Internet Technology

15r. Spring 2016 Exam 3 Review

Paul Krzyzanowski

Rutgers University

Spring 2016

Question 1

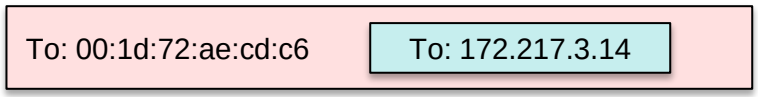
Suppose a computer needs to send a datagram outside its local area network. We studied how this works: the destination address is looked up in a routing table using a longest-prefix match. This lookup gives us the IP address of the next-hop router. Suppose we have a datagram with a destination address of 172.217.3.14 and the address of the next hop router is 128.6.4.1. How does the datagram get to the router when the router's IP address (128.6.4.1) is not in the original datagram?

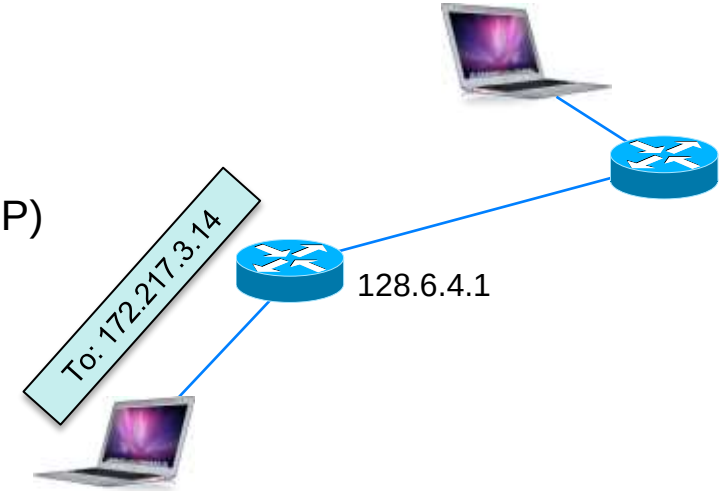
How does a datagram get to the next hop when the next hop has an IP address different than the destination?

This is key to getting routing to work!

The Data Link Layer is responsible for this.

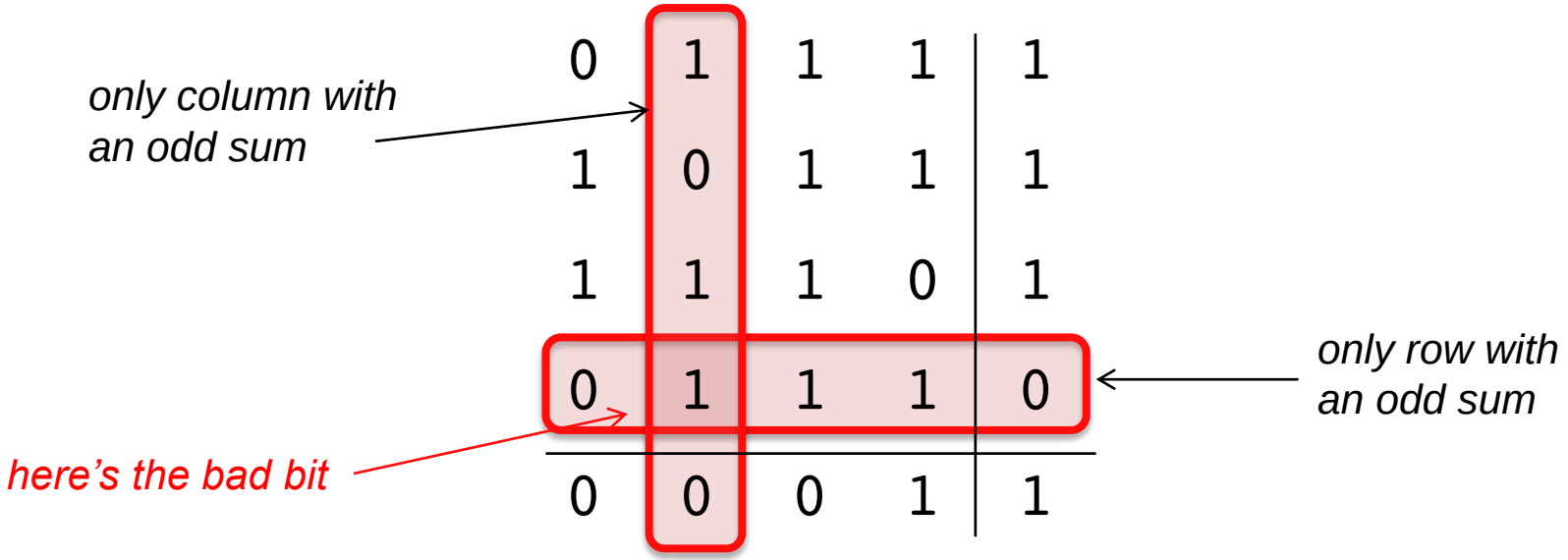
Look up the MAC address of the next hop (use ARP)
Encapsulate the datagram in a link layer frame
Link layer MAC address = address of next hop





