

Author : Tony Hill

Date : 23rd March 2013

Version : 1-1

Linux OS: Ubuntu 12.04.2 LTS (precise)

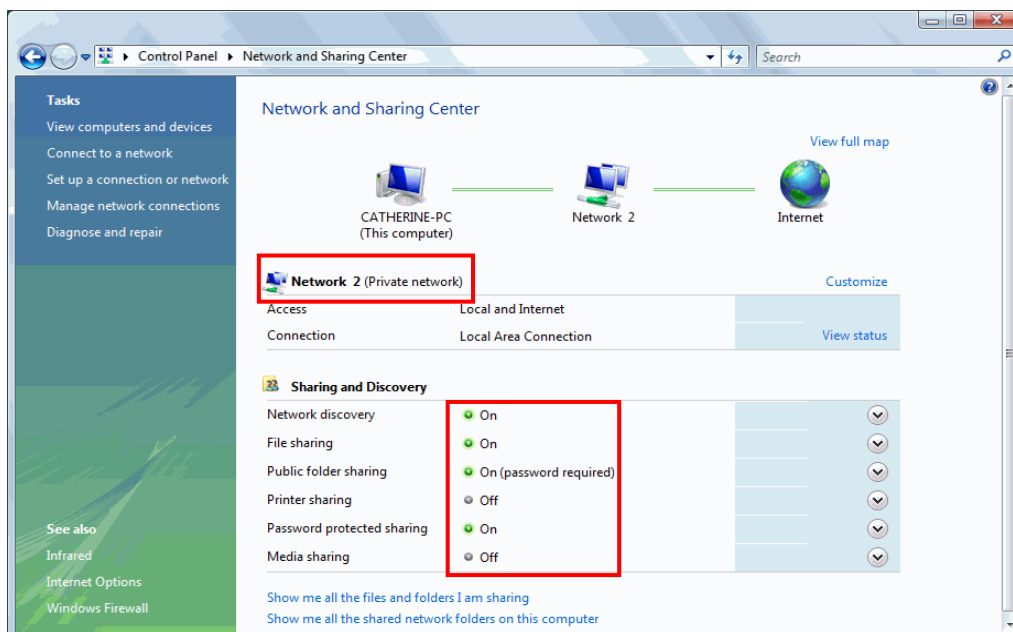
Kernel : v3.2.0-39

Samba2 : v3.6.3-2

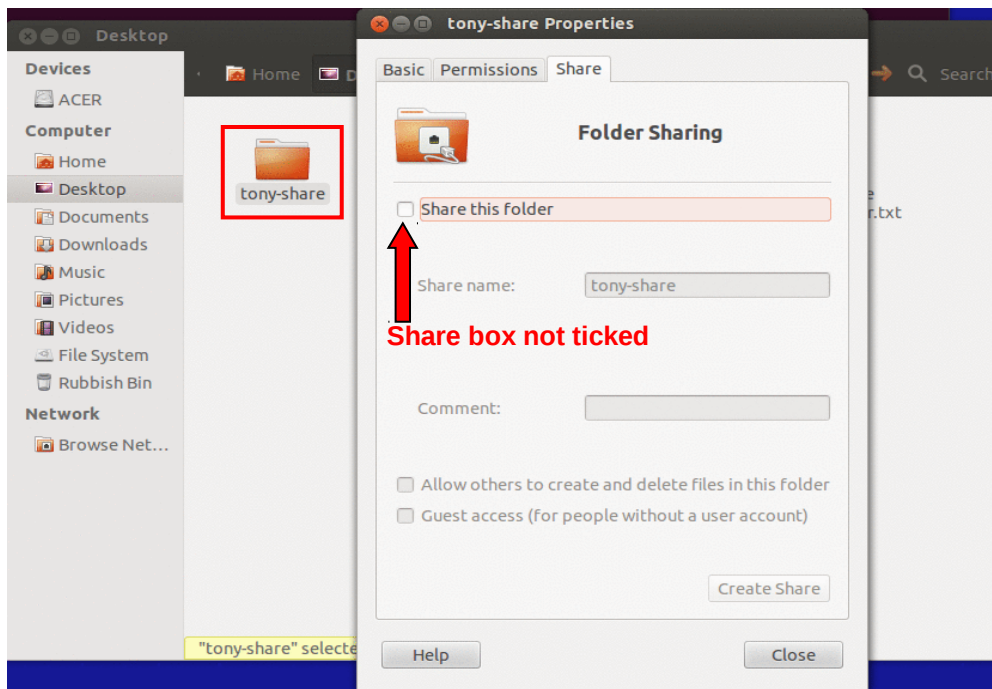
1 Introduction

This paper describes how to set up SAMBA shares between a Windows Vista (Home Premium) PC running native Microsoft networking and a Ubuntu PC running Samba.

The Windows PC is sharing only its “*public*” folders with the settings below. Note that the network is configured to be a Private network and that password protected sharing is enabled.



The Ubuntu PC uses Samba to share the folder “*/home/tony/Desktop/tony-share*”. The folder itself is NOT set up as a share i.e. the “Share this folder” box is not ticked.



The name of the Windows Vista PC is “catherine-pc” and the name of the Ubuntu PC is “tony-laptop”.

