

## D-Link DI-604 Ethernet Broadband Router

Download manual at:

[http://legacyfiles.us.dlink.com/DI-604/REVE/DI-604\\_REVE\\_MANUAL\\_2.06\\_EN.PDF](http://legacyfiles.us.dlink.com/DI-604/REVE/DI-604_REVE_MANUAL_2.06_EN.PDF)

Read through the manual and complete the following questions and exercises:

1. Why is it called a **Broadband** ethernet router (pg. 3)?

Because it connects multiple computers to a high-speed broadband internet connection using Ethernet ports.

2. It can act as a switch. What does this mean (pg. 3)?

This means it can allow multiple devices to communicate with each other over a local area network (LAN) without internet access.

3. What does its ability to Content Filter mean(pg. 4)?

It allows the router to restrict access to specific websites or internet services based on user-defined rules.

4. It can act as a DHCP server. Explain this(pg.4 )

The router can assign IP addresses automatically to devices on the network, reducing manual configuration.

5. Describe what would be connected to each of the 5 ethernet ports(4 LAN and 1 WAN):

LAN ports: 4 client devices (PCs, printers, etc.)

WAN port: Modem or external internet connection



6. What is the purpose of the reset button?

To restore the router to factory default settings.

7. Explain how to properly reset the Router.

Hold the reset button for 10 seconds while powered on until lights blink, then release.

8. What does resetting a router do?

It erases all user settings and restores factory defaults.

9. What is the default IP address of this router?

192.168.0.1

10. Why is this important to know?

It is used to access the router's configuration page.

11. What is the default subnet mask?

255.255.255.0

12. Why is this important to know?

It defines the network range and helps determine which IP addresses are in the same network.

13. To be able to connect your computer to the router it is suggested that you "configure your computer IP as 192.168.0.3, subnet mask as 255.255.255.0 and gateway as 192.168.0.1 ". Explain why you should use each of these 3 IP address values?

192.168.0.3 (unique host IP), 255.255.255.0 (subnet mask), 192.168.0.1 (gateway to router)

14. Another suggestion is to "configure your computers to obtain TCP/IP settings automatically from the DHCP server feature of the DI-604". Why? What is the role of DHCP in a network?

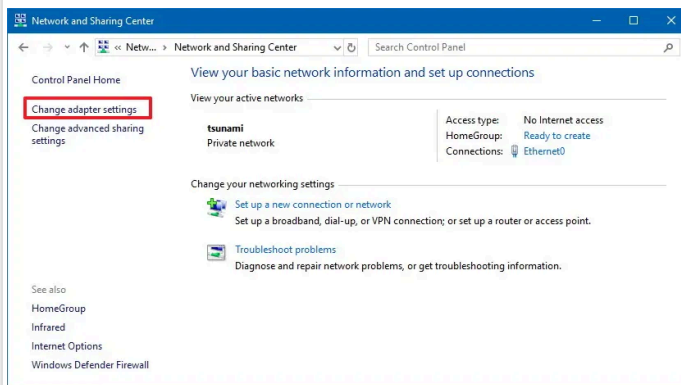
DHCP simplifies network setup and avoids IP conflicts.

15. Use the steps described in step #13 to set up your computer

## **How to change the IP address settings using the Control Panel**

Use these steps to assign a static or dynamic IP configuration using Control Panel:

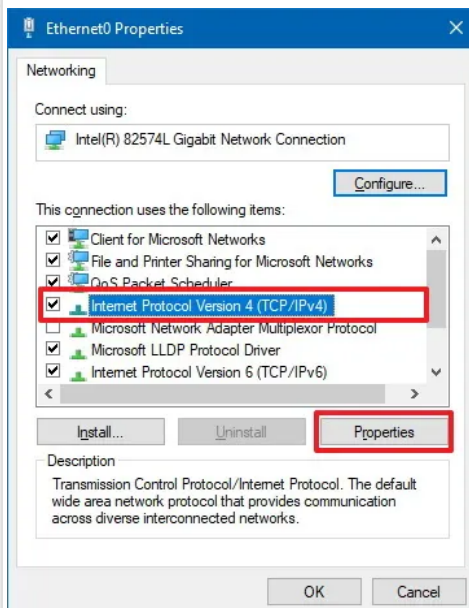
1. Open Control Panel.
2. Click on Network and Internet.
3. Click on Network and Sharing Center.
4. Click the Change adapter settings option on the left navigation pane.



5. Right-click the network adapter and select the Properties option.

6. Select the Internet Protocol Version 4 (TCP/IPv4) option.

7. Click the Properties button.



8. Select the Use the following IP address option.

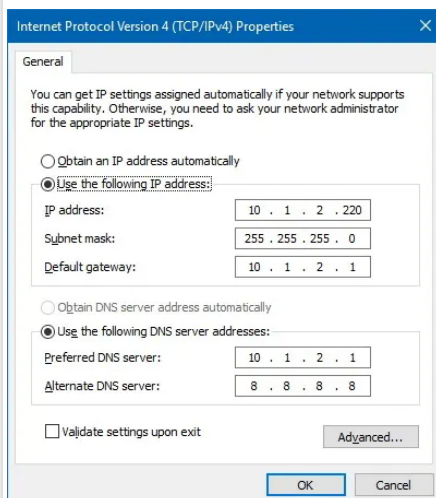
9. Assign the static IP address – for example, 192.168.0.3.

10. Specify a Subnet mask. Typically, on a home network, the subnet mask is 255.255.255.0.

11. Specify a Default gateway. (Usually, your router's IP address. For example, 192.168.0.1.)

12. Since we are not connecting to the internet, the DNS settings can be left to anything.

14. Click the OK button.



16. Connect the router to power. Using an ethernet cable connect one of the LAN ports to the ethernet port on your computer (usually found at the back). Open a browser window and enter <http://192.168.0.1> into the address bar and then hit enter. In the log in console use 'admin' for the username and a blank for the password. Log in.

