CompTIA Network+ (N10-009) - Quiz Questions with Answers

1.0 Networking Concepts

1.0 Networking Concepts

1.

Which of the following BEST describes a network?

A group of interconnected computers

A switch with multiple ports

A connection between a router and a host

Two or more servers

Correct answer: A group of interconnected computers

A network is a group of interconnected computers. Standalone devices are not part of a network until they are connected in some way.

A switch with multiple ports would only be part of a network if it was properly connected.

A router connected to a single host would not constitute a network in the accepted sense. The host would need to connect to another device.

Two or more servers would not constitute a network unless connected to client devices.

2.

The 802.11n wireless standard offers a maximum speed of which of the following?

300 Mbps

1 Gbps

54 Mbps

11 Mbps

Correct answer: 300 Mbps

The wireless standard 802.11n operates on both 2.4 GHz and 5 GHz bands, providing versatility as well as maximum throughput. The maximum speed for 802.11n is upwards of 300 Mbps, especially when using the more powerful 5 GHz band.

The maximum speed for IEEE 801.11ac is 1 Gbps.

The maximum speed for 802.11a and 802.11g is 54 Mbps.

The maximum speed for 802.11b is 11 Mbps.

3.

Which of the following is one of the three PRIMARY functions of a switch?

Address learning

MAC synchronization

Routing

Filtering

Correct answer: Address learning

As switches operate, they memorize the MAC addresses of all the devices they interface with. This data is stored in a forward/filter table which is initially empty until the switch is used, allowing it to collect and remember the MAC addresses.

MAC synchronization involves ensuring that devices have the same MAC address table to improve performance and reduce broadcasts. While switches forward traffic based on MAC addresses and populate this table, this is not one of the primary functions of a switch. Routing is performed at layer 3, while switches operate at layer 2. Filtering is typically performed based on IP addresses and content, which is also higher on the OSI model.

4.

A user has plugged an Ethernet cable into the Network Interface Card (NIC) of their computer. At which level of the Open Systems Interconnection (OSI) model does a NIC operate?

Layer 2

Layer 3

Layer 5

Layer 7

Correct answer: Layer 2

A Network Interface Card (NIC) physically connects to wires, but it also works with MAC addresses, which are located at Layer 2, the data link layer of the OSI model. This makes it a Layer 2 system. Layer 2 handles such things as media access control and error checking.

Layer 3 is the network (or packet) layer, which deals with message forwarding and IP addressing. The session layer, or layer 5, sets up, manages, and breaks down sessions between devices. Users are most familiar with layer 7, the application layer, where their favorite email and browser programs reside.

5.

Which of the following specifications identifies the cable television frequencies used for data transmission?

DOCSIS

HFC

DSLAM

TDM

Correct answer: DOCSIS

The Data-Over-Cable Service Interface Specification (DOCSIS) identifies the frequencies dedicated to data transmission and handling.

A Hybrid Fiber-Coaxial (HFC) network is how cable companies provide high-speed transmission to specific locations before it is broken down into a slower-speed coaxial configuration. A DSL Access Multiplexer (DSLAM) is a device that terminates multiple DSL connections from customers. Time Division Multiplexing (TDM) is a technology that enables multiple transmissions to share the same medium.

6.

Of the following, which is used to retrieve email from an email server on port 110?

POP3

IMAP4

TLS

SSL

Correct answer: POP3

The Post Office Protocol version 3 (POP3) is used to retrieve and download email from an email server. It downloads the complete message and removes it from the server.

POP3 differs from Internet Message Access Protocol version 4 (IMAP4) primarily by how it operates and by the port it operates on. IMAP4 provides greater control over messages, along with enhanced security.

Transport Layer Security (TLS) and Secure Socket Layer (SSL) are both encryption and security protocols not used for email.

7.

Which of the following is NOT a common component of a zero-trust security strategy?

Separation of duties

Network segmentation

Least privilege

Strong user authentication

Correct answer: Separation of duties

Separation of duties is designed to protect against fraud by separating processes into multiple tasks assigned to different employees. It is not a concept related to a zero-trust architecture.

Network segmentation, least privilege, and strong user authentication are all parts of a zero-trust security strategy, which limits users to only the permissions needed to do their jobs.

Network segmentation involves dividing the network into smaller, isolated segments. It prevents lateral movement through the corporate network.

Authentication proves the user's identity. Policy-based authentication uses rules to manage authentication processes.

The principle of least privilege restricts a user's access to only those resources needed to do their job.

8.

You are working as an engineer on a network design project. Your colleague recommends choosing a ring network topology. Of the following, which is a trait of ring networks?

Complicated and hard to reconfigure

Simple and easy to reconfigure

Easy to troubleshoot

One station fails but does not cause the entire network to fail

Correct answer: Complicated and hard to reconfigure

Since each system must relay a token to another, any failures take down the entire network. If this happens, it can be difficult to determine which one is causing the fault in the network. Thus, ring networks are complicated and hard to reconfigure.

None of the other statements about a ring topology would be true. It is not necessarily easy and simple to reconfigure or troubleshoot. Any node on a ring network could be a Single Point Of Failure (SPOF), potentially losing connectivity along the entire network.

9.

Which of the following are the frequency band and maximum bandwidth values for 802.11a?

5 GHz, 54 Mbps

2.4 GHz, 54 Mbps

2.4 GHz, 11 Mbps

5 GHz, 11 Mbps

Correct answer: 5 GHz, 54 Mbps

The frequency bands and maximum bandwidth values of wireless standards are as follows:

- *802.11a: 5 GHz, 54 Mbps*
- *802.11b: 2.4 GHz, 11 Mbps*
- *802.11g: 2.4 GHz, 54 Mbps*
- *802.11n: 2.4 and 5 GHz, >300 Mbps*
- *802.11ac: 5 GHz, >3 Gbps*
- *802.11ax: 2.4, 5, and 6 GHz, 9.6 Gbps*

10.

Which of the following is a layer 2 device?

Switch

Router

Hub

Firewall

Correct answer: Switch

Layer 2 is the Data Link Layer, which uses MAC addresses to route traffic. Switches are designed to translate IP addresses to MAC addresses and route traffic to the various devices on a subnet or outside of the subnet.

A router is a Layer 3 device, encapsulating data link frames and forwarding IP packets.

A hub is a Layer 1 (physical layer) device. Unlike a switch, a hub is essentially a repeater and does not forward frames based on MAC addresses.

A firewall security device can operate at multiple OSI layers, including 3, 4, and 7.

11.

IEEE 802.11ax extends Wi-Fi into which frequency range?

6 GHz

5 GHz

3 GHz

2 GHz

Correct answer: 6 GHz

IEEE 802.11ax or Wi-Fi 6 extends into the 6 GHz frequency band.

Wireless LAN (WLAN) standards are defined in IEEE 802.11.

12.

You are evaluating different options for data storage. One option you have exposes a pool of hard disks to clients over the network as one or more logical disks. Which type of data storage is being described?

SAN

NAS

SDN

NGFW

Correct answer: SAN

A Storage Area Network (SAN) makes a pool of hard disks accessible to client machines over the network. The SAN can pretend to be one or more logical hard disks and enables clients to read and write blocks of data to these disks.

Network Attached Storage (NAS) provides centralized file storage for clients on the network. It has its own built-in file system and is built specifically for file management with dedicated hardware and software.

SDN stands for Software-Defined Networking and is not a type of data storage.

NGFW stands for Next-Generation Firewall and is not a type of data storage.

13.

How many collision domains does a switch with 12 ports have?

12

6

2

1

Correct answer: 12

A switch, by design, will make each of its ports a unique, singular collision domain. This enables a switch to segment each port so that collisions are nonexistent due to each node communication being on its own personal collision domain. This network still falls under one broadcast domain as routers connect broadcast domains.

The answers 6, 2, and 1 are incorrect.

14.

Which of the following terms is often considered synonymous with 4G?

LTE

CDMA

HSPA+

TDMA

Correct answer: LTE

Long-Term Evolution (LTE) is a standard used in fourth-generation (4G) cellular networks, and the terms are often used interchangeably. 4G has been an evolving standard with many implementations, but it's now being replaced by 5G in many locations. 4G/LTE and 5G networks use Orthogonal Frequency Division Multiple Access (OFDMA), which is an advanced combination of Frequency-Division Multiple Access (FDMA) and Time-Division Multiple Access (TDMA).

