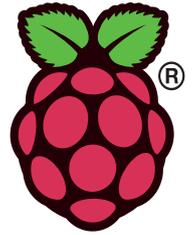


CLASSROOM CHALLENGE

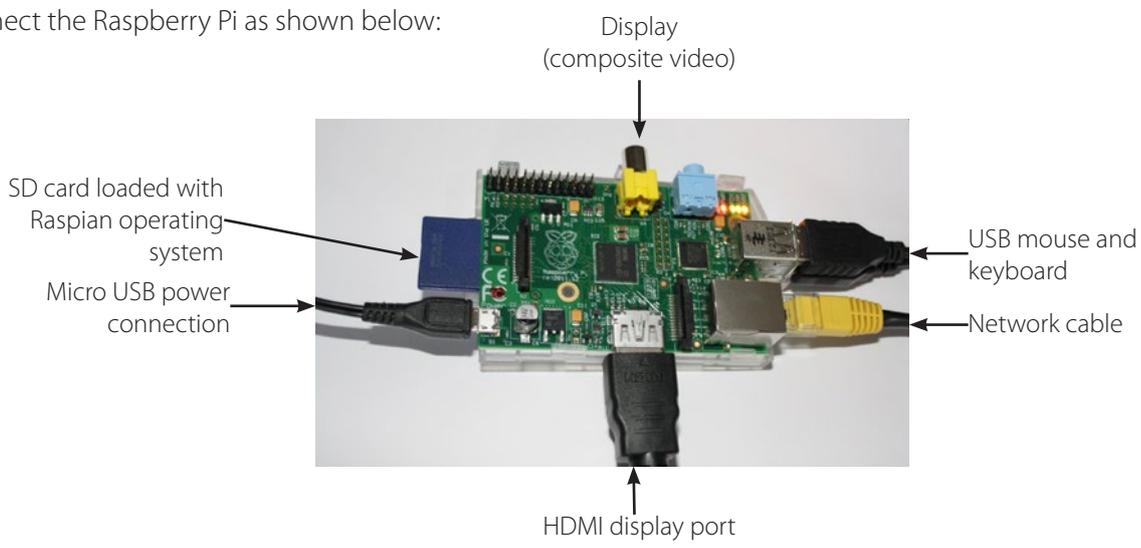


CONNECTING THE RASPBERRY PI TO A NETWORK

In this lesson you will learn how to connect the Raspberry Pi computer to a network with both a wired and a wireless connection. To complete this activity you will need to have access to a network connected to the internet or network equipment such as an integrated wireless router with switch ports.

TASK 1 (5 minutes)

Connect the Raspberry Pi as shown below:



Connect the network cable to a network port. This may be an integrated wireless router similar to what you may use in a home network. The switch ports are usually at the back of the device. Alternatively, you can plug your Raspberry Pi into a network hub or switch. The connector type is called **RJ45**. It will give a definite “click” when plugged in and you will see the Raspberry Pi’s network LED light up.

TASK 2 (10 minutes)

The next step is to check that the network device will provide the Raspberry Pi with an IP address automatically. You need to know that a **DHCP (Dynamic Host Configuration Protocol)** service is running on the integrated wireless router. It is usually on by default. We could assign a **static IP address** manually however, this is not usually done with client devices – only servers, network devices and printers because their IP address must not change and will be manually entered into client devices’ configuration.

LAN Settings	
LAN/WLAN MAC	00-1C-DF-22-46-13
IP Address	192.168.0.1 ← IP address of the router
Subnet Mask	255.255.255.0
DHCP Server	Enabled (3 LAN, 5 WLAN Clients) ← DHCP is enabled

To check that the Raspberry Pi has a valid IP address, open an **LX Terminal** session:



Type in the command: **ip addr**. You should see similar to the following output:

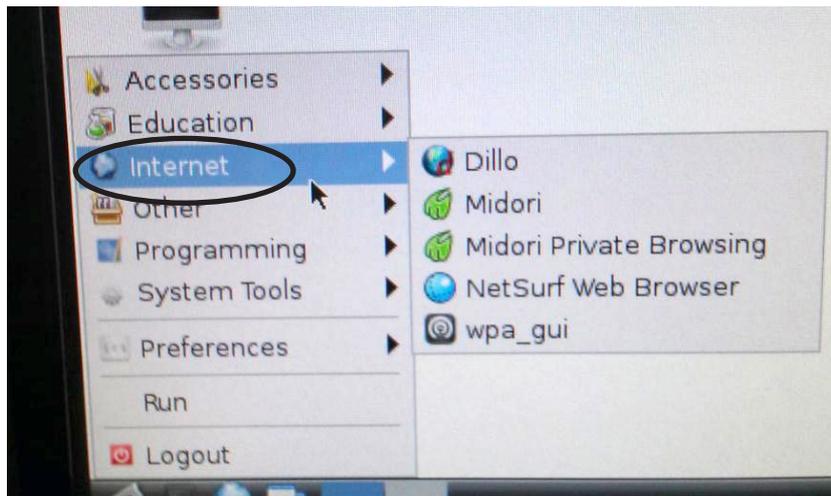
```
pi@raspberrypi:~  
File Edit Jobs Help  
pi@raspberrypi ~$  
pi@raspberrypi ~$ ip addr  
lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN  
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
  inet 127.0.0.1/8 scope host lo  
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql  
  n 1000  
  link/ether b8:27:eb:a3:31:f7 brd ff:ff:ff:ff:ff:ff  
  inet 192.168.0.14/24 brd 192.168.0.255 scope global eth0  
pi@raspberrypi ~$
```

This Raspberry Pi does have a valid IP address of **192.168.0.14** on the **192.168.0.0** network. The **broadcast address** for this network is **192.168.0.255**. This is the address that is used to send a message to all devices on the **192.168.0.0** network.

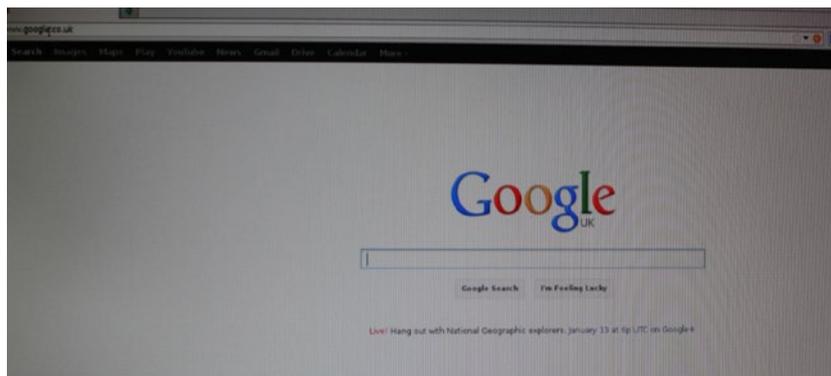
TASK 3 (10 minutes)

We will now test the network connection. If you are successfully connected to the network and your router connects to the internet, you can follow these steps:

- i) Select **internet** from the program menu.
- ii) Select the **Midori** compact browser.



- iii) Type a valid web address into the browser such as www.google.co.uk
- iv) If you have a successful connection, the webpage should be displayed.



If your connection is unsuccessful, check the following:

- That the cable is properly connected at both ends.
- That the **DHCP** service is turned on on the integrated wireless router.
- That the Raspberry Pi has received a valid IP address by using the **ip addr** command in LX Terminal.
- Ping the wireless router by typing: **ping ip address of router** in the **LX Terminal** window and see if you receive a response from the router. An example would be: **ping 192.168.0.1**

If none of these checks are successful, reboot the Raspberry Pi and start again.

```
pi@raspberrypi:~$ ping 10.96.10.1 -c 4
PING 10.96.10.1 (10.96.10.1) 56(84) bytes of data:
64 bytes from 10.96.10.1: icmp_req=1 ttl=255 time=13.2 ms
64 bytes from 10.96.10.1: icmp_req=2 ttl=255 time=8.60 ms
64 bytes from 10.96.10.1: icmp_req=3 ttl=255 time=7.55 ms
64 bytes from 10.96.10.1: icmp_req=4 ttl=255 time=7.14 ms

--- 10.96.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 7.148/9.138/13.250/2.433 ms
pi@raspberrypi:~$
```

This image shows a ping between a Raspberry Pi and the router which in this case, has an IP address of **10.96.10.1**. The **-c 4** option sends 4 packets and the echo replies are shown below with the time taken.

