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 . . . . . . . . . . . . : JOBBS
   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 06:29:42
   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 Search 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 2 Ping www.reading.ac.uk

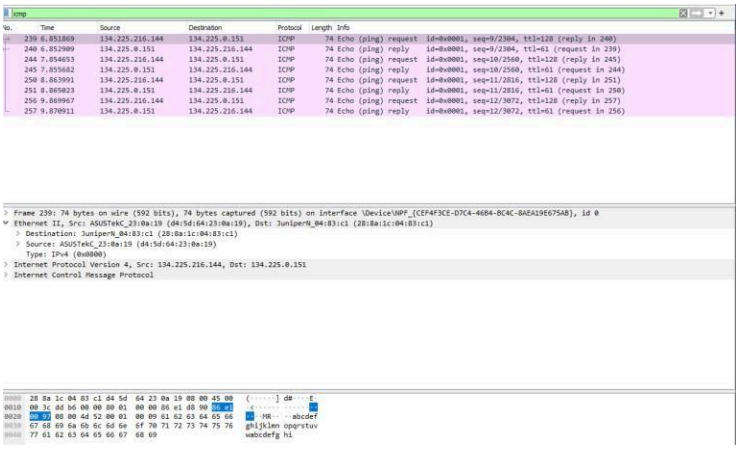


Figure 3 Data Capture of www.reading.ac.uk using Wireshark

Figure 6 Data Capture of pinging 134.225.216.170 using Wireshark

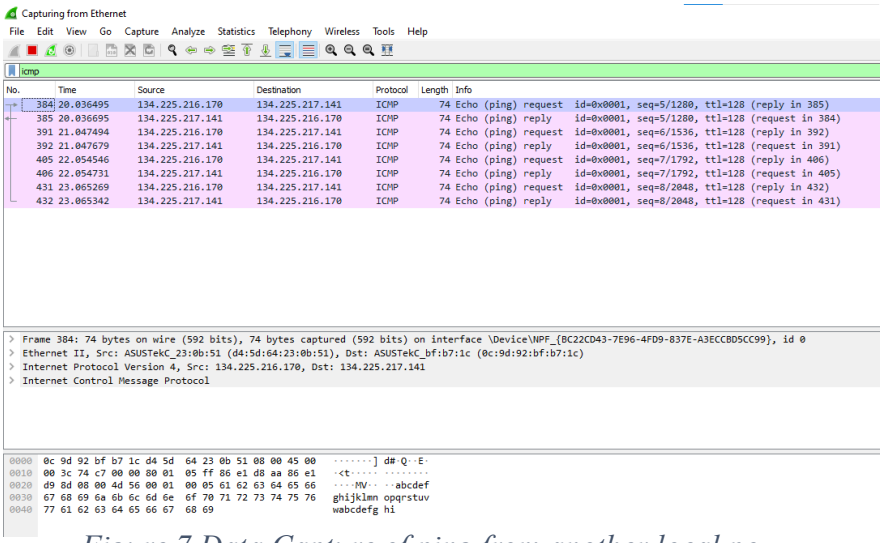


Figure 7 Data Capture of ping from another local pc

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 (Figure 3). From Wireshark I found that the IP 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 website. Figure 1, 2 and 3

Reflection about MAC address

When pinging 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)

