1. MAC means Media Access Control
A. True
B. False

2. The MAC address has 6 groups of 2 hexadecimal numbers
A. True
B. False

A MAC (Media Access Control) address is a unique, 12-character hexadecimal string that identifies a device on a network. It is often referred to as a "physical address" or "hardware address." The format of a MAC address is XX:XX:XX:XX:XX:XX, where each X represents a hexadecimal digit (0-9 or A-F). The first six digits (XX:XX:XX) identify the manufacturer of the device, while the last six digits (XX:XX:XX) identify the specific device.

3. UDP guarantees datagram delivery
A. True
B. False

No, UDP (User Datagram Protocol) does not guarantee datagram delivery.

UDP is a connectionless and unreliable protocol, which means that it does not establish a connection before sending data and does not guarantee that the data sent will be received or that it will be received in the order it was sent.

UDP does not provide any mechanism for error checking, retransmission, or flow control. This means that if a UDP packet is lost or corrupted during transmission, the sender will not know and the packet will not be retransmitted. This is different from TCP (Transmission Control Protocol) which establishes a connection before sending data and guarantees that the data sent will be received and that it will be received in the order it was sent.

UDP is typically used for applications that require fast, efficient transfer of data, such as streaming audio and video, where the loss of a small number of packets is acceptable. Applications that require reliable delivery of data, such as file transfers, typically use TCP.

It's worth noting that, even though UDP doesn't guarantee the delivery, it has lower overhead and it's faster than TCP, and that's why it's used in applications where the lost of packets is acceptable.

4. The socket type used by TCP is SOCK_STREAM
A. True
B. False

Yes, the socket type used by TCP is SOCK_STREAM.

TCP (Transmission Control Protocol) is a connection-oriented transport protocol. It establishes a reliable, two-way connection between two devices before sending data, and guarantees that the data sent will be received and that it will be received in the order it was sent.

In order to use TCP, a socket must be created with the socket type SOCK_STREAM. This tells the operating system to use TCP as the transport protocol. When a socket is created with this type, it is bound to a specific port on the local machine, which is used to identify the process that is providing the service.

On the other hand, UDP (User Datagram Protocol) is a connectionless and unreliable protocol, it doesn't establish a connection before sending data and it doesn't guarantee that the data sent will be received or that it will be received in the order it was sent. For this reason, the socket type used by UDP is SOCK_DGRAM.

It's worth noting that, both SOCK_STREAM and SOCK_DGRAM are constants defined in the C library, and are used to indicate the type of socket you want to create.

5. The connect system call is normally called by the client process in order to connect to a server process.
A. True
B. False

Yes, the connect system call is normally called by the client process in order to connect to a server process.

The connect system call is used to establish a connection between a client and a server process. It is typically used with the socket type SOCK_STREAM, which is used for TCP connections. The connect system call takes as input the socket descriptor, the IP address and port number of the server, and attempts to establish a connection with the server.

When a client process calls connect, it sends a connection request to the server. The server, in turn, can either accept or reject the connection request. If the server accepts the connection, the client and server can then send data to each other.

It's worth noting that, the connect system call is not used with the socket type SOCK_DGRAM, which is used for UDP connections, because UDP is a connectionless protocol and does not establish a connection before sending data. Instead, the sendto and recvfrom system calls are used with SOCK_DGRAM sockets.

It's also important to mention that, The connect system call can also be used to connect to a specific IP address and port number on the local machine, this is useful for testing a server program without having to set up a separate client program.

6. The listen system call indicates to the protocol that the client process is ready to accept new incoming connections on the socket.
A. True
B. False

The listen system call is typically used on the server side of a network connection, and it is used to indicate to the protocol stack that the server process is willing to accept new incoming connections on the socket. The listen call takes two arguments: the first is the file descriptor of the socket, and the second is the maximum number of connections that the server is willing to queue up in the backlog. This means that if a client tries to connect to the server and the server is not ready to accept the connection, the connection request will be added to a queue and the server will process the connection request once it is ready.
Once the listen system call is made, the server can use the accept system call to accept incoming connections from clients.

7. At the level of a TCP client, the bind system call is mandatory
A. True
B. False

At the level of a TCP client, the bind system call is not mandatory. TCP clients typically use the connect system call to initiate a connection to a server. The connect system call automatically binds the socket to a local IP address and port number before sending the connection request to the server. The IP address and port number are usually chosen by the operating system from the available IP addresses and port numbers on the client machine.
However, if the client wants to bind the socket to a specific IP address and port number before making the connection, it can use the bind system call before the connect system call.
It is worth noting that in some cases, when the client is behind a NAT (Network Address Translation) device, it may need to bind to a specific address and port in order to be able to establish a connection with the server.

8. The high order bits of an IP Address represent the host part.
A. True
B. False

No, the high order bits of an IP address represent the network portion, not the host portion.

IP addresses are divided into two parts: the network portion and the host portion. The network portion identifies the specific network that the device is connected to, and the host portion identifies the specific device within that network.
In IP version 4 (IPv4), IP addresses are 32-bits long and are typically represented in dotted decimal notation (e.g. 192.168.0.1). The number of bits used for the network portion of the address is determined by the subnet mask.

The subnet mask is a 32-bit value that is used to divide the IP address into the network and host portions.
For example, if the subnet mask is 255.255.255.0, the first 24 bits of the IP address represent the network portion, and the last 8 bits represent the host portion.

In IP version 6(IPv6) addresses are 128 bits long, it uses the CIDR notation (Classless Inter-Domain Routing) and the prefix notation to define the network and host portions.

In summary, the high-order bits of an IP address represent the network portion, not the host portion.

9. All the hosts from the same network can physically reach each other without an intervening router
A. True
B. False

Yes, all the hosts from the same network can physically reach each other without an intervening router, as long as they are connected to the same LAN (Local Area Network).

A LAN is a group of devices that are connected together in a specific geographic area, such as a building or campus. Devices on a LAN can communicate with each other directly, without the need for an intervening router. This is because they share the same broadcast domain, meaning that they can all reach each other by broadcasting a message to all devices on the network.

However, if the hosts are on different network they will need a router to forward their packets to the corresponding network. The router will use the IP addresses and the routing tables to determine to which network the packet should be sent.

It's worth noting that, even if the hosts are on the same LAN, if they are on different subnets, they will still need a router to communicate with each other.

10. A network address can be determined based on a IP Address from the network and the netmask.

A. True

B. False

Yes, a network address can be determined based on an IP address from the network and the netmask.

The network address is the logical AND of the IP address and the netmask. The netmask is used to separate the IP address into the network portion and host portion, and it is typically represented in the same format as an IP address.

To determine the network address, the IP address and the netmask are converted to binary and then a logical AND operation is performed bit-by-bit. The result of this operation is the network address.

Example:

IP Address: 192.168.1.25 (11000000.10101000.00000001.00011001)
Netmask: 255.255.255.0 (11111111.11111111.11111111.00000000)
Network Address: 192.168.1.0 (11000000.10101000.00000001.00000000)
It's worth noting that this method is only valid for IPv4, in IPv6 the netmask is replaced by the prefix notation (prefix/length)

By using the network address and the netmask, it is possible to know the range of valid IP addresses that belong to the same network.

11. Always, in a class of addresses, the first and last IP addresses are reserved.

A. True

B. False

In a class of addresses, the first and last IP addresses are reserved for specific purposes.

In IPv4, IP addresses are divided into classes: A, B, C, D and E. Each class has a different number of bits for the network portion and the host portion of the address, and different ranges of valid IP addresses.

For class A addresses, the first IP address (network address) is reserved for identifying the network and the last IP address (broadcast address) is reserved for broadcasting messages to all hosts on the network.

For class B addresses, the first and last IP addresses of the second and third octet are also reserved for the network and broadcast addresses respectively.

