Lab Book: Identify Devices and Protocols Used in Computer Networks

Contents

Identify Devices and Protocols Used in Computer Networks

Lab Objectives

1. Use CASBIT to identify/research the network devices utilised in a typical computer network.
2. Identify the protocols used to support Internet services.

Lab Resources

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

Task 1 – Identify Network Devices

1. Open the pre-built Packet Tracer file *CASBIT.pkz* . This network simulates basic Internet services, and is fully operational.

2. Slowly move your cursor over the icons on the left of the *Device Selection* area, as shown in Fig 1 below to display the categories of devices available.

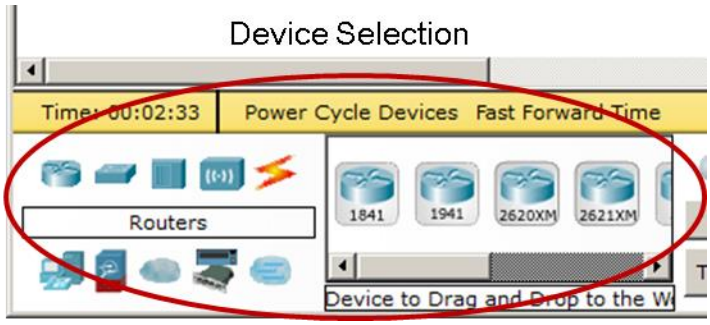


Figure 1 – Device Selection Area

3. Write the displayed name shown in the *Device Selection* Area against the icons in Table 1 below:

Icon	Device Name

4. Select the ISP Router in the CASBIT topology, and then select the physical tab, as shown in Fig 2 below. Note that this router would typically be found in small to medium sized business, and is not really suitable for household use due to its cost.

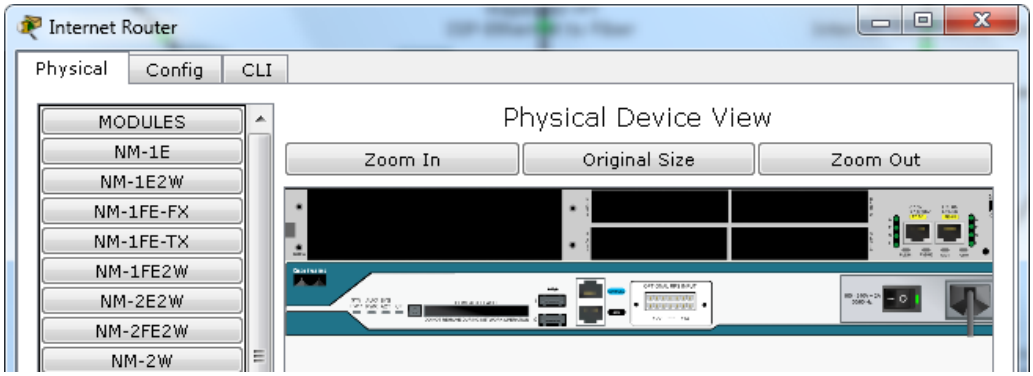


Figure 2 – Router Physical View

5. Use the *Zoom In* button to take a closer look at the router. How many FastEthernet interfaces does the router provide?

6. It is possible to add additional modules to this type of router, to allow it to support a wide range of different transmission media, such a copper cabling, fibre optic and wireless. If you select one of the available modules on the left of the physical tab, its capabilities will be displayed at the bottom of the window. You can then drag the card to the router, and place it in one of the empty slot – don't forget to turn the router power off first!

