workgroup
WORKGROUP on subnet 172.30.4.131
Apr 23 20:22:22 elrond nmbd[677]:
Apr 23 20:22:22 elrond nmbd[677]:   *****
Apr 23 20:22:22 elrond nmbd[677]: [2010/04/23 20:22:22, 0]
nmbd/nmbd_become_lmb.c:become_local_master_stage2(396)
Apr 23 20:22:22 elrond nmbd[677]:   *****
Apr 23 20:22:22 elrond nmbd[677]:
Apr 23 20:22:22 elrond nmbd[677]:   Samba name server ELROND is now a local master browser for workgroup
WORKGROUP on subnet 192.168.2.1
Apr 23 20:22:22 elrond nmbd[677]:
Apr 23 20:22:22 elrond nmbd[677]:   *****
[root@elrond ~]#
```

# Samba

## Step 9 *Monitor log files*

```
[root@elrond ~]# tail -20 /var/log/samba/nmbd.log
[2010/04/23 20:14:40, 0] nmbd/nmbd.c:main(724)
  Netbios nameserver version 3.0.33-3.15.el5_4.1 started.
  Copyright Andrew Tridgell and the Samba Team 1992-2008
[2010/04/23 20:16:39, 0] nmbd/nmbd.c:terminate(58)
  Got SIGTERM: going down...
[2010/04/23 20:16:40, 0] nmbd/nmbd.c:main(724)
  Netbios nameserver version 3.0.33-3.15.el5_4.1 started.
  Copyright Andrew Tridgell and the Samba Team 1992-2008
[2010/04/23 20:22:22, 0] nmbd/nmbd_become_lmb.c:become_local_master_stage2(396)
  *****

  Samba name server ELROND is now a local master browser for workgroup WORKGROUP on subnet 172.30.4.131

  *****
[2010/04/23 20:22:22, 0] nmbd/nmbd_become_lmb.c:become_local_master_stage2(396)
  *****

  Samba name server ELROND is now a local master browser for workgroup WORKGROUP on subnet 192.168.2.1

  *****
[root@elrond ~]#
```

# Logs

## Step 9 *Monitor log files*

```
[root@elrond ~]# tail -20 /var/log/samba/smbd.log
192.168.2.105 (192.168.2.105) connect to service depot192 initially as user cis192 (uid=500, gid=500) (pid
30617)
[2010/04/23 05:45:43, 1] smbd/service.c:close_cnum(1239)
  192.168.2.105 (192.168.2.105) closed connection to service depot192
[2010/04/23 05:45:49, 1] smbd/service.c:make_connection_snum(1042)
  192.168.2.105 (192.168.2.105) connect to service depot192 initially as user cis192 (uid=500, gid=500)
(pid 30619)
[2010/04/23 19:22:01, 1] smbd/service.c:close_cnum(1239)
  192.168.2.105 (192.168.2.105) closed connection to service depot192
[2010/04/23 19:22:04, 0] smbd/server.c:main(944)
  smbd version 3.0.33-3.15.el5_4.1 started.
  Copyright Andrew Tridgell and the Samba Team 1992-2008
[2010/04/23 19:30:24, 1] smbd/service.c:make_connection_snum(1042)
  192.168.2.105 (192.168.2.105) connect to service depot192 initially as user cis192 (uid=500, gid=500)
(pid 504)
[2010/04/23 20:14:39, 1] smbd/service.c:close_cnum(1239)
  192.168.2.105 (192.168.2.105) closed connection to service depot192
[2010/04/23 20:14:40, 0] smbd/server.c:main(944)
  smbd version 3.0.33-3.15.el5_4.1 started.
  Copyright Andrew Tridgell and the Samba Team 1992-2008
[2010/04/23 20:16:40, 0] smbd/server.c:main(944)
  smbd version 3.0.33-3.15.el5_4.1 started.
  Copyright Andrew Tridgell and the Samba Team 1992-2008
[root@elrond bin]#
```

# Security

# Samba

**Step 10** *Configure additional security*

- Maintain a firewall that prevents Internet access to ports 137-139 and 445

- smb.conf
  - [global] host based security example:
    hosts allow = 127.0.0.1 172.30.4.0/24
    hosts deny = 0.0.0.0/0

  - [global] Interface based security example:
    interfaces = lo eth1

  - [share-name] User based security example:
    valid users = cis192, cis192

# SWAT

# SWAT

## Overview

SWAT (Samba Web Administration Tool) is a web base configuration tool for samba shares

- Works under xinetd super daemon.
- Install the samba-swat package on Red Hat family of systems
- Edit the /etc/xinetd.d/swat configuration file and set *disable=no*
- Start or restart the xinetd service
- Browse to http://localhost:901
- Make a backup of your smb.conf file because it will be modified by SWAT
- For remote access, open firewall port tcp/901 and edit the *only_from* setting in /etc/xinetd.d/swat

# SWAT

```
[root@elrond samba]# yum install samba-swat
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package samba-swat.i386 0:3.0.33-3.7.el5 set to be updated
--> Processing Dependency: samba = 3.0.33-3.7.el5 for package: samba-swat
--> Processing Dependency: xinetd for package: samba-swat
--> Running transaction check
---> Package samba.i386 0:3.0.33-3.7.el5 set to be updated
--> Processing Dependency: perl(Convert::ASN1) for package: samba
--> Processing Dependency: samba-common = 3.0.33-3.7.el5 for package:
samba
---> Package xinetd.i386 2:2.3.14-10.el5 set to be updated
--> Running transaction check
--> Processing Dependency: samba-common = 3.0.28-1.el5_2.1 for package:
samba-client
---> Package perl-Convert-ASN1.noarch 0:0.20-1.1 set to be updated
---> Package samba-common.i386 0:3.0.33-3.7.el5 set to be updated
--> Running transaction check
---> Package samba-client.i386 0:3.0.33-3.7.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved
```

# SWAT

```
Dependencies Resolved

================================================================================
 Package                  Arch       Version           Repository         Size
================================================================================
Installing:
 samba-swat               i386       3.0.33-3.7.el5    base              8.2 M
Updating:
 samba                    i386       3.0.33-3.7.el5    base               16 M
 samba-common             i386       3.0.33-3.7.el5    base              8.7 M
Installing for dependencies:
 perl-Convert-ASN1        noarch     0.20-1.1          base               42 k
 xinetd                   i386       2:2.3.14-10.el5   base              124 k
Updating for dependencies:
 samba-client             i386       3.0.33-3.7.el5    base              5.7 M

