THE THREE WAY HANDSHAKE

SOME DEFINITIONS:-

Routing Table: A table which stores information on how to reach some destination network. It usually has two or more columns, depending on the routing protocol used. It will at least have a *destination address*, that is, an IP address in the destination field of an IP header examined at the network layer, and a *next-hop address*, which is the IP address of the next interface that a packet should be forwarded to in order to reach the destination address.

MAC Address: A globally unique address consisting of 6 bytes of data which represents a card on the internet. The first three octets of the address(if the second least significant bit of the first octet is set to 0) represent the manufacturer, and the last three bits represent the Network Interface Controller of the network card. Required by the ethernet protocol of the data link layer.

IP Address: A 4 byte number used to address networks by the Network Layer's Internet Protocol(IP). It is divided into 2 parts, where the prefix represents the network id of an address, or the address of a network, and the suffix is the host id, or the id of a device on that network. The network id and host id are obtained by means of a network mask.

TCP Port: A number which allows the protocol handling traffic at the traffic layer to demultiplex data(which may come for various processes running on the device) and deliver it to the correct device.

TTL : Time To Live. A field in the IP header which tells a device that receives it how many hops the packet is allowed to live through before being dropped. This is done to reduce traffic by preventing the packet from looping endlessly in case of some routing error. The value in this field is decremented with each hop.

The Three Way Handshake - The three way handshake is how connections are established at the traffic layer using the connection-oriented TCP protocol. It comprises of three messages, the SYN message, sent by the computer wanting to establish a connection with another computer, the SYN/ACK message, which is sent in acknowledgement of the SYN message sent by the computer requesting a connection, and the ACK message, which is sent to acknowledge the SYN/ACK message. Once these steps are complete, a connection is established between the two computers, and they may start sending data to each other.

THE HANDSHAKE:-

I) SYN

Computer A

Application Layer:

A browser on Computer A needs an HTML document served by Computer B's server application running on port 80. The browser was supplied with Computer B's IP Address, 10.1.1.10. The browser requests a connection with the 10.1.1.10:80 from it's traffic layer running TCP.

Traffic Layer:

It is found that the ephemeral port 62345 is free and may be used in establishing a connection. 62345 is filled in the 16 bit source port field, and port 80 is filled in the destination port field of the TCP header. A sequence number is also found and filled in the sequence number field of the header, and the control flag SYN is set. A checksum is calculated for the TCP packet and filled in the checksum field, the length of the header is filled in the header length field, and then the packet is passed down to the network layer.

Network Layer:

IP is used at this layer. It is found that the address of Computer A is 172.16.21.21, and that Computer A resides on a network 172.16.21.0/24, which is not where Computer B lives. Computer A knows from its routing table that it has to send a packet to a router whose interface that faces Computer A's network has an address of 172.16.21.1. Computer A fills the source address field in the IP header with 172.16.21.21 and the destination address field with 10.1.1.10, version with 4, TTL with 64, calculates the header length length and total length and fills them in, and finally calculates the checksum and fills that in. It attaches the TCP packet to the IP header to form the IP packet and passes it down to the data link layer

Data Link Layer:

Ethernet is used at this layer. It knows that it has to send data to the router situated at 172.16.21.21, but it can't find said router's MAC address on its ARP table. Therefore, it sends out an ARP broadcast(an ethernet packet with the destination MAC address octets all set to FF). Every other device on the network ignores the request(because they drop it once the networking stack examines the IP address and finds that the request wasn't addressed to them), but the router with the IP address 172.16.21.21 sends an ARP response back to Computer A with its MAC address, 44:55:66:77:88:99. This information is used to make an entry on the ARP table.

Computer A then constructs an ethernet frame using the MAC address received in the response as the destination address, the IP packet as its payload, and its own MAC address as the source address. It then calculates the checksum and fills it in in the tail of the frame.

Physical Layer:

Computer A is connected to the router via a cat5e cable. The ethernet frame is sent across this cable by modulating the electric signal on the cable with the message.

Router

Physical Layer:

Receives signal from Computer A on one of its ports.

Data Link Layer:

Examines the destination MAC address, finds that it matches its own MAC address, therefore keeps the ethernet frame. Then, it calculates the checksum of the packet using CRC, and compares it to the checksum on the frame. If it finds that they don't match, it knows that there was an error during transmission, and it drops the frame. If they match, it decapsulates the message and passes it on to the network layer.

Network Layer:

Calculates the checksum of the IP header, compares it to the checksum in the IP header checksum field, finds that they match. The destination address is then compared to the entries it has on its routing table and the router finds it belongs to a node on a network it is connected to, which it faces on an interface with an IP address of 10.1.1.1. It then decrements the TTL and recalculates a checksum for the IP header. Once its done, it passes the IP header down to the data link layer.

Data Link Layer:

Consults its ARP table, finds that it already has an associated MAC address for the destination IP address, fills this in the destination MAC address field of the header, fills its own physical address in the source field, calculates a frame check sequence and places it in the tail of the header passes the ethernet frame down to the physical layer.

Physical Layer:

Sends data by modulating electrical signal.

Computer B

Physical Layer – Data Link Layer:

Same as Router

Network Layer:

After calculating and comparing checksums, finds that the destination IP address matches its own IP address, so it strips the IP header away and passes the remaining data up to the traffic layer.

Traffic Layer:

Calculates checksum, compares it to checksum in header, finds that they match and knows that the message arrived intact. Examines destination port, sees if there is any service listening on that port. In this example, there is. It looks at the control flags and finds that the SYN flag is set, so it looks at the sequence number. It decides to accept the connection, and so it constructs a response. The source and destination ports are switched, the sequence number of the received packet is used to fill the acknowledgement number of the response packet. It fills its own sequence number in the sequence number field, and sets the SYN and ACK flags in the control fields section of the header. It then passes the TCP datagram down.

II) SYN/ACK

Every subsequent step happens in a similar manner to how it did when Computer A sent its message to Computer B.

III) ACK

Once Computer A gets Computer B's SYN/ACK message, it constructs a response to B where acknowledgement = received packet's sequence number and ACK=1, and sends this to B. B receives this, the three way handshake is complete, and a connection between A and B has been established.