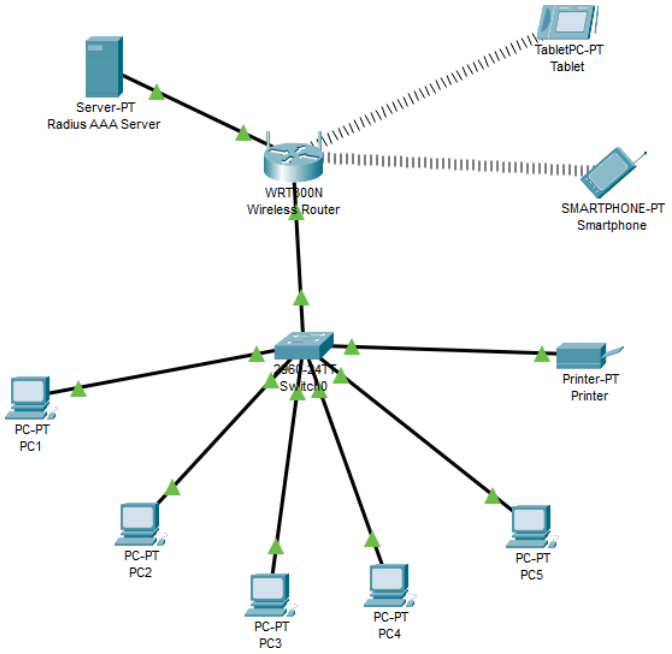


Figure 8 Small Office Network Configuration using Packet Tracer

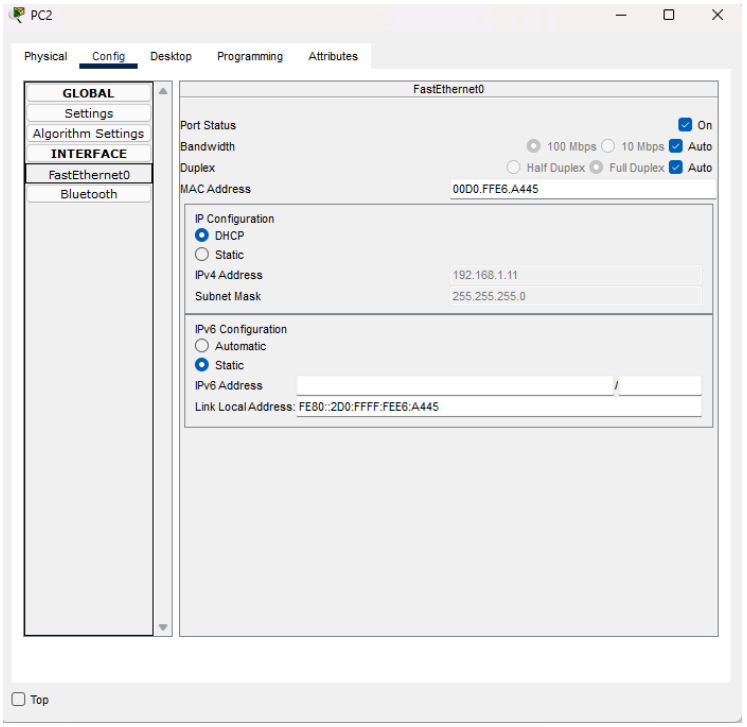


Figure 10 Configuration of PC2

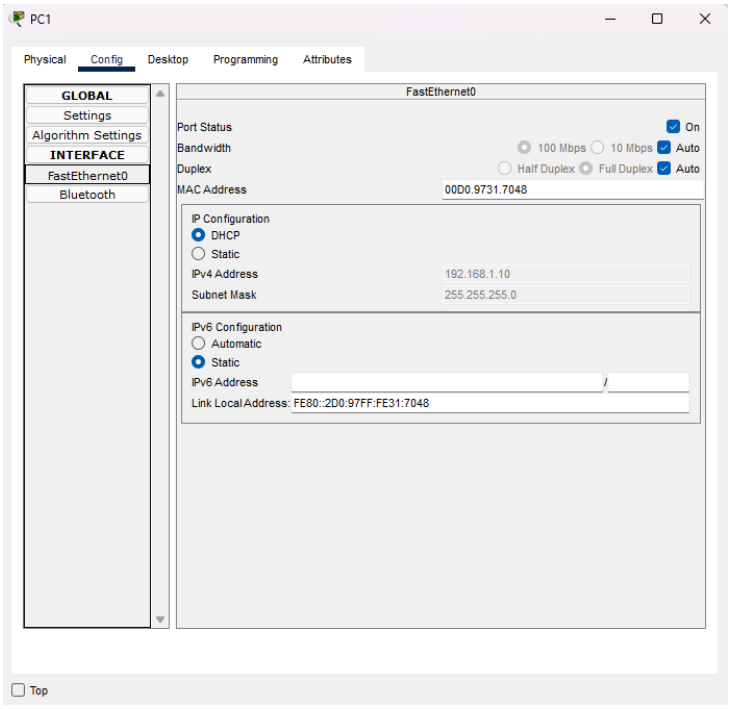


Figure 9 Configuration of PC1

