Internet Technology

14r. 2015 Exam 3 Review

Note: questions that are not in scope for the next exam are not covered – read the exam outline for the list of topics. This also does not cover all topics you need to know for the exam

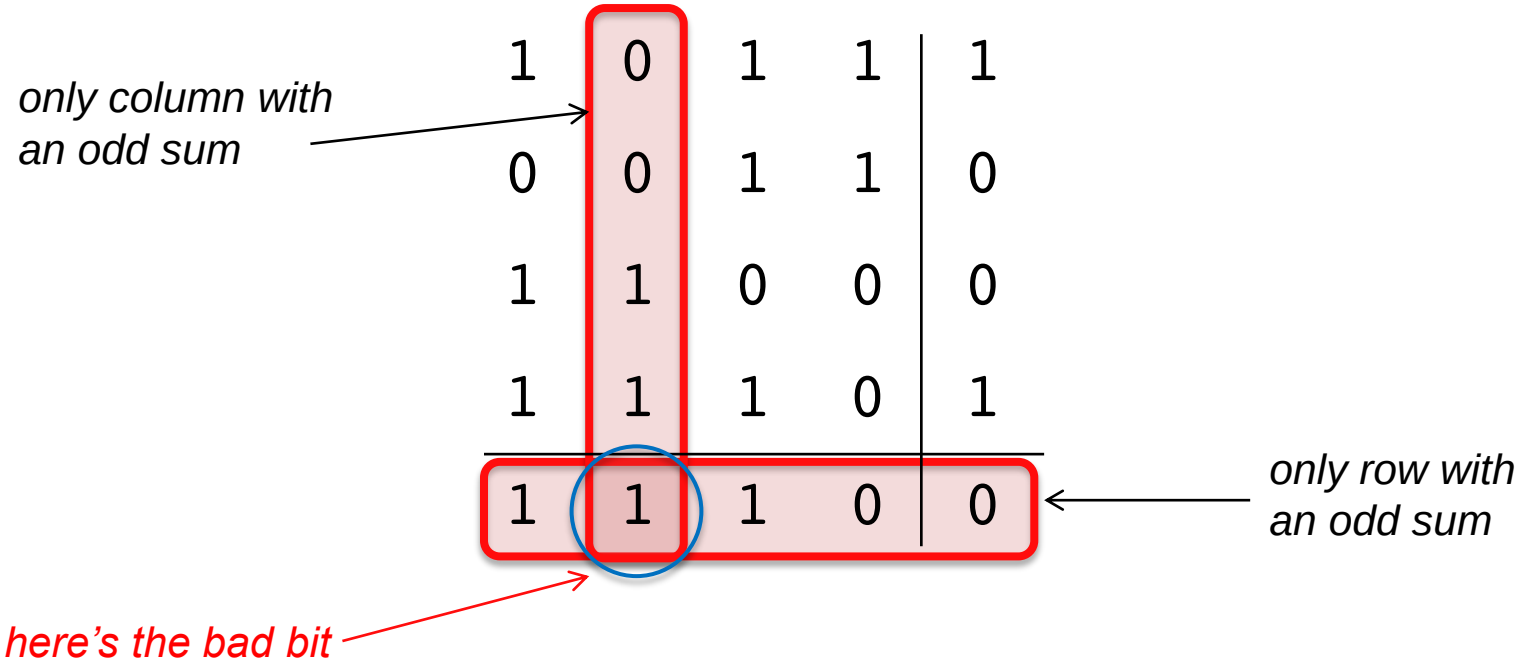
Paul Krzyzanowski

Rutgers University

Spring 2016

Question 3

The data shown uses two-dimensional parity and has a one-bit error. Locate and correct the error.



- The question does not tell you if it's even or odd parity but it does say that only one bit has the error, so there should be only one row & 1 column with a different parity.
- Bad bits can show up inside the EDC/ECC data just as they can in the regular data.

