Transport And application Layer

the physical layer , data link layer and the network layer defines how a node communicate with other node at the same network or the other network . But the individual program in a computer need to communicate with eatch other too.when we say we want to send data to another computer we actually ment we want our computer program to communicate with our network resources .so the different process of out computer need to communicate with the network.transport and the application layer do. Transport allows traffic to be directed to specfic network application through port.and the application layer allows these application to communicate in a way they understand

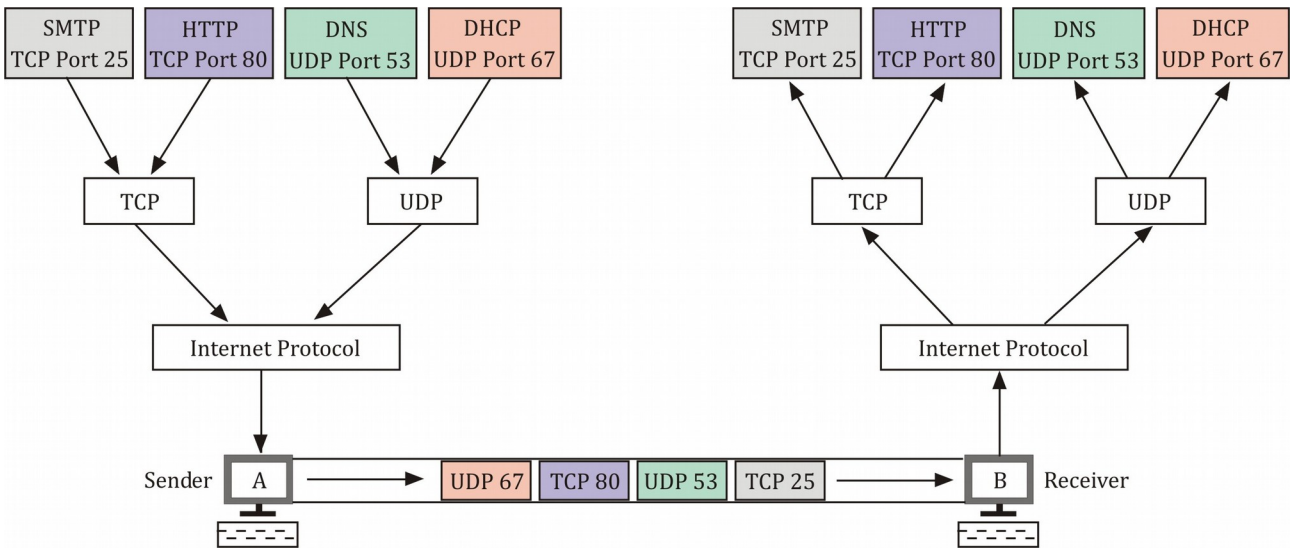
Transport Layer

Transport layer has a unique job which makes it so special.that is multiplexing and demultiplexing along with that it also does the error checking and data verification

lets discuss the demultiplexing first. When a traffic come to a node not all the information is served for

the same purpose in other word for different traffic can be send for different application. Suppose a server can run the database server,file server,mail server at the same time and when a data segment is coming to a node some of them may be intended for the database application some of them may be mail application .The Transport layer examine this the receiving process and direct the signal to the process .Thats how you can serve multiple application in a computer and still the correct data goes to its intended application.

Multiplexing is the opposite process in networking. the job of the multiplexing is gathering data from from different application/process in the computer and then enveloping with the header information and then passing the data to the network layer



now the question arise is how the network layer identifiy the different application ?
Well the find it through port.Port is a 16 bit number that is used to direct traffic to a specific services running on a networked computer.different services on computer run on different port .for example http run on port 80 and https runs on port 443
here is a list of different application running on different port number,