Transaction Summary
================================================================================
Install      3 Package(s)
Update       3 Package(s)
Remove       0 Package(s)

Total download size: 39 M
Is this ok [y/N]: y
```

# SWAT

```
Is this ok [y/N]: y
Downloading Packages:
(1/6): samba-swat-3.0.33- 100% |=========================|  8.2 MB    00:45
(2/6): samba-client-3.0.3 100% |=========================|  5.7 MB    00:34
(3/6): samba-common-3.0.3 100% |=========================|  8.7 MB    00:47
(4/6): xinetd-2.3.14-10.e 100% |=========================|  124 kB    00:01
(5/6): perl-Convert-ASN1- 100% |=========================|   42 kB    00:00
(6/6): samba-3.0.33-3.7.e 100% |=========================|   16 MB    01:34
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating  : samba-common                 ########################### [1/9]
  Installing: xinetd                       ########################### [2/9]
  Installing: perl-Convert-ASN1            ########################### [3/9]
  Updating  : samba                        ########################### [4/9]
  Updating  : samba-client                 ########################### [5/9]
  Installing: samba-swat                   ########################### [6/9]
  Cleanup   : samba                        ########################### [7/9]
  Cleanup   : samba-common                 ########################### [8/9]
  Cleanup   : samba-client                 ########################### [9/9]
```

# SWAT

```
Installed: samba-swat.i386 0:3.0.33-3.7.el5
Dependency Installed: perl-Convert-ASN1.noarch 0:0.20-1.1 xinetd.i386
2:2.3.14-10.el5
Updated: samba.i386 0:3.0.33-3.7.el5 samba-common.i386 0:3.0.33-3.7.el5
Dependency Updated: samba-client.i386 0:3.0.33-3.7.el5
Complete!
[root@elrond samba]#
```

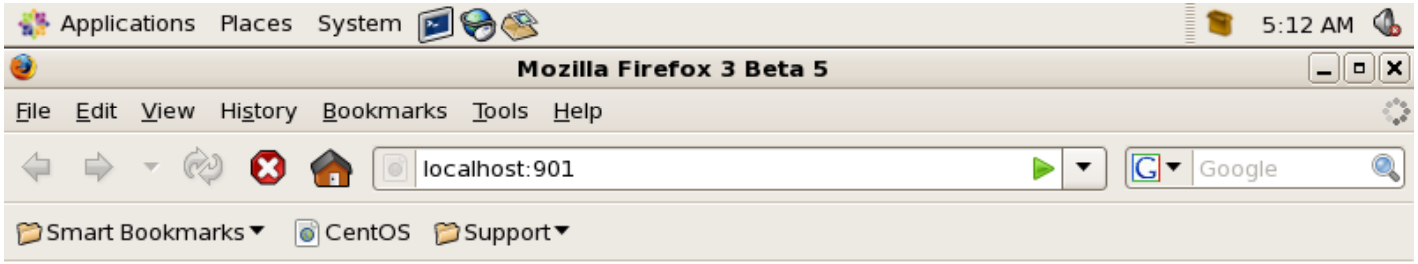
# Samba and SWAT

```
[root@elrond samba]# cat /etc/xinetd.d/swat
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#              to configure your Samba server. To use SWAT, \
#              connect to port 901 with your favorite web browser.
service swat
{
        port            = 901
        socket_type     = stream
        wait            = no
        only_from       = 127.0.0.1
        user            = root
        server          = /usr/sbin/swat
        log_on_failure  += USERID
        disable         = no
}