Question 4a

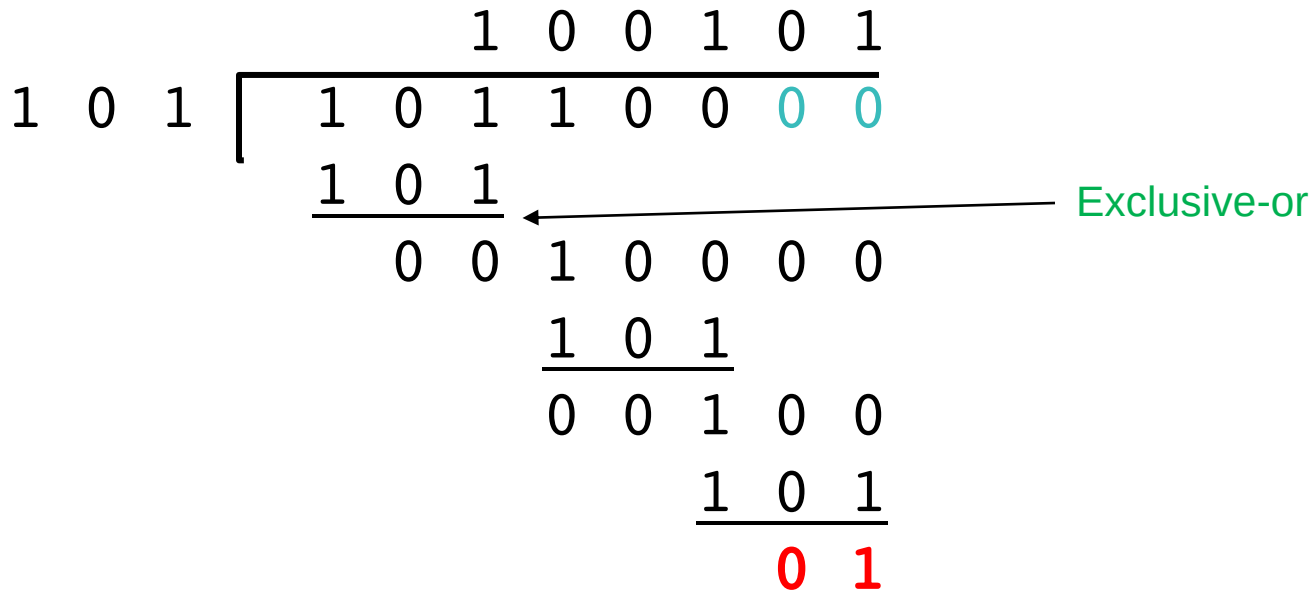
(a) State the number of bits that the CRC code will occupy given a generator of 101.

For a CRC code of *r* bits, the generator will have to be *r + 1* bits long.

CRC code = 2 bits

Question 4b

(b) Compute the CRC code for the bits 101100 with the generator 101.



CRC = remainder = 01

Question 8

Reverse Path Forwarding (RPF) is used to:

a) Route messages from the receiver back to the sender.

b) Build a spanning tree.

c) Duplicate multicast packets and send them to interested destinations.

d) Ensure that forwarding loops do not develop.

Reverse Path Forwarding is designed to avoid routing loops. Each router will:

- Check the route to the source address of an incoming datagram
- If the datagram came over that link (shortest path) then a copy will be sent onto every other link
- Otherwise it will be dropped

(a) No – RPF does not send anything back to the sender

(b) No – RPF does not build a spanning tree. RPF is an example of controlled flooding – a way to broadcast a packet only the router has not broadcast that same packet before

(c) Yes, a router using RPF does that but so does uncontrolled flooding: this isn't the best answer

(d) Yes.

Question 9

The Internet Group Multicast Protocol (IGMP):

a) Allows hosts to inform their connected routers that they are interested in joining a multicast group.

b) Allows a multicast sender to inform its connected router that it is interested in sending to a multicast group.

c) Establishes routes between multicast senders and multicast receivers.

d) All of the above.

- IGMP is used only within a LAN to allow hosts to tell a connected router that they want to receive multicast datagrams that contain a specific multicast address
- Senders don't have to do anything
- IGMP does not establish routes

Question 10

Channel partitioning protocols such as TDM or FDM:

a) Have a high probability of collisions.

b) May fail if any node in the network goes down.

c) Pass a token to nodes to give them permission to access the network.

d) Will never allow a node to use the full channel capacity.

- TDM = time division multiplexing
- FDM = frequency division multiplexing
- They give each node a fixed % of time slots (TDM) or a frequency range (FDM) even if no other node is using the network

Question 11

Collisions can occur in this form of MAC protocol:

a) Frequency division multiplexing.

b) Random access.

c) Token passing.

d) Polling.

