CompTIA Network+ (N10-008) - Quiz Questions with Answers

1.0 Networking Concepts

1.

Which cellular signal modulation technique breaks the frequency range into bands assigned to each cellular device?

FDMA

CDMA

TDMA

SDMA

Correct answer: FDMA

Frequency Division Multiple Access (FDMA) enables parallel transmission of signals by assigning each to a band of frequencies.

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

Time-Division Multiple Access (TDMA) divides time into slots and allows multiple different signals to use the same frequency.

SDMA is a fabricated term.

2.

You want to prioritize real-time applications on your network. What is this process called?

QoS

Classification

Packet priorization

Congestion avoidance

Correct answer: QoS

Quality of Service (QoS) involves the prioritization of network traffic to ensure a desired performance level. QoS priorities may be real-time, high, medium, or low.

The classification of traffic types may be involved, but that is not the network term for this process.

Packet prioritization is involved, but it is an incorrect term.

Congestion avoidance is desirable and may be achieved by proper QoS.

3.

On which of the following devices does each interface have its own broadcast domain?

Router

Hub

Access point

WAN link

Correct answer: Router

Each of a router's interfaces is a different broadcast domain.

This differs from a hub, where all ports are within the same broadcast domain.

An access point is a networking device that enables Wi-Fi devices to connect to a wired network.

A Wide Area Network (WAN) link is a connection for a network to forward data over long distances.

4.

Of the following, which is a specialized technology that takes physical hardware and abstracts it for a virtual server?

Hypervisor

Virtual NIC

Content switch

Supervisor

Correct answer: Hypervisor

Virtualization is made possible by hypervisors. A hypervisor is a specialized software that takes physical hardware and abstracts it for the virtual server.

Virtual Network Interface Cards (NICs) are used to provide network access to the virtual servers. Content switches are not specifically related to virtualization but rather are used for load balancing. Supervisor is a somewhat antiquated term referring to a computer operating system or kernel.

5.

What is the maximum speed and transmission distance of 1000Base-TX?

1000 Mbps, 100 meters

100 Mbps, 100 meters

1000 Mbps, 250 meters

1000 Mbps, 150 meters

Correct answer: 1000 Mbps, 100 meters

1000Base-TX uses two pairs of CAT5e or higher cable, enabling it to carry 1000 Mbps or 1GB over a maximum distance of 100 meters.

100Base-TX has a maximum transmission speed of 100 Mbps and a maximum distance of 100 meters per segment.

The maximum transmission distance of 250 meters does not align with a common Ethernet cable type.

The maximum transmission distance of 150 meters does not align with a common Ethernet cable type.

6.

Which of the following services would likely NOT require QoS?

Web research

Online gaming

Videoconferencing

Streaming media

Correct answer: Web browsing

Web research is not a highly critical time-bound service and would likely not have any requirement for Quality of Service (QoS) management.

Online gaming, videoconferencing, and streaming media are all services that might need the priority traffic management provided by QoS.

7.

Translate the following IP address to binary:

172.16.20.25

10101100.00010000.00010100.00011001

10101100.01110000.00010100.00011001

10101100.00010000.00010101.00011011

10101100.11010000.00010100.00011111

Correct answer: 10101100.00010000.00010100.00011001

The reverse of the binary-to-decimal process involves making comparisons against the chart below. For example, if the number is over 128, a 1 is placed at the beginning of the octet, then the remainder is compared against the chart again.

The decimal equivalent to 10101100.01110000.00010100.00011001 is 172.112.20.25.

The decimal equivalent to 10101100.00010000.00010101.00011011 is 172.16.21.27.

The decimal equivalent to 10101100.11010000.00010100.00011111 is 172.208.20.31.

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

8.

You are using a web browser to securely connect to the web management portal of your network monitoring application. Which remote access method are you likely using in this scenario?

HTTPS

HTTP

RDP

Telnet

Correct answer: HTTPS

When connecting to a system via a web browser, you will be using either Hypertext Transfer Protocol (HTTP) or its secure version, Hypertext Transfer Protocol Secure (HTTPS). The given scenario states that this is a secure connection, so the assumption can be made that HTTPS is being used.

HTTP is similar but insecure.

Remote Desktop Protocol (RDP) is used to access a remote computer as if you were sitting in front of it.

Telnet is an insecure remote access protocol.

You would not use Remote Desktop Protocol (RDP) or Telnet to securely access a web management portal via a web browser.

9.

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.

10.

Which IPS detection method requires frequent updates to be effective?

Signature-based

Policy-based

Statistical anomaly

Nonstatistical anomaly

Correct answer: Signature-based

The Intrusion Prevention System (IPS) detection method that requires frequent updates is the signature-based method. Signature-based detection identifies threats based on known patterns or signatures and requires frequent updates to the signature library.

Policy-based detection would only require updates when corporate policies change.

Statistical and nonstatistical anomaly detection detect deviations from normal traffic, which does not require updates.

11.

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.

12.

Which of the following BEST defines an Intrusion Detection System (IDS)?

It receives a copy of traffic being analyzed and generates alerts about potential attacks.