Figure 11 Configuration of PC3

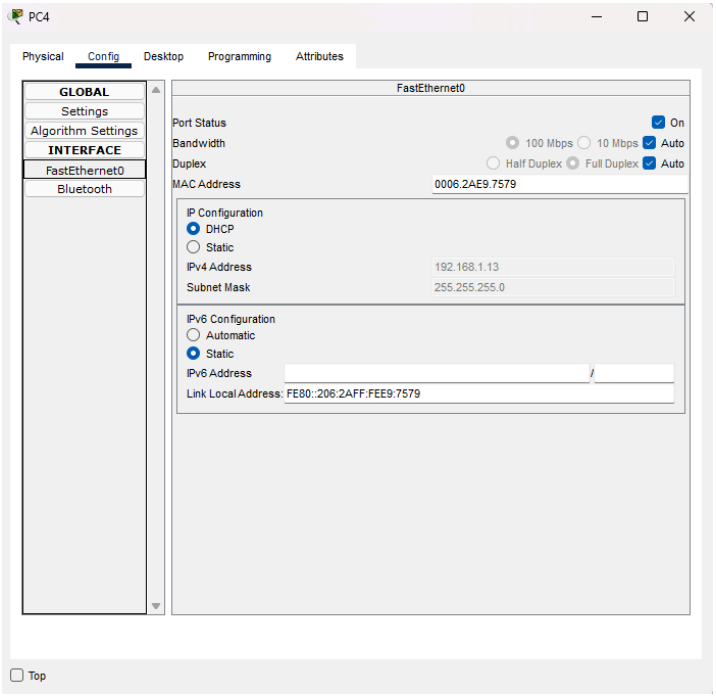


Figure 12 Configuration PC4

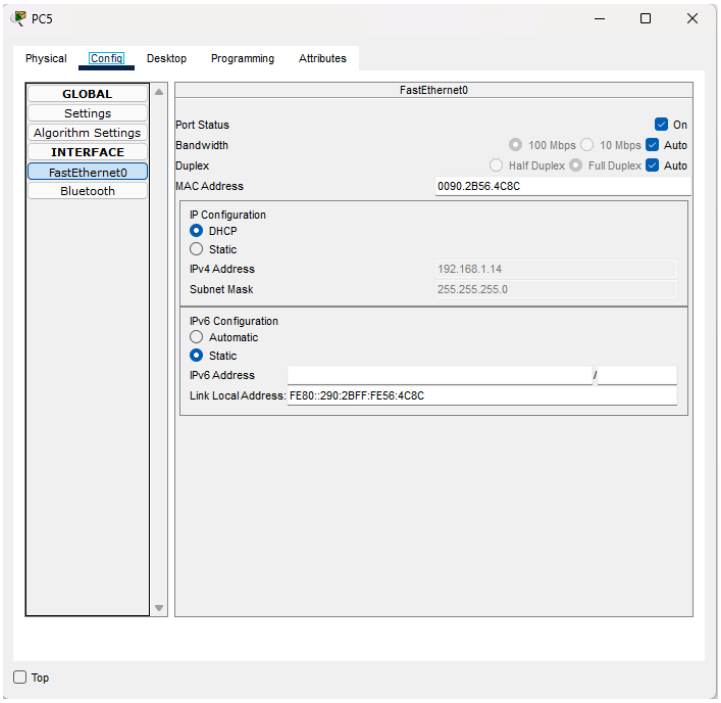


Figure 13 Configuration PC5

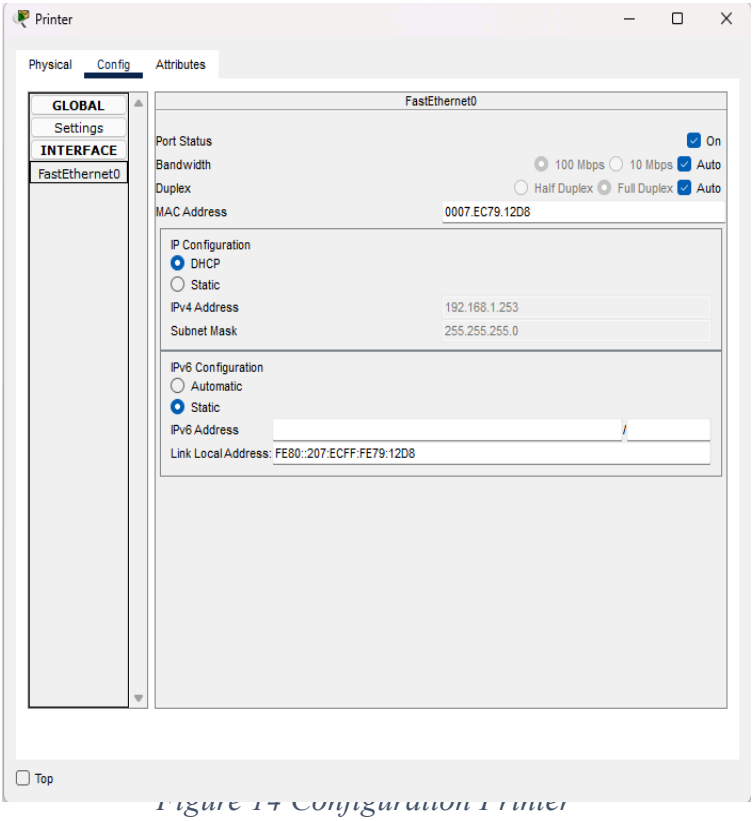


Figure 14 Configuration Printer