17. Reset the password. Why is this important?

To prevent unauthorized access to router settings.

18. We will not be connecting to an ISP so in the 'Select and Internet Connection Type' screen you can make any selection (just leave it to Dynamic IP" as this is what you should do if we were in fact to connect to an ISP).

19. On the next screen click the 'Clone MAC address'. What is a MAC address?

Where on your router can you find this (i.e. physically located)?

A MAC address is a hardware ID for network interfaces. It's printed on the router label.

20. What number system is used for MAC addresses? Why?

Hexadecimal; it efficiently represents large binary values.

21. Save your changes and click the reboot button.

22. Log in again using your password. Access the screen shown below:

The screenshot shows the D-Link DI-604 Ethernet Broadband Router configuration interface. The top navigation bar includes 'Home', 'Advanced', 'Tools', 'Status', and 'Help'. The 'Advanced' tab is selected, and the 'WAN' sub-tab is active. The 'WAN Settings' section prompts the user to select an option to connect to their ISP. Three radio buttons are present: 'Dynamic IP Address' (selected), 'Static IP Address', and 'PPPoE'. Below these, the 'Dynamic IP' section contains a 'Host Name' field with 'DI-604' and an 'optional' label, and a 'MAC Address' field with a hexadecimal value '00-03-2F-FF-FC-09' and an 'optional' label. A 'Clone MAC Address' button is located below the MAC address field. At the bottom right, there are three icons: a green checkmark, a red 'X', and a red plus sign, with labels 'Apply', 'Cancel', and 'Help' respectively.

23. Explain the three settings you see on this page.

24. Under what circumstances would you choose Static IP Address? Who do you think would choose this and why?

Used by servers or devices needing fixed IPs for port forwarding.

25. Click on the LAN button and explain the settings on this screen:

The screenshot shows the LAN Settings page for a D-Link DI-604 router. The left sidebar has buttons for Wizard, WAN, LAN (highlighted), and DHCP. The main content area has tabs for Home, Advanced, Tools, Status, and Help. Under the LAN Settings section, it says "The IP address of the DI-604." and shows fields for IP Address (192.168.0.1), Subnet Mask (255.255.255.0), and Local Domain Name (optional). At the bottom right are Apply, Cancel, and Help buttons.

26. Click on the DHCP button and explain the settings:

The screenshot shows the DHCP Server page for a D-Link DI-604 router. The left sidebar has buttons for Wizard, WAN, LAN, and DHCP (highlighted). The main content area has tabs for Home, Advanced, Tools, Status, and Help. Under the DHCP Server section, it says "The DI-604 can be setup as a DHCP server to distribute IP addresses to the LAN network." and shows fields for DHCP Server (Enabled), Starting IP Address (192.168.0.100), Ending IP Address (192.168.0.199), and Lease Time (1 Hour). At the bottom right are Apply, Cancel, and Help buttons. Below this is a DHCP Client Table with columns for Host Name, IP Address, MAC Address, and Expired Time.

Host Name	IP Address	MAC Address	Expired Time
unknown	192.168.0.103	08-00-46-4B-F2-96	Feb/05/2106 23:32:34
unknown	192.168.0.102	00-00-E2-6D-5A-F2	Feb/05/2106 23:32:34
unknown	192.168.0.101	00-90-96-0F-49-DF	Feb/05/2106 23:32:34
unknown	192.168.0.100	00-00-E2-4F-C4-F3	Feb/05/2106 23:32:34

27. Click the Advanced tab and then click on the Virtual Server button. Explain the purpose of this page and all its settings.

28. Click the Advanced tab and then the Filter button. Explain the purpose of this page. What is the difference between MAC and Domain and URL Blocking?

Controls traffic by MAC, IP, Domain, or URL. MAC blocks specific devices, Domain/URL blocks content

29. Click on the Advanced Tab and then the DMZ button. What does DMZ stand for? What is the purpose of this page?

DMZ (Demilitarized Zone) exposes one device to all incoming traffic for troubleshooting

30. Click on the Tools tab and then the Admin button. What is the purpose of Remote management? Why is it important that you don't leave the IP setting to \*?

Enables admin access from outside the network. Don't leave IP as \* to avoid unauthorized access

31. If you set the IP address of the Remote management IP Address setting to 192.168.0.10 and the port number to 1010 what would be the address you enter in the browser bar to access the router?

<http://192.168.0.10:1010>

32. What is the purpose of the Tools tab Firmware button page?

Update router software for performance or security fixes

33. Click on the Tools tab and then the Misc. button. What is the ping test for? Attach another computer to your router. Determine its IP address. Then use this feature to ping it and see if it is accessible on your network via this router.

Tests connectivity between router and another device on the network

34. Click on the Status tab and then the Device Info button. Why are there two IP addresses assigned to this router? What is the difference between the LAN and the WAN IP address? Why two MAC addresses? What is the Default Gateway of the WAN referring to? What is DNS and why are there several DNS IP addresses?