For class C addresses, the first and last IP addresses of the third and fourth octet are reserved for the network and broadcast addresses respectively.

It's worth noting that the use of classful addressing is outdated and it was replaced by the Classless Inter-Domain Routing (CIDR) notation that allows for more efficient use of IP addresses by allowing for more specific subnetting. In CIDR notation, the number of bits used for the network portion of the address is determined by the prefix, not by the class of the address.

It's also important to mention that, due to the depletion of IPv4 addresses, some IP ranges that were reserved for special use, such as private IP ranges, are now being used for production purposes.

12. For connecting a host with a private address to the Internet, it has to be translated to a public address, process named ARP.
A. True
B. False

No, the process of connecting a host with a private address to the Internet is called NAT (Network Address Translation), not ARP (Address Resolution Protocol).

ARP is a protocol that is used to map a network address (such as an IP address) to a physical address (such as a MAC address) on a LAN (Local Area Network). It is used to determine the physical address of a device on the network when you only know its IP address.

NAT, on the other hand, is a technique used to allow hosts on a private network to communicate with hosts on a public network, such as the Internet. The hosts on the private network have private IP addresses that are not globally unique, so they cannot communicate directly with hosts on the public network. NAT allows these hosts to communicate by translating their private IP addresses to a public IP address that is globally unique.

NAT is typically implemented at the edge of the network, by a device called a NAT router. The NAT router has two interfaces, one connected to the private network and one connected to the public network. When a host on the private network initiates a connection to a host on the public network, the NAT router intercepts the packet, changes the source IP address to the public IP address and forwards the packet to the public network.

In summary, ARP is used to determine the physical address of a device on a LAN, NAT is used to allow hosts on a private network to communicate with hosts on a public network by translating their IP addresses.

13. 172.16.0.0/12 refers to a private address space.
A. True
B. False

Yes, 172.16.0.0/12 refers to a private address space.

In IPv4, there are three ranges of IP addresses that are reserved for use on private networks, and are not globally unique. These ranges are:

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
The notation 172.16.0.0/12 is called CIDR notation and it's used to represent IP ranges. It's a combination of an IP address and a prefix length. In this case, the IP address is 172.16.0.0 and the prefix length is 12, which means the first 12 bits of the IP address are used to identify the network. This range includes all the IP addresses from 172.16.0.0 to 172.31.255.255

These ranges are intended for use on private networks, such as home or corporate networks, and are not supposed to be routed on the public Internet.

It's also worth noting that private IP addresses can be used behind a NAT router that connects a private network to the Internet. The NAT router will translate the private IP addresses to public IP addresses before sending the packets to the Internet.

14. A DNS server is responsible with translating numerical IP addresses to domain names.
A. True
B. False

Yes, a DNS (Domain Name System) server is responsible for translating numerical IP addresses to domain names (and vice versa).

DNS is the system that translates domain names, such as www.example.com, into IP addresses, such as 192.168.1.1. This is done using a hierarchical system of DNS servers. When a client wants to access a website, it sends a request to the local DNS resolver, which is typically provided by the client's ISP (Internet Service Provider). The local DNS resolver then checks its cache to see if it has a recent copy of the DNS record for the domain name. If it doesn't, it sends a request to a root DNS server, which tells it the address of the top-level domain (TLD) DNS server responsible for the domain. The local DNS resolver then sends a request to the TLD DNS server, which tells it the address of the authoritative DNS server for the domain. The local DNS resolver then sends a request to the authoritative DNS server, which responds with the IP address associated with the domain name.

It's worth noting that, in addition to resolving domain names to IP addresses, DNS servers also provide other information, such as email servers or name servers for a domain.

It's also important to mention that, DNS resolution process is done recursively, meaning that the client's DNS resolver will go through the hierarchy of DNS servers, starting with the root, to find the authoritative DNS server for the domain and retrieve the IP address associated with it.

15. The network address can be obtained from an IP address and the netmask using the logical operation "OR"
A. True
B. False

No, The network address can be obtained from an IP address and the netmask using the logical operation "AND", not "OR".

The network address is the result of applying a bitwise AND operation between the IP address and the netmask. The netmask is used to separate the IP address into the network portion and host portion, and it is typically represented in the same format as an IP address.

To determine the network address, the IP address and the netmask are converted to binary and then a logical AND operation is performed bit-by-bit. The result of this operation is the network address.

Example:

IP Address: 192.168.1.25 (11000000.10101000.00000001.00011001)
Netmask: 255.255.255.0 (11111111.11111111.11111111.00000000)
Network Address: 192.168.1.0 (11000000.10101000.00000001.00000000)
It's worth noting that this method is only valid for IPv4, in IPv6 the netmask is replaced by the prefix notation (prefix/length)

By using the network address and the netmask, it is possible to know the range of valid IP addresses that belong to the same network.

The OR operation instead is used to obtain the broadcast address, which is the result of applying a bitwise OR operation between the IP address and the inverted netmask.

16. When NAT is involved, the local network uses just one IP address as far as outside world is concerned

A. True

B. False

Yes, when NAT is involved, the local network uses just one IP address as far as the outside world is concerned. This is called a "one-to-one" NAT, also known as "simple NAT".

In this type of NAT, a single public IP address is used to represent all the devices on the private network. Each device on the private network has a unique private IP address, but when it sends a request to the outside world, its private IP address is replaced with the public IP address.

This allows multiple devices on the private network to share a single public IP address, which is useful in situations where the number of available public IP addresses is limited. It also provides a level of security by hiding the private IP addresses of the devices on the local network.

When a device on the local network initiates a connection to an external device, the NAT router maps the internal IP address and port number to a unique external IP address and port number. Once the connection is established, the NAT router keeps track of the mapping and uses it to forward incoming packets to the correct internal device.

It's worth noting that there are other types of NAT such as Port Address Translation (PAT) and dynamic NAT, which can also be used to map multiple private IP addresses to a single public IP address.

17. The number of IP addresses allocated for each subnet block has to be a power of 4.

A. True

B. False

No, the number of IP addresses allocated for each subnet block does not have to be a power of 4.

The number of IP addresses allocated for each subnet block is determined by the number of bits used for the host portion of the IP address, which is determined by the subnet mask. The subnet mask is a 32-bit value that is used to divide the IP address into the network portion and host portion.

A subnet mask can be used to create any number of subnets, as long as it meets the requirement of having a unique network address and a valid range of host addresses.

For example, the subnet mask 255.255.255.248 (11111111.11111111.11111111.11111000) can be used to create 6 subnets. Each subnet will have 6 usable IP addresses.

In general, the number of IP addresses allocated for each subnet block can be calculated by using the formula 2^n - 2 where n is the number of bits used for the host portion of the IP address.

It's worth noting that, in practice, the number of IP addresses allocated for each subnet block is usually a power of 2, because it makes it easier to calculate the number of usable IP addresses and to manage the subnets. But it's not a requirement.

18. 209.220.186.8/255.255.255.248 is a invalid IP/Netmask combination
A. True
B. False

209.220.186.8/255.255.255.248 is not an invalid IP/Netmask combination but it is a valid IP address and a valid netmask.

In this combination, 209.220.186.8 is a valid IP address and 255.255.255.248 is a valid netmask. It is also called CIDR notation, where the IP address and netmask are combined to represent the IP range.

The prefix length of 255.255.255.248 is 29, which means that the first 29 bits of the IP address are used to identify the network and the last 3 bits are used for the host portion. This netmask can create 8 subnets, each one with 6 usable IP addresses.

It's worth noting that the IP address 209.220.186.8 can be either a public or private IP address, whether it's public or private depends on the IP range it belongs to, not the netmask.

It's also important to mention that, in this specific IP address, it's not possible to say if it's a valid IP address or not without further context, as it depends on the IP allocation of the organization or the service provider.