Figure 15 Configuration Smartphone

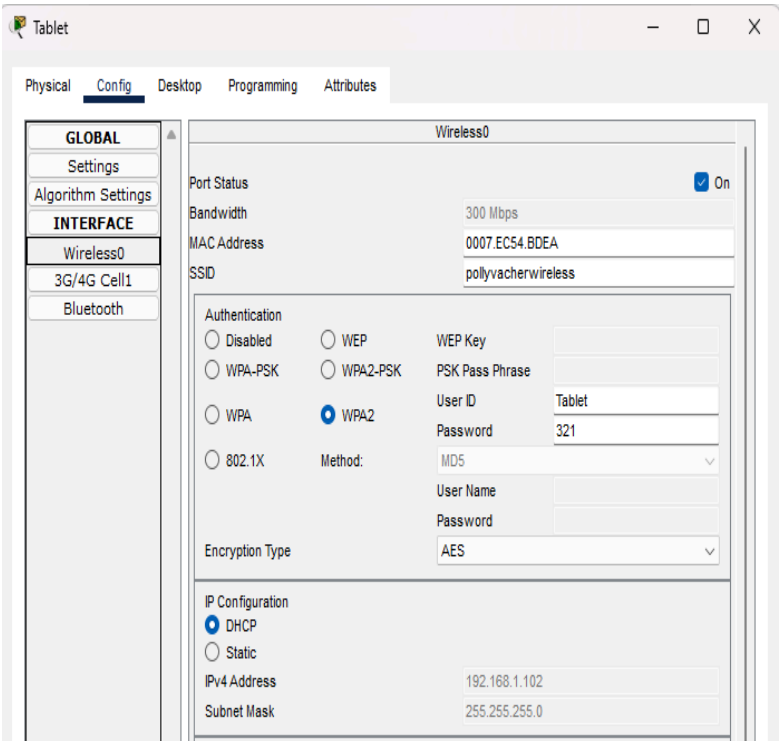


Figure 16 Configuration Tablet

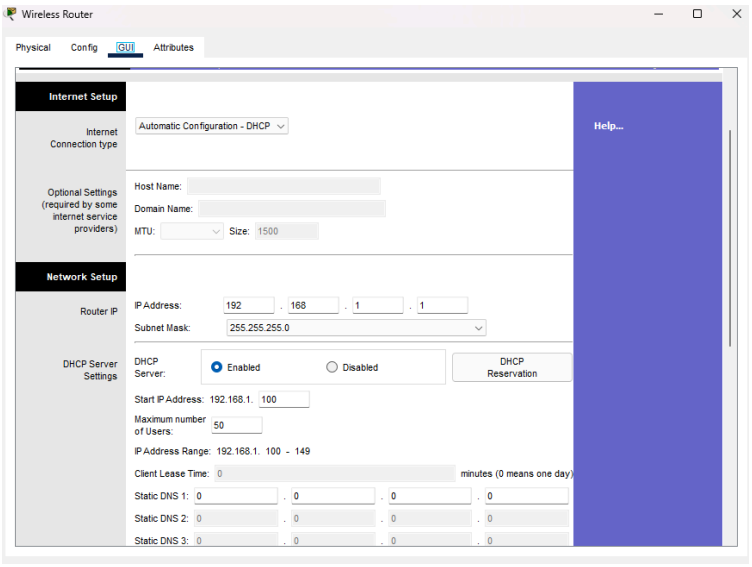


Figure 17 Configuration of Wireless Router DHCP Reservation

Figure 18 Configuration of Wireless Router DHCP Reservation