Question 2

Here's some data with a two-dimensional parity error detecting code expanded into a grid. Circle the one bad bit.



Question 3

Ethernet switches are said to be self-learning. How does the switch learn the output port to use for a given frame?

The switch looks at each incoming frame and adds

(source_MAC_address, source_interface)

to its forwarding table (or resets the timeout if the entry is already there

Destination	Port	Timeout
74:c2:46:3e:1a:76	2	300
58:94:6b:22:27:d4	2	21
a8:8e:24:6c:ed:e4	8	300
58:55:ca:27:d7:a6	5	291

Page 3

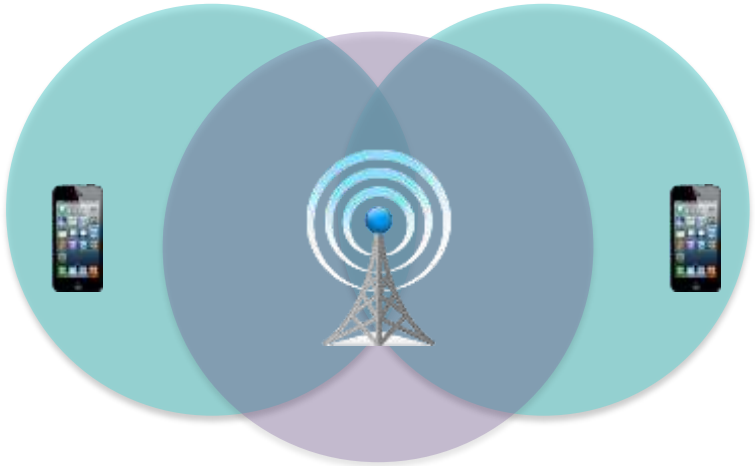
Question 4

Even if a wireless radio could listen while transmitting, why would CSMA/CD still not be viable on a wireless network?

Why do we use CA instead of CD? Because we cannot listen.

Unlike CSMA/CA, CD has the advantage of shutting off transmission once a collision is detected – leads to more efficient use of the network

Problem with wireless networks: you might not be in range of the other transmitter – hidden node problem



Question 5

With *Reverse Path Forwarding* (RPF), a router will:

(a) Forward a datagram to at most one link, which is the shortest path to the destination.

(b) Never receive duplicate datagrams.

(c) Forward a multicast datagram from the receiver to the sender to enable the receiver to join the multicast group.

(d) Forward a datagram only if it arrived via the shortest path link.

RPF: a router will discard any datagram that came in on an interface that is NOT the route back to the source (i.e., shortest path)

(a) No. It will forward a datagram to every other interface
(b) No. A router may receive duplicate datagrams. It will reject those that came in on the wrong interfaces.
(c) No. RPF has nothing to do with sending *join* messages.
(d) Yes.