19. The default gateway serves as an access point or IP router that a networked computer uses to send information to a computer in the same network or the Internet.
A. True
B. False

Yes, the default gateway serves as an access point or IP router that a networked computer uses to send information to a computer in the same network or the Internet.

A default gateway is the IP address of the router that is used to connect a local network to the Internet or to another network. It acts as a gateway, directing traffic between the local network and other networks.

When a device on a local network wants to communicate with a device on a different network, it sends the packet to the default gateway. The gateway then checks its routing table to determine the next hop for the packet, and forwards it to the next hop. If the destination is on a different network, the packet is forwarded to the router that connects the local network to the Internet or to other networks.

The default gateway is usually configured on a device during the initial network setup and is used by all the devices on the network. It's usually the IP address of the router on the local network.

It's worth noting that, the default gateway is a necessary configuration for devices to be able to access the Internet or other networks and it's a key element in the communication between the local network and other networks.

20. A 255.255.255.240 netmask is capable of supporting 16 hosts.
A. True
B. False

No, A 255.255.255.240 netmask is not capable of supporting 16 hosts.

The number of hosts that can be supported by a subnet is determined by the number of bits used for the host portion of the IP address, which is determined by the subnet mask.

A subnet mask of 255.255.255.240 is a valid subnet mask, it corresponds to a CIDR prefix of /28, which means that the first 28 bits of the IP address are used to identify the network, and the remaining 4 bits are used for the host portion.

The number of hosts that can be supported by this subnet mask can be calculated by using the formula 2^n - 2, where n is the number of bits used for the host portion of the IP address (4 in this case).

So, 2^4 - 2 = 14, which means that this subnet mask is capable of supporting 14 hosts. This subnet has 14 usable IP addresses, typically the first and last IP addresses are reserved as network and broadcast addresses respectively.

It's worth noting that this calculation only applies to IPv4, in IPv6, the subnetting is done using the prefix notation (prefix/length), and the number of hosts supported by a subnet is calculated differently.

An example of using a 255.255.255.240 subnet mask could be for a small office network.

Let's say the office has been assigned the IP range of 209.220.186.0/22 by their ISP. To divide this range into smaller subnets to better organize and manage the network, the network administrator could choose to use a 255.255.255.240 subnet mask for one of the subnets.

Using the 255.255.255.240 subnet mask, the subnetting would be:

Network Address: 209.220.186.8
Broadcast Address: 209.220.186.15
Usable IP range: 209.220.186.9 - 209.220.186.14
In this example, the subnet 209.220.186.8/28 has 14 usable IP addresses, enough for 14 hosts, such as desktops, laptops, printers, and servers.

It's worth noting that this is just an example and that the actual IP addresses and the number of hosts in a network can vary depending on the actual network topology, security policies and the organization's needs.

Also, it's important to mention that the network administrator can use different subnet masks and IP ranges to create different subnets according to the organization's needs and the size of the network.

21. A computer uses HTTP to look up domain names and get the associated IP address.
A. True
B. False

No, a computer does not use HTTP to look up domain names and get the associated IP address. HTTP (Hypertext Transfer Protocol) is a protocol used for transferring data over the internet, it is used for communication between web clients and servers, but it doesn't have anything to do with domain name resolution.

A computer uses DNS (Domain Name System) to look up domain names and get the associated IP address. DNS is a hierarchical system of servers that translate domain names into IP addresses. When a client wants to access a website, it sends a request to the local DNS resolver, which is typically provided by the client's ISP (Internet Service Provider). The local DNS resolver then checks its cache to see if it has a recent copy of the DNS record for the domain name. If it doesn't, it sends a request to a root DNS server, which tells it the address of the top-level domain (TLD) DNS server responsible for the domain. The local DNS resolver then sends a request to the TLD DNS server, which tells it the address of the authoritative DNS server for the domain. The local DNS resolver then sends a request to the authoritative DNS server, which responds with the IP address associated with the domain name.

It's worth noting that, DNS is a separate service that runs on its own network protocol, not on HTTP.

22. There is no routing based on MAC addresses

A. True

B. False

Yes, There is no routing based on MAC addresses.

Routing is the process of forwarding a packet from one network to another based on the destination IP address. Routing is performed by routers, which use routing tables to determine the next hop for a packet. The routing tables are based on the IP addresses of the destinations and not on the MAC addresses.

MAC (Media Access Control) addresses are used at the data link layer of the OSI model and are used for addressing devices on a local network. They are used to identify devices on a local network and for the purpose of the ARP (Address Resolution Protocol) to map IP addresses to MAC addresses.

MAC addresses are not used for routing because they are not unique on a global scale, and are only unique on the local network. Routing decisions are based on IP addresses, which are unique and globally routable. Additionally, MAC addresses are not included in the IP packet headers, they are only used at the data link layer to identify the destination device on a local network.

It's worth noting that, the use of MAC addresses is only for the purpose of communication within a network and it's not used for communication between different networks.

23. A proxy server acts as an intermediary for requests from clients seeking resources from other servers.

A. True

B. False

Yes, A proxy server acts as an intermediary for requests from clients seeking resources from other servers.

A proxy server is a server that sits between a client and a remote server and acts as an intermediary for requests from clients seeking resources from other servers. The client sends a request to the proxy server, which then forwards the request to the remote server. The remote server then sends the response back to the proxy server, which then forwards it to the client.

There are different types of proxy servers such as:

Transparent proxy: A transparent proxy is a type of proxy server that acts as an intermediary for requests from clients without requiring any special configuration on the client side.
Anonymous proxy: An anonymous proxy is a type of proxy server that acts as an intermediary for requests from clients and hides the client's IP address.

Distorting proxy: A distorting proxy is a type of proxy server that acts as an intermediary for requests from clients and changes the client's IP address.
High anonymity proxy: A high anonymity proxy is a type of proxy server that acts as an intermediary for requests from clients and hides the client's IP address and other identifying information.
The main benefits of using a proxy server are:

Security: It can act as a firewall and a shield for the client machine, protecting it from malicious attacks.
Anonymity: It can mask the client's IP address, making it difficult for third parties to track or identify the client.
Caching: It can cache frequently requested web pages, which can speed up future requests for the same page.
Content Filtering: It can block access to certain websites or online content, and filter the type of information that is allowed to pass through.
It's worth noting that, different types of proxy servers can provide different levels of security and anonymity and can be used for different purposes such as, anonymity, caching, and content filtering.

24. The combination DNS server = Default Gateway is not possible
A. True
B. False

The combination of DNS server = Default Gateway is possible.

A DNS server is a server that is responsible for resolving domain names to IP addresses. A default gateway is an IP address that is used to forward packets to other networks when the destination IP address is not on the local network.

A router is a device that connects multiple networks together and serves as the default gateway for the devices connected to it. A router can also be configured to act as a DNS server, by having the capability to resolve domain names to IP addresses locally.

When a device on a local network wants to communicate with a device on a different network, it sends the packet to the default gateway (the router). The router then checks its routing table to determine the next hop for the packet, and forwards it to the next hop. If the destination is on a different network, the packet is forwarded to the router that connects the local network to the Internet or to other networks.

If the router is configured to act as a DNS server, it can resolve domain names to IP addresses and forward the packets to the correct destination, this eliminates the need for an external DNS server to be involved in the process.

It's worth noting that, it's also possible to have separate devices for DNS and default gateway, depending on the network topology, security policies and the organization's needs.

25. A collection of computers (PCs, Workstations) and other devices interconnected represent a computer network.
A. True
B. False

Yes, a collection of computers (PCs, Workstations) and other devices interconnected represent a computer network.

A computer network is a group of interconnected devices, such as computers, servers, printers, and routers, that are connected together to share resources and exchange information. These devices can be connected together using a variety of technologies such as wired or wireless connections, and are connected through network devices such as switches, routers, and hubs.