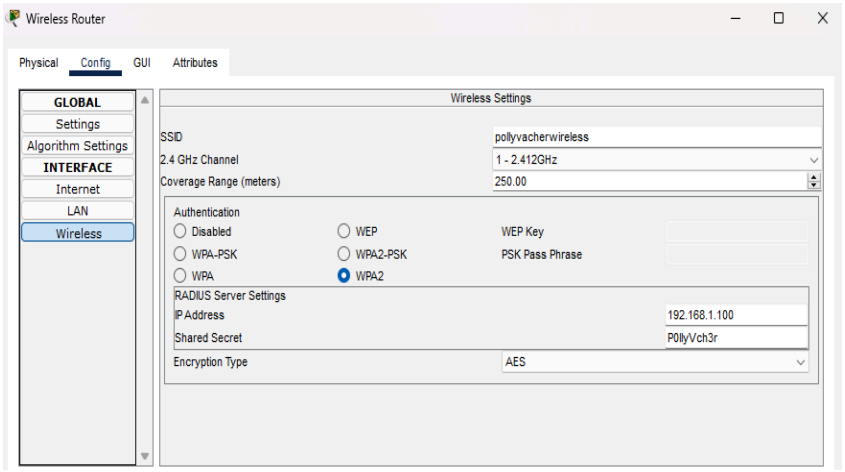


Figure 19 Configuration Wireless Router

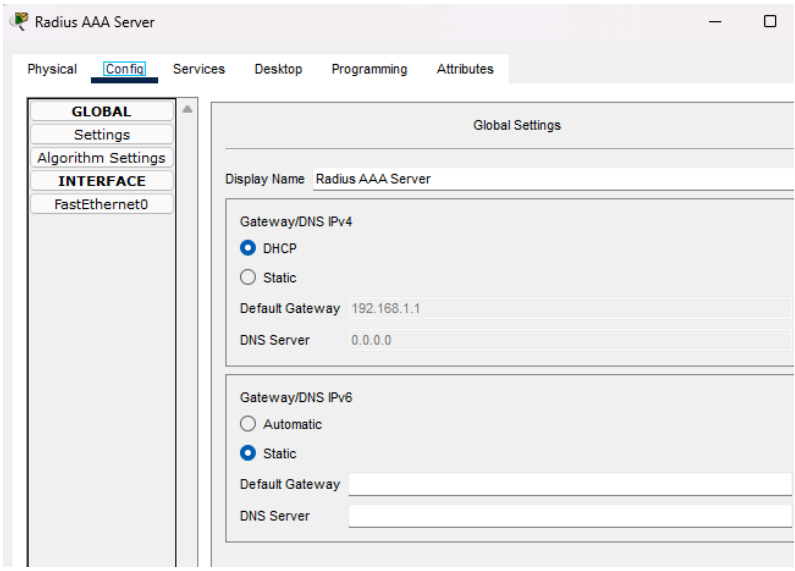


Figure 20 Configuration AAA Server

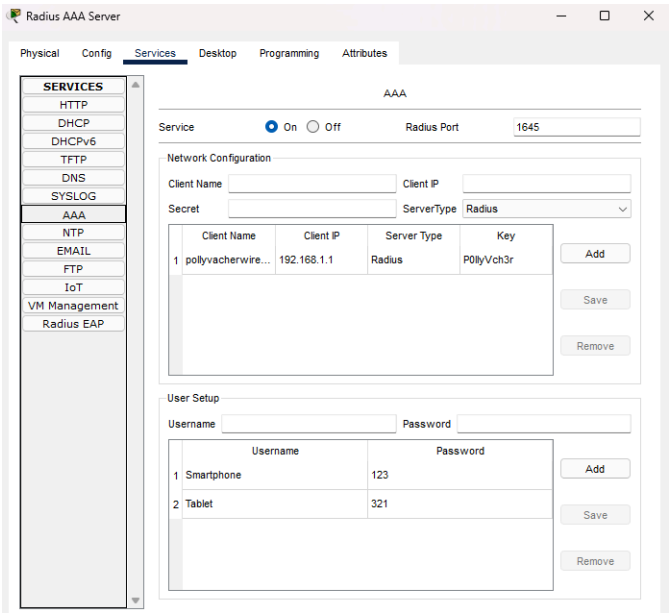


Figure 21 Services AAA Server