Service Name	Port	Comment
ftp	20	FTP - data
ftp	21	FTP - control
ssh	22	SSH Remote Login Protocol
telnet	23	TELNET
smtp	25	Simple Mail Transfer Protocol
domain	53	Domain Name Server
bootps	67	Bootstrap Protocol - server
bootpc	68	Bootstrap Protocol - client
tftp	69	Trivial File Transfer
http	80	World Wide Web
pop3	110	Post Office Protocol - version 3
sunprc	111	SUN Remote Procedure Call
Netbios-ssn	139	NETBIOS Session Service (SMB)
imap	143	Internet Message Access Protocol
snmp	161	Simple Network Management Protocol
bgp	179	Border Gateway Protocol
irc	194	Internet Relay Chat Protocol
ldap	389	Lightweight Directory Access Protocol
https	443	http secure
ipp	631	Internet Printing Protocol
wins	1512	Windows Internet Name Service
nfsd	2049	NFS server
squid	3128	Squid Web Proxy
mysql	3306	MySql

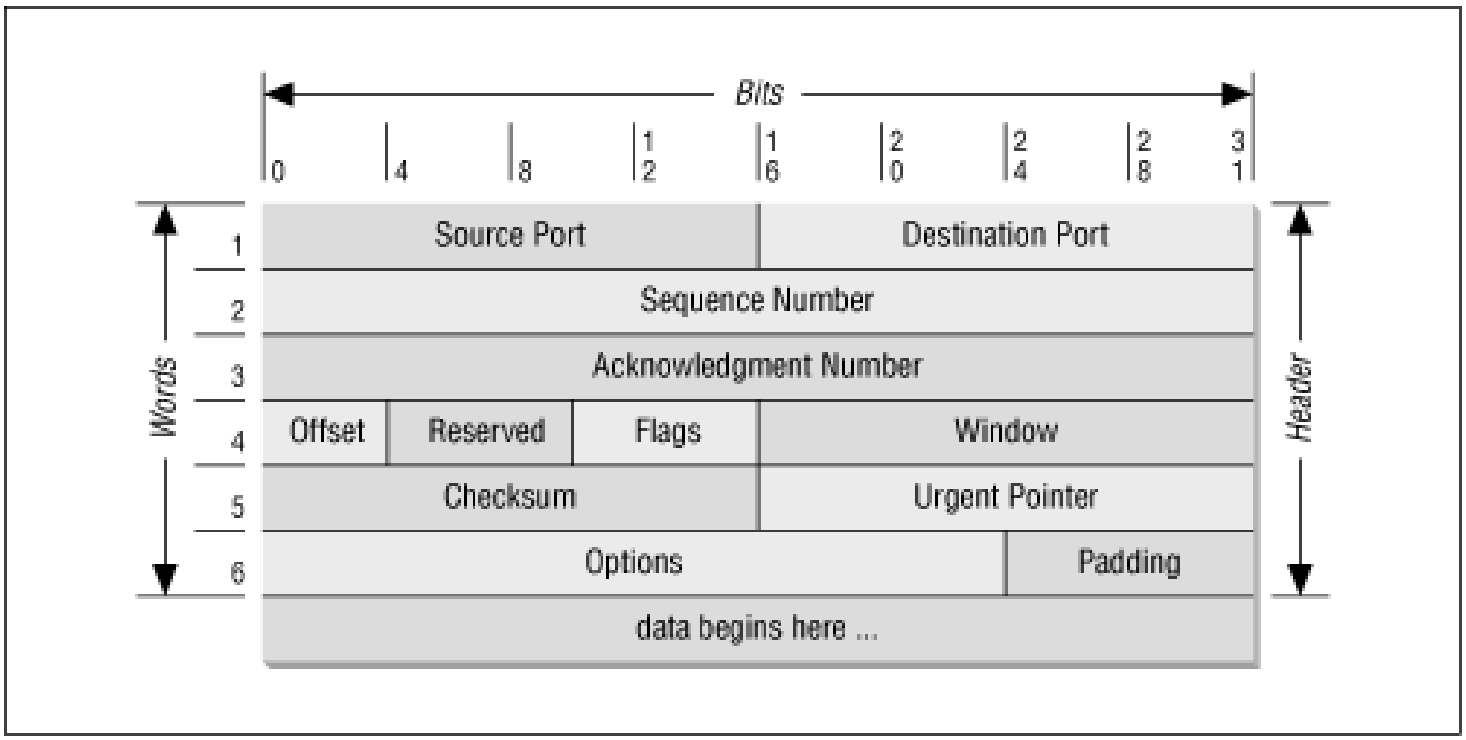
so if a client request a web page from a server which has ip address 10.0.0.200. the traffic will be redirect to the port 80 of that server and the full address will be ip address and the port address joining with a colon[:] like 10.0.0.200:80 and then this address called socket address and socket port. Now if the same server run a database server .then the request for database will be redirect to port 3306.this is possible for multiplexing and demultiplexing