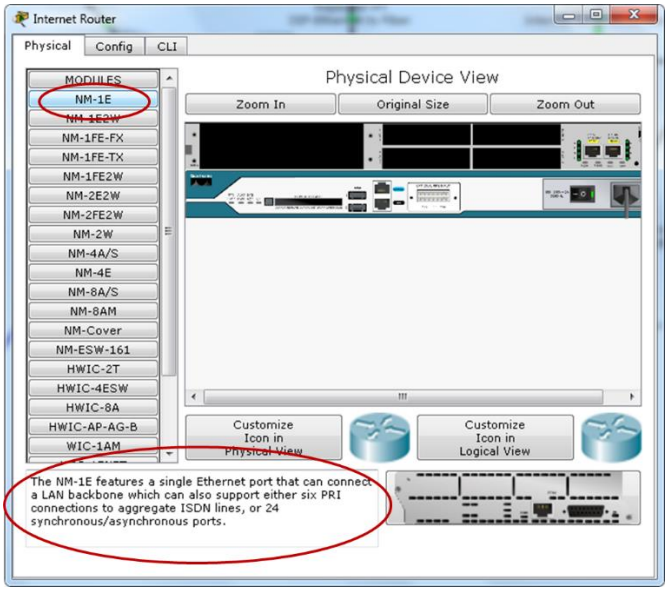


Figure 3 – Router Module Selection

7. Try and fit a module to the router that will support two FastEthernet ports. Which card did you select?

8. Close the router window, and select the Inspect tool. Use this to examine the routing table of the router:

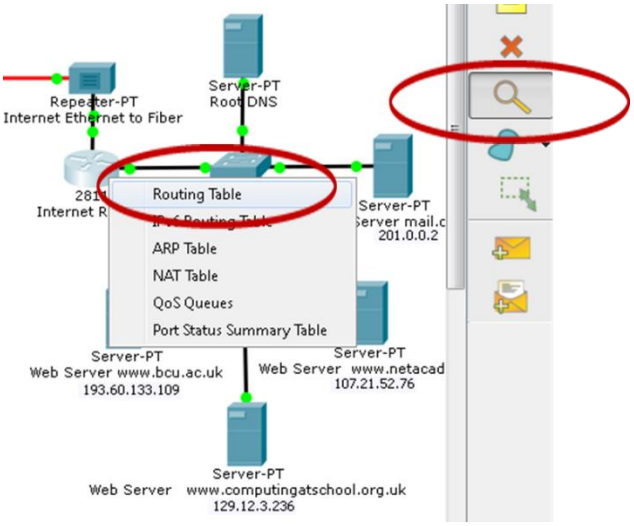


Figure 4 – Examine the Routing Table

9. When you examine the routing table, you should be able to see the three networks that house the web servers, which mean that the router knows how to reach these networks. The purpose of a router is to forward IP packets to destination networks, based on the destination IP address carried in each IP packet. In this case, as the router has the web server networks in its routing table, it is able to forward Internet Protocol (IP) packets from Bob and Ann's houses to the web server.

10. Select the Internet Switch in the CASBIT topology, and then select the physical tab, as shown in Fig 5 below. Note that this switch would typically be found in small to medium sized business, and is not really suitable for household use due to its cost.

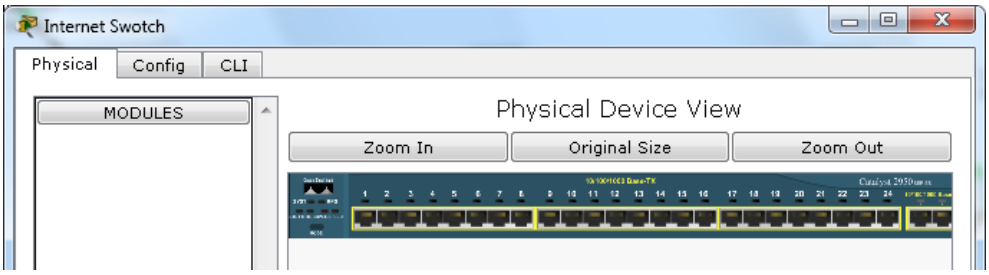


Figure 5 – Router Physical View

11. Use the *Zoom In* button to take a closer look at the switch. How many FastEthernet interfaces does the router provide? Can you add additional modules to this switch if you need more interfaces?