Code Division Multiple Access (CDMA) is used by 2G and 3G networks, which have served as backup to 4G networks for some carriers.

High-Speed Packet Access Plus (HSPA+) was released in 2008 as part of Wideband Code Division Multiple Access (WCDMA) in 3G networks.

The Global System for Mobile Communications (GSM) is a 2G network that uses Time-Division Multiplexing (TDMA) to allow multiple users to share the same channel.

15.

What virtual service stores user data and the desktop GUI in a central server, as compared to the hard drive on a user's computer?

Virtual desktop

Virtual PBX

Virtual switch

Virtual server

Correct answer: Virtual desktop

A virtual desktop stores user data and the desktop GUI in a central server rather than on the user's local machine.

A virtual private branch exchange (PBX) is usually a Voice-over Internet Protocol (VoIP) solution, where voice is encapsulated inside data packets for transmission across a data network. Virtual switches provide layer 2 control for co-resident virtual machines on the same server, enabling the use of VLANs. A virtual server allows multiple virtual machines (potentially with different operating systems) to reside on the same physical server.

16.

Of the following, which provides interconnection between Wireless Local Area Network (WLAN) and wired LAN?

AP

RSSI

RFI

CSMA/CA

Correct answer: AP

An Access Point (AP) connects to a wired Local Area Network (LAN) and generates a Wireless Local Area Network (WLAN).

The Received Signal Strength Indicator (RSSI) is a measure of the strength of a wireless signal. Signal strength can drop with distance or due to objects blocking line-of-sight signal transmission. WLANs may tune their transmission rates based on RSSI.

Radio Frequency Interference (RFI) can disrupt wireless networks. For example, some cordless phones, microwaves, and other devices use the 2.4 GHz spectrum, which can cause interference with Wi-Fi networks using this spectrum.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) introduces random delays before sending data to avoid collisions. This can increase latency in a WLAN.

17.

A network administrator is working to determine a solution for providing various large data files, such as meeting recordings, training materials, and call recordings, to the remote branches that have slower connections. Which of the following would alleviate the issue?

Content caching

Client-to-site VPN

Hardware redundancy

Load balancing

Correct answer: Content caching

Content caching helps to improve performance and reduce load on backend servers when serving data to geographically-distributed clients. A copy of data is "cached" on a server, which provides it to local clients. The backend server only needs to serve content to the remote servers, and users have the benefit of lower latency because they are served content by a nearby server rather than the remote backend server. In a Content Delivery Network (CDN), edge servers act as caching servers to deliver content faster and more efficiently.

A Virtual Private Network (VPN) creates an encrypted tunnel for data to travel through, which would not solve bandwidth issues. A client-to-site VPN would not alleviate a slow connection.

Hardware redundancy uses multiple copies of IT infrastructure to protect against outages.

Load balancing uses multiple servers to respond to requests, but the server is not the problem in this case.

18.

A crossover cable would be used to connect which of the following?

Switch to a switch

Router to a switch

Host to a switch

Host to a hub

Correct answer: Switch to a switch

A crossover cable is used to connect the following:

- *Switch to switch*
- *Hub to hub*
- *Hub to switch*
- *Host to host*
- *Router direct to host*

A straight-though cable is used to connect a router to a switch, a host to a switch, or a host to a hub.

19.

Dynamic Frequency Selection (DFS) was introduced to prevent interference with radar signals operating in which band?

5 GHz

5 MHz

2.4 GHz

2.4 MHz

Correct answer: 5 GHz

The 5GHz Wi-Fi band can also be used by some radar signals. Dynamic Frequency Selection (DFS) monitors for radar signals and will not use frequency bands that could interfere with them.

Wireless Local Area Network (WLAN) standards are described in 802.11. None of these standards correspond to 5 MHz or 2.4 MHz. IEEE 802.11b and 802.11g are both 2.4 GHz standards.

20.

An application is performing a query to a database. Which of the following ports is it LEAST LIKELY to be using?

3389

1433

1521

3306

Correct answer: 3389

Port 3389 is used by the Remote Desktop Protocol (RDP). Querying is a function of databases, and RDP does not necessarily involve a database like the other three answers. Using a port associated with a database would be more likely.

Ports 1433, 1521, and 3306 are all used by various databases.

Port 1433 is the default port for the Structured Query Language (SQL) server.

Port 1521 is used by the Oracle database.

Port 3306 is used by MySQL.

21.

What is 126.255.255.255 interpreted as?

All hosts on the 126 network

Any host outside of the 126 network

The external address for the 126 network

The gateway host of the 126 network

Correct answer: All hosts on the 126 network

A packet sent to the address 126.255.255.255 would subsequently be sent out to every host on the network. An IP address with 255 at the end would normally be considered a broadcast address.

A packet sent to 126.0.0.0 would be sent to any host on the network. A gateway host for the 126 network would typically be 126.0.0.1, meaning data would be sent to this address if a specified address wasn't found on the network. External addresses are part of Network Address Translation (NAT), and any IP address could be the external address of a computer or network.

22.

Which of the following enables Ethernet nodes to detect if data was damaged during transit?

Frame check sequence

Half-duplex mode

Start of frame delimiter

Frame error flag

Correct answer: Frame check sequence

Before transmitting data, the sender calculates a Cyclic Redundancy Check (CRC) value for it, creating a frame check sequence field in the Ethernet frame that allows the recipient to determine if the data has been damaged in transit.

Half-duplex mode allows bidirectional traffic but only in one direction at a time.

The Start Of Frame (SOF) delimiter is a 1-byte field that indicates the end of the preamble in an Ethernet frame.

Frame error flag is a fabricated term.

23.

Of the following, which is the BEST option for remote locations that have limited Wide Area Network (WAN) connectivity choices?

Satellite

HSPA+

LTE

Radio

Correct answer: Satellite

Many types of Wide Area Network (WAN) connectivity, such as Digital Subscriber Lines (DSLs) and cable modems, are not available in remote areas. Satellite internet provides connectivity in these areas by bouncing traffic off a satellite to a ground station connected to wired networks.

Evolved High-Speed Packet Access (HSPA+) is a mobile communications technology that may not be as available as satellite for remote locations.

Long-Term Evolution (LTE) is a form of 4G cellular technology.

Radio is not considered a wide area network service.

24.

What is the term that describes private, dedicated domains on each port of a switch?

Collision domains

Broadcast domains

Anycast domains

IP domains

Correct answer: Collision domains

Every port on a switch has its own collision domain, which protects the data from being corrupted by simultaneous transmissions by multiple devices.

A broadcast domain includes all devices on a LAN segment or bridged to other LAN segments that can be reached by a broadcast. Broadcast domains can be divided by routers or VLANs.

Anycast is used in IPv6 and is similar to broadcast in IPv4.

IP domains operate at layer 3, the network layer, while collision domains operate at layer 2, the data link layer.

25.

After traveling partway to its destination, a packet is dropped. What is the MOST LIKELY cause?

TTL exhaustion

Invalid MAC address

Invalid IP address

Invalid port numbers

Correct answer: TTL exhaustion

A packet's Time To Live (TTL) defines the maximum number of hops that it can take to reach its destination. If the TTL is exhausted because the distance is too far, the packet will be dropped.

If the MAC address, IP address, or port number is incorrect, a packet is likely to go to the wrong place. An invalid IP address (i.e., one that doesn't fit the format) is unlikely to be sent at all.

26.

How do rates of data transfer on Ethernet compare to Wi-Fi?

Higher

Smaller

Slower

Less reliable

Correct answer: Higher

Wired Ethernet speeds can reach up to 40 Gbps, whereas wireless speeds at their current level can only reach a rate of about 2 Gbps. Wi-Fi 7 promises higher theoretical speeds, but they remain limited because of current implementations.

Data transfer rates would be neither smaller nor slower with Ethernet compared to Wi-Fi.

Ethernet is generally more stable and reliable for data transfer than Wi-Fi.

27.

According to the IEEE 802.3 standard, what is the MINIMUM length of an Ethernet frame?