TCP

lets talk about the TCP (transmission Control Protocol).TCP is a networking protocol that allows two or more computer to communicate with each other.

previously we said that an ethernet frame actually encapsulated a ip datagram in his payload section.and then we say the ip datagram also have a payload section.now this ip datagram encapsulate the TCP segment in this payload section.
This TCP segment also have a TCP header and a Payload section.To understand how data is in a correct

port .we need to analyze the TCP header of a TCP segment



A TCP header is based on these following section

Source port

source port is a ephemeral port. ephemeral port is temporary communication hub used for the communication .in a client server communication the client initiates the communication with a server .when

we say the client initiates a HTTP connection in port 443 or 80 we actually mean the destination port but the client’s port is chosen from a ephemeral port range and this range is varied depending on your os . It make sure that the response of the server that is generated from the server due to the request from the host can reach to the correct client application.for example if you browsing the web with a web browser then the source port assure that the response from your server will directly go to the browser .

Destination Port

destination port is the port of the service that the traffic is intended for

Sequence Number

the Sequence number is a 32 bit number that is used to identify the sequence of its segment.using this number the tcp segment finds its position in a sequence.like the layed discussed the TCP segments are also break down into pieces

Acknowledgment Number

it is a 32 bi number that is used to find the next expected segment.

Header Length

this is a 4 bit number that tells the length of the header .So the receiving end understand where the payload begins

Control Flag

TCP established a connection using different control flag.there are six different control flag

1)URG (urgent) a value of one here indicats that the segment is considered urgent and the urgent pointer field has more data about this.this is normally not seen
2) ACK (acknowledged) A value of one in this field means the acknowledgment number field should be examined
3) PSH(push) it means the transmitting data wants the receving devices to push the buffered data to the application as soon as possible

buffer means a part of the data that is stored in a place before sending somewhere else
4) RST:If one of the sides in a TCP connection cant properly recover from a series of missing or corrupted segment this side send the signal to repeat the whole process again

5)SYN (synchronize) it is used when first establishing a TCP connection and make sure the receiving end knows the sequence number field
6)FIN (finish) it means the data transfer is finished and terminate the connection

TCP Window
this is a range of sequence number that might be sent before an acknowledgment is required

Checksum value

its 16 bit number.its operate just like the checksum value of the ip datagram at the ethernet level.the receiving devices generated the checksum of the entire segment and compare with the segment that is in the header just to make sure that there is no error and the data is intact

