

Telnet & Remote Desktop

A. Creating a User Account

In this exercise, you will create a user account with a password. The user account name will be your **first name** and the password will be **ist220**.

1. Go to **Start** and click **Control Panel**, then select **Add or remove user accounts** under **User Accounts and Family Safety**
2. Click **Create a new account**
3. Type your first name as the account name (do not use any spaces)
4. Keep **Standard user** selected as the account type, and then click **Create Account**
5. Click on the account that you created, then select **Create a password**
6. Type **ist220** and confirm it as the password, then click **Create password**

B. Telnet

In this exercise, you will activate the Telnet service on two PCs. You should now designate one PC as PC1, and the other as PC2. You will log on to PC2 from PC1 and to PC1 from PC2 using the Telnet command. This involves several setups as follows:

- Activating the Telnet service
- Assigning proper rights to users to use the Telnet service
- Testing the Telnet service by logging on to PCa and PCb using the Telnet command

B.1 Telnet Overview

Telnet is a terminal emulation program for TCP/IP networks, such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers and routers. In this exercise, you will activate the Telnet service in your computer.

B.2 Starting the Telnet Service

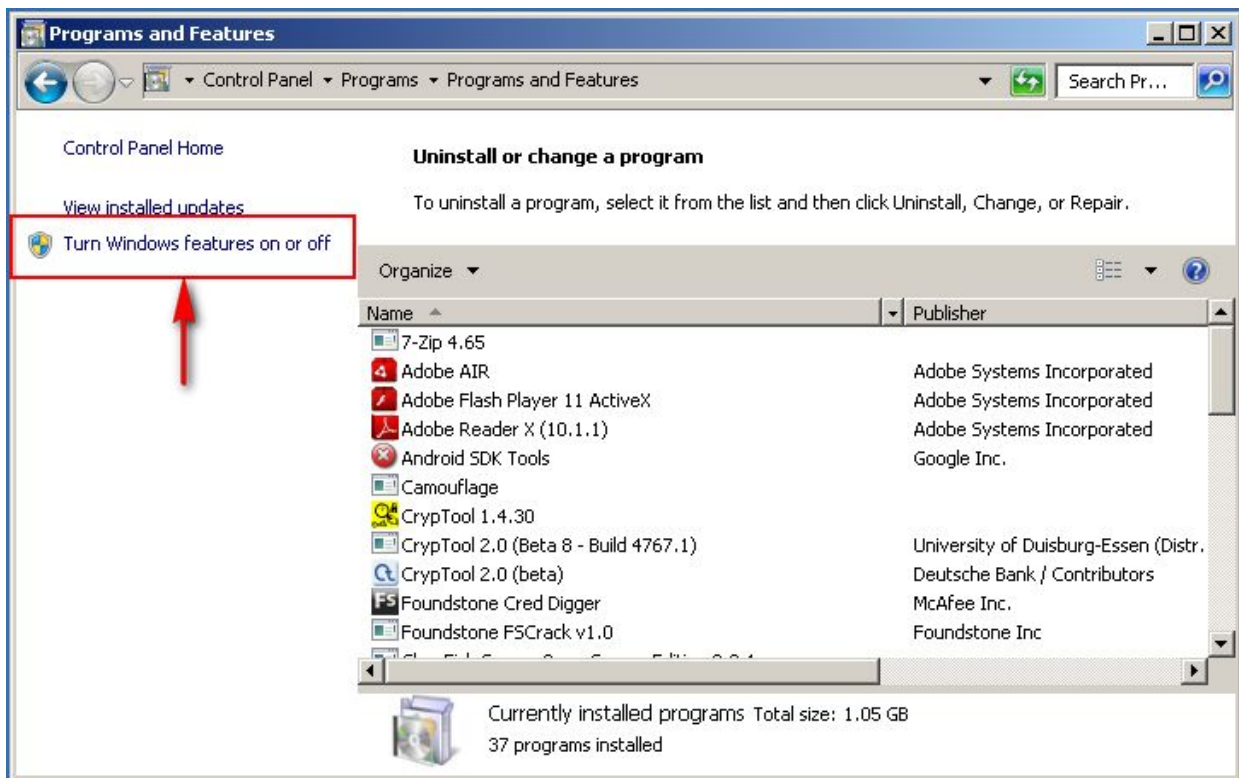
In this exercise, you will start the Telnet service in PC1 and PC2 so that users can log on to them remotely. Telnet runs on port 23. To check whether it is or not, type:

`nmap <PartnerIP> -n` into the command line.