12. Use the *Inspect* tool on the switch. Note that there is no routing table displayed, as this model of switch is not capable of carrying out the routing of packets between different IP networks. Its main function in this network is to provide plenty of FastEthernet interfaces, to allow the connection of many devices to the network. Packets that require routing between networks are directed towards the attached router.

13. The switch uses **Media Access Control** (MAC) addresses to allow it to make switching decisions, and these addresses are actually associated with the network interfaces of the devices (PCs, tablets, smart phones, etc) that are generating the IP packets sent to the switch. Use the *Inspect* tool again, and select the *MAC address table*, which will display the MAC addresses that the switch is currently aware of.

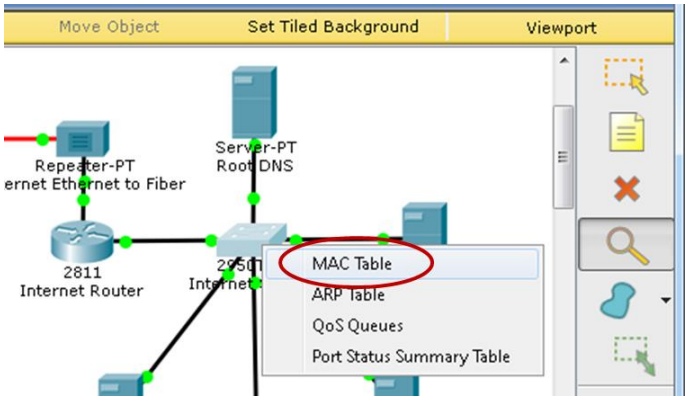


Figure 6 – Examine the MAC Address Table

14. Select the Ann's home router in the CASBIT topology, and then select the physical tab, as shown in Fig 7 below:

Figure 7 – Home Router Physical View

15. Use the *Zoom In* button to take a closer look at the home router. How many FastEthernet interfaces does the router provide? Can you add additional modules to this router if you need more interfaces?

16. The home router is a relatively low-cost device that enable home users to connect to the Internet, providing sufficient FastEthernet (perhaps even GigabitEthernet) ports to connect a small number of PCs. It also typically provides wireless services, so that tablets, smartphones, etc, can also be supported. Although it provides basic IP routing, it does not provide as many features as the Cisco router that you viewed previously.

17. Ann's home router is connected to the ISP using a cable modem, as shown in Fig 8. This is required because the router supports only FastEthernet interfaces, whereas the cable network that is used to connect to the ISP utilizes a different type of transmission system (Google 'DOCSIS' to learn more). The cable modem thus translates the FastEthernet signal into something suitable for use by the cable network, and vice versa.

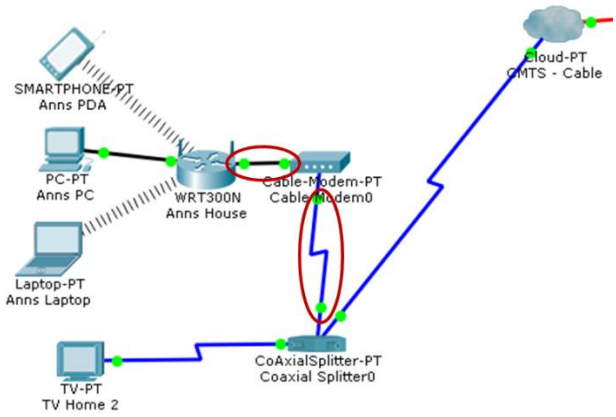


Figure 8 – Cable Modem

18. What type of modem is used to connect Bob's home router to the ISP? What does it do?

19. Most home routers now have modems built-in, but you must make sure that you select one that will work with your home ISP. Use the Internet to identify two home routers, one that supports cable, and one that supports DSL:

20. Select Bob's PC in the CASBIT topology, and then select the physical tab, as shown in Fig 8 below:

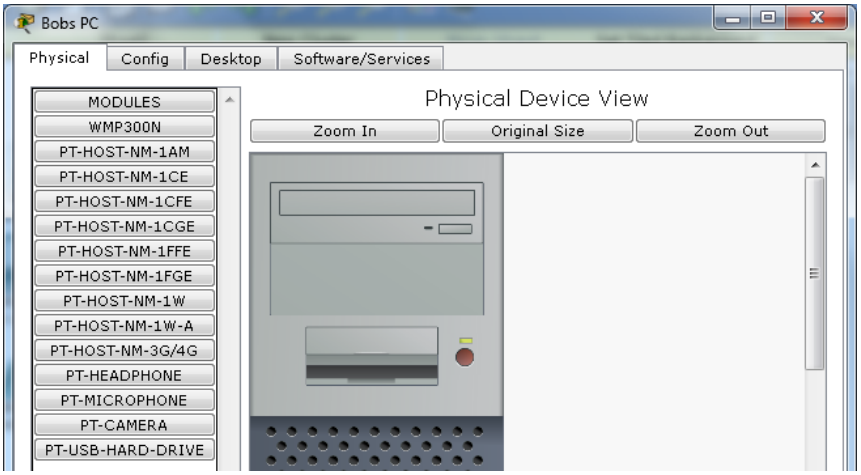


Figure 8 – Bob's PC

21. Use the *Zoom In* button to take a closer look at the PC. How many FastEthernet interfaces does it provide? Can you add additional modules to this PC if you need a different type of interface?

22. Now select Bob's Laptop and Tablet. Comparing them to Bob's PC, how easy would it be to add additional modules to them?

23. Why do you think that Bob's devices only seem to need one network interface (either FastEthernet or wireless)?

24. Select the DHCP server in the CASBIT topology, and then select the *Services* tab, as shown in Fig 9 below:

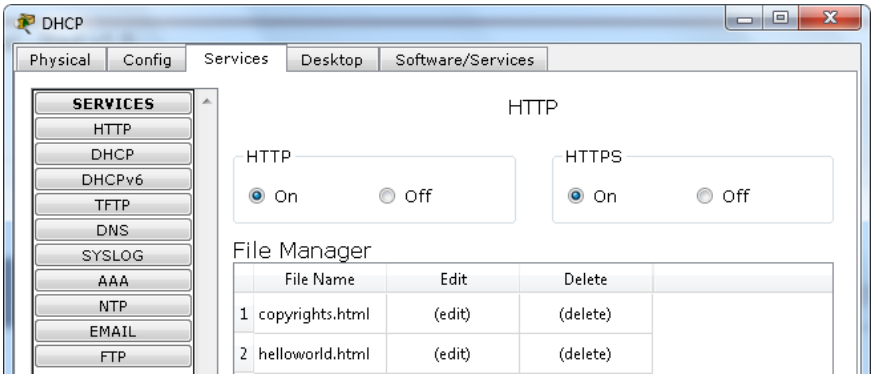


Figure 9 – Server

25. A server is a computer that is running software that provides *services* to other PCs. In Packet Tracer, this is simulated by having specific devices that can run services such as web, file sharing and email. In reality, any computer can act as a server by installing appropriate software on it. Typically, services provided by software will utilize different network protocols to support their operation:
    - Web – Hyper Text Transfer Protocol (HTTP)
    - File Sharing – File Transfer Protocol (FTP)
    - Email – Post Office Protocol 3 (POP3) and Simple Mail Transfer Protocol (SMTP)