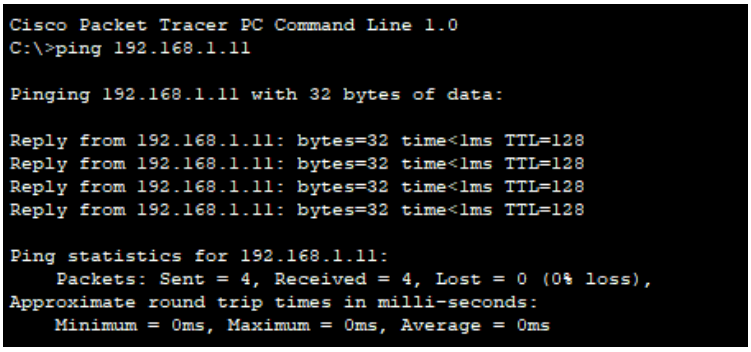


Figure 22 Ping PC-PC

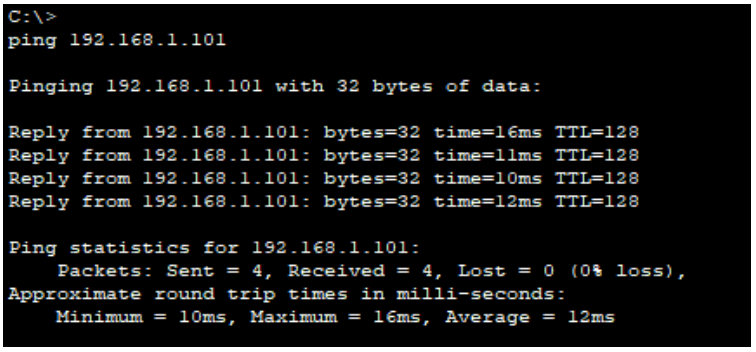


Figure 23 Ping PC-Smartphone

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 (P0llyVch3r) 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

