Question 1
Defend or contradict this statement: for maximum efficiency, at the expense of reliability, an application should bypass TCP or UDP and use IP directly for communication.

No.
Applications need to use the transport layer (e.g., TCP or UDP).
If you just use IP, how will the message find its way to the application?

Question 2
What is the security danger of having an intruder hack into a DNS resolver?

The hacked DNS resolver can give applications incorrect IP addresses, redirecting them to other nodes.

Poor answer: the intruder will get access to the cache of frequently-used lookups.

Totally wrong:
- The intruder will get access to your name, address, and other personal info.
- The intruder will be able to connect to other machines.

Question 3
Why does VoIP (Voice over IP) telephone software usually use UDP instead of TCP?

UDP is ideal for loss-tolerant, real-time streaming services. There is no time to retransmit packets if they have errors.

UDP transmission gives lower latency and very low jitter – which matters a lot in VoIP.

Speed of the connection is generally not an issue. VoIP tends to be low bandwidth (a few tens of kbps).

Bad answers:
- No need to set up a connection (that would be a one-time overhead).
- Out of order messages are ok (not really – they would cause glitches in the voice).

Question 4
Circuit switching does not require packetizing data and the overhead of adding a destination header to each packet. What makes packet switching preferable?

It can make more efficient use of the network.

An application is not limited to a fixed % of the available bandwidth and bandwidth does not get wasted if one app has nothing to send.
- It ensures that time slots will not be wasted.

Question 5
In a negative acknowledgement protocol:
(a) The receiver notifies the sender that a message was not received or received with errors.
(b) The sender does not transmit the next message until the previous one was acknowledged.
(c) The receiver notifies the sender that a message was received correctly.
(d) The sender gives the receiver confirmation that an acknowledgement message was received.

A negative acknowledgement (NAK) is the opposite of a positive acknowledgement (ACK).
It indicates that a message is missing or contained errors.
Question 6

Which was not a design principle of the ARPANET?
(a) Support the interconnection of different types of physical networks.
(b) Provide centralized control and monitoring of the core network.
(c) Use routers to forward packets.
(d) Assume unreliable end-to-end communication.

The Internet was designed to be decentralized.

Question 7

Devices on a LAN are considered peers because:
(a) They are all directly connected to each other.
(b) They all have equivalent computing capabilities.
(c) Any device can send data to any other device.
(d) They work together to provide a single service.

Peer devices on a LAN:
- All devices have equal control of the network
- Any device can initiate data transfer with any other device on the network

That's a peer in peer-to-peer app architectures

Question 8

IP (Internet Protocol) provides us with this type of message delivery:
(a) Unreliable but with a notification of lost data or damaged data.
(b) Reliable end-to-end.
(c) Reliable but only within the network core, not the edges.
(d) Best-effort delivery, where some messages might be lost.

(a) If packets are dropped by routers, nobody gets notified.
(b, c) IP does not assume that any part of the network is reliable

Question 9

Peering among ISPs means:
(a) ISPs agree to forward and receive traffic between each other without charge.
(b) ISPs are connected together but charge for moving traffic between them.
(c) Hosts on multiple ISPs may form a peer-to-peer network.
(d) A single host may be connected to several ISPs for fault tolerance

Another use of the word peering
For ISPs, peering refers to an agreement to exchange traffic.

The accepted meaning of peering is that there is a mutual exchange of data at no cost.
Some people started to use peering to refer to cases where there is a fee but that is not the standard usage.

Question 10

TCP occupies which layer of the OSI protocol model?
(a) Physical.
(b) Data Link.
(c) Network.
(d) Transport.

Layer 1: Physical = hardware (voltages, connectors)
Layer 2: Data Link = transfers data between nodes in a LAN or between adjacent nodes in a WAN
Layer 3: Network = manages the route of data
Layer 4: Transport = application-application communication (TCP, UDP)

Question 11

UDP occupies which layer of the OSI protocol model?
(a) Physical.
(b) Data Link.
(c) Network.
(d) Transport.

UDP is not a lower level protocol than TCP

Layer 1: Physical = hardware (voltages, connectors)
Layer 2: Data Link = transfers data between nodes in a LAN or between adjacent nodes in a WAN
Layer 3: Network = manages the route of data
Layer 4: Transport = application-application communication (TCP, UDP)
Question 12
Which Windows socket (Winsock) system call causes a socket to wait for an incoming connection?
(a) connect
(b) bind
(c) accept
(d) listen

Windows socket calls = mostly the same as sockets on other systems
connect: sent by client to establish a connected socket to the server
bind: associate a local IP address & port number with a socket
accept: wait for and accept an incoming connection, creating a new socket
listen: used by the server to make a socket into one that can listen for and accept connections

Question 13
Threads within a process share:
(a) A common stack.
(b) Open file descriptors and sockets.
(c) Processor registers and the instruction pointer.
(d) Local variables.