It defines a set of rules dictating which types of traffic are permitted or denied as that traffic enters or exits a firewall interface.

It secures communication between two sites over an untrusted network.

It sits in line with traffic being analyzed and can drop the traffic.

Correct answer: It receives a copy of traffic being analyzed and generates alerts about potential attacks.

An Intrusion Detection System (IDS) generates alerts about potential attacks, but it takes no action.

A firewall uses a set of predefined rules to determine if traffic should be permitted to enter or leave a protected network or be blocked from doing so.

A Virtual Private Network (VPN) encrypts traffic flowing over a public network, enabling secure communications without the risk of eavesdropping. With a VPN, you can send secure traffic over an untrusted network.

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

13.

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.

14.

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.

15.

Which OSI layer handles LLC and MAC?

Data link

Physical

Network

Application

Correct answer: Data link

The data link layer uses Logical Link Control (LLC) and Media Access Control (MAC) to perform data transmission, error notification, and flow control.

The physical layer handles the physical media, such as cabling, that the data link layer controls access to.

The network layer interfaces with the data link layer.

The application layer is at the top and doesn't control media access.

16.

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.

17.

An Intrusion Prevention System (IPS) is deployed at which layer of the three-tiered network architecture model?

Distribution

Access

Core

Link

Correct answer: Distribution

An Intrusion Prevention System (IPS) would be deployed at the distribution layer of the three-tiered network architecture model. This is the layer that implements network links between devices.

The access layer connects end-user host devices.

The core layer implements high-speed links between data centers and an organization's on-premise networks.

The link layer is not a layer of the three-tiered network architecture model.

18.

Translate the following binary IP address:

00001010.00001011.00001100.01100011

10.11.12.99

11.12.13.100

9.10.11.98

8.10.13.98

Correct answer: 10.11.12.99

To convert the binary to decimal, each position of the 1s needs to be added. By taking each position of the 1, and then referring to the chart below, you can add the values together to get the binary address.

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

19.

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.

20.

Which of the following is NOT an advanced security feature found in an NGFW?

Port-based filtering

Threat intelligence

Deep packet inspection

Application awareness

Correct answer: Port-based filtering

Traditional firewalls provide basic filtering of network traffic based on source or destination Internet Protocol (IP) addresses as well as port numbers. Port-based filtering is not an advanced feature of a Next-Generation Firewall (NGFW).

Threat intelligence includes information about potential security threats and how to mitigate them.

Deep Packet Inspection (DPI) involves the examination of the contents of network packets. DPI can be used for:

- *Data leak prevention*
- *Intrusion detection*
- *Identifying threats*

Application awareness is the ability to distinguish between specific applications.

21.

Which of the following is another term for a multilayer switch?

Layer 3 switch

Layer 2 switch

Layer 4 switch

Layer 5 switch

Correct answer: Layer 3 switch

A switch that works at more than one layer of the Open Systems Interconnection (OSI) model is called a multilayer switch. Multilayer switches are also referred to as layer 3 switches because of their ability to make forwarding decisions like a router.

22.

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+).

23.

Which of the following refers to the theoretical maximum rate at which data can be transmitted over a medium?

Speed

Throughput

Velocity

Pace

Correct answer: Speed

Speed is the theoretical maximum rate at which data can be transmitted over a medium. Speeds differ depending on industry standards. Ethernet Local Area Network (LAN) speeds are defined in 802.3 and wireless LAN speeds are defined in 802.11.

Throughput is the actual rate observed in a particular implementation. Throughput testers are used to determine the performance of network connections.

Velocity and pace are not used to describe network rates.

24.

Which of the following is a Layer 1 solution?

Media converter

Bridge

Switch

Router

Correct answer: Media converter

Media converters are used to transition from one transport medium to another, such as converting from fiber to Ethernet cable. This means that they operate at the Physical layer and are a Layer 1 solution.

Bridges, switches, and routers all work with MAC and IP addresses and operate at OSI levels 2 and above.

25.

A straight-through cable is used to connect which of the following?

Host to a switch

Switch to a switch

Hub to a hub

Hub to a switch

Correct answer: Host to a switch

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

A crossover cable, on the other hand, can be used to connect the following:

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

26.

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.

27.

Which of the following is NOT an advantage of using a switch rather than a hub?

Total cost of ownership

Increased functionality

Separate collision domains

Better security

Correct answer: Total cost of ownership

The total cost of ownership may be significantly lower with a hub. That may be a reason to use a hub rather than a switch, but you would miss out on all the features that switches offer.

Compared to hubs, switches provide:

- *Increased functionality*
- *Separate collision domains*
- *Better security*
- *Improved performance*
- *Scalability*
- *Increased efficiency*

28.

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.

29.

You are a systems administrator and need to access a Windows computer remotely and control it as if you were sitting right in front of it. Which of the following remote access methods allows you to do this?

RDP

SSH

SFTP

BYOD

Correct answer: RDP

The Remote Desktop Protocol (RDP) allows you to connect to a remote system as if you were sitting right in front of it at the remote location.