64 octets

64 bits

1500 bits

1500 octets

Correct answer: 64 octets

The minimum length of an Ethernet frame is 64 octets. An octet is a series of eight bits, also known as a byte. Frames smaller than this are referred to as runts and are often caused by collisions or issues with network cards.

The 802.3 Ethernet frame includes the following allocation of 64 bytes as a minimum:

- *Destination MAC address - 6 bytes*
- *Source MAC address - 6 bytes*
- *Ethertype or length - 2 bytes*
- *Payload - 46 bytes (up to 1500)*
- *Frame check sequence - 4 bytes*

The answers 64 bits, 1500 bits, and 1500 octets are incorrect.

28.

Which Registered Jack (RJ) connector has two wire pairs?

RJ-11

RJ-12

RJ-45

RJ-48c

Correct answer: RJ-11

RJ-11 connectors have two wire pairs.

RJ-12 has three pairs, and RJ-45 and RJ-48c have four pairs.

29.

An RJ45 modular plug has how many pins?

Eight

Six

Four

16

Correct answer: Eight

An RJ45 modular plug has eight pins. Following the T565B standard, the wire colors are in this order:

- *Pin 1 - White/Orange*
- *Pin 2 - Orange*
- *Pin 3 - White/Green*
- *Pin 4 - Blue*
- *Pin 5 - White/Blue*
- *Pin 6 - Green*
- *Pin 7 - White/Brown*
- *Pin 8 - Brown*

30.

An e-commerce company is concerned about sudden surges of traffic to its sites during Black Friday sales. Which of the following cloud features would be the MOST beneficial to them?

Elasticity

Scalability

Flexibility

Agility

Correct answer: Elasticity

Elasticity refers to the cloud's ability to automatically scale up rapidly to meet sudden surges in demand, which would be useful in this case.

Scalability refers to the ability to support more long-term growth, such as when a company grows or shifts more services to the cloud. Scalability generally refers to planned, manual changes, while elasticity refers to the capacity for automatic and dynamic allocation of resources.

Flexibility in cloud computing is a more general term, referring to the ability to adapt to changing business needs quickly. Flexibility can encompass many areas, such as scalability, agile development, and real-time processing.

Agility in cloud computing involves the capability to rapidly develop, test, and deploy applications.

31.

An engineer is looking for a crossover cable to connect a switch to a switch. The engineer will be able to tell that it's a crossover cable when looking at it because the wires connect to which pins on each end?

Opposite

Same

Rolled-over

Straight-through

Correct answer: Opposite

A crossover cable is used to connect a switch to a switch, a hub to a hub, and a host to a host, as well as others. When creating crossover cables, it's important to remember that the pins do not match on either side of the connection with several pins crossed. Instead of showing 1 to 1 and 2 to 2 like on a straight cable, the four wires on the crossover cable are crossed to show the following matchup on the ends:

- *1 to 3*
- *2 to 6*
- *3 to 1*
- *6 to 2*

If the pins were the same on both ends, it would be a straight-through cable.

A rollover cable uses eight wires to connect a Telecommunications Industry Association and Electronic Industries Alliance (TIA-EIA) 232 interface to a router console com port.

A straight-through cable shows the same pins on both ends.

32.

In the EIA/TIA 568B wiring standard, what is the fifth pin color?

White/Blue

Green

Blue

White/Brown

Correct answer: White/Blue

The pinout for the EIA/TIA 568B standard is as follows:

- *Pin 1 - White/Orange*
- *Pin 2 - Orange*
- *Pin 3 - White/Green*
- *Pin 4 - Blue*
- *Pin 5 - White/Blue*
- *Pin 6 - Green*
- *Pin 7 - White/Brown*
- *Pin 8 - Brown*

33.

Of the following, which technologies operate on the session layer of the Open Systems Interconnection (OSI) model?

RPC

HTTP

TCP

DNS

Correct answer: RPC

The Remote Procedure Call (RPC) involves a computer program calling a subroutine to reach out to another resource (computer) on the network for procedure execution. In this way, the RPC protocol creates and breaks down sessions between computers, thus operating on Layer 5.

Hypertext Transfer Protocol (HTTP) is an application layer protocol used to transfer information between computers. It is commonly used in web browsers. Transmission Control Protocol (TCP) is a transport layer protocol used to ensure the reliable transmission of network data. Domain Name System (DNS) works at the application layer, handling the domains that we use in browsing web traffic.

34.

Translate the following binary IP address:

11000000.10101000.00000001.00000001

192.168.1.1

192.168.1.2

192.168.1.0

10.0.1.1

Correct answer: 192.168.1.1

To convert the binary to decimal, each position of the ones needs to be added. By taking each position of the one, and then referring to the chart below, you can add the values together to get the full binary address for each octet, which leads to the full Internet Protocol (IP) address.

Using the first octet (192) as an example, you can determine whether the full binary address equals 192.168.1.1 by using the values below.

The first octet 11000000 (192) would be the equivalent of 10000000 (128) plus 01000000 (64). 128 + 64 = 192. You can do the same binary to decimal conversion with the rest of the address.

Binary Value	***Decimal Value***
00000001	*1*
00000010	*2*
00000100	*4*
00001000	*8*
00010000	*16*
00100000	*32*
01000000	*64*
10000000	*128*

35.

Which of the following is NOT an advantage of Fibre Channel over iSCSI?

Better scalability

Lower latency

Higher performance

Greater reliability

Correct answer: Better scalability

Both Fibre Channel and Internet Small Computer System Interface (iSCSI) are used for Storage Area Networks (SAN). Fibre Channel has become more prevalent than iSCSI, but iSCSI remains a more scalable solution that is cheaper and easier to implement. Since iSCSI is based on Ethernet networks, it is more scalable using standard networking devices. Fibre Channel does not use Ethernet, but it can be configured for it using Fibre Channel over Ethernet (FCoE).

Compared to iSCSI, Fibre Channel offers:

- *Lower latency*
- *Higher performance*
- *Greater reliability*

36.

What is the LOWEST OSI layer that a router can operate at?

3

2

4

1

Correct answer: 3

A router can operate at the Open Systems Interconnection (OSI) model Layers 3 and above. This is because it performs routing based on Internet Protocol (IP) addresses, which exist at Layer 3. Routers forward and manage IP packets, which encapsulate Protocol Data Units (PDUs) from the higher layers. Routers may forward Virtual Local Area Network (VLAN) traffic from switches, but they are still operating at layer 3 when they do this.

Layer 2 is the OSI layer for switches and bridges.

Firewalls, load balancers, and gateways operate at Layer 4.

Equipment and cabling operate at Layer 1.

The seven layers of the OSI model are:

- *Layer 7 - Application*
- *Layer 6 - Presentation*
- *Layer 5 - Session*
- *Layer 4 - Transport*
- *Layer 3 - Network*
- *Layer 2 - Data link*
- *Layer 1 - Physical*

37.

What port is commonly used by the Secure File Transfer Protocol (SFTP)?

[✓ **22**]

20

21

23

Correct answer: 22

Secure File Transfer Protocol (SFTP) uses Secure Shell (SSH) to transfer data, so it provides a secure platform. By design, File Transfer Protocol (FTP) does not encrypt or protect the credentials used to log in, so it's incredibly insecure. To counteract this, SFTP is used. It operates on Transmission Control Protocol (TCP) port 22.

Ports 20 and 21 are used by FTP.

Port 23 is used by telnet and insecure remote access protocol.

38.

Of the following, which is a characteristic of IP addresses?

They are considered logical addresses

They are technically physical addresses

They can be found on the Network Interface Card (NIC)

They cannot be determined by an "ipconfig/all" command

Correct answer: They are considered logical addresses

An IP address is a logical address.

The physical address is a Media Access Control (MAC) address, and MAC addresses are those found on the Network Interface Card (NIC).

Both MAC and IP addresses can be located via the "ipconfig/all" command.

39.

Which of the following controls inbound and outbound traffic to a virtual machine in a VPC?

Security group

ACL

WAF

Network firewall

Correct answer: Security group

Security groups are used to control inbound and outbound traffic to resources in a Virtual Private Cloud (VPC), such as virtual machines.

A VPC security group acts as a virtual firewall at the resource level, while Access Control Lists (ACLs) apply controls at the subnet level.

A Web Application Firewall (WAF) applies security controls to applications on Layer 7.