26. Hosts (computers), links (coaxial cable, twisted pair, optical fiber, radio, satellite), switches/routers (intermediate systems) are all components of a computer system.
A. True
B. False

Hosts (computers), links (coaxial cable, twisted pair, optical fiber, radio, satellite), switches/routers (intermediate systems) are all components of a computer network, but not of a computer system.

A computer system typically consists of the following components:

Hardware: The physical components of the computer, such as the central processing unit (CPU), memory (RAM), storage (hard drive), and input/output devices (keyboard, mouse, monitor).
Operating System: The software that controls the basic operations of the computer, such as managing memory, input/output, and processes.
Applications: Software programs that run on the computer, such as word processors, web browsers, and games.

27. Big Endian means 'most significant byte first' while little endian means 'least significant byte first.
A. True
B. False

Yes, Big Endian means 'most significant byte first' while little endian means 'least significant byte first.'

Endianness is the order in which a computer stores the bytes of a multi-byte value in memory. There are two types of endianness:

Big Endian: The most significant byte of the value is stored at the lowest memory address, and the least significant byte is stored at the highest memory address.
Little Endian: The least significant byte of the value is stored at the lowest memory address, and the most significant byte is stored at the highest memory address.

For example, let's consider the 32-bit value 0x12345678.

Big Endian representation: 12 34 56 78 (most significant byte first)
Little Endian representation: 78 56 34 12 (least significant byte first)
It's worth noting that different computer architectures and processors use different endianness, and this can cause compatibility issues if data is exchanged between different systems.

Big endian is used in some network protocols such as IPv4, IPv6, and TCP while little endian is used in most of the Intel and AMD processors, and some other architectures

28. SOCK_STREAM is used for UDP connections.
A. True
B. False

No, SOCK_STREAM is not used for UDP connections.

SOCK_STREAM is used for TCP connections. It is a socket type that creates a reliable, two-way connection between two devices before sending data, and guarantees that the data sent will be received and that it will be received in the order it was sent.

TCP is a connection-oriented transport protocol that establishes a reliable, two-way connection between two devices before sending data, and guarantees that the data sent will be received and that it will be received in the order it was sent.

29. SOCK_DGRAM is used for UDP connections.
A. True
B. False

On the other hand, SOCK_DGRAM is used for UDP connections. It is a socket type that creates a connectionless and unreliable transport protocol, it does not establish a connection before sending data and does not guarantee that the data sent will be received or that it will be received in the order it was sent.

UDP is a connectionless and unreliable protocol, it doesn't establish a connection before sending data and it doesn't guarantee that the data sent will be received or that it will be received in the order it was sent. It's used for applications that require fast, efficient transfer of data, such as streaming audio and video, where the loss of a small number of packets is acceptable.

It's worth noting that, when creating a socket, you must specify the socket type, whether it's SOCK_STREAM for TCP or SOCK_DGRAM for UDP, depending on the protocol you want to use.

30. The optical fiber cable theoretically has unlimited bandwidth.
A. True
B. False

The optical fiber cable has a very high bandwidth compared to other types of cables such as copper cables, but it is not theoretically unlimited.

Optical fiber cables are made of thin glass or plastic fibers that are used to transmit data in the form of light. They have several advantages over traditional copper cables, including:

High bandwidth: Optical fiber cables can carry much more data than copper cables, and have a higher data transfer rate.
Immunity to electromagnetic interference (EMI): Optical fiber cables are not affected by EMI, which can cause errors and slowdowns in copper cables.
Long distance: Optical fiber cables can transmit data over much longer distances than copper cables, which makes them suitable for long-distance communication.
However, the theoretical maximum bandwidth of an optical fiber cable is limited by the properties of light and the physical limitations of the cable. The amount of data that can be transmitted over an optical fiber cable depends on several factors such as the type of modulation used, the wavelength of the light, the quality of the cable, and the noise level in the environment.

It's worth noting that the available bandwidth of an optical fiber cable is also influenced by the technology and equipment used at both ends of the cable.

As the technology progresses, the optical fibers and its components tend to improve in terms of their capabilities, and the bandwidth is continuously increasing, but it's not theoretically unlimited.

31. Every domain name that is not already in use is free to claim as your own.
A. True
B. False

No, not every domain name that is not already in use is free to claim as your own.

Domain names are used to identify and locate websites on the internet. They are managed by organizations called domain name registrars, which are accredited by the Internet Corporation for Assigned Names and Numbers (ICANN).

When a domain name is registered, the registrant (the person or organization that registered the domain name) has the exclusive right to use that domain name for a specific period of time, usually one or more years. After that period, the domain name can be renewed by the registrant, or it can be made available for registration by someone else.

However, not all domain names are available for registration. There are some domain names that are reserved for specific uses, such as country-code top-level domains (ccTLDs) and generic top-level domains (gTLDs) like .com, .net, and .org, and some domain names that are considered premium domain names. Premium domain names are domain names that are considered to be high-value domain names, and are priced higher than standard domain names.

It's also worth noting that, some domain names are already in use, and are not available for registration, but it's possible to buy them from the current owner if they are willing to sell it.

It's important to mention that, the process of registering a domain name involves verifying that the domain name is available, and that the registrant meets certain requirements, such as providing accurate contact information and agreeing to the terms and conditions of the registration agreement.

32. 255.255.255.128 starts with 1 zero and ends with 7 zeros.
A. True
B. False

No, 255.255.255.128 does not start with 1 zero, but ends with 7 zeros.

255.255.255.128 is a subnet mask, it is used to determine the network address of an IP address. A subnet mask is a 32-bit binary number that is used to divide an IP address into two parts: the network address and the host address.

The subnet mask 255.255.255.128 is represented in binary as 11111111.11111111.11111111.10000000, it starts with 25 ones and ends with 7 zero.

It's worth noting that, the number of ones in the subnet mask indicates the number of bits used for the network address, and the number of zeroes indicates the number of bits used for the host address.

For example, with the subnet mask 255.255.255.128, the first 25 bits are used for the network address and the last 7 bits are used for the host address. This means that this subnet mask can support 2^7 (128) hosts.

It's also important to mention that, the subnet mask 255.255.255.128 is also equivalent to /25 in CIDR notation, which is a shorthand way of representing subnet masks. The number following the slash represents the number of bits used for the network address.

33. 255.255.255.128 ends with 7 zeroes.
A. True
B. False

34. Port forwarding is a use of NAT.
A. True
B. False

Yes, port forwarding is a use of Network Address Translation (NAT). NAT is a method used by routers to map a public IP address to a private IP address on a LAN (Local Area Network).

35. Mac addresses are not guaranteed to be unique.
A. True
B. False

MAC (Media Access Control) addresses, also known as hardware addresses or physical addresses, are unique identifiers assigned to network interfaces for communications on the physical network segment. ***While they are intended to be unique****, it is possible for manufacturers to produce devices with duplicate MAC addresses, or for an attacker to change a device's MAC address to a duplicate address. This can cause issues with network connectivity and security. To avoid these issues, network administrators can use techniques such as DHCP snooping and dynamic ARP inspection to validate the authenticity of MAC addresses on a network.*

36. When can a DHCP server relay IP addresses to clients on a network segment separated from the server's location?
A. DHCP server can only relay IP addresses to the clients found on the same network segment
B. when the router separating them acts as a relay agent
C. when the dhcp server uses the same IP address as the router that supports the network segment where the clients are located
D. when there are more logical routes between the dhcp server and the subnetwork clients

A DHCP server can relay IP addresses to clients on a network segment that is separated from the server's location when the DHCP relay agent is configured on a network device (such as a router) that connects the two segments. The DHCP relay agent acts as a go-between for DHCP client requests and DHCP server responses, forwarding DHCP messages between the client and server. This allows clients on the remote segment to receive IP addresses from the DHCP server on the main segment.

It is important to note that DHCP relay agent does not provide additional security features, it only helps to forward DHCP messages between different network segments. To secure DHCP communication, DHCP snooping and IP source-guard should be enabled on switch or router.

