**T04: Data Link Layer II**

**Q1:** Show **byte-stuffing & destuffing** steps for the following data bits if **PPP** **frame** is used.

01000001 01111101 01000010 01111110 01010000 01110000 01000110

**Bitstuffing:**

41 7D 42 7E 50 70 46

Control escape 7D exists, therefore 7E is not a flag

**Bytestuffing:**

Sending:

7D will be replaced by 7D and 5D

7E will be replaced by 7D and 5E

7E 41 7D 5D 42 7D 5E 50 70 46 7E

Receiving:

Replace 7D(next byte) with (next byte)

7E 41 7D 42 7E 50 70 46 7E

**Q2:** Describe the MAC protocol used in IEEE 802.3 Ethernet. Explain the purpose of exponential backoff delay.

CSMA/CD – uses binary exponential backoff delay

After a collision has occurred, each node waits either 0 or 1 time slots before retransmitting

If a further collision occurs each node waits 0,1,2 or 3 time slots

In general, after **n collisions** a random number between **0 and 2n-1** time slot is chosen and the node waits that number of time slots before attempting to retransmit for **n<=10**

**Q3:** How many broadcast domains and collisions domains are in the following network?

Each link on router is a broadcast domain = 7 (broadcast = look at the router connections)

Collision domains = 14 (collision = look for the switch connections)

Wireless Communication

Swtich

Router

Hub



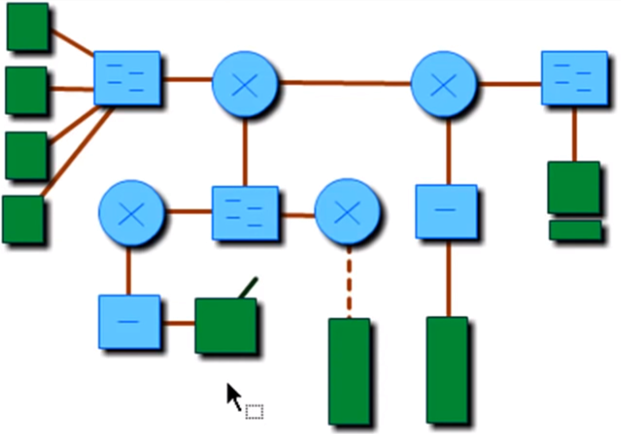
CNCO2000

–

Tutorial 0

4





**Q4:** Why is CSMA/CD infeasible for wireless communication? Name and explain a solution in detail for sharing the wireless medium.

CD is not feasible as the signal can be interrupted by many factors. Detecting a collision is hard, avoidance is preferred. CSMA/CA is preferred

**Q5:** Why is it not safe to connect to a public WiFi access point or hotspot?

Malicious actors can fake an access point by naming it to a reputable network. All network traffic will be routed to the malicious entity.

1 | P a g e