

Module Code: CS2CA17

Assignment report Title: Internet Control Message Protocol (ICMP) and Small Network configuration

Student Number: 3002069

Date (when the work completed): 2/12/2022

Actual hrs spent for the assignment: 6

Assignment evaluation (3 key points):

- Learnt how to use Wireshark to capture and analyse ICMP data.
- Learnt how to use Cisco Packet Tracer to set up a small office
- The assignment brief was clear and very helpful in making me understand the task

## **Introduction**

In this coursework there are three questions that will be answered in this report. The first question is the use of Wireshark to capture and analyse LAN and Remote Internet Control Message Protocol (ICMP) data. The second question is the use of a software called Cisco Packet Tracer which is a simulation tool to help configure and visualise network logical and physical mode, the task was to create/configure a small office Local Area Network (LAN) by setting up five PCs, 1 printer, wireless router, 1 mobile and 1 tablet PC through a Dynamic Host Configuration Protocol (DHCP) server and a default gateway Internet Service Provider (ISP) to connect all the devices together to internet and make communication between them. The final task was to install/set up a Domain Name System (DNS) server and a Hypertext Transfer Protocol (HTTP) server to create a mapping between a website and the HTTP server to check if the devices get connection and gain access.

## Use of Wireshark

```
Microsoft Windows [Version 10.0.19042.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ez020691>ipconfig -all

Windows IP Configuration

   Host Name . . . . . : JOBB8S
   Primary Dns Suffix . . . . . : rdg.ac.uk
   Node Type . . . . . : Hybrid
   IP Routing Enabled. . . . . : No
   WINS Proxy Enabled. . . . . : No
   DNS Suffix Search List. . . . . : rdg.ac.uk
                                       private.rdg.ac.uk
                                       reading.ac.uk

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . : rdg.ac.uk
   Description . . . . . : Intel(R) Ethernet Connection (7) I219-LM
   Physical Address. . . . . : D4-5D-64-23-0A-19
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e8b2:fbf8:d752:c01b%12(Preferred)
   IPv4 Address. . . . . : 134.225.216.144(Preferred)
   Subnet Mask . . . . . : 255.255.252.0
   Lease Obtained. . . . . : 30 November 2022 00:24:15
   Lease Expires . . . . . : 01 December 2022 00:29:42
   Default Gateway . . . . . : fe80::2a8a:1cff:fe04:83c1%12
                               134.225.216.254
   DHCP Server . . . . . : 134.225.214.15
   DHCPV6 IAID . . . . . : 114580836
   DHCPV6 Client DUID. . . . . : 00-01-00-01-2A-85-54-6A-D4-5D-64-23-0A-19
   DNS Servers . . . . . : 134.225.254.48
   Primary WINS Server . . . . . : 134.225.32.179
   Secondary WINS Server . . . . . : 134.225.32.178
   NetBIOS over Tcpip. . . . . : Enabled
   Connection-specific DNS Suffix List :
       rdg.ac.uk
       private.rdg.ac.uk
       reading.ac.uk
```

Figure 1 IP Address

```
Microsoft Windows [Version 10.0.19042.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ez020691>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . : rdg.ac.uk
   Link-local IPv6 Address . . . . . : fe80::aebb:505f:d1af:254b%11
   IPv4 Address. . . . . : 134.225.217.141
   Subnet Mask . . . . . : 255.255.252.0
   Default Gateway . . . . . : fe80::2a8a:1cff:fe04:83c1%11
                               134.225.216.254

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix . : 
   Link-local IPv6 Address . . . . . : fe80::14d9:5ee0:908c:9f12%9
   IPv4 Address. . . . . : 192.168.56.1
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix . : 
   Link-local IPv6 Address . . . . . : fe80::7c9:f2d4:339e:5865%34
   Autoconfiguration IPv4 Address. . : 169.254.151.33
   Subnet Mask . . . . . : 255.255.0.0
   Default Gateway . . . . . :
```

Figure 4 LAN IP Address

```
C:\Users\ez020691>ping www.reading.ac.uk

Pinging wap-slb-vip.rdg.ac.uk [134.225.0.151] with 32 bytes of data:
Reply from 134.225.0.151: bytes=32 time=1ms TTL=61
Reply from 134.225.0.151: bytes=32 time=1ms TTL=61
Reply from 134.225.0.151: bytes=32 time=1ms TTL=61
Reply from 134.225.0.151: bytes=32 time=1ms TTL=61

Ping statistics for 134.225.0.151:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\ez020691>
```