37. Choose the correct use of the Straight through and the Cross over cable

A. cross cable to connect a PC to a PC and straight through to connect a switch to a hub

Cross cable to connect a PC to a PC and straight through to connect a switch to a hub is correct. A crossover cable should be used to connect two PCs together, and a straight-through cable should be used to connect a switch to a hub.

B. cross cable to connect a router to a PC and straight through to connect a switch to a server

Cross cable to connect a router to a PC and straight through to connect a switch to a server is incorrect. A straight-through cable should be used to connect a router to a PC or a switch to a server. A crossover cable is not needed in this scenario.

C. cross cable to connect a switch to a hub and straight through to connect a router to a switch

A straight-through cable should be used to connect a switch to a router, while a crossover cable should be used to connect two switches or hubs together.

D. cross cable to connect a switch to a switch and straight through to connect a hub to a switch

A crossover cable should be used to connect two switches together and a straight-through cable should be used to connect a hub to a switch.

38. Choose the correct use of the following cables:

A. straight through to connect a hub to a switch or a hub to a PC

A straight-through cable can be used to connect a hub to a switch, as it connects the MDI port of the hub to the MDI port of the switch, allowing the hub to communicate with the switch.
A straight-through cable can also be used to connect a hub to a PC, as it connects the MDI port of the hub to the MDI port of the PC's NIC (Network Interface Card), allowing the hub to communicate with the PC.

B. cross cable to connect a PC to a server or a PC to a router

To connect a PC to a server and a PC to a router, a straight-through cable should be used.

C. straight through to connect a PC to a PC or a switch to a router

a straight-through cable can be used to connect a PC to another PC, as both PCs will have a NIC (Network Interface Card) which will have a MDI port; the straight-through cable will connect the MDI port of one PC to the MDI port of the other PC.

It is also correct to use a straight-through cable to connect a switch to a router, as it connects the MDI port of the switch to the MDI-X port of the router, allowing the switch to communicate with the router.

D. cross cable to connect a router to a router or a hub to a switch

A straight-through cable can be used to connect a hub to a switch.

39. In what situation is a PC unable to ping another PC ?
A. PCs are on two different network segments on the same network

The router is responsible for forwarding the packets between network segments, so if a PC from one network segment wants to communicate with a PC from another network segment, the router needs to be configured to forward the packets between them. If the router is not configured correctly or if there is a problem with the router, the PCs will not be able to communicate with each other, and the ping command will fail.

B. firewall is disabled on both of the PCs

no problem

C. one of the PCs is connected to the router by cross over cable

A router is a different type of device that connects different networks together, and it's not designed to communicate with a PC directly. A router has multiple network interfaces, each with its own IP address, and each interface is connected to a different network.

To connect a PC to a router, you need to use a straight-through cable, also called a patch cable. A straight-through cable connects the PC to the router's LAN port, which is the port that connects to the local network. This allows the PC to communicate with other devices on the local network and access the Internet through the router.

D. firewall is enabled on both computers
If the firewall is enabled on both computers, it might block the incoming ping request and the PCs will not be able to ping each other.

40. Which of the following is not a characteristic of the IP protocol?
A. It affects packet routing

The IP protocol is responsible for routing packets of data across different networks. It uses IP addresses to identify the source and destination of each packet, and it uses routing tables to determine the best path for each packet to take through the network. When a packet is sent, the IP protocol looks at the destination IP address and compares it to the routing table to determine the next hop. It will then forward the packet to the next hop until it reaches its final destination. This process is known as IP routing.

B. Is considered an unreliable protocol

IP is considered an unreliable protocol because it does not guarantee the delivery of packets. It is possible for packets to be lost, delayed, or delivered out of order. This is in contrast to protocols such as TCP (Transmission Control Protocol) which provide reliability by retransmitting lost packets and ordering packets that are received out of order. IP protocol only provides best effort delivery, meaning it will try to deliver the packets to the destination but it does not guarantee the successful delivery. It is up to other protocols such as TCP or the application layer to handle errors, retransmission and confirmation of receipt.

C. Is a connection-oriented protocol

It does not establish a dedicated end-to-end connection before sending data. Instead, it simply sends packets of data to a destination IP address without first confirming that the destination is ready to receive the data. IP is considered a "best-effort" delivery protocol, which means that it will make its best effort to deliver the packets to the destination, but it does not guarantee that all packets will be delivered. Connection-oriented protocols such as TCP, on the other hand, establish a dedicated end-to-end connection before sending data and guarantee the delivery of data with the help of retransmission and confirmation of receipt.

D. It defines the Internet addressing system

IP addresses are used to identify devices on the Internet and to route packets of data to their intended destinations. The IP protocol provides the mechanism for addressing and routing packets of data across networks. Each device connected to a network is assigned a unique IP address, which identifies the device and its location on the network. This allows packets of data to be directed to the correct device.

41. Having more than one DHCP server on the same subnet of a network is :

A.possible , if all server besides one are offline , so that the client requests for IP addresses only reach that server

This is a failover configuration, in case one DHCP server goes down, the other one will take over and provide IP addresses to clients.

B. possible, as long as they share the same address pool to give to the clients

When DHCP servers are not aware of each other, they can assign the same IP addresses to different clients. This can cause multiple clients to have the same IP address, leading to connectivity issues and unexpected behavior.
Additionally, DHCP servers can also assign duplicate IP addresses to the same client. This can cause conflicts, as the client would be unable to communicate with other devices on the network.
Having DHCP servers with different address pools can prevent this kind of IP address conflicts.

C. possible only if each of them has a different pool of addresses, without sharing any address

This can be done by configuring DHCP servers to use different address pools, so that each DHCP server is responsible for assigning IP addresses from a different range. This can prevent IP address conflicts and ensure DHCP service availability.

D. not possible

42. What is the main function of DNS?
A. maps a known IP address to a MAC layer address

The function of mapping an IP address to a MAC address is performed by the Address Resolution Protocol (ARP), not DNS.

B. provides host names to TCP/IP address resolution

The main function of DNS (Domain Name System) is to provide host names to IP address resolution. DNS is the system that translates human-friendly domain names (e.g. www.example.com) into the IP addresses (e.g. 192.0.2.1) that computers use to identify each other on the internet. When a client wants to access a website or other network resource, it sends a request to the DNS server to resolve the domain name to an IP address. The DNS server then looks up the IP address for the domain name in question and returns it to the client, allowing the client to establish a connection to the website or resource.

C. automatically assigns IP addresses to the devices across the network

DHCP(Dynamic Host Configuration Protocol) is the one that assigns IP addresses.

D. provides network connectivity to a computer

DNS is responsible for resolving domain names to IP addresses, not providing network connectivity.

43. Gateways are used for:
A. providing connectivity between two or more network segments

A gateway is a networking device that connects two or more separate networks together, allowing them to communicate with each other. Gateways are commonly used to connect different types of networks, such as a LAN (Local Area Network) to a WAN (Wide Area Network) or a LAN to the internet. They act as a bridge between the different networks, allowing devices on one network to communicate with devices on another network.

B. providing network connectivity to a computer

A gateway connects networks together.

C. tracing the route taken by data from the router to the destination network

This is the function of traceroute or tracert command.

D. transfer files between different platforms

This is the function of file transfer protocol (FTP) or other file transfer protocols.