WAN IP: external (internet), LAN IP: internal (local network)

Two MACs for WAN and LAN interfaces

Default Gateway: ISP or upstream router

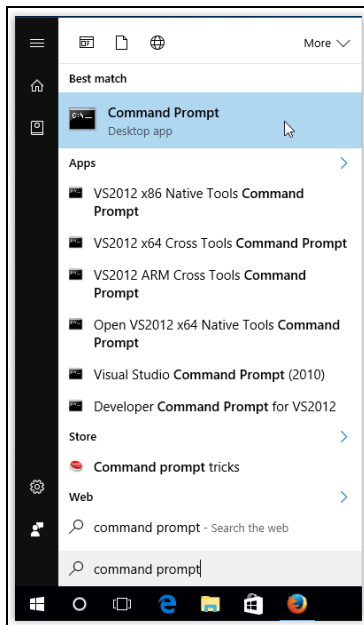
DNS: Resolves domain names; multiple for redundancy

35. To check the IP address of your computer do the following:

### Find your IP Address on Windows 10: Using the Command Prompt

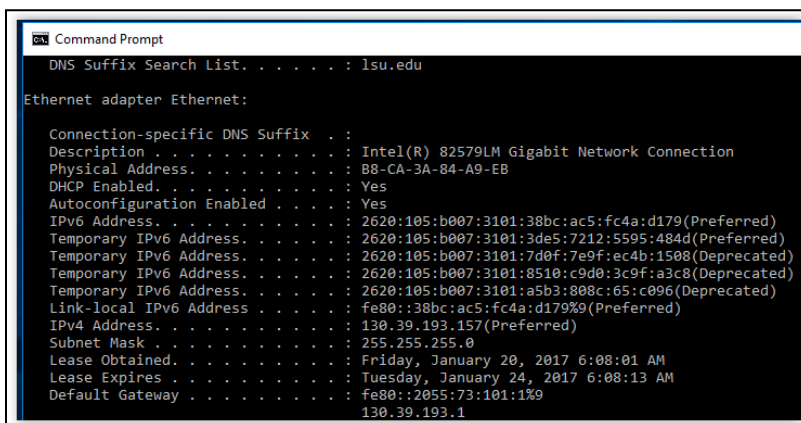
1. Open the **Command Prompt**.

a. Click the **Start** icon, type **command prompt** into the *search bar* and press click the **Command Prompt** icon.



2. Type `ipconfig/all` and press **Enter**.

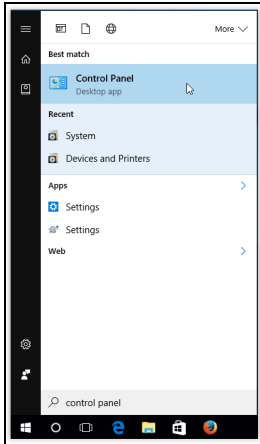
3. The *IP Address* will display along with other LAN details.



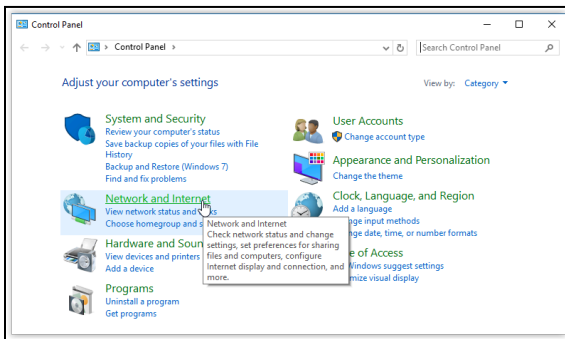
Find your IP Address on Windows 10: [Using the Control Panel](#)

1. Click the **Start** button, type in **control panel**, then click the **Control Panel** icon.

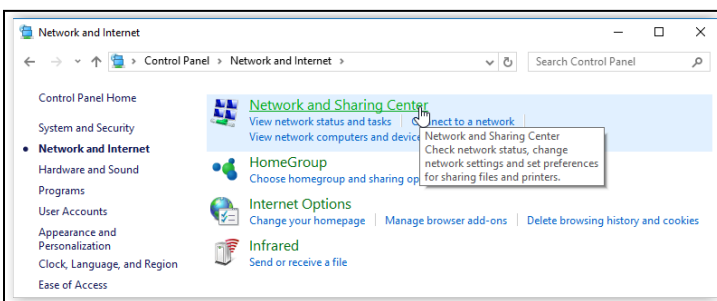




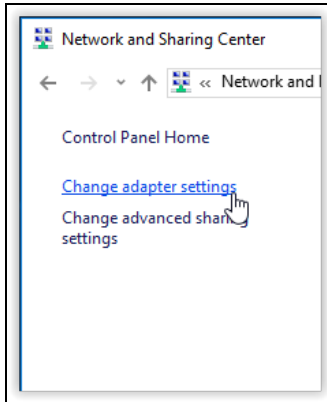
2. Click **Network and Internet** when the *Control Panel* opens.



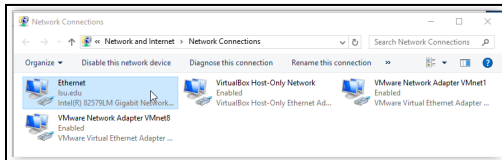
3. Select **Network and Sharing Center**.



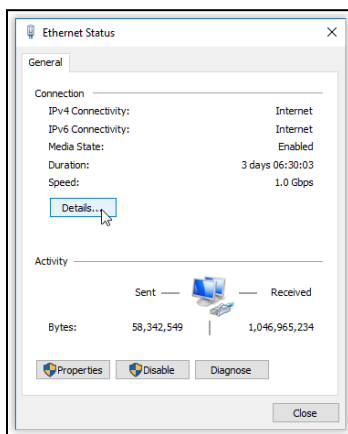
4. Click the **Change adapter settings** link, located on the left.



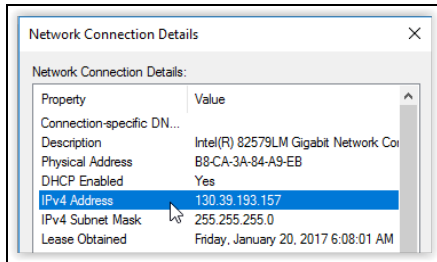
5. Double-click **Ethernet**.



