COE768 Exam Cheat Sheet

F2016

CSMA/Collision Detection (CD)

- Senses before Transmitting (Is Medium Idle?)
- If Idle:Send Frame. Else: Wait until Idle, then send.
- Collision May occur in first T_c seconds of transmission. $T_c = \frac{\text{Len}}{C}$ C=2×10^8
- Collision will make channel unusable for a duration of T seconds, T=Transmission Time of a Frame.
- Transmitting Stn. Monitors the channel. If collision is detected, it ceases transmitting and reschedules it.
- Collision Period = $2T_c$. In LAN, $T_c << T$
- Binary Exponential Backoff: user for re-transmission scheduling.
- Stations involved in collision generate a `rand()` Delay $r = k(2T_c)$, and schedule the re-transmission r seconds after. Stations that generate smallest k will transmit first.
- After m consecutive collisions, the `rand()` val. of k is chosen from the contention window: $[0, 1, ..., 2^n - 1]$, where $n = min(m, 10)$
- After 16 consecutive collisions, MAC sublayer gives up and reports `sysErr` to Network Mgmt.
- Probability of a transmission requiring k attempts: $P_k = P(k^{th} \text{ success}) \prod_{i=1}^{k-1} P(i^{th} \text{ faliure})$
- Expected number of transmissions: $E = \sum_{k=1}^{\infty} kP_k$

Ethernet

- Ethernet Frame (DIX)

Preamble	DA	SA	Type	Data	PAD	FCS

Preamble=7 Bytes of `10101010` and 1 Byte of `10101011`, DA=SA=6 bytes, Type=`0x0800` for IP, `0x0806` for ARP, Data = ≤ 1500 bytes, PAD = 0-46 bytes, FCS 4 bytes.

- If DA+SA+Type+Data+FCS< 64, Insert PAD to ensure 64 byte min is met.
- To Detect Collsion: Min. $\texttt{size}(\texttt{Frame}) = 2T_cR_b$
- Three types of transmission types: Unicast (U), Multicast(M), Broadcast(B).

0 – 2	3 – 5
OUI_ID	M_ID

- `M_ID`: Unique for every device set by the manufacturer, U: `OUI_ID`[0] = `BIN : xxxxxxx0`, M: `OUI_ID`[0] = `BIN : xxxxxxx1`, B: `OUI_ID` = `0xFFFFFF`,

Bridging

- Basic Operation: Promiscuous Mode: Passing Frames are Inspected. If both the Dest. and Src. are located at same side of Bridge, frame is dropped. If different, the frame will be forwarded.
- Frame Forwarding depends on MAC (Medium Access Control) Table

MAC Table	
Host	Port
A	1
B	2

- Backward Learning: Location of Station of Network can be learned dynamically
- Flooding: If Bridge does not know where destination is, it sends frame to all other ports.
- Network cannot contain loops.
- Spanning Tree is required to complete this operation
  - Determine the Root Bridge: Bridge ID = Priority + MAC address
  - The Smallest Bridge ID is the root bridge (unless directed otherwise).
  - Spanning Tree is formed by setting up least cost paths from others bridges and LAN segments.
  - Must find Designated, Blocked, and Root ports.
  - All Bridges send BPDU's which contain: Root BID, BID of sender, and the RPC (Root Path Cost).
  - Initially, all bridges claim to be the root. Lowest BID is chosen as root.
  - Root Path Cost is analyzed at every bridge in order to determine the Root port. The port with the lowest RPC is selected as the Root Port.
  - The Designated Port is determined from the lowest RPC, which will touch another LAN segment.
  - Tie Breaker: If multiple BPDUs from different bridges carried the same RPCs, select BPDU with lowest BID.
  - Tie Breaker: If multiple BPDUs from same bridge, select lowest port ID.
  - Any port not in spanning tree is in the `BLOCKED` state (no data frames can be sent or received. BPDUs can still get through).

VLAN

- One Physical Infrastructure to support logical LANs.
- Different Switch Ports in a LAN can create different VLANS.
- IEEE 802.1Q requires extra 4 bytes

Preamble	DA	SA	VLAN	Type	Data	PAD	FCS

Preamble=7 Bytes of `10101010` and 1 Byte of `10101011`, DA=SA=6 bytes, VLAN=

TPID: 16 bits	PRI: 3 bits	CFI: 1 bit	VID: 12 bits

VID= VLAN Identifier, Type=`0x0800` for IP, `0x0806` for ARP, Data = ≤ 1500 bytes, PAD = 0-46 bytes, FCS 4 bytes.