Figure 5 Ping to a local pc using the IP 134.225.216.170

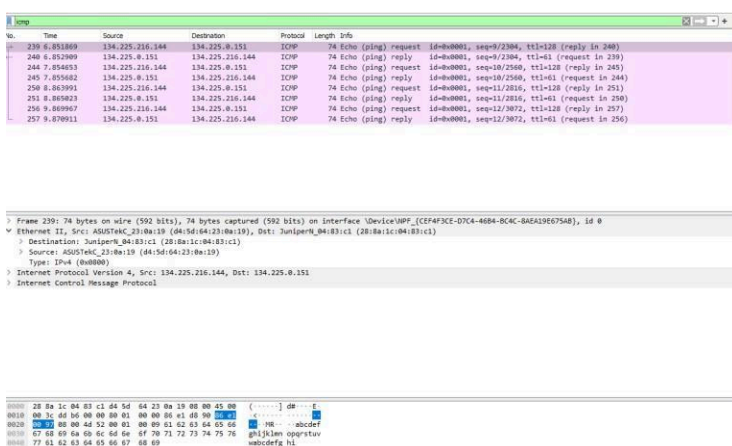


Figure 3 Data Capture of [www.reading.ac.uk](http://www.reading.ac.uk) using Wireshark

Figure 6 Data Capture of pinging 134.225.216.170 using Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
384	20.036495	134.225.216.170	134.225.217.141	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 385)
385	20.036695	134.225.217.141	134.225.216.170	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 (request in 384)
391	21.047494	134.225.216.170	134.225.217.141	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 392)
392	21.047679	134.225.217.141	134.225.216.170	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 (request in 391)
405	22.054546	134.225.216.170	134.225.217.141	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 406)
406	22.054731	134.225.217.141	134.225.216.170	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=128 (request in 405)
431	23.065269	134.225.216.170	134.225.217.141	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 432)
432	23.065342	134.225.217.141	134.225.216.170	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=128 (request in 431)