*Class A: The first bit of the first octet is set to 0, the remaining 7 bits are used for the network address, and the remaining 24 bits are used for the host address. This means that Class A addresses can support up to **126 networks** (since the first and last network addresses are reserved) and up to **16,777,214 hosts per network.***

10.0.0.1, 20.1.2.3

*Class B: The first two bits of the first octet are set to 10, the remaining 14 bits are used for the network address, and the remaining 16 bits are used for the host address. This means that Class B addresses can support up to **16,384 networks** and up to **65,534 hosts per network.***

172.16.0.1, 128.2.3.4

*Class C: The first three bits of the first octet are set to 110, the remaining 21 bits are used for the network address, and the remaining 8 bits are used for the host address. This means that Class C addresses can support up to **2,097,152 networks** and up to **254 hosts per network.***

192.168.1.1, 223.255.254.253

44. What is the maximum number of hosts for a class C network ?
A. 65.534
B. 65.535
C. 128
D. 254

In IP addressing, the first three octets of an IP address are used to identify the network, and the last octet is used to identify individual hosts on that network. Class C networks use a 24-bit subnet mask, which means that the first three octets of the IP address are used to identify the network, and the last octet is used to identify individual hosts. Since the last octet can be any value from 1 to 255, this means that a class C network can have a maximum of 254 hosts.

45. What is the maximum number of networks in a class A network ?
A. 126
B. 128
C. 16,384
D. 254

46. Determine how many subnets are found in the above given network :
A. 7
B. 9
C. 5
D. 11

Private IP addresses are typically in the ranges of 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Any IP addresses outside of these ranges are likely to be public IP addresses.

IANA (Internet Assigned Numbers Authority) has also reserved certain subnet masks for private IP addresses, such as /8, /12, and /16. Any IP address with a subnet mask other than these is likely to be a public IP address.

47. Which one of the following addresses is a public IP address ?
A. 10.0.0.0/8
B. 207.46.130.0/24
C. 172.16.0.0/12
D. 1.0.0.0/8

1.0.0.0/8 is not a private IP address range, it is a public IP address range and it is assigned by the IANA for use on the public internet.

48. NAT is :
A. a connection between computers and other network devices that are located within a small physical location

NAT is not a connection between devices, it is a technique used by routers to map private IP addresses used on a local network to a single public IP address.

B. a protocol providing a way for multiple computers on a common network to share single connection to the Internet

NAT (Network Address Translation) is a technique used by routers to allow multiple devices on a local network to share a single public IP address and access the internet. NAT maps the private IP addresses used on the local network to a single public IP address, allowing the devices on the local network to communicate with devices on the public internet. This allows for the efficient use of IP addresses and provides an added layer of security by keeping the devices on the local network hidden from the public internet.

C. a protocol used by routers to send data from one network to another

NAT is a technique used by routers to map the private IP addresses used on a local network to a single public IP address, it is not a protocol used to send data between networks. It's important to note that routers use other protocols such as IP and ICMP to send data between networks.

D. a set of protocol layers designed to make data exchange possible on different types of computer networks

NAT is not a set of protocol layers, it is a technique used by routers to map private IP addresses used on a local network to a single public IP address.

49. Which one is not true about classless routing protocols :
A. RIPv1 supports classless routing protocols

RIP version 1 (RIPv1) is a classful routing protocol, meaning it does not support VLSMs or classless routing. It does not support the use of variable-length subnet masks, it uses a fixed-length subnet mask, and it does not allow the use of discontiguous networks. On the other hand, RIP version 2 (RIPv2) is a classless routing protocol, it supports the use of variable-length subnet masks and allows for the use of discontiguous networks.

B. RIPv2 supports classless routing protocols
C. It is allowed to a use a variable length mask
D. It is allowed to use discontiguous network

50. Which one of these is a RIPv2 characteristic ?
A. maintains a routing table as in RIPv1 without the mask information
B. is a classful routing protocol
C. supports maximum metric(hop count) value up to 15 . Any router further than 15 hops is considered unreachable

RIP version 2 (RIPv2) is an updated version of the Routing Information Protocol (RIP) routing protocol, which is a distance-vector routing protocol. One of the characteristics of RIPv2 is that it supports a maximum metric (hop count) value of 15, meaning that any router further than 15 hops is considered unreachable. Additionally, RIPv2 supports subnet masks, unlike RIPv1, which makes it a classless routing protocol, and it also supports triggered updates and authentication of update messages.

D. does not support triggered updates or authentication of ripv2 update messages

51. Which one is true about RIPv1?
A. It is easier to configure than RIPv2

RIP version 1 (RIPv1) is an older version of the Routing Information Protocol (RIP) routing protocol, which is a distance-vector routing protocol. One of the characteristics of RIPv1 is that it is considered to be easier to configure than RIPv2. Additionally, RIPv1 does not support subnet masks, unlike RIPv2, which makes it a classful routing protocol and it does not have mask information in its routing table. It has a higher administrative distance than RIPv2 and its timers are different from those of RIPv2.

B. It maintains a routing table as in RIPv2 , including mask information

RIPv2, on the other hand, is a classless routing protocol, which means it includes subnet mask information in its routing updates, allowing for more efficient use of IP addresses and support for VLSMs.

C. It has a lower administrative distance than RIPv2

RIPv1 has a default administrative distance of 120, while RIPv2 has a default administrative distance of 120 too.

D. It has the same timers ad RIPv2

RIPv1 uses a fixed update interval of 30 seconds and a fixed invalidation interval of 180 seconds. While RIPv2 uses configurable update and invalidation intervals.

52. An IP address is :
A. 64 bits
B. 32 bytes
C. 128 bytes
D. 32 bits

53. Which of the following are valid IP addresses to mark a sub network ?
A. 177.91.107.144/29

The IP address 177.91.107.144 with a subnet mask of 255.255.255.248 (or /29 in CIDR notation) creates a subnetwork that can contain 6 hosts.

B. 177.91.107.0/32

The IP address 177.91.107.0 with a subnet mask of 255.255.255.255 (or /32 in CIDR notation) creates a subnetwork that can contain only one host. This is not a valid subnet mask for subnetting.

C. 177.91.107.1/25

The IP address 177.91.107.1 with a subnet mask of 255.255.255.128 (or /25 in CIDR notation) creates a subnetwork that can contain 128 hosts.

D. 177.91.154.2/30

The IP address 177.91.154.2 with a subnet mask of 255.255.255.252 (or /30 in CIDR notation) creates a subnetwork that can contain 2 hosts.

54. What is the range of network IPs in which the following given IP resides :194.168.19.65/28 ?
A. 194.168.19.64 – 194.168.19.87
B. 194.168.19.64 – 194.168.19.79

The IP address 194.168.19.65 with a subnet mask of 255.255.255.240 (or /28 in CIDR notation) is in a network with a range of IP addresses from 194.168.19.64 to 194.168.19.79.
The /28 subnet mask allows for 14 valid host IP addresses. The network IP address in this case is 194.168.19.64 (the first IP address in the range) and the broadcast IP address is 194.168.19.79 (the last IP address in the range)

C. 194.167.19.62 – 194 .167.19.87
D. 194.168.19.0 - 194.168.19.64

55. Which of the following is the correct host range for the subnet in which we can find the IP address 192.168.168.188 255.255.255.192 ?
A. 192.168.168.129-191
B. 192.168.168.128-190
C. 192.168.168.128-192
D. 192.168.168.129-190

The network address (or subnet ID) is always the first IP address in the range, and the host addresses are the rest of the IP addresses in the range. In this case, the network address is 192.168.168.128, which cannot be assigned to a host, and the host addresses range from 192.168.168.129 to 192.168.168.190.

56. Which protocol does DHCP use at the Transport Layer ?
A. IP
B. UDP

DHCP (Dynamic Host Configuration Protocol) uses the User Datagram Protocol (UDP) at the Transport Layer.

C. TCP
D. ARP

57. Which class of IP address has the most host addresses available by default?
A. A

Class A IP addresses have a default subnet mask of 255.0.0.0, which means that the first 8 bits are used for the network address and the last 24 bits are used for the host address. This allows for 2^24 (16,777,214) - 2 = 16,777,214 host addresses to be available by default.
This is significantly more host addresses than Class B and Class C addresses, but they are intended for large networks with a large number of hosts.