[root@elrond samba]# service xinetd start
Starting xinetd:                                           [  OK  ]
[root@elrond samba]#
```

*Change to no to enable SWAT service*

# SWAT

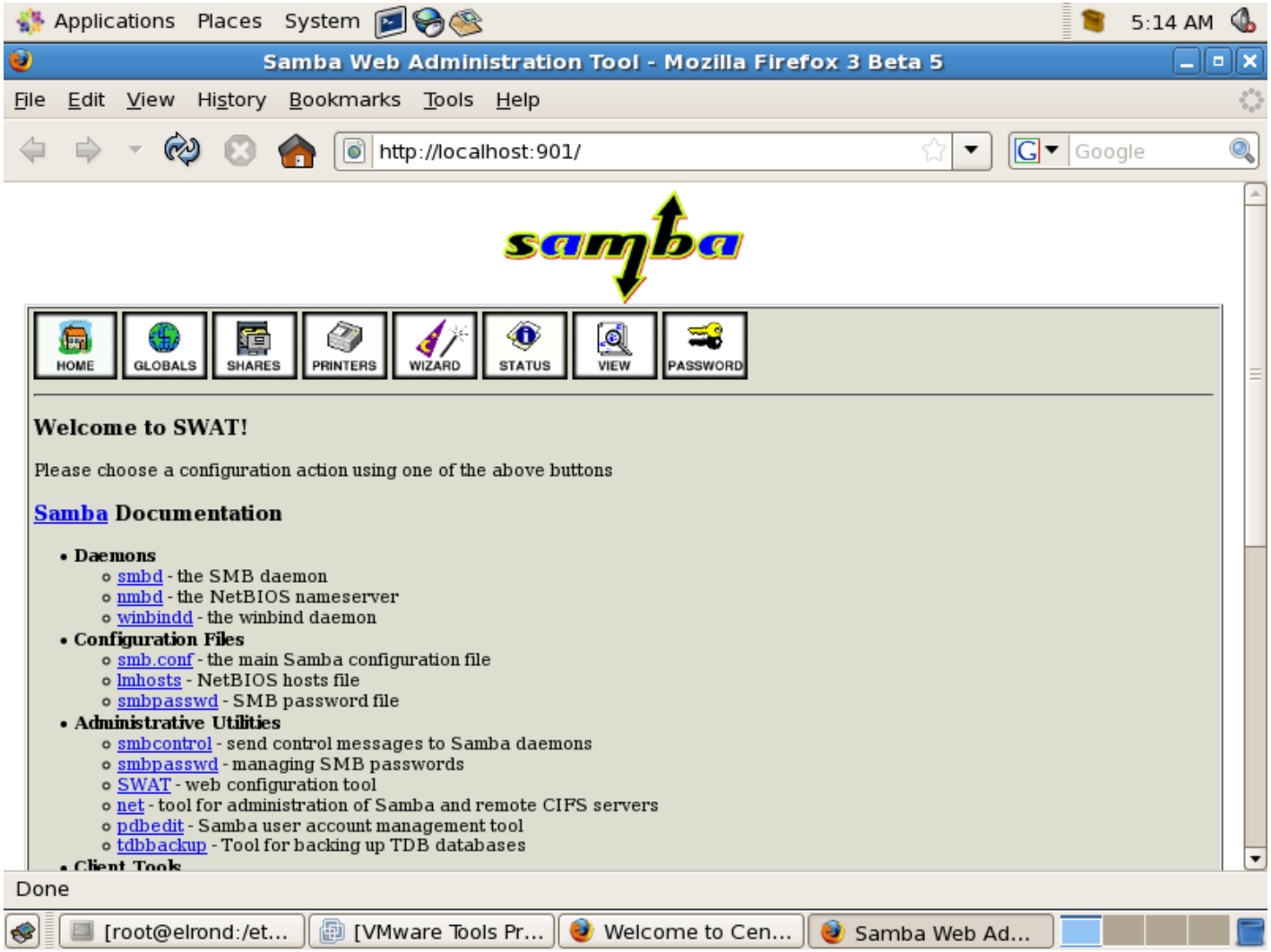
*Browse to http://localhost:901 and login*





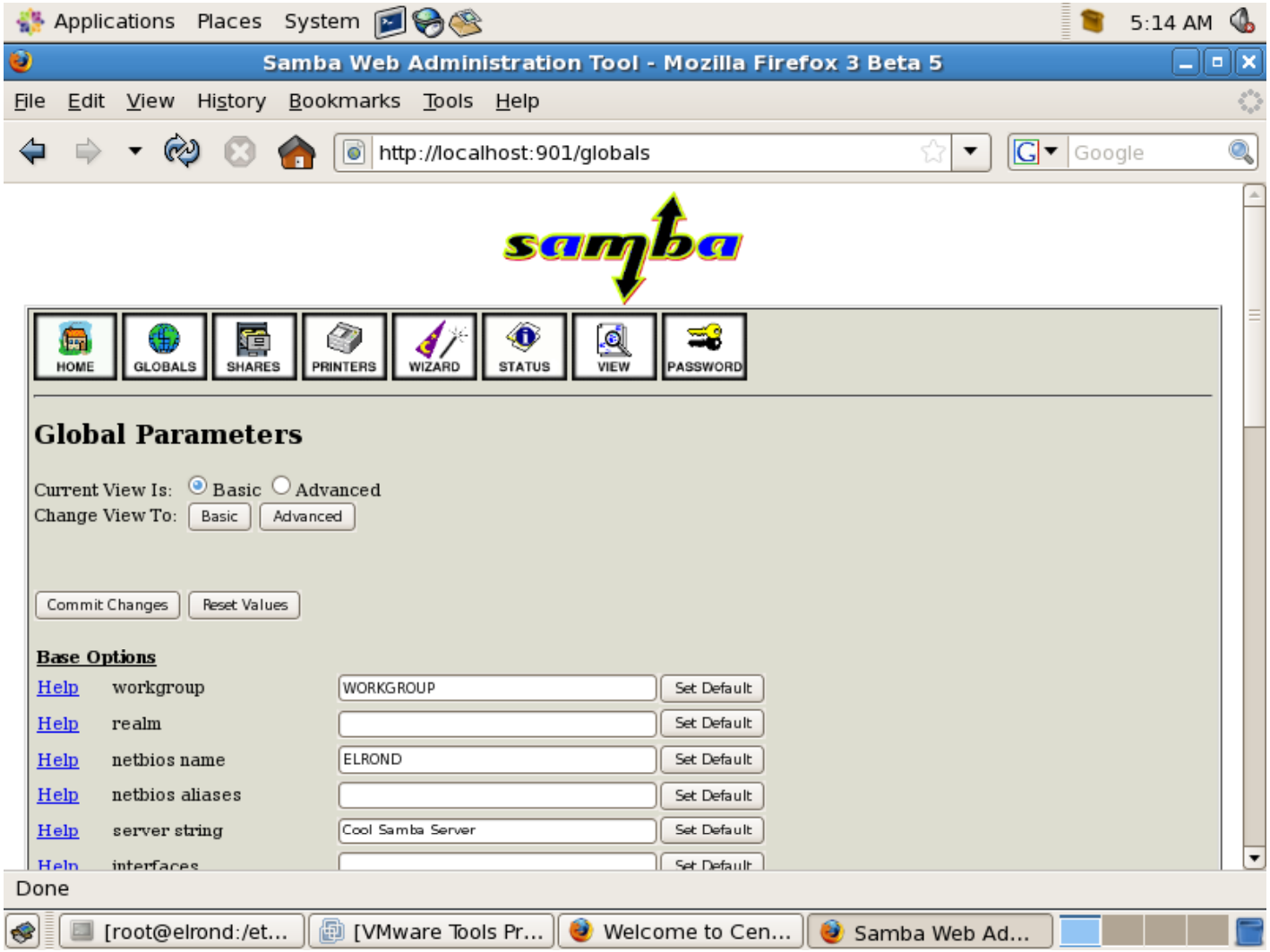
# SWAT

*Home page has documentation*



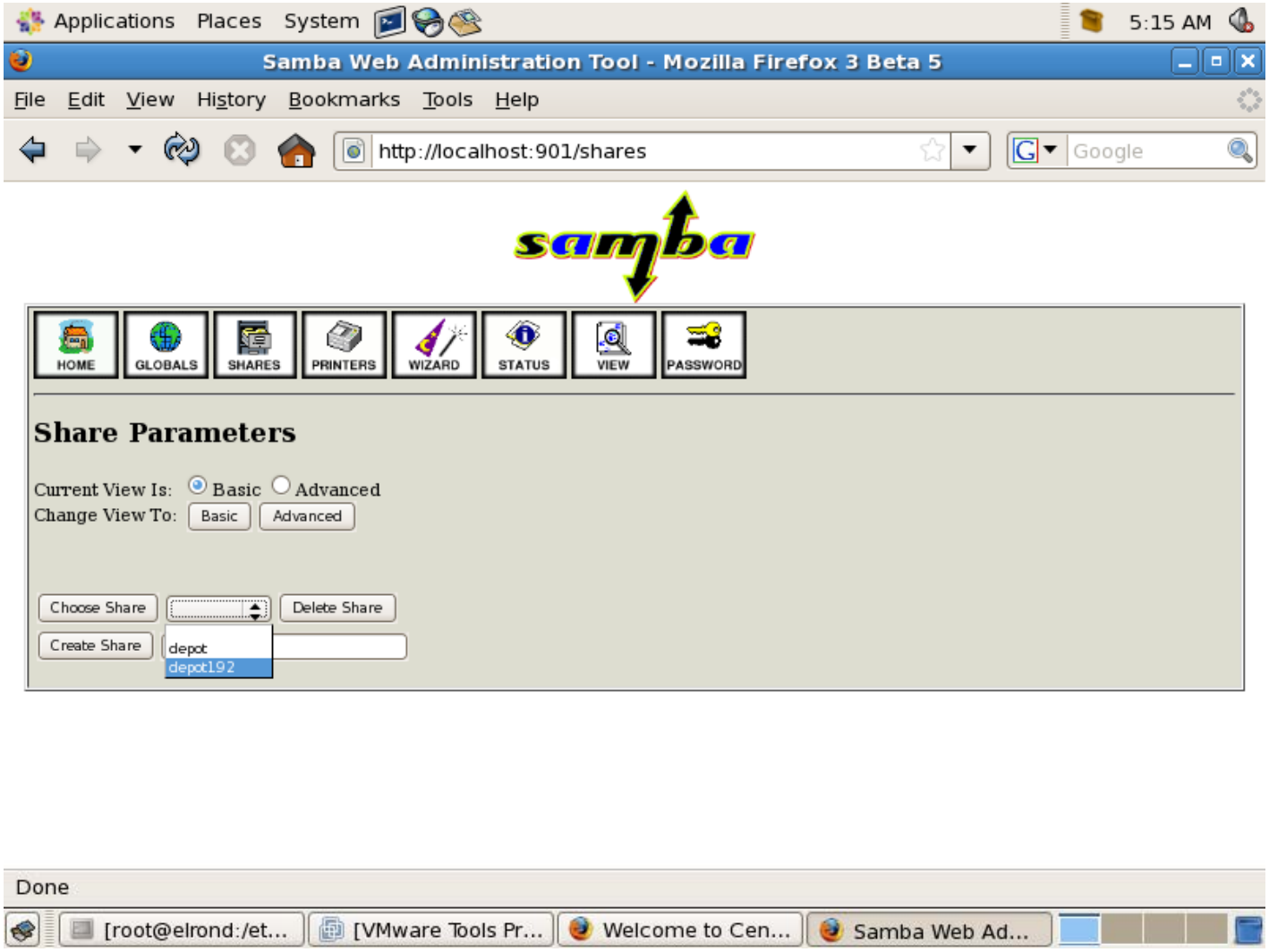
# SWAT

*Globals page*



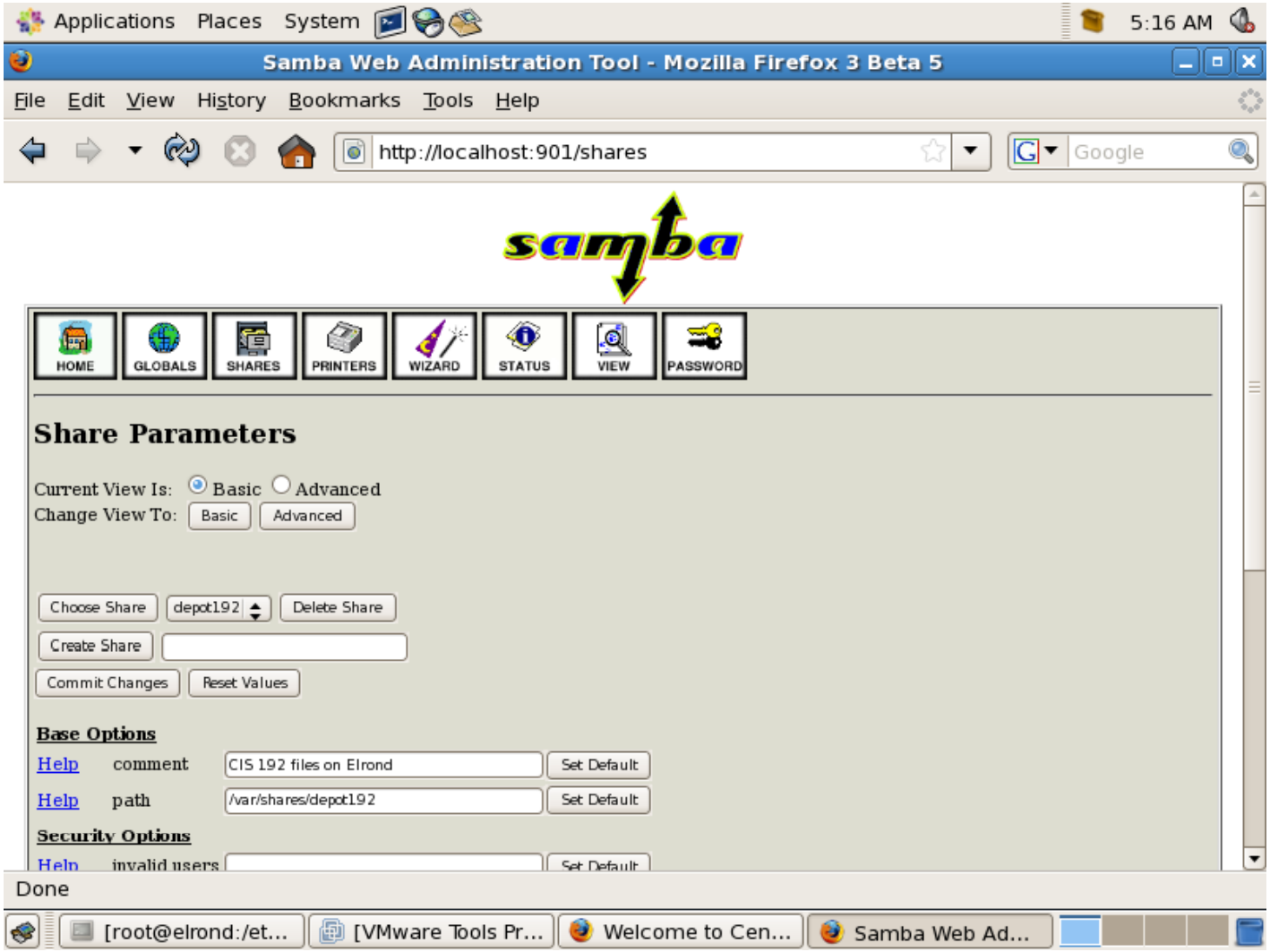
# SWAT

*Shares page where a share can be selected*



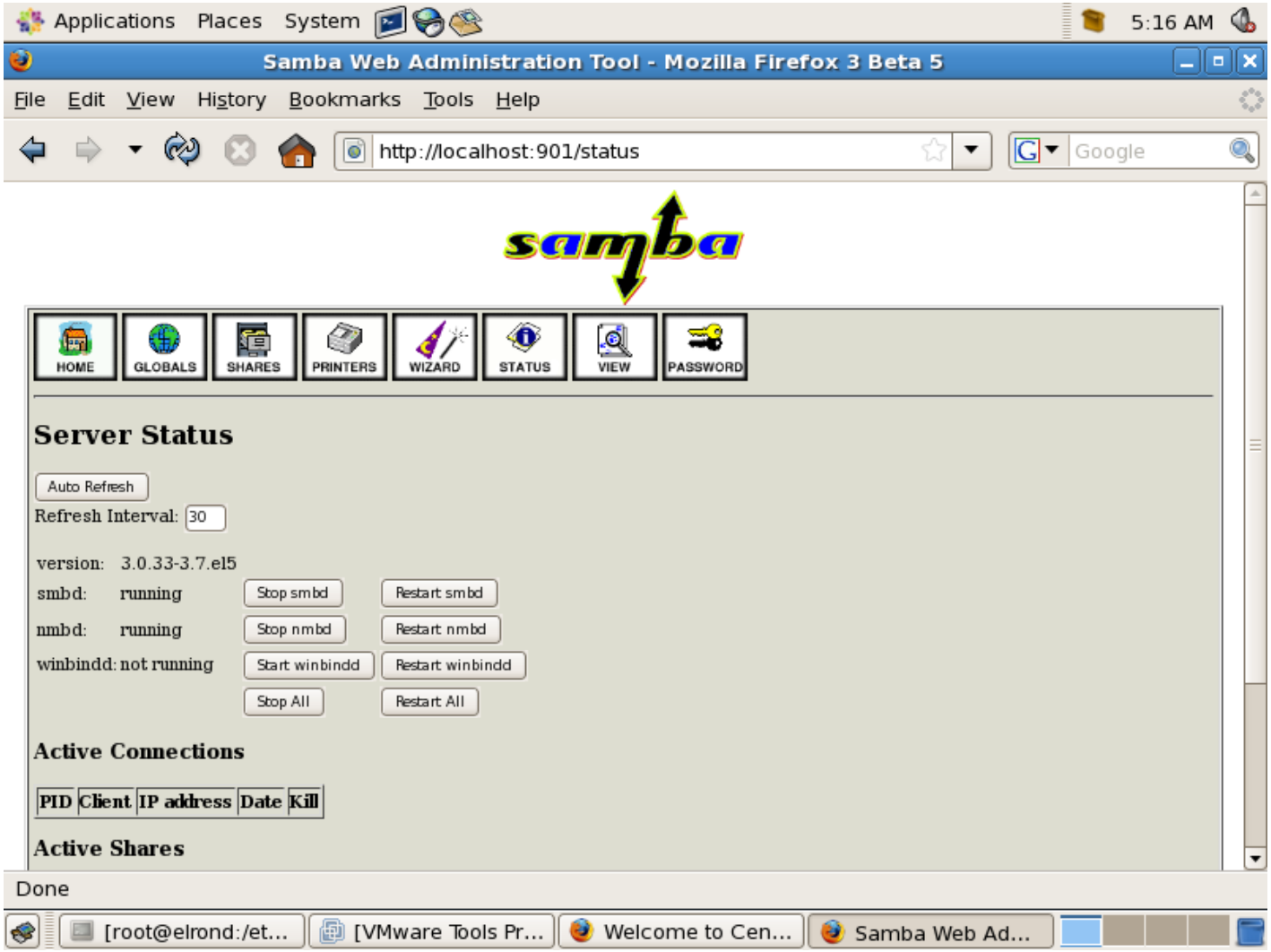
# SWAT

*Configure a specific share*



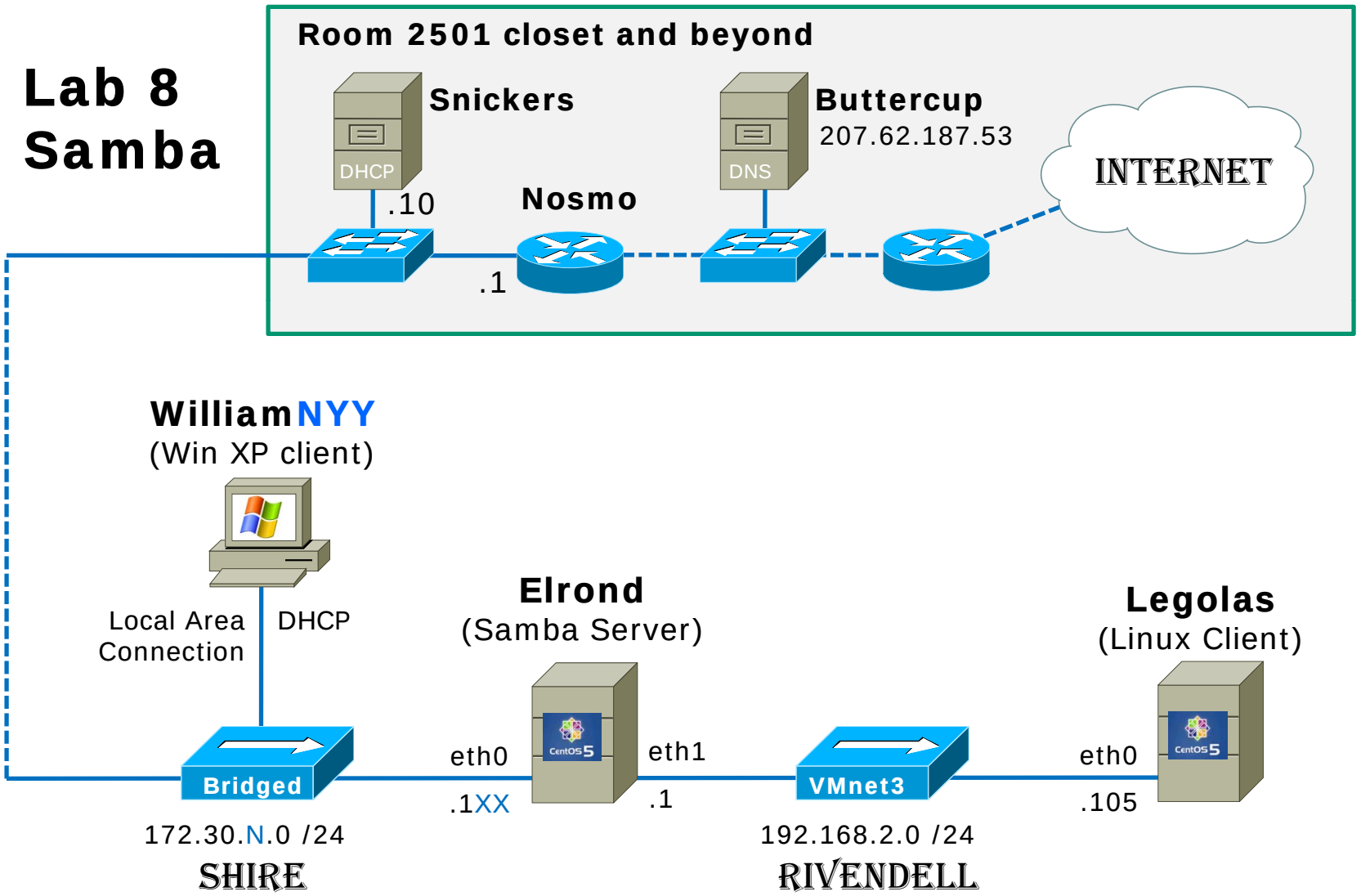
# SWAT

*Overall service status*




- Install samba-swat with **yum install samba-swat**
- Edit /etc/xinetd.d/swat and set *disable=no*
- Start xinetd with **service xinetd start**
- Browse to SWAT at http://localhost:901
- How would you make the SWAT available for remote access?

# Lab 8


Lab 8
Samba
Room 2501 closet and beyond
Snickers
DHCP
.10
Nosmo
.1
Buttercup
207.62.187.53
DNS
INTERNET
WilliamNYY
(Win XP client)
Local Area Connection
DHCP
Bridged
172.30.N.0 /24
SHIRE
Elrond
(Samba Server)
eth0
.1XX
eth1
.1
VMnet3
192.168.2.0 /24
RIVENDELL
Legolas
(Linux Client)
eth0
.105

# Wrap

# References

**Samba**

- http://www.samba.org
- http://www.rxn.com/services/faq/smb/samba.history.txt