> Frame 384: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{BC22CD43-7E96-4FD9-837E-A3ECC8D5CC99}, id 0  
 > Ethernet II, Src: ASUSTekC\_23:0b:51 (d4:5d:64:23:0b:51), Dst: ASUSTekC\_bf:b7:1c (0c:1d:92:bf:b7:1c)  
 > Internet Protocol Version 4, Src: 134.225.216.170, Dst: 134.225.217.141  
 > Internet Control Message Protocol

```

0000  0c 9d 92 bf b7 1c d4 5d 64 23 0b 51 08 00 45 00  ....] d#Q·E:
0010  00 3c 74 c7 00 00 00 01 05 ff 06 e1 d8 aa 86 e1  -Ct-----
0020  d9 8d 08 00 4d 56 00 01 00 05 61 62 63 64 65 66  -...MV...·abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklm opqrstu
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

*Figure 7 Data Capture of ping from another local pc*

## Task 1 Definition of ICMP

ICMP stands for Internet Control Message Protocol is a network level protocol. ICMP messages communicate information about network connectivity issues back to the source of the compromised transmission. It sends control messages such as destination network unreachable, source route failed and source quench.

### Examine IP and MAC address from the LAN and Remote Host

When examining the difference between the LAN and remote, I found that there is less delay and latency on the signal that travels on the LAN host. On the remote host there is a bit of delay and latency when the signal travels back and forth, the website that is being pinged is [www.reading.ac.uk](http://www.reading.ac.uk) (Figure 3). From Wireshark I found that the IP [www.reading.ac.uk](http://www.reading.ac.uk) is 134.225.0.151 and the MAC address of the website is JuniperN\_04:83:c1 (28:8a:1c:04:83:c1).