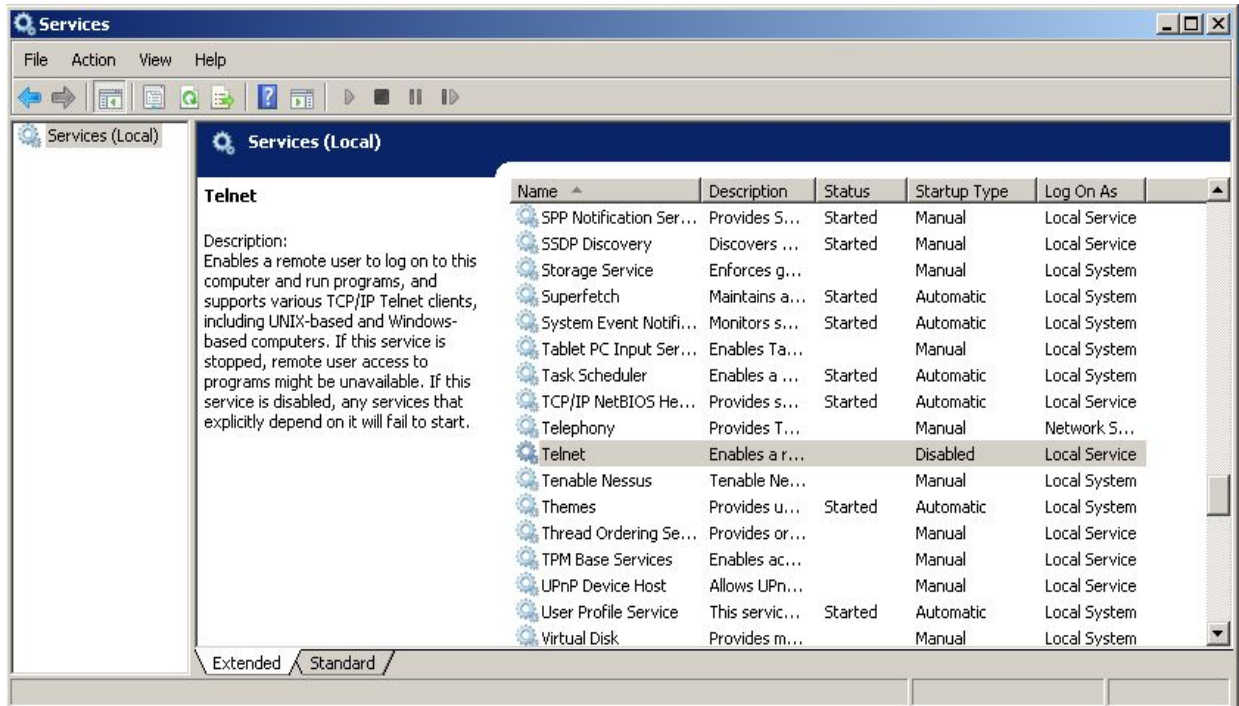
```
Ca. Command Prompt
Starting Nmap 5.21 < http://nmap.org >
Nmap scan report for 192.168.4.37
Host is up (0.00s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
```

Is **port 23** (the Telnet service) open in your teammate's computer? Complete the following steps to start the Telnet service, and then inform your teammate that you have done so.