2 SAMBA Configuration

2.1 SMB Configuration File

Carry out the following steps to configure the Samba server on the Ubuntu PC:

- 1) Choose an existing Linux user to own the share, or add a new Linux user. This example uses the pre-existing Linux user “tony”.
- 2) Add the Samba user. A matching Linux user must already exist on the PC:

```
smbpasswd -a tony
```

- 3) Verify that the Samba user has been added successfully to the back-end password database:

```
pdbedit -L -v
```

- 4) Configure the following parameters in the “/etc/samba/smb.conf” file:

```
[global]
workgroup = home                << essential
server string = tony-laptop     << optional description
netbios name = tony-laptop     << essential
smb ports = 139 445            << essential

wins support = yes              << only on one Samba PC
name resolve order = wins bcst << optimum
dns proxy = no                  << essential if not using DNS

interfaces = eth0               << add wlan0 if needed

<snip - skip logging & accounting>
```

```
security = user                << recommended
encrypt passwords = yes       << essential for security
obey pam restrictions = yes   << passw authentication module
unix password sync = yes     << recommended
pam password change = yes    << passw authentication module
map to guest = bad user      << recommended
```

<snip - skip domains>

<snip - skip printing, can be changed later>

```
domain master = no            << explained below
local master = yes           << explained below
preferred master = yes       << explained below
os level = 65                 << explained below
```

```
[tony-share]                   << define shares
path = /home/tony/Desktop/tony-share
writeable = yes               << adjust accordingly
browseable = yes              << adjust accordingly
valid users = tony            << match Samba user
```

Note: The Password Authentication Module (PAM) is a Linux mechanism to enforce standards for password creation and maintenance, such as password length, expiry, number of retries etc.

- 5) Issue the following command to restart the Samba daemon for the above configuration to take effect:

```
service smbd restart
```

2.1.1 WINS

The “*wins support = yes*” line in step (4) instructs the Samba server to support the Windows Internet Name Service (WINS). This causes the server to instantiate a WINS server to process NETBIOS Name resolution requests from Windows clients. Only one WINS server should exist on the LAN at any given time otherwise name resolution will break.

If there is already a WINS sever on the LAN, configure the Samba server to point to it using the following entry in the “*smb.conf*” file:

```
wins server = <ip address of WINS server>
```

Configuration of “*wins server = <ip address>*” and “*wins support = yes*” is mutually exclusive. One or the other must be configured but not both.

2.1.2 Broadcasts

The “*name resolve order*” in step (4) is configured to support both WINS and broadcast for name resolution. If all of the Windows clients are configured to support the sending of WINS resolution requests it is not necessary to configure broadcast. In fact, the ideal situation is for all clients to be configured to either support WINS or broadcast, but not both.

Note: The Vista PC is not configured to support WINS in this example, mainly because clients that don't support WINS may be connected to the LAN at some

point in the future. Also, this allows me to demonstrate that accessing shares is still possible even with the most basic, default set-up.

Use the following procedure to set up WINS support on the Windows PC if you do wish to use WINS for name resolution:

- 1) Control Panel → Network and Internet → Network and Sharing Centre
- 2) Click on Manage Network Connections in the left-hand pane
- 3) Right click on the active Local Area Connection and select Properties
- 4) Scroll down to and select Internet Protocol Version 4 (TCP/IPv4)
- 5) Click on Properties and then Advanced
- 6) Select the WINS tab and click on Add
- 7) Enter the IP address of the WINS server (the Samba or other WINS server)

2.1.3 LMHOSTS

With LMHOSTS, static IP address to NETBIOS Name mappings are configured on every client and the Samba server. This is more efficient in one sense in that it eliminates name resolution broadcast traffic on the LAN segment but is too fiddly and time consuming for networks that have many connected PCs.

Please note that it is important for the name resolution method to be consistent across all PCs on the LAN so choose either WINS, LMHOSTS or broadcast but do not mix them.

Perform the following steps on the Windows PC if you do wish to use LMHOSTS:

- 1) Follow the same procedure as above in the WINS configuration to step (5)
- 2) Ensure that the “Enable LMHOSTS lookup” box is ticked (do not add a WINS server)
- 3) Open Notepad in elevated privilege mode
- 4) Open the file “C:\Windows\System32\drivers\etc\lmhosts” and enter the IP address to name mappings at the foot of the file. In this example the Samba server’s NETBIOS name is “tony-laptop”
192.168.1.66 tony-laptop

Perform the following steps on the Ubuntu PC to configure LMHOSTS:

- 1) Edit the file “/etc/samba/smb.conf” and enter the following line in the global section:
name resolve order = lmhosts wins bcast
- 2) Restart “smbd” for the change to take effect:
service smbd restart
- 3) Create the file “lmhosts” in the “/etc/samba” directory
- 4) Enter the IP address to name mappings at the foot of the file. In this example the Windows PC’s NETBIOS name is “catherine-pc”
192.168.1.73 catherine-pc
- 5) Issue the following command to tell the Samba server’s network message block daemon (nmbd) the location of the “lmhosts” file:
nmbd -H /etc/samba/lmhosts -D

6) Restart the “nmbd” daemon for the change to take effect:

```
service nmbd restart
```

2.2 NETBIOS Browser Service

2.2.1 Browser Service Overview

Windows network devices use the NETBIOS browser service (UDP port 138) to advertise who they are, their configured workgroups, the file and print shares they offer, and any other capabilities that they support. The devices advertise this information in “browse lists”. This exchange of information can be very inefficient in large network environments due to the amount of broadcast traffic that is generated.

To overcome this, the browser service elects a master and backup browser to collect information from all the clients on the LAN segment. When a client wishes to know what workgroups, shares or printers are available on the network it interrogates only the master browser, or the backup browser if the master is out of action. The master browser is referred to as the Local Master Browser (LMB).

There is also a Domain Master in Windows networking. This is used only for extended Windows networks that encompass multiple NETBIOS LAN segments that are inter-connected over a wide area network. The Domain Master function is not relevant to this example and is not configured.

2.2.2 The Local Master Browser

Configure the Samba server to win the LMB election by setting its “**os level**” to a high value in the following lines of the “**smb.conf**” file:

```
domain master = no
local master = yes
preferred master = yes
os level = 65
```

The default value of the “**os level**” is usually 32.