The Secure Shell Protocol (SSH) allows you to send commands to a remote system securely, but it would not allow you to control the device as if you were right in front of it like RDP would.

Secure File Transfer Protocol (SFTP) is a protocol that permits the transfer of files over a network, but it would not be used to connect to a device and control it.

Bring Your Own Device (BYOD) is a company policy whereby users are permitted to use their own network devices for work.

30.

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.

31.

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.

32.

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.

33.

Which layer of the three-tiered network architecture is MOST focused on security?

Distribution

Access

Edge

Core

Correct answer: Distribution

The distribution/aggregation layer is where most of the security functionality is deployed in a three-tiered network model.

While the access and core layers may have some security functionality, it is less of a focus.

The access layer is where end-user hosts are connected.

Edge is not a layer in the three-tiered model.

The core layer is also called the backbone.

Here is the three-tiered networking model:

- *Core layer*
- *Distribution layer*
- *Access layer*

34.

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.

35.

What is a rolled/rollover cable used for?

Connecting a host interface to a COM port

Connecting a switch with a fiber-optic port

Connecting a host to a switch

Connecting two COM ports together

Correct answer: Connecting a host interface to a COM port

A rolled/rollover cable is not used to connect Ethernet connections but to allow a host to communicate with a router through its console or communication (COM) port. This enables the user to program and configure the router directly, as opposed to using any Graphical User Interface (GUI) or software.

Fiber cables are used to connect to fiber-optic ports; no special cable is required. To connect a host to a switch, you would use a straight-through cable. You would not normally connect two COM ports together. A console communications (COM) port is used to connect a laptop to a device such as a switch or router in order to gain administrative access and control.

36.

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.

37.

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.

38.

What type of cable can be used to link a computer to a switch?

Straight-through cable

Crossover cable

Rollover cable

Straight cable

Correct answer: Straight-through cable

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

A crossover cable is used to connect a host to another host, a switch to another switch, or a host directly to a router.

A rollover cable is used for a host to interface with a router or switch's console COM port.

Straight cable is a fabricated term.

39.

Of the following, which is the software that resides on a single computer and seeks to detect potential attacks?

HIDS

APIDS

IPS

PPTP

Correct answer: HIDS

By definition, a Host Intrusion Detection System (HIDS) is an installed software package that monitors a single host for suspicious activity by analyzing events occurring within that host.

An Application Protocol-based Intrusion Detection System (APIDS) focuses on threats to applications that may be spread across multiple servers and protects an entire network. An Intrusion Prevention System (IPS) not only detects threats, it can also take actions to remedy them. The Point-to-Point Tunneling Protocol (PPTP) is an obsolete and insecure VPN protocol.

40.

Translate the following IP address to binary:

10.11.12.99

00001010.00001011.00001100.01100011

00101010.00011011.00001100.01100011

10001010.00001011.00001100.01101011

01101010.00001011.01101100.01100011

Correct answer: 00001010.00001011.00001100.01100011

The IP address 10.11.12.99 converts to 00001010.00001011.00001100.01100011.

The binary value 00101010.00011011.00001100.01100011 translates to 42.27.12.99.

The binary value 10001010.00001011.00001100.01101011 converts to 138.11.12.107.

The binary value 01101010.00001011.01101100.01100011 converts to 106.11.108.99.

The reverse of the binary-to-decimal process involves making comparisons against the chart below. For example, if the number is over 128, a 1 is placed at the beginning of the octet, then the remainder is compared against the chart again.

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

41.

An organization wants to ensure that whatever network topology they choose, a single connection break will not result in a breakdown of the entire network.

Which network topology should they avoid in this case?

Ring

Full mesh

Partial mesh

Dual-ring

Correct answer: Ring

Ring topologies, in some instances, have only one connection between two systems. This can result in what is known as a "single point of failure" (SPOF). A break in the connection can result in a disruption that compromises the entire ring topology. To prevent this, one can use a dual-ring topology.

A full mesh topology offers many physical paths between two devices, but can be expensive to implement.

A partial mesh will offer greater connectivity, but not as much as a full mesh.

A dual-ring topology is more fault-tolerant because it offers a backup communications route.

42.

A load balancer sits at which layer of a software-defined network?

Application layer

Control layer

Infrastructure layer

Spine layer

Correct answer: Application layer

The application layer implements the normal functions of a network, including load balancing.

The control layer interfaces between the application and infrastructure layers, implementing application-layer requests within the infrastructure layer. The infrastructure layer implements the physical network. Spine layer is a fabricated term.

43.

A hub can be described as which of the following?

Multiport repeater

Switched device

Router

Transparent bridge

Correct answer: Multiport repeater

A hub is considered a dumb device. It technically operates at the physical layer because it simply repeats signals received out to every port. This is why it's considered a multiport repeater, and because it simply replicates the bits out to every port, it interfaces directly with the medium.

A switched device operates at layer 2, the data link layer. Unlike a hub, a switch separates traffic into separate, unique collision domains for each port.

A router operates at layer 3 and performs different functions from a hub.

Like a switch, a transparent bridge separates collision domains and does not replicate bits out to every port.

