Class Notes

Chapter 6: The Link Layer and Local Area Networks (LANs)

Multiple Access Links and Protocols:

(1) Revision from the last lecture:
   a. Pure-Aloha has maximum efficiency of 18%
   b. Slotted-Aloha has maximum efficiency of 36%

(2) Comparison of Pure-Aloha and Slotted-Aloha:

Comparison Table

Feature	ALOHA (Pure ALOHA)	Slotted ALOHA
Transmission Time	Anytime	Only at the beginning of slots
Time Synchronization	Not required	Required
Collision Window	Twice the packet time	One slot duration
Efficiency	18.4%	37%
Collision Probability	Higher	Lower

Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

(1) Why detecting that shared medium is free is not sufficient to guarantee collision-free communication?

(2) Nodes need to wait random time after detecting a collision to break any synchrony between the colliding nodes. (If different colliding nodes don't wait a different random amount, they will collide again!)

(3) Next important question is that how large such be the wait value?
   a. If the interval to pick random wait value is very small, all colliding nodes will pick pretty much the same value.
   b. If the interval is very large, channel might remain idle, especially under light load conditions.
   c. We need: Start with some reasonably sized wait interval on first collision but make that interval larger when many nodes are colliding on the channel.

(4) Binary Exponential Backoff Algorithm
   a. Used by Ethernet and DOCSIS
   b. If n collision experienced then choose value of K at random from {0,1,2,3,….,2^n - 1}. The maximum value of n is capped at 10

    c. Then wait K * 512 bit time (i.e. K times the time to transmit 512 bits into the Ethernet) (Isn't is curious that smallest Ethernet two packet is 64 Bytes and that is 512 bits?)

(5) Example: Suppose that a node attempts to transmit a frame for the first time and while transmitting it detects a collision.
    a. The node then chooses K=0 with probability 0.5 or chooses K=1 with probability 0.5. If the node chooses K=0, then it immediately begins sensing the channel. If the node chooses K=1, it waits 512 bit times (e.g., 5.12 microseconds for a 100 Mbps Ethernet) before beginning the sense-and-transmit-when-idle cycle.
    b. After a second collision, K is chosen with equal probability from {0,1,2,3}. After three collisions, K is chosen with equal probability from {0,1,2,3,4,5,6,7}. After 10 or more collisions, K is chosen with equal probability from {0,1,2,. . .,1023}.
    c. Thus, the size of the sets from which K is chosen grows exponentially with the number of collisions; for this reason, this algorithm is referred to as binary exponential backoff.

(6) We also note here that each time a node prepares a new frame for transmission, it runs the CSMA/CD algorithm, not taking into account any collisions that may have occurred in the recent past.

CSMA/CD Efficiency:

(1) Go to slides

Taking-Turns Protocols:

(1) Go to slides

CSMA/CD used in older Ethernet (for example 10BASE-T, modern ethernet is switched and hence they have eliminated the collision problem, or more accurately have transformed that problem into queuing and congestion problems).

CSMA/CA (CA for collision avoidance) is used in 802.11 (WiFi)

Address Resolution Protocol (ARP):

(1) From Wikipedia:

Offset	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	3
0	0	*Hardware Type (1)*																*Protocol Type (0x0800)*														
4	32	*Hardware Length (6)*								*Protocol Length (4)*								*Operation*														
8	64	*Sender Hardware Address*																														
12	96																	*Sender Protocol Address*														
16	128	↪ *Sender Protocol Address (cont.)*																*Target Hardware Address*														
20	160																															
24	192	*Target Protocol Address*																														

Hardware Type (HTYPE): 16 bits

This field specifies the network link protocol type.[2] In this example, a value of 1 indicates Ethernet.

Protocol Type (PTYPE): 16 bits

This field specifies the internetwork protocol for which the ARP request is intended. For IPv4, this has the value `0x0800`. The permitted PTYPE values share a numbering space with those for EtherType.[2][3]

Hardware Length (HLEN): 8 bits

Length (in octets) of a hardware address. For Ethernet, the address length is 6.

Protocol Length (PLEN): 8 bits

Length (in octets) of internetwork addresses. The internetwork protocol is specified in PTYPE. In this example: IPv4 address length is 4.

Operation (OPER): 16 bits

Specifies the operation that the sender is performing: 1 for request, 2 for reply.

Sender Hardware Address (SHA): 48 bits

Media address of the sender. In an ARP request this field is used to indicate the address of the host sending the request. In an ARP reply this field is used to indicate the address of the host that the request was looking for.

Sender protocol address (SPA): 32 bits

Internetwork address of the sender.

Target hardware address (THA): 48 bits

Media address of the intended receiver. In an ARP request this field is ignored. In an ARP reply this field is used to indicate the address of the host that originated the ARP request.

Target protocol address (TPA): 32 bits

Internetwork address of the intended receiver.

ARP parameter values have been standardized and are maintained by the Internet Assigned Numbers Authority (IANA).[2]

The EtherType for ARP is `0x0806`. This appears in the Ethernet frame header when the payload is an ARP packet and is not to be confused with PTYPE, which appears within this encapsulated ARP packet.

IPv6 does not use ARP rather a neighbor discovery protocol.