

# Lab Book: Understand the Devices and Protocols Used in LAN and WAN Networks

**Contents**

Understand the Devices and Protocols Used in LAN and WAN Networks .....	3
Lab Objectives .....	3
Lab Resources .....	3
Task 1 – Identify WAN Connection Types .....	3
Task 2 – WAN Challenge Activities.....	5
Task 3 – Identify Protocols used to Support LAN and WAN Operation. ....	6
Task 4 – ARP Challenge Activities.....	17

## **Understand the Devices and Protocols Used in LAN and WAN Networks**

### **Lab Objectives**

1. Use CASBIT\_4G to identify/research the network devices utilised in WANs.
2. Identify the protocols used to support LAN and WAN services.

### **Lab Resources**

- Packet Tracer (PT) 6.01 or higher.
- Computer with Windows OS, XP or higher.

### **Task 1 – Identify WAN Connection Types**

1. A WAN operates over longer distances than LANs, and are used to interconnect LANs to remote LANs in branch sites and telecommuter sites.
2. A WAN is typically owned by a service provider. An organization must pay a fee to use the service provider's network services to connect remote LANs. WAN service providers include carriers, such as a telephone network, cable company, or satellite service. Service providers use WAN links to interconnect remote sites for the purpose of transporting data, voice, and video.
3. In contrast, LANs are typically owned by households or companies, and are used to connect local computers, peripherals, and other devices within a single building or other small geographic area. Home computer users need to send and receive data via a WAN in order to communicate with online banks, stores and other providers of goods and services.
4. What is the name of the service provider that your family uses? Do you know what type of WAN technology they provide to allow access to the Internet (e.g. DSL, cable, fibre, wireless)?

---

---

---

---

---

5. There are four main types of **broadband** WAN connectivity available to home users via UK service providers:
- a. **DSL:** DSL technology is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, and provides IP services to subscribers. Multiple DSL subscriber lines are multiplexed into a single, high-capacity link using a DSL access multiplexer (DSLAM) which is installed in the local phone exchange by the service provider. DSL connectivity is only possible if the household is within 5.5km of the local exchange.
  - b. **Cable:** Coaxial cable is widely used in urban areas to distribute television signals and provide IP services to subscribers. Cable systems support higher data rates than is possible over twisted-pair cabling. Cable subscribers must use the ISP associated with the service provider. All the local subscribers share the same cable bandwidth, so as more users join the service, available bandwidth may be below the expected rate. P
  - c. **Fibre Optic:** Fibre to the home (FTTH) is the installation and use of optical fibre to connect household to a service provider's network, providing very high-speed Internet access. Implementing FTTH on a large scale is costly because it requires installation of optical fibre over the "last mile" from the service providers existing network to individual user premises. Some service providers have implemented "fibre to the cabinet" (FTTC) service, which refers to the installation and use of optical fibre cable to the street cabinets near homes, with a traditional cable or twisted-pair link running to the household.
  - d. **3G/4G Wireless:** Increasingly, cellular wireless WAN technology being used to connect users and remote locations where no other WAN access technology is available. Many users with smart phones and tablets can use cellular data to email, surf the web, download apps, and watch videos. Cellular technology uses radio waves to communicate with a nearby mobile phone tower, which then connects to the rest of the service provider's network using a variety of different media types, such as microwave and fibre-optic.
6. Open the *CASBIT\_4G.pkz* file and examine the different types of WAN connection options in use in Bob and Ann's homes. Note that both homes use the same type of wireless routers, but connect to the different service providers via modems, which translate the Ethernet protocol frames used in each LAN to a suitable signal for crossing the DSL or cable links.
7. Why is Ethernet not generally seem as a suitable protocol for using to provide connectivity to a service provide network?

---

---

---

---

8. Bob and Ann can both use 4G to connect to the Internet – check that you can use the 4G-enabled laptops to connect to the [www.bcu.ac.uk](http://www.bcu.ac.uk) website. Check the IP address that has been assigned to the 4G laptop – how has this been assigned?

---

---

9. How is the 4G cellular connecting to the service provider's network? What other technology/media could have been used?

---

---

### Task 2 – WAN Challenge Activities

10. What is the advantage of using wireless 4G compared to using DSL or cable connectivity?

---

---

---

---

11. What are the disadvantages of using 4G when compared to using DSL or cable connectivity?

---

---

---

---

12. Why would Bob and Ann chose 4G instead of the WiFi provided by the home router to connect to the Internet?

---

---

### Task 3 – Identify Protocols used to Support LAN and WAN Operation.

13. Computers in a LAN are typically connected together using Ethernet switches, which are used to forward data between devices by examining the *destination* MAC address within received frames. Switches store the *source* MAC address found in a frame within a **MAC Address Table**, where the address is associated with the interface on which it was received.
14. Use the Inspect tool to examine the MAC address table of the Local ISP switch:

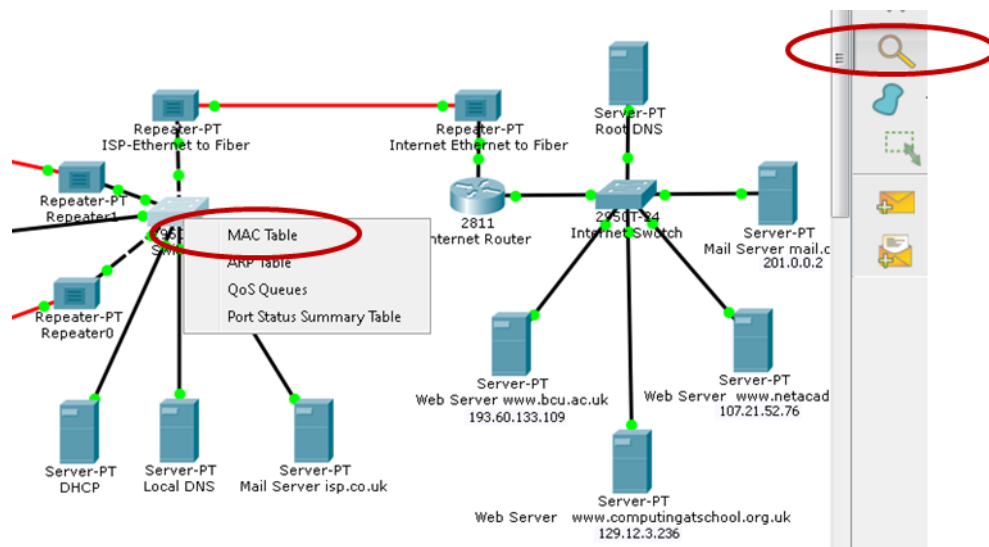


Figure 1 – Examining the MAC Address Table

15. The MAC address table should be almost empty, as the switch is not receiving many data frames, so it has not been able to learn the MAC addresses associated with the three computers to which it is connected:

MAC Table for Switch0

VLAN	Mac Address	Port
1	0001.42C1.0901	FastEthernet0/5

Figure 2 – MAC Address Table Contents

16. The only MAC address that should currently be in the MAC address table is that of the Internet Router, which will be sending some management traffic to the switch. Use the *Inspect* tool to determine which Internet Router interface has the MAC address shown:

17. Go to the desktop of the three server that are connected to the Local ISP Switch, and open a Command Line Interface (CLI) window. Use the ipconfig /all command to display the IP and MAC addresses for each device, recording them in Table 1 below:

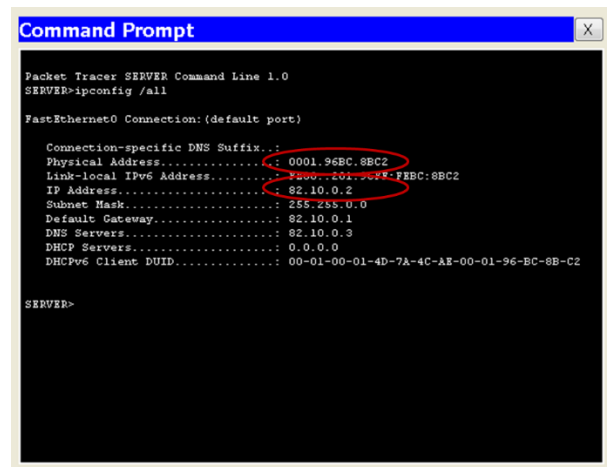
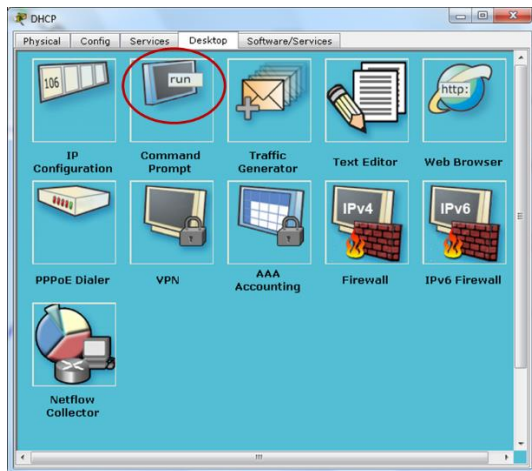