- http://www.samba.org/samba/docs/Samba-HOWTO-Collection.pdf
- http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch10_:_Windows,_Linux,_and_Samba

**Samba and the firewall**

- http://troy.jdmz.net/samba/fw/

**TDB database**

- http://www.linuxtopia.org/online_books/network_administration_guides/samba_reference_guide/07_install_06.html#tdbpermfiledesc
- http://www.centos.org/docs/4/html/rhel-rg-en-4/s1-samba-account-info-dbs.html

**Network Browsing**

- http://www.centos.org/docs/4/html/rhel-rg-en-4/s1-samba-network-browsing.html

**Share options**

http://oreilly.com/catalog/samba/chapter/book/ch04_05.html

**ELinux**

http://www.crypt.gen.nz/selinux/faq.html#WWW.1
http://www.linuxtopia.org/online_books/getting_started_with_SELinux/SELinux_overview.html

**New commands, daemons:**
chcon –Rv –t samba_share_t *
ls -lRZ
smbclient –L computername
smbtree
testparm
smbd -b | grep PRIVATE_DIR

**Windows commands**
net view
net view \\computername
net use driveletter: \\computername\sharename
net use * /DELETE

**Configuration files**
/etc/samba/smb.conf

**Windows configuration files**
C:\WINDOWS\system32\drivers\etc\hosts

# Next Class

Assignment: Check Calendar Page
http://simms-teach.com/cis192calendar.php

Lab 8 and five posts due

Quiz questions for next class:

- What firewall ports must be opened for Samba?