Question 6

How can an IP multicast sender discover all the nodes that joined its host group?

(a) It can request a list from the rendezvous point.

(b) It can use IGMP to query the router for all group members.

(c) It receives *join* messages from each node that wants to receive messages for that group.

(d) It can't.

IP multicast does not provide any mechanisms for discovering group members (host group)

(a) No. The rendezvous point only stores addresses of next-hop routers for each group.
(b) No. You can't query a router for group members and IGMP is only used for the router on your LAN – you cannot find all other edge routers for a host group.
(c) No. A sender never receives *join* messages from receivers.
(d) Yes.

Question 7

Because it is a *soft state* protocol, IGMP (Internet Group Management Protocol) does not require:

(a) A host to send a *leave_group* command to leave a multicast group.

(b) A router to send periodic *membership_query* commands.

(c) A host to send a *membership_report* command to join a multicast group.

(d) A router to keep track of which of its connected networks need to receive traffic for a multicast group.

Soft state = state that gets refreshed periodically.

(a) Yes. If you don't send a *leave_group* message, eventually your membership will expire.
(b) No. This is crucial for soft state: the router periodically refreshes its membership list.
(c) No. This is crucial for any state: a host needs to tell a router it is interested in a group.
(d) No. A router keeps information from which links (connected subnets) it received *join* messages.

Question 8

To deliver a datagram with an IP multicast destination address on an Ethernet LAN:

(a) The MAC address is derived from selected bits of the IP multicast address.

(b) The sender does an IGMP query to find group members and delivers a copy of the datagram to each member.

(c) The sender uses an Ethernet broadcast and relies on the network layer in receiving hosts to filter unwanted datagrams.

(d) The sender builds a spanning tree and relays the datagram to its nearest neighbor.

The question only asks about LAN delivery.

(a) Yes. The MAC multicast address is derived from the IP multicast address.
(b) No. There is no IGMP query to find group members & hosts do not do N unicasts.
(c) No. A host sends multicast addresses. A receiver may choose to use promiscuous mode if it cannot filter the required frames.
(d) This makes no sense on a LAN.

Question 9

To find the MAC address for an IP address, ARP (Address Resolution Protocol):

(a) Derives the MAC address from selected bits of the IP address.

(b) Broadcasts a query to all hosts on the local area network.

(c) Sends a query to the host's DNS server.

(d) Sends a query to the gateway router.

(a) No. There is no relation between an admin-assigned IP address and the manufacturer-assigned MAC address.

(b) Yes. ARP broadcasts a query and the host that owns the IP address responds, providing its MAC address.

(c) No. DNS does not keep track of MAC addresses.

(d) Routers do not keep track of hosts on the LAN … or their MAC addresses.

Page 4

Question 10

IPv6's *Neighbor Discovery Protocol* is an improvement over ARP because:

(a) Its multicast query does not have be to processed by most hosts on the local area network.

(b) It sends the query to its nearest neighbor, which may forward it if necessary.

(c) It contacts the gateway router over an encrypted connection.

(d) Every host caches previous responses to queries to avoid making repeated requests.

(a) Yes. Every host must listen on a multicast address that is derived from its IP address. A query for an IP address is directed only to that multicast MAC address – usually there will only be one host on the LAN with that address.

(b) No – there is no concept of "nearest neighbor" on a LAN.

(c) No – The gateway plays no part in this.

(d) No – ARP does this too.

Question 11

Unlike older Ethernet hubs, an Ethernet *switch* has the advantage of:

(a) Allowing multiple switches to be cascaded together to connect more devices.

(b) Supporting multicasting and broadcasting.

(c) Integrating IP routing functions into the switch to support multiple subnets.

(d) Ensuring that collisions cannot occur.

Hub: Shared access – Takes any incoming data and sends it onto all its interfaces

(a) No – You can cascade hubs.

(b) No – That works just fine with a hub.

(c) No – Neither switches nor hubs care about IP routing.