6. Click **Details**, located under the *Connection* section for the *Local Area Connection Status*.



7. Scroll down until you find the **IPv4 Address**.



Make sure you have at least 2 computers connected to your router. We will now learn how to use some basic command line utilities to test our network.

1. First determine the IP address of all the computers in your mini network/LAN as well as that of your router. Write this down somewhere.
2. Open the windows command prompt.
3. At the command prompt type `ping <ip address>` where the ip address is that of another computer on your network.
4. At the command prompt, type, `ping <IP address>`, as shown below (you will replace 8.8.8.8 with the other computers ip address. Note: if you do not get a successful reply then it's possible that the other computer's firewall is blocking incoming request so you will need to turn it off (not a good idea normally but it exposes you to security risks if connected to the internet and since we are not connected it's OK!). To do that type 'firewall' in the windows task search bar. Then select Private Network and then find the option to turn off the firewall. Try pinging again.

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=14ms TTL=47
Reply from 8.8.8.8: bytes=32 time=14ms TTL=47
Reply from 8.8.8.8: bytes=32 time=14ms TTL=47
Reply from 8.8.8.8: bytes=32 time=16ms TTL=47

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 16ms, Average = 14ms

C:\Users>
```

## Understanding Ping results

Ping operates by sending ICMP Echo Request packets to the target device and waiting for an ICMP Echo Reply. The program reports errors, packet loss, and a statistical summary of the results.

Note:

The Google DNS server IP address, **8.8.8.8**, or the BBC server domain address, **bbc.co.uk**, are both commonly used as ping destinations to check outgoing connectivity. In the following examples, the Ping command was used to check the connection to device 192.168.1.1, with 32 bytes of data.

#### **Example: a successful Ping**

The following example shows the screen display after a successful ping attempt, where four packets were sent, and four packets received.

**Pinging 192.168.1.1 with 32 bytes of data:**

**Reply from 192.168.1.1: bytes=32 time=48ms TTL=50**

**Reply from 192.168.1.1: bytes=32 time=22ms TTL=50**

**Reply from 192.168.1.1: bytes=32 time=16ms TTL=50**

**Reply from 192.168.1.1: bytes=32 time=15ms TTL=50**

**Ping statistics for 192.168.1.1:**

**Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),**

**Approximate round trip times in milli-seconds:**

**Minimum = 15ms, Maximum = 48ms, Average = 25ms**

#### **Example: target device not responding**

A ping result, where the target device is not responding, or there is a connection issue,

**Pinging 192.168.1.1 with 32 bytes of data:**

**Request timed out.**

**Request timed out.**

**Request timed out.**

**Request timed out.**

**Ping statistics for 192.168.1.1:**

**Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),**

will look like this: Although four packets were sent, none have been received, showing a 100% loss of packets, and indicating an issue with either the connection or the target device.**Note:**

A result like this does not always mean the device is not online or working correctly. Many devices have ICMP ping responses disabled for security or service reasons. So even if they are up and running it will appear as if they are unreachable.

36. Explain your results.

Successful = device is reachable

Failure = blocked or unreachable (check firewall or connection)

37. Try pinging your router's ip address. What happens?

Should reply if connected

38. Trying ping 127.0.0.1. What happens? Do some research to learn why and explain your findings here.

Always replies; tests local TCP/IP stack

39. Try pinging 111.111.111.111. What happens? Why?

Likely fails; no real device has this IP

40. Explain why this utility is useful.

Diagnoses connectivity, network delays, or unreachable devices

## Using Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays, of packets across an Internet Protocol (IP) network. This section shows how to run Traceroute, and how to interpret the results.

### Running Traceroute

To run the Traceroute utility, proceed as follows.

1. Open a Windows Command Prompt window.
2. At the command prompt, type, `tracert <domain.ext>` (replace `<domain.ext>` with the domain name and extension that you would like to trace a route to). Try to traceroute the router. Next traceroute a second computer connected to your network. How many hops are required to reach each IP address? Why do both tracerts have the same number of hops?

It may take a few seconds to respond, but this command will give a traceroute from your computer to the destination you selected.

```
c:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\24-7webs>tracert 24-7webs.com

Tracing route to 24-7webs.com [75.126.38.238]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.2.1
  2  43 ms    49 ms    42 ms    64.230.197.205
  3  41 ms    40 ms    41 ms    dis11-toronto12_0lan14.net.bell.ca [64.230.222.41]
  4  41 ms    41 ms    42 ms    core3-toronto12_GE11-0.net.bell.ca [64.230.159.17]
  5  52 ms    52 ms    51 ms    core1-chicago23_po313-0-0.net.bell.ca [64.230.147.18]
  6  55 ms    52 ms    54 ms    bx2-chicago23_po2-0-0-0.net.bell.ca [64.230.203.146]
  7  52 ms    51 ms    52 ms    206.111.3.45.ptr.us.xo.net [206.111.3.45]
  8  52 ms    52 ms    52 ms    207.88.14.9.ptr.us.xo.net [207.88.14.9]
  9  78 ms    78 ms    78 ms    207.88.14.10.ptr.us.xo.net [207.88.14.10]
 10 81 ms    80 ms    81 ms    207.88.185.74.ptr.us.xo.net [207.88.185.74]
 11 80 ms    81 ms    81 ms    border3.tge4-1-bbnet2.ext1.dal.pnap.net [216.52.191.83]
 12 77 ms    77 ms    76 ms    te2-1.cer03.dal01.dallas-datacenter.com [216.52.189.30]
 13 77 ms    77 ms    76 ms    po3.dar02.dal01.dallas-datacenter.com [66.228.118.211]
 14 77 ms    78 ms    78 ms    po2.fcr01.dal01.dallas-datacenter.com [66.228.118.158]
 15 78 ms    78 ms    78 ms    75.126.38.238-static.reverse.softlayer.com [75.126.38.238]

Trace complete.
```

Note:

You can interrupt Traceroute at any time by holding down the CTRL key, and pressing C on your keyboard. **Copying Traceroute results** To copy the results of your Traceroute, proceed as follows.

1. Right click on the Command Prompt Window and, from the menu, click Select All.

