- Destination MAC address is the MAC address of the gateway iff the final target is NOT in the same LAN. Destination and source IP addresses are ALWAYS the ultimate source and destination IP address.
- In each BSS, there's only one frequency. AP is NOT a transparent device.
- In CSMA/CA, a node detects collision occurs when it does not receive ACK. If so, node goes back to sensing, DIFS and even longer random wait period before sending.
- There's no guarantee for delivery in CSMA/CA.
- CSMA/CA defines several IFS (Inter-frame Spacing), a Node cannot transmit continuously.
- Reason CSMA/CD won't work in Wireless: Signal Fading, Hidden Terminal, Interference, Multi-path.
- In CSMA/CD based LAN, the stations must always listen to the media even if they have no frames to transmit.
- NAT is a proxy server allowing hosts on the internet the ability to communicate with hosts on a private network.
- TCP uses checksum, ACK, and time-out mechanism for end-to-end error detection and control.
- Route calculation is a function of the IP protocol.
- IP is implemented in every end system, and every router in the network layer. Transport Layer Protocol (TCP/UDP) is implemented in end system only, not in router.
- IP is best effort service, reliability is added in TCP in transport layer
- IP checks header for error only
- TCP & UDP checks payload for error
- The port field in the TCP/UDP header is to identify the application to which an IP packet should be delivered
- UDP provides for error-free delivery of the message to the application layer.
- Routers forward traffic (packet) based on destination net ID
- Packet is always addressed by the ultimate source & destination. No place for router IP address.
- Every fragmented packet will have the same identifications.
- The length of the header & payload exceeds MTU, it means fragmentation is required.
- MTU does not include Header and Trailer of the **Frame.**
- Fragment payload has to be multiple of 8, 20 is the packet header.
  ie 8*x + 20 <= MTU, x fragment payload. 8*x is the actual payload in the fragment
  Difference, when TCP layer segment/datagram is passed to IP layer, the data + TCP header is considered as data in the IP packet.
- Destination IP is responsible for putting fragment back to a packet.
- 1^{st}. fragment will have offset of 0
- 2^{nd}. Fragment will be offset from the **start** of the packet payload by the size of 1^{st}. fragment payload
- IP Fragmentation is not necessary if every transit network on the route has at least as large as the MTU as the source network.
- IPv4 address: 32bits, MAC address, 48 bits
- Private host communicates with a public host via NAT
- The number of addresses in each subnet should be a power of 2.
- Subnet structure of a network is never visible outside of the organization's private network.
- IP Forwarding: only interested in the next route
- IP Routing: process of discovering and selecting the path.
- Distance Vector: RIP, Routing Info Protocol
- Link State: OSPF, Open Shortest Path First
- RIP: Each node shares its routing table with its immediate neighbors **periodically and when there's a change.**
- OSPF, router only sends info iff there's a change in router's status.
- OSPF: Every router will have the exact replicate of the map.
- RIP, router only knows its distance to its neighbors ONLY
- IP is implemented in every end system, including routers
- In link state routing, every router has exactly the same link state database but the routing tables are different in each router.
- If there're 5 routers and 6 networks in an internetwork, there're **only 1** link state database.

- Subnet Masking is the process of extracting the network address from an IP address
- Transport layer is loaded at end system ONLY, not in router.
- TCP Sequence number in the header identifies the number of **first byte** in the payload.
- TCP only ACK bytes up to **the first missing byte** in the stream.
- TCP ACK number in the header is the number of **next byte** expected to be received.
- TCP SYN & ACK segment doesn't carry data, but consumes a sequence number.
- Control segment: No payload, does not consume sequence number.
- Data segment: Send data along with ACK on previous segments.
- TCP Flow control: receiver's advertised window size. Sender won't overflow receiver's buffer.
- TCP Congestion Control: Too many sources sending too much data. Too fast for the network (router side) to handle.
- The minimum window size in TCP is limited by the round trip time RTT of the connection.
- Timeout Expires: reaching capacity of the network (Bandwidth Delay Product).
- Suppose host A send a large file to host B over TCP connection, the number of "unACKed bytes" that A sends can't exceed the size of the receiver buffer.
- Link utilization = throughput/Bandwidth
- Symmetrical Key Cryptography: Shared the same key, both sides use the same key
- Asymmetric Key: Sender encrypts using receiver's public key
  receiver decrypts using receiver's private key
  m = KB+ (KB-(m));
- Digital Signature: message can be viewed, but not altered. It does not provide privacy.
- KDC: generate shared key (Symmetric cryptography) between sender and receiver
- CA: public key distributor. (asymmetric cryptography, decrypted using public key).
- A sender sends an unencrypted message and its encrypted digest over the network, Integrity is ensured in this scenario.
- A sender sends a message encrypted by a public key of the recipient, Authentication is not provided in this scenario. (receiver doesn't know who the sender is)
- A sender sends a message encrypted by a private key of the recipient, Confidentiality is not provided in this scenario. (Anyone can get the public key)

F	Congestion control seeks to prevent sender from overburdening the network and thus from causing the router's buffers to overflow.
F	Switched hubs have multiple broadcast domains whereas shared hubs have single broadcast domain
F	Switched hubs have multiple collision domains whereas shared hubs have single collision domain
F	The maximum window size in TCP is limited by the RTT of the connection
F	TCP has the property of slow start to avoid congestion in the network
F	In switched hubs, all ports are dedicated to the stations attached to them
F	In distance vector routing, each router receives routing tables from every router in the network
F	The ACK number in the header of TCP segment identifies the sequence number of the next segment expected to be received.
F	In switched hubs, all ports are dedicated to the stations attached to them.
F	A network has a faulty router (one produces errors during route calculation). The LS routing protocol is more likely to propagate this route calculation error than a DV routing protocol
F	TTL is a field in the TCP header that keeps track of the number of hops before a router must drop the packet.
F	If all links in the Internet were to provide reliable delivery service, the TCP reliable service would be redundant.
F	In TCP Congestion Control, when a timer expires at the sender, the threshold is set to one half of the previous threshold value.