(d) Yes – Collisions cannot take place with switches

- Frames are queued & forwarded to outbound links and communication is full-duplex
- Separate channels for inbound and outbound traffic on each link

Question 12

A virtual local area network (VLAN) allows:

(a) A collection of systems on the Internet to appear as if they are on one local area network.

(b) A local area network to be set up without using a switch or hub.

(c) One switch to define multiple distinct local area networks.

(d) Multiple switches to be connected together to create a single larger local area network.

Hub: Shared access – Takes any incoming data and sends it onto all its interfaces

(a) No – VLANs do not span subnets.

(b) No – You need a VLAN switch.

(c) Yes – The purpose of a VLAN is to partition a network into multiple LANs.

(d) No – You can cascade regular switches to do that and still have one LAN.

Question 13

Passive scanning in 802.11 wireless networks refers to:

(a) A station listening for beacon frames from base stations.

(b) A station broadcasting probe request frames and waiting for responses from base stations.

(c) A station listening for traffic from other stations to deduce what devices are active on the network.

(d) Scanning for traffic on various frequencies to find the cleanest frequency for transmission.

(a) Yes – Passive scanning = listen for a beacon - an advertisment of a base station.

(b) No – That's active scanning.

(c) No – Stations don't do that (and with encrypted traffic, cannot do that).

(d) No – Scanning has nothing to do with finding the cleanest frequency.

Question 14

The Media Access Control (MAC) protocol for 802.11 shares this in common with Ethernet:

(a) Acknowledgements and retransmissions.

(b) Collision detection.

(c) Binary exponential backoff.

(d) Error correcting code.

(a) No – 802.11 uses an ARQ protocol – Ethernet never acknowledges frames.

(b) No – 802.11 cannot listen while transmitting and hence cannot detect collisions.

(c) Yes – Both CSMA/CA and CSMA/CD perform binary exponential backoff:

- CSMA/CA: Pick random backoff value in a time interval – count down while channel is idle – transmit. If no ACK received, assume collision, double interval & try again.
- CSMA/CD: Pick a random backoff value in a time interval – wait that interval – wait for channel to be idle – transmit. If collision detected, double interval & try agein.

(d) No – Ethernet only uses CRC – an error detecting code. Some versions of 802.11 (802.11ac and 802.11n) support the optional use of ECC.

Question 15

RTS/CTS (request-to-send/clear-to-send) in 802.11 is used by the:

(a) Access point to poll for messages from sending devices.

(b) Access point to make sure that the wireless device is awake to receive a message.

(c) Sending device to make sure that the receiving device is awake.

(d) Sending device to reserve a communication channel with the access point.

RTS/CTS is used by a station to request a time interval for transmission. The base station will tell other stations to keep quiet – solves hidden node problem (at the cost of extra messages)

(a) No – the AP never polls for messages from senders.

(b) No – RTS/CTS has nothing to do with sleep/wake power management.

(c) No – RTS/CTS has nothing to do with sleep/wake power management.

(d) Yes.

Question 16

Why does an 802.11 frame contain more than two addresses in infrastructure mode?

(a) To identify the access point as well as the sending and receiving nodes.

(b) To specify both the Ethernet and 802.11 addresses of the access point.

(c) To identify the addresses of the access point and Ethernet switch as well as the source and destination nodes.

(d) To define a route through other wireless nodes if the sender is out of range of the access point.

In 802.11, the base station is not invisible to like a switch. It has MAC addresses and traffic is explicitly directed to it from wireless stations.

(a) Yes

(b) No – A frame will never contain both the Ethernet and 802.11 MAC addresses – makes no sense.

(c) No – An Ethernet switch is not addressable.

(d) No – 802.11 does not have these routing capabilities.

Question 17

In CSMA/CA, collision avoidance is accomplished by:

(a) Having each transmitting node wait a random time after sensing a channel is clear.

(b) Receiving a token from the access point that grants the node permission to transmit.

(c) Having each node transmit on a different frequency.

(d) Assigning distinct time slots to each node when it associates with an access point.