B. B
C. C
D. A and C

58. Which protocol does Ping use?
A. TCP
B. ARP
C. ICMP

Ping uses the Internet Control Message Protocol (ICMP) at the Network Layer (Layer 3) of the OSI Model. ICMP is a protocol that allows a host to send error messages and operational information indicating success or failure when communicating with another IP address.
When you use the ping command, the host sends an ICMP Echo Request packet to the target host, the target host then sends an ICMP Echo Reply packet back to the source host. The ping utility uses these packets to determine if the target host is reachable and able to respond. The ping command is used to check connectivity and verify that a host is reachable on a network.

D. IP

59. Which of the following does not use TCP?
A. HTTP
B. DHCP
C. FTP
D. SMTP

60. Which of the following is a private IP address ?
A. 12.0.0.2
B. 168.172.19.40
C. 172.15.14.36
D. 192.168.24.43

A private IP address is an IP address that is not globally unique, but is unique within a private network. These IP addresses are typically used on internal networks and are not reachable from the internet.

The IP addresses that are reserved for use in private networks are:

Class A: 10.0.0.0 to 10.255.255.255
Class B: 172.16.0.0 to 172.31.255.255
Class C: 192.168.0.0 to 192.168.255.255

61. Which class of IP address provides a maximum of only 254 host addresses per network ID?
A. class A
B. class B
C. class C

A Class C IP address has a default subnet mask of 255.255.255.0, which means that the first 24 bits are used for the network address and the last 8 bits are used for the host address. This allows for 2^8 (256) - 2 = 254 host addresses to be available by default. This is fewer host addresses than Class A and Class B addresses, but they are intended for small to medium-sized networks.

Class A addresses have 8 bits available for host addresses which is 2^24-2 = 16,777,214 host addresses and Class B has 16 bits available which is 2^16-2 = 16,384 host addresses.

D. class B and C

62. Which one is true about ICMP packets ?
A. They are encapsulated within IP datagrams.

ICMP (Internet Control Message Protocol) is a network protocol that is used to send error messages and operational information indicating success or failure when communicating with another IP address. ICMP packets are encapsulated within IP datagrams and are sent as the payload of an IP datagram. This allows ICMP messages to be sent to and received from any host on an internetwork, regardless of the upper-layer protocol.
ICMP packets do not provide guarantee of delivery, they provide hosts with information about network problems.

B. ICMP is encapsulated within UDP datagrams.
no

C. They do not provide hosts with information about network problems.

ICMP does provide hosts with information about network problems

D. They guarantee datagram delivery.

63. Which of the following is considered to be the destination host before translation?
A. Inside local host

The inside local host is considered to be the destination host before translation. The Inside local host is the host on the inside of a network that is being translated to a different IP address, typically a public address, when it communicates with hosts on the outside of the network (outside local host).

B. Outside local host
C. Inside global host
D. Outside global host

64. Which of the following is considered to be the address after translation?
A. Inside local host
B. Outside local host
C. Inside global host

The Inside global host is the host on the inside of a network that has a globally routable IP address, which means that it can be directly accessed from the internet after the translation process occurred.

D. Outside global host

66. Which one of the following is not an advantage of using NAT?
A. Conserves legally registered addresses.

NAT conserves the use of IP addresses by allowing a single device, such as a router, to be used as an agent between the private network and the internet.

B. Translation introduces switching path delays

NAT introduces delays to the communication process because the router must perform the necessary translation before forwarding the packet to its destination. This is because the router needs to examine and update the IP header of each packet passing through it, which can introduce additional latency.

C. Increases flexibility when connecting to the Internet

NAT increases flexibility when connecting to the internet by allowing multiple private networks to use a single public IP address.

D. Reduces address overlap occurrence

67. Which one is true about NAT ?
A. Causes loss of end-to-end IP traceability

NAT causes loss of end-to-end IP traceability because the IP addresses of the hosts on the private network are replaced with the IP addresses from the NAT pool. This means that it is not possible to trace a connection back to the original host on the private network using the IP address.

B. Does not conserve legally registered addresses

NAT does conserve legally registered addresses, it allows a single device, such as a router, to be used as an agent between the private network and the internet, thus conserving the use of IP addresses.

C. Decreases flexibility when connecting to the Internet and certain applications will not function with NAT enabled

NAT increases flexibility when connecting to the internet by allowing multiple private networks to use a single public IP address. Certain applications that rely on end-to-end IP address preservation may not function with NAT enabled, but it's not decreasing the flexibility.

D. Increases address overlap occurrence

NAT reduces address overlap occurrences, which can occur when two or more private networks use the same IP address space.

68. Which of the following is true about the IP address 10.16.3.65/23?
A. The subnet address is 10.16.3.0 255.255.254.0
B. The last valid host address in the subnet is 10.16.2.254 255.255.254.0
C. The broadcast address of the subnet is 10.16.3.0 255.255.254.0
D. The lowest host address in the subnet is 10.16.2.1 255.255.254.0

69. Which of the following are valid subnet addresses ?
A. 177.91.107.0 ,177.92.107.97, 177.92.107.144
B. 177.91.107.0 , 1.0.0.0 , 0.0.0.0
C. 191.91.168.1 , 177.91.107.152, 177.91.168.127
D. 177.91.107.0 , 177.91.107.144, 1.0.0.112

An IP address can be divided into a network and host portion, and the network address is considered to be a subnet address. The subnet address is the first address in a range of IP addresses that have been divided into smaller networks, also called subnets.

70. What does a mask /28 mean?
A. the maximum number of IP addresses that can be assigned to hosts is 16
B. the maximum number of IP addresses that can be assigned to hosts is 14

The /28 subnet mask uses 28 bits for the network portion and 4 bits for the host portion of the IP address. This means that there are 14 IP addresses available in the network, including the network address and the broadcast address. (2^4 - 2)

C. the maximum number of IP addresses that can be assigned to hosts is 8
D. the maximum number of IP addresses that can be assigned to hosts is 30

71. A submask /30 can be given to:
A. a subnet with 3 PC's, connected to a router by a switch
B. a subnet with 2 PC's and a Server , connected to a router by a switch
C. a subnet with 2 PC's connected directly to the router
D. a subnet with 2 routers connected

A subnet mask of /30 uses 2 bits for the host portion of the IP address and 30 bits for the network portion. This means that there are only 2 IP addresses available in the network, including the network address and the broadcast address.

This subnet mask is commonly used in point-to-point networking where only two devices are connected, such as a router-to-router link, or a router-to-switch link. In such a scenario, one IP address is assigned to one device and the other IP address is assigned to the other device.

It's worth noting that, with a /30 subnet mask, the first and last addresses are reserved and cannot be assigned to hosts. The first address is the network address and the last address is the broadcast address. With a /30 subnet mask there are only 2 assignable IP addresses available.

72. You need to subnet a network that has 7 subnets, each with at least 16 hosts. Which classful subnet mask would you use?
A. 255.255.255.192
/26 also good

B. 255.255.255.224

/28 -> 2^4 - 2 -> 14 hosts (< 16)
/27 -> 2^5 - 2 -> 30 hosts (> 16)
/27 = 255.255.255.224
([255][255][255][2^7 + 2^6 + 2^ 5 + 0 + 0000])
8 + 8 + 8 + 3 = 27

C. 255.255.255.240
/28 - not enough hosts

D. 255.255.255.252
/29 - *not enough hosts*

73. You have an interface on a router with the IP address of 192.168.192.10/29. Including the router interface, how many hosts can have IP addresses on the LAN attached to the router interface?
A. 6
A subnet mask of /29 uses 3 bits for the host portion of the IP address and 29 bits for the network portion. This means that there are 6 IP addresses available in the network, excluding the network address and the broadcast address.

3^2 - 2 = 6.