The other devices on the LAN segment argue amongst themselves until a backup browser is elected.

Only one Samba server should be configured to be the LMB. If there is more than one Samba server on the network configure the other Samba server’s “**os level**” to be lower than 65 but higher than the default value of 32.

The packet captures below show the election process and various capabilities exchanges taking place. The Samba server uses the browser service (BROWSER UDP port 138) to broadcast its intention to become the LMB forcing an election to be initiated. It sends out a number of broadcasts specifying its priority and waits to see if any other devices contest its claim.

192.168.1.66	192.168.1.255	BROWSER	236 Browser Election Request
--------------	---------------	---------	------------------------------

The Samba server has the highest priority (“os level”), no other devices contest its claim so it becomes the LMB. It then uses the NETBIOS Name Service (NBNS UDP port 137) to broadcast its registration as the master browser for the LAN segment.

```
192.168.1.66      192.168.1.255      NBNS      110 Registration NB <01><02> __MSBROWSE__ <02><01>
```

It then broadcasts (NBNS UDP port 137) its registration of the workgroup HOME, which is configured in the “*smb.conf*” file.

```
192.168.1.66      192.168.1.255      NBNS      110 Registration NB HOME<1d>
```

The LMB broadcasts (BROWSER UDP port 138) its capabilities as a workstation, file server, print queue server etc.

```
192.168.1.66      192.168.1.255      BROWSER   254 Local Master Announcement TONY-LAPTOP, Workstation, Server,
```

The Windows Vista PC broadcasts (BROWSER UDP port 138) its browser list containing its capabilities i.e. workstation, file (share) server, NT machine etc.

```
192.168.1.73      192.168.1.255      BROWSER   243 Host Announcement CATHERINE-PC, Workstation, Server, M
```

From this point onwards the Windows PCs periodically connect (NBNS TCP port 137) to the LMB (Samba server) to refresh their knowledge of the workgroups, devices and capabilities that exist on the LAN segment.

2.2.3 Browser Service Services

The list below shows examples of the services that the devices advertise using the browser service (UDP port 138). The Ubuntu and Vista PCs advertise, amongst other things, File Server Service <20> because they are both offering shares to the network.

Name	Number (h)	Type	Usage
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<\\--__MSBROWSE__>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Microsoft Exchange Interchange(MSMail)
<computername>	23	U	Microsoft Exchange Store

<snip>

<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections

2.3 NEBIOS Name Cache

Having obtained the NETBIOS name to IP address mappings, be it through WINS, LMHOSTS or broadcasts, each device on the network maintains a local name cache so that it can contact or connect to other devices on the LAN segment.

The output below is the name cache entry that the Ubuntu PC holds for the Vista PC (CATHERINE-PC). Note that the services that the Vista PC offers are also shown. For example, CATHERINE-PC is a workstation <00>, and a file server <20> in workgroup HOME <00>. CATHERINE-PC is eligible to participate in browser service elections within that workgroup <1e>.

```
root@tony-laptop:~# nmblookup -A 192.168.1.73
Looking up status of 192.168.1.73
CATHERINE-PC    <00> -          B <ACTIVE>
HOME            <00> - <GROUP> B <ACTIVE>
CATHERINE-PC    <20> -          B <ACTIVE>
HOME            <1e> - <GROUP> B <ACTIVE>
```

MAC Address = 00-1D-72-D6-CA-D2

The output below is the name cache entry that the Ubuntu PC (TONY-LAPTOP) holds for itself. Note that TONY-LAPTOP is a workstation <00>, supports inter-device messaging <03>, and is a file server <20> in workgroup HOME <00>. It is eligible to participate in master browser elections <1e> and is the elected Master Browser <01> for the workgroup.

```
root@tony-laptop:~# nmblookup -A 192.168.1.66
Looking up status of 192.168.1.66
TONY-LAPTOP     <00> -          B <ACTIVE>
TONY-LAPTOP     <03> -          B <ACTIVE>
TONY-LAPTOP     <20> -          B <ACTIVE>
.._MSBROWSE_.. <01> - <GROUP> B <ACTIVE>
HOME            <1d> -          B <ACTIVE>
HOME            <1e> - <GROUP> B <ACTIVE>
HOME            <00> - <GROUP> B <ACTIVE>
```

MAC Address = 00-00-00-00-00-00

The equivalent command to examine the name cache on the Vista PC is “nbtstat”.

3 Users

The Windows PC is configured with users “Catherine” and “tony”, and the Ubuntu PC is configured with both a Linux user “tony” and a Samba user “tony”. User “tony’s” password is the same on both PCs.

Both machines are members of workgroup “HOME”.

Samba on the Ubuntu machine is set up for “user” sharing i.e. authentication is carried out on a per username / password basis every time someone attempts to access the share.

For “user sharing” to work in Samba on Linux it is necessary to configure both a Linux user and a corresponding Samba user. The Linux user is added in the usual way and the Samba user is added with the command:

```
smbpasswd -a tony
Password: <string>
Confirm: <string>
```

The “pdbedit” command is used to list the entries contained in the Samba user password database. It is NOT possible to add a Samba user unless a Linux user already exists.