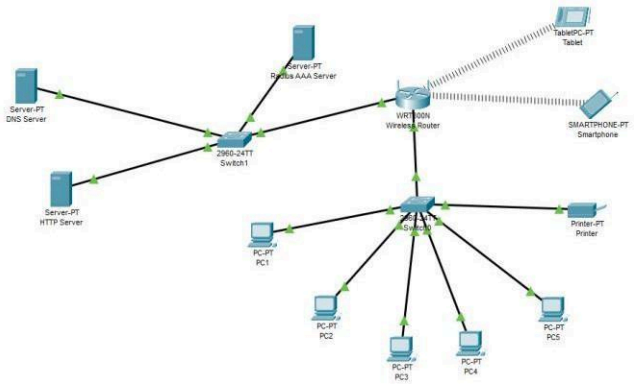


Figure 24 Small Office Network

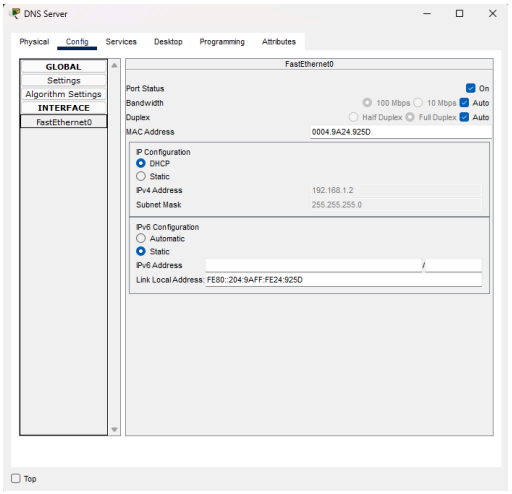


Figure 25

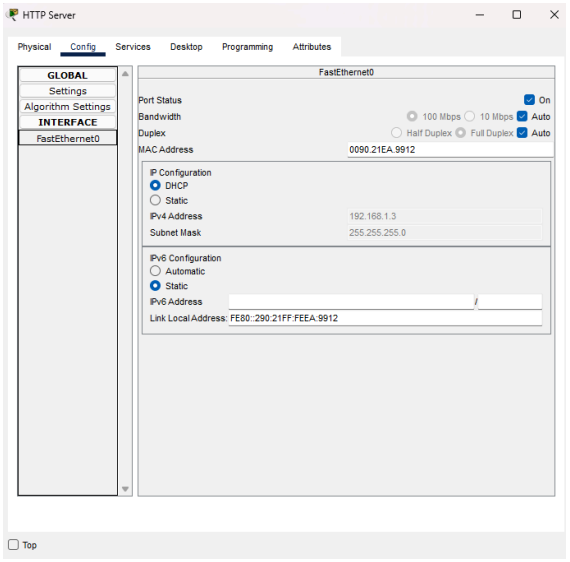
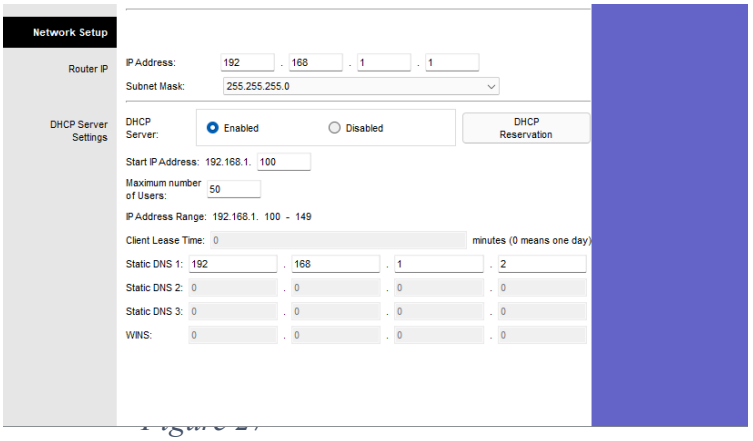


