

Internet Technology

12r. Assignment 8 review

Paul Krzyzanowski

Rutgers University

Spring 2016

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...

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 **soft state**: information goes away unless it is refreshed

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

IP Multicast– Quick Review

PIM: Protocol Independent Multicast

- Most widely used Internet multicast routing protocol
- Used among routers in the Internet – not with hosts

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

IP Multicast– Quick Review

PIM: Protocol Independent Multicast

- Most widely used Internet multicast routing protocol
- Used among routers in the Internet – not with hosts

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
- 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

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)

CSMA/CD Review

Carrier Sense Multiple Access with Collision Detection

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: $\{0, 3\}$
 - Nth time: $\{0, 2^b-1\}$, where b is the backoff (collision) count
- Values are multiplied by 512 bit-times
 - **Bit-time** = time to transmit 512 bits

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?

After the 5th collision

the adapter chooses from $\{0, 1, 2, \dots, 31\}$

The probability that it chooses 4 is $1/32$

Bit-time on a 10 Mbps network = $51.2 \mu\text{s}$

$K=4 \Rightarrow 4 \cdot 51.2 \mu\text{s}$

It waits **204.8 microseconds**

Question 3

Consider the 5-bit generator, $G=10011$, and suppose that D has the value 0101101010 . What is the value of R ?

$$\begin{array}{r} 0 \\ 10011 \overline{) 01011010100000} \\ \underline{00000} \\ 1011 \end{array}$$

← shift D by r (4) bits = add 4 zeros

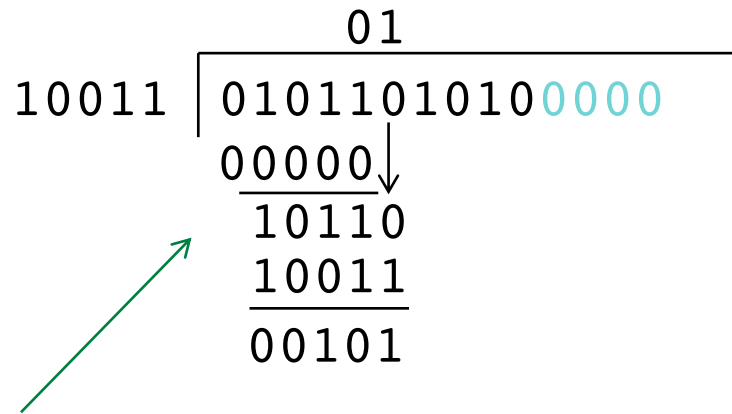
If the top bit of the value is 0:

- The quotient digit is 0
- We xor 00000 (do nothing)

[continued]

Question 3

Consider the 5-bit generator, $G=10011$, and suppose that D has the value 0101101010 . What is the value of R ?

$$\begin{array}{r} 10011 \quad | \quad \begin{array}{r} \\ \\ 01 \\ \hline 01011010100000 \\ \\ 00000 \downarrow \\ \hline 10110 \\ 10011 \\ \hline 00101 \end{array} \end{array}$$