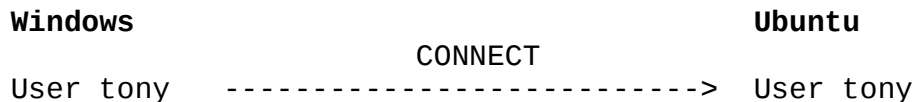
```
root@tony-laptop:~# pdbedit -L
```

```
tony:1000:tony
```

4 Accessing the Shares

4.1 Windows to Ubuntu (same user on both machines)

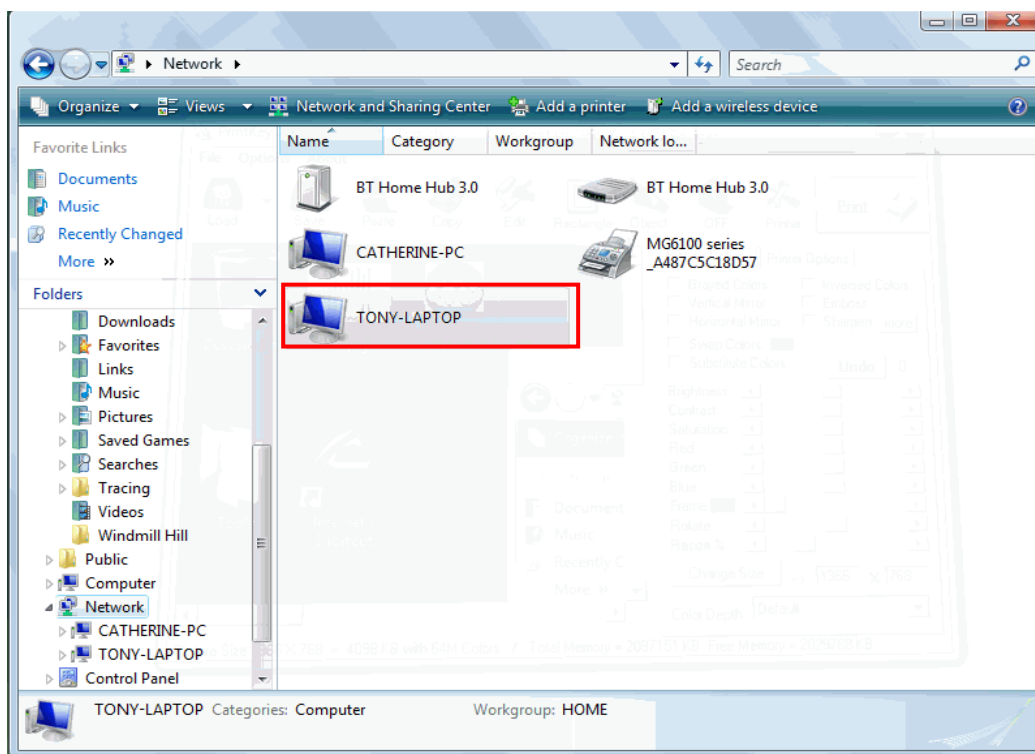
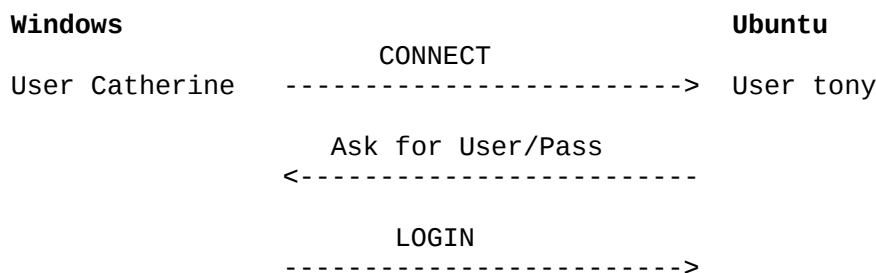
Log in to the Vista PC with user "tony". Open Windows file explorer and click on Network. Double click on TONY-LAPTOP followed by "tony-share".



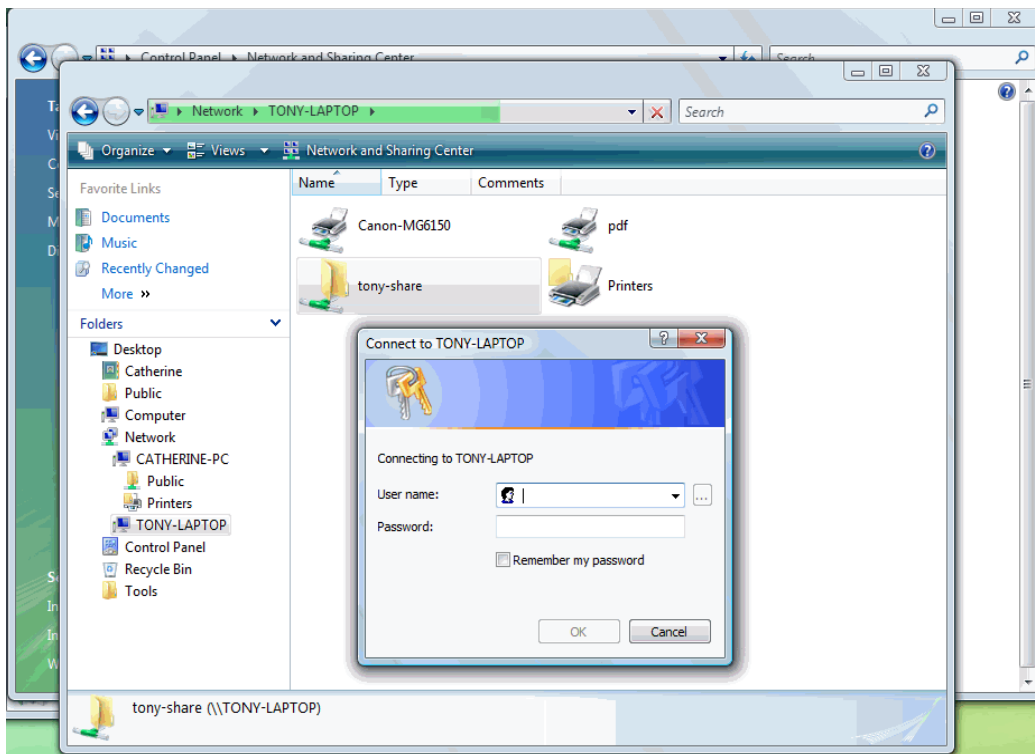
The share is accessed successfully. The Ubuntu PC does not prompt for a username and password because the user authentication information is the same on both machines. The Vista PC passes its authentication information to the Ubuntu PC in the SMB connection request.