### Significant about this information

What makes this information significant is that the IP and MAC address that is shown in the Wireshark is the same IP that is shown in the command prompt when pinged the [www.reading.ac.uk](http://www.reading.ac.uk) website. Figure 1, 2 and 3

### Reflection about MAC address

When pinged a device connected to the same network, such as Wi-Fi, Wireshark would display the MAC address; but, if you ping a website, the MAC address would be encrypted. This is how I understand MAC addresses in terms of local hosts.

## Small Office Network (Cisco Packet Tracer)

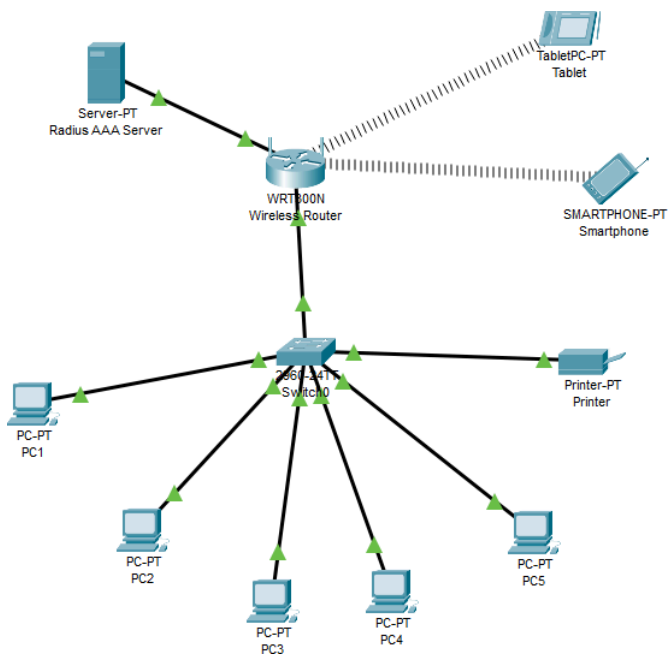


Figure 8 Small Office Network Configuration using Packet Tracer

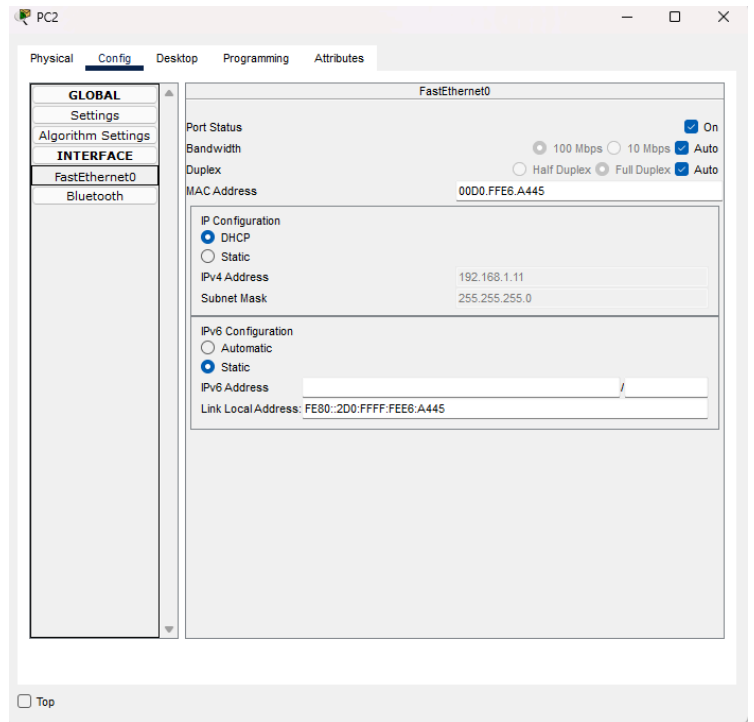


Figure 10 Configuration of PC2

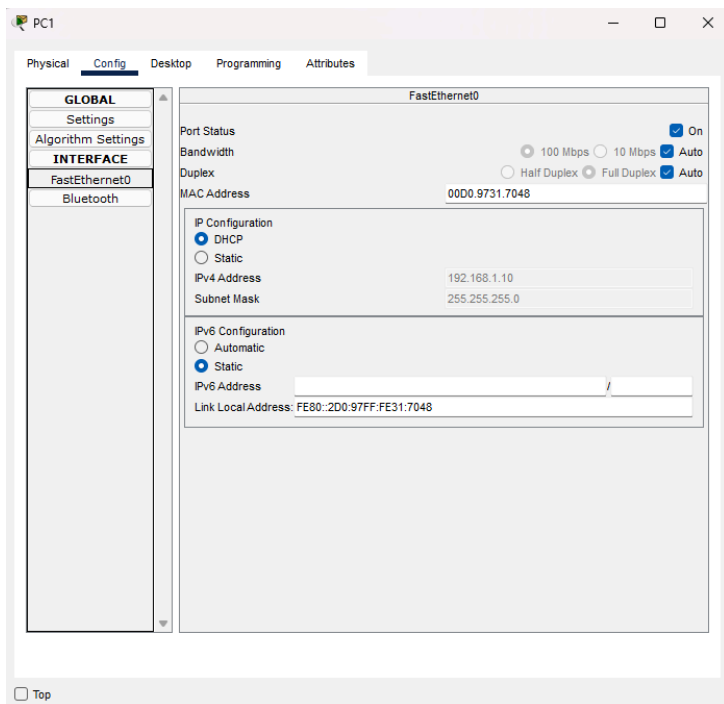


Figure 9 Configuration of PC1

Figure 11 Configuration of PC3

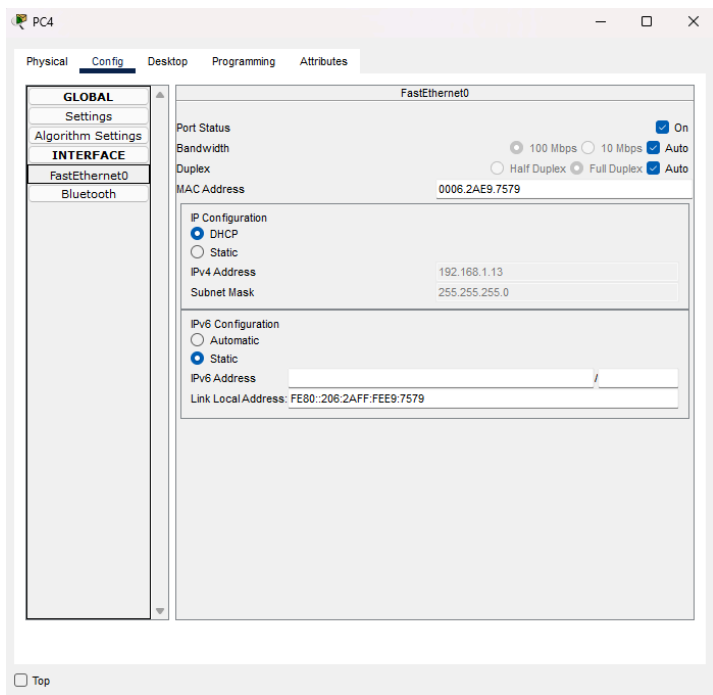


Figure 12 Configuration PC4

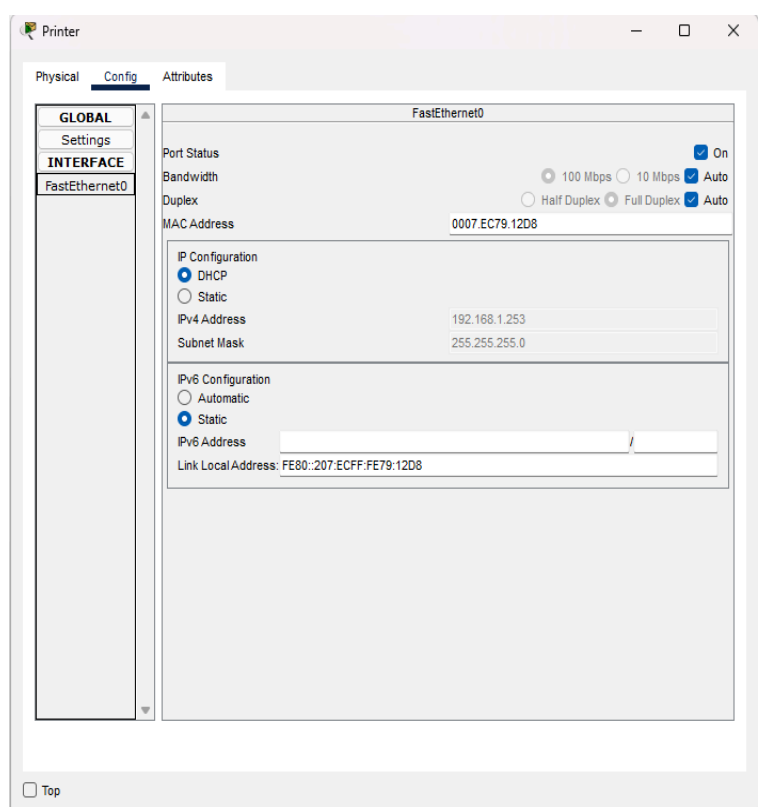


Figure 14 Configuration Printer

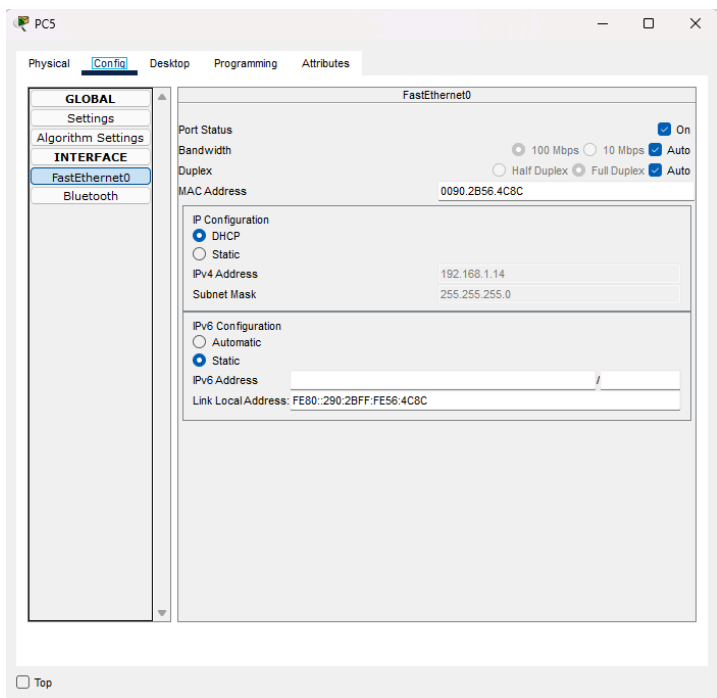


Figure 13 Configuration PC5

Figure 15 Configuration Smartphone

The screenshot shows the 'Tablet' configuration window with the 'Config' tab selected. The left sidebar has a tree view with 'GLOBAL' (Settings, Algorithm Settings) and 'INTERFACE' (Wireless0, 3G/4G Cell1, Bluetooth). The 'Wireless0' interface is selected, showing the following settings:

- Port Status:** On (checked)
- Bandwidth:** 300 Mbps
- MAC Address:** 0007.EC54.BDEA
- SSID:** pollyvacherwireless
- Authentication:**
  - ☐ Disabled
  - ☐ WEP
  - ☐ WPA-PSK
  - ☐ WPA
  - ☒ WPA2
  - ☐ 802.1X
- WEP Key:** (empty field)
- PSK Pass Phrase:** (empty field)
- User ID:** Tablet
- Password:** 321
