Q1
TCP - Transmission Control Protocol: is one of the main protocol used in the TCP/IP protocol stack. TCP is a connection ordinated protocol which means it provides reliable end to end communication. TCP is how we establish and maintain a network conversation through which data is exchanged. TCP does this by accepting data from a stream of data and devices it up into smaller parts and adds a TCP header. The TCP segment is encapsulated by an IP.

802.11 - IEEE 802.11: is a set of protocol and standards used for specifying MAC & physical layer protocols for implementing WLAN computer connections. One of its main functions is to transmit data over a wireless network.

DNS - Domain Name System: DNS assigns various information with domain names assigned to each of the participating entities. DNS helps users of the internet and network devices discover websites by using readable host names in place of an IP address because DNS keeps a list of domain names and translates them to IP addresses.

IP - Internet Protocol: is the main protocol in the TCP/IP stack as it is responsible for relaying packets across network boundaries by routing and addressing these packets of data so that they arrive at the right destination. IP does this by attaching IP information to each packet and this helps the router know the correct place to send the packet.

Q1 d)

DHCP - Dynamic Host Configuration: DHCP sends a series of packets to get an IP address. These packets are called DHCP DISCOVER, DHCP OFFER, DHCP REQUEST, DCHP ACK. DHCP
DHCP DISCOVER - The Discover packet contains the client's computer name and MAC address so the DHCP servers can respond to it with an IP address lease.
DHCP OFFER - DHCP servers on the network respond to the broadcast with a "DHCP Offer". The DHCP server reserves an IP address for the client and makes a lease offer by sending an offer message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.
DHCP Request - In response to the DHCP offer, the client replies with a request message. This message is broadcast to the server, requesting the offered address. A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer. Based on the required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they have made to the client.
DHCP Acknowledgement - When the DHCP server receives the request message from the client, the configuration process enters its final phase. This phase consists of sending a DHCPACK packet to the client, which includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed. The protocol expects the DHCP client to configure its network interface with the negotiated parameters. After the client obtains an IP address, ARP prevents address conflicts caused by overlapping address pools of DHCP servers.

ARP - Address Resolution Protocol: the ARP finds the MAC address of the host machine from its know IP address. ARP converts an IP into a MAC address. We need the MAC address because they are used to identify machines within the same network on layer 2, while IP addresses are used on to identify machines throughout different networks.

- Protocol - A protocol is a set of standards and policies for transmitting data between electronic devices such as computers. Policies are made up of rules, procedures and formats that define communication between two or more devices over a network. They are needed to change data types, to ensure that data sent correctly, synchronisation of data, etc.
- Response Code 200 (in the context of HTTP) - This is the 200 OK response code. 2xx are successful requests. 200 OK means that the request was successful. Successful requests mean that your request to access a file was successful.
- Communications Medium - Communications Medium refers to the physical channel through which data can be sent and received. Examples of physical mediums are telephone networks , cable television or internet access , and fiber optic-communication. Examples of wireless mediums are radio broadcast , Infrared, satellite, microwave, and Bluetooth.
- Cyclic Redundancy Code (CRC) - CRC is an error - detecting code. Parts of data entering get a short check value attached. This value is based on the remainder of a polynomial division of their contents.
- Retransmission - Retransmission is the resending of packets that have been lost or damaged. These packets my be lost or damaged due to network congestion. TCP uses positive acknowledgement with retransmission to handle lost packets. If it has to send multiple retransmissions, it will eventually give up and declare that it is impossible to communicate.
- Protocol Encapsulation - Protocol Encapsulation is the process of taking data from one protocol and translating it into another protocol. For example a HTTP encapsulated in TCP/IP protocol stack.
- Protocol Layering - Protocol Layering is a technique used to simplify networking designs by splitting the layers into functional layers and assigning protocols to perform the task each layer has been assigned to do. It is important because it allows different types of network software and hardware to communicate.
- Acknowledgement - Acknowledgement is also known as ACK. It is a signal, used by many protocols, that is sent during communication processes or devices to notify the sender that their packet has been received. Protocols such as DCHP and TCP.
- Signal Attenuation - Signal Attenuation refers to any reduction that may occur in the strength of a signal. The signal may be reduced for a number of reason but one main reason is noise. Extra noise can be created from radio frequencies, electrical currents, and wire leakage.
- Payload - Payload refers to the part of data in a packet that is not a header or trailer. Headers and trailers are attached for transport but are discarded when the packet reaches its destination. This data in the middle can be referred to as actual data.
- Heuristics - Heuristics is a type of routing system. It is used to determine and describe problems that may arise in a network topology.
- GET - GET is a HTTP request. The GET method is used by clients to request data from a web server. The GET method is used to request an entire representation of the specified resource.

- Physical Address - Physical Address refers to the media access control (MAC) address of a device. A MAC address is unique to every device and is used to identify a device within a network.
- Reliability - Reliability is an attribute that consistently preforms according to its specifications.

Q2 b)

DNS - Domain Name System: Domain Name System: DNS assigns various information with domain names assigned to each of the participating entities. DNS helps users of the internet and network devices discover websites by using readable host names in place of an IP address because DNS keeps a list of domain names and translates them to IP addresses. It starts when visiting a website. If the information the user is looking for isn't stored on the computer the computer will then make a request to the DNS server. The DNS server then translates this domain name and returned the IP address.

Q2 c)

Ping - The Ping command used in the terminal can be used to determine of a website is reachable and to ensure a host computer the user is trying to reach is opperating. . Ping is an internet program that allows user to check that a particular IP address (the website) exists and if it accepts requests. The Ping works by sending an ICMP Echo request to a specified destination on the network and waiting for reply.

Q3 a)
Packet 115 - TCP SYN (Synchronise) : the TCP SYN message is used to start and establish a connection between client and server. Its function is to synchronise sequence numbers between devices
Packet 117- TCP SYN ACK (Synchronise and acknowledgement): The TCP SYN message from local device and the TCP ACK is the acknowledgment of the previous packet.
Packet 118 - TCP ACK (Acknowldgement): The TCP ACK message is used to confirm that the syn message have been received.
Packet 119 - HTTP GET: The HTTP GET method is used by clients to request data from a web server. The GET method is used to request an entire representation of the specified resource.
Packet 121 - HTTP Response Code 200 OK: 200 OK means that the request was successful. Successful requests mean that your request to access a file was successful. In this case the access to the HTML was successful.

Q3 b)
Clear ARP cache - arp -d
Info about machine - ifconfig /all
Clear DNS cache - ipconfig /flushdn
Finished with an IP - ifconfig /release
New IP - ipconfig /renew

Q3 c)
Pipelining is used when there is little delay. The purpose of the pipeline protocols is that the sender can send more than one packet before it receives acknowledgment for the previously sent packet. Purpose of pipeline protocols as TCP is to increase the usage of available link capacity. It is a much faster way of sending data than ‘stop-and-wait’.