4.2 Windows to Ubuntu (different users on each machine)

Log in to the Vista PC with user "Catherine". Open Windows file explorer and click on Network. Double click on TONY-LAPTOP followed by "tony-share2".

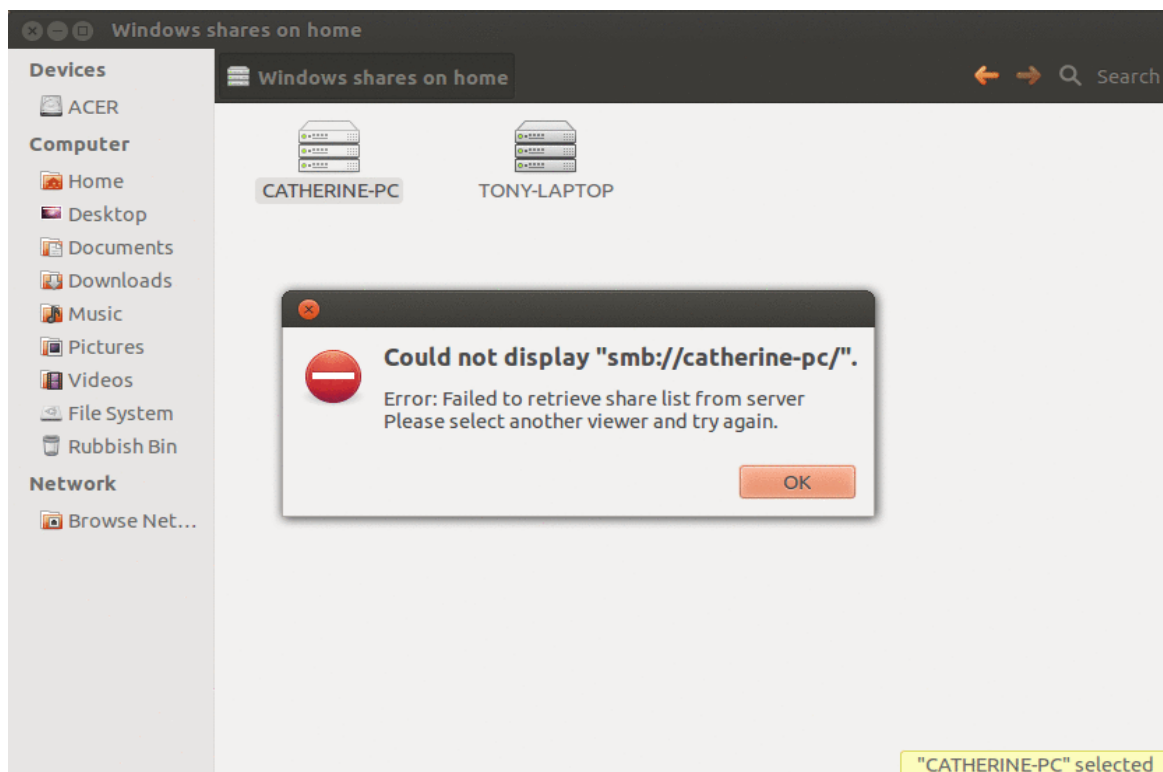


The Ubuntu PC presents Catherine with a username and password prompt. Catherine logs into the Samba PC's share successfully.



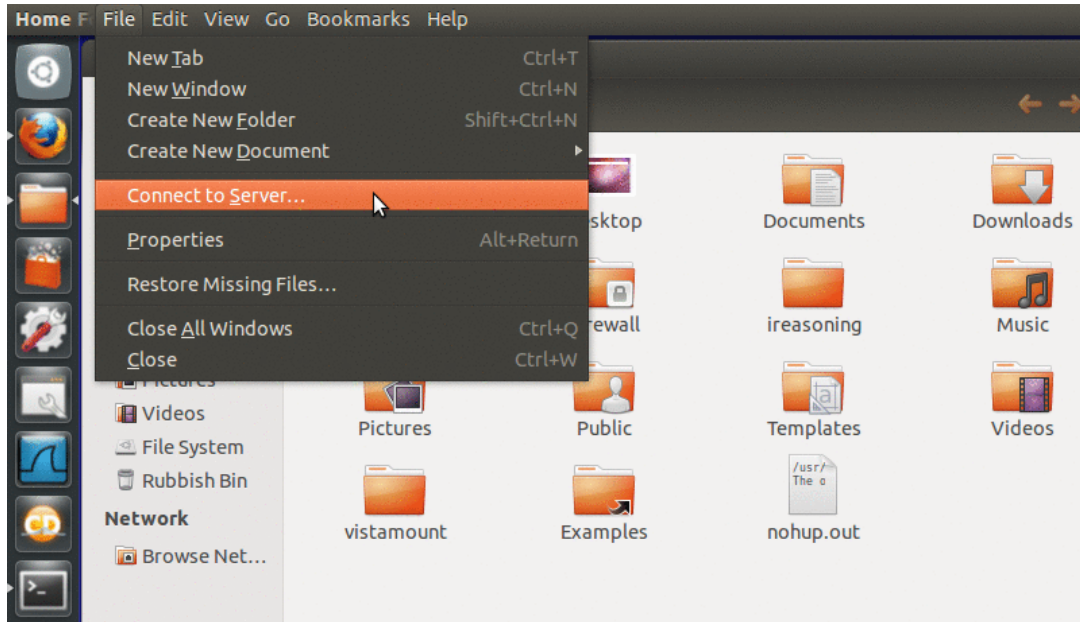
4.3 Ubuntu to Windows (same user on both machines)

Log in to the Ubuntu PC with user "tony". Open Nautilus file explorer and select Browse Network. Double click on workgroup HOME to see the devices it contains. Double click on CATHERINE-PC. The following error message is displayed.