- Method:** MD5 (dropdown)
- User Name:** (empty field)
- Password:** (empty field)
- Encryption Type:** AES (dropdown)
- IP Configuration:**
  - ☒ DHCP
  - ☐ Static
- IPv4 Address:** 192.168.1.102
- Subnet Mask:** 255.255.255.0

Figure 16 Configuration Tablet

The screenshot shows the 'Wireless Router' configuration window with the 'Config' tab selected. The left sidebar has a tree view with 'Internet Setup' and 'Network Setup'. The 'Network Setup' section is expanded, showing the 'Router IP' and 'DHCP Server Settings'.

- Internet Setup:**
  - Internet Connection type:** Automatic Configuration - DHCP (dropdown)
  - Optional Settings (required by some internet service providers):**
    - Host Name:** (empty field)
    - Domain Name:** (empty field)
    - MTU:** (dropdown) Size: 1500
- Network Setup:**
  - Router IP:**
    - IP Address:** 192 . 168 . 1 . 1
    - Subnet Mask:** 255.255.255.0 (dropdown)
  - DHCP Server Settings:**
    - DHCP Server:** ☒ Enabled ☐ Disabled
    - DHCP Reservation:** (button)
    - Start IP Address:** 192.168.1.100
    - Maximum number of Users:** 50
    - IP Address Range:** 192.168.1.100 - 149
    - Client Lease Time:** 0 minutes (0 means one day)
    - Static DNS 1:** 0 . 0 . 0 . 0
    - Static DNS 2:** 0 . 0 . 0 . 0
    - Static DNS 3:** 0 . 0 . 0 . 0

Figure 17 Configuration of Wireless Router DHCP Reservation

Figure 18 Configuration of Wireless Router DHCP Reservation

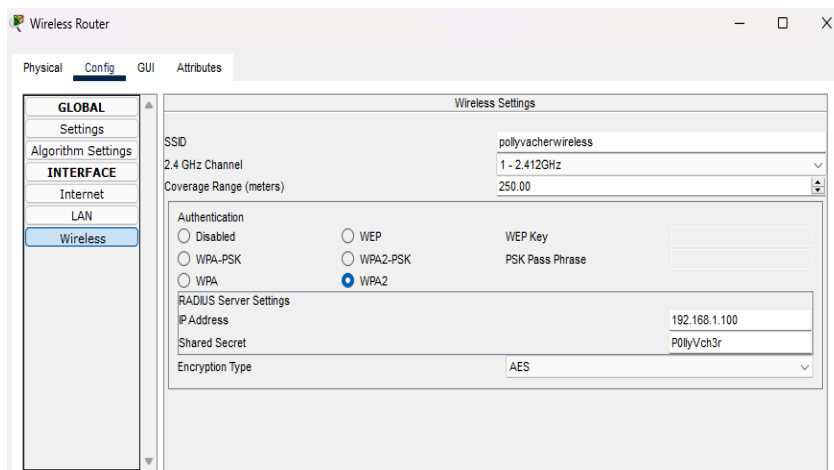


Figure 19 Configuration Wireless Router

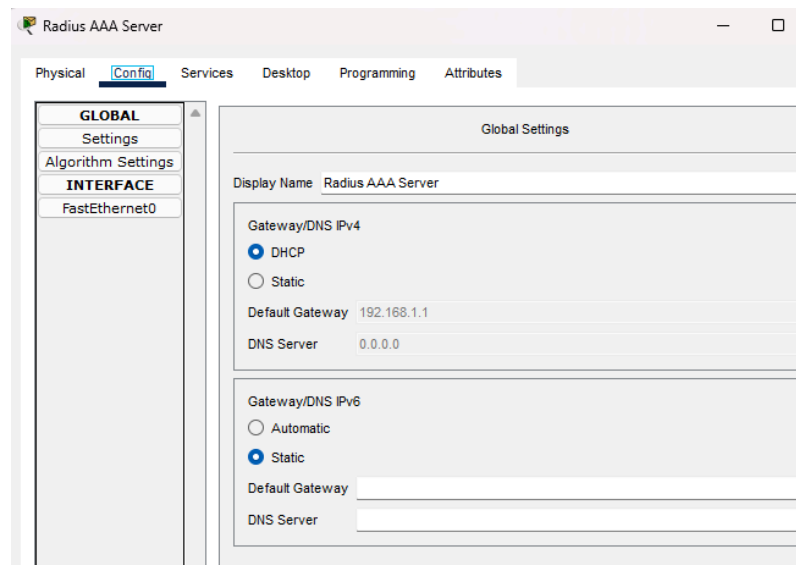


Figure 20  
Configurat  
ion AAA  
Server

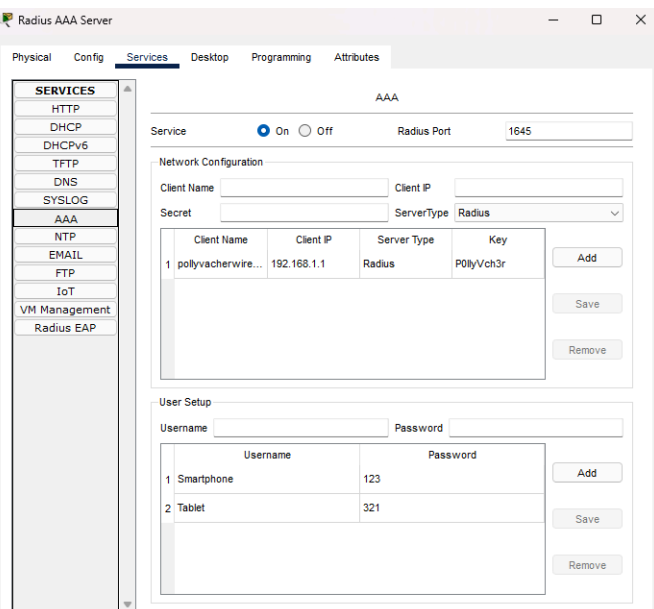


Figure 21 Services AAA Server