- If you see the IPC$, ADMIN$ and C$ shares on a server is the server most likely running Linux or Windows?
- What option on the ls command will let you view the SELinux security contexts?

# Backup

## Classroom Static IP addresses for VM's

| Station | IP | Static 1 |
|---|---|---|
| Instructor | 172.30.1.100 | 172.30.1.125 |
| Station-01 | 172.30.1.101 | 172.30.1.126 |
| Station-02 | 172.30.1.102 | 172.30.1.127 |
| Station-03 | 172.30.1.103 | 172.30.1.128 |
| Station-04 | 172.30.1.104 | 172.30.1.129 |
| Station-05 | 172.30.1.105 | 172.30.1.130 |
| Station-06 | 172.30.1.106 | 172.30.1.131 |
| Station-07 | 172.30.1.107 | 172.30.1.132 |
| Station-08 | 172.30.1.108 | 172.30.1.133 |
| Station-09 | 172.30.1.109 | 172.30.1.134 |
| Station-10 | 172.30.1.110 | 172.30.1.135 |
| Station-11 | 172.30.1.111 | 172.30.1.136 |
| Station-12 | 172.30.1.112 | 172.30.1.137 |

| Station | IP | Static 1 |
|---|---|---|
| | | |
| Station-13 | 172.30.1.113 | 172.30.1.138 |
| Station-14 | 172.30.1.114 | 172.30.1.139 |
| Station-15 | 172.30.1.115 | 172.30.1.140 |
| Station-16 | 172.30.1.116 | 172.30.1.141 |
| Station-17 | 172.30.1.117 | 172.30.1.142 |
| Station-18 | 172.30.1.118 | 172.30.1.143 |
| Station-19 | 172.30.1.119 | 172.30.1.144 |
| Station-20 | 172.30.1.120 | 172.30.1.145 |
| Station-21 | 172.30.1.121 | 172.30.1.146 |