1. Click **Start**, select the **Control Panel**, and then click **Programs**
2. Under **Programs and Features**, select **Turn Windows features on or off** (see the figures below)



3. Locate **Telnet Client** and **Telnet Server** in the list, and make sure both are checked and Click OK.
4. Click **Start**, then select the **Control Panel**. Click **System and Security**, followed by **Administrative Tools**. Double-click **Services**. The following window should appear.



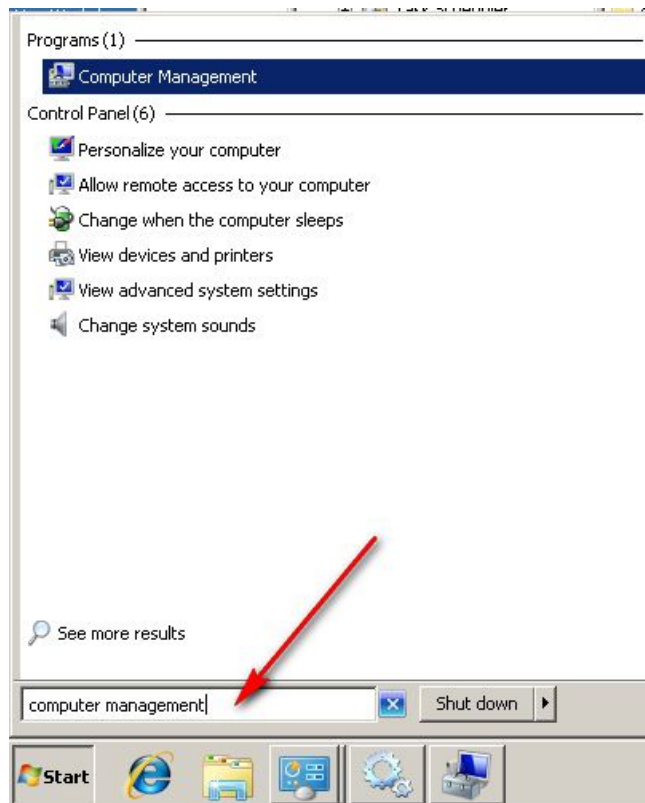
5. Scroll through the list and locate "Telnet". Right-click it and select **Properties**
6. Change the **Startup type** from Disabled to **Manual**, and click **OK**
7. Right-click **Telnet** again, and select **Start**. The Telnet service should now be running on your computer
8. Use **nmap** to check the open ports again as described above. Is port 23/Telnet open? Type **nmap <PartnerIP> -n** into the command line to test your partner's computer. Ask your partner to test your computer as well. You should be able to see port number 23.

```
CA: Command Prompt
C:\Users\Student1>nmap 192.168.4.38 -n
Starting Nmap 5.21 < http://nmap.org > at 2012
Nmap scan report for 192.168.4.38
Host is up (0.00s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
```

B.3 Adding Users to TelnetClients group

In the following steps, you will create a user group called **TelnetClients**. The members of the TelnetClients user group have permission to access your computer through a Telnet session.