Figure 3 – Server Command Line Interface Window

Device	IP Address	MAC Address
DHCP Server		
Local DNS Server		
Mail Server		

Table 1 – Device Addresses

18. From the DHCP server CLI window, carry out ping tests to the other two servers:

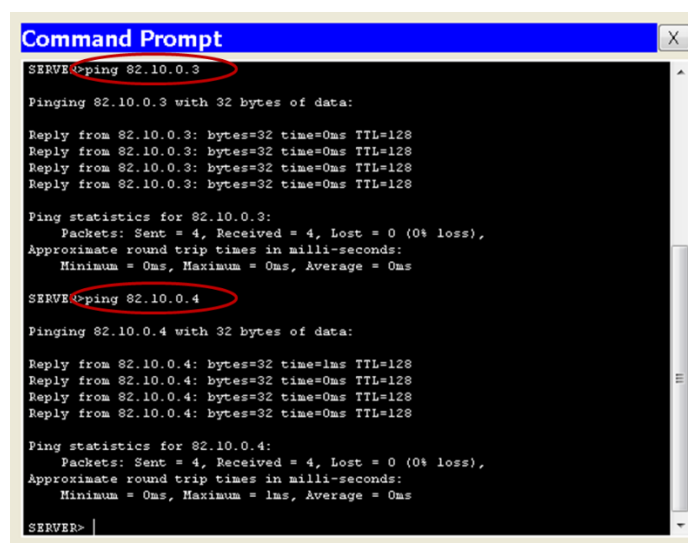


Figure 4 – Server Ping Testing

19. Use the *Inspect* tool to re-examine the MAC address table of the Internet Switch:

MAC Table for Switch0

VLAN	Mac Address	Port
1	0001.42C1.0901	FastEthernet0/5
1	0001.96BC.8BC2	FastEthernet0/3
1	0003.E4B4.2443	FastEthernet0/6
1	00D0.BCE7.E1B8	FastEthernet0/4

Figure 5 – MAC Address Table Contents

20. Copy the IP and MAC address information from Table 1 into Table 2, and then add the Fast Ethernet port that matches the learnt MAC address from your MAC address table output.

Device	IP Address	MAC Address	Port
DHCP Server			
Local DNS Server			
Mail Server			

21. This confirms that each port or interface on the switch has learnt the MAC address being used by the server to which it is attached. You can quickly check the switch ports to which the servers are connected by 'hovering' your cursor over the cable between each server and the switch in turn. **Top Tip:** spread the servers out on the topology diagram, as shown below, to prevent the port identities clashing.

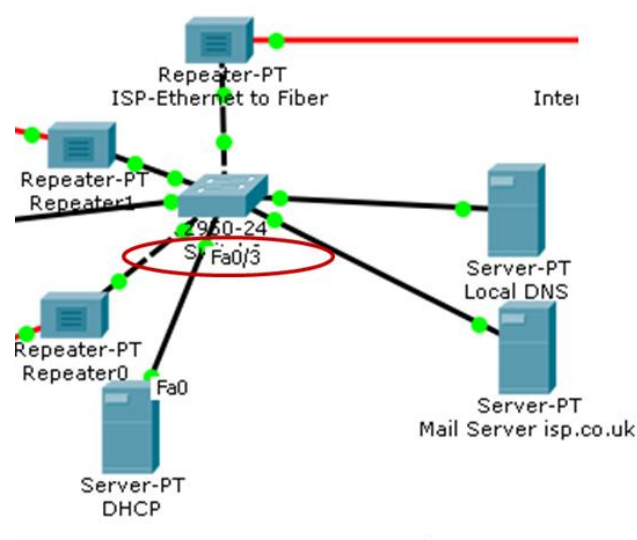


Figure 6 – Switch Port Identification



22. When you sent *ping* packets between the servers in step 18, the servers use the **Internet Command and Messaging Protocol (ICMP)** to generate test traffic called *echoes*, which are encapsulated within IP packets. This means that destination and source IP addresses must be added to allow the packet to reach a destination device, and enable that device to send an echo reply to the originating source. What would be the source and destination IP address used in an IP packet carrying an ICMP echo request from the DHCP server to the DNS server?

23. The IP addresses required are easily available to the originating device, as you have identified the destination address using the ping command, and the device can refer to its own NIC configuration to learn its own IP address:

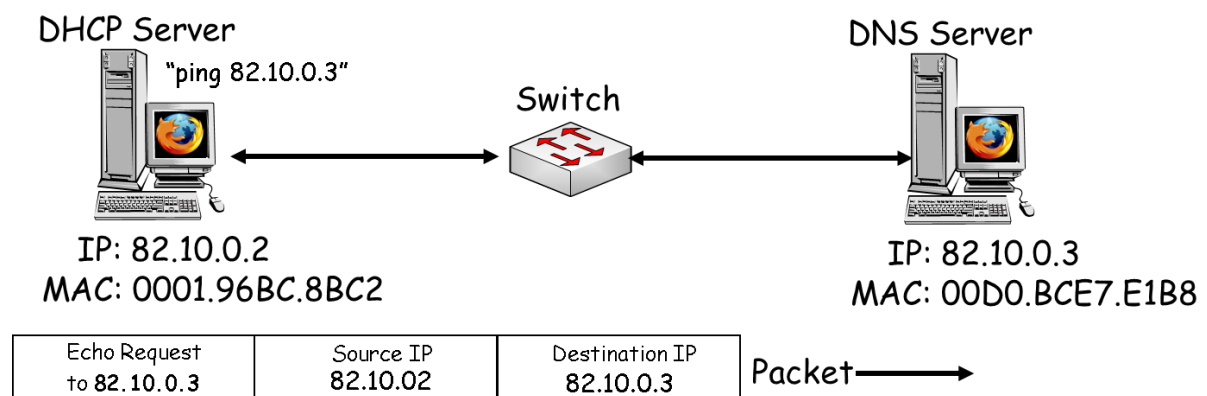


Figure 7 – IP Packet containing ICMP Echo Request

24. Fig 7 shows the DHCP server sending an ICMP echo request to the DNS server at 82.10.0.3, using its own IP address of 82.10.0.2 as the source IP address. When the DNS server receives the echo request, it will respond with an echo reply, as shown in Fig 8:

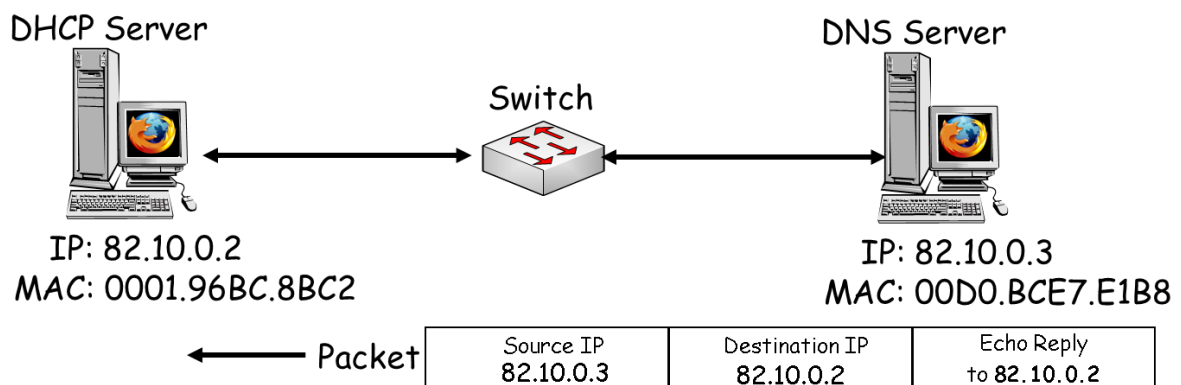


Figure 8 – IP Packet containing ICMP Echo Reply

25. Enter Packet Tracer Simulation mode, and select ICMP using *Edit Filters* within the *Events List*. Repeat the ping test between the DHCP and DNS servers, and ensure that it shows the correct source and destination IP addresses being used, in accordance with figures 7 and 8 above.
26. The IP packets carrying ICMP must be encapsulated in an Ethernet frame to allow them to be forwarded by the Ethernet switch used to connect the DHCP and DNS servers. The switch needs to look at the destination MAC address contained in the frame in order to switch it to the port to which the destination device is connected. Seems straightforward, but how is the source device going to learn the destination MAC address? It knows the source MAC address, as it is assigned to its NIC, but is unable to determine the required destination MAC address based on the IP address that you typed in within the **ping** command:

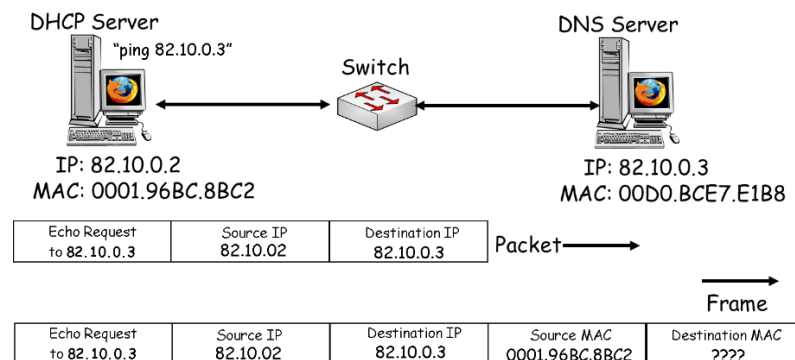


Figure 9 – Echo Request Destination MAC Problem

27. The sending device uses a protocol called *Address Resolution Protocol (ARP)* to discover the destination MAC address of other devices on the LAN. The sending host sends an ARP Request message to all the devices on the LAN. The ARP Request is sent as a broadcast message, which means that it uses a special MAC destination address, to ensure that all LAN device will look at the ARP Request. The ARP Request contains the IP address of the destination device for which a *destination* MAC address is required.
28. Every device on the LAN examines the ARP Request to see if it contains its own IP address. Only the device with the IP address contained in the ARP Request responds with an ARP Reply. The ARP Reply includes the MAC address associated with the IP address in the ARP Request:

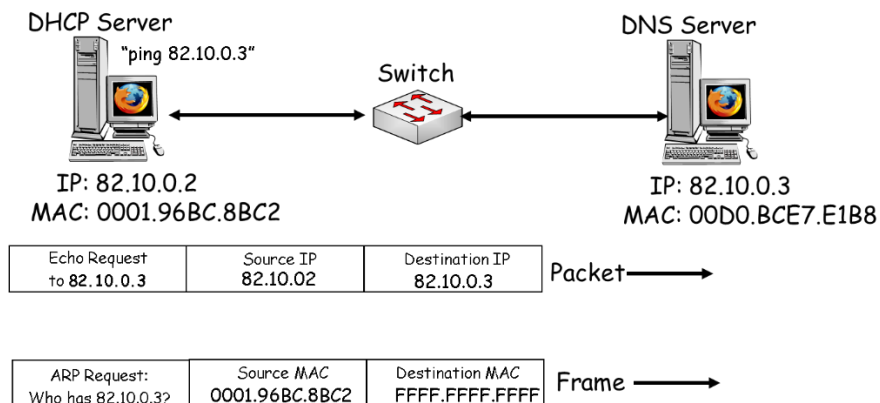


Figure 10 – Address Resolution Protocol Request

29. Look at the destination MAC address in Fig 10, which is FFFF.FFFF.FFFF respectively. This is an example of a broadcast address, and all devices on the LAN will accept the ARP Request and see if the requested IP address is theirs.

30. Convert the MAC broadcast addresses into binary – what do you notice about the result?

31. In the case of the DNS server, the received ARP Request will contain its IP address, so it will send an ARP reply, which contains its own MAC address:

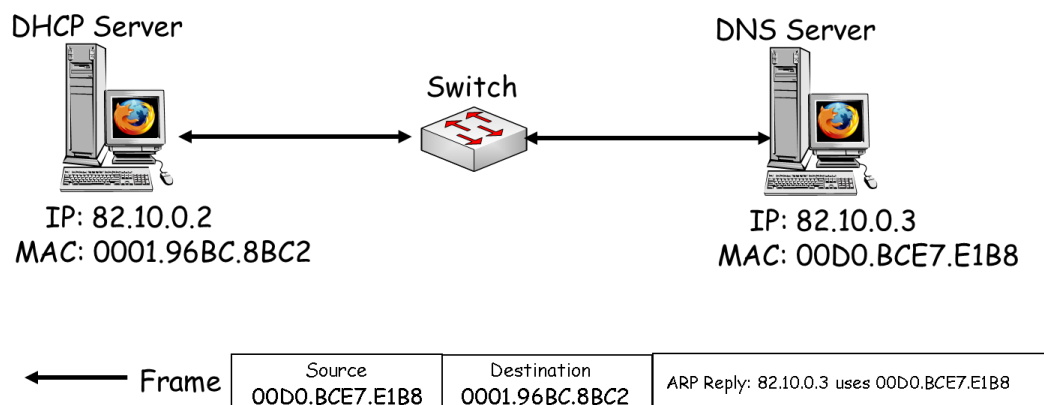


Figure 11 – Address Resolution Protocol Reply

32. Fig 11 shows that the DNS server can use the correct MAC address for the DHCP server in its ARP reply frame, as it learnt it from the frame that delivered the ARP request. Once the DHCP server learns the MAC address of the DNS server, it can then create a correctly addressed frame to deliver the ping request:

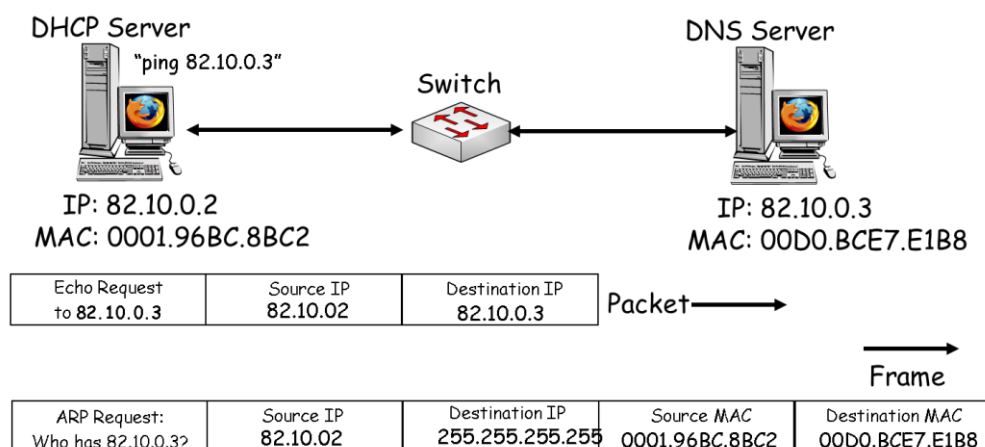
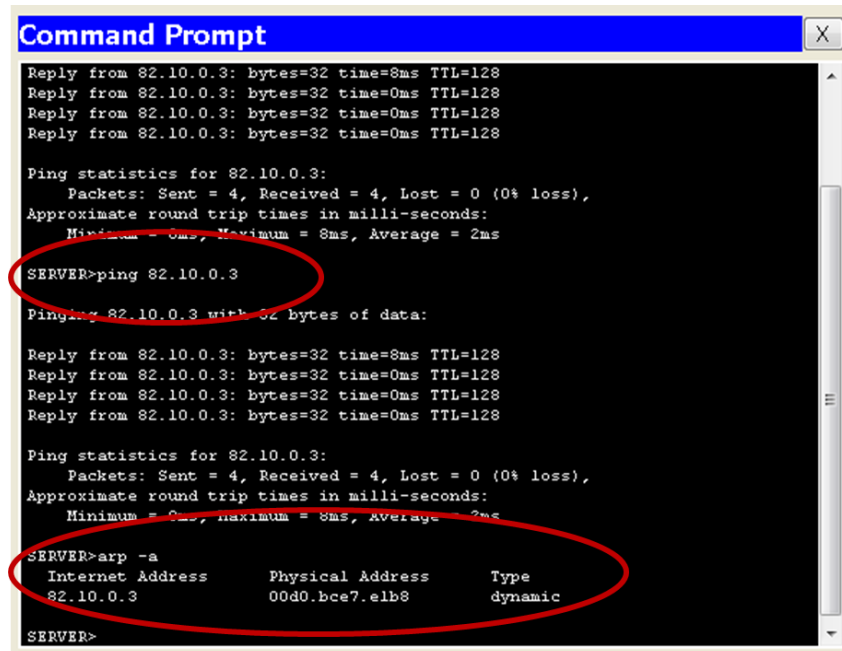