B. 7
C. 8 D. 14

74. The network address of 172.16.0.0/19 provides how many subnets and hosts?
A. 7 subnets, 30 hosts each
B. 8 subnets, 8,190 hosts each

*172.16.[**000**0 0000].[0000 0000]*
3 zeros under the mask -> 2^3 = 8 subnets
13 zeros for hosting -> 2^13 - 2 = 8190 hosts (each)

C. 8 subnets, 2,046 hosts each
D. 7 subnets, 2,046 hosts each

76. Which of the following affirmations about UDP is not true ?
A. Writes packets of bytes

it is a packet-based protocol that sends packets of bytes to the destination.

B. No read bytes from a packet are lost

UDP (User Datagram Protocol) is a connectionless, unreliable transport protocol. It does not guarantee that packets will be delivered to the destination and does not guarantee that packets will be received in the order they were sent. Therefore, it's possible that some packets may be lost or dropped along the way, and some bytes from a packet may be lost or not received.

C. Neither party can overflow the other. Traffic is controlled by the OS

In UDP, there is no flow control mechanism to ensure that the receiver is able to handle the incoming traffic. Therefore, if the sender is sending data faster than the receiver can handle it, the receiver may become overwhelmed and drop packets, this is known as buffer overflow.

While the operating system does play a role in managing network traffic, it does not prevent buffer overflow from occurring in UDP.

77. Which one is not a principle to the OSI model?
A. A layer should be created where a different abstraction is needed.

Each layer of the OSI model provides a different level of abstraction, or a different way of thinking about the data being transmitted. This allows the different layers to perform their specific functions while still working together to achieve the overall goal of communication.

B. Each layer should perform a well-defined function.

Each layer in the OSI model is responsible for performing a specific set of functions that contribute to the overall process of communication.

C. The layer boundaries should be chosen to maximize the information flow across the interfaces.

The OSI model is designed to minimize the amount of information that needs to be passed between layers, in order to maximize the efficiency of communication.

D. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

The OSI model is designed to be a standardized framework that can be used to develop communication protocols that are compatible with different types of devices and networks.

The OSI model is divided into 7 layers:

1. *Physical Layer: It is responsible for the physical connection between devices.*
2. *Data Link Layer: It is responsible for maintaining the link between devices and ensuring that data is transmitted error-free.*
3. *Network Layer: It is responsible for routing data between different networks*
4. *Transport Layer: It is responsible for ensuring that data is delivered reliably and in the correct order.*
5. *Session Layer: It is responsible for managing the sessions between devices.*
6. *Presentation Layer: It is responsible for converting data into a format that can be understood by the application layer.*
7. *Application Layer: It is responsible for providing services to the user.*

78. Which of the following layers, controls the operation of a subnet and handles how packets are routed from source to destination ?

A. The Network Layer

The Network Layer is the third layer of the OSI model and it is responsible for routing data between different networks. It is responsible for controlling the operation of a subnet and for handling the delivery of packets from the source to the destination.

The Network Layer uses logical addressing (IP addresses) to route packets to the correct destination. It also uses routing tables and protocols to determine the best path for data to travel from the source to the destination.

B. The Transport Layer
C. The Session Layer
D. The Presentation Layer

79. Which protocol handles mail exchange?
A. FTP *(File Transfer Protocol)*
B. TELNET

(Teletype Network) is a protocol that allows a user to connect to a remote host and interact with it as if the user were physically present at the host. It is a terminal emulation protocol, which means it allows a user to use a local computer or device to access and control a remote host as if they were using the host's own terminal.

C. SSH *(Secure Shell)*

D. SMTP

SMTP (Simple Mail Transfer Protocol) is a protocol for sending email messages between servers. Most email systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an email client using either POP or IMAP.

80. Which one of the following is a Natural Mask?
A. 255.255.255.255
B. 255.255.255.0

In IP networking, a natural mask is a subnet mask that corresponds to the class of an IP address. For example, Class A IP addresses have a default subnet mask of 255.0.0.0, Class B IP addresses have a default subnet mask of 255.255.0.0, and Class C IP addresses have a default subnet mask of 255.255.255.0.

In this case, 255.255.255.0 is the natural mask for a class C IP address.

C. 255.255.255.128
D. 255.255.255.64

81. IP - best effort protocol - does its best effort to transfort datagram from one machine to another with no guarantee of an
A. Successful delivery
B. Duplication/Unicity
C. Data integrity
D. All of the above

82. Which affirmation is not true about The Network Address Translation:
A. No need to be allocated range of addresses from ISP:- just one IP address is used for all devices
B. Can change addresses of devices in local network without notifying outside world
C. Can change ISP only by changing addresses of devices in local network

NAT does not change the ISP (Internet Service Provider) of a device. It is a function that is typically performed by a router on a local network, and it is used to allow devices on the local network to access the internet using a single public IP address that is assigned to the router by the ISP.

NAT does not change the address of the devices on the local network, it only changes the source IP address of the packets leaving the local network. The devices on the local network still use the private IP addresses assigned to them by the administrator, but when they try to access the internet, the router translates those private IP addresses to the public IP address assigned to it by the ISP.

D. devices inside local net not explicitly addressable, visible by outside world

83. Which of the following affirmations about TCP is not true?
A. Client process must first be running

In a typical scenario, a server process will be running on a host and listening for incoming connections. The client process, on the other hand, can start at any time and initiate a connection to the server.

So, it's not necessary for the client process to be running before the server process, the client can initiate a connection to a server at any time, as long as the server is running and listening for incoming connections.

B. Server must have created socket that welcomes clientís contact
C. Allows server to talk with multiple clients
D. Source port numbers are used to distinguish clients

84. IP Routing is based on the:
A. Source IP
B. Destination IP

IP routing is the process of forwarding a packet to its destination based on the destination IP address. The router uses the routing table, which is a database that contains information about the networks a router is connected to, and the routing protocols to determine the best path for a packet to take to reach its destination.

When a packet arrives at a router, the router examines the destination IP address in the packet's header, and then compares it to the entries in its routing table. If the router finds a match, it uses the information in the entry to determine the next hop for the packet and forwards the packet to the next hop.

C. Network Address
D. Broadcast Address

85. Which is not a Service of a Data Link Layer?
A. Framing and link access
B. Flow Control
C. Error Correction
D. Traffic isolation

Traffic isolation is a service provided by Network Layer, it's responsible for providing a logical separation of different networks and subnetworks.

86. What are the protocols involved in sending an email?
A. FTP
B. SMTP
C. TCP

The email protocols, SMTP, POP, and IMAP, are built on top of the Transmission Control Protocol (TCP) as part of the TCP/IP protocol stack.

D. POP3
E. HTTP

HTTP is a protocol used for transferring data over the internet, mainly used for web pages and other related web-based applications. It's the foundation of the World Wide Web and it's used for requesting and receiving data from web servers.

SMTP, POP, IMAP, DNS and MIME are the main protocols used to send an email, they are specific for email communication and work together to ensure that the message is delivered to the correct recipient. ***(totuși)*** *HTTPS (HTTP Secure) which is a combination of HTTP and SSL/TLS protocol may be used to access web-based email services such as Gmail or Yahoo Mail.*

87. TCP stands for...
A. Transfer Control Protocol
B. Transmission Connection Protocol
C. Transformation Central Protocol
D. Transmission Control Protocol

88. What is a datagram?
A. A structure used to get data from the user in order to synchronize the server
B. A basic transfer unit used in packet-switched networks, providing a connectionless comunnication service

Datagrams are used in connectionless protocols such as the User Datagram Protocol (UDP), where each datagram is sent and received independently of any other datagrams. In contrast, in a connection-oriented protocol such as the Transmission Control Protocol (TCP), a virtual circuit is established between the sender and the receiver and all data is sent as a stream, rather than as individual datagrams.

C. Information that can harm your computer if you're not careful with it
D. Millions of bytes configured in a big cluster which can be easily transferred