CSMA/CA: Pick random backoff value in a time interval – count down while channel is idle – transmit. If no ACK received, assume collision, double interval & try again.

(a) Yes

(b) No – There is no token granting mechanism. You can use RTS/CTS in 802.11 but that is not part of CSMA/CA.

(c) No – They might use frequency hopping or spread spectrum. Frequency is still a shared resource and there is always a chance of collision

(d) No – That would be TDMA.

Question 18

Jitter is:

(a) The variation in bandwidth over time.

(b) The variation in delay among packets.

(c) The percentage of packets received with errors.

(d) The percentage of lost packets.

.

Page 5

Question 19

Hard QoS (Quality of Service) differs from soft QoS because *hard QoS*:

(a) Is responsible for the quality of service on a single system while Soft QoS manages it end-to-end.

(b) Manages routing while Soft QoS is responsible for queue management.

(c) Is implemented in hardware for efficiency while Soft QoS is a software solution.

(d) Provides bandwidth reservations through the entire path while Soft QoS does not.

Hard QoS provides end-to-end reservation for - and commitment to – a service level.

Question 20

The key difference between a *leaky bucket* and a *token bucket* is that a token bucket:

(a) May create high-bandwidth bursts of traffic.

(b) Converts an irregular flow of data into a constant bandwidth flow.

(c) Prioritizes traffic based on its associated token.

(d) Supports bidirectional data flows.

Token bucket: accumulate "tokens" at a constant rate. Need a token to transmit data.

Leaky bucket: transmit data at a constant rate – queue if it comes in too fast.

(a) Yes – if there's an accumulation of tokens, a burst of data can be sent out immediately

(b) No – a leaky bucket does that.

(c) No – There's no association of tokens to types of traffic in the algorithm.

(d) No – The algorithm only handles traffic in one direction – use another instance if needed.

Question 21

The *Differentiated Services Codepoint* (DSCP) field in an IP header:

(a) States that the datagram contains quality of service configuration data instead of application data.

(b) Is a pointer to a set of rules in the IP options field that define quality of service criteria.

(c) Identifies a grade of service and priority for the datagram.

(d) Contains a token count representing the cost of the datagram.

DSCP: 6-bit field in the IP header to classify a level of service for the datagram (QoS profile)
Support for this & interpretation/implementation of traffic management is dependent on individual routers and endpoints

(a) No – the datagram contains application data

(b) No – there is no additional data in the options field of the datagram.

(c) Yes

(d) No

Question 22

RTP, the Real-time Transport Protocol:

(a) Provides applications with time and sequence number information for each received message.

(b) Allows two endpoints to negotiate on a desired quality of service across the network.

(c) Is used to reserve routing capacity at each router between two endpoints.

(d) Is a version of TCP with latency guarantees.

RTP – application-layer header on top of UDP that identifies:
payload type, sequence number, timestamp, source ID

(a) Yes

(b) No – RTP does not support that – the apps have to figure out how to do this

(c) No – RTP does not control or indicate the quality of service

(d) No – RTP expects UDP as the underlying transport-layer protocol

Question 23

A DMZ (demilitarized zone) is a subnet:

(a) With no machines in it that serves as a barrier between the LAN and Internet.

(b) That is outside of the company's firewall and hosts Internet-facing services.

(c) That contains internal machines that cannot be accessed from the Internet.

(d) Protected by a firewall that contains machines that provide Internet-facing services.

DMZ: perimeter network that hosts systems with externally-facing services

(a) No – what's the point of a subnet with no systems in it?

(b) No – the systems in the DMZ are protected with a firewall

(c) No – they contain systems that offer Internet-facing services

(d) Yes

Question 24

A packet filter (screening router) most likely cannot do this:

(a) Block all access to your email server from machines in the 128.6.0.0/16 network.

(b) Drop all incoming packets that are forged to look like they originated from the internal network.

(c) Reject all incoming packets to the web server that contain URLs that have a .php suffix.