Figure 12 – Correctly Addressed Frame from DHCP Server

33. The ARP process described above is repeated every time any IP addressed device on a LAN is unsure of the correct destination MAC address to use within a frame. Once it has learnt the correct MAC address, it is stored on the local device in an ARP cache. Carry out another ping test between the two servers, and then check the ARP cache on both devices from the Command Line Interface using the **arp -a** command:



```
Command Prompt
Reply from 82.10.0.3: bytes=32 time=8ms TTL=128
Reply from 82.10.0.3: bytes=32 time=0ms TTL=128
Reply from 82.10.0.3: bytes=32 time=0ms TTL=128
Reply from 82.10.0.3: bytes=32 time=0ms TTL=128

Ping statistics for 82.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

SERVER>ping 82.10.0.3

Pinging 82.10.0.3 with 32 bytes of data:

Reply from 82.10.0.3: bytes=32 time=8ms TTL=128
Reply from 82.10.0.3: bytes=32 time=0ms TTL=128
Reply from 82.10.0.3: bytes=32 time=0ms TTL=128
Reply from 82.10.0.3: bytes=32 time=0ms TTL=128

Ping statistics for 82.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

SERVER>arp -a
Internet Address      Physical Address      Type
82.10.0.3             00d0.bce7.e1b8       dynamic
SERVER>
```

Figure 13 – Viewing the ARP Cache

34. Confirm that the correct IP and MAC addresses are shown in the ARP cache. These entries will remain in the cache for as long as the device is actively sending frames to the MAC addresses it contains. Once the entry becomes inactive for 5 minutes, it will be removed from the cache.
35. Why do you think it is a good idea to remove old MAC address entries from the ARP cache?
- 
- 
36. You can manually remove all MAC addresses from the ARP cache using the **arp -d** command. Use this on your DHCP and DNS servers and check that the ARP cache is empty.
37. Enter Packet Tracer Simulation mode, and select ICMP and ARP using *Edit Filters* within the *Events List*. Repeat the ping test between the DHCP and DNS servers, and observe the flow of ARP packets. Which devices are receiving the ARP requests?
- 
-

38. Open up the very first ARP Request packet that is sent by the device originating the ping test (DHCP server in this example). Confirm that it is using a broadcast MAC addresses and is requesting the MAC address of the host for which you have issued the ping test:

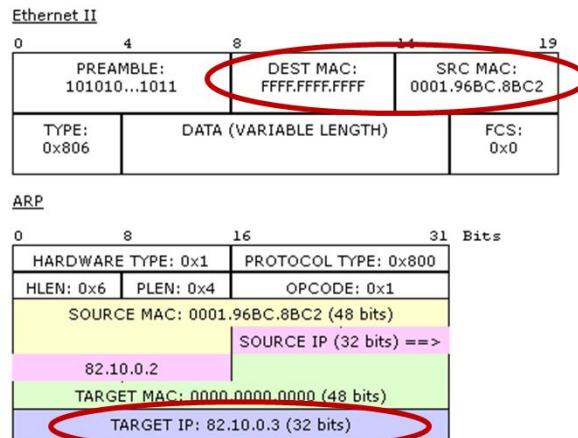


Figure 14 – ARP Request from DHCP Server

39. Locate the ARP Reply packet returning from the DNS server, and confirm that ARP is carrying the IP and MAC address for the DNS server. You should also see that the ARP query is not using a MAC broadcast destination address:

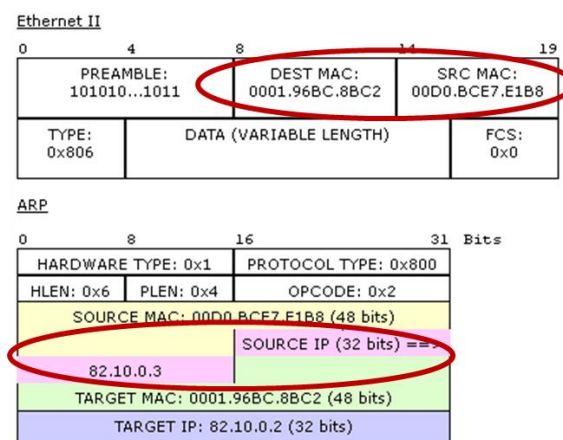


Figure 15 – ARP Reply from DNS Server

40. What are all the other devices in the LAN doing when they receive the ARP requests, and why are they doing it?

---



---



---



---

41. Try running the ARP/ICMP simulation several times, and observe what happens when the ARP requests arrive on a router. You should see that the ARP requests are not forwarded, as routers are designed not to forward broadcast traffic. What do you think the effect on the Internet would be if routers did forward broadcast traffic?

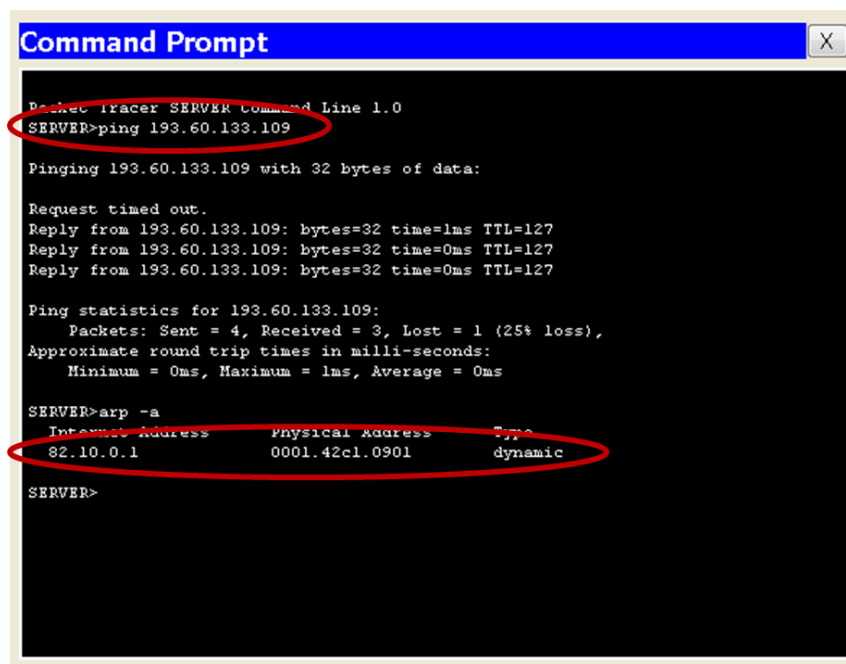
---

---

---

---

42. If routers do not forward ARP requests, how can a device learn the destination MAC address required to reach a computer located on a different LAN? Analyze the operation of ARP when sending packets to another LAN by sending a ping from the DHCP server to the [www.bcu.ac.uk](http://www.bcu.ac.uk) server at 193.60.133.109, and then examine the ARP cache:



```
Command Prompt
Packet Tracer SERVER Command Line 1.0
SERVER>ping 193.60.133.109

Pinging 193.60.133.109 with 32 bytes of data:

Request timed out.
Reply from 193.60.133.109: bytes=32 time=1ms TTL=127
Reply from 193.60.133.109: bytes=32 time=0ms TTL=127
Reply from 193.60.133.109: bytes=32 time=0ms TTL=127

Ping statistics for 193.60.133.109:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

SERVER>arp -a
Internet Address      Physical Address      Type
82.10.0.1             0001.42c1.0901        dynamic
SERVER>
```

Figure 16 – ARP Reply from Ping Test to Web Server

43. The ARP cache shows only one IP/MAC address pairing, and it not correct for the [www.bcu.ac.uk](http://www.bcu.ac.uk) server. Whilst the IP address is obviously wrong, you can check that the MAC address is also incorrect using the ipconfig /all command in the CLI window on the [www.bcu.ac.uk](http://www.bcu.ac.uk) server.
44. Examine the devices in your Packet Tracer topology to locate the device with the IP address shown in the ARP cache. You'll discover that it is Internet Router, which also has the MAC address shown in your ARP cache.

