Mounting your Physics home directory using SSH
for Windows 10

Introduction

This tutorial contains screenshots for the English version of Windows 10.

To be able to mount a Windows share over SSH we will need

- Administrator access to the local computer, including the ability to *elevate* privileges. If you don't know what I am talking about then stop reading right here.
- Tunnelier, which is an excellent and free implementation of SSH for Windows. It is assumed that you are familiar with the Tunnelier user interface.
- One real or virtual network adapter, bound to the *Client for Microsoft Networks* driver. Normally you should already have such an adapter, as otherwise you would not be able to mount any Windows shares.
- One real or virtual network adapter, **NOT** bound to the *Client for Microsoft Networks* driver.

Note that this is slightly different from the requirements for Windows 2000/XP, as with Vista/7 a different protocol driver (`SMB`) is used compared to the older versions of Windows (`Netbios over TCP/IP` or `CIFS`).

This part of the tutorial is split into the following steps:

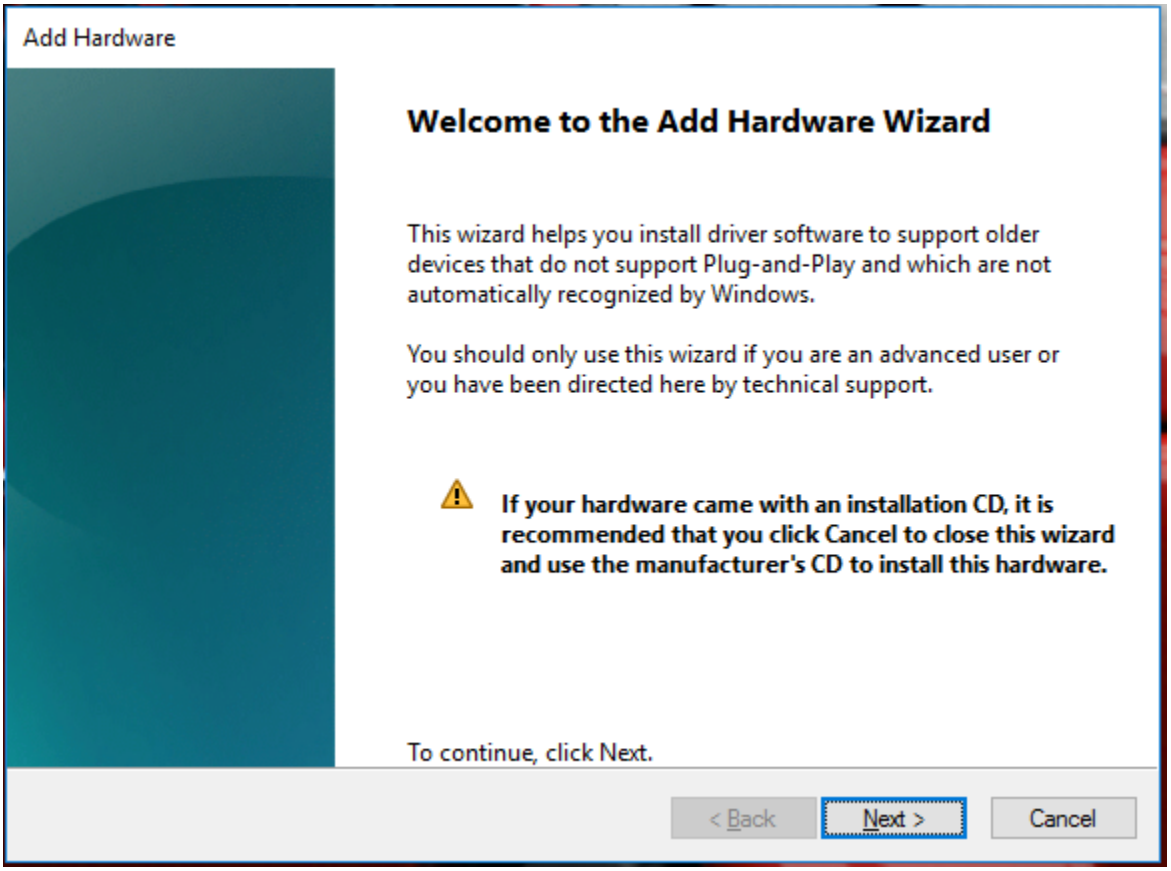
1. As most people do not have a spare real network adapter in their computer, we will add an extra virtual network adapter by installing the **Microsoft Loopback Adapter**.
2. After that, the network adapter must be properly configured.
3. Furthermore, a Windows system driver needs to be tweaked.
4. And we need to create a Task for the Windows Task Scheduler.
5. Reboot Windows and verify that all changes were applied successfully.
6. Then we set up a special Tunnelier session with the right port-forwarding.
7. Finally, we start Tunnelier and mount our Physics home directory.
8. For those wishing to undo the above steps follow the instructions at the bottom of this tutorial.

Installing the Loopback Adapter

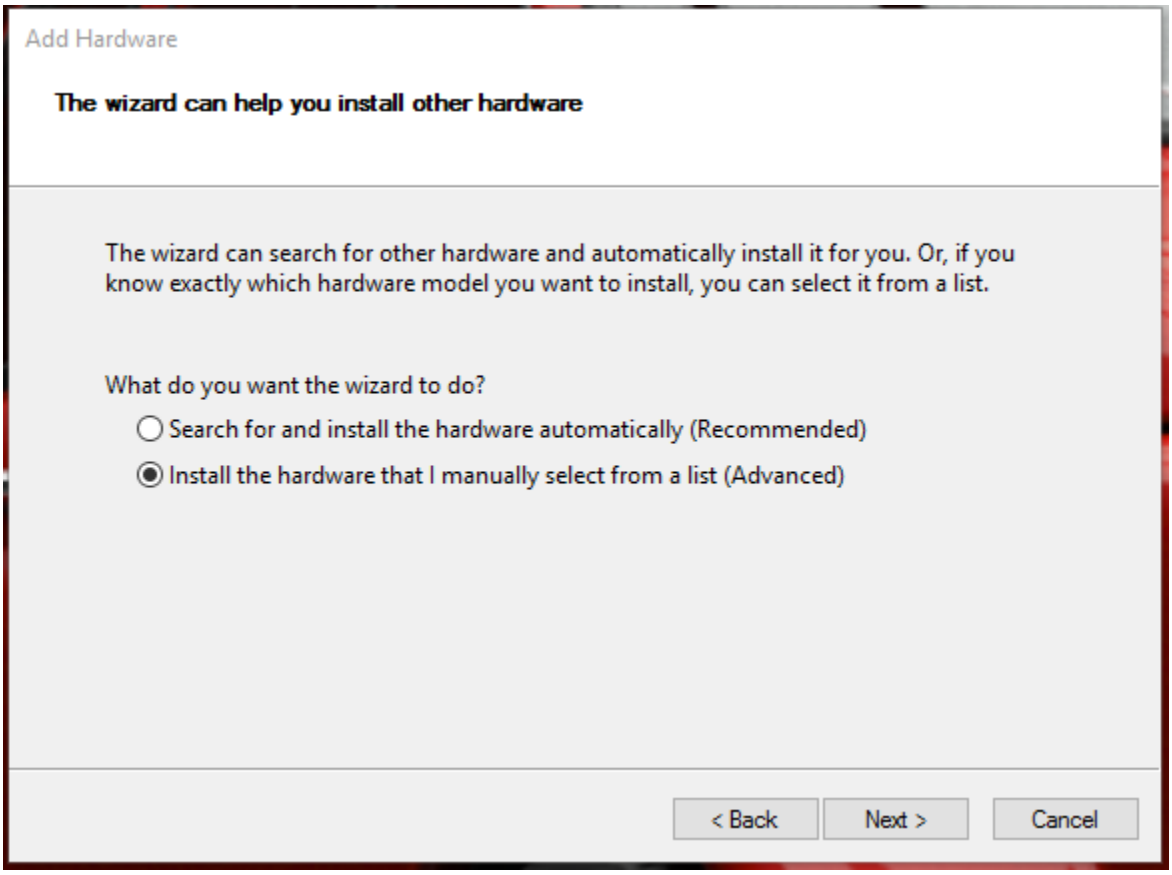
To install the Loopback adapter follow these steps:

- Start the **Add Hardware Wizard** by either going **Start->Settings->Control Panel->Add Hardware** or by starting a console window with elevated (Administrator) privileges. In the console window type
- `hdwwiz.exe`

  The Hardware Wizard will come up:

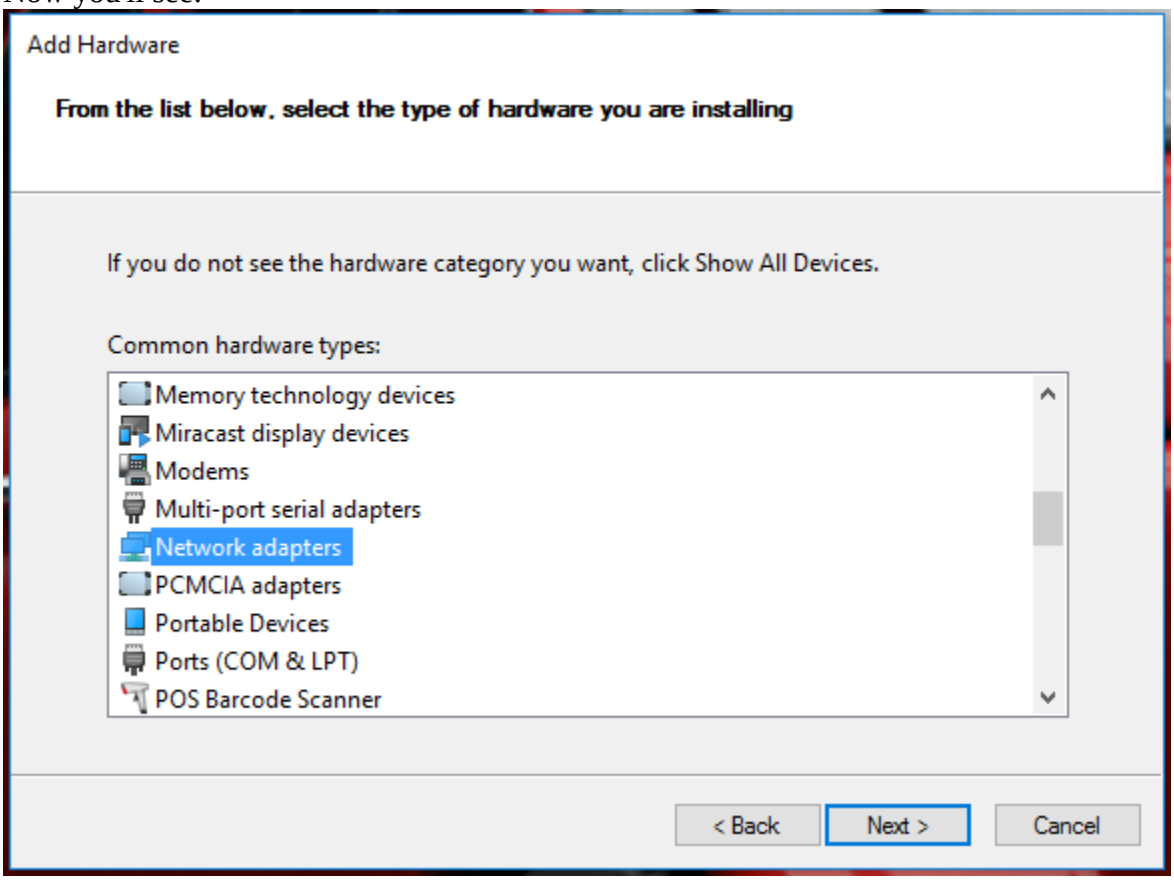


- Click **Next** to continue:



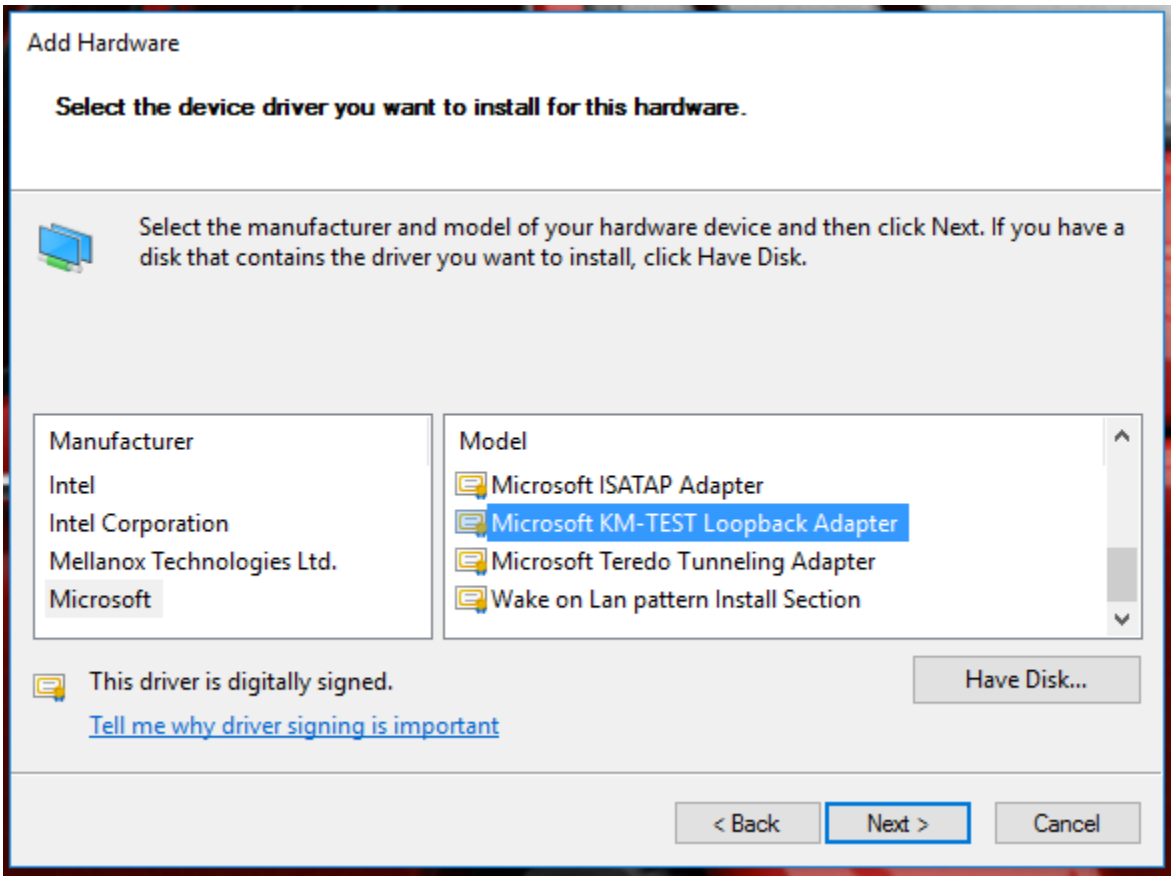
Select **Install the hardware that I manually select from a list** and click **Next**.

- Now you'll see:



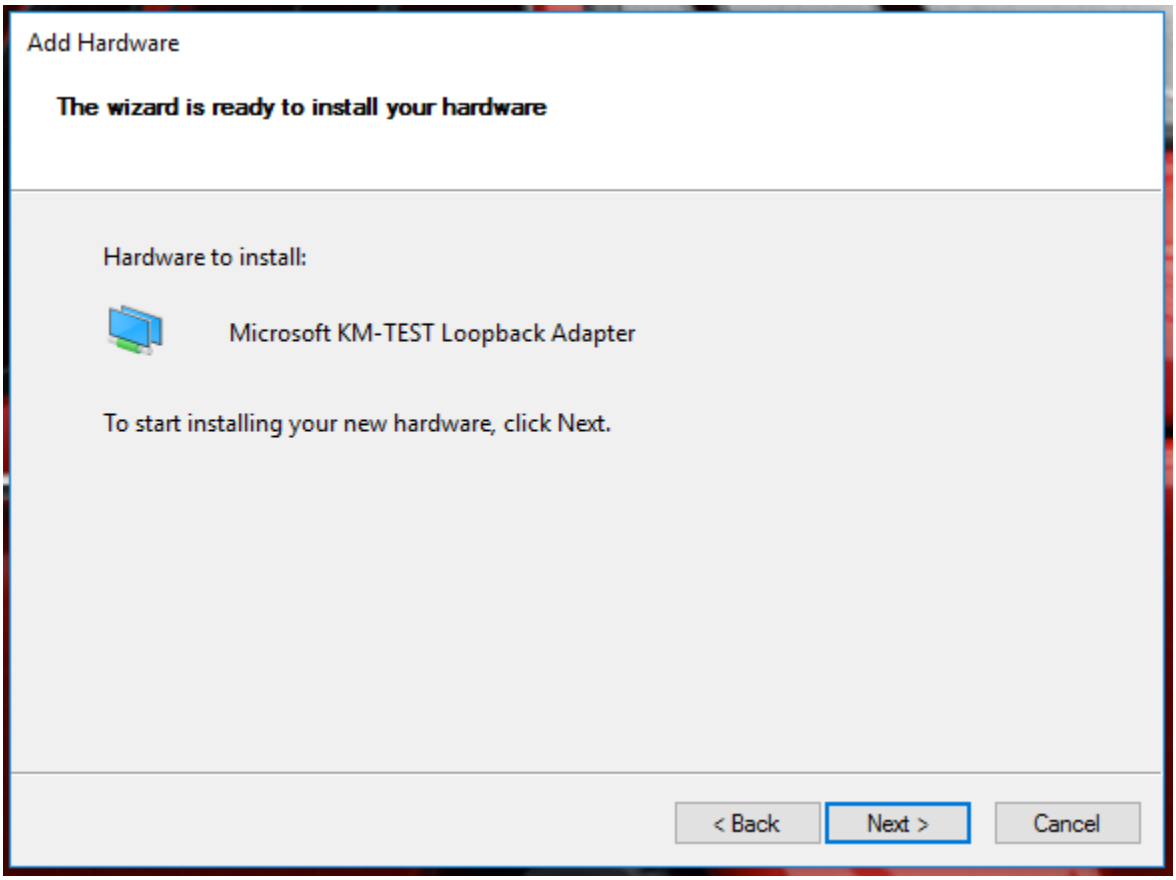
Select the entry **Network adapters** and click **Next**.

- In the next screen



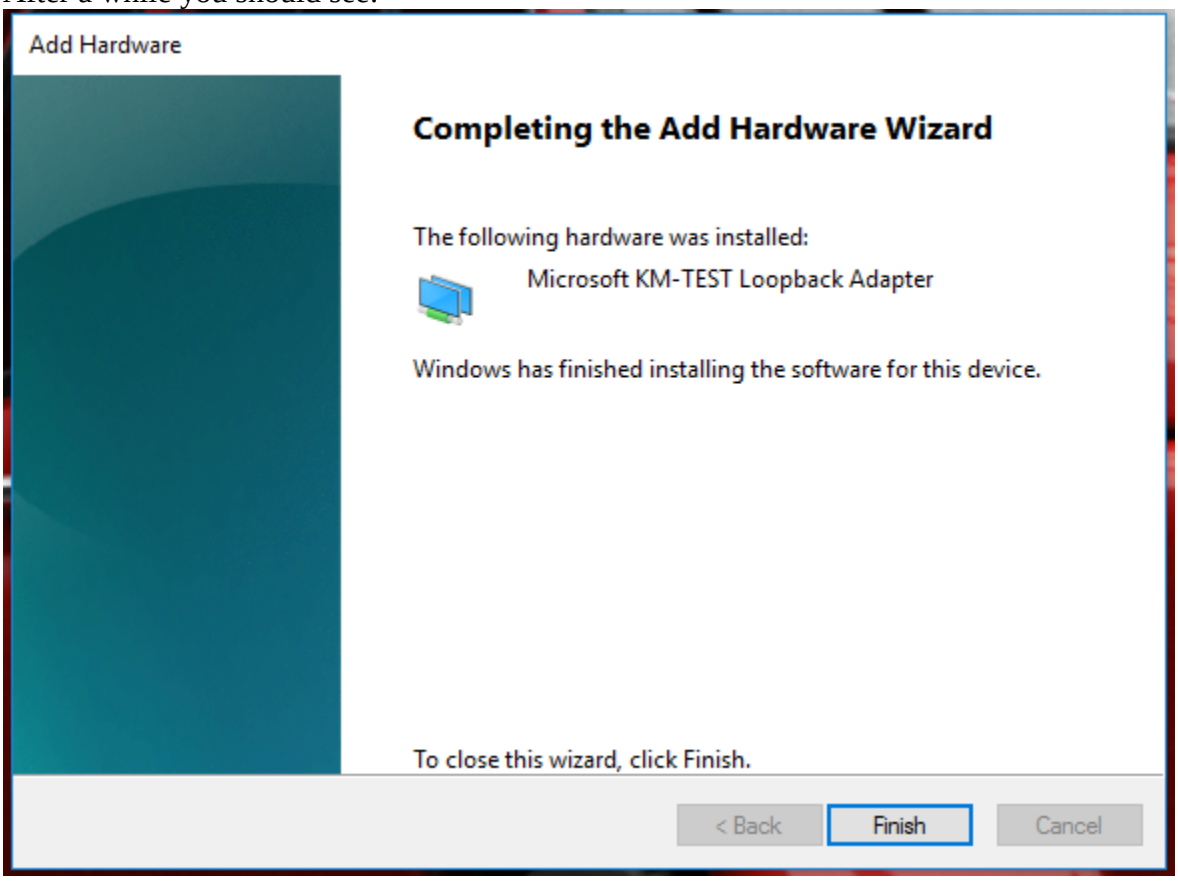
first select **Microsoft** from the list of *Manufacturers* and then select **Microsoft KM-TEST Loopback Adapter** from the list of *Network Adapters*. Finally, click **Next** once more.

- Almost finished:



This is your last chance to abort, otherwise, click **Next**.

- After a while you should see:

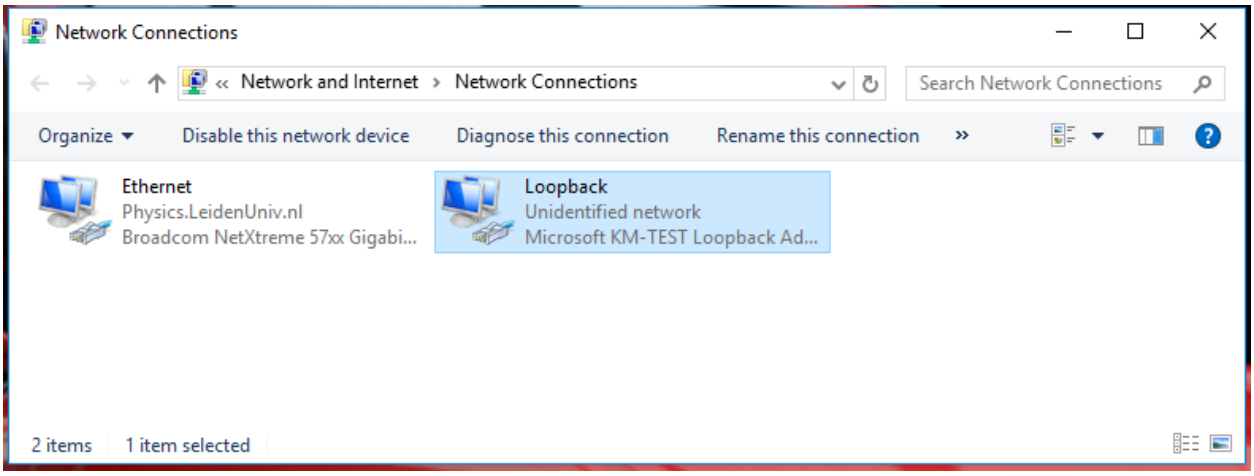


  Click **Finish** to exit the Hardware Wizard.