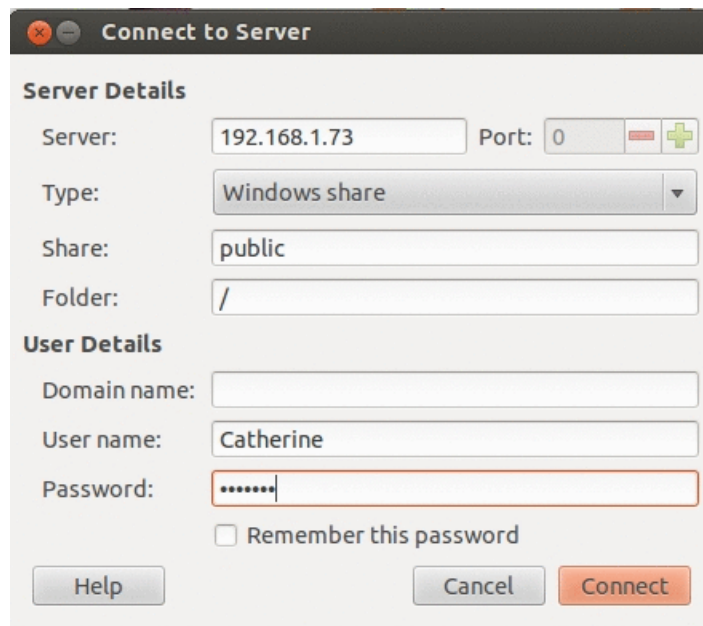


Unlike Windows file explorer, Nautilus does not support automatic connection to devices by double clicking them. Nautilus provides a different mechanism to access remote shares.

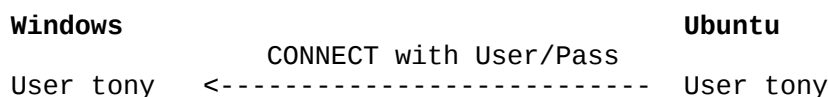
Select File → Connect to Server from the top menu bar.

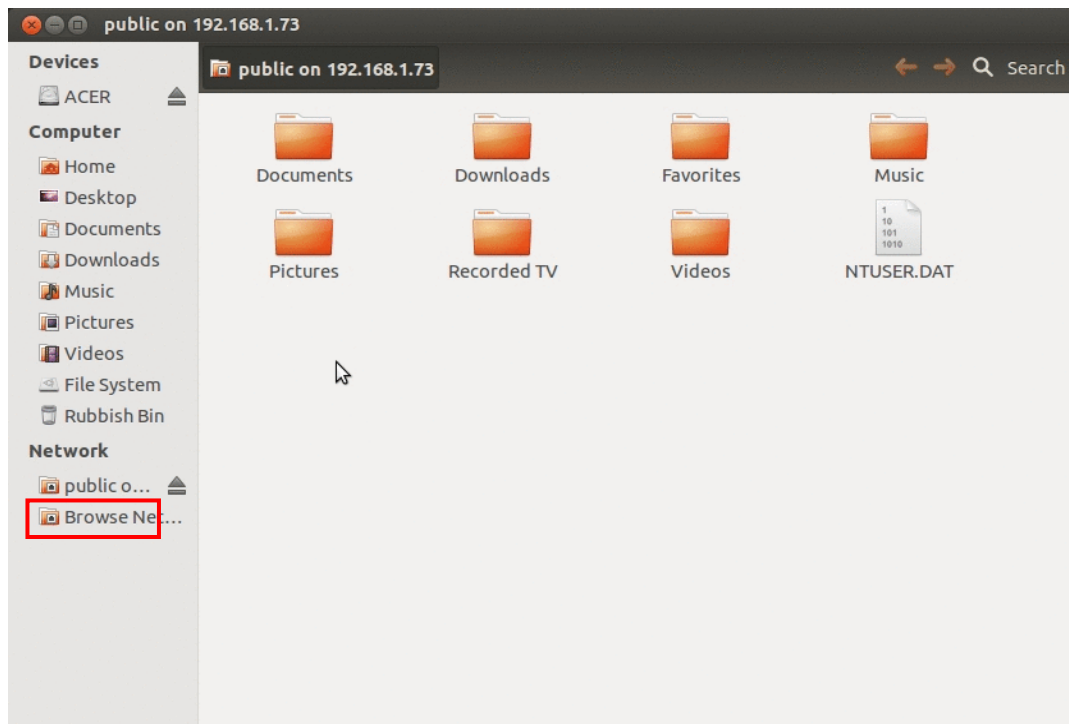


Enter the IP address of the target machine, the connection Type (Windows Share), the share name (public), the Vista username and password. Leave the Folder as "/" and the Domain field blank. Click Connect.



The connection is successful because the Vista username and password have been provided. It is now possible to browse the Vista PC's share.

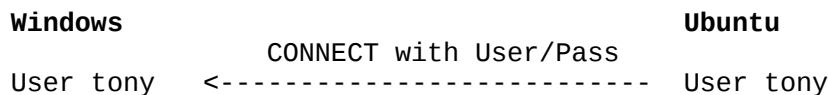




For security reasons, Windows rejects connections unless explicit login credentials are provided, even if the user and login credentials are the same on both machines.