Urgent Pointer Field

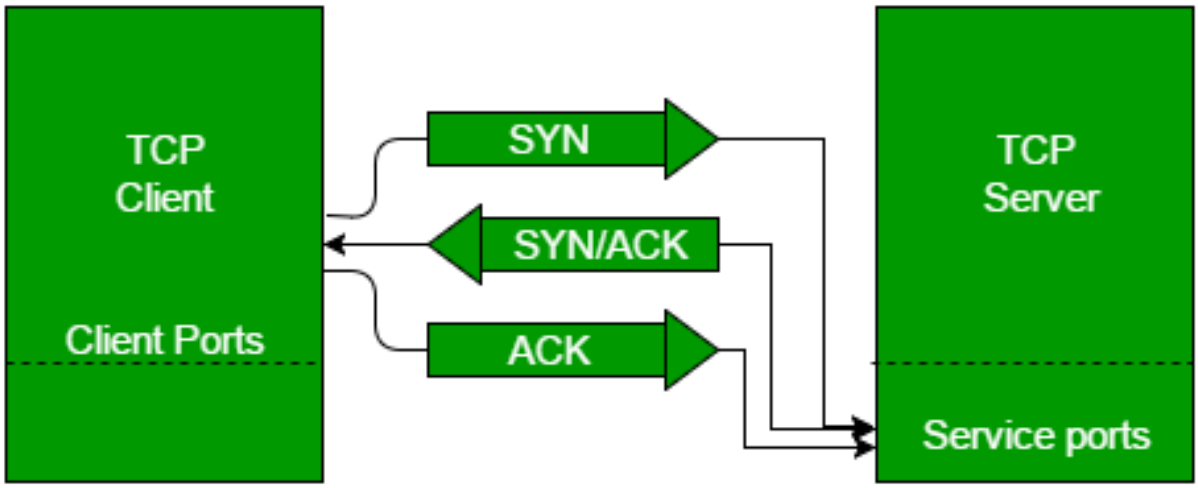
It is used with the TCP controll flags to point out perticular sengment that might be important than the others

paddding

padding is a list of zeros that is used to fill up the space so the data payload can start at the exact location

Establish a TCP connection
The Three Way Handshake

Handshake is a way for devices to ensure that they are speking in the same protocol and also they nderstand each other



A TCP connection is made with a three way handshake.

1) First the Client send the server a TCP segment a SYN flag to establish a connection and check the sequence number filed for starting a conversetion

2) if the server is ready for that it will send the client both the SYN and the ACK signal to accept his request
3) Then the client send another ACK signal that the client understand the receiver is ready to communication

for closing the function Four way handshake happened

1) server send the FIN flag
2) The client send the ACK flag
3) is the client ready then it again send the FIN flag
4) at last the server send the ACK flag and terminate the connection

SOCKET

Socket is a endpoint of a potential TCP connection.you can send data to any port but you will get response if any program opens a socket in that port

* Listen: it means the socket is ready and listening for incoming connections.if you ever develop any server

side application then you are already very familiar to this

*SYN-SENT: it means client send a synchronization request but the connection is not established yet.since the client initiate a connection you can see it only on the client side

*SYN-RECEIVED:server send this when any socket in the LISTEN state has received the synchronization request from the client and send a SYN/ACK back

*ESTABLISHED: you see this state on both client and server side when the connection is finally established

*FIN_WAIT: this state means a FIN is sent by the client

*CLOSE_WAIT: The connection is closed at TCP layer the application is still holding the socket and haven’t released yet

*CLOSED: Connection is terminated and no transaction is possible now

CONNECTION ORIENTATED PROTOCOL

When a connection is established and ensures that all data has been properly transmitted .TCP is a

connection oriented protocol .this way the both sending and receiving node make sure that data is definitely delivered .
Checking the data is very important when sending data because even a single bit missing due to any reason can discard the whole segment of the data.

The transport layer different ACK signal for assuring sending and receiving data.and if it not send properly the data is requested to send again.
In the datalink and the network layer the checksum is used for checking the data integrity.but if the checksum is not matched thse two layer dont send the request to resend the data .it directly discard the data .Only the TCP layer knows when to resend the data.because it send bit by bit with ACK flag

CONNECTION LESS PROTOCOL

when TCP is used a lot of other traffic like ACK,SYN,FIN is used for assurance that the data is sent.If The data is not that important then you can avoid this using a connection less protocol called UDP it dont send any ACK flag.it just set the destination ans send the data.Souppose you are watching a video for best experience you sant every single frame but if some of them loose on its way it still does not matter The video is still watchable .you can send higher

quality video if you use the UDP because the bandwidth used for the TCP flag is no longer used

Firewall

firewall is a device and can be a program that blocks traffic that meets certain criteria.Firewall operate in Transport layer most of the time.Firewall in transport layer generally blocks traffic on certain port based on their configuration.you can block certain port and certain service for the public and allowing them for some soecfic people with firewall