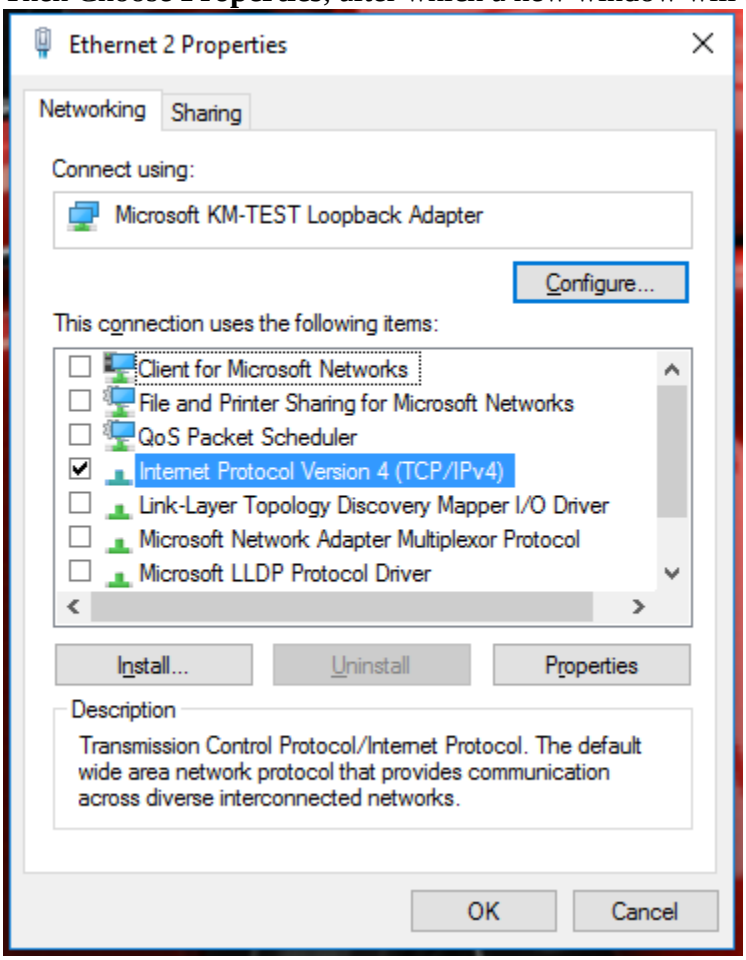
You are now ready to configure your newly installed Loopback adapter. Even though Windows might not ask you to, reboot anyways (heey, it's a Microsoft OS ;-)).
From reports I've seen on the Internet a reboot is sometimes required for the loopback adapter to come up properly.

Configuring the Loopback Adapter

Now that your newly installed loopback adapter is up and running we must configure it properly:

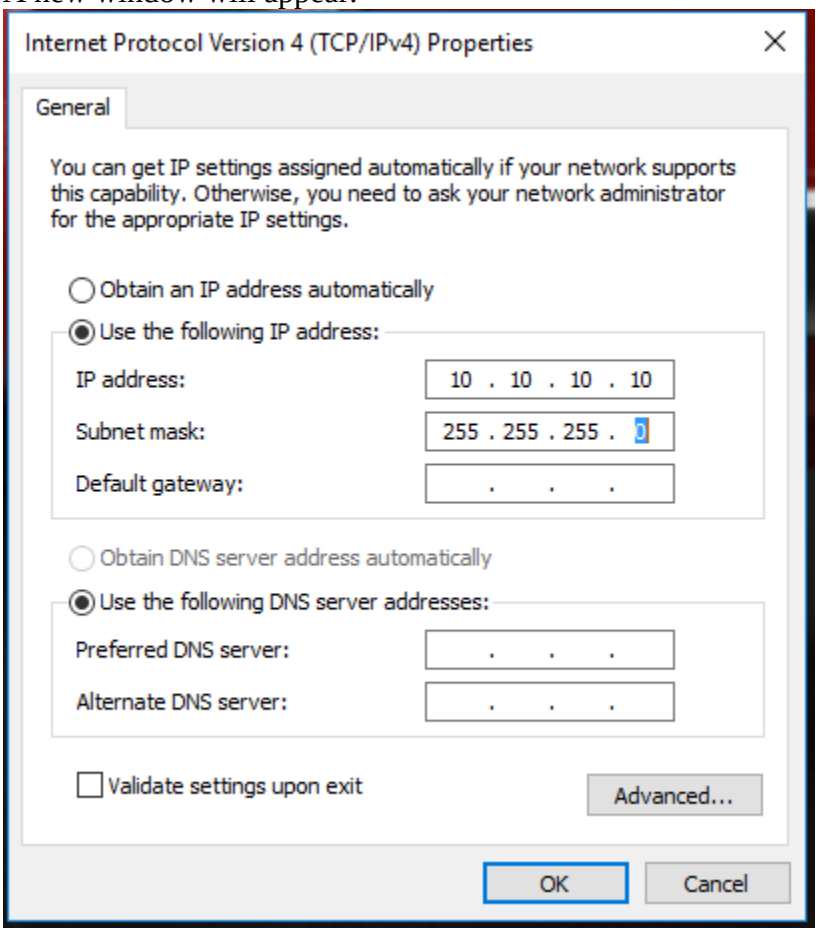
- 

- Choose the loopback adapter (usually it is named "Local Area Connection #3") and right-click on it. Choose **Rename** and type loopback.
- Then Choose **Properties**, after which a new window will appear



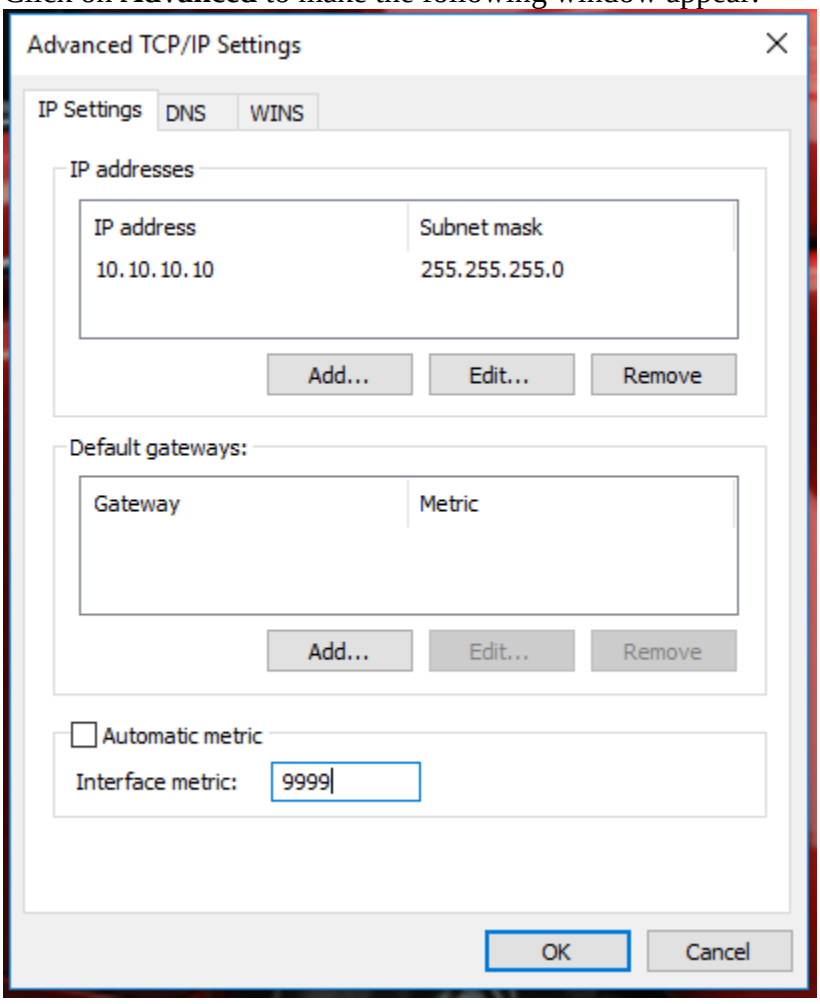
Make sure that
  - Only the entry **Internet Protocol (TCP/IP)** is enabled.
- Select the entry **Internet Protocol (TCP/IP)**, then click on **Properties**.

- A new window will appear:



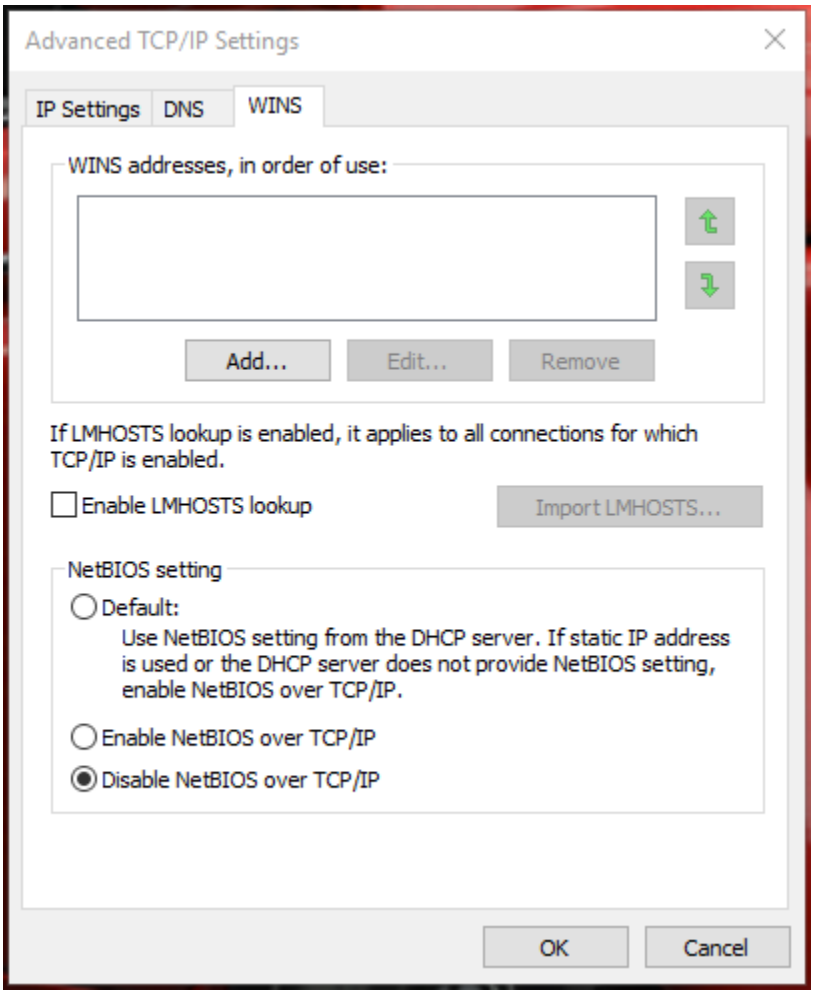
Select **Use the following IP address** and fill in the 'IP address' and 'Subnet mask' as above.
It is not necessary to fill in the 'Default gateway' or a 'DNS server'.

- Click on **Advanced** to make the following window appear:



Deselect **Automatic metric** and fill in the value of **9999** as the 'Interface metric' as shown above.