44.

Which of the following does NOT support encryption protocols and CANNOT participate in an encrypted session?

Hub

Firewall

VPN concentrator

Router

Correct answer: Hub

A hub operates at layer 1, focuses on transferring bits, and has no support for encryption.

Enterprise firewalls, VPN concentrators, and routers all have the ability to support encryption algorithms (like AES) and operate at higher levels of the OSI model.

45.

A switch differs from a hub in which of the following ways?

It isolates portions of the network

It connects nodes to networks

It replicates network traffic to ports

It is used to connect network segments

Correct answer: It isolates portions of the network

A hub is capable of connecting network segments and hosts to the rest of the network as well as replicating data to its ports, but switches are capable of isolating network segments, as well. For example, when computers are within the same collision domain, it is possible for two computers to send traffic at the same time, causing a collision. Switches have individual collision domains for each port, negating this issue.

Both switches and hubs can connect nodes to networks, replicate network traffic to ports, and connect network segments.

46.

What is the maximum bandwidth of the wireless standard 802.11a?

54 Mbps

11 Mbps

2 Mbps

> 300 Mbps

Correct answer: 54 Mbps

The 802.11a WLAN standard has a maximum bandwidth of 54 Mbps. The 802.11g WLAN standard also has a maximum bandwidth of 54 Mbps.

The 802.11b WLAN standard has a maximum bandwidth of 11 Mbps. The 802.11 standard, the original WLAN standard, had a maximum bandwidth of 2 Mbps. The 802.11n WLAN standard has a maximum bandwidth greater than 300 Mbps.

47.

A Shielded Twisted Pair (STP) cable has all of the following attributes, EXCEPT:

Issues with EMI

Metallic shield

Protection from external EMI

Individually insulated wires

Correct answer: Issues with EMI

The S in STP refers to the fact that the wires are twisted with a piece of foil. This helps to block Electromagnetic Interference (EMI), making it ideal for EMI-prone environments.

An STP cable has a metallic shield placed around it.

An STP cable is also protected from EMI.

Both STP and Unshielded Twisted Pair (UTP) cables have individually insulated wires.

48.

Which of the following is a private IP address?

192.168.1.1

192.169.1.1

169.03.02.14

171.16.0.1

Correct answer: 192.168.1.1

Of those listed, only 192.168.1.1 falls within the following private IPv4 address ranges:

- *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*

49.

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.

50.

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.

51.

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.

52.

Of the following copper connector types, which is an eight-pin connector used most often in Ethernet networks?

RJ-45

F connector

RJ-11

DB-9

Correct answer: RJ-45

The RJ-45 connector is the most ubiquitous connection for Ethernet, especially in the home. Store-bought Ethernet cables come with the connector, though it is possible to make your own when purchasing the cable and connectors in bulk.

The F connector, or F-type connector, is used to attach coaxial cables commonly used in cable TV or video connections.

An RJ-11 connector has four wires and it's commonly used to connect phones.

A DB-9 connector is used for computer peripheral devices.

53.

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.

54.

What does the protocol MPLS stand for?

Multiprotocol Label Switching

Multiple Policy Label System

Multiprotocol Layer Switching

Multiposition Layer System

Correct answer: Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS) is a switching mechanism that puts labels on data and then uses those labels to forward the data when it reaches the MPLS network.

The other three responses are incorrect.

55.

What kind of firewall examines traffic exiting an inside network as it proceeds out to the internet and enables return traffic belonging to that session to get back through?

Stateful

Packet filtering

Perimeter

NAT

Correct answer: Stateful

A firewall uses a set of predefined rules to determine if traffic should be permitted to enter or leave a protected network or be blocked from doing so. Stateful firewalls keep track of the state of a network session, enabling it to permit legitimate packets from a session but block packets that are not valid in context, such as a TCP SYN/ACK without a preceding SYN. Stateful firewalls can be used to permit outbound connections while blocking inbound ones.

Packet filtering firewalls inspect packet headers and permit or deny traffic based on predefined rules such as permitting certain IP addresses or protocols. Packet filtering is performed by both stateless and stateful firewalls.

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

Network Address Translation (NAT) converts internal, private IP addresses to publicly routable IP addresses at the network boundary. This allows a many-to-one relationship between internal and external addresses.

56.

A transport layer protocol will be encapsulated within packets at which layer of the Open Systems Interconnection (OSI) model?

Layer 3

Layer 4

Layer 2

Layer 5

Correct answer: Layer 3

The transport layer is Layer 4 of the Open Systems Interconnection (OSI) model. Layer 4 packets will be encapsulated within Layer 3 packets.

In the transmission of data over a network, information (in the form of Protocol Data Units, or PDUs) passes through succeeding layers of the OSI model from the origin to the destination. Encapsulation or de-encapsulation of PDUs occurs between each layer. Data that starts at Layer 7, the application layer, will become encapsulated into datagrams, and information will move downward through each layer of the process. At the destination, the reverse process will occur, from the physical layer to the application layer.

In other words, datagrams are encapsulated into packets, which are then encapsulated into frames. Frames are encapsulated into bits and the data is then sent to the destination where de-encapsulation occurs.