```
c:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\24-7webs>tracert 24-7webs.com

Tracing route to 24-7webs.com [75.126.38.238]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms
  2  43 ms    49 ms    42 ms
  3  41 ms    40 ms    41 ms
  4  41 ms    41 ms    42 ms
  5  52 ms    52 ms    51 ms
  6  55 ms    52 ms    54 ms
  7  52 ms    51 ms    52 ms
  8  52 ms    52 ms    52 ms
  9  78 ms    78 ms    78 ms
 10 81 ms    80 ms    81 ms
 11 80 ms    81 ms    81 ms
 12 77 ms    77 ms    76 ms
 13 77 ms    77 ms    76 ms
 14 77 ms    78 ms    78 ms
 15 78 ms    78 ms    78 ms

t.bell.ca [64.230.222.41]
.net.bell.ca [64.230.159.17]
net.bell.ca [64.230.147.18]
et.bell.ca [64.230.203.146]
[206.111.3.45]
[207.88.14.9]
[207.88.14.10]
t [207.88.185.74]
.dal.pnap.net [216.52.191.83]
atacenter.com [216.52.189.30]
acenter.com [66.228.118.211]
acenter.com [66.228.118.158]
75.126.38.238-static.reverse.softlayer.com [75.126.38.238]

Trace complete.
```

This will copy the contents to your clipboard. The Command Prompt Window contents

will turn white with black text.

```
C:\Documents and Settings\24-7webz>tracert 24-7webz.com

Tracing route to 24-7webz.com [75.126.38.238]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    192.168.2.1
  1  43 ms    49 ms    42 ms    64.230.197.205
  2  41 ms    40 ms    41 ms    dis11-toronto12_0lan114.net.bell.ca [64.230.222.41]
  3  41 ms    41 ms    42 ms    core3-toronto12_GE11-0.net.bell.ca [64.230.159.17]
  4  52 ms    52 ms    51 ms    core1-chicago23_pos13-0-0.net.bell.ca [64.230.147.18]
  5  55 ms    52 ms    54 ms    bx2-chicagodd_co-2-0-0-0.net.bell.ca [64.230.283.146]
  6  52 ms    51 ms    52 ms    206.111.3.45.ptr.us.xo.net [206.111.3.45]
  7  52 ms    52 ms    52 ms    207.88.14.9.ptr.us.xo.net [207.88.14.9]
  8  78 ms    78 ms    78 ms    207.88.14.10.ptr.us.xo.net [207.88.14.10]
  9  81 ms    80 ms    81 ms    207.88.185.74.ptr.us.xo.net [207.88.185.74]
 10  80 ms    81 ms    81 ms    border3.tge4-1-bbnet2.ext1.dal.paap.net [216.52.191.83]
 11  77 ms    77 ms    76 ms    te2-1.car03.dal01.dallas-datacenter.com [216.52.189.30]
 12  77 ms    77 ms    76 ms    po3.dar02.dal01.dallas-datacenter.com [66.228.118.211]
 13  77 ms    78 ms    78 ms    po2.fcr01.dal01.dallas-datacenter.com [66.228.118.158]
 14  78 ms    78 ms    78 ms    75.126.38.238-static.reverse.softlayer.com [75.126.38.238]

Trace complete.
```

1. Go to the document you want to put the results into, right click and click Paste (or Ctrl-V).

The results are pasted into your document. You may now close the Command Prompt Window.**Understanding Traceroute results** The Traceroute tool is used to map the hops between the end user and the destination server. This can help determine where any issues may lie on the network. The examples below were collected after tracing a route to server 192.168.1.8, over a maximum of 30 hops. They show a good traceroute, then two bad traceroutes; one a failed hop, and one a routing loop.

**Example: a good traceroute**

```
1  20 ms    1 ms    <1 ms    192.168.1.1
2   3 ms     3 ms     1 ms    192.168.1.2
3   3 ms     2 ms     4 ms    192.168.1.3
4   5 ms     3 ms     4 ms    192.168.1.4
5  11 ms     7 ms     8 ms    192.168.1.5
6  10 ms    10 ms    11 ms    192.168.1.6
7   *       *       *       Request timed out.
8  13 ms    13 ms    11 ms    192.168.1.8
```

The following example shows a good traceroute.

You can see each step the data takes when it travels to the destination server of 192.168.1.8. These are called hops, and represent a system or router the data passes through. As you can see, hop 7 in this example has not responded, but hop 8 has, meaning that hop 7 is not responding to the request but is handling the packets properly and forwarding traffic to the next hop.

### Example: a failed hop

In the good traceroute example earlier, hop 7 was not responding to the request, but had not failed, as it was forwarding traffic to hop 8. The result of a test where one hop isn't responding, and is not forwarding traffic, would look something like this:

```
1  20 ms  1 ms  <1 ms 192.168.1.1
2  3 ms   3 ms  1 ms 192.168.1.2
3  3 ms   2 ms  4 ms 192.168.1.3
4  5 ms   3 ms  4 ms 192.168.1.4
5  *      *      *   Request timed out.
6  *      *      *   Request timed out.
...
30 *      *      *   Request timed out.
```

This shows the test failing at hop 5, and continuing to fail all the way to hop 30 (the default max hops for the trace route tool) this means that hop 5 is unresponsive and not responding, or forwarding traffic for subsequent hops.

### Example: a routing loop

When a routing loop occurs it stops data from reaching the final destination. Unlike the failed hop, the routing loop simply loops data back and forth between two hops. In the example below, a loop has occurred between 192.168.1.4 and 192.168.1.5. Data will pass back and forth from one to the other until the session times out or, in this particular

