IP Multicast– Quick Review

**IGMP: Internet Group Management Protocol**
- Designed ONLY for the LAN: hosts talking to a directly-connected router
- Enables a host to tell the router that it is interested in receiving a specific multicast stream
- Operations
  - Membership, query
    - Sent by a router to all hosts on an interface to determine the set of all multicast groups that have been joined by the hosts
  - Membership, report ("join group")
    - Host response to a query or an initial join or a group
  - Leave, group
    - Host indicates that it is no longer interested
    - Optional: router infers this if the host does not respond to a query
    - Example of state: information goes away unless it is refreshed

**PIM: Protocol Independent Multicast**
- Most widely used Internet multicast routing protocol
- Used among routers in the Internet – not with hosts
- Two mechanisms are supported

**PIM Dense Mode**
- Uses a source-based tree
  - Multicast datagram is sent from source to all connected routers
  - Each router sends a copy of the datagram to each connected router
  - Use Reverse Path Forwarding (RPF) to avoid loops
  - Routers that don’t need the datagram send prune messages to stop getting traffic
- Define a rendezvous point – some router in the network (administrator does this)
- Edge routers send a join message to the rendezvous point
  - Intermediate routers will forward the join message unless they already joined

**PIM Sparse Mode**
- Uses a group shared tree
  - Goal: build a spanning tree that includes only the hosts that are interested
  - Define a rendezvous point – some router in the network (administrator does this)
  - Edge routers send a join message to the rendezvous point
  - Intermediate routers will forward the join message unless they already joined

---

**Question 1**

What is an advantage of multicast routing using a group-shared tree (this is called PIM Sparse Mode) over multicast routing using a source-based tree (this is also known as PIM Dense Mode)?

First, a review…

**Answer**

Multicast datagrams are sent from source to all connected routers. In PIM Sparse Mode, intermediate routers forward the join message unless they have already joined. In PIM Dense Mode, each router sends a copy of the datagram to each connected router. This can lead to increased traffic. Using the rendezvous point helps to minimize the number of routes and prune unnecessary traffic.
IP Multicast—Quick Review

PIM: Protocol Independent Multicast
- Most widely used Internet multicast routing protocol
- Used among routers in the Internet – not with hosts
- Two mechanisms are supported
  - PIM Dense Mode – uses a source-based tree
    - Multicast datagram is sent from source to all connected routers
    - Each router sends a copy of the datagram to each connected router
    - Use Reverse Path Forwarding (RPF) to avoid loops
    - Routers that don't need the datagram send prune messages to stop getting traffic
  - PIM Sparse Mode – uses a group shared tree
    - Goal: build a spanning tree that includes only the hosts that are interested
    - Define a rendezvous point – some router in the network (administrator does this)
    - Edge routers send a join message to the rendezvous point
      - Intermediate routers will forward the join message unless they already joined

Question 1

What is an advantage of multicast routing using a group-shared tree (this is called PIM Sparse Mode) over multicast routing using a source-based tree (this is also known as PIM Dense Mode)?

Using a group shared tree (PIM Sparse Mode) avoids sending traffic to networks that have no hosts that are interested in the multicast stream.

With a source-based tree (PIM Dense Mode), traffic is replicated to every router, which must then perform a process of pruning to tell its connected router to stop sending the stream.

Question 2

In CSMA/CD, after the fifth collision, what is the probability that a node chooses $K = 4$? The result $K = 4$ corresponds to a delay of how many seconds on a 10 Mbps Ethernet?

First, a review...

CSMA/CD Review

Carrier Sense Multiple Access with Collision Detection
Rules:
- Listen to the medium and wait for quiet (no messages being sent)
- Transmit your frame
  - BUT … listen while transmitting
- If you detect a collision (someone else is transmitting): STOP
- Wait a random interval
- Try again (listen & transmit)

Random interval to wait before retransmitting
- Pick a random value from a time interval $W$
- $W$ gets longer each time a collision is detected
  - 1st time: $\{0, 1\}$
  - 2nd time: $\{0, 3\}$
  - $N$th time: $\{0, 2^{n-1}\}$, where $b$ is the backoff (collision) count
- Values are multiplied by 512 bit-times
  - Bit-time = time to transmit 512 bits

In CSMA/CD, after the fifth collision, what is the probability that a node chooses $K = 4$? The result $K = 4$ corresponds to a delay of how many seconds on a 10 Mbps Ethernet?

After the 5th collision
the adapter chooses from $\{0, 1, 2, \ldots, 31\}$
The probability that it chooses 4 is $1/32$
Bit-time on a 10 Mbps network = 51.2 µs
$K=4 \Rightarrow 4 \cdot 51.2 \mu s$
It waits 204.8 microseconds
Consider the 5-bit generator, \( G = 10011 \), and suppose that \( D \) has the value \( 0101101010 \). What is the value of \( R \)?

If the top bit of the value is 0:
- The quotient digit is 0
- We xor 00000 (do nothing)

If the top bit of the value is 1:
- Xor the generator (10011)

The CRC is the remainder

What is ARP Spoofing?
(You'll have to look on the web to find the answer)

First, a review...

A malicious host will send an ARP reply containing an incorrect association between an IP address and MAC address. Other hosts pick up the reply and place it in their ARP cache, avoiding having to make a future ARP request but not realizing that the binding is incorrect. ARP does not have a mechanism to validate that the response is coming from the legitimate host. Some systems, like Linux, ignore unsolicited replies.
The end