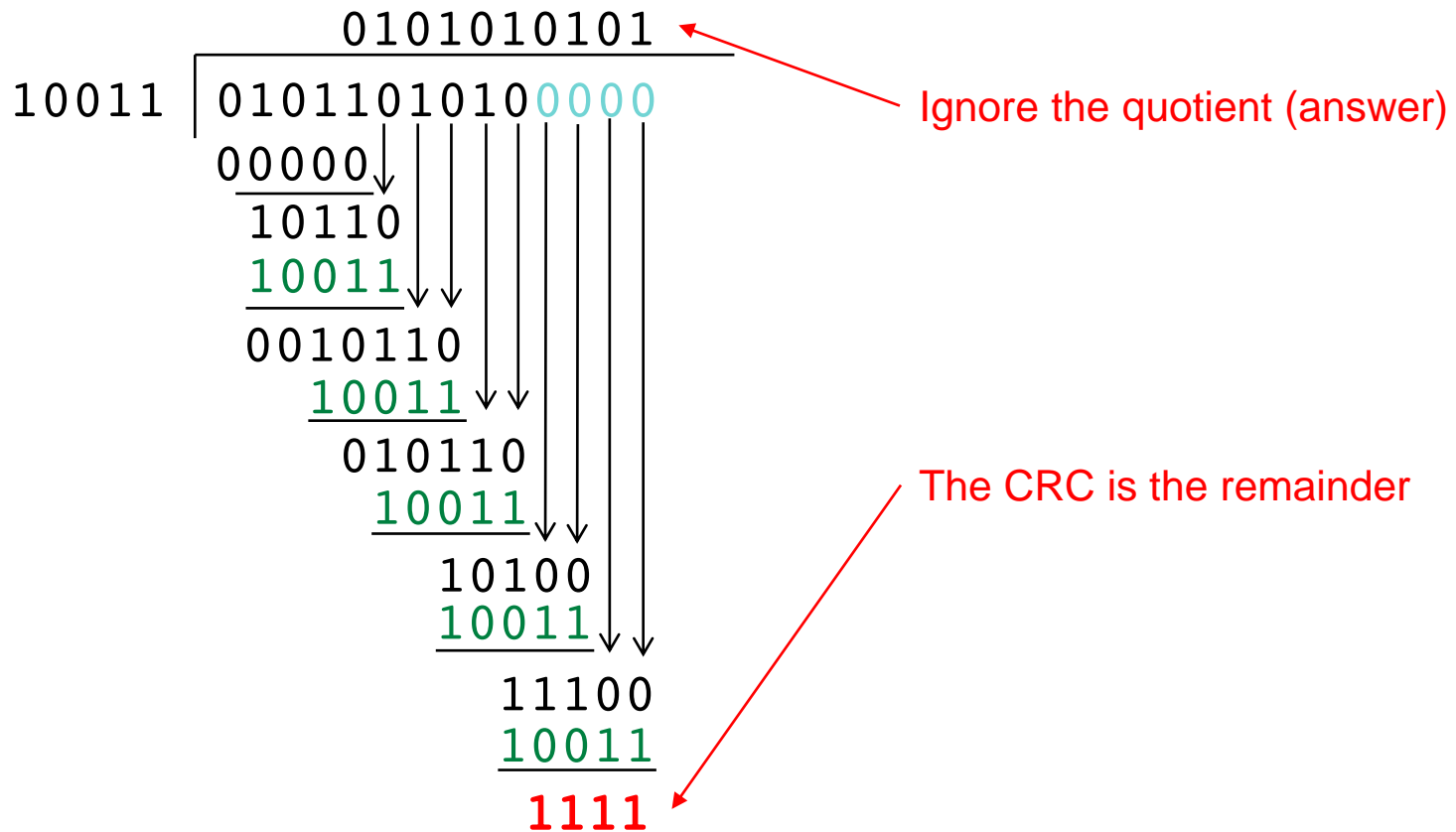
If the top bit of the value is 1:

- Xor the generator (10011)

[continued]

Question 3

Consider the 5-bit generator, $G=10011$, and suppose that D has the value 0101101010 . What is the value of R ?



Question 4

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

First, a review...

ARP – Address Resolution Protocol

- Find the MAC address given an IP address
 - A host needs to know this so it can send the IP datagram to the correct next hop
- Protocol:
 - Create an **ARP query message** containing the IP address we want to look up
 - Send it via an Ethernet broadcast – all hosts on the LAN receive it
 - If a host owns that IP address
 - It sends an **ARP response** containing the IP address and the corresponding MAC address

Question 4

What is ARP Spoofing?

(You'll have to look on the web to find the answer)

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 mechanisms to validate that the response is coming from the legitimate host.

Some systems, like Linux, ignore unsolicited replies.

The end