Computer Networks

Gateways : Way to connect different types of networks. Like when we have different protocols at the network layer. Here routers fail!!!

IP and ATM we want to connect. Then we use Gateway.
Gateways are used as protocols converters
Gateworks work at the Application layer.

Advantages
Protocol converter
Proxy
Deep packet inspection
Inflow(x) is greater than Outflow(y) then buffer added is (x-y)t

Collision domain and Broadcast domain

Wire, hub, repeater, bridges and switches are LAN components.
The broadcast domain is LAN only
Router and gateways divide broadcast domain as well as collision domain
Bridges/Switch/Hub/Wire/Repeater never stop any broadcasting packet.
Bridges and switches reduce collision domain

Spanning Tree Algorithm

Inside a LAN, we are avoiding Infinite loop using spanning tree algorithm
In Internet, we avoid Infinite loop using TTL
Facility of TTL is not provided in Ethernet that is why we use a spanning tree algorithm to avoid infinite loops. We do not have TTL

Spanning Tree Algorithm
Every bridge has a build in ID. The one with the smallest ID is taken as the root bridge.
Mark one port of each bridge which is closest to the root bridge as the root port
Every LAN chooses a bridge closest to it as a designated bridge for that LAN. Make the corresponding port as designated port.
Mark the root port and designated port as forwarding ports and block remaining

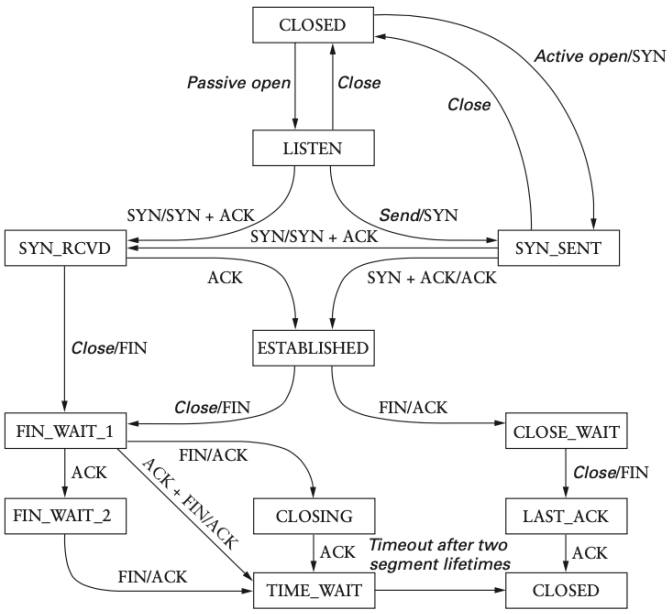
Total Length: TCP
Total length is 16 bits
With 16 bits we can represent 65535 unique numbers
Max size of segment at Transport layer is 65535-20 i.e. 65515 payload/data
Application layer can give any amount of data to the transport layer.
Max amount of data can come and sit in TCP is 65495 amount of message of Application layer
That is why the Transport layer's responsibility is segmentation.
Ethernet can only handle packets of size 1500 bytes only.
When a network layer divides packets so that they can come and sit in an ethernet frame it is known as fragmentation.

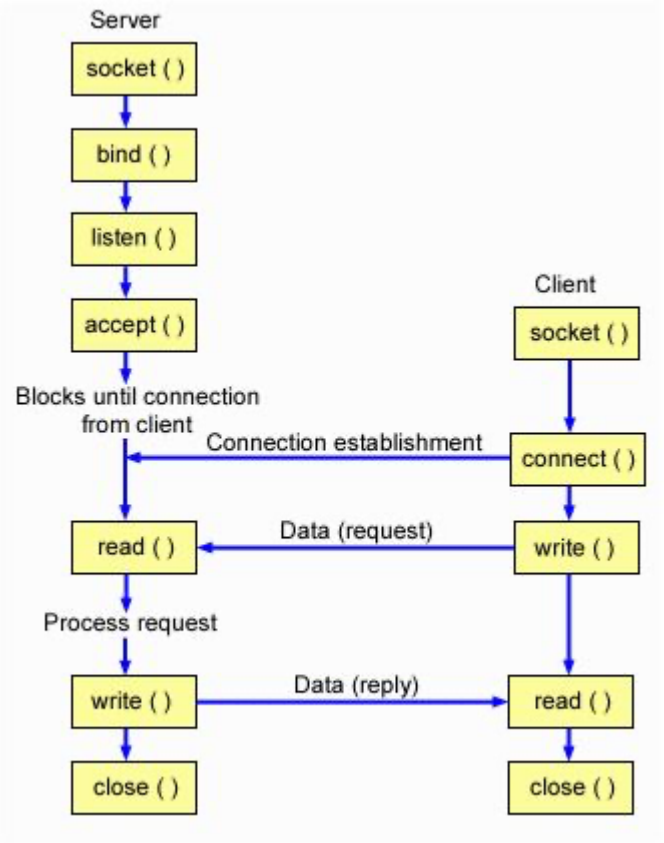
We dont send more than what a data link layer can carry.
Framing is done at DLL
Fragmentation is done at NL
Segmentation is done at TL
Network layer is the bottleneck.
Doing segmentation once and then fragmentation is not good
Transport layer will do something clever
Transport layer checks who is bottleneck and then divide the packet considering it, so that it can go and sit peacefully in the DLL
1500 of ethernet frame, 20B is NL header
Now 1480 is TL data + header
1460 is the TL payload
AL will divide like every packet into 1460 and doing this will solve our problem.
Segmentation is done at TL wisely such that there is no need of fragmentation
Fragmentation is not done at Sender
Fragmentation is done at intermediate routers.