```
1  20 ms  1 ms  <1 ms 192.168.1.1
2  3 ms   3 ms  1 ms 192.168.1.2
3  3 ms   2 ms  4 ms 192.168.1.3
4  5 ms   3 ms  4 ms 192.168.1.4
5  13 ms  13 ms  11 ms 192.168.1.5
6  17 ms  13 ms  10 ms 192.168.1.4
...
30 17 ms  13 ms  10 ms 192.168.1.4
```

case, the maximum hop limit is reached.

### Note:

You will often see this if the end user has been 'wall gardened'. A 'walled garden' refers to a browsing environment that controls the information and Web sites the user is able to access. This is a popular method used by ISPs in order to keep the user navigating only specific areas of the Web. This is often for the purpose of shielding users from information, such as restricting children's access to unsuitable material.

Hostname



1. Your computer device or host name is useful to allow others on the shared network to identify you. In windows 10 enter the command prompt and type hostname. Write down your hostname:
2. Let's change this name to reflect you and your group. Come up with a descriptive group name. Read the following to change your computer's name. When done, restart your computer and use the hostname command to again check your name.

## How to Change Your PC's Name in Windows 10

In modern versions of Windows 10, the Settings panel is the best place to change your computer's name. Open Settings by clicking the gear icon on the Start menu, or using the shortcut **Win + I**. In Settings, select **System**, followed by the **About** tab on the left. You'll see some basic information about your PC here, including the current **Device name** and installed hardware.

Click the **Rename this PC** button to choose a new name for your computer. The name can't contain spaces or special characters, so use only letters, numbers, and hyphens. For best results, create a name that's unique, short, and clear.

Once you've made the tweak, you'll have to restart your computer for the name change to take effect. Upon rebooting, open the same **Settings > System > About** panel and you should see the **Device name** field updated. Now you'll see this name used when you connect other devices to your PC using Bluetooth, when browsing the list of connected devices in your router's admin panel, and similar. No longer will you have to wonder what computer "HP-R41PQ86Z" actually is.

Now that we have a mini network i.e. a LAN set up with a few computers we can experiment with a few things.

## Server-Clients

The internet is based on the server client model of networking. In this scenario you have a computer i.e. the server that serves up resources to another computer i.e. the client. Usually a single server can provide services to many, many clients. A good example is the WWW whereby there are computers that act as web servers. A web server is software running on a computer on a network i.e. the internet, that serves up web pages to clients connecting to it. Clients use browser software to access the web pages on the computers serving up the web pages.

Let's set up and test our own little internet with our own little WWW. Download and extract the [USBWebserver file](#) on the computer you want to act as the server. When extracted go into the folder and find the file 'usbwebserver'. Double click to run it. The web server is now running! You can access the web files found in the 'root' folder. Before you do this from one of the client computers go inside the 'root' folder and list below the files found there.

Next, start up a client computer and open a browser window. In the window type the following:

**http://<ip address of server>:8080**

Hit enter. What file did the web server send back to your browser?

Create a simple web page in a text editor (notepad is fine) on the server computer. Add the following code and save the file in the '**root**' folder as **test1.html**:

```
<html>
  <head>
    <title>Hi there!</title>
  </head>
  <body>
    <h1>Welcome to the test page!</h1>
  </body>
</html>
```

Once saved go back to your client computer and type the following address in the browser address bar:

http:<ip address of server>:8080/test1.html

What happens?

By default what page do you think a URL loads if it's not specified?

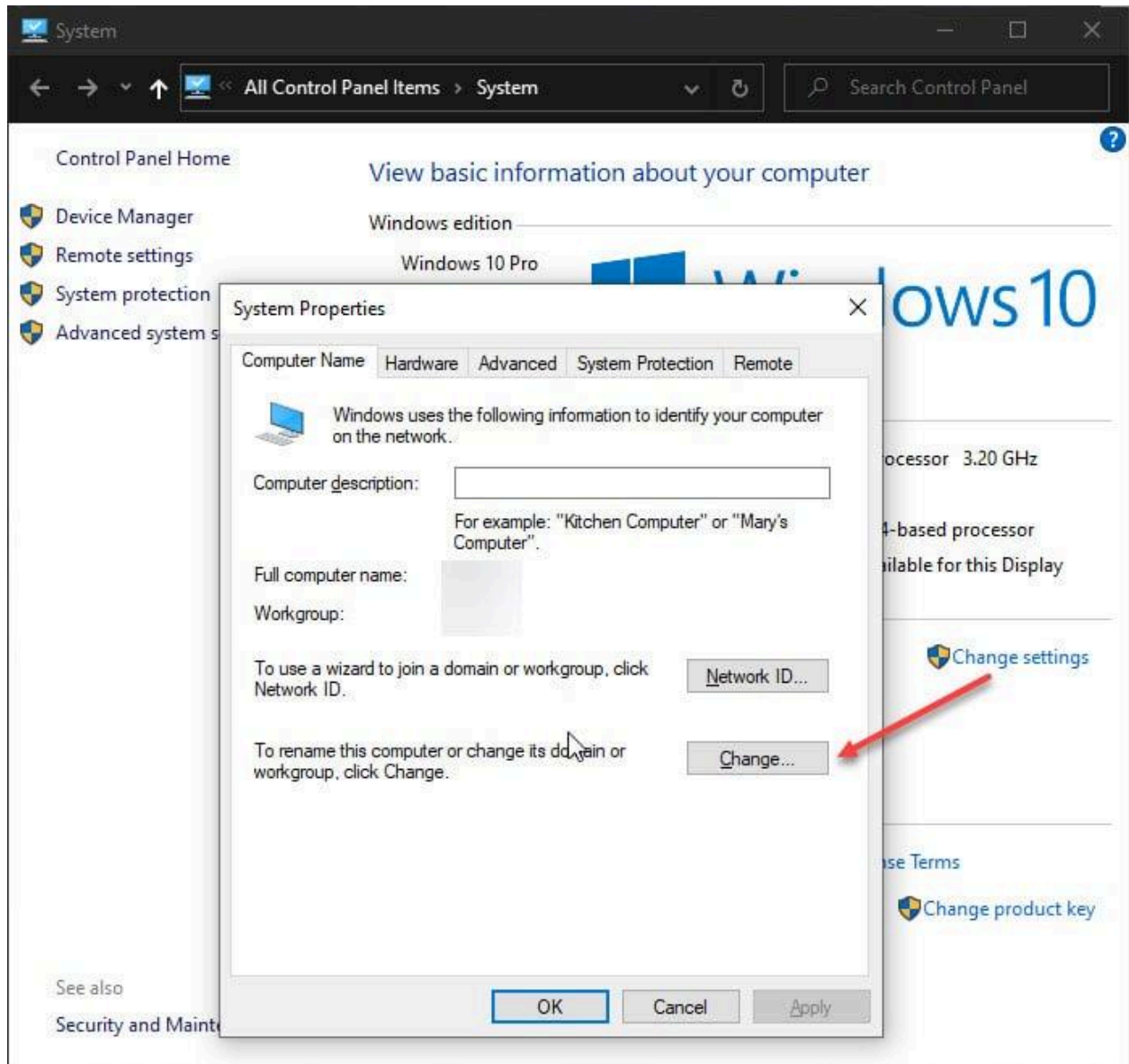
Go back to the 'root' folder and create a new sub folder called **PAGES**. In it add another web page similar to the last one but this time use a different message and save the file with the name '**test2.html**'. Use the client and try browsing for this page. What address did you use?

There is another major style of networking where resources are shared called peer-to-peer. Do some research and describe the difference between it and the server-client model of networking:

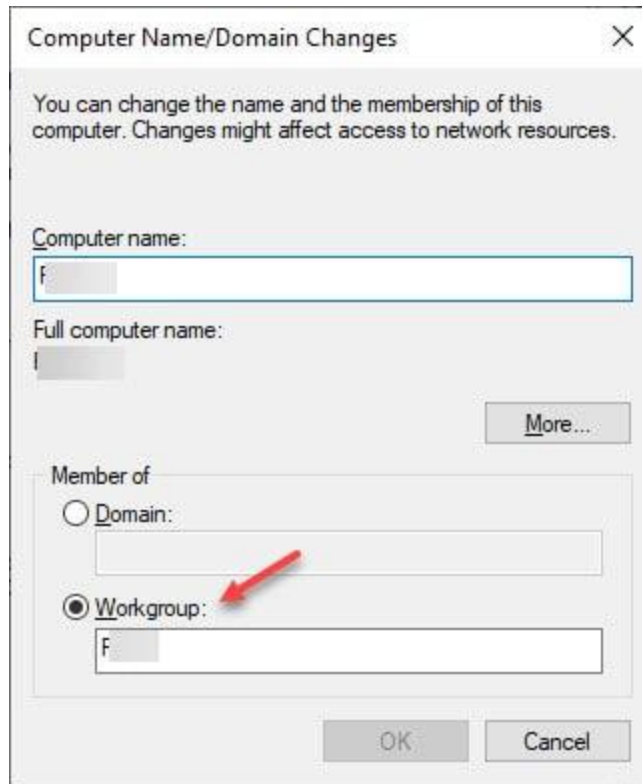
### **How To Setup A Peer-To-Peer Network In Windows 10?**

To share files across P2P networks, you first need to set up a network for the same. This can be done for both cabled and router connections, so follow these steps for **peer-to-peer network setup** for your workgroup on Windows 10:

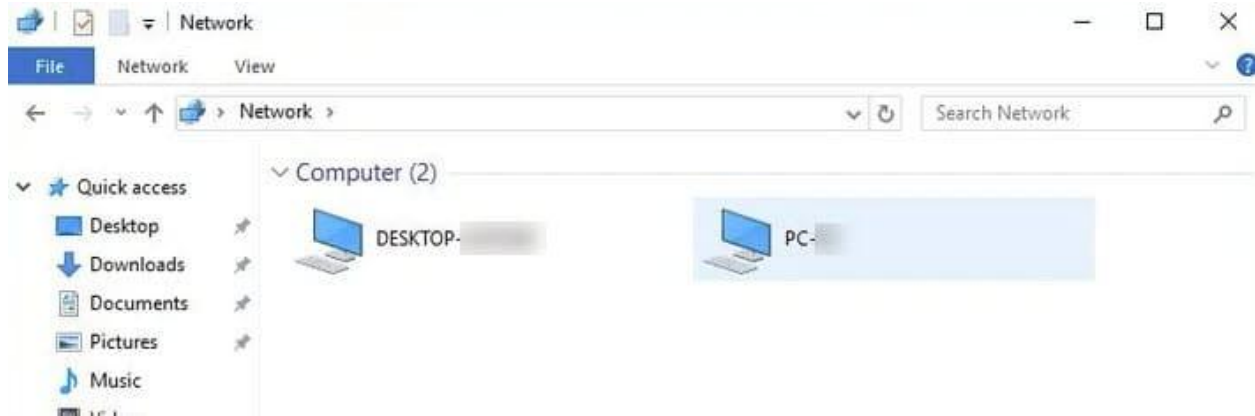
1. On your desktop, right-click on the **This PC** to reveal the context menu and select **Properties**. This should open a control panel window.
2. Locate and click on **Change Settings** in the window that opens. This will open a **System Properties**
3. Under the **Computer Name** tab, click on the **Change** button.



4. Click on the radio button next to how you wish to connect to the P2P network.  
If the network you wish to connect to has a domain, enter the name next to the **Domain** radio button.  