- Click on the **WINS** tab:

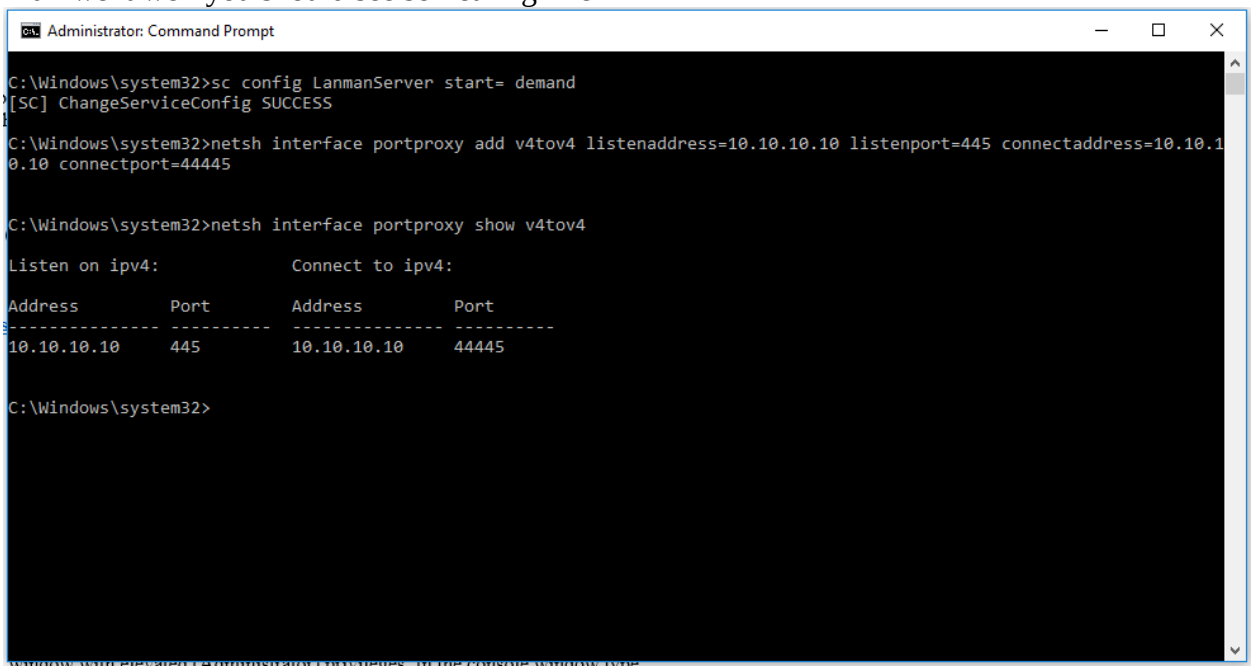


  and select **Disable NetBIOS over TCP/IP**.
- Click on **OK**.
- You are now back in the main 'TCP/IP Properties' screen. Click **OK** again.
- You are now back in the main 'Loopback Properties' screen. Click **Close**.

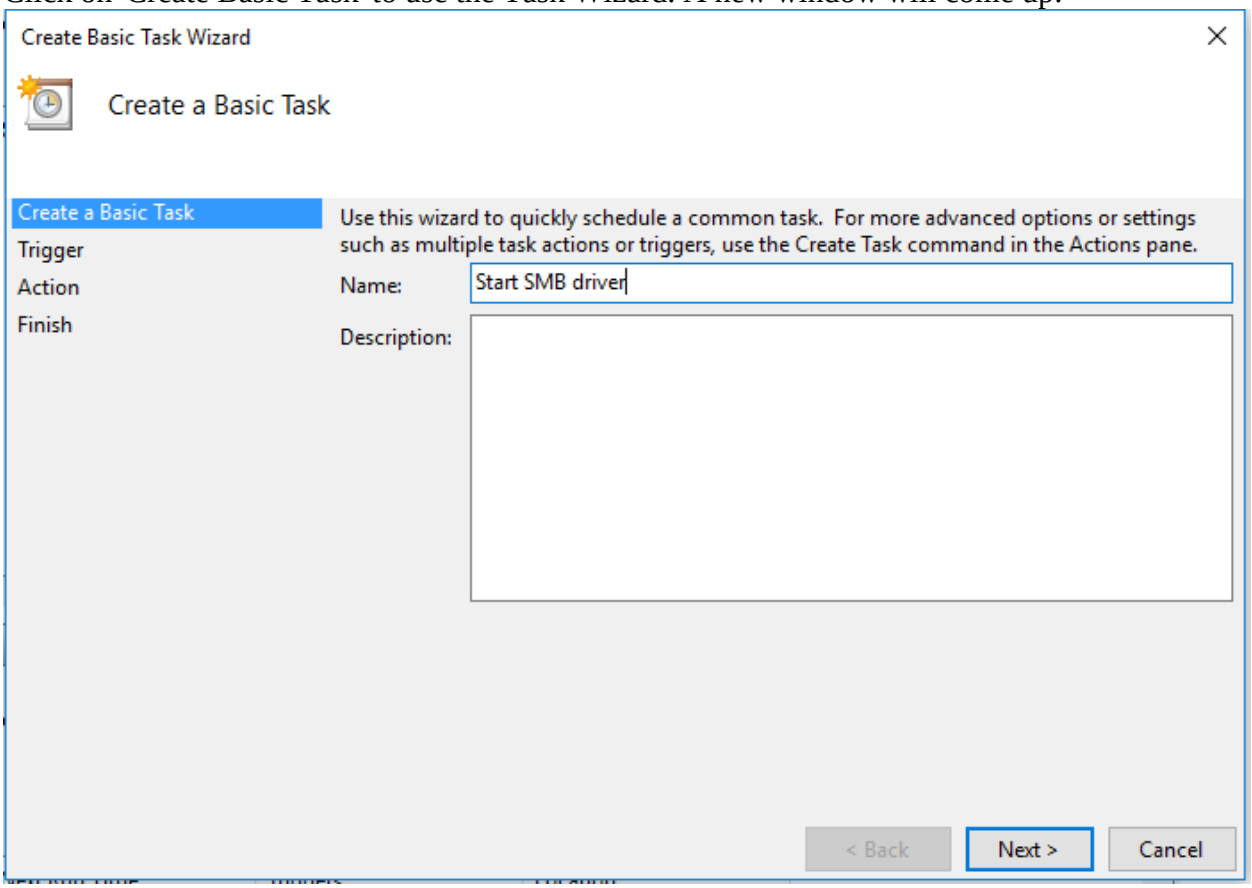
Tweaking the 'SMB' driver

Now we first need to tweak a Windows system driver to overcome the thing that Microsoft broke. The root cause of the problem is that we need to access the file share using TCP port **445**. However, when Windows 10 boots this port is grabbed by the system `smb` driver for all interfaces. By delaying the startup of the `smb` driver and by installing a `portproxy` rule we can circumvent this. This section explains how to do this:

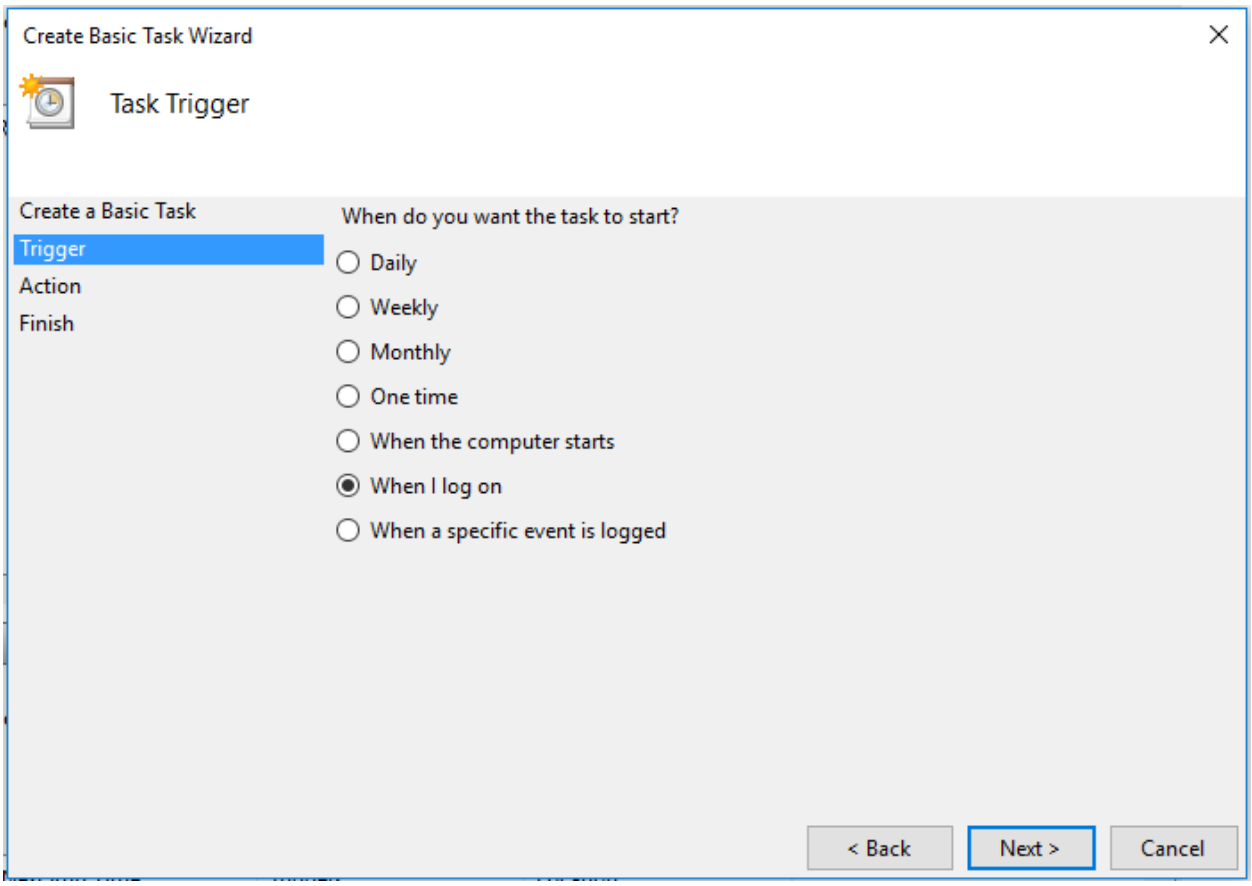
- Start a console window with elevated (Administrator) privileges.
- First, we disable the automatic starting of the `smb` driver:
- ```
  sc config LanmanServer start= demand
  ```

  NOTE the space after the `start=` !
  ```

- Next we add a `portproxy` rule to reroute TCP port 445 to a port of our choosing. For this tutorial, I choose **44445**:
- ```
  netsh interface portproxy add v4tov4 listenaddress=10.10.10.10 listenport=445 connectaddress=10.10.10.10 connectport=44445
  ```

  IMPORTANT NOTES:

  - The `listenaddress` is the address of the Loopback adapter configured in the section earlier
  - The `connectaddress` must be identical to the `listenaddress`
  - Using `listenaddress=127.0.0.1` does not work. Believe me, I've tried.

  If all went well you should see something like



  The `portproxy` rule is persisent , so there should be no need to repeat this step after a reboot.

Creating a task to start the 'SMB' driver

Of course, now that we have disabled the automatic startup of the 'SMB' driver we need to start it manually when Windows comes up, or rather, when a user logs in. For this we use the Vista/7 Task Scheduler:

- Start the 'Task Scheduler' from the 'Administrative Tasks' menu:
  ```

- Click on 'Create Basic Task' to use the Task Wizard. A new window will come up:

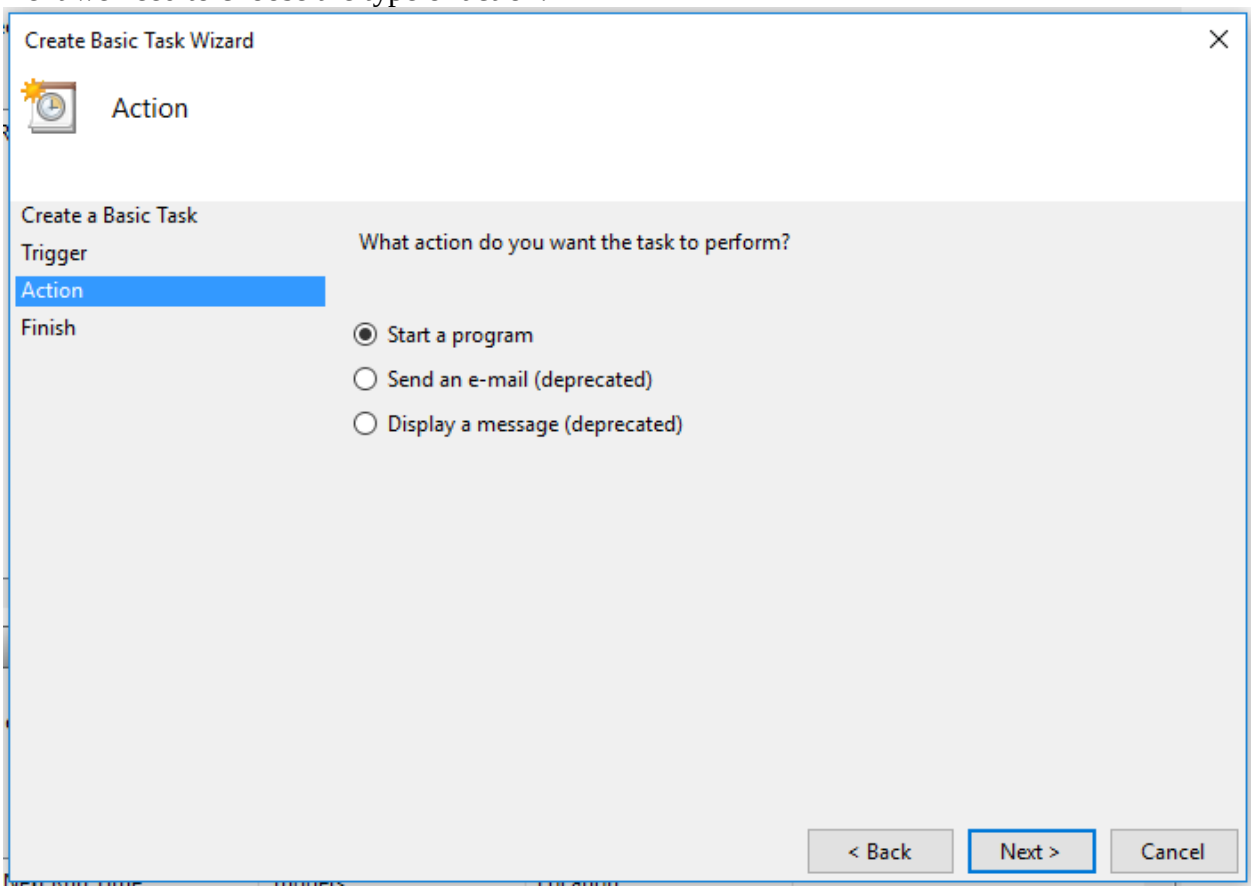


  Enter the name of the task, e.g. **Start SMB driver** and click **Next**.
- Choose an event to trigger the execution of the task. We will change this later on, so for now, choose **When I log in**:



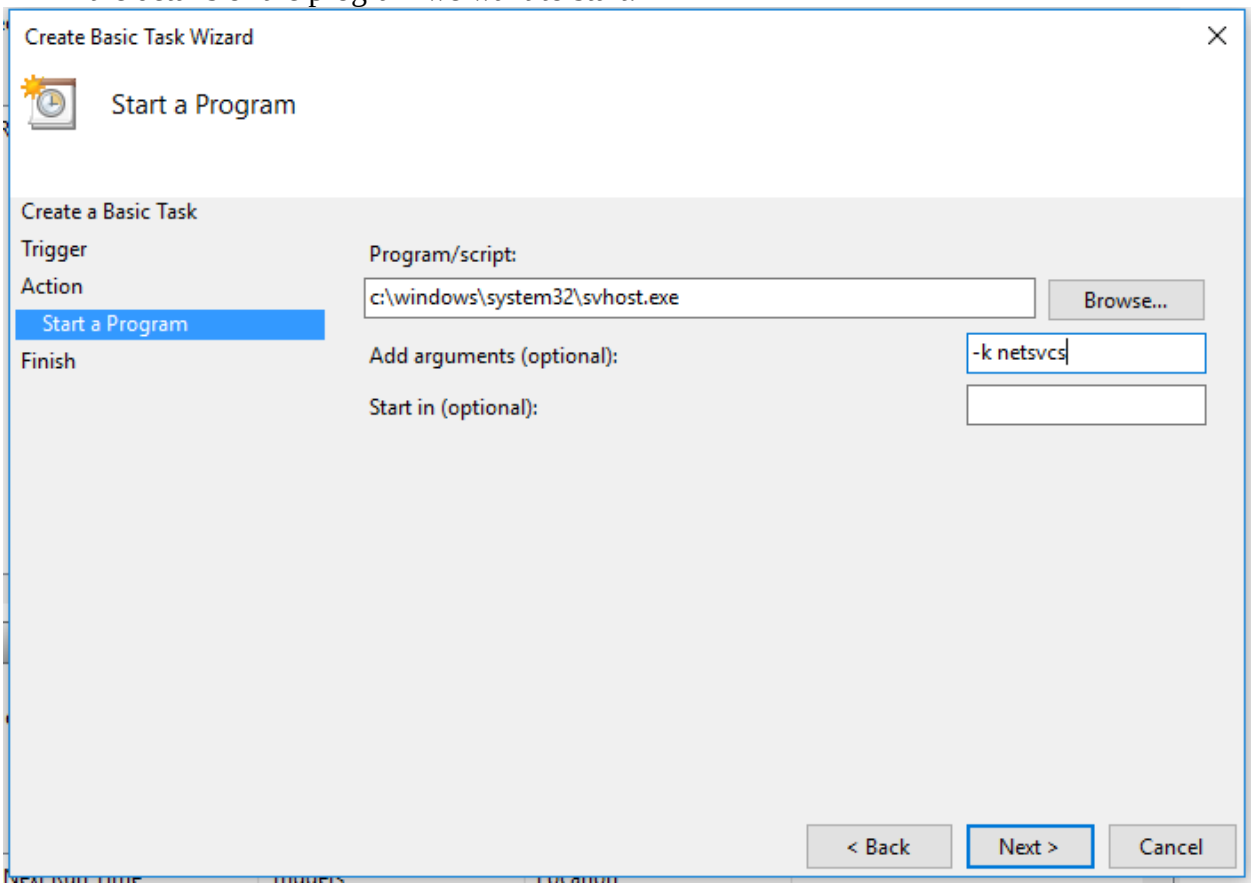
and click **Next**.

- Next we need to choose the type of action:



Select the entry **Start a program** and click **Next**.

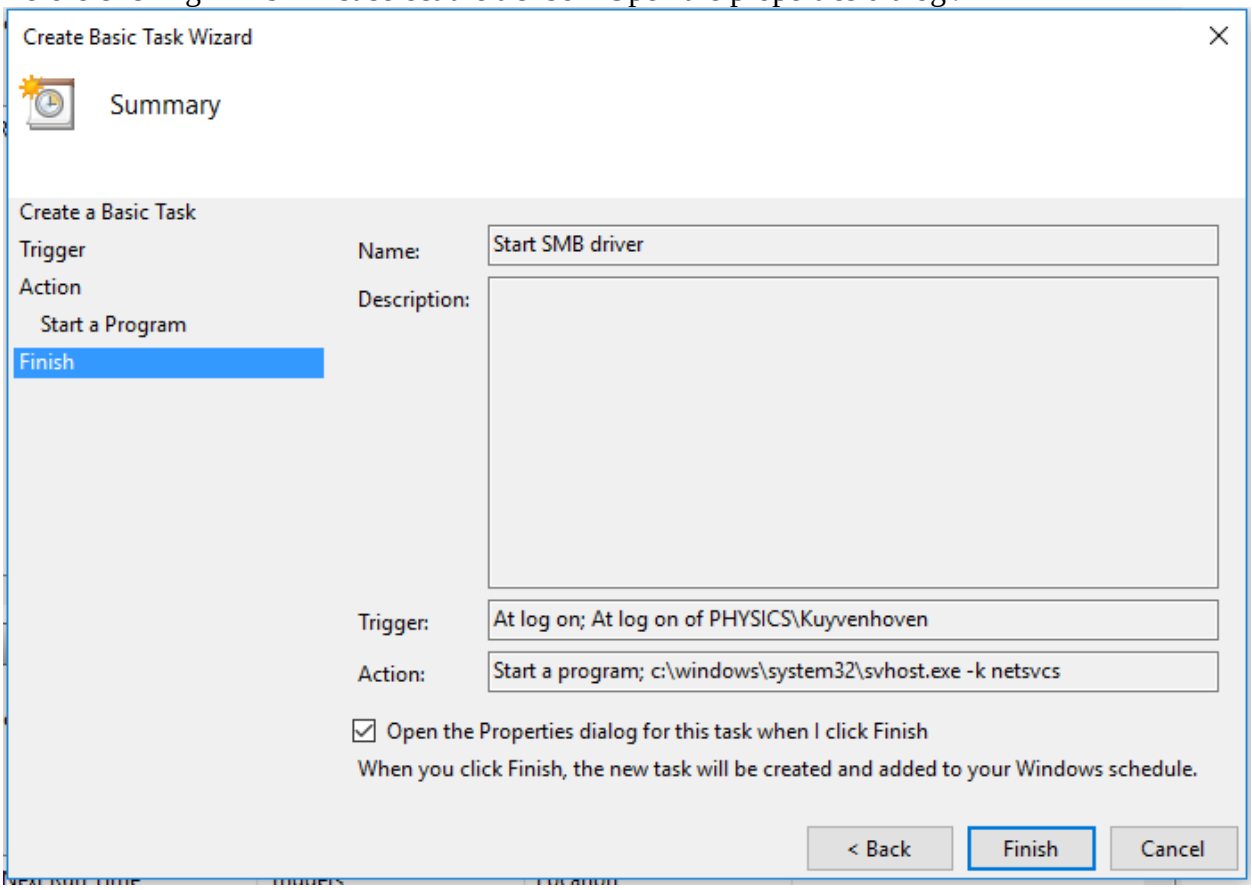
- Fill in the details of the program we want to start:



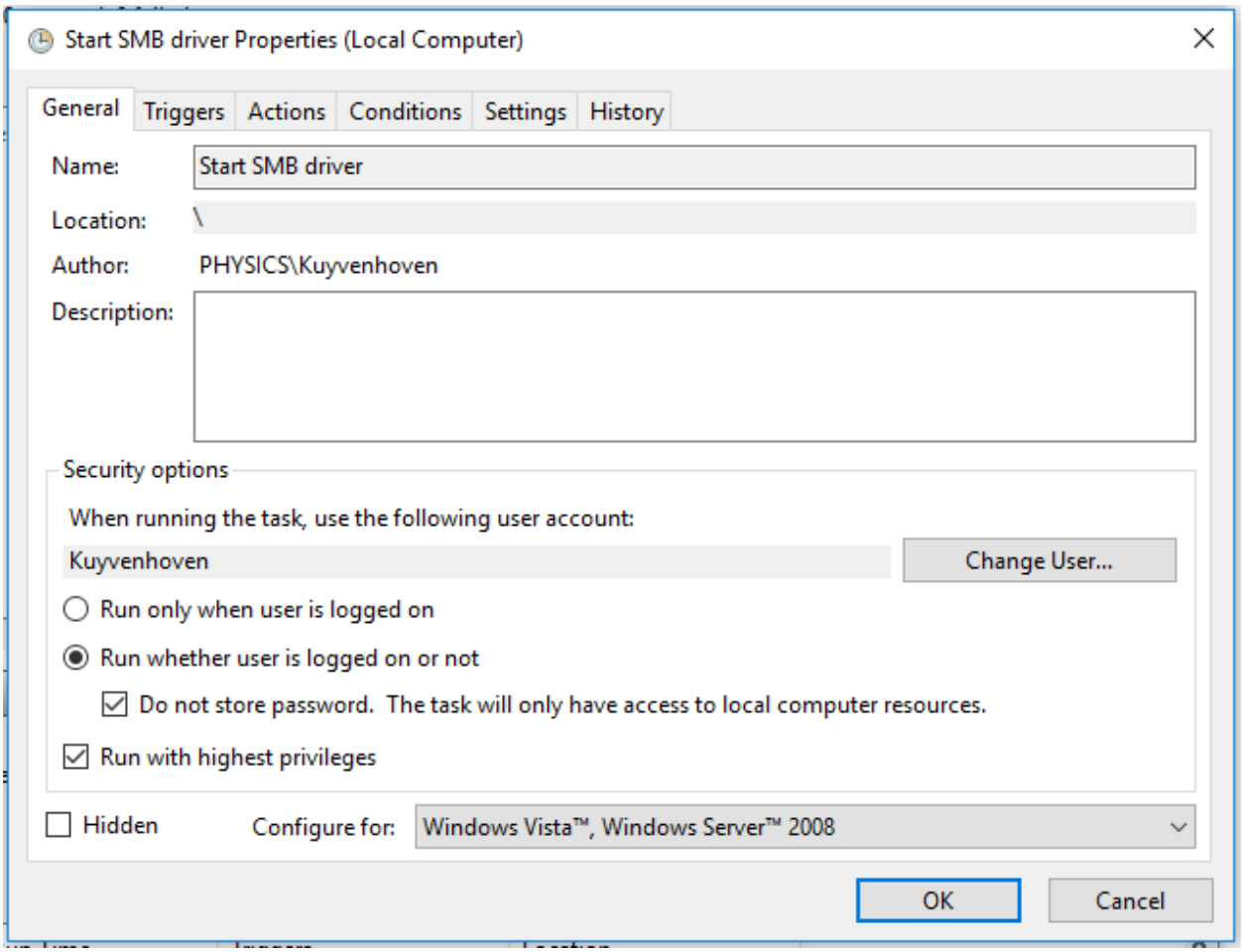
  - The **Program** is '`c:\windows\system32\svhost.exe`'
  - The **Arguments** are '-k netsvcs'

Then click **Next** to continue.

- Before clicking 'Finish' first select the tickbox 'Open the properties dialog':

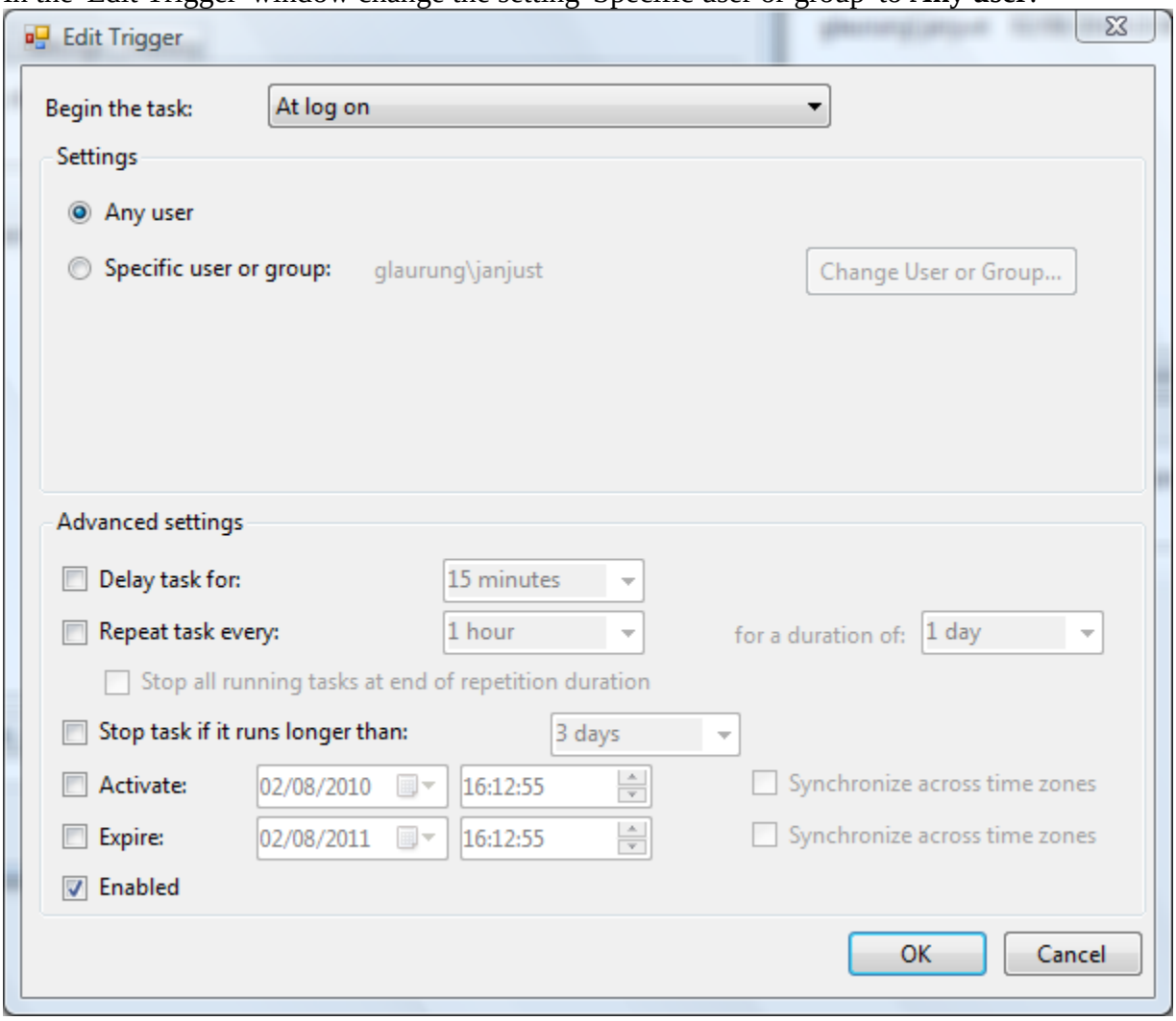


  and then click **Finish**.
- In the 'Task Properties' window select **Run whether user is logged on or not**, then select **Do not store password**. After that, also select the tickbox **Run with highest privileges**:



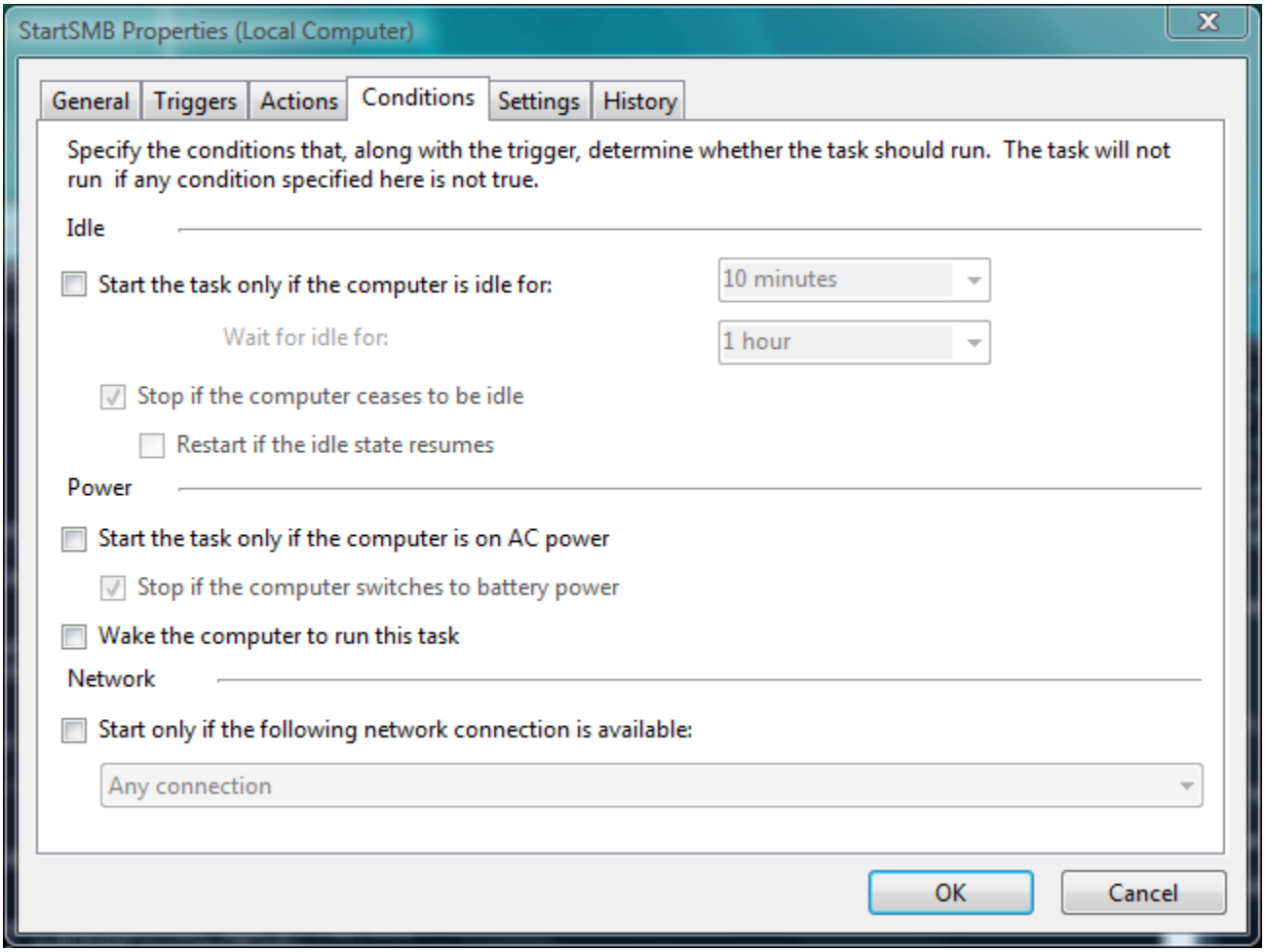
Do **NOT** click 'OK' just yet, but go to the 'Triggers' tab, then double-click the 'At log on' trigger to edit it.

- In the 'Edit Trigger' window change the setting 'Specific user or group' to **Any user**:



then go to the 'Conditions' tab:

- In the 'Conditions' window make sure the setting '**Start the task only if the computer is on AC power**' is **NOT** set:



and then click **OK**.

The task is now configured. Close the Task Scheduler.

Reboot and verify

Of course, now that we have disabled the automatic startup of the 'SMB' driver we have to reboot Windows before proceeding.

- After Windows comes up and you have logged in, check the status of the 'SMB' driver. Open a command console (no privilege elevation is required) and type
- `sc query LanmanServer`

  The SMB driver should be in the state **Running**.