A cloud network firewall is a more comprehensive tool, filtering traffic from multiple sources across the cloud infrastructure.

40.

Which of the following Quality of Service (QoS) concepts allows you to control the flow of packets into and out of the network according to the type of packet or similar rules?

Traffic shaping

Traffic sharing

Neighbor discovery

Port bonding

Correct answer: Traffic shaping

Traffic shaping can be used to implement Quality of Service (QoS) on advanced routers and switches. Traffic shaping is a bandwidth management process in which the flow of packets into and out of the network is controlled based on the type of packet or other rules.

Traffic sharing is a fabricated term.

Neighbor discovery protocol is used by Internet Protocol version 6 (IPv6) for Stateless Address Autoconfiguration (SLAAC) and IP address resolution.

Port bonding is the aggregation of multiple interfaces into a single logical interface.

41.

Which of the following quality of service mechanisms marks packets to impact the behavior of traffic?

DiffServ

IntServ

Best Effort

Applied Priority

Correct answer: DiffServ

Differentiated services (DiffServ) mark packets enabling different traffic flows to be treated in different ways. Quality of Service (QoS) is all about prioritizing network traffic. Many QoS approaches are based on DiffServ. QoS deals with problems such as dropped packets, delay, jitter, and errors. You can learn more about differentiated services in IETF RFC 7657, among others.

The three main models for QoS are diffserv, intserv, and best effort. Intserv includes the explicit reservation of resources to manage traffic flow. This method is much more labor-intensive and is not highly scalable. Best effort is the default QoS model. It just means that there is no implementation of any traffic control mechanisms and there is no special treatment for any types of traffic. Applied priority has to do with the classification of network traffic by type and destination to give some traffic higher priority.

42.

How many antennas are included in Wi-Fi 6?

8

4

16

6

Correct answer: 8

Wi-Fi 6 includes MU-MIMO 8x8. This means that it uses Multi-User, Multiple Input, Multiple Output (MU-MIMO) technology as well as eight antennas with eight transmitters and eight receivers.

Wi-Fi 5 also uses MU-MIMO, but with 4x4 antennas.

The answers 16 and six are incorrect.

43.

Which of the following is an optical module transceiver?

SFP+

ANT+

OFDM

RS-232

Correct answer: SFP+

A Small Form-factor Pluggable (SFP) is a pluggable module transceiver that can be used in either Ethernet or optical data transmission. SFP+ is an enhanced version with speeds up to 16 Gbit/s. Ethernet applications of SFP+ include 10 Gigabit Ethernet and 8 Gbps Fibre Channel. Quad Small Form-factor Pluggable (QSFP) is another compact, hot-pluggable transceiver.

Adaptive Network Topology+ (ANT+) is a wireless protocol used in the Internet of Things (IoT) for short-distance connections.

Orthogonal Frequency Division Multiplexing (OFDM) is a modulation technique used in cellular networks.

RS-232 is an industry standard commonly used in serial cables.

44.

A router's forwarding decisions are based primarily on which of the following?

Destination IP address

Destination MAC address

Source IP address

Source MAC address

Correct answer: Destination IP address

Routers are Layer 3 devices, therefore, they use the logical network address, IP address, to interpret and determine where packets should be forwarded. Since a router is a gateway to other routed domains, it uses IP addresses to keep track of the other routing points.

Switches make forwarding decisions based on the destination MAC address.

A router would not make a decision based on the source IP address. The forwarding decision answers the question: Where is this packet going?

The source MAC address is incorrect.

45.

Which of the following is a security solution installed on a host that blocks malicious traffic to it?

HIPS

NIPS

NIDS

Perimeter network

Correct answer: HIPS

An Intrusion Prevention System (IPS) monitors network traffic and can identify and block connections containing known attacks. To accomplish this, it must be deployed in line with the monitored network traffic.

An IPS can be deployed as a dedicated network device known as a Network Intrusion Prevention System (NIPS) or on an individual host known as a Host Intrusion Prevention System (HIPS).

An Intrusion Detection System (IDS) identifies known malicious content in network traffic and generates an alert. It can also be deployed as a dedicated device known as a Network-based Intrusion Detection System (NIDS).

A perimeter network or screened subnet hosts servers that should be accessible from the public Internet (web, email, etc.). The perimeter firewall allows through legitimate protocols for these services (HTTP, SMTP, etc.) but blocks others.

46.

Which of the following are the frequency band and maximum bandwidth values for 802.11n?

2.4 GHz or 5 GHz, 300 Mbps

2.4 GHz, 54 Mbps

2.4 GHz, 11 Mbps

5 GHz, 54 Mbps

Correct answer: 2.4 GHz or 5 GHz, 300 Mbps

The frequency bands and maximum bandwidth values of wireless standards are as follows:

- *802.11a: 5 GHz, 54 Mbps*
- *802.11b: 2.4 GHz, 11 Mbps*
- *802.11g: 2.4 GHz, 54 Mbps*
- *802.11n: 2.4 and 5 GHz, >300 Mbps*
- *802.11ac: 5 GHz, >3 Gbps*
- *802.11ax: 2.4, 5, and 6 GHz, 9.6 Gbps*

47.

What address is reserved for loopback tests?

127.0.0.1

169.254.0.1

192.168.0.1

255.255.255.255

Correct answer: 127.0.0.1

The 127.0.0.1 address is reserved for loopback testing, enabling an administrator to determine if the TCP/IP stack is working on a computer. This mirrors the actions of sending and receiving a packet on the network. Sending a packet to the 127.0.0.1 address, also called "localhost," sends the packet outside the interface only to have it come right back in to be processed. This can determine if there are any errors with the local machine's hardware or TCP/IP configurations.

An IP address beginning with 169.254 is called an Automatic Private IP Addressing (APIPA) IP address. It generally is assigned to a computer when an automatic IP address assignment from a DHCP server fails. The address 192.168.0.1 is often the default IP address for wi-fi or LAN routers. The IP address 255.255.255.255 is a subnet mask address.

48.

Which of the following involves the use of JSON to automatically create and configure network environments?

IaC

NFV

IFC

LDAP

Correct answer: IaC

Infrastructure as Code (IaC) is a method to automatically create and configure network infrastructure. It involves writing reusable code with either JavaScript Object Notation (JSON) or Yet Another Markup Language (YAML).

Network Function Virtualization (NFV) adds a layer of abstraction from hardware resources using virtualization and cloud computing.

IFC is a fabricated term.

Lightweight Directory Access Protocol (LDAP) is used to query directory services such as Active Directory.

49.

A network administrator is experiencing issues with choppy video conference streaming and stuttering call audio. Which of the following would MOST LIKELY help resolve the issue?

Quality of service

Acceptable use policies

Content caching

Hardware redundancy

Correct answer: Quality of service

Quality of Service (QoS) technologies make it possible to improve network performance by prioritizing certain types of traffic. For example, videoconferencing traffic may be more important than and prioritized over web traffic to social media sites.

An acceptable use policy would not affect network performance or QoS.

Content caching is a way of storing data in servers that are closer to the user. It would not directly affect performance or QoS.

Hardware redundancy is important but is not a QoS issue.

50.

Which of the following network types focuses on smartphones, laptops, and Bluetooth devices in close proximity?

PAN

SAN

MAN

CAN

Correct answer: PAN

A Personal Area Network (PAN) includes short-distance connections between a user's devices, such as smartphones, laptops, or wireless earbuds. Connections can be made wirelessly across Bluetooth or a Wireless Local Area Network (WLAN), or they may be linked through Ethernet or USB cables.

A Storage Area Network (SAN) is designed for storage arrays or other storage media.

A Metropolitan Area Network (MAN) covers a metropolitan area such as a large city or a collection of several smaller cities.

A Campus Area Network (CAN) covers a smaller area like a college or corporate campus.

51.

How many broadcast domains does a router with 12 active ports have?

12

6

2

1

Correct answer: 12

Consider a router as a device to connect network segments together, providing an internetwork. In this way, routers create separate broadcast domains to segregate and connect many different networks. Routers create a separate broadcast domain for each interface. A router with 12 active ports would have 12 broadcast domains. Each active port on a router also has a separate collision domain.

The answers six, two, and one are incorrect.