Threads share:
- Process ID, open files (& sockets), signals, memory map
Threads get their own:
- Thread ID, CPU state, stack (=local variables)

Question 14
What is the delay for a transmission that traverses five (5) network links that are each 1 Gbps with an average packet size of 1,000 bytes?
(a) 5 μs
(b) 5 ms
(c) 40 μs
(d) 40 ms

N = # links = 5
L = packet size = 8 * 1,000 bytes = 8,000 bits
R = transmission rate = 1 Gbps = 1 × 10^9 bits/s = 1,000 × 10^6 bits/s

\[ \text{Trafic intensity} = \frac{L}{R} = \frac{8,000}{1,000 \times 10^6} = 8 \times 10^{-3} \text{ packets/s} \]

Question 15
If packets in the above problem arrive at an average rate of 200,000 packets per second, what is the traffic intensity?
(a) 0.2
(b) 1.0
(c) 1.6
(d) 8.0

a = arrival rate = 200,000 packets per second
L = packet size = 8 * 1,000 bytes = 8,000 bits
R = transmission rate = 1 Gbps = 1 × 10^9 bits/s = 1,000 × 10^6 bits/s

\[ \text{Trafic intensity} = \frac{L}{R} = \frac{8,000}{1,000 \times 10^6} = 8 \times 10^{-3} \text{ packets/s} \]

Question 16
Which traffic intensity value will likely result in little or no packet loss:
(a) 0.18
(b) 0.92
(c) 1.0
(d) 1.024

Java's synchronized block of code is a way:
(a) Request that multiple threads be created to run the block of code in parallel.
(b) Force a thread to execute code at a specific time of day.
(c) Enable several threads to run the block of code at the exact same time.
(d) Ensure that only one thread at a time executes within that block of code.

The synchronized provides a way to lock a region of code so that only one thread – holding that lock – can have access to that code

```
private Object lock = new Object();
synchronized(lock) {
    name = myname;
    age = myage;
}
```
Question 18
A race condition is:
(a) The condition where the outcome of a program is dependent on a specific order of thread scheduling.
(b) A bug where one thread keeps another thread from executing.
(c) The behavior of threads where the operating system schedules one thread more frequently than another.
(d) A situation where multiple concurrent threads are competing to finish their task first.

A race condition is a bug where the results of a program are due to exactly how the threads are scheduled.
• It occurs because mutual exclusion (locks) for critical sections is not defined

Question 19
You can register a domain name via any one of multiple domain name registrars because:
(a) The registrar simply keeps track of the mapping between your domain name and IP address.
(b) DNS servers are decentralized and the registrar can act as a DNS zone for your domain.
(c) The database of domain names for each top-level domain is distributed across all registrars.
(d) Registrars all interact with the same master database for the top-level domain held by a registry operator.

A race condition is a bug where the results of a program are due to exactly how the threads are scheduled.

Question 20
A DNS record for a canonical name (CNAME) contains:
(a) The IP address for that domain name.
(b) A domain name that for which the queried name is an alias.
(c) The domain name that is the immediate parent of the one being queried.
(d) The name server that is responsible for that domain name.

CNAME = alias name

Question 21
If a root name server cannot answer an iterative query for a valid domain name, it will:
(a) Forward the query to a name server responsible for that domain.
(b) Forward the query to a name server one level lower in the domain hierarchy.
(c) Return a referral to another root name server that may have the answer.
(d) Return a referral to another non-root name server lower in the domain hierarchy.

(a, b) Iterative queries ⇒ no forwarding
(c) A referral will not be sent to another root DNS server – they all have the same data

Question 22
Names under the in-addr.arpa domain are:
(a) IP addresses, which are resolved through DNS servers run by Regional Internet Registries.
(b) Systems that used to be on the old ARPANET but have not migrated to hierarchical domain names.
(c) Domain names for private nodes within an organization.
(d) ISP names to allow routers to query destination routes

Used for reverse DNS
.in-addr.arpa = Address and Routing Parameter Area top-level domain
Referrals to Regional Internet Registries, which handle address assignments
• RIPE will send referrals to ISPs

Question 23
Why do DNS (Domain Name System) servers use UDP by default?
(a) It is faster.
(b) It is more reliable.
(c) It makes it easier to associate responses with requests.
(d) It is more secure.

