# CS 655: Introduction to Computer Networks
# Fall 2022
# Professor Matta

***Additional Final Review Questions***

1. Consider a transport protocol over a wide-area network. The protocol uses an error control scheme where every ACK (acknowledgment) carries the sequence number of the last in-sequence packet seen by the receiver (also called the *cumulative acknowledgment*).

(a) How can a sender use repeated (duplicate) ACKs to improve its detection of packet loss? Would you use a different number of repeated ACKs depending on whether the network is connectionless or connection-oriented? Explain.

(b) An extension to the basic scheme in part (a) is for each ACK from a receiver to carry, in addition to the cumulative acknowledgment, the sequence number of the packet that caused the ACK to be sent. Under this scheme, what do ACKs contain when a receiver receives packets with sequence numbers 5, 7, 8, 10? What should the sender do upon the receipt of each ACK? Does the additional information carried in each ACK help improve performance? If so, explain why.

*Answer:* (a) When sender receives a duplicate ACK instead of incremented (or next) sequence number as ACK, we know packet has been lost. Of course, between connectionless and connection-oriented, there would be difference in the number of repeated ACKs because for connectionless the number would be higher, we would have to be parsimonious with assumption of packet loss.

(b) If the sender has information about which packet caused the ack, they can then use this information to figure out where packet loss happened and resend only lost packets.

2. A group of $N$ users located in the same building are all using the same remote computer via a connection-oriented network. On the average, a user generates $L$ data packets per hour of $P$ bytes each. The packet carrier charges $C$ cents per byte of user data transported, plus $X$ cents per hour for each virtual circuit open. Under what conditions is it cost effective to multiplex all $N$ transport connections onto the same virtual circuit, if such multiplexing adds 2 bytes of data to each packet? Assume that even one virtual circuit has enough capacity for all users. Comment on when it becomes more likely that such multiplexing is beneficial. [*Hint:* compute cost expressions for the case when one virtual circuit is used and the case when $N$ virtual circuits are used.]

For 1 virtual connection: $\text{cost}(1\ VC) = 2(N)+N*L*P*C + X$
For N virtual connections: $\text{cost}(N\ VC) = 0(N)+N*L*P*C+N*X$
Find when $\text{cost}(1\ VC)<\text{cost}(N\ VC) \Rightarrow 2(N)+N*L*P*C+X<0(N)+N*L*P*C+N*X$
Thus, this condition is met when $\mathbf{(2N/N-1)<X}$

3. Describe the *Split-Horison* and *Split-Horison with Poison Reverse* heuristics used by RIP. Explain how they address the problem of routing loops.

   *Answer*: "Split Horizon" is a strategy where nodes will never advertise a path to the next hop along said path. Split horizon solves some (but not all) persistent counting loops (the "counting to infinity" problem), such as the following:

   A ← B ← C ← D

   The link between A and B fails. Node C advertises to B its path to A before B can deliver the "bad news" that the link has failed. B and C are now pointing to each other as next hops and will continue to send each other updated distances that increase by 1 each time. This problem would *not* have occurred if C hadn't advertised to its next hop (B) in the first place.

   "Split Horizon with Poison Reverse" is an amended version of Split Horizon where nodes advertise an infinite distance from the path's destination to their next hop (indicating that the destination is unreachable). This fixes the following scenario:

   ```
      A
    /   \
   B —  C
   ```

   Both links to A fail at the same time, but B and C have just sent out new distance vectors moments beforehand. B and C each receive the new path from the other (neither of the two are using the other as their next hop *yet*) and both will **start** using each other as the next hop to reach A. They will continue to send each other updated distances (counting to infinity).

   This problem can be avoided if B advertises a distance of infinity to C (its new next hop) after they first attempt to use each other as next hops: this will inform C that C is also B's next hop, allowing the "bad news" of the link failure to propagate correctly.

   Neither strategy is sufficient to avoid all routing loops — there are many possible scenarios that involve cycles of more than two nodes (where "next hop" information alone is not enough to detect a cycle). One solution is to advertise the complete path along with the distance.