WLAN

- IBSS (Independent Basic Service Set) BSS, without an Access Point (AP). This is an Ad-Hoc Network
- BBS with AP (Infrastructure BSS) Stations inside BSS usually communicate directly with their AP. A station must first establish a security association with AP before any data transfer can take place (Authentication, Key Generations)
- Extend Service Set (ESS) Extension of BSS+AP, where multiple WLAN connections managed by a distribution system. A station in the network can move to another BSS by associating with another AP.
- Medium Access Control
  PCF (Point Coordination Function): Based on polling by the AP
  DCF (Distributed Coordination Function): Contention-Based, Based on CSMA with CA (Collision Avoidance)
  HCF (Hybrid Coordination Function): Support both polling and contention-based access, support service differentiation
- CSMA/CA
- Collision Detection to hard to implement, Hidden Station Problem: two or more stations that are outside the transmission ranges of each cannot detect their collision, acknowledgment mechanism is used to detect unsuccessful transmission.
- Interframe Space (IFS): Indicates the amount of wait time before transmission attempt. Uses different frame types: SIFS - ACK, CTS (Clear to Send), fragment in DCF mode
  PIFS - Data Frames in PCF mode
  DIFS - Data, RTS in DCF mode
  EIFS - Used when corrupted frame is received.
- Transmission Priority Assignment: SIFS < PIFS < DIFS < EIFS
- Exponential Backoff
- Backoff Time = `rand()`*time slot, `rand()` uniform over interval $[0, CW - 1]$
- $CW_{min} \leq CW \leq CW_{max}$
- $CW_{min} = 8$, and $CW_{max} = 1024$
- If unsuccessful transmission:$CW = 2 \times CW$ else: $CW = CW_{min}$
- Virtual Carrier Sense Mechanism
- In order for a Stn. to send a data frame, the Stn. must send an RTS frame to the AP. This contains the total time required to send the data frame AND Ack.
- Upon reception of RTS, the AP will broadcast a CTS frame. This gives the sender explicit permission and instructs other senders to not send for the intended duration.
- RTS/CTS has relatively small frame sizes and solves the hidden station problem.

To DS	From DS	ADDR1	ADDR2	ADDR3	ADDR4

DS:T	DS:F	ADDR1	ADDR2	ADDR3	ADDR4
0	0	Destin.	Src.	BSS ID	N/A
0	1	Destin.	AP (Sndr)	Src.	N/A
1	0	Recv. AP	Src.	Destin.	N/A
1	1	Recv. AP	AP (Sndr)	Destin.	Src.

Internet Protocol

- Internet Protocol is used to forward datagrams from one net to another.
- Packet (datagram) forwarding inside a net is based on native tech.
- IP Datagram Structure

0	4	8	16			20	24	28 31
Ver	Hlen	TOS	Length					
Identification			D	M	Fragment Offset			
TTL		Protocol	Header Checksum					
Source Address								
Destination Address								
Options(Variable)						Pad (Variable)		
Data								

- Max Length of IP Datagram = 2^{16}
- Version Number (Ver): IPv4 or IPv6
- Header Length (Hlen): Integer Multiple of 4 bytes, Min Len=20 bytes, Max Len =60 bytes
- Type Of Service (TOS): Different types of traffic (VoIP, IP, etc.)
- (D)on't Fragment: Used to calculate MTU. Usually set to '0'
- (M)ore Fragements: If '1', used to indicate more fragments are coming, '0' if this is the last fragment
- Identification used for Fragment ID.
- Fragment Offset = Starting Byte/8
- TTL (Time To Live): Indicates how many networks this packet can traverse
- Checksum: Only checks against the header (uses one's complement).
- Protocol: Identifies the process using IP (UDP, TCP, ICMP, etc).
- IPv4 Address Structure:

0	31
Net ID: n bits	*Host ID: 32-n bits*

- Hierarchical Addressing: All hosts in the same network have the same Net ID. Net ID locates Destination Network, and Host ID specifies exactly the location to go to.
- Address Classes: A has 2^{24} hosts, B has 2^{16}, and C has 2^8
- Address Classes:

Class A: Dot Format: [0-127].h.h.h where h ∈ [0 - 255]

0	31
`0nnnnnnn`	...hhh...