(b-d) do not make sense
Attraction of UDP for DNS:
• DNS queries are short: typically one query message & one reply
  - TCP will require an extra handshake for connection setup & will be 2x slower
• Require no memory to store connection state in the OS kernel
  - Heavily used DNS servers won’t waste lots of memory keeping track of connections
Question 24

Persistent HTTP connections:
(a) Allow multiple objects to be sent in parallel over the same connection.
(b) Are more user-friendly since the user does not need to authenticate for each page access.
(c) Speed up object access by not requiring a connection to be set up for each object accessed.
(d) All of the above.

(a) No. That's pipelining or multiplexing
(b) HTTP authentication isn't connection-specific (we didn't even cover this)
(c) Yes: one connection, many requests

Question 25

HTTP cookies:
(a) Are mini databases that contains things like shopping cart contents, passwords, and user preferences.
(b) Enable the passing of state between clients and servers even though HTTP itself is stateless.
(c) Store a complete browsing history of all sites that a user visited.
(d) Enable third parties to insert ads into a web page that a user requested

(a) No. Cookies were not designed for this – that data is stored on servers.
(b) HTTP authentication isn't connection-specific (we didn't even cover this)
(c) Yes: one connection, many requests
(d) No. A server may use 3rd party components but, on their own, third parties cannot manipulate your page via cookies.

Question 26

An HTTP Conditional GET request enables:
(a) A server to send additional objects that are associated with the requested objects.
(b) A client to request content for specific media formats and screen resolutions.
(c) A client to avoid contacting the server if its cached content has not reached its expiration time.
(d) A server to return content only if the client's cached copy is no longer valid.

Conditional GET = server request to get content if it has been modified

Question 27

HTTP/2 multiplexing improves on pipelining by allowing a client to:
(a) Send successive requests without waiting for responses.
(b) Receive responses that can be intermingled or out of order.
(c) Open multiple connections to the server and send requests in parallel.
(d) Compress headers to reduce the number of packets that need to be transmitted.

Parallel Connections
Different requests for objects are sent on separate connections.

Pipelining
Send multiple requests but responses must come in order.
One long response (e.g., high resolution photo or video) will hold up other objects

Multiplexing
Send multiple requests
Responses can arrive in any order and be interleaved (a long response may be chopped into multiple pieces with other responses in between)

Question 28

Passive FTP:
(a) Uses a single TCP connection for both data and commands, similar to HTTP.
(b) Accepts scripted commands instead of an interactive session with a user.
(c) Ensures that clients cannot perform destructive operations, such as overwriting or deleting files.
(d) Requires the client to open both command and data connections to the server.

(a) No. Both active and passive FTP use two connections
(b) That's up to the shell.
(c) No.
(d) Yes. With active FTP, the server opens the data connection to the client.

Question 29

Which system uses a central server as a content directory?
(a) Napster.
(b) Gnutella.
(c) Kazaa.
(d) BitTorrent.

Gnutella and Kazaa have decentralized directories.
BitTorrent doesn't handle naming.
**Question 30**

In peer-to-peer systems, an overlay network is:
(a) A graph of nodes that know about each other.
(b) A set of high-speed links that connect specific nodes together.
(c) A secondary network to provide fault tolerance.
(d) A set of persistent connections among nodes to optimize message delivery.

For software systems, an overlay network isn’t a real network. It’s the knowledge that each machine has of others
E.g., a gnutella peer knows of five other peers. They, in turn, know other machines. Flooding enables a message to get relayed and distributed to a large set of systems.

**Question 31**

BitTorrent differs from Kazaa and Gnutella in that:
(a) Provides distributed file storage.
(b) Provides scalable performance when there are more downloads of a specific file.
(c) Provides a decentralized naming system.
(d) Uses flooding to locate content.

With Kazaa and Gnutella, content sits as a single file on a node ⇒ many downloaders = heavy load

With BitTorrent, downloaders can serve partial content.

**Question 32**

A finger table in the Chord distributed hash table (DHT):
(a) Is a hash table that stores the mapping between names and node addresses.
(b) Stores a partial list of nodes in the system.
(c) Keeps track of the relocation of content among nodes.
(d) Keeps track of which nodes hold backup content.

It stores nodes that are $2^0$, $2^1$, $2^2$, $2^3$, $2^4$, $2^5$, ... hops away.

The end