4.4 Ubuntu to Windows (different users on each machine)

This is exactly the same as Scenario 3.3 because the Vista PC's username and password are provided at connection time using the Nautilus "Connect to Server" mechanism.



Note: The Ubuntu Nautilus GUI may operate differently to file browsers on other Linux machines when connecting to Windows shares. Unlike Windows file explorer, Nautilus does NOT open a browser window when you double click on the Windows machine's icon. You must use the File → Connect to Server mechanism to browse the Windows share.

4.5 Firewall Configuration

The Nautilus GUI directs the Ubuntu PC to use the Vista PC's IP address to connect to the Vista share. The first thing the Ubuntu PC does is to negotiate with the Vista PC the protocol to use. By default, the Vista PC is configured to use NETBIOS over TCP so it tells the Ubuntu PC to use SMB over NETBIOS over TCP port 445 to access the share.

A similar negotiation takes place when the Vista PC connects to the Ubuntu PC's share. However, the connection is initiated in a different way. It is instigated by double clicking on the Ubuntu PC's icon in the Vista PC's file explorer. The Vista PC resolves the Ubuntu PC's name to IP address mapping and establishes an initial connection to the IP address using SMB over NETBIOS over TCP port 139. The

Vista PC then negotiates with the Ubuntu PC the protocol it should use to access the Ubuntu PC's share. By default the Vista PC is configured to use NETBIOS over TCP so the protocol is negotiated to be SMB over NETBIOS over TCP port 445.

Efficiencies can be gained by disabling NETBIOS over TCP to allow SMB to run direct over TCP. Disabling NETBIOS reduces both the packet header overhead and the amount of broadcast traffic on the LAN segment. To disable NETBIOS over TCP, open Control Panel and select the LAN adapter. Right click on the adapter and select Properties. Scroll down to and select Internet Protocol Version 4, click Properties and Advanced. Select the WINS tab and tick the box "Disable NetBIOS over TCP/IP".

Beware! Disabling NETBIOS over TCP has a downside because the NETBIOS name resolution and browser service mechanisms will no longer function so it won't be possible to connect to network shares by browsing the Windows network neighbourhood and clicking on devices. If you disable NETBIOS over TCP you must either use DNS or Active Directory (AD) to map IP addresses to file, folder and printer locations. Alternatively, you can connect to the remote machine's resources manually using the explicit Uniform Naming Convention (UNC) method, which is similar to the way that Nautilus does things. UNCs are described briefly in Section 4.7 below.

It is vital that the firewalls on both PCs permit the relevant protocols and ports to allow successful completion of name resolution, browser service and session establishment. The firewall rules below show how IPTABLES is configured on the Ubuntu PC to support all of the functionality required.

NETBIOS Name Service:

```
iptables -A INPUT -i eth0 -p udp --dport 137 -s 192.168.1.0/24 -j ACCEPT
```

NETBIOS Datagram Service:

```
iptables -A INPUT -i eth0 -p udp --dport 138 -s 192.168.1.0/24 -j ACCEPT
```

NETBIOS Session Service:

```
iptables -A INPUT -i eth0 -p tcp --dport 139 -s 192.168.1.0/24 -j ACCEPT
```

Microsoft Directory Service:

```
iptables -A INPUT -i eth0 -p tcp --dport 445 -s 192.168.1.0/24 -j ACCEPT
```

4.6 Mounting Windows Shares in Ubuntu

It is possible to mount Windows shares manually on the Ubuntu PC by specifying the Vista username and password in the mount command:

```
mkdir /home/tony/vistamount
```

```
mount -t cifs -o username=Catherine,password=<password>  
//192.168.1.73/public /home/tony/vistamount
```

4.7 Browsing the Windows Share with Firefox

To browse Windows shares using Firefox or another web browser it is necessary to either disable Password Protected sharing on the Vista PC or to specify a username and password in the browser's URL box.

Enter the following URL into Firefox to browse the Vista PC shares with Password Protected sharing disabled:

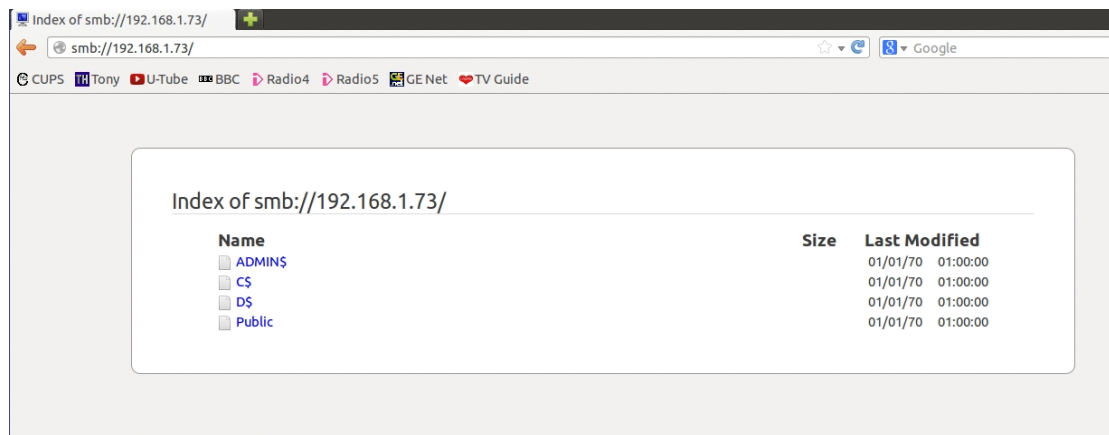
smb://192.168.1.73/

Enter the following URL into Firefox to browse the Vista PC shares with Password Protected sharing enabled:

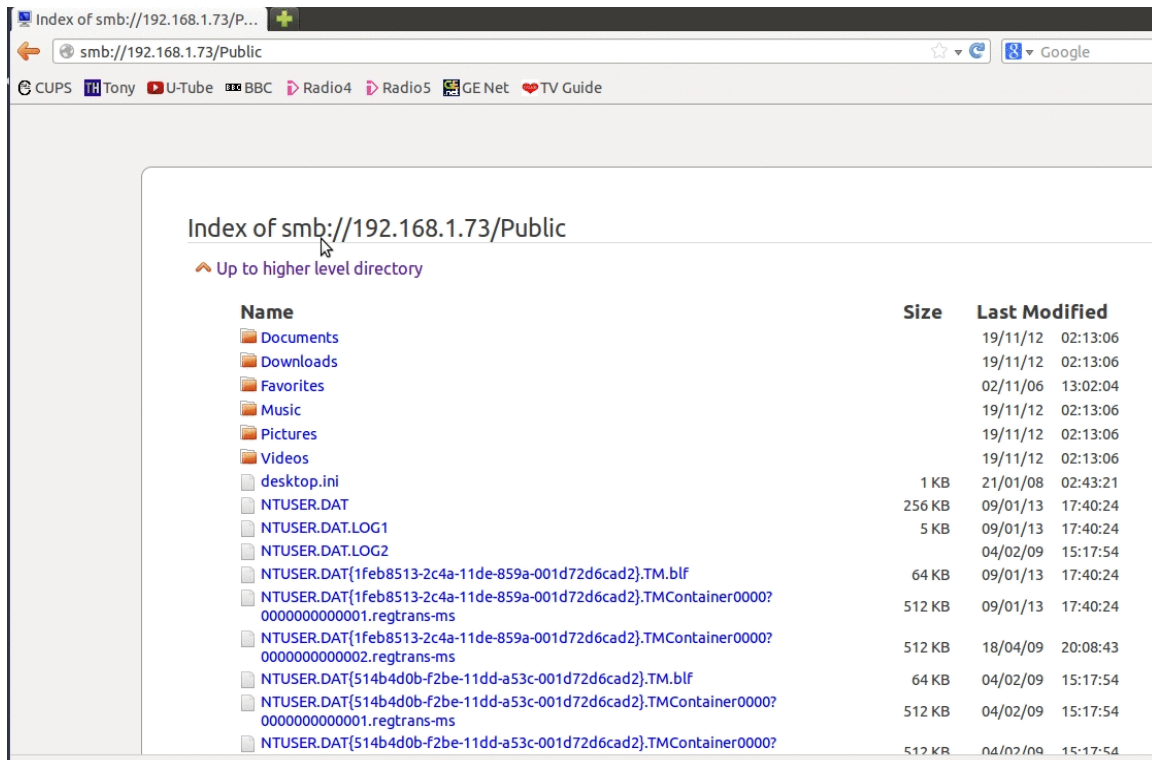
smb://<username>:<password>@192.168.1.73/

Please Note: The above strings are sometimes referred to as UNC's (Uniform Naming Convention) rather than URLs.

Thee UNC's retrieve a list of the IPC\$ indexes for the Windows shares on the Vista PC.



Click on the share to which you have access rights and browse the directories and files within it. In this case the share is "Public".



4.8 Share Access Packet Capture

The packet capture below shows the Ubuntu PC requesting a connection to the “public” share on the Vista PC in workgroup “HOME”.

The Ubuntu PC requests access to the “PUBLIC” share on the Vista PC using “Catherine’s” authentication credentials. It follows this with a request for the share’s file system attribute information (read / write etc.) and a list of the files and folders that the share contains.

192.168.1.66	192.168.1.73	SMB	492	Session Setup AndX Request, NTLMSSP_AUTH, User: HOME\Catherine
192.168.1.73	192.168.1.66	SMB	298	Session Setup AndX Response
192.168.1.66	192.168.1.73	SMB	164	Tree Connect AndX Request, Path: \\192.168.1.73\PUBLIC
192.168.1.73	192.168.1.66	SMB	132	Tree Connect AndX Response
192.168.1.66	192.168.1.73	SMB	142	Trans2 Request, QUERY_FS_INFO, Query FS Attribute Info
192.168.1.73	192.168.1.66	SMB	146	Trans2 Response, QUERY_FS_INFO
192.168.1.66	192.168.1.73	SMB	146	Trans2 Request, QUERY_PATH_INFO, Query File All Info, Path:
192.168.1.73	192.168.1.66	SMB	228	Trans2 Response, QUERY_PATH_INFO

The Vista PC returns the share’s content and the Ubuntu PC requests further information on each of the files and directories within the share.

192.168.1.66	192.168.1.73	SMB	170	Trans2 Request, QUERY_PATH_INFO, Query File All Info, Path: \desktop.ini
192.168.1.73	192.168.1.66	SMB	252	Trans2 Response, QUERY_PATH_INFO
192.168.1.66	192.168.1.73	SMB	166	Trans2 Request, QUERY_PATH_INFO, Query File All Info, Path: \Documents
192.168.1.73	192.168.1.66	SMB	248	Trans2 Response, QUERY_PATH_INFO
192.168.1.66	192.168.1.73	SMB	166	Trans2 Request, QUERY_PATH_INFO, Query File All Info, Path: \Downloads
192.168.1.73	192.168.1.66	SMB	248	Trans2 Response, QUERY_PATH_INFO
192.168.1.66	192.168.1.73	SMB	166	Trans2 Request, QUERY_PATH_INFO, Query File All Info, Path: \Favorites
192.168.1.73	192.168.1.66	SMB	248	Trans2 Response, QUERY_PATH_INFO
192.168.1.66	192.168.1.73	SMB	158	Trans2 Request, QUERY_PATH_INFO, Query File All Info, Path: \Music

----- This ends the Samba How To -----