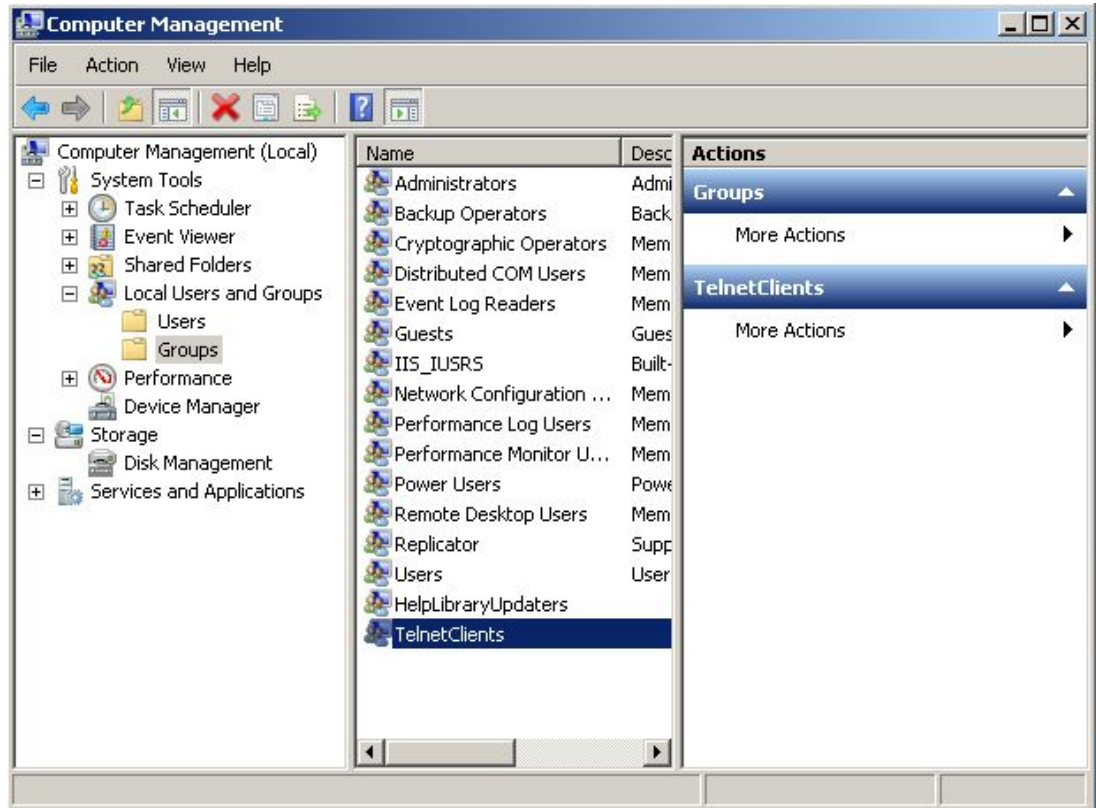
1. Click **Start**, then select the **Control Panel**. Click **System and Security**, followed by **Administrative Tools**. Double-click **Computer Management**. (*Alternatively, you can type **computer management** in the Search Window of the Start menu as shown below.*)



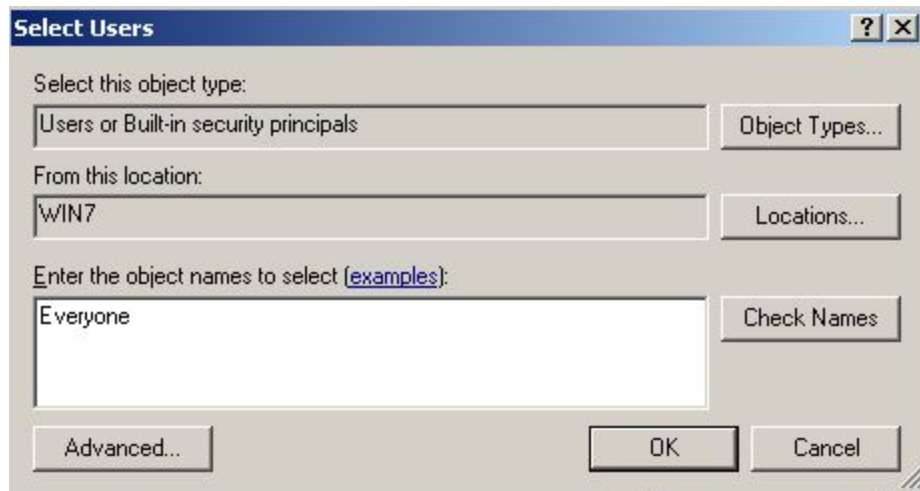
2. In the console tree, expand **Local Users and Groups** by clicking on (+) and then

click **Groups**.