The seven layers of the OSI model with their associated PDUs are:

- *Layer 7 - Application - Datagrams*
- *Layer 6 - Presentation Datagrams*
- *Layer 5 - Session - Datagrams*
- *Layer 4 - Transport - Segments*
- *Layer 3 - Network - Packets*
- *Layer 2 - Data link - Frames*
- *Layer 1 - Physical - Bits*

57.

Of the following, which protocol helps control a VoIP gateway?

SIP

SDN

POTS

STP

Correct answer: SIP

Session Initiation Protocol (SIP) is a signaling protocol that supports VoIP gateways to transmit voice traffic. Voice over Internet Protocol (VoIP) transmits voice data (i.e., phone calls) over an IP network. When combined with data and video transfer, this is called Unified Communications (UC). Other protocols that support VoIP gateways include Media Gateway Control Protocol (MGCP) and Lightweight Telephony Protocol (LTP).

Software-Defined Networking (SDN) uses software controllers for network infrastructure.

Plain Old Telephone System (POTS) is another name for the traditional analog phone network.

Spanning Tree Protocol (STP) stops loops in a network.

58.

Which of the following is NOT a feature of IPsec?

Broadcast

Integrity

Anti-replay

Authentication

Correct answer: Broadcast

Internet Protocol Security (IPSec) does not support either IP broadcast or IP multicast.

Integrity, anti-replay, and authentication are all features of IPSec.

IPSec is a key component of Virtual Private Networks (VPNs). IPSec uses two primary security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). The five components of ESP are:

- *Confidentiality (encryption)*
- *Data Integrity*
- *Authentication*
- *Anti-Replay Service*
- *Traffic flow*

As shown above, IPsec fulfills the CIA triad:

- ***Confidentiality:** Encryption protects the privacy of data and ensures that it cannot be read by anyone without the encryption keys.*
- ***Integrity:** Integrity protections, provided by checksums, ensure that data has not been modified in transit.*
- ***Authentication:** Authentication protections verify the identities of both parties in a conversation.*

59.

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.

60.

Which cloud service model enables an end user's applications and data to be hosted securely within a cloud data center?

DaaS

SaaS

PaaS

IaaS

Correct answer: DaaS

Desktop as a Service (DaaS) hosts end users' desktops (including data and applications) within a cloud data center.

Software as a Service (SaaS) provides customers with access to applications developed and hosted by the cloud provider. Platform as a Service (PaaS) offers a managed environment for an organization's applications. Infrastructure as a Service (IaaS) provides a platform for a customer to install their own operating system.

61.

A software developer would like to use the cloud to generate code without dealing with any infrastructure. Which cloud service model would meet that requirement?

PaaS

HaaS

NaaS

SaaS

Correct answer: PaaS

Platform as a Service (PaaS) is a service-based model where a service provider gives customers access to a managed environment in which they can deploy code without worrying about managing the environment themselves.

Hardware as a Service (HaaS) is a service-based model for leasing hardware components.

Network as a Service (NaaS) offerings enable a company to lease virtualized network infrastructure from their service provider.

Software as a Service (SaaS) provides customers with access to software solutions (such as Google Docs or Microsoft 365) under a service-based model.

62.

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.

63.

What is the equivalent IP address for the following binary address?

00001010.00000000.00000000.00000001

10.0.0.1

192.168.0.1

12.0.0.1

127.0.0.1

Correct answer: 10.0.0.1

To convert binary to decimal, each position of the 1s needs to be added. By taking each position of the 1, and then referring to the chart below, you can add the values together to get the decimal address.

The equivalent to 00001010.00000000.00000000.00000001 is 10.0.0.1.

The equivalent to 11000000.10101000.00000000.00000001 is 192.168.0.1.

The equivalent to 00001100.00000000.00000000.00000001 is 12.0.0.1.

The equivalent to 01111111.00000000.00000000.00000001 is 127.0.0.1.

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

64.

Of the following, which is NOT another name for a Media Access Control (MAC) address?

Multicast address

Ethernet address

Physical address

Hardware address

Correct answer: Multicast address

A Media Access Control (MAC) address is often called a hardware, Ethernet, or physical address, but it is not a multicast address.

A multicast address is used in situations where packets need to be forwarded to multiple nodes. When configured, a multicast address will take packets it receives and send them to multiple configured destinations.

Ethernet operates at the data link layer of the OSI model. Ethernet MAC addresses are written in hexadecimal.

A MAC address is normally linked to a physical component, so it is sometimes referred to as a physical address.

The term hardware address is also associated with MAC address.

65.

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.

66.

What is the maximum transmission distance of 1000Base-T?

100 m

10 km

40 km

300 m

Correct answer: 100 m

1000Base-T uses UTP as its media type, has a bandwidth capacity of 1000 Mbps, and has a distance limitation of 100 m.

Ethernet physical layer standards are found in IEEE 802.3. The maximum transmission distances vary with each standard.

A maximum distance of 10 km applies to 10GBaseLR and 10GBaseLW.