Figure 26



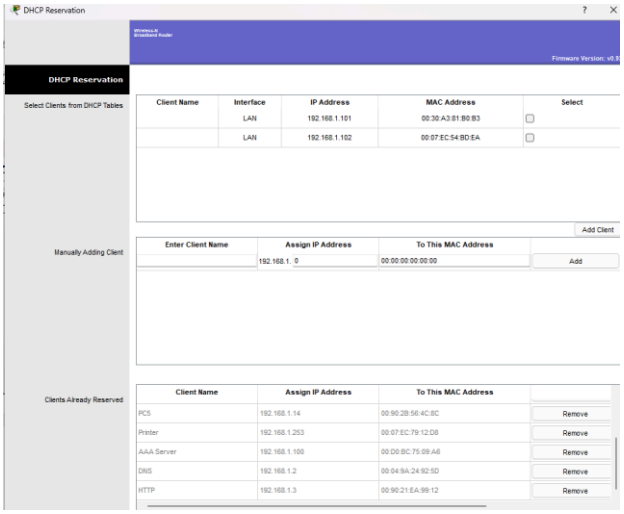


Figure 28

Figure 29

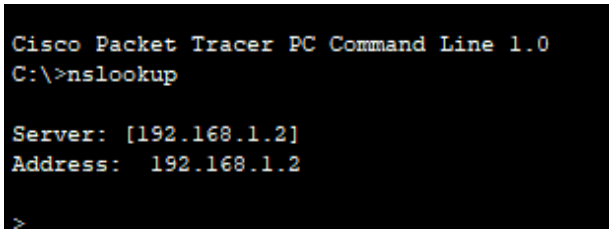


Figure 30

Fig ure 31

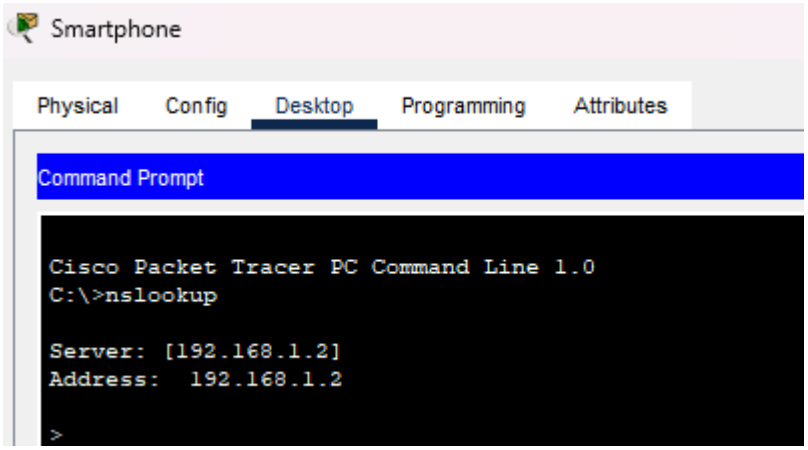


Figure 32

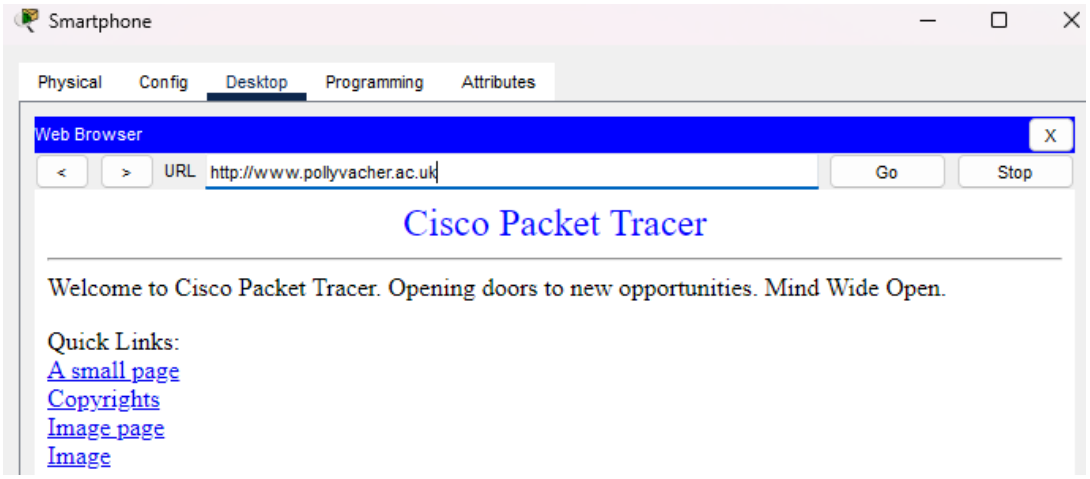


Figure 33

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 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 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)	**Wireshark** [X] Definition of ICMP [X] Examine IP and MAC address from LAN and Remote Host [X] Significant about this information [X] Reflection about MAC address	(total 30) 5 10 5 10
2. (25 marks)	**Small Office Network** [X] All devices connection [X] All devices IP configuration [X] DHCP server configuration [X] Wireless router and AAA server setup [X] Connectivity tests (x2)	(total 25) 5 5 5 5 5
3. (25 marks)	**DNS and HTTP Servers** [X] All devices connection and IP configuration [X] DNS Server configuration [X] HTTP Server configuration [X] DNS resolution tests (x2) [X] HTTP service tests (x2)	(total 25) 5 5 5 5 5
4. (20 marks)	**Quality of the submitted report** [X] Introduction [X] Detailed WireShark testing with screenshots [X] Small Office Network Setup with tests [X] DNS and HTTP Servers Setup with tests [X] Discussion, conclusion, and personal reflection	(total 20) 2 5 5 5 3
5. (5 marks)	Bonus marks for: [ ] Use of custom domain names (say, pc1.pollyvacher.ac.uk) 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/