Class B: Dot Format: [128-191].n.h.h where n ∈ [0 - 255]

0	31
`10nnn...`	...hhh...

Class C: Dot Format: [192-223].n.n.h where n ∈ [0 - 255]

0	31
`110nnn...`	...hhh...

- Special IP Address:

0	31
Prefix	*Suffix*

-

Prefix	***Suffix***	***Type***	***Purpose***
All '0'	All '0'	This Comp.	Bootstrap
All '1'	All '1'	Local BCast	BCast on Local Net
Net ID	All '1'	Direct BCast	BCast on Spec. Net
Net ID	All '0'	Net ID	Identify a Net
1110	ADDR	MCast	MCasting
127	Any	Loopback	Testing

- Private Address: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 –Not Globally Unique. Requires NAT for outside communication.
- Packet Forwarding relies on routing table.

Routing Table		
Dest.	Intf.	NextHop
192.168.0.1	eth0	DC
201.234.1.1	eth1	9.10.1.5

- Forwarding Algorithm:

```
if(Dest==NetID of Entry){
if(NextHop == DC)
     Deliver Packet to Dest.
    else:
     Deliver to NextHop.
}
```

Subnets

- Class A and B Have too many address. Class C may have too few.
- Subnetting - Partition the classful network in a number of subnets.
-

Original Prefix	*Subnet ID*	*Host ID*

- Since the length of the Net ID is no longer pre-defined, network mask identifies new Net ID. Let R be the number of required hosts. Then, `Netmask` $= 32 - \lceil log_2(R) \rceil$ where the `Netmask` = to # of bits for masking.
- Can be expressed as Netmask: 255.255.252.0 or 141.117.5.1/22
- Netmask information stored in the routing table, after collecting it from a routing protocol or manual config.
- If R is not a power of 2, go to next power of two. This means the next subnet will begin at this new value.
- Subnet Forwarding:

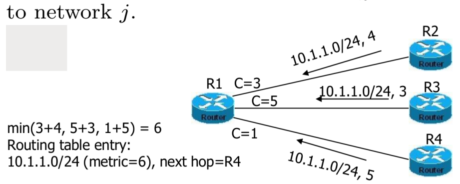
```
for each entry in the routing table:
Dest1=netmask&&Dest.
if(Dest1==NetID of Entry){
if(NextHop == DC)
     Deliver Packet to Dest.
    else:
     Deliver to NextHop.
}
```

Supernets

- Supernetting is also known as Classless Interdomain Routing (CIDR)
- In supernetting, a large number of small nets are aggregated (bunched together) to form a larger network space.
- Supernetting reduces routing table size.
- To aggregate, address space must be contiguous.
- Example:
Address: 192.10.64.0, 193.10.65.0, 193.10.66.0, 193.10.67.0 192.10.[010000]00.0 193.10.[010000]01.0, 193.10.[010000]10.0, 193.10.[010000]11.0 aggregates to: 193.10.64.0/22
- Oversummarization: the aggregated address may not represent the space it claims. Therefore, if a packet matches two entries on the Routing Table, take the Route with longest Netmask.

Routing & ARP

- Route Advertisement: Routers exchange their routing tables periodically.
- Each Advertised route has a metric (distance) associated with it.
- Router i uses $D_{i,j} = min_k(C_{i,k} + D_{k,j})$, $C_{i,k}$ is the cost from Router i to its neighbor k, $D_{k,j}$ is the metric from k to network j.



- ARP: Address Resolution Protocol. Maps the IP to the MAC (Hardware Address)
- In order to resolve the address mapping, the sender sends two Ethernet Frames

`BCast`	`MAC(host)`	`0x0806`	Data	PAD	`FCS`

Data="What is Destinations MAC?". Once the query is answered, the sender sends:

`MAC(Dest)`	`MAC(host)`	`0x0800`	Data	PAD	`FCS`

Data contains the IP of both the sender (Ex: SA: 192.168.1.1, DA 203.45.2.1)