26. Use the Internet to identify **software** that can be used to provide the following services:

    - Web Server
    - Mail Server
    - File Server

Task 2 – Investigate the operation of DHCP

27. Select Bob's home router and select the *GUI* tab, and examine the settings:

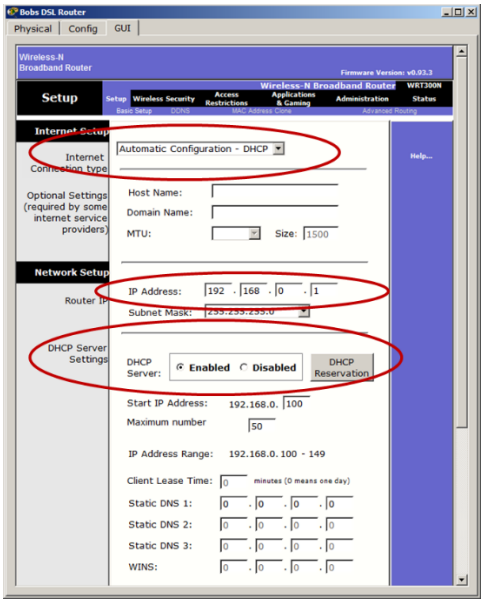


Figure 10 – Wireless Router Configuration

28. The wireless router is configured by default to use the Dynamic Host Configuration Protocol (DHCP) to automatically obtain an IP address from the ISP DHCP server for its Internet interface. It is also configured to act as a DHCP server to offer DHCP addresses to the devices on Bob's LAN that connect to the Internet via the wireless router. Currently, the wireless router interface on the LAN is set to 192.168.0.1, and will offer addresses to the other devices from the range (or 'pool') 192.168.0.100 to 192.168.0.150.

29. Check each of Bob's devices to ensure that the have received an IP address via DHCP from the wireless router LAN pool by selecting each device in turn and opening up the *desktop* tab to review the *IP configuration*:

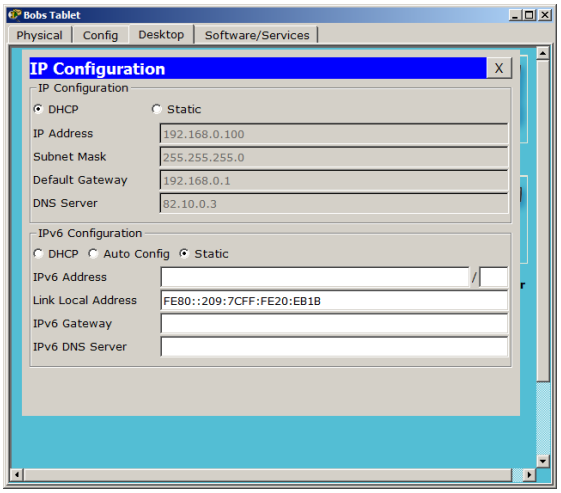


Figure 11 – Client DHCP Configuration

30. Ensure that all of Bob's devices are set to use DHCP, and that they have obtained IP address information, and then consider the following questions:

31. Which device is identified by the default router address?

32. Perform steps 7 to 8 on Ann's network and compare the addresses used. What do you notice about the addresses used on Bob and Ann's networks?

33. The default gateway is the device used to connect local devices to devices located on other networks. As Bob and Ann connect to other networks via their respective Internet Service Providers (ISPs), then their home routers are providing access to all other networks, and are thus acting as default gateways. Therefore, each home router has used DHCP to advertise its own configured LAN interfaces (192.168.0.1) as the default gateway for all devices in their respective LANs.

34. Is the default router IP address in the same network as Bob's other devices?

35. It is possible to examine the DHCP process in operation using the PT simulation mode, which is accessed by selecting the *Simulation* tab hiding behind the *Realtime* tab at the bottom right of the workspace. Select the *Event List* on the left of the simulation tab, and ensure that DHCP packets are selected for capture:

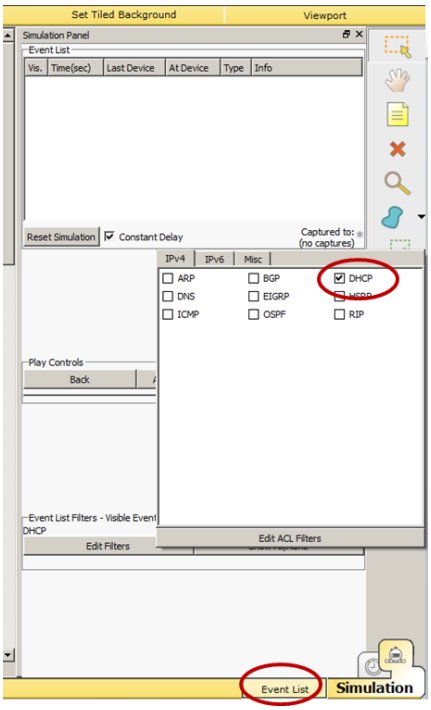


Figure 12 – Simulation Mode Configuration

36. Staying in simulation mode, access one of Bob's devices and select the Desktop tab and then IP configuration. Toggle the *DHCP* radio button to *Static*, and then back to *DHCP* to force the device to send out a DHCP request to the wireless router. Because you are in *Simulation* mode, an IP address will not be received, as the simulation must be run using the *Auto Capture/Play* link in the centre of the *Simulation* tool bar:

Figure 13 – Simulation Auto Capture/Play

37. You should now see DHCP packets travelling between Bob's devices and the wireless router which is acting as a DHCP server. As packets are created, they will appear as captures in the *Simulation Panel*, which is at the top of the Event List shown in Figure 23. You can analyse the DHCP information by selecting the coloured boxes within the *Info* heading of the Simulation Panel.

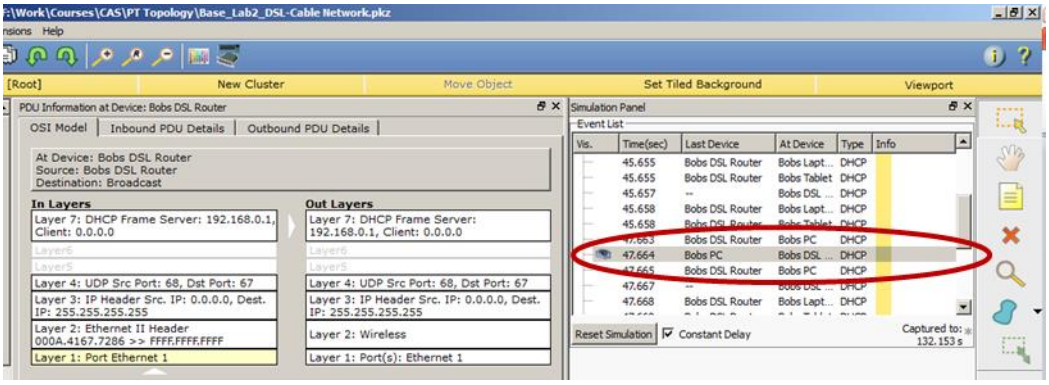


Figure 14 – Simulation DHCP Packet Analysis

38. What source address and destination IP address is Bob's PC using when asking for an IP address via DHCP? Use the Internet to research what these addresses mean.

39. Use the *Delete* button under the *Capture/Forward* on the *Simulation* tool bar to clear all the captured packets.

Task 3 – Investigate Network Address Translation (NAT) and HTTP

41. But IP addresses are used to uniquely identify devices on the Internet, so how come Bob and Ann's networks seem to be using the same address pools? Because IPv4 has effectively run out of new addresses, address conservation techniques have to be employed to keep the Internet working until IPv6 can take over. Bob and Ann's wireless routers are using a well-known private address range (anything starting with 192.168.x.x), which cannot be used on the Internet. When they send data packets from their networks, they are sourced with private addresses, which are converted to the single **public** address assigned to the home router Internet interface, which has been assigned using DHCP by the ISP. This process is called Network Address translation (NAT).

42. Return to Bob and Ann's home router's GUI and select the *Status* link. What IP address has been assigned to each routers Internet interface and what ISP default gateway is being used?