| Station-22 | 172.30.1.122 | 172.30.1.147 |
| Station-23 | 172.30.1.123 | 172.30.1.148 |
| Station-24 | 172.30.1.124 | 172.30.1.149 |


*Note the static IP address for your station to use in the next class exercise*

# Classroom DHCP IP allocation pools table by station number

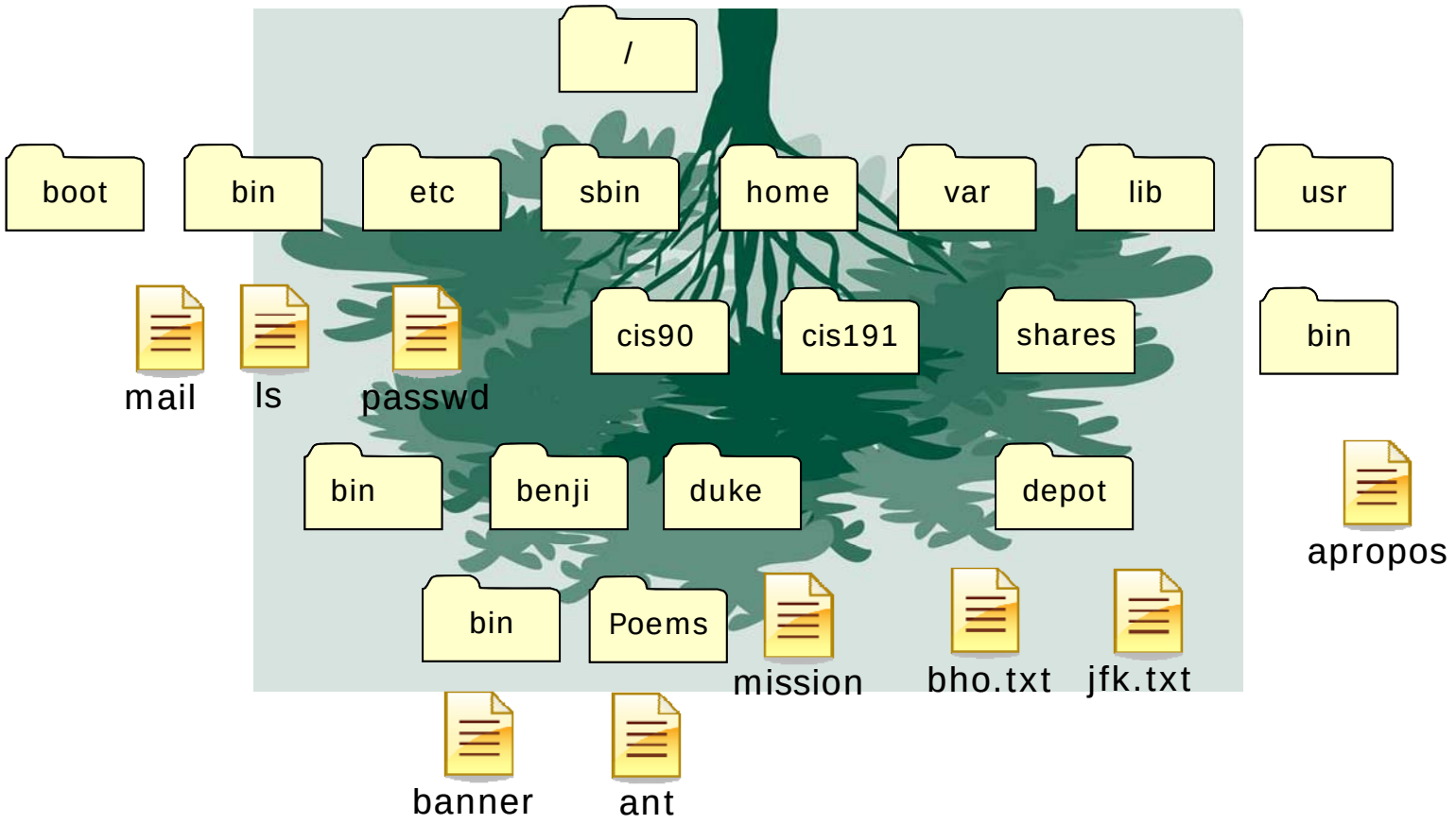
| Station | IP | Start | End |
|---|---|---|---|
| 01 | 172.30.1.101 | 172.30.1.50 | 172.30.1.54 |
| 02 | 172.30.1.102 | 172.30.1.55 | 172.30.1.59 |
| 03 | 172.30.1.103 | 172.30.1.60 | 172.30.1.64 |
| 04 | 172.30.1.104 | 172.30.1.65 | 172.30.1.69 |
| 05 | 172.30.1.105 | 172.30.1.70 | 172.30.1.74 |
| 06 | 172.30.1.106 | 172.30.1.75 | 172.30.1.79 |
| 07 | 172.30.1.107 | 172.30.1.80 | 172.30.1.84 |
| 08 | 172.30.1.108 | 172.30.1.85 | 172.30.1.89 |
| 09 | 172.30.1.109 | 172.30.1.90 | 172.30.1.94 |
| 10 | 172.30.1.110 | 172.30.1.95 | 172.30.1.99 |
| 11 | 172.30.1.111 | 172.30.1.200 | 172.30.1.204 |
| 12 | 172.30.1.112 | 172.30.1.205 | 172.30.1.209 |
| | | | |

| Station | IP | Start | End |
|---|---|---|---|
| 13 | 172.30.1.101 | 172.30.1.210 | 172.30.1.214 |
| 14 | 172.30.1.102 | 172.30.1.215 | 172.30.1.219 |
| 15 | 172.30.1.103 | 172.30.1.220 | 172.30.1.224 |
| 16 | 172.30.1.104 | 172.30.1.225 | 172.30.1.229 |
| 17 | 172.30.1.105 | 172.30.1.230 | 172.30.1.234 |