```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

*Figure 22 Ping PC-PC*

```

C:\>
ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:

Reply from 192.168.1.101: bytes=32 time=16ms TTL=128
Reply from 192.168.1.101: bytes=32 time=11ms TTL=128
Reply from 192.168.1.101: bytes=32 time=10ms TTL=128
Reply from 192.168.1.101: bytes=32 time=12ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 16ms, Average = 12ms

```

*Figure 23 Ping PC-Smartphone*

## Task 2

### Small Office Network

Using Cisco Packet Tracer, the goal was to configure a small office LAN which contains 5 PCs, 1 Printer which they are connected using a copper straight through wire to a switch using FastEthernet port. The wireless router is also connected to the switch using the same copper straight through wire into a gigabitEthernet port. The mobile (smartphone) and tablet PC are both connected to the wireless router. To ensure they are connected and are communicating with the PC the router serves as the DHCP, and default gateway provided by the ISP so that all the devices are connected to the internet.

The PCs and Printer were configured with certain IP addresses and subnet masks as shown in figure 9-14. This is done by using the wireless router and setting up a DHCP reservation for each device as shown in figure 17 and 18. The wireless router also had a SSID (pollyvacherwireless), WPA2 Enterprise AES connection with a shared secret key (PollyVch3r) as shown in figure 19, this is used to connect to the Radius AAA server which allows it to create a network configuration of a username and password which will be used to connect to the mobile devices and tablet PC (Figure 15, 16, 20 and 21).

To ensure that the devices can communicate and send signals to each other there was a PING command used on one of the devices to another device to show they are communicating. PING command was also used to show that the PCs can communicate with the wireless smartphone and tablet PC as it is shown in figure 22 and 23.

# DNS and HTTP Server Setup

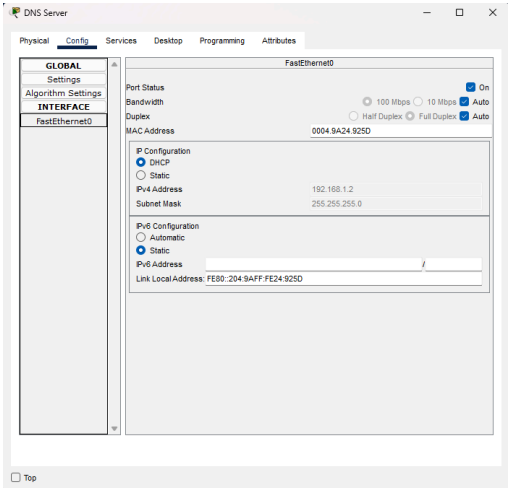
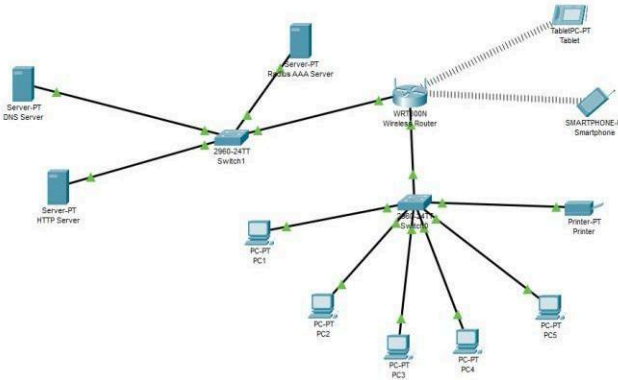