If you wish to connect through a local Workgroup, enter the name of the **Workgroup** after selecting the radio button for the same.



5. Click on **OK**. You will see a prompt for restarting your PC.
6. **Restart** your PC.
7. After your PC has rebooted, open **File Explorer**. You can use the keyboard shortcut **Win + E**.
8. From the left quick access menu, click on **Network**.
9. You should see the other computers on your Network in the top row. If you do not see your computers, you will instead be presented with a yellow bar saying **Network computers are not visible**. Click on this bar to change the settings.
10. Select **Turn on network discovery and file sharing**.
11. **Refresh** the explorer by pressing F5, or from the right-click context menu.

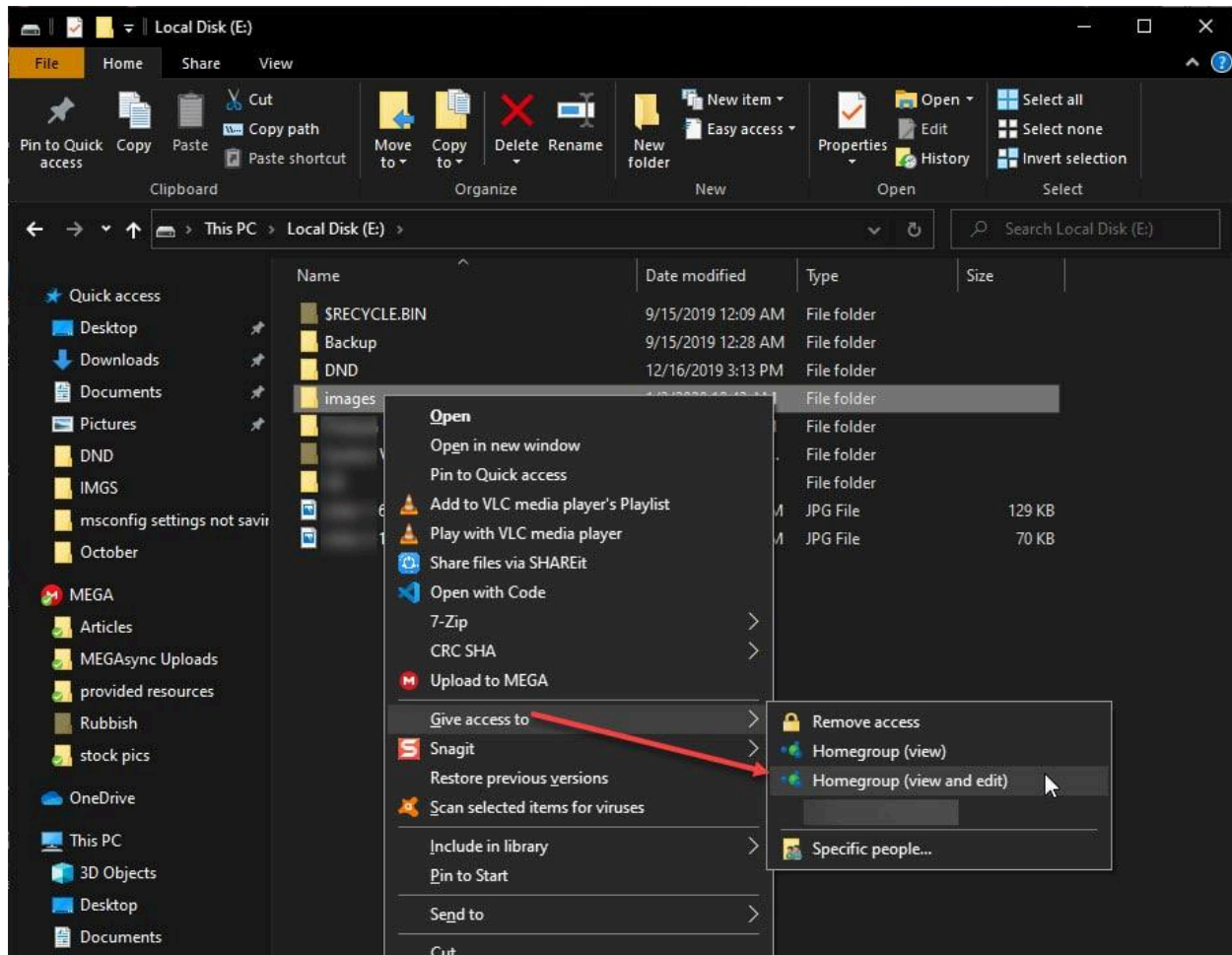


You should see all your computers present on the network now.

### How To Access Files On Another PC Using Peer To Peer Connection?

You can also access the files present on another PC on your network. To do this, you need to allow access to the file that you wish to share.

1. To share a file, open the folder of the file in **File Explorer**.
2. Right-click on the file that you wish to share to reveal the context menu.
3. Hover over '**Give access to**' to reveal additional settings. Select **Homegroup (view and edit)**.



4. On another PC, create a peer-to-peer network using the steps given above.
5. Double click on any PC to access the files on your PC.
6. **Enter the credentials** of the PC that you wish to gain access to and click on **OK**.
7. You will be able to see the folders that you shared in step 3.

Finally, let's have some fun using networks! Download any free LAN game (one will be provided to you if you can't find and/or download one... [PedalPower](#),

[Unreal Tournament](#)). Install the game on all computers connected to your LAN.  
Have fun and play!