A switch with 12 active ports would have one broadcast domain and 12 collision domains. A switch with two Virtual Local Area Networks (VLANs) would have two broadcast domains because each VLAN has its own broadcast domain.

52.

Which Open Systems Interconnection (OSI) model layer contains technology such as antennas, hubs, and fiber optic cabling?

Layer 1

Layer 2

Layer 3

Layer 4

Correct answer: Layer 1

Layer 1 of the Open Systems Interconnection (OSI) model deals with the physical transmission of bits, which is the role of cabling.

The OSI model is a conceptual framework. Layers 2, 3, and 4 are not associated with issues related to physical infrastructure, although all higher-level protocols run over physical resources.

The seven layers of the OSI model are:

- *Layer 7 - Application*
- *Layer 6 - Presentation*
- *Layer 5 - Session*
- *Layer 4 - Transport*
- *Layer 3 - Network*
- *Layer 2 - Data link*
- *Layer 1 - Physical*

53.

Which of the following will be the destination IP and MAC addresses of a packet going to a computer on a different subnet?

Dest. IP: IP address of the remote host. Dest. MAC: MAC address of the default gateway.

Dest. IP: IP address of the default gateway. Dest. MAC: MAC address of the default gateway.

Dest. IP: IP address of the remote host. Dest. MAC: MAC address of the remote host.

Dest. IP: IP address of the remote host. Dest. MAC: MAC address of the local PC.

Correct answer: Dest. IP: IP address of the remote host. Dest. MAC: MAC address of the default gateway.

The destination Internet Protocol (IP) address remains the same throughout the connection, but the Media Access Control (MAC) address would be confined to the local network. When the packet/frame header is created for a host on a different network, the destination IP address is configured to that of the remote host. The destination MAC address, however, is configured for the MAC address of the default gateway of the Personal Computer's (PC's) local network so that it can be routed to its final destination.

54.

Which of the following addresses sends packets to multiple interfaces using one address?

Multicast

Anycast

Link-local address

Unicast

Correct answer: Multicast

IPv4 and IPv6 multicast are "one to many" addresses designed to send a packet to multiple different interfaces with a single address.

Anycast addressing is designed to deliver a packet to the IPv6 address with the shortest routing distance.

Link-local addresses are non-routable IPv6 addresses in the FE80::/10 range. They are similar to Automatic Private IP Addressing (APIPA) addresses in IPv4.

Unicast addresses are used to send packets to a particular interface. Unicast addressing exists for both IPv4 and IPv6.

55.

Traffic entering a data center from the outside is moving in which direction?

Southbound

Northbound

Eastbound

Westbound

Correct answer: Southbound

North-south traffic flows are entering or leaving the data center network. Traffic entering a data center from the outside is moving southbound. Picture a network with two axes. The north-south axis represents the traffic between the external network and the internal network. The east-west axis represents traffic within the data center. The external network (the public Internet), to the north, lies beyond the firewall and any Demilitarized Zone (DMZ). The internal network, to the south, contains protected assets and resources, such as databases and workstations. Any traffic moving from the external network to the internal network would be considered traveling southbound.

Any traffic moving from the internal network to the external network would be considered traveling northbound.

East-west traffic moves laterally within a data center.

56.

You have just been made aware that an employee who works for you has been transferring files using a protocol that offers no security. Which protocol is likely being used by the negligent employee?

FTP

HTTP

Telnet

SSH

Correct answer: FTP

File Transfer Protocol (FTP) permits the transfer of files over a network. However, FTP does not offer any security whatsoever. FTP has been superseded by more secure protocols, such as Secure File Transfer Protocol (SFTP) and File Transfer Protocol Secure (FTPS).

Hypertext Transfer Protocol (HTTP) is an insecure protocol used in web browsers. Most websites have now moved to the more secure Hypertext Transfer Protocol Secure (HTTPS).

Telnet is an insecure network access protocol. Telnet was commonly used before being replaced by SSH.

Secure Shell (SSH) is a command-line tool that allows you to transmit commands to a remote system securely.

57.

A user is attempting to access a site using Hypertext Transfer Protocol (HTTP). Which default port can they use?

80

443

21

23

Correct answer: 80

By default, Hypertext Transfer Protocol (HTTP) uses Transmission Control Protocol (TCP) port 80.

HTTPS, the secure version of HTTP, uses port 443.

FTP uses ports 20 and 21.

Telnet operates on port 23.

58.

Which of the following devices ALWAYS has multiple collision domains but a single broadcast domain?

Bridge

Hub

Switch

Router

Correct answer: Bridge

Bridges have a single broadcast domain, but each port is its own collision domain.

Hubs have a single collision and broadcast domain.

Each of a switch's ports has its own collision domain, and it has a single broadcast domain unless those broadcast domains are broken up into different Virtual Local Area Networks (VLANs).

A router's ports all have different collision domains, and they can be configured to belong to different broadcast domains.

59.

Which WLAN standard does NOT support Orthogonal Frequency-Fivision Multiplexing (OFDM)?

802.11b

802.11a

802.11g

802.11n

Correct answer: 802.11b

Direct Sequence Spread Multiplexing (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM) are two transmission methods used by WLANs. Support for these methods among wireless standards is as follows:

- *802.11b: DSSS*
- *802.11a: OFDM*
- *802.11g: DSSS and OFDM*
- *802.11n: OFDM*

60.

What are the two primary security protocols used by IPSec?

AH and ESP

IKE and AES

ISAKMP and GRE

TLS and SFTP

Correct answer: AH and ESP

Internet Protocol Security (IPSec) is a set of protocols used to protect data in transit. The two primary security protocols used by IPSec are Authentication Header (AH) and Encapsulating Security Payload (ESP).

Internet Key Exchange (IKE) is a management protocol used by IPSec. Advanced Encryption Standard (AES) is a form of symmetric block encryption.

Internet Security Association and Key Management Protocol (ISAKMP) is used by IKE to manage connections. Generic Routing Encapsulation (GRE) is a tunneling protocol.

Transport Layer Security (TLS) may be used by IPSec for authentication. Secure File Transfer Protocol (SFTP) is used for file transfer.

61.

You are in the process of adding a web server to your organization's network. The web server needs to be accessible from the public Internet. Which measure should be put in place when adding this new web server to the network?

It should be placed in the perimeter network.

It should be placed in the external network.

It should only be accessible using a VPN.

It should be placed in the internal network.

Correct answer: It should be placed in the perimeter network.

Devices that need to be accessible from the public internet, such as web servers and email servers, should be placed in a perimeter network. Perimeter networks may allow users on the internet to initiate an email or web session coming into the organization, but they block all other protocols. A perimeter network is also known as a Demilitarized Zone (DMZ) or a screened subnet.

The external network refers to the public Internet. You would not place your resources there.

Limiting access to Virtual Private Network (VPN) access only defeats the purpose of a public-facing web server.

A publicly-accessible web server would not be placed in the internal network. That is where protected resources like databases and user devices should be placed.

62.

An engineer is adding a new router to the network. At which level of the Open Systems Interconnection (OSI) model will this router operate?

Network

Transport

Session

Physical

Correct answer: Network

Since the network layer manages logical device addressing, tracks the locations of devices on the network, and determines the best way to deliver that data, it's easy to see that a router encompasses all of these operations. A router routes and controls the flow of traffic based on the logical addresses and Internet Protocol (IP) addresses, and determines how to get the data from point A to point B.

The transport layer works closely with the network layer, although they are separate concepts. For instance, Transmission Control Protocol/Internet Protocol (TCP/IP) is the combination of a Layer 4 protocol (TCP) with a Layer 3 protocol (IP). The routing takes place in the IP part, while TCP handles reliable transmission.

The session and physical layers are distinct from Layer 3 networking. Care should be taken to learn the Open Systems Interconnection (OSI) model thoroughly.

The seven layers of the OSI model are:

- *Layer 7 - Application*
- *Layer 6 - Presentation*
- *Layer 5 - Session*
- *Layer 4 - Transport*
- *Layer 3 - Network*
- *Layer 2 - Data link*
- *Layer 1 - Physical*

63.

SSE is a connectivity option for which of the following?