Figure 24 Small Office Network

Figure 25

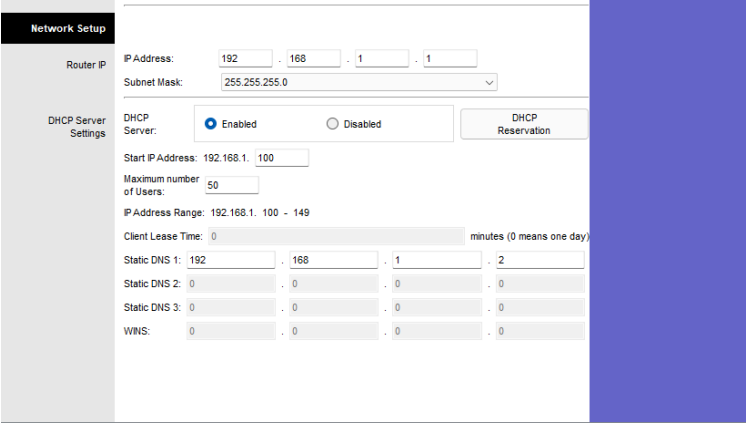
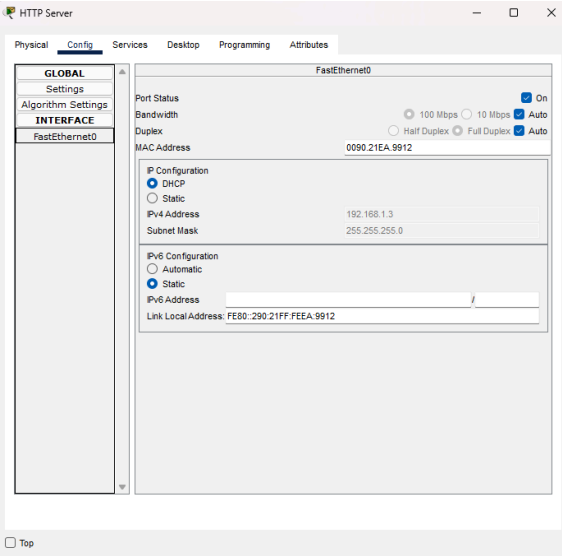


Figure 26

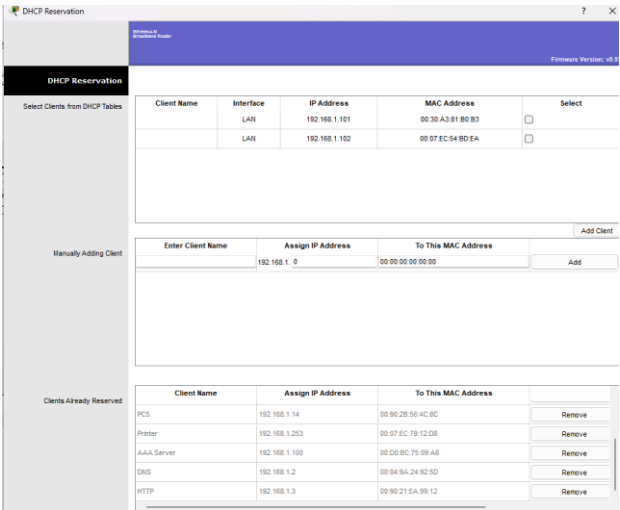


Figure 29

Figure 28

```
Cisco Packet Tracer PC Command Line 1.0
C:\>nslookup

Server: [192.168.1.2]
Address: 192.168.1.2

>
```