43. Examine the Packet Tracer topology and locate the DHCP server. Select the device and open it up and select the Services tab and then the DHCP link:

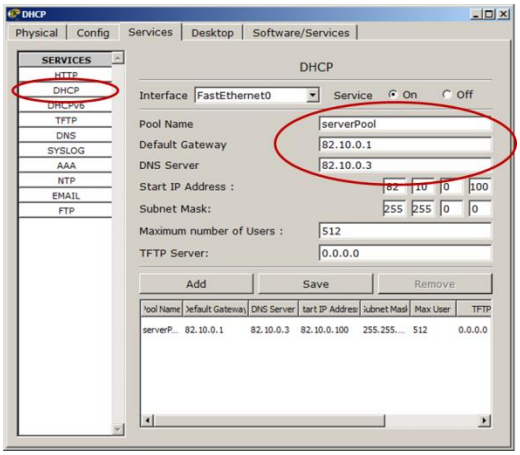


Figure 15 – ISP DHCP Server Configuration

44. How does the ISP DHCP server configuration relate to the addresses assigned to the home routers Internet interfaces?

45. Select *Simulation* Mode, then the *Event List* on the left of the simulation tab, and ensure that Hyper Text Transfer Protocol (HTTP) packets are selected for capture. HTTP is the protocol used to transfer web pages from the web server on which they are stored, to the web browser on Bob's PC.

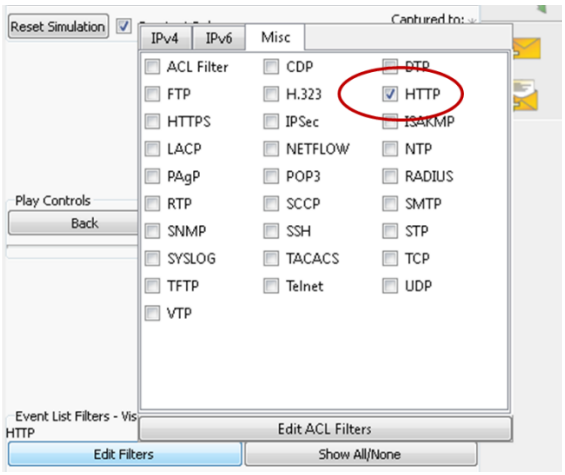


Figure 15 – HTTP Filter Configuration

46. Go to Bob's PC and select the *Desktop* tab, and then the *Web Browser*. Type the address of the Birmingham City University Web Site, *www.bcu.ac.uk* into the address bar. Select the *Go* button – what does the address you just typed in change to? What does this tell you about the network protocol the web browser is using?

47. Select Auto Capture/Play on the Simulation tool bar, and watch the HTTP packets traverse the network. Which device does HTTP access to retrieve the web page?

48. Examine the first packet in the *Simulation Panel* Event List – what is the source IP address? (Clue – the packet came from Bob's PC):

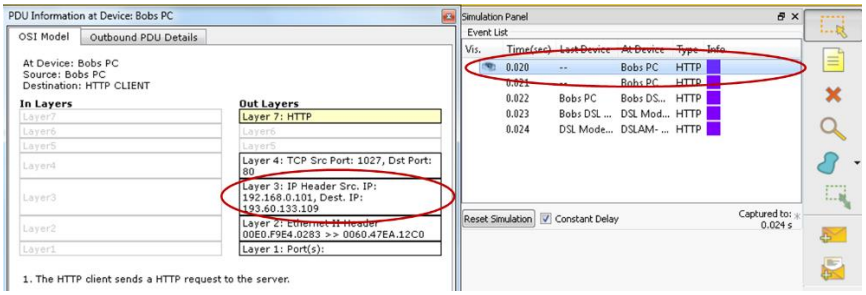


Figure 16 – Source Address Inspection

49. Examine the 4th packet shown in the Event List (any packet that has passed through Bob's home router will suffice), which should have performed a NAT translation – what is the source address of the packet?