4. Consider an arbitrary network topology that contains cycles/loops. If a message is flooded over such network, the message can loop. Briefly describe two techniques to avoid this message-looping problem completely.

   A: Either set max num of hops or TTL, or use reverse path forwarding

5. In IP, why is it necessary to have one address per interface, rather than just one address per host?

Answer: It is necessary to have one address per interface because it allows for communication between different hosts on different networks. Each interface needs to have its own unique address in order for it to send and receive data on its own network. It also allows for communication between two different networks, as each interface will have its own address and can forward packets to the other network. Without multiple addresses per interface, there would be no way to differentiate between different networks and therefore the hosts on those networks would not be able to communicate

6. In IP, the checksum covers only the header and not the data. Why do you suppose this design was chosen?

Answer: This design was chosen because the header is typically much smaller than the data portion of a packet. Since the checksum is used to ensure that the data is not corrupt, it is more efficient to only check the header, which is much smaller than the data. This design also allows for the data portion of a packet to be larger than the header, which is important for applications such as streaming media.

7. In a global internet, for two machines on the same subnet to communicate, they need to know each other's physical address. So, the source machine has to map the internet address of the destination into a physical address. (a) Why is this address mapping important? Couldn't the two machines just communicate using their internet addresses? (b) Describe at least two solutions to address mapping. Describe the conditions under which each solution is appropriate. State any advantages or disadvantages each solution might have.

8. (a) In a global internet, different subnets may have different Maximum Transfer Unit (MTU). Why is there a different MTU for different subnets? (b) An intermediate router must fragment the internet packet if its size is larger than the MTU of the subnet over which the packet will be routed. Two approaches can be used to reassemble a fragmented packet. The *first* approach is to reassemble it immediately after the subnet with smaller MTU. A *second* approach is to reassemble the fragmented packet at the destination host. What are the advantages and disadvantages of each approach to reassembly? (c) A TCP segment of 1500 bytes is to be transmitted over a network with MTU of 252 bytes. Assuming the header in each IP datagram requires 20 bytes, would fragmentation take place? Explain why or why not? If fragmentation takes place, derive the number of datagrams (fragments) required. Also, show how many bytes are in each fragment, and how many of those bytes correspond to headers and data (payload) fields. [*Note*: in IPv4, the fragmentation-offset field is expressed in multiple of 8 bytes, i.e., the amount of original payload data from the original datagram that each fragment carries (except the last fragment) must be multiple of 8 bytes.]

9. Fragmentation of an IP datagram takes place if its size is larger than the MTU of the subnet over which the datagram will be routed. Most IP datagram reassembly algorithms have a timer to avoid having a lost fragment tie up reassembly buffers

forever. Suppose a datagram is fragmented into four fragments. The first three fragments arrive, but the last one is delayed. Eventually the timer goes off and the three fragments in the receiver's memory are discarded. A little later, the last fragment stumbles in. What should be done with it?

10. What are the CIDR addresses for a network and its two subnets, if the network's addresses all start with 135.104, and one subnet should support 500 hosts and the other subnet should support 4000 hosts?

    For network:
    Total hosts = 4000 + 500 = 4500
    No. of subnets required = 4000 / 256 = 17.57 ~ 18
    ⇒ IP range = 135.104.0.0 - 135.104.17.255
    ⇒ CIDR for the network = 135.104.0.0/19

    For subnet 1:
    500 hosts / 256 hosts per octet = 1.95 ~ 2
    ⇒ IP range = 135.104.0.0 - 135.104.1.255 (512 hosts)
    ⇒ CIDR for subnet 1 = 135.104.0.0/23

    For subnet 2:
    IP range should start right after subnet 1 to not waste addresses, so the start will be from 135.104.2.0. The required range is till 135.104.17.255. (4096 hosts)
    ⇒ CIDR for subnet 2 = 135.104.2.0/19 (**Please confirm this.**)

    I have omitted the Gateway and Broadcast addresses per subnet, but there are extra IP addresses per subnet to include them if required.