| 18 | 172.30.1.106 | 172.30.1.235 | 172.30.1.239 |
| 19 | 172.30.1.107 | 172.30.1.240 | 172.30.1.244 |
| 20 | 172.30.1.108 | 172.30.1.245 | 172.30.1.249 |
| 21 | 172.30.1.109 | 172.30.1.250 | 172.30.1.254 |
| 22 | 172.30.1.110 | 172.30.1.30 | 172.30.1.34 |
| 23 | 172.30.1.111 | 172.30.1.35 | 172.30.1.39 |
| 24 | 172.30.1.112 | 172.30.1.20 | 172.30.1.44 |
| Instruct | 172.30.1.100 | 172.30.1.45 | 172.30.1.49 |


*Use these pools of addresses based on your station number to avoid conflicts on the classroom network*

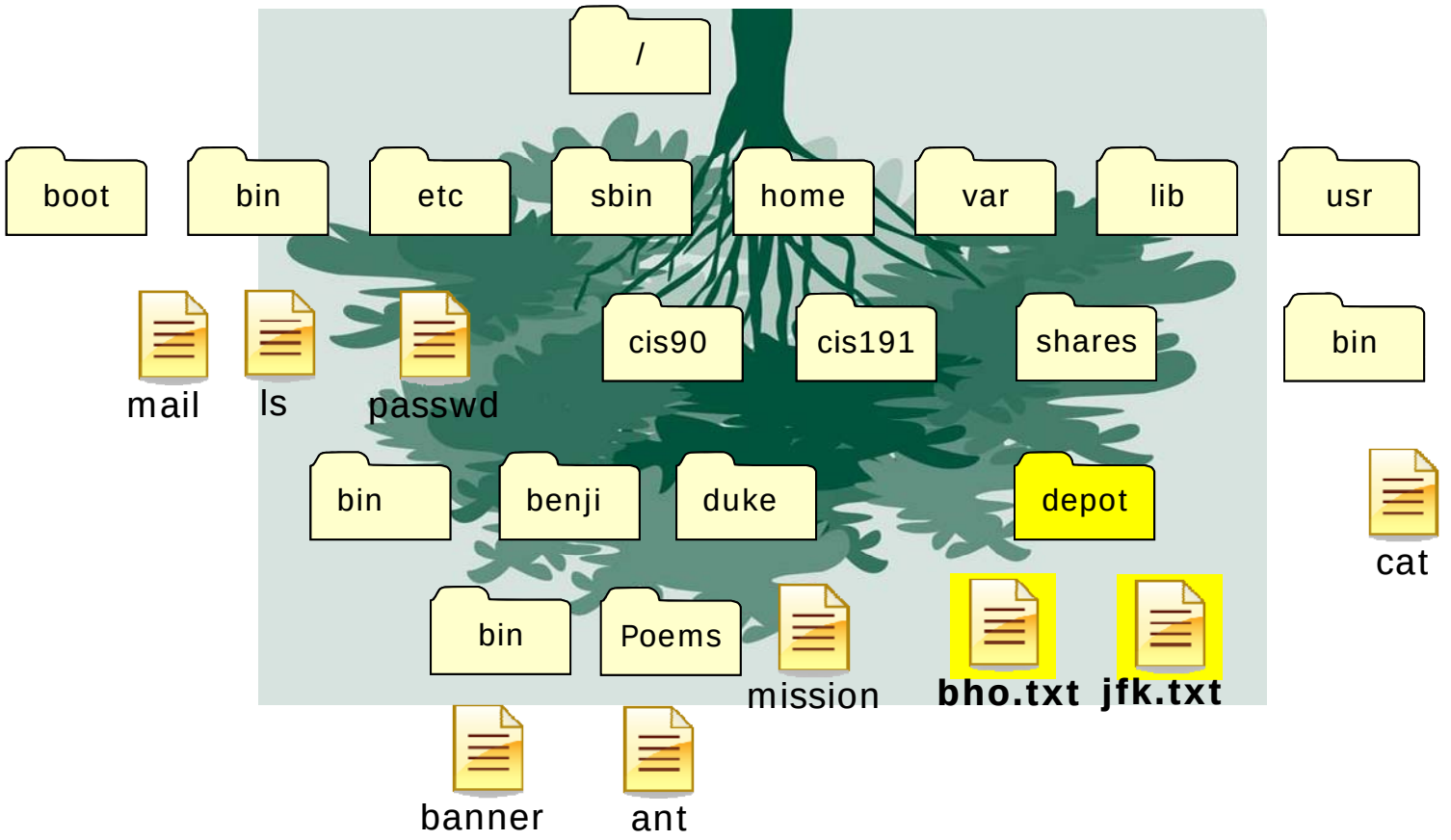
# Samba

## Overview



# Samba

## Overview



# Samba

***I. Four main goals of Samba software***

- *File and print services*
- *Authentication and authorization*
- *Name Resolution*
- *Service announcement or browsing*

***II. Software downloads from www.samba.org***

***III. Samba may be configured for one of four security modes:***

- *Share - no user-level authentication required*
- *User - Authenticates against the local /etc/passwd file*
- *Server - Uses a Microsoft server for its accounts database*
- *Domain - Uses a Domain Controller to authenticate the incoming user*

# Samba

***IV. Microsoft networking concepts***

- *NetBIOS - Network Basic Input Output System*
- *SMB - Server Message Blocks protocol - performs file and print sharing*
- *NMB - Name Message Blocks - name resolution and browsing functions*

***V. Connecting to Microsoft systems***

- ***smbclient*** *- used to list and connect to shares on an MS client*
  ***smbclient -L Servername -U account%password***
  ***smbclient //Servername/sharename -U account[%password]***
- *smb interpreter: cd, ls, get, put, mget, mput, md, lcd, !*

# Samba

## *VI. Mounting a remote file share*

*For a persistent share, you can mount a remote filesystem with:*

- *mount -t smbfs -o username=username,password=password //servername/sharename /mntpoint*
- *smbmount //servername/sharename /mntpoint -o username=username*

## *VII. Configuring the Samba software*

- *rpm -qi samba*
- *smb.conf:*
  - *Global Section - server-wide parameters*
  - *Share Definitions - share listings are specified here*

# Samba

***VIII. Creating file shares for use with the Samba Server***

- *Home directories are shared by default*
- *Each share needs a section with one or more of the following defined:*

*comment - a descriptive comment about the share visible to those browsing*

*path - the absolute path to the share directory on the Samba server*

*writable - allows users connected to the share to add or modify files in the share*

*browseable - specifies whether the share should be visible in Network Neighborhood and other share lists*