Both 10GBaseER and 10GBaseEW have a maximum distance of 40 kilometers.

10GBaseSR has a maximum distance of 300 meters.

67.

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.

68.

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.

69.

Which of the following is TRUE?

Telnet is a command-line tool.

Telnet operates on TCP port 22.

Telnet is a secure protocol and was developed as a replacement for SSH.

You do not need a username or password to access a Telnet server.

Correct answer: Telnet is a command-line tool.

Telnet is a command-line tool that runs on port 23. It is insecure and has been replaced by SSH but does require a username and password.

70.

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*

71.

Which of the following is NOT a type of WAN?

PAN

Cloud

Internet

LTE

Correct answer: PAN

A Personal Area Network (PAN) is neither a Local Area Network (LAN) nor a Wide Area Network (WAN). A typical PAN might use Bluetooth to connect a laptop, smartphone, and a set of earphones for a single individual.

A cloud network is a type of WAN that uses virtual devices and may be accessible worldwide.

The public Internet is considered a distributed WAN.

Long-Term Evolution (LTE) is a cellular WAN that is associated with Fourth-Generation (4G) wireless telephony.

72.

Which of the following statements regarding the protocol Secure Shell (SSH) is FALSE?

SSH sends data in plain text.

SSH is a more secure option than Telnet.

SSH is a command-line tool.

SSH operates on port 22.

Correct answer: SSH sends data in plain text.

Unlike Telnet, which does not offer any encryption, Secure Shell (SSH) does not send data in plain text. This makes it a more secure alternative to Telnet.

SSH is a command-line tool, just like Telnet, that operates on port 22. The main difference between SSH and Telnet is that SSH adds an additional layer of security.

73.

Which type of network uses baseband?

LAN

WAN

SAN

WLAN

Correct answer: LAN

Local Area Networks (LANs) use baseband, which uses all of the bandwidth of the physical media for a single signal.

Broadband uses multiple frequency bands and can carry many signals at once.

Wide Area Networks (WANs) use broadband connections, such as cable broadband, Digital Subscriber Line (DSL), and satellite.

A Storage Area Network (SAN) is dedicated to the storage of data and is separated from the LAN.

Wireless Local Area Network (WLAN) is not simply a baseband technology; it sends radio signals, and baseband is usually thought of as a wired technology.

74.

Which of the following is a stripped-down version of File Transfer Protocol (FTP), providing quick transfer speeds?

TFTP

SFTP

microFTP

QFTP

Correct answer: TFTP

The Trivial File Transfer Protocol (TFTP) is a simpler and less secure version of FTP.

Secure File Transfer Protocol (SFTP) is a secure FTP protocol that uses Secure Shell (SSH). It is a full file transfer program, unlike FTP.

MicroFTP is an FTP client program.

QFTP is a file transfer protocol written in the Qt programming framework.

75.

What type of firewall filters traffic by only inspecting packet headers?

Packet filtering

Stateful

Perimeter network

NAT

Correct answer: Packet filtering

A firewall uses a set of predefined rules to determine if traffic should be permitted to enter or leave a protected network or blocked from doing so. Packet-filtering firewalls inspect packet headers and permit or deny traffic based on predefined rules such as permitting certain IP addresses or protocols.

Stateful firewalls keep track of the state of a network session, enabling it to permit legitimate packets from a session but block packets that are not valid in context, such as a TCP SYN/ACK without a preceding SYN. Stateful firewalls can be used to permit outbound connections while blocking inbound ones.

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.

Network Address Translation (NAT) converts internal, private IP addresses to publicly-routable IP addresses at the network boundary. This allows a many-to-one relationship between internal and external addresses.

76.

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.

77.

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.

78.

You need to divide the 192.168.1.0/24 network into eight equal-sized subnets while maximizing the size of each. Which of the following is one of the subnets that you will create?

192.168.1.128/27

192.168.1.128/26

192.168.5.97/27

192.168.5.160/26

Correct answer: 192.168.1.128/27

The creation of eight subnets requires three borrowed bits (2^3=8). This will create a 27-bit subnet mask (255.255.255.224). In this case, the "interesting octet" is the last one, so the block size is 256-224=32. Therefore, the eight possible subsets are:

192.168.1.0/27

192.168.1.32/27

192.168.1.64/27

192.168.1.96/27

192.168.1.128/27

192.168.1.160/27

192.168.1.192/27

192.168.1.224/27

The subnet 192.168.1.128/26 is one of the possible subnets, but a /26 network would yield four possible subnets instead of eight. The four possible subnets would be:

192.168.1.0/26

192.168.1.64/26

192.168.1.128/26

192.168.1.192/27

192.168.5.97/27 would not be a subnet of 192.168.1.0/24.

192.168.5.160/26 would not be a subnet of 192.168.1.0/24.

79.

Which of the following enables administrators to perform maintenance on a web server without services going down?

Load balancing

Multipathing

Backup

API gateway

Correct answer: Load balancing

Load balancing stores identical content on multiple web servers and distributes requests across them. This enables maintenance on a single web server without bringing down the service.