ARP: IP not known but MAC is known. So sending MAC of someone on broadcast and getting IP as a unicast is known as ARP

Distance vector uses RIP as subroutine
Count to infinity problem: resolved by split horizon and split horizon poison reverse

OSPF : link state routing: every node has global info
It uses flooding





Persistent Timer avoids deadlock situations by sending a probe of 1B to know what the current situation is.
Karn's algorithm ignores retransmitted packets while updating the round trip time estimate.

TCP TIMERS

AIMD algo: on timeout, go to 1 and start Slow start phase till half the previous threshold.
On 3 duplicate ACK's reduce the congestion window to half the threshold and go into congestion avoidance phase(increase by 1MSS).

SBLAC socket bind listen accept RCV SND close for TCP server
Socket CONNECT close for TCP client
The binding procedure on the client is entirely optional.
Client moves FIN-Wait-1 → FIN-Wait-2 → Timeout → Closed.
Loss of Ack from Client does not affect termination of connection
Bandwidth delay product is B*Tp for single side, and B*RTT for both the sides.
DNS maps hostnames to IP addresses
Computer networks key pointers
The same subnet mask was applied in CIDR. This was a waste of space. Waste of space on the network a is higher than b and that of b is higher than c and so on.
VLSM allows you to use different masks for each subnet.

For M hops and N packets –

```
Total delay
= M*(Transmission delay + propagation delay)+
                (M-1)*(Processing delay + Queuing delay) +
                (N-1)*(Transmission delay)
```

HTTP is stateless, and by default uses persistent mode where there is only 1 connection open.
For persistent, time is Tt+x(RTT).
For non persistent , time is Tt+(2RTT)(1+x)
TCP uses window size to provide flow control

1. Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. Flow Control: The data rate must be constant on both sides or else the data may get corrupted thus, flow control coordinates that amount of data that can be sent before receiving an acknowledgement.

Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

In IPv4 header, the IDENTIFICATION NUMBER field is needed to allow the destination host to determine which datagram a newly arrived fragment belongs to.
The distance-vector routing protocol sends its complete routing table out all active neighbouring interfaces at periodic time intervals. Link-state routing protocols send updates containing the state of its own links to all routers in the internetwork.

Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP	TCP
Remote terminal access	Telnet	TCP
Web	HTTP	TCP
File transfer	FTP	TCP
Remote file server	NFS	Typically UDP
Streaming multimedia	typically proprietary	UDP or TCP
Internet telephony	typically proprietary	UDP or TCP
Network management	SNMP	Typically UDP
Routing protocol	RIP	Typically UDP
Name translation	DNS	Typically UDP

Congestion control cannot be avoided, but it is less in packet switching as compared to circuit switching

If a DF(do not fragment) bit is set and a router needs to fragment the datagram to send it further then ICMP error message must be sent to the sender.

If TTL is exceeded then also it should report to the sender by sending ICMP error message.

A dedicated switch port is required for each full-duplex node

Hubs can only run in half duplex mode

Half-duplex Ethernet shares a collision domain and provides a lower effective throughput than full-duplex Ethernet

Example 12.3

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second
b. 500 frames per second
c. 250 frames per second

Solution

The frame transmission time is *2001200* kbps or 1 ms.

a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ or $S = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.
b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is *(112).* In this case $S = G \times e^{-2G}$ or $S = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.
c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.