- Verify that the `portproxy` was applied successfully by checking the open ports on the system. Type in the command console
- `netstat -an | find ":445 "`

You should see something like

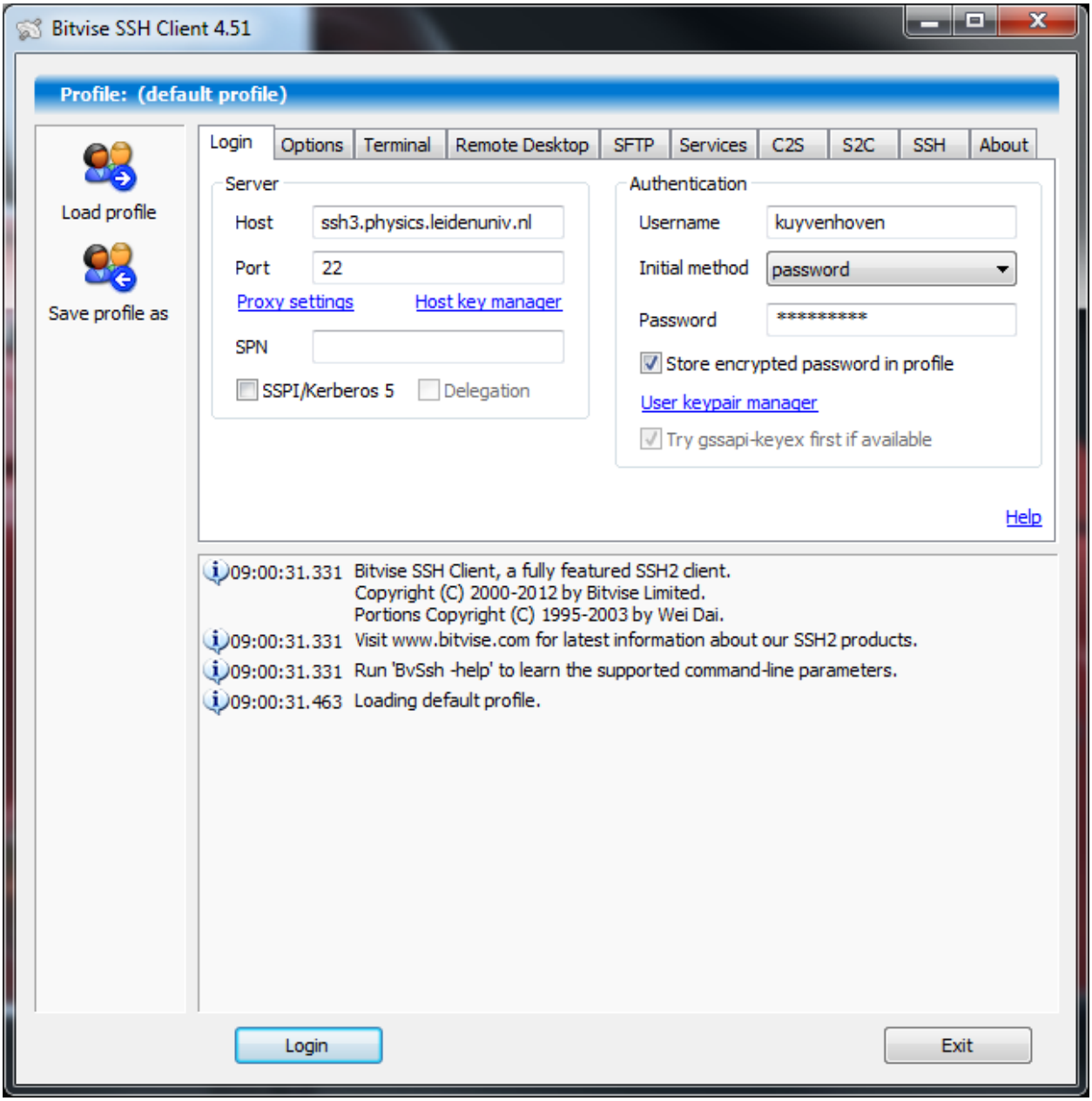
```
TCP    10.10.10.10:445    0.0.0.0:0        LISTENING
```

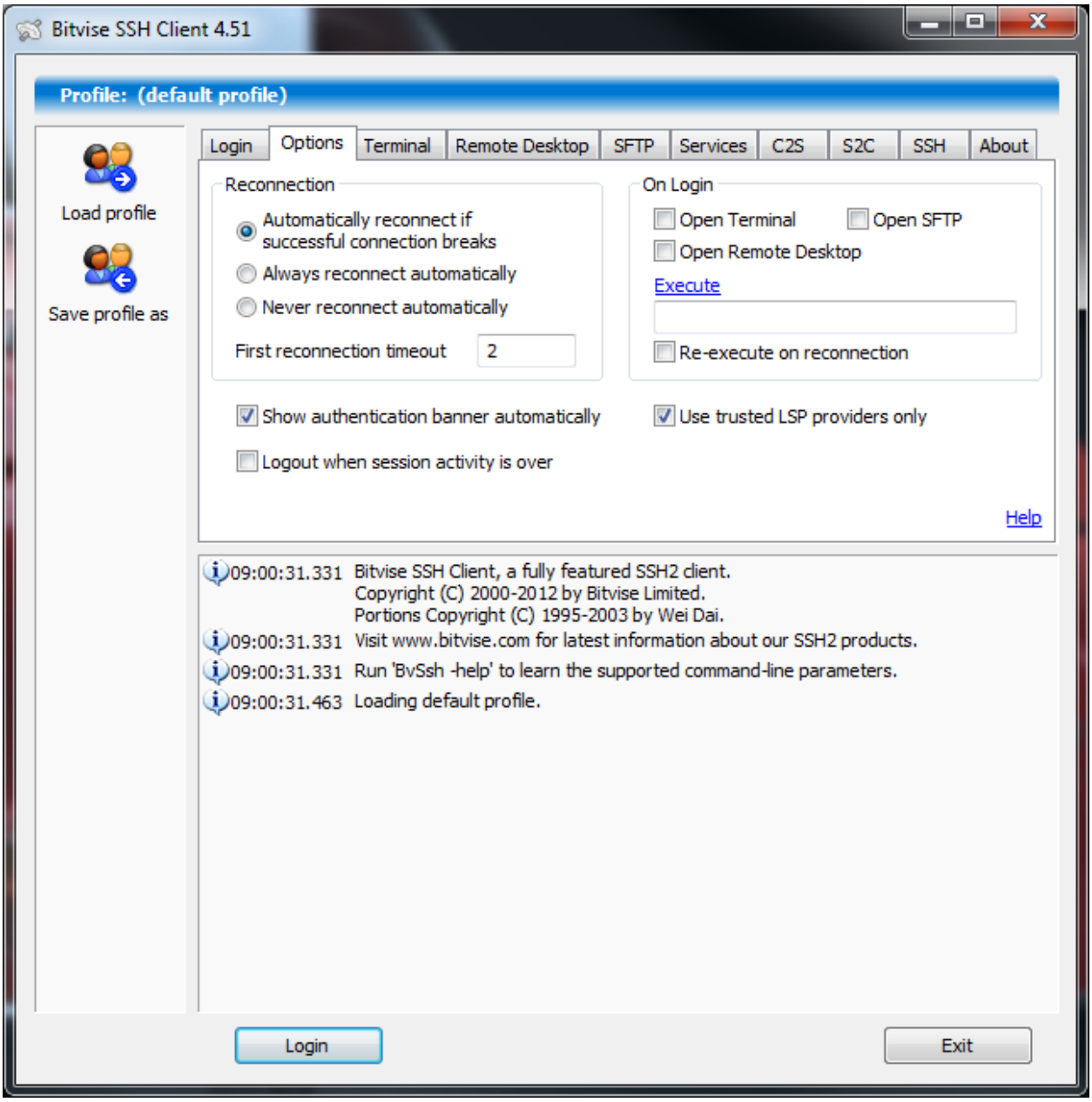
If you see '`0.0.0.0:445`' instead then the 'portproxy' rule was not applied correctly.

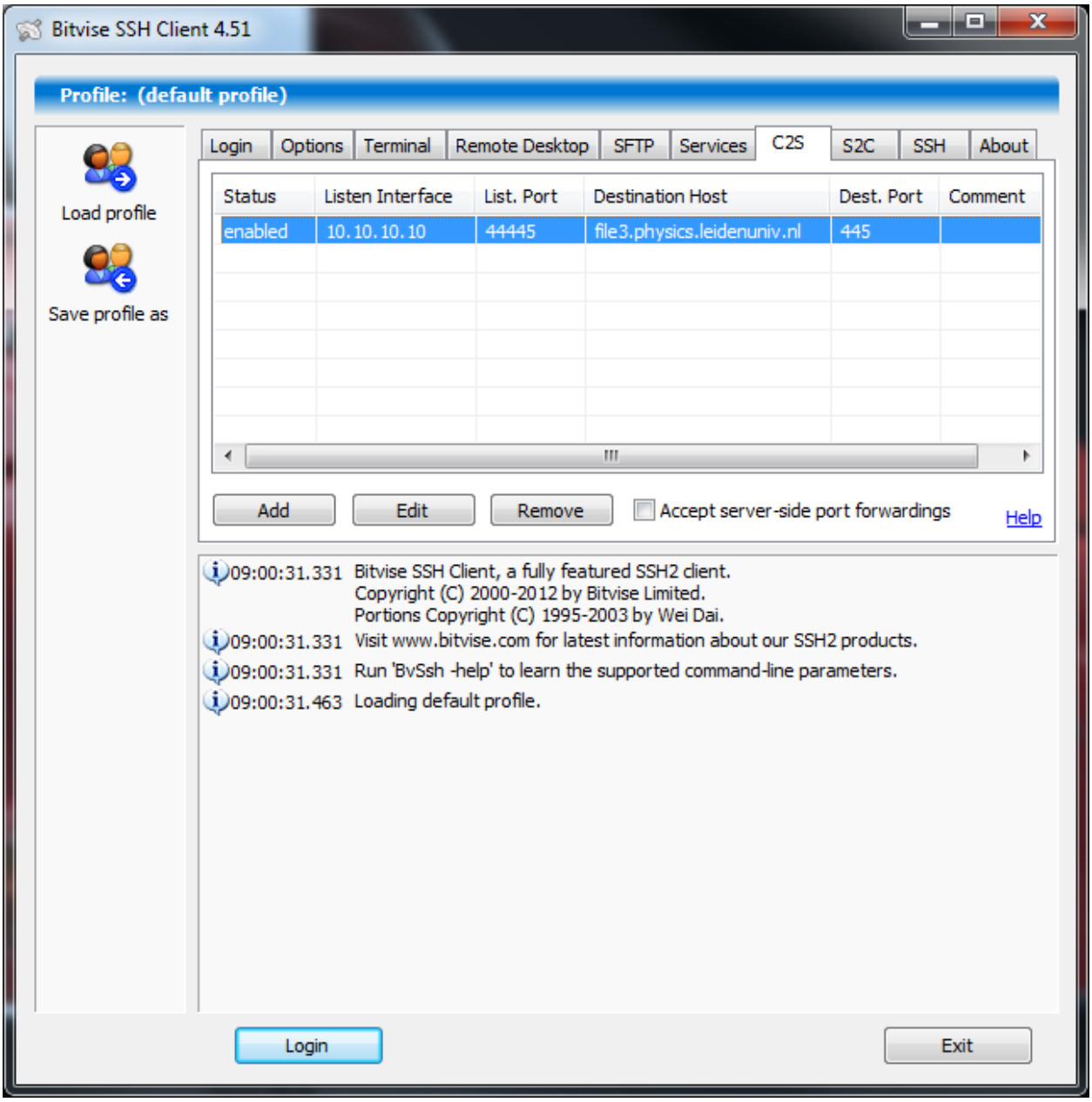
Configuring Tunnelier

Set up a special Tunnelier session with the appropriate `port-forwarding`:

- Start Tunnelier and configure it as the screenshots
-



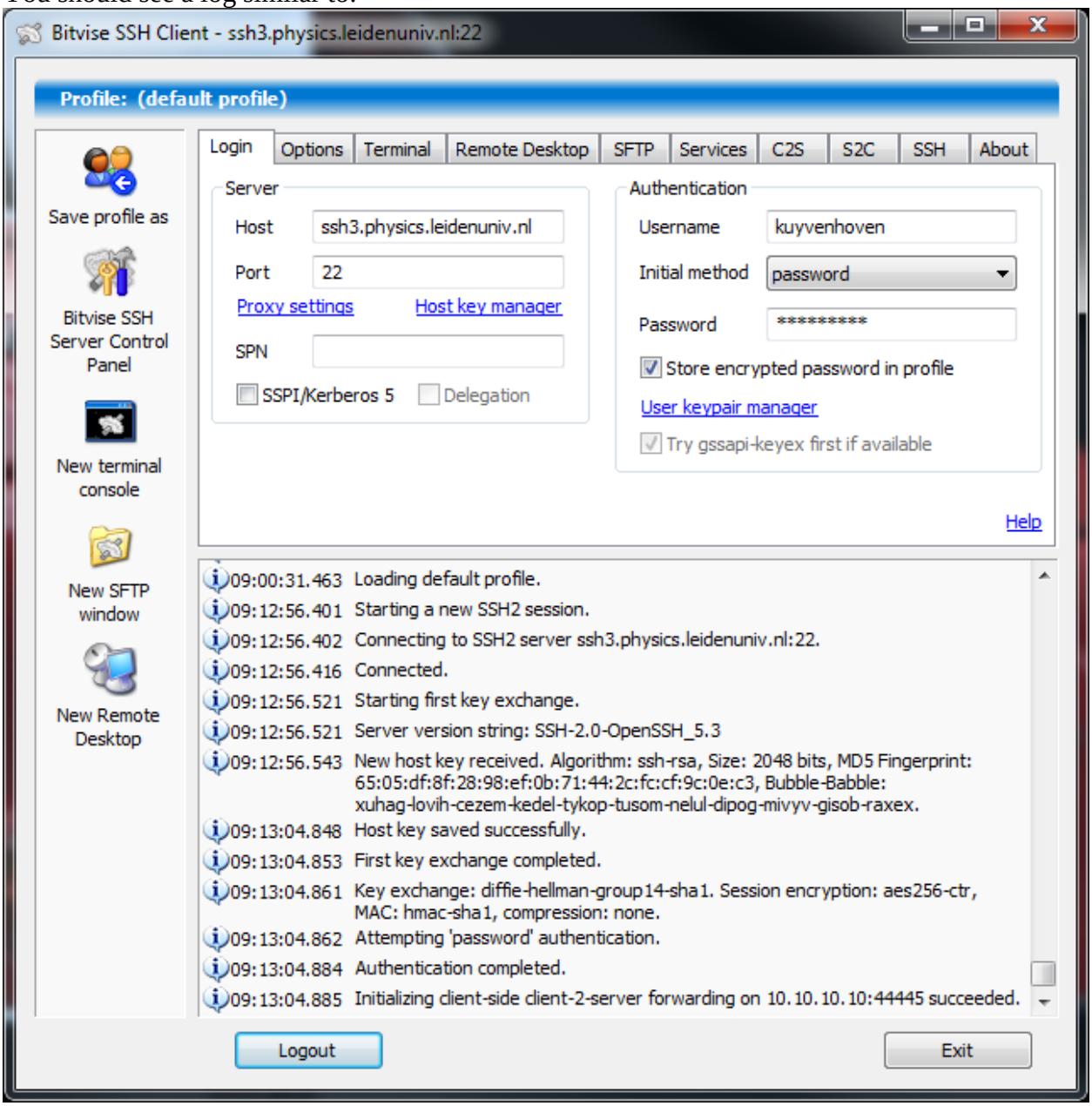

Bitvise SSH Client 4.51
Profile: (default profile)
Load profile
Save profile as
Login
Options
Terminal
Remote Desktop
SFTP
Services
C2S
S2C
SSH
About
Reconnection
Automatically reconnect if successful connection breaks
Always reconnect automatically
Never reconnect automatically
First reconnection timeout
2
On Login
Open Terminal
Open SFTP
Open Remote Desktop
Execute
Re-execute on reconnection
Show authentication banner automatically
Use trusted LSP providers only
Logout when session activity is over
Help
09:00:31.331 Bitvise SSH Client, a fully featured SSH2 client.
Copyright (C) 2000-2012 by Bitvise Limited.
Portions Copyright (C) 1995-2003 by Wei Dai.
09:00:31.331 Visit www.bitvise.com for latest information about our SSH2 products.
09:00:31.331 Run 'BvSsh -help' to learn the supported command-line parameters.
09:00:31.463 Loading default profile.
Login
Exit



Putting it all together

Now that we have configured both our loopback adapter and Tunnelier we can put it all together and mount our Physics home directory as a Windows share:

- Start your newly created Tunnelier session and login on
- Make sure port-forwarding is working properly by checking the Tunnelier event log..
  You should see a log similar to:



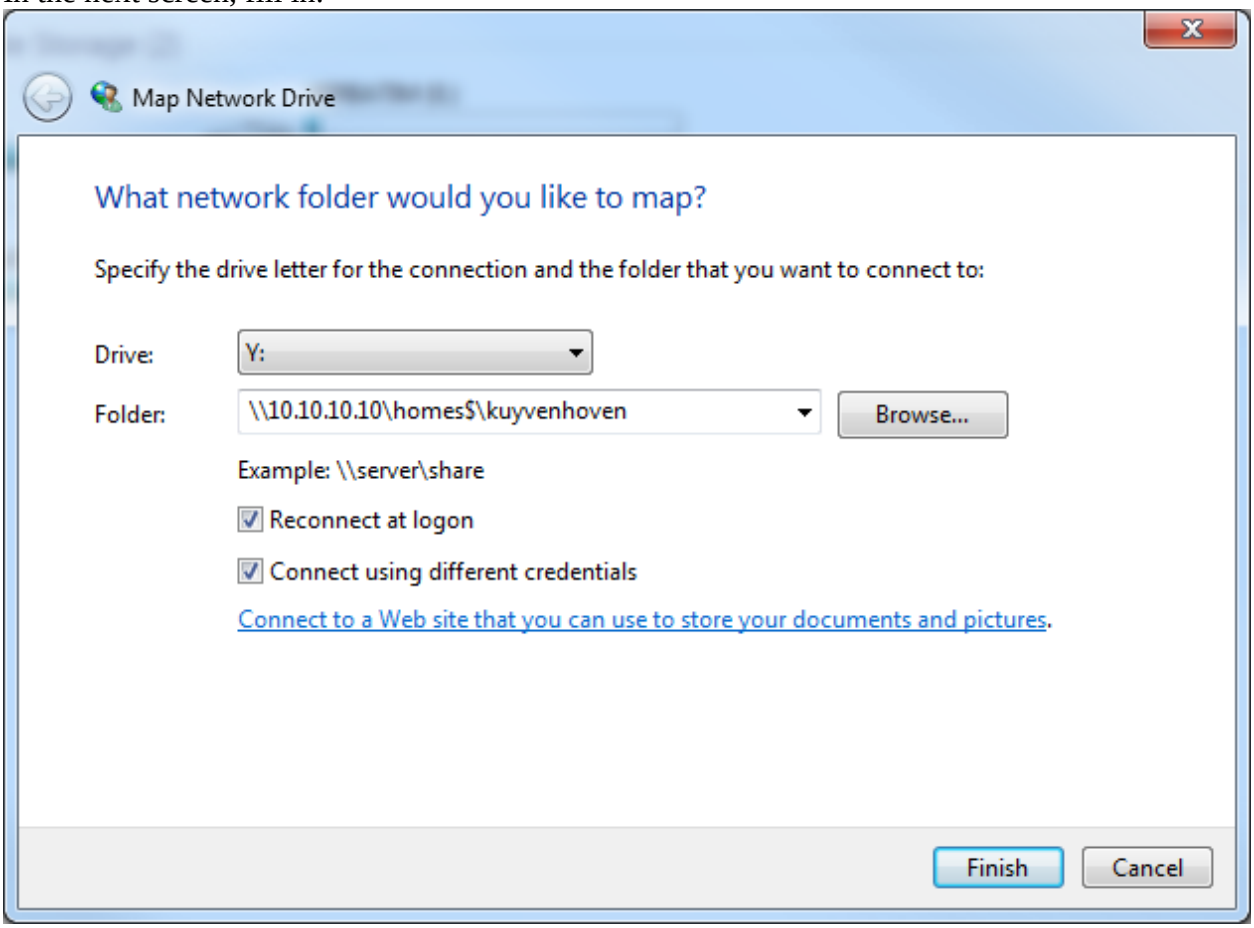
  If not, then check your Tunnelier session options first.

Mapping a network drive

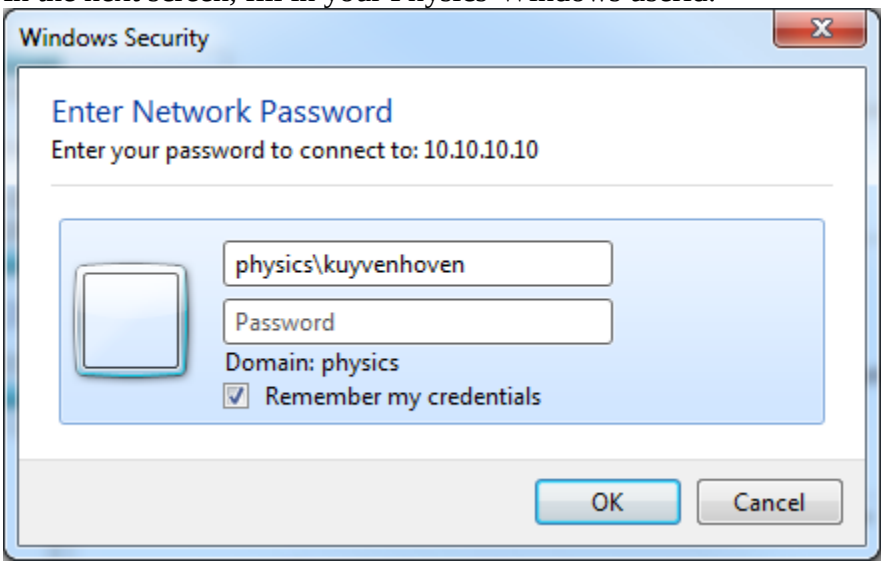
To make life even easier it might be handy to map a network drive to your Physics home directory:

- Start Windows Explorer and choose **Tools->Map Network Drive**.

- In the next screen, fill in:



  - Choose an available drive letter.
  - Do **NOT** click on *Browse* but type in as the *Folder* name: **\\10.10.10.10\homes$\<Your-physics-userid>**
  - Do **NOT** click on *Finish*, click on **Different user name**.
- In the next screen, fill in your Physics-Windows userid:



For the *User name*, fill in the domain **Physics** followed by your Physics-Windows

userid.
For the *Password*, fill in your Physics-Windows password and press **OK**.

- Click on **Finish** to complete the network drive mapping.
- You should now see a new drive letter appear in the *Folders* tree-list in Windows Explorer. Click on it to verify that you are indeed viewing your Physics home directory.

Control+Z! Undo! Undo!

For those wishing to undo the CIFS-over-SSH trick follow these steps:

1. Start a console window with elevated (Administrator) privileges.
2. Restore the automatic startup of the `smb` driver by typing

```
3.   sc config LanmanServer start= auto
```

   NOTE the space after the `start= `!

4. Remove the `portproxy` rule by typing

```
5.   netsh interface portproxy delete v4tov4 listenaddress=10.10.10.10
listenport=445
```

6. Start a `Device Manager` by typing

```
7.   devmgmt.msc
```

   Expand the 'Network Adapters', right-click on **Loopback adapter** and select **Uninstall**.

8. Use the 'Task Scheduler' from the 'Administrative Tasks' menu to delete the task 'Start SMB driver'