Figure 30



Figure 31

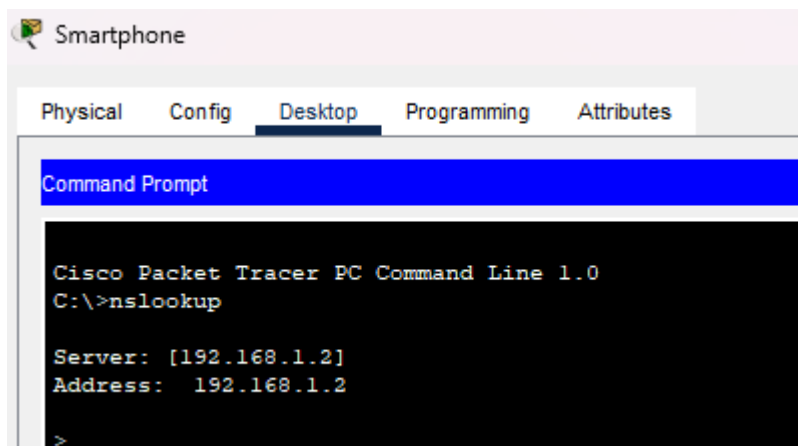


Figure 32

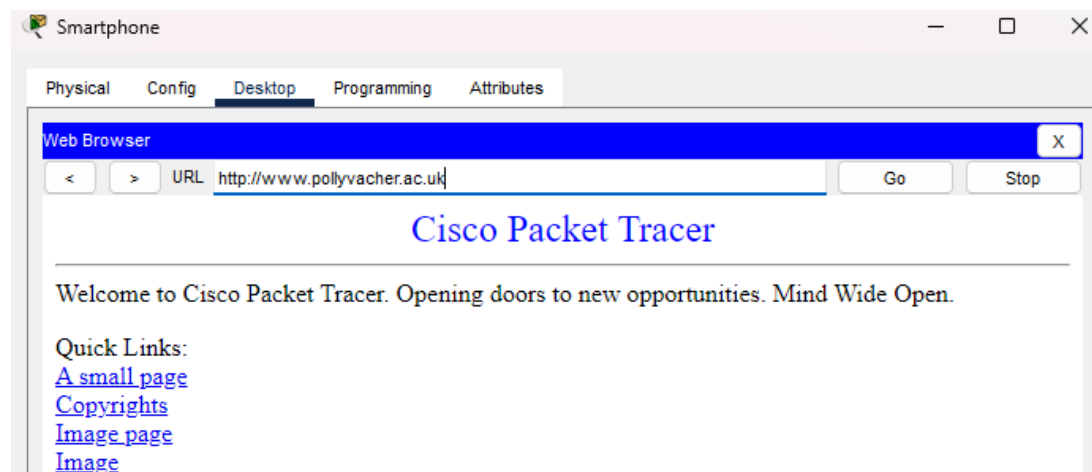


Figure 33

### **Task 3**

#### **DNS and HTTP Server Setup**

Domain Name System (DNS) server and Hypertext Transfer Protocol (HTTP) server were configured to create a mapping between [www.pollyvacher.ac.uk](http://www.pollyvacher.ac.uk) and the HTTP server. This is done by updating the DHCP configuration to reserve the IP address in the wireless router. Figure 25, 26, 27 and 28.

Figure 29 shows the website link [www.reading.ac.uk](http://www.reading.ac.uk) and the address to 192.168.1.3 which is the HTTP server to request content.

Figure 30, 31, 32 and 33 shows the nslookup to find out the corresponding DNS record. As shown in the figure both the PCs and the Smartphone can access and retrieve data from the web browser.

#### **Discussion, Conclusion and Personal Reflection**

During this coursework, I have learnt to ping websites to be able to find and identify the IP and MAC address of both the remote and the website. Another key skill I have learnt was how to use and understand the Cisco Packet Tracer by creating a small office LAN and getting the devices to communicate with each other using different commands.

Section (# marks)	Students own assessment	Marks
1. (30 marks)	<b>Wireshark</b> <input checked="" type="checkbox"/> Definition of ICMP <input checked="" type="checkbox"/> Examine IP and MAC address from LAN and Remote Host <input checked="" type="checkbox"/> Significant about this information <input checked="" type="checkbox"/> Reflection about MAC address	(total 30) 5 10 5 10
2. (25 marks)	<b>Small Office Network</b> <input checked="" type="checkbox"/> All devices connection <input checked="" type="checkbox"/> All devices IP configuration <input checked="" type="checkbox"/> DHCP server configuration <input checked="" type="checkbox"/> Wireless router and AAA server setup <input checked="" type="checkbox"/> Connectivity tests (x2)	(total 25) 5 5 5 5 5
3. (25 marks)	<b>DNS and HTTP Servers</b> <input checked="" type="checkbox"/> All devices connection and IP configuration <input checked="" type="checkbox"/> DNS Server configuration <input checked="" type="checkbox"/> HTTP Server configuration <input checked="" type="checkbox"/> DNS resolution tests (x2) <input checked="" type="checkbox"/> HTTP service tests (x2)	(total 25) 5 5 5 5 5
4. (20 marks)	<b>Quality of the submitted report</b> <input checked="" type="checkbox"/> Introduction <input checked="" type="checkbox"/> Detailed WireShark testing with screenshots <input checked="" type="checkbox"/> Small Office Network Setup with tests <input checked="" type="checkbox"/> DNS and HTTP Servers Setup with tests <input checked="" type="checkbox"/> Discussion, conclusion, and personal reflection	(total 20) 2 5 5 5 3
5. (5 marks)	Bonus marks for: <input type="checkbox"/> Use of custom domain names (say, <a href="http://pc1.pollyvacher.ac.uk">pc1.pollyvacher.ac.uk</a> ) for PCs in connectivity tests.	(total 5) 5

## References

*ICMP: Definition & How it Works* | *Protocol Support Library* | *ExtraHop*. (2021). Extrahop. Retrieved 1 December 2022, from <https://www.extrahop.co.uk/resources/protocols/icmp/>