11. How many addresses are spanned by the CIDR address 205.12.192.0/20, and what range do they span?

$32 - 20 = 12 \rightarrow 2^{12} = 4096$ addresses

205.12.192.0/20 → 205.12. 1100 | 0000 .0 through 205.12. 1100 | 1111 .255
205.12.192.0 through 205.12.207.255

12. The new IP protocol (IPv6) uses 16-byte addresses. When IPv6 is employed, does the ARP protocol have to be changed? If so, are the changes conceptual or technical?

Yes, the ARP protocol does need to be changed when IPv6 is employed. The changes are both conceptual and technical. Conceptually, the changes involve the way in which the ARP protocol is used and the way it is implemented. Technically, the changes involve the way the ARP protocol processes the 16-byte addresses to map them to MAC addresses.

13. One IP option is loose "source route". A datagram with this option carries in its header a list of IP addresses of routers that the datagram must visit on its way to the destination. Successive routers specified in the list do not have to be neighbors (i.e. directly connected). In general, the processing cost of options in IP routers is typically high. Specifically, a datagram with no options has a *fixed* length header, which is processed very fast after loading its five 32-bit words in as many registers. On the other hand, datagrams with options are processed slowly and sometimes with a lower priority to limit performance loss. (a) Devise an alternative technique to specify a loose source route that does not entail the performance penalty associated with the use of options, even if the source sends only one datagram. Assume no fragmentation is ever needed. (b) Consider a situation where we want to specify a loose source route from host A to host B through router C for a datagram carrying a TCP segment. Using IP options, this datagram looks as shown in Figure below. Using your alternative technique in (a), what will the datagram look like?

```
source -->     protocol   option
destination    type
--------------------------------------------------------
|   A --> B   |    TCP   |    C   |  TCP header + data  |
--------------------------------------------------------

<---------- IP header ------------><------- data ------>
```

Solution:
(a) We can use encapsulation.
(b) Datagram sent from A to C will look like this. Note that C will then decapsulate the original datagram that now has no option, i.e. fixed header size.
source --> protocol
destination type

```
source --> protocol
destination type
---------------------------------------------------------------
| A → C | IP-in-IP | A → B | TCP | TCP header + data |
---------------------------------------------------------------
<--- IP header ---><--------------- data ----------------->
```

14. Why is the data link layer in IEEE 802 LANs divided into sublayers? What does each sublayer implement?

15. Describe at least one way by which bit-oriented framing methods achieve data transparency, *i.e.* make sure that the closing flag does not appear within the frame.

Bit Stuffing

16. Suppose you are connecting ethernet segments together to build a campus-wide network. Describe three different ways a given pair of segments might be connected. For each, briefly discuss the ramifications (e.g., limitations, advantages, disadvantages).

    - All machines connected to each other with individual links.
        - Obviously very inefficient
    - All machines connected to a central switch.
    - Multiple bridges throughout the network,

17. List at least three reasons why would an Ethernet adaptor accept (pass to the host's memory) a frame.

    Some acceptance reasons:
    - If the Frame was specifically intended for that machine. (Exact destination Ethernet address match.)
    - If the Frame is a part of a broadcast.
    - If the adaptor is operating in Promiscuous Mode.
    - If the machine's Ethernet address was a part of the Multicast group the Frame was sent to.

18. Although CSMA/CD is still needed for legacy LAN configurations, it is not needed in modern Ethernet networks where computers and Ethernet switches are connected via full-duplex point-to-point links. Explain why.

Full-duplex means data can be transmitted in both directions at the same time, so we don't need to detect collisions. Point-to-point links allow a pair of computers/switches to communicate directly. At no point will there be more than 2 computers/switches using any link, ie no transmission link sharing needs to happen.

19. On an Ethernet, IP addresses are resolved by using the ARP protocol to obtain corresponding Ethernet addresses. With the help of a diagram, explain how ARP works.