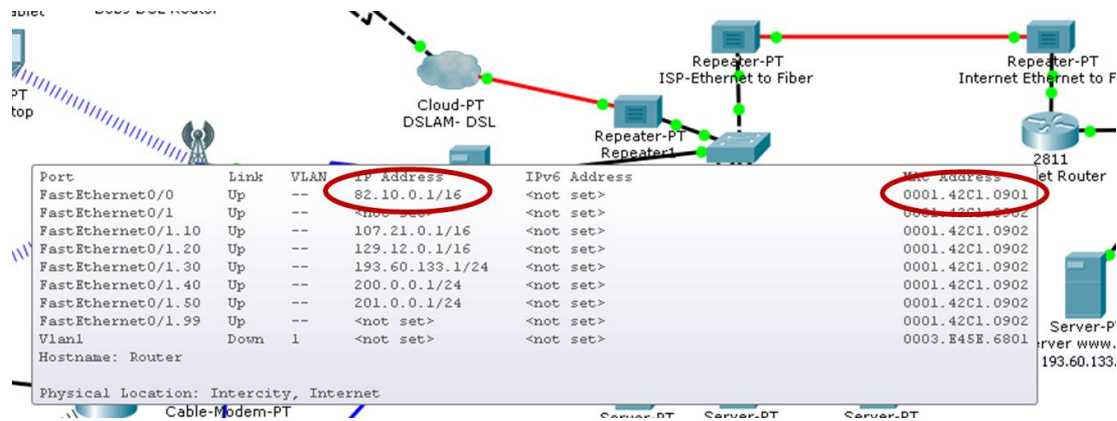


Figure 17 – Internet Router IP and MAC Addresses for Local ISP Switch LAN

45. What is the default gateway being used by all the servers connected to the Local ISP Switch:

46. When you entered the ping to 193.60.133.109 on the DHCP Server, it checked its local IP address with the destination address identified by the ping command, and noticed that the two addresses are within different IP networks. It then checked its IP configuration for the identity of the default gateway (i.e. router) that it must send packets to that require routing to remote networks. Check the IP default gateway configured on the DHCP server:

**IP Configuration**

Interface: FastEthernet0

IP Configuration:

☐ DHCP ☒ Static

IP Address: 82.10.0.2

Subnet Mask: 255.255.0.0

Default Gateway: 82.10.0.1

DNS Server: 82.10.0.3

IPv6 Configuration:

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address:

Link Local Address: FE80::201:96FF:FEBC:8BC2

IPv6 Gateway:

IPv6 DNS Server:

Figure 18 – DHCP Server IP Configuration

47. The DHCP server will now use ARP to learn the MAC address it requires to forward the ping packet to the default gateway, and will then place the ping packet in a frame with the default gateway MAC address as its destination, allowing the switch to forward the frame directly to the local router. Once the frame arrives at the router, the frame is accepted, then stripped to reveal the ping packet, which will be re-encapsulated in a new frame using MAC addresses relevant to the exit interface used by the router to forward the packet to its final destination.



48. Enter Packet Tracer Simulation mode, and select ICMP using *Edit Filters* within the *Events List*. Repeat the ping test between the DHCP and web server, and then examine the second ICMP packet to leave the server:

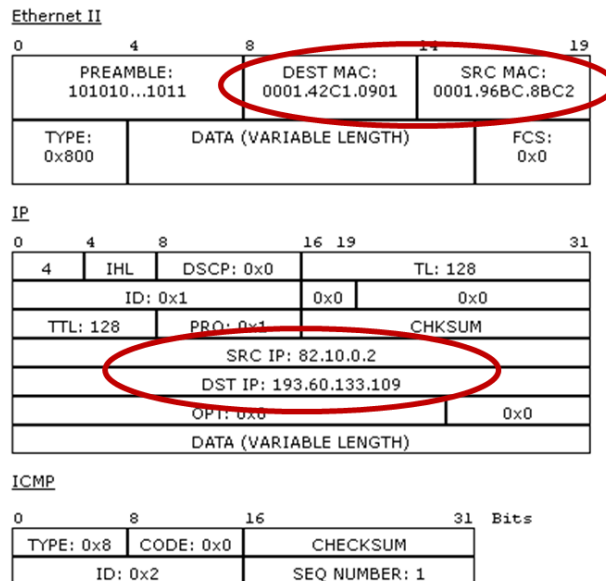


Figure 19 –IP/MAC Address Analysis

49. Looking at the packet, you can see that the IP address of the packet is that of the DHCP server (source) and the web server (destination). However, the MAC addresses used are from the DHCP server (source) and the local router (destination). This test demonstrates that IP addresses are used to provide end-to-end connectivity between computers, and remain unchanged as they travel through routers (unless NAT is used). MAC addresses are used to deliver packets to the correct devices within the LAN, and therefore are frequently changed as a packet is passed between routers.



**Task 4 – ARP Challenge Activities**

50. Clear the ARP cache on the DHCP server and then ping any of the web servers. What happen to the first echo reply message?

---

---

51. What happen when you repeat the ping test to the same web server?

---

---

52. Explain what might be causing this issue with ARP.

---

---

---

---