Multipathing provides a backup path for connectivity between network hosts and storage devices.

Backup prevents loss of data, but it does not provide real-time redundancy in case of device failure or administrative maintenance.

An Application Programming Interface (API) gateway manages the calls and requests from application users to backend services.

80.

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*

81.

Which of the following is NOT a factor used by load balancers?

Dynamic performance metrics

Response time

Weighted percentage

Server status

Correct answer: Dynamic performance metrics

Load balancers may take into account server health checks, but real-time performance metrics are beyond their scope.

Response time from configured servers is a consideration of load balancing.

Load balancing aims to distribute traffic evenly, but you can assign weighted percentages to servers to manage distribution.

Health checks can provide server status information to load balancers, such as whether one has gone down.

82.

A team of network engineers is designing a new network for their client. One engineer is recommending a star network topology, and another engineer believes they need to choose a mesh network instead.

What is one advantage of a mesh network topology?

Fault tolerance

Load balancing

Error correction

Less expensive

Correct answer: Fault tolerance

A mesh topology connects each device with all other devices. In this way, each device can connect to the others despite breaks in connection on one specific line. The disadvantage of mesh networks is cost; they require more cables and connectors.

Load balancing is used to provide redundant connectivity to multiple devices, such as servers. The term does not describe network topology.

The use of a mesh network does not provide error correction.

A mesh network is generally more expensive than other network topologies because connections are required between each device.

83.

What is the most commonly used Virtual Private Network (VPN) protocol that supports HTTPS?

TLS

PPTP

L2TP

IPsec

Correct answer: TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which has mostly replaced SSL, provide Confidentiality, Integrity, and Authentication (CIA) protection for Layers 5 through 7 of the Open Systems Interconnection (OSI) model. Hypertext Transfer Protocol Secure (HTTPS) is a secure web browser protocol that uses TLS.

Many VPN providers include TLS in their offerings, along with PPTP, IPSece, and L2TP.

Point-to-Point Tunneling Protocol (PPTP) is an older protocol rarely used today. PPTP is not associated with HTTPS.

Layer Two Tunneling Protocol (L2TP) is an extension of PPTP.

Internet Protocol Security (IPsec) is a security protocol that can be used in either tunneling or transport mode. IPSec is not normally used in conjunction with HTTPS.

84.

Which cloud model might be used to support collaboration between multiple organizations within the same industry?

Community cloud

Public cloud

Private cloud

Hybrid cloud

Correct answer: Community cloud

A community cloud is created by a group of organizations to support a common goal.

A public cloud is hosted by a third-party provider. A private cloud is hosted on dedicated infrastructure for a company's own use. A hybrid cloud combines public and private cloud offerings.

85.

Of the following security solutions, which consists of software that will monitor applications and logs on one computer in order to detect known attacks?

HIDS

PIDS

APIDS

IPS

Correct answer: HIDS

A Host-based Intrusion Detection System (HIDS) runs on one computer and will monitor the host rather than simply the network traffic. A HIDS will monitor applications and logs to identify vulnerabilities.

A Protocol-based Intrusion Detection System (PIDS) monitors one protocol on one server. An Application Protocol-based Intrusion Detection System (APIDS) monitors servers running the same application. An Intrusion Prevention System (IPS) not only monitors networks for malicious activity, it can also take corrective action.

86.

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.

87.

Which of the following is the IPv6 equivalent to Automatic Private IP Addressing (APIPA)?

Link-local addresses

APIPAv6

Multicast

Unicast

Correct answer: Link-local addresses

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.

APIPAv6 is a fabricated term.

IPv4 and IPv6 multicast addresses are "one to many" addresses. Multicast works by sending data to an IP multicast group address then routers forward the data to all devices subscribed to that address. Multicast is designed to send a packet to multiple different interfaces with a single address.

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

88.

Of the following, which is a wavelength of multimode fiber?

850 nm

1350 nm

1310 nm

1550 nm

Correct answer: 850 nm

Most Multimode Fiber (MMF) cables transmit on wavelengths from 850 nm to 1300 nm.

1350 nm is a wavelength of Single-Mode Fiber (SMF), which transmits on wavelengths from 1310 nm to 1550 nm.

1310 nm is a wavelength of SMF.

1550 nm is a wavelength of SMF.

89.

Which of the following wireless standards uses the DSSS transmission method?

802.11b

802.11a

802.11ac

802.11ax

Correct answer: 802.11b

Of the options given, only 802.11b uses the Direct-Sequence Spread Spectrum (DSSS) transmission method.

802.11a and 802.11ac use the Orthogonal Frequency-Division Multiplexing (OFDM) transmission method.

802.11ax uses Orthogonal Frequency-Division Multiple Access (OFDMA). OFDM is designed for a single user, while OFDMA is designed for multiple users.

90.

Which of the following terms is associated with routing?

Packet switching

Circuit switching

Message switching

Frame switching

Correct answer: Packet switching

Routing involves the selection of a connection path through a network. Routers also perform packet switching, which is the forwarding or filtering of Layer 3 network packets. Sometimes the terms routing and packet switching are used interchangeably.