(d) Allow internal systems to access only web sites (TCP ports 80 and 443) on the Internet and nothing else.

Packet filter: filters based on interface, network (IP), and transport (TCP/UDP) layers

(a) No – Block traffic from src_addr = 128.6.0.0/16 to the address of your mail server

(b) No – Block traffic where src_addr = your network & incoming interface = external

(c) Yes – This information is in the application-specific data – need deep packet inspection

(d) No – Block src_addr = your network & (protocol != TCP || dest_port != {80,443})

Question 25

Unlike a packet filter, an application proxy may:

(a) Block packets from known malicious IP addresses.

(b) Log attempts to connect to a service.

(c) Guard against the exploitation of bugs in the server.

(d) Detect port scanning attacks.

Application proxy – inspect incoming protocol & access internal service

(a) No – A packet filter can do that

(b) No – A packet filter can do that

(c) Yes. The goal of a proxy is to avoid protocol attacks (bad commands, ordering, buffer overflow, etc.)

(d) No – An application proxy cannot do that; it listens on the port(s) for the service

Question 26

For Alice to send a message that only Bob can read, she will encrypt it with:

(a) Alice's private key.

(b) Alice's public key.

(c) Bob's private key.

(d) Bob's public key.

Alice has to encrypt the message so that only Bob can decrypt it.

Only Bob has Bob's private key so she needs to encrypt it with Bob's public key.

Question 27

Alice can create a digital signature for a message to Bob by taking a hash of a message and encrypting it with:

(a) Alice's private key.

(b) Alice's public key.

(c) Bob's private key.

(d) Bob's public key.

Alice has to encrypt the message so that only Bob will know that ONLY she could could have created her.

Only Alice has access to her private key.

If she encrypts the message with her private key, Bob can decrypt it with Alice's public key

Page 6

Question 28

10% got this wrong – read the instructions!

Cipher Block Chaining (CBC):

(a) Allows the use of the same key for decryption as for encryption.

(b) Applies multiple levels of encryption to each block of data for added security.

(c) Uses a different encryption key for each block of data.

(d) Ensures that the receiver can detect if a block of data in a stream has been deleted, added, or replaced.

Each data block is exlusive-ored with the ciphertext of the previous block before it is encrypted. This makes the next block dependent on the previous one.

(a) Usually, but that's not the point of CBC – that's up to the encryption algorithm used

(b) No – each block of data is encrypted just once

(c) No – the same key is used for each block of data

(d) Yes – CBC was created to ensure that an attacker cannot replace, add, or delete bytes in the data stream without invalidating the rest of the encryption

Question 29

A hybrid cryptosystem uses:

(a) Two levels of encryption on each block of data for added security.

(b) A different encryption algorithm in each direction of data movement.

(c) Symmetric cryptography to send a session key and public key cryptography to encrypt blocks of data.

(d) Public key cryptography to send a session key and symmetric cryptography to encrypt blocks of data.

Question 30

A digital certificate is:

(a) Is a block of data containing a user's public and private keys, both encrypted by a certification authority.

(b) An encrypted hash of a message.

(c) Any message that is encrypted with a public key encryption algorithm.

(d) A secure way to associate a user's identity with their public key.

X.509 digital certificate:

{ your identitiy information and your public key } signed by a Certification Authority (CA)

Signature = hash of data encrypted with the CA's private key

(a) No – the certificate does not contain a private key and the data is not encryoted

(b) No – that's just the definition of a MAC or digital signature

(c) No

(d) Yes – anyone can validate that the data in the certificate has not been modified

Question 31

An IP tunnel:

(a) Is a network path between two endpoints where all traffic is encrypted.

(b) Is a network path between two networks that bypasses the public Internet.

(c) Encapsulates one IP datagram inside another IP datagram.

(d) Combines multiple distinct datagrams into a single datagram over the Internet.

Z

(a) No – A tunnel does not mean that the data is encrypted or signed

(b) No – A tunnel will often use the public Internet

(c) Yes

(d) No – This makes no sense

The end