ZTA

ZTE

SDN

NFV

Correct answer: ZTA

Secure Service Edge (SSE) is a connectivity option for Zero Trust Architecture (ZTA). SSE provides safe access to websites and applications using capabilities such as:

- *Secure Web Gateway (SWG)*
- *Cloud Access Security Broker (CASB)*
- *Firewall as a Service (FWaaS)*

Another connectivity option for ZTA is Secure Access Secure Edge (SASE).

ZTE is a telecommunications device vendor.

Software-Defined Networking (SDN) is a flexible approach that uses software to manage networks.

Network Function Virtualization (NFV) involves abstracting the functions of network devices, such as routers and switches, and turning them into software rather than hardware devices.

64.

Which of the following statements about RDP is TRUE?

RDP is a proprietary protocol.

RDP uses port 3398.

RDP sends raw pixel data.

RDP uses port 5900.

Correct answer: RDP is a proprietary protocol.

Remote Desktop Protocol (RDP) is a proprietary protocol of Microsoft, although there are now some open-source alternatives based on the protocol.

RDP does not use port 3398; it uses Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port 3389.

RDP does not send raw pixel data, but the open-source protocol Virtual Networking Computing (VNC) does. This allows VNC to operate on any desktop type.

RDP does not use port 5900; that is used by VNC.

65.

Which of the following is a feature of anycast addressing?

Selecting a destination address based on the closest routing distance

Sends packets to multiple addresses

Delivers packets to one interface specifically

Similar to APIPA addresses in IPv4

Correct answer: Selecting a destination address based on the closest routing distance

Anycast addressing is designed to deliver a packet to the IPv6 address with the shortest routing distance.

Anycast identifies multiple interfaces but delivers packets to only one address, so the answer "sends packets to multiple addresses" would be incorrect.

The answer "delivers packets to one interface specifically" is incorrect. That would be true of unicast, not anycast.

Link-local addresses are non-routable IPv6 addresses in the FE80::/10 range. They are similar to Automatic Private IP Addressing (APIPA) addresses in IPv4.

66.

Which of the following networks is NOT reflected by physical infrastructure?

SD-WAN

CAN

PAN

WAN

Correct answer: SD-WAN

A Software-Defined Wide Area Network (SD-WAN) is a virtual overlay on top of other networks.

A Wide Area Network (WAN), Personal Area Network (PAN), and Campus Area Network (CAN) are all networks with a certain physical footprint.

67.

Which of the following is MOST closely related to the principle of least privilege?

Zero trust

Defense in depth

Separation of duties

Multifactor authentication

Correct answer: Zero trust

A zero-trust security model implements the principle of least privilege.

Defense in depth is the practice of not relying on a single layer of security.

Separation of duties states that critical processes or ones that may be at risk of fraud should be broken up into stages that require different employees.

Multifactor authentication uses more than one authentication medium (passwords, biometrics, one-time passwords, etc.) to provide access to a system or service.

68.

Which cellular signal modulation technique is used by 3G networks?

CDMA

FDMA

TDMA

SDMA

Correct answer: CDMA

3G networks use Code Division Multiple Access (CDMA) technologies. CDMA uses the entire spectrum for each call, assigning a unique code to each.

Frequency Division Multiple Access (FDMA) enables parallel transmission of signals by assigning each to a band of frequencies. FDMA was used in 1G cellular.

Time-Division Multiple Access (TDMA) divides time into slots and allows multiple different signals to use the same frequency. TDMA was used in 2G cellular.

SDMA is a fabricated term.

69.

You and a colleague are working to implement a new wireless network for a client. Your colleague thinks that 802.11n will be sufficient, but you recommend that the devices chosen be 802.11ac. Which of the following is an advantage of 802.11ac?

High speed

Compatibility with 802.11g

Compatibility with 802.11a

Use of infrared instead of radio

Correct answer: High speed

The 802.11ac wireless standard was designed for extremely high speeds and improved scalability. Like 802.11n, it uses Multiple-Input, Multiple-Output (MIMO), which uses multiple antennas to transmit and receive to increase data throughput. 802.11ac enhancements over 802.11n include eight spatial streams instead of four, 256 Quadrature Amplitude Modulation (QAM) instead of 64 QAM, and support for up to eight antennas instead of four with 802.11n.

Here are speeds for various standards:

- *802.11ax: 3.5+ Gbps*
- *802.11ac: 1 Gbps*
- *802.11n: 300 Mbps*
- *802.11g: 54 Mbps*
- *802.11a: 54 Mbps*
- *802.11b: 11 Mbps*

IEEE 802.11n is backward compatible with 802.11a/b/g, but that does not constitute an advantage over 802.11n.

The original 802.11 standard used infrared, but the Wi-Fi Alliance later dropped it.

70.

Which of the following is NOT the same as the others?

Switch

Hub

Repeater

Network adapter

Correct answer: Switch

A switch is a Layer 2 (data link layer) device.

A hub is a Layer 1 device. Unlike a switch, it does not use its ports to separate traffic into different broadcast domains. It is basically a "dumb" device.

A repeater is also a Layer 1 device and is similar to a hub. It simply forwards (repeats) bits through the network without any processing.

A network adapter is also a Layer 1 device and does not process traffic.

71.

Of the following, which represents how a Class C network's bytes are allocated?

Network.Network.Network.Host

Network.Host.Host.Host

Network.Network.Host.Host

Host.Host.Host.Host

Correct answer: Network.Network.Network.Host

The three classes of networks allocate their bytes as follows:

- *Class A: Class A networks use 8 bits for the network and 24 for the host (Network.Host.Host.Host)*
- *Class B: Class B networks use 16 bits for the network and 16 for the host (Network.Network.Host.Host)*
- *Class C: Class C networks use 23 bits for the network and 8 for the host (Network.Network.Network.Host)*

Host.Host.Host.Host addresses don't exist.

72.

You are looking into implementing a Storage Area Network (SAN) and Fibre Channel is at the top of your list. Which of the following makes Fibre Channel (FC) more flexible within a local wired network?

FCoE

Jumbo frames

IB

FCoL

Correct answer: FCoE

Fibre Channel over Ethernet (FCoE) makes Fibre Channel (FC) more flexible within a local wired network because you can configure FCoE to run a unified network for your Storage Area Network (SAN) and non-storage data traffic.

Jumbo frames are larger-than-normal frames used in an IP-based Small Computer System Interface (iSCSI) network. InfiniBand (IB) is another infrastructure that competes with FC and iSCSI. FCoL is a fabricated term.

73.

Of the following WAN technologies, which does NOT typically use an Unshielded Twisted Pair (UTP)?

Cable modem

ISDN

DSL modem

POTS dial-up modem

Correct answer: Cable modem

Cable modems are usually connected via an F-connector attached to an RG-6 coaxial line.

Integrated Services Digital Network (ISDN) connects via an Unshielded Twisted Pair (UTP), typically with an RJ-11 connector.

The same is true for Digital Subscriber Line (DSL).

The Plain Old Telephone System (POTS) dial-up modem also uses UTP.

74.

Which of the following network protocols is commonly used to distribute software images and configuration files to a device?

TFTP

FTP

SSH

HTTP

Correct answer: TFTP

The Trivial File Transfer Protocol (TFTP) is a lightweight file transfer utility. It is commonly used to transfer software and other information to a device, particularly during commissioning. Network professionals may connect their laptops to a device using a console cable to install a configuration.

The File Transfer Protocol (FTP) can serve a similar purpose, but it is bulkier and can also incorporate features such as authentication.

Secure Shell (SSH) is an authenticated, encrypted remote access protocol that also supports file transfer.

The Hypertext Transfer Protocol (HTTP) is the protocol used to request and deliver webpages when browsing the Internet.

75.

Of the following, which operates on port 143 and is a protocol used for retrieving email from a server?

IMAP4

POP3

SMTP

SIP

Correct answer: IMAP4

The Internet Message Access Protocol version 4 (IMAP4) is the protocol currently replacing the Post Office Protocol 3 (POP3) protocol due to enhanced control over email on the server. This enhanced control increases security and reduces threat vectors.

POP3 is also an email download protocol, but it operates on port 110.

Simple Mail Transfer Protocol (SMTP) is an email transfer protocol that operates on port 25.

Session Initiation Protocol (SIP) is used frequently in VoIP and operates on ports 5060 and 5061.

76.

Which of the following is the correct order of the Open Systems Interconnection (OSI) model, starting with Layer 1?