Circuit switching makes use of dedicated circuits to divide and forward traffic through a connection. The traditional Plain Old Telephone System (POTS) used circuit switching.

Message switching uses an entire message to store and forward data. Email is an example of message switching.

Frame switching is the forwarding of Ethernet frames on Layer 2, the data link layer. Frame Relay is a frame switching protocol.

91.

Traffic over which of the following ports is an indication of INSECURE network traffic?

23

22

443

587

Correct answer: 23

23 is the port assigned to Telnet, which is an insecure protocol for remotely accessing a system.

Port 22 is SSH, which is a secure alternative to Telnet. Port 443 is used by HTTPS for TLS-encrypted web traffic. Port 587 is used by TLS-encrypted SMTP email traffic.

92.

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.

93.

You have been asked to implement IPv6 in all of a client's network devices. All devices currently have IPv4 addresses, but those IP addresses should remain. The customer would like to complete the upgrade gradually.

Which migration strategy would you recommend?

Dual stack

Teredo

6to4

ISATAP

Correct answer: Dual stack

Dual stack is the most common strategy for migration to Internet Protocol version six (IPv6). It allows communication using either IPv4 or IPv6, and the strategy allows applications and devices to be upgraded one at a time.

Teredo allows IPv6 devices to connect to an IPv4 network. It does so by encapsulating IPv6 packets within IPv4 user packets.

6to4 tunneling allows IPv6 traffic to tunnel through an IPv4 network.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is a similar tunneling protocol.

94.

What is the term for the configuration settings of a device deviating from defaults over time?

Configuration drift

Configuration mismanagement

Configuration deviation

Configuration normalization

Correct answer: Configuration drift

Configuration drift is when configuration settings move away from defaults over time. Ansible and similar tools can help to prevent and manage configuration drift.

Configuration mismanagement, deviation, and normalization are fabricated terms.

95.

In which of the following services does a service provider enable developers to develop, use, and deploy software to computing platforms hosted, owned, and maintained by the provider without the need to think about hardware requirements?

PaaS

SaaS

HaaS

NaaS

Correct answer: PaaS

Platform as a Service (PaaS) enables developers and coders to use a computing environment without concern for hardware compatibility or capability. The developers can push the deployment to the platform, and the computing platform takes over to create the proper interfaces to provide a functional application that is ready to use.

Software as a Service (SaaS) enables users to access online applications without dealing with any underlying infrastructure at all. Examples include Yahoo! Mail and Google Docs.

Hardware as a Service (HaaS) enables customers to use equipment owned by a provider without dealing with capital expenditures.

Network as a Service (NaaS) gives customers the use of networks offered by cloud providers.

96.

Which of the following allows strategic performance optimization for particular types of network traffic?

Quality of service

Quality assurance

Network load management

Load balancing

Correct answer: Quality of service

Quality of Service (QoS) is a set of tools used to improve network performance for certain types of traffic. Often, this is used to ensure that latency-sensitive protocols (such as teleconferencing) have the performance that they need even in congested environments. This is accomplished by prioritizing this traffic over less-important traffic (such as social media).

Quality assurance is not the correct term for this issue.

Network load management may refer to the way load balancers can be managed to balance network traffic. However, it would not distinguish between types of traffic.

The same is true for the incorrect answer load balancing.

97.

IEEE 802.11i offers improved security for wireless networks. Which wireless standard implements it?

WPA2

WEP

WPA

TKIP

Correct answer: WPA2

802.11i was implemented in Wi-FiProtected Access 2 (WPA2) to provide improved security over Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

802.11i uses an Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher.

Temporary Key Integrity Protocol (TKIP) is a wireless encryption method that was designed by the 802.11i task force.

98.

What is the name for the process of routing MPLS frames through the MPLS cloud?

Label switching

Frame switching

Circuit switching

Route switching

Correct answer: Label switching

Label switching uses Multiprotocol Label Switching (MPLS) labels to route frames through a service provider's MPLS cloud.

Frame switching is the process of forwarding frames based on source or destination Media Access Control (MAC) addresses in frames. Frame Relay is considered a type of frame switching.

Circuit switching requires an established connection to transfer data. Examples of circuit switching are the traditional telephone system and dial-up networking connections. It is considered less efficient than modern switching technologies.

Routing and switching are two separate processes. Routing takes place at Layer 3 while switching operates on Layer 2. Routing can take place between two Local Area Networks (LANs) or between Virtual LANs (VLANs) using Layer 3 packet forwarding.

99.

Translate the following binary IP address:

10101100.00010000.00010100.00110111

172.16.20.55

152.42.51.66

152.55.42.11

172.17.21.56

Correct answer: 172.16.20.55

To convert the binary to decimal, each position of the 1s needs to be added. By taking each position of the 1, then referring to the chart below, you can add the values together to get the binary address.

The binary equivalent for 152.42.51.66 is 10011000.00101010.00110011.01000010.

The binary equivalent to 152.55.42.11 is 10011000.00110111.00101010.00001011.

The binary equivalent to 172.17.21.56 is 10101100.00010001.00010101.00111000.

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