- (a) FDM – gives each node a specific frequency range
- (c) Token passing – a node cannot transmit until it gets a token
- (d) Polling – a coordinator checks with each node to see if it has something to send
- (b) Random access – all nodes compete for access to the network

Question 12

In CSMA/CD, binary exponential backoff is used to:

a) Make an adapter wait exactly double the previous interval whenever a frame experiences a collision.

b) Increase the chance that an Ethernet adapter will wait longer times as a frame experiences more collisions.

c) Require that an adapter first listen to the channel to sense that it is clear before transmitting.

d) Ensure that collisions cannot occur because two adapters will never transmit during the same time slot.

(a) No. Each host picks a random time to wait. This makes it unlikely that hosts that experienced a collision will wait the same amount of time and have another collision

(b) Yes. Each time there's a collision, the interval from which a host picks a random time doubles

(c) A transceiver will listen first to see that the channel is clear but that is not binary exponential backoff

(d) There's no promise that collisions will not occur

Question 13

IPv6's Neighbor Discovery protocol differs from ARP (Address Resolution Protocol) because:

a) It uses TCP instead of UDP for greater reliability.

b) A query is not sent to every host on the LAN.

c) Hosts never have to send queries because every host periodically sends announcements.

d) It uses a three-way handshake instead of a query-response.

- ARP – sends a broadcast to all hosts on the LAN, asking "*do you have this IP address?*"
- With IPv6, each host listens on a multicast address that is derived from its IP address (a 104-bit prefix appended with the last 24 bits of the host's IP address)
- If a node needs to find a MAC address for an ethernet address, it will send a multicast message using that address
- Most (usually all) hosts on the LAN will listen on other addresses and not get the query

Question 14

An Ethernet switch knows which interface to use to forward an incoming frame based on:

a) Having seen a source address in an earlier frame that arrived from that destination interface.

b) The administrator having configured a switch table to identify which addresses are at which interfaces.

c) The use of ARP to find the corresponding MAC address for an IP address.

d) Each interface on a switch having a distinct MAC address and the sender using it as a destination address.

- A switch is self-learning: by looking at interface *& source address* of incoming frames, it builds a switch table
- The switch table enables the switch to look up the destination address and find the interface
- If a destination MAC address is not in the table, the switch forwards the frame to all interfaces

Question 15

CSMA/CA:

a) Waits a random time interval before transmitting after a channel is sensed to be busy.

b) Is a taking-turns protocol; a device cannot transmit until it gets a token from the access point.

c) Waits a random time interval if a transmitted frame resulted in a collision.

d) Allocates time slots for each wireless station, which has to wait for its time slot before transmitting.

It picks a random time from a time interval. The time interval is doubled each time there is a collision (binary exponential backoff)

Question 16

Unlike Ethernet, 802.11 uses sequence numbers in its frame to allow the receiver to:

a) Detect and discard duplicate frames.

b) Ensure that all frames are delivered to upper protocol layers in the proper order.

c) Request retransmission of missing frames.

d) All of the above.

802.11 adds acknowledgements & retransmissions:

- Since the sender cannot listen while sending and detect collisions
- Data loss is much more likely in a wireless network

(b) Frames are delivered in the order they were successfully received. Sequence numbers are not used to enforce delivery order. Certain frames may be dropped if the sender gave up on retransmitting.

(c) The receiver does NOT request retransmission of frames. It is up to the sender to detect missing acknowledgements and retransmit.

Question 17

Request to Send / Clear to Send (RTS/CTS) is a feature of the 802.11 MAC to:

a) Provide acknowledgements from the access point to indicate that a frame has been received successfully.

b) Enable power management by telling the access point that a station will or will not be transmitting anymore.

c) Allow all stations to know that one station will be transmitting even if they are out of range of that station.

d) Allow one station to negotiate to receive a frame from another station, bypassing the access point.