Physical, data link, network, transport, session, presentation, application

Physical, network, transport, session, data link, presentation, application

Application, network, transport, data link, session, presentation, physical

Application, network, transport, session, presentation, data link, physical

Correct answer: Physical, data link, network, transport, session, presentation, application

The Open Systems Interconnection (OSI) model is a seven-layered model starting with physical at Layer 1 and ending with application at Layer 7. One common mnemonic used to help memorize the order of the OSI model is "Please Do Not Throw Sausage Pizza Away."

The seven layers of the OSI model are:

- *Layer 7 - Application*
- *Layer 6 - Presentation*
- *Layer 5 - Session*
- *Layer 4 - Transport*
- *Layer 3 - Network*
- *Layer 2 - Data link*
- *Layer 1 - Physical*

77.

A colleague has just mentioned that the office will be getting Fast Ethernet. The term "Fast Ethernet" typically refers to which speed?

100 Mbps

10 Mbps

1 Gbps

10 Gbps

Correct answer: 100 Mbps

Although there are much faster versions of Ethernet now, such as Gigabit Ethernet, the term "Fast Ethernet" is still used to describe the 100 Mbps Ethernet standard known as 100BaseT. Also included in this standard are 100BaseTX, 100BaseT4, and 100BaseT2.

10BaseT is an Ethernet standard that can reach a speed of 10Mbps. Ethernet standards with a maximum transmission speed of 1 Gbps are generally referred to as the equivalent of 1000 Mbps. These include 1000BaseTX, 1000BaseSX, 1000BaseCX, and 1000BaseLX. There are several 802.3 standards for 10Gbps Ethernet, including 10GBaseT, 10GBaseSR, and 10GBaseLR.

78.

Which cloud model offers the greatest scalability and elasticity?

Public cloud

Private cloud

Hybrid cloud

Community cloud

Correct answer: Public cloud

In the public cloud, an organization is using a shared infrastructure managed by a cloud service provider, which allows them to expand or contract their cloud deployment as needed. The public cloud also includes on-demand access and pay-as-you-go pricing.

Private, hybrid, and community clouds all use at least some dedicated or customer-owned infrastructure, which limits scalability and elasticity.

79.

In which network topology do all systems have a connection to a central point?

Star

Bus

Mesh

Point-to-point

Correct answer: Star

In a star (hub-and-spoke) network, each node is connected to a central point, with direct connections between the host and the switch or hub. It represents a concept known as single point of failure, or SPOC, because if the central hub or switch fails, it will take down the network. While a star network might also be considered a point-to-multipoint topology, the distinction may be argued that star networks connect hosts while point-to-multipoint networks connect switches or routers.

A bus topology is a continuous wire that is terminated at each end with each node plugged into the wire. A mesh topology has each node connected to more than one other node to provide a web-like structure. A point-to-point topology connects two devices through a single link.

80.

Which of the following is used to define the boundary of a protected network, such as a corporate network?

Firewall

IDS

Geofencing

Bridge

Correct answer: Firewall

A firewall defines the boundary of a protected network because it filters inbound and outbound traffic based on predefined rules.

An Intrusion Detection System (IDS) is designed to identify and alert for or block malicious content.

Geofencing uses global positioning to define a geographic boundary for wireless signaling.

A bridge is used to link similar network segments to one another.

81.

The Internet Protocol (IP) address 10.8.25.250 is an example of which of the following?

Class A private address

Class B private address

Class C private address

Class A public address

Correct answer: Class A private address

Any address that begins with 10 is a private, Class A Internet Protocol (IP) address that is not routable on the public internet. These Class A address ranges permit companies to create extremely large private networks, broken up into many different subnetworks.

As defined by RFC 1918, the reserved address space for private IP addresses is as follows:

- *Class A: 10.0.0.0 through 10.255.255.255*
- *Class B: 172.16.0.0 through 172.31.255.255*
- *Class C: 192.168.0.0 through 192.168.255.255*

The IP address 10.8.25.250 is a private address, not a public one.

82.

CSMA/CA is a contention method for which of the following standards?

802.11

802.1

802.3

802.2

Correct answer: 802.11

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) is a contention method for IEEE 802.11 standards, which deal with wireless Local Area Networks (LANs). CSMA/CA is a technology deployed with wireless networks to reduce collisions. Because wireless networks inherently operate within the same collision domain, they will no doubt have to handle collisions. CSMA/CA allows the wireless network to appropriately queue and handle all the wireless communications.

IEEE 802.1 is a family of standards that deal with higher-layer LAN protocols, such as 802.1Q for Virtual LAN (VLAN) tagging and 802.1X for network access control.

IEEE 802.3 contains the standards for Ethernet. CSMA/CD is a contention method for Ethernet.

IEEE 802.2 is the standard for Logical Link Control (LLC), the upper part of the data link layer.

83.

How many bits are in a Media Access Control (MAC) address?

48 bits

8 bits

24 bits

16 bits

Correct answer: 48 bits

A Media Access Control (MAC) address is a unique identifier that exists on every Network Interface Card (NIC). No two NICs will ever share the same MAC address. MAC addresses consist of 48 bits.

These 48 bits are divided into two parts. The Organizationally Unique Identifier (OUI) is 24 bits and is assigned by IEEE. The other 24 bits are assigned by the vendor.

The responses 8 bits, 24 bits, and 16 bits are incorrect.

84.

With which Wi-Fi version was MU-MIMO introduced?

Wi-Fi 5

Wi-Fi 6

Wi-Fi 4

Wi-Fi 7

Correct answer: Wi-Fi 5

Wi-Fi 5 (802.11ac) introduced the use of Multi-User Multiple-Input Multiple-Output (MU-MIMO), which allows more devices to use Wi-Fi at the same time by coordinating multiple streams across antennas on multiple independent wireless Access Points (APs).

Wi-Fi 6 (802.11ax) also uses MU-MIMO, but it came after Wi-Fi 5.

Wi-Fi 4 (802.11n) uses MIMO, not MU-MIMO.

Wi-Fi 7 is not in the scope of Network+ at this time.

85.

A wireless Access Point (AP) is MOST similar to which of the following devices?

Hub

Switch

Bridge

Router

Correct answer: Hub

A wireless Access Point (AP) operates like a hub where all connected devices are on the same collision domain.

The primary difference is that an AP communicates over radio signals rather than via cables. An AP can be connected to a switch, bridge, or router to increase functionality.

A switch has multiple collision domains. Each interface has a separate collision domain unless they are grouped using Virtual Local Area Networks (VLANs).

A bridge can be used to create multiple collision domains.

A router has a separate collision domain on each interface. Many APs include router functionality in the same device, but not all APs are routers.

86.

Which of the following is NOT a common Layer 3 switching technique?

Frame switching

Circuit switching

Packet switching

Message switching

Correct answer: Frame switching

Frame switching is a Layer 2, data link layer, switching technique. Frames are the Protocol Data Units (PDUs) exchanged at Layer 2.

The three common Layer 3 switching techniques are packet switching, circuit switching, and message switching.

Circuit switching involves setting up circuits for the transmission of traffic. An example is the Plain Old Telephone System (POTS).

Packet switching involves breaking data into packets and forwarding them across the network. Packet switching is a part of routing at Layer 3, the network layer.

Message switching includes sending data as messages. An example is email. It is a store-and-forward approach.

87.

Which of the following is a non-overlapping 2.4 GHz channel that is NOT supported within the United States?

14

1

6

11

Correct answer: 14

Four non-overlapping channels exist within the 2.4 GHz band: 1, 6, 11, and 14. However, channel 14 is not supported within the US.

*Traffic within a channel can spread over 22 MHz, so a "non-overlapping" channel is at least 22 MHz away from another channel. All 2.4 GHz channels (except 14) are separated by 5 MHz, so non-overlapping channels have numbers 5 apart (5 * 5 MHz = 25 MHz > 22 MHz). Channel 14 is 12 MHz away from Channel 13, which is why it is also non-overlapping despite being closer in number to Channel 11.*

The non-overlapping channels 1, 6, and 11 are permitted in the US.

88.

Of the following, which represents how a Class B network's bytes are allocated?