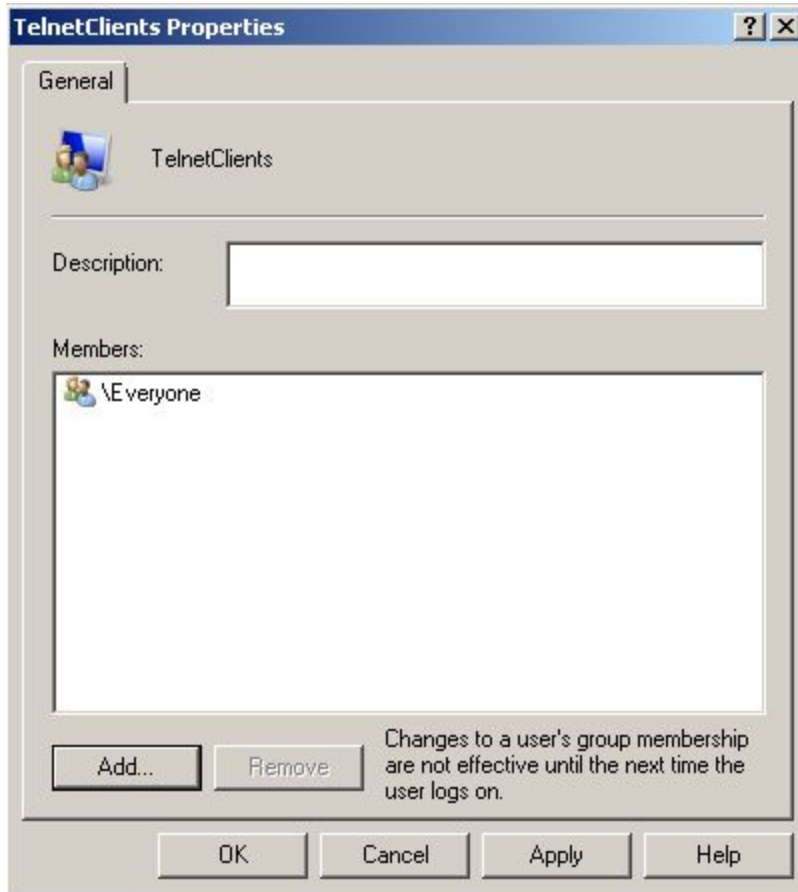
3. Check whether a group called **TelnetClients** exists or not.



4. Right-click on TelnetClients group and select “Add to Group...”. then Click **Add**, type “**Everyone**” to give all users on your computer the right to access the Telnet service as shown in the picture below.