50. You should see a new source address related to Bob's home router, which means that NAT is operational and effectively 'hiding' the private IP addresses assigned to Bob's device behind a single public IP address, assigned to the home router by the ISP using DHCP. This can then be routed through the Internet to the destination address.

51. Returning to the *Simulation Panel*, select the 4th packet and the then select the *Outgoing PDU Details* tab:

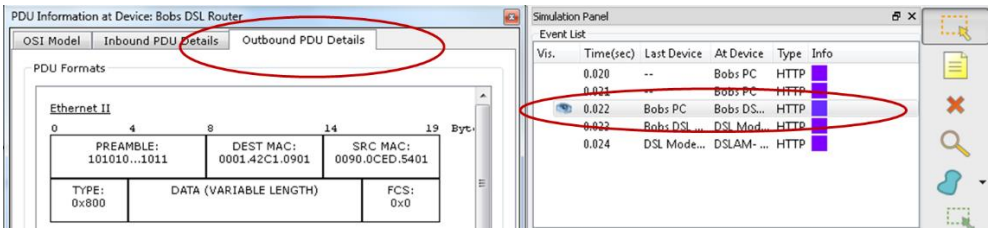
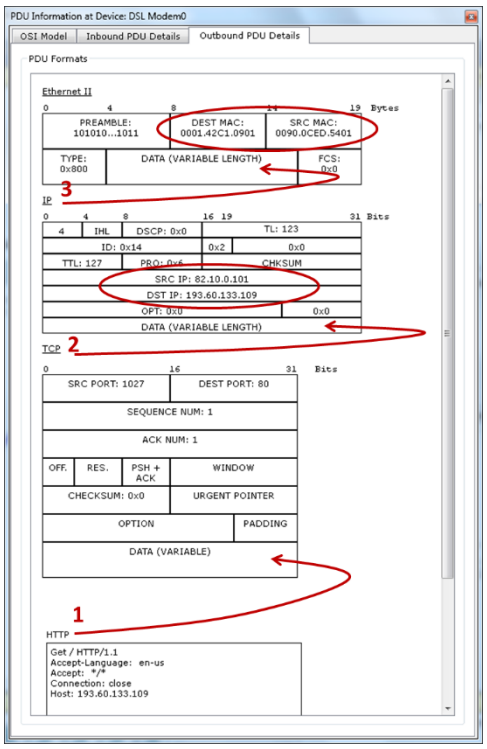


Figure 17 – Protocol Inspection

52. This provides a pictorial representation of all the various network protocols involved in the transmission of this particular packet:



53. Starting at the bottom at '1', you can see that HTTP has issued a request for a web page (GET/HTTP/1.1).

54. It has then passed this to TCP, placing it in the *Data (Variable)* field. Remember that TCP is responsible for chopping up data into chunks suitable for transmission in IP packets, but in this case, the HTTP data is quite small, so this is not necessary. TCP adds additional information to allow it to control the re-assembly of data **segment** in the correct order at the receiving device.

55. At '2', TCP places its data segment into the *Data (Variable Length)* field of IP, which adds additional information such as a destination and source IP address to create a **packet**.

56. At '3' IP places its data packet into the *Data (Variable Length)* field of an Ethernet (it's actually FastEthernet) **Frame**, which adds information such as destination and source MAC addresses.

Figure 18 – Detailed Protocol Inspection

Task 4 – Challenge Activity: Investigate email operation.

57. In Simulation mode, exchange emails between Bob and Ann, and analyze the packets as you did for HTTP. Is there any difference in the protocols that are being used to exchange emails? Explain any differences you discover.

58. Which devices in the CASBIT network will use the addresses contained in a **frame** to make forwarding decisions?

59. Which devices in the CASBIT network will use the addresses contained in a **packet** to make forwarding decisions?