Network.Network.Host.Host

Network.Host.Host.Host

Network.Network.Network.Host

Host.Host.Host.Host

Correct answer: Network.Network.Host.Host

The three classes of networks allocate their bytes as follows:

- *Class A: Class A networks use 8 bits for the network and 24 for the host (Network.Host.Host.Host)*
- *Class B: Class B networks use 16 bits for the network and 16 for the host (Network.Network.Host.Host)*
- *Class C: Class C networks use 24 bits for the network and 8 for the host (Network.Network.Network.Host)*

There is no such thing as a Host.Host.Host.Host address.

89.

How many watts does the 802.3af standard provide?

15.4

30

11

25.5

Correct answer: 15.4

The 802.3af standard is capable of providing up to 15.4 watts of power on the network and up to 44 volts. 802.3af is the standard for Power over Ethernet (PoE).

The answers 30 and 11 are incorrect.

The 802.3at standard is capable of providing up to 25.5 watts. 802.3at is the standard for Power over Ethernet Plus (PoE+).

90.

What is the maximum distance of 10GBase-EW?

40 km

25 km

30 m

10 km

Correct answer: 40 km

Ethernet standards are defined by IEEE 802.3. A few of the standards are listed below.

	Fiber Type	Bandwidth Capacity	Maximum Distance
10GBase-EW	Single-Mode Fiber (SMF)	10 Gbps	40 km
10GBase-LW	Single-Mode Fiber (SMF)	10 Gbps	10 km
10GBase-LR	Single-Mode Fiber (SMF)	10 Gbps	10 km
10GBase-T	UTP CAT8	40 Gbps	30 m
1000BaseCX	Balanced, shielded copper	1000 Mbps	25 m

91.

Which of the following is the MOST prevalent protocol used in Storage Area Networks (SAN)?

Fibre Channel

NFS

iSCSI

Infiniband

Correct answer: Fibre Channel

Fibre Channel is the most prevalent protocol used in Storage Area Networks (SAN). Fibre channel is used in 70-80% of SAN markets.

Network File System (NFS) is more commonly used with the file-based storage technology called Network-Attached Storage (NAS).

Internet Protocol (IP)-based Small Computer Systems Interface (iSCSI) can also be used by a Storage Area Network (SAN) to transfer data between network storage and servers.

Infiniband (IB) is used to connect storage systems and other network devices in a High-Performance Computing (HPC), or supercomputer, environment. IB uses unique network interface cards and cabling and often aggregates multiple (four or eight) physical links to improve throughput, performance, and latency.

92.

Which of the following access technologies is used by Wi-Fi 6/802.11ax?

OFDMA

OFDM

DSSS

FHSS

Correct answer: OFDMA

Wi-Fi 6 uses Orthogonal Frequency-Division Multiple Access (OFDMA), which uses smaller packet sizes than Orthogonal Frequency-Division Multiplexing (OFDM) to support more devices and decrease overhead and latency.

OFDM is used on 802.11a, 802.11g, 802.11n, and 802.11ac.

Direct-Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS) are earlier access technologies.

DSSS is used on 802.11, 802.11b, 802.11g, and 802.11n.

FHSS is used on 802.11.

93.

What is the 127.0.0.1 address used for?

Loopback testing

Sending data to all hosts on a network

Private IP address

APIPA

Correct answer: Loopback testing

The 127.0.0.1 address is reserved for loopback testing, enabling an administrator to determine if the Transmission Control Protocol/Internet Protocol (TCP/IP) stack is working on a computer. This mirrors the actions of sending and receiving a packet on the network.

Sending a packet to the 127.0.0.1 address, also called "localhost", sends the packet outside the interface only to have it come right back in to be processed. This can determine if there are any errors with the local machine's hardware or TCP/IP configurations.

Sending data to all hosts on a network refers to transmitting broadcast messages.

Private IP addresses are defined by RFC 1918 and use the following ranges:

- *10.0.0.0 to 10.255.255.255*
- *172.16.0.0 to 172.31.255.255*
- *192.168.0.0 to 192.168.255.255*

An Automatic Private IP Addressing (APIPA) address is self-configured by a device when the Dynamic Host Configuration Protocol (DHCP) fails. The IP address range for APIPA is 169.254.0.1 to 169.254.255.254.

94.

What is a CSU/DSU?

A modem

A switch

An adapter

A signal generator

Correct answer: A modem

A Channel Service Unit/Data Service Unit (CSU/DSU) is a type of modem. As a standalone device, it was commonly used as Data Communications Equipment (DCE) in legacy technologies such as Frame Relay. Today, the functions of a CSU/DSU may be integrated into devices such as a router or a network interface card. The word modem is a combination of the concepts modulate and demodulate. The function of a modem is the conversion of analog and digital signals over a telecom line.

A CSU/DSU is not a switch, which is used to forward communication on a Local Area Network (LAN).

While in a general sense, a CSU/DSU does adapt signals between analog and digital, the proper term for that would be modem.

A signal generator is an electronic device that creates electrical signals.

95.

Of the following protocols, which lack built-in security features?

PPTP and L2TP

SSL and TLS

802.1X and RADIUS

SSH and IPsec

Correct answer: PPTP and L2TP

The Layer 2 Tunneling Protocol (L2TP) is an unencrypted Virtual Private Network (VPN) protocol. To be secure, it must be combined with a protocol that provides authentication and encryption.

The Point-to-Point Tunneling Protocol (PPTP) is a deprecated VPN protocol that lacks basic security features. Microsoft extended the protocol with built-in security and integrated it into earlier versions of Windows.

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are both secure protocols providing encryption in transit.

802.1X and Remote Authentication Dial-In User Service (RADIUS) are both secure authentication protocols.

Secure Shell (SSH) is used for secure remote connections, and Internet Protocol Security (IPSec) is a secure protocol used in VPNs.

96.

Which of the following is the set of shared configurations used in an ISAKMP session?

Security association

Diffie-Hellman

Secure sockets layer

Perfect forward secrecy

Correct answer: Security association

A Security Association (SA) is the set of parameters that two devices agree upon for use in an Internet Security Association and Key Management Protocol (ISAKMP) session.

Diffie-Hellman (DH) creates a shared encrypted key over a public channel.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) provide Confidentiality, Integrity, and Authentication (CIA) protections for the Open Systems Interconnection (OSI) model Layers five through seven.

Perfect Forward Secrecy (PFS) makes it impossible to derive a session key from a compromised private key.

97.

Which of the following is NOT a private IP address?

172.32.1.1

172.16.5.2

10.0.1.1

192.168.100.100

Correct answer: 172.32.1.1

All those listed, except 172.32.1.1, fall within the following private IPv4 address ranges as defined by RFC 1918:

- *10.0.0.0 through 10.255.255.255*
- *172.16.0.0 through 172.31.255.255*
- *192.168.0.0 through 192.168.255.255*

98.

How many channels does a leased line connection E1 have?

32

30

24

20

Correct answer: 32

An E1 line has 32 channels, of which 30 can be used for data transfer. A T1 line has 24 channels.

99.

How would you describe SDWAN?

Zero touch

Virtual storage network

Transport independent

Inflexible

Correct answer: Zero touch

Zero-Touch Provisioning (ZTP) is a feature of a Software-Defined Wide Area Network (SDWAN). ZTP is an automatic process that installs network devices in SDWAN without manual intervention.

SDWAN is not a virtual storage network. One example of a virtual storage network is a Virtual Storage Area Network (VSAN).

SDWAN is transport dependent. As a virtual WAN architecture, SDWAN can integrate with supporting transport architectures such as Long-term Evolution (LTE), Multiprotocol Label Switching (MPLS), and broadband.

SDWAN is a flexible and cost-effective virtual WAN architecture.

100.

Which type of cable has an insulator embedded in the cable that is fire-retardant and reduces the dangerous fumes emitted in the event of a fire?

Plenum

STP

UTP

HVAC

Correct answer: Plenum

Plenum cabling has a fire-retardant insulating coating that protects against poisonous fumes being pumped through a building during a fire. In some cases, plenum cabling also minimizes dangerous fumes by using Fluorinated Ethylene Polymer (FEP) or low-smoke polyvinyl chloride.

Shielded Twisted-Pair (STP) has a metallic shield surrounding twisted-pair cabling.

Unshielded Twisted-Pair (UTP) does not have this outer shielding.

HVAC stands for heating, ventilation, and air conditioning.