5. Click **OK**, then click Apply when you see the following TelnetClients Properties Window.



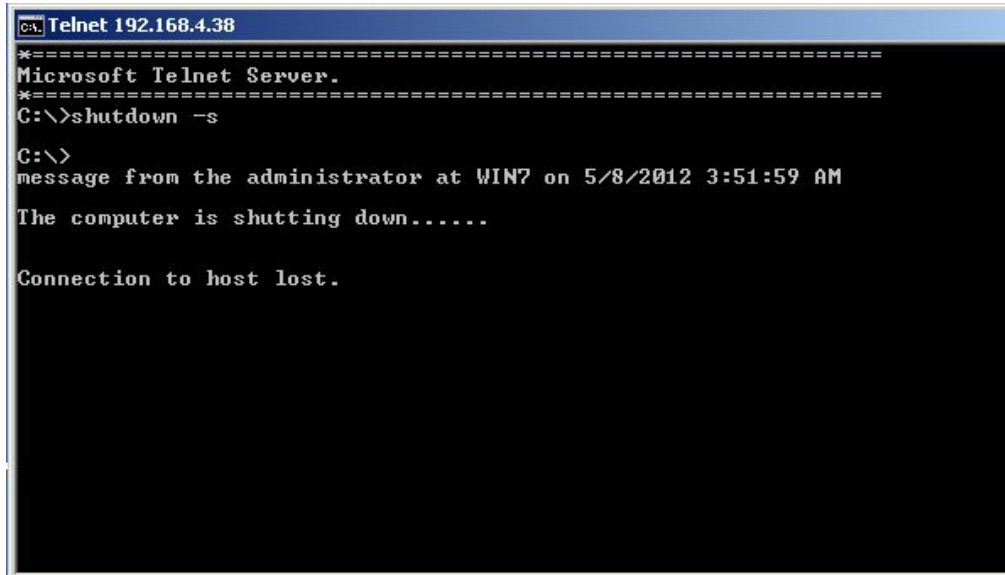
B.4 Testing Telnet

In this exercise, you will use the TCP/IP Telnet program to log on to PC1 from PC2 and to PC2 from PC1. Try the following steps first in PC1 and then in PC2. Bring up the command prompt in both computers. Your partner will try to shutdown your computer. In the command prompt type **shutdown -a** to abort shutdown.

In PC1

1. Bring up the command prompt and type **telnet <PartnerIP>**. Press enter.
2. Read the prompted warning and press Enter **without doing anything else**. Enter the user name (ask your teammate for the user name he/she created in Step A) and the password (ist220).
3. To make sure that you are logged into your teammate's computer, type **ipconfig** at the command line and press Enter.

4. In the Telnet command prompt, type **shutdown -s** and press Enter to shut down your teammate's computer.



```
Ca. Telnet 192.168.4.38
=====
Microsoft Telnet Server.
=====
C:\>shutdown -s
C:\>
message from the administrator at WIN7 on 5/8/2012 3:51:59 AM
The computer is shutting down.....

Connection to host lost.
```

C. Remote Desktop

C.1 Overview

With Remote Desktop in Windows 7, you can have access to a Windows session that is running on your computer when you are at another computer. This means, for example, that you can connect to your work computer from home and have access to all of your applications, files, and network resources as though you were in front of your computer at work. You can leave programs running at work and when you get home, you can see your desktop at work displayed on your home computer, with the same programs running. Remote Desktop also allows more than one user to have active sessions on a single computer. This means that multiple users can leave their applications running and preserve the state of their Windows session even while others are logged on.

C.2 Set up the Remote Desktop Connection

In this exercise, you will configure your computer for the Remote Desktop Connection.

1. Open the **Control Panel** and click **System and Security**, then click **System** and select **Remote settings**
2. Under Remote Desktop, click the radio button at **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**
3. Click **Select Users**, then click **Add**. Type **Student2**, then select **Check Names** and click **OK**, and click **OK** once again
4. Select **OK** to close the Remote Settings window

C.3 Using Remote Desktop

In this exercise, you will first access PC1's Desktop from PC2, and then repeat the same exercise by accessing PC2 from PC1.

1. In PC2, go to **Start**, click **All Programs**, select **Accessories**, and then click **Remote Desktop Connection**
2. In the window, type **<PartnerIP>** and click **Connect**. Click **User Another Account** if student 2 does not appear. Enter **student2** as the user name and **student2** as the password. Click **OK**.

3. In the window that pops up, click **Yes** to continue despite certificate errors
4. After connecting to PC1, disconnect and try the same process on PC1 to connect to PC2.

D. Capturing and Analyzing Telnet Packets

In this exercise, you will capture Telnet packets and discover user account and password information from the packets captured. PC1 will capture packets while PC2 is connecting to the Telnet service.

1. Repeat B.3 for any computers that have been logged off/shut down, since the desktop image has been reset. Use **nmap <PartnerIP> -n** if you are unsure.
2. Make sure to create the TelnetClients group and include everyone. You do not have to recreate another user account.
3. Open **Wireshark** (on the Desktop) on both computers and begin capturing packets
4. Click **Capture > Interfaces > Start** to begin
5. On **PC2**, bring up the command prompt and type **telnet <PartnerIP>** and press Enter to log on to PC1
6. Use student2 and student2 as username and password.
7. Stop capturing packets on both computers
8. Analyze each captured packet and try to find out which packets transfer the password and user name information by looking at their content. Can you see the password transmitted?