TASK 4 (approximately 10 minutes)

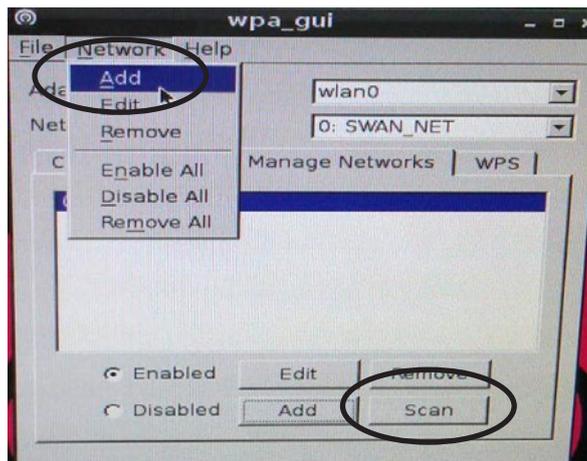
You are now going to connect the Raspberry Pi using a wireless connection. To do this you will need a USB wireless network adapter. Plug this into the Raspberry Pi and locate the WiFi configuration utility on the Raspberry Pi desktop:



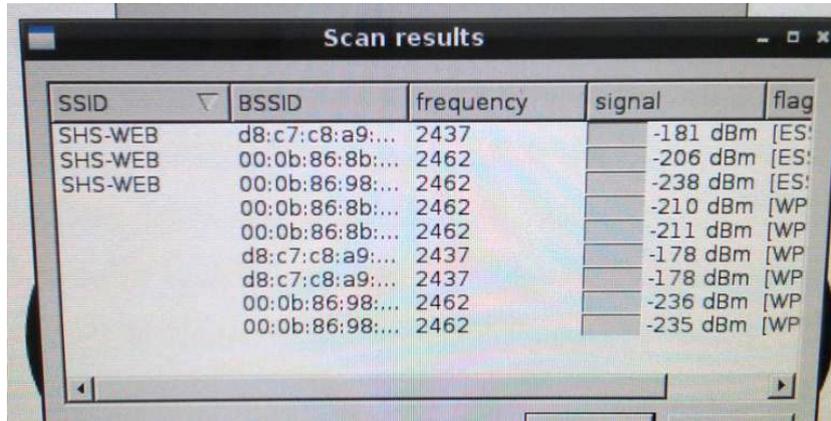
There are two methods for adding a new wireless network to the Raspberry Pi. The first is to scan for available networks and to select one from those available. The second is to manually add in all of the wireless network details.

To scan for an available network:

- i) Select the network tab from the utility.
- ii) Click the scan button.



iii) Select the network you wish to connect to.



SSID	BSSID	frequency	signal	flag
SHS-WEB	d8:c7:c8:a9:...	2437	-181 dBm	[ES:...
SHS-WEB	00:0b:86:8b:...	2462	-206 dBm	[ES:...
SHS-WEB	00:0b:86:98:...	2462	-238 dBm	[ES:...
	00:0b:86:8b:...	2462	-210 dBm	[WP...
	00:0b:86:8b:...	2462	-211 dBm	[WP...
	d8:c7:c8:a9:...	2437	-178 dBm	[WP...
	d8:c7:c8:a9:...	2437	-178 dBm	[WP...
	00:0b:86:98:...	2462	-236 dBm	[WP...
	00:0b:86:98:...	2462	-235 dBm	[WP...

To manually add a wireless network:

- i) You will need to know the following information: the **SSID (Service Set Identifier)** for the network (network name), what type of **authentication** is used on the network e.g. none (**open**), **WEP (Wired Equivalent Privacy)**, **WPA (WiFi Protected Access)** or **WPA2**. For **WEP, WPA or WPA2** networks, the type of **encryption** used and you must also know the **network key** (password). WEP is not considered to be very secure as it uses a static key to encrypt packets. WPA is more secure and uses a type of encryption called TKIP (Temporal Key Integrity Protocol). More modern devices will support WPA2 which uses a type of encryption called AES (Advanced Encryption Standard). This is sufficiently secure for most home and small business networks. AES applies a number of complex operations on the data being sent across the wireless network making it far less likely to be decrypted by hackers.