20. Describe a resource discovery protocol that allows mobile IP users to rediscover the location of local area network resources (e.g. local printer) each time they move to a different LAN. Your protocol should allow the mobile user to request the location of any type of resource any time the user needs to. Your protocol can make use of existing TCP/IP protocols. Specify the format of your protocol messages and at which layer of the TCP/IP protocol stack your protocol belongs. Your protocol should be simple and flexible!

21. Why can't the CSMA/CD protocol be used as is in a wireless LAN? State at least two reasons.

    Collisions might not be detected due to the following reasons:

- Hidden Terminal Problem (Obstacles in the way, or geographic location makes it hard to detect other transmitters)
- Signal Fading problem
    - Transmitters cannot listen and send at the same time, so it cannot use the same mechanism as CSMA/CD to detect collisions.

22. How many addresses are spanned by the CIDR address 214.13.192.0/21, and what range do they span?

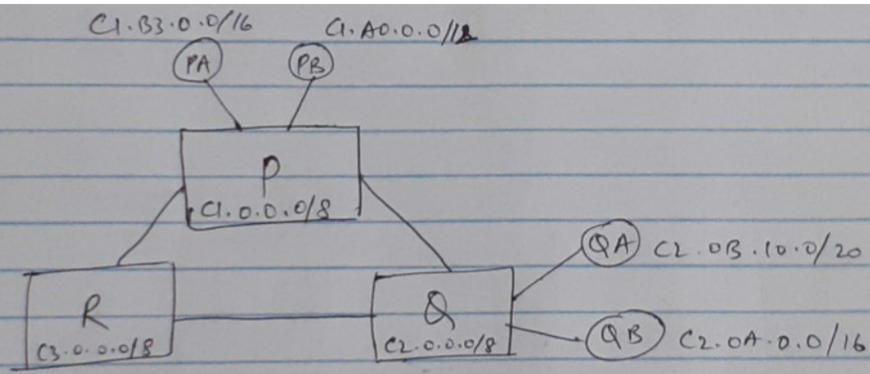
    Range: 214.13.192.0 - 214.13.199.255
    Total no. of IP addresses: 8 * 256

23. Suppose P, Q, and R, are network service providers, with respective CIDR address allocations C1.0.0.0/8, C2.0.0.0/8, and C3.0.0.0/8 (using hexadecimal dotted notation with mask). Each provider's customers initially receive address allocations that are a subset of the provider's address space.
    P has the following customers:
    - PA, with allocation C1.B3.0.0/16, and
    - PB, with allocation C1.A0.0.0/12.

    Q has the following customers:
    - QA, with allocation C2.0B.10.0/20, and
    - QB, with allocation C2.0A.0.0/16.

    (a) Assume there are no other providers or customers, and that each provider connects to both of the others. Give the routing table for a router in provider **P** and indicate, for each destination entry, the next hop using the name of the domain (provider or customer). Also assume that we want to be able to send a datagram to any destination address, i.e. we have routing entries for the address range/subrange that contains that destination. Also, you may assume that the path selection is based on the shortest AS path criterion. (Please make any other assumptions clear in your answer.)

    (b) Now suppose customer PB switches to provider Q and customer QA switches to provider R. Use the CIDR longest prefix match rule to give the routing table for a router in **P** that allows PB and QA to switch without renumbering (i.e., keeping their initial address allocations).




(a) At P

| IP | Next Hop |
|---|---|
| C3.0.0.0/8 | R |
| C2.0.0.0/8 | Q |
| C1.B3.0.0/16 | PA |
| C1.A0.0.0/12 | PB |

(b) At P

| IP | Next Hop |
|---|---|
| C3.0.0.0/8 | R |
| C2.0.0.0/8 | Q |
| C1.B3.0.0/16 | PA |
| C2.0B.10.0/20 | ~~QA~~ R |
| C1.A0.0.0/12 | Q |