- Hidden node problem: A transmitter may be out of range from another transmitter and cannot detect that the channel is busy
- RTS/CTS: send a small message asking the access point to inform everyone that you want to transmit and they should be silent for a while
- Used for larger frames to avoid wasting time transmitting a large frame that would get mangled due to a collison

Question 18

Differentiated Services (DiffServ) is a technique for:

a) Providing quality of service on a network by reserving router resources ahead of time.

b) Grouping datagram streams from different servers together if they are routed to the same client.

c) Identifying and prioritizing classes of network traffic by tagging IP datagrams.

d) Transforming an IP network into one with the properties of a circuit switched network.

- Use a field in the IP header to define a class of traffic
- Routers may be programmed to prioritize one flow vs. another
- There is no *a priori* reservation with differentiated services

Question 19

A weighted fair queuing link scheduling discipline:

a) Services output queues in strict priority order to ensure that their quality of service needs are met.

b) Uses multiple output queues and gives each of them an equal percentage of link bandwidth.

c) Prioritizes output queues but ensures that each gets a defined minimum percentage of link bandwidth.

d) Uses a single output queue per link and transmits packets in the order that they arrive.

- **Fair queueing (round robin)** – divides a link capacity into equal parts – every queue (holding traffic that has been grouped into a flow) gets equal priority
- **Priority queueing** – reads from a high priority queue until there are no packets to transmit
- **Weighted fair queueing** – Like round robin but allows a weight to be assigned to each queue so some queues can get preferential treatment

Question 20

A leaky bucket algorithm primarily addresses which quality of service (QoS) problem?

a) Bandwidth

b) Delay

c) Jitter

d) Packet loss.

- The leaky bucket algorithm converts a bursty flow of packets into a smooth flow.

(a) It converts variable bandwidth to constant bandwidth – but average bandwidth remains the same

(b) Average end-to-end latency does not change

(c) Jitter = variation in latency – the leaky bucket was designed to reduce this

Question 21

The Reservation Protocol (RSVP) is used to:

a) Schedule packets in a router's output queue.

b) Reserve socket resources on both the client and server.

c) Specify the quality of service needs for a stream of datagrams.

d) Police traffic to drop any datagrams that exceed a bandwidth threshold..

- RSVP is used to have routers along a path to commit to providing a requested quality of service for a specific stream of datagrams

Question 22

The RTP Control Protocol, RTCP:

a) Is a version of the RTP (Real-Time Protocol) that uses reliable datagram delivery.

b) Dynamically modifies an RTP datagram stream to enforce quality of service guarantees.

c) Provides a sender with feedback on the quality of service that a receiver is getting.

d) Allows an administrator to configure quality of service parameters on an RTP datagram stream.

- RTP (real-time protocol) basically adds a timestamp to a datagram
- This allows a receiver to deliver packets to an application at the same intervals as they were transmitted (e.g., for voice or video)
- RTCP allows the receiver to send feedback on packet count, packet loss, delay, and jitter

Some Key Concepts in Firewalls

- Packet filter
  - Pass or block datagrams based on IP/TCP/UDP headers (source address, destination address, protocol, source port, destination port) and interfaces (incoming interface and outgoing)
- Filter chain
  - Set of rules that define the filters
- DMZ
  - Protected subnet that hosts Internet-facing services
  - It is separate from the internal network
  - Traffic between the Internet and DMZ must pass through a firewall
  - Traffic between the DMZ and internal net must also pass through a firewall

Some Key Concepts in Cryptography

- Symmetric cryptography
  - Use one shared key to encrypt & decrypt messages
- Public key cryptography
  - Use two related keys
    - K1 = private key, which you do not share with anyone
    - K2 = public key, which you can share with everyone
  - If you encrypt with K1, you can only decrypt with K2
    - Encrypt with private key – something only you can do – this is used to prove your identity
    - Encrypt with public key – something anyone can do but only the user with the matching private key can decrypt – this is used to keep messages secret
- Diffie Hellman key exchange
  - Not encryption but a way to use public and private "keys" to create a common key that can be used to encrypt a random session key

Some Key Concepts in Cryptography

- Hybrid cryptosystem
  - Use public key cryptography to transmit a random session key
    - Encrypt session key with the remote side's public key
  - Use the session key to encrypt the communication session
- Session key
  - Throw-away key that is used for one communication session
- Message authentication
  - Message Authentication Code
    - Hash(message) encrypted with a shared symmetric key
  - Digital signature
    - Hash(message) encrypted with the owner's private key

The end