Wireless > Security

Security Mode > WPA/WPA2-Personal (PSK) ▾

Authentication > WPA-PSK+WPA2-PSK ▾

Encryption Technique > TKIP+AES ▾

This setting will support older WPA and more modern WPA2 devices

Pre-shared Key (PSK) >

Obscure PSK

WPA-PSK (no server): Wireless Protected Access with a Pre-Shared Key. The key is a password, in the form of a word, phrase or series of letters and numbers. The key must be between 8 and 63 characters long and can include spaces and symbols, or 64 Hex (0-F) only. Each client that connects to the network must use the same key (Pre-Shared Key). [More Info](#)

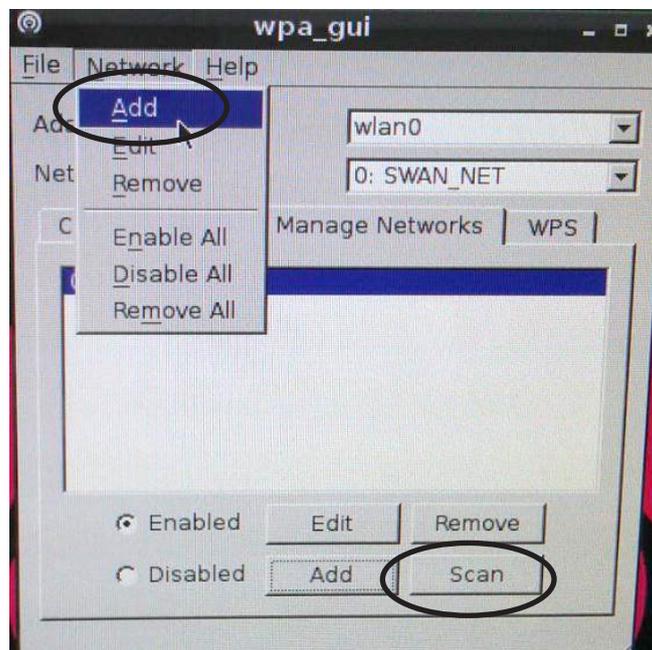
Clear Changes

Apply Changes

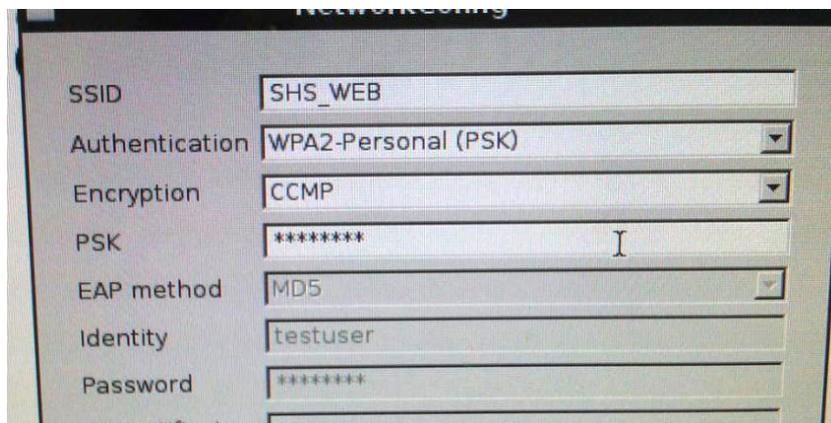
ii) Complete the following table with these details:

SSID	
Authentication	
Encryption	
Network key	
IP address of Wireless Access Point	

iii) Select add network.



iv) Enter in the details from your table above into the dialogue box then click OK.



Repeat Task 3 (above) to verify that you have established a functioning wireless network connection. Use a test plan to ensure that you record the outcomes of testing your network.

Test plan

ADDITIONAL ACTIVITIES (40 minutes)

Answer the following questions:

- a) Research and explain the process of a client device obtaining an IP address from the DHCP server running on the wireless router.
- b) Find out which is the most secure wireless network from WEP, WPA and WPA2. What are the differences between them?
- c) Produce a simple troubleshooting guide to Raspberry Pi networking.