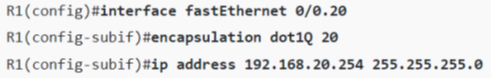
Advanced Networking

MCQs

1. Version 6 of IP address has how many bits.
2. 64 bits
3. 128 bits
4. 32 bits
5. 256 bits
6. Given an IP address 172.16.28.252 with a subnet mask of 255.255.240.0, what is the correct

network address?

1. 172.16.16.0
2. 172.16.0.0
3. 172.16.24.0
4. 172.16.28.0
5. Which IPv6 address is the equivalent of the IPv4 interface loopback address 127.0.0.1?
6. ::1
7. ::
8. 2000::/3
9. 0::/10
10. Which command enables IPv6 forwarding on a Cisco router?
11. ipv6 local
12. ipv6 host
13. ipv6 unicast-routing
14. ipv6 neighbor
15. What is known as "one-to-nearest" addressing in IPv6?
16. global unicast
17. anycast
18. multicast
19. unspecified address
20. What is the network mask for n=13?
21. 255.247.0.0
22. 255.246.0.0
23. 255.248.0.0
24. 255.249.0
25. Which of following statement is incorrect?
26. The role of prefix is defining the network to which the host belongs
27. In subnetting, the value of prefix is always less than the value of the prefix of the original network
28. In CIDR, the prefix is always added to the address separated by a slash
29. In the network mask, the rightmost 32-n bits are set to 0's
30. Which of these addresses cannot be used as source address?
31. 0.0.0.0
32. 255.255.255.255
33. 192.168.1.7
34. 172.16.0.1
35. You are the new IT admin, and you need to find the network configuration. What should you use?
36. ipconfig
37. cmd
38. netchange
39. newnet
40. To get the most detailed network configuration, use this command.
41. ipconfig /all
42. ipconfig
43. ipconfig /renew
44. ipconfig /most
45. This command sends a request out and expects a response, indicating that both hosts are communicating.
46. ping
47. tracert
48. ipconfig /renew
49. nslookup
50. If you wanted to ping a host but also follow the path at which it pings, what would you use?
51. tracert
52. ping
53. tracert /ping
54. ipconfig /most
55. The IP network 192.168.50.0 is to be divided into 10 equal sized subnets. Which of the following subnet masks can be used for the above requirement?
56. 255.243.240
57. 255.255.0.0
58. 255.255.255.0
59. 255.255.255.255
60. Which of the following is correct IPv4 address?
61. 124.201.3.1.52
62. 300.142.210.64
63. 10110011.32.16.8
64. 128.64.0.0
65. What IP address class allocates 8 bits for the host identification part?
66. Class A
67. Class B
68. Class C
69. Class D
70. Default Administrative Distance Value of RIP routing Protocol is:
    1. 0
    2. 1
    3. 100
    4. 120
71. MPLS in WAN Technologies expands to:
    1. Multiprotocol Label Switching
    2. Mono-protocol Label Switching
    3. Multiple Protocol Layer Switching
    4. Monotonous Protocol Layer Subnetting
72. Which of the following is TRUE for etherchannel protocols?
    1. PAgP is a Cisco proprietary protocol for Ether Channel.
    2. LACP is a Cisco proprietary protocol for Ether Channel.
    3. LACP is an open-source IEEE 802.1ad standard.
    4. PAgP is an open-source IEEE 802.1ad standard.
73. Which of the following is TRUE for Router-on -stick inter VLAN routing?
    1. Each VLAN is connected to a different physical router interface.
    2. Large networks with large number of VLANs require many router interfaces.
    3. Logical sub interfaces are created, one sub-interface per VLAN.
    4. IP routing needs to be enabled.
74. \_\_\_\_\_\_\_\_\_ is one way to set up a direct point-to-point connection across a network, for the purpose of simplifying connections between separate networks.
    1. CDP
    2. PgDP
    3. LACP
    4. GRE
75. If one needs to pass traffic over an incompatible network, a \_\_\_\_\_\_ should be implemented.
    1. VPN
    2. GRE Tunnel
    3. VLAN
    4. PAN



The above set of commands are part of:

1. Legacy inter VLAN routing
2. Router-on-a-stick inter VLAN routing
3. Multilayer switch inter VLAN routing
4. Difficult VLAN routing
5. Administrative distance is used to rate routing protocol’s:
   1. Time management
   2. Trustworthiness
   3. Path selection criteria
   4. Ip address management
6. A default administrative distance value 0 denotes:
   1. Static route out an interface
   2. Static route to a next-hop
   3. Connected interface
   4. IGRP
7. Which of the following is NOT a part of WAN optimization?
   1. Compression
   2. Protocol optimization
   3. Traffic shaping
   4. No caching
8. An \_\_\_\_\_\_\_\_ is a data communications technique in which software is used to create virtual networks on top of another network, typically a hardware and cabling infrastructure.
   1. Overlay network
   2. Partial Network
   3. Relay Network
   4. Underlay Network
9. PoS in WAN technologies expands to:
   1. Packet over SONET
   2. Process of SDWAN
   3. Packet of Successful delivery
   4. Process of Synchronization
10. The correct order of Configuring PAP Authentication on WAN interface is:
    1. Step 1 is ‘creating the account’

Step 2 is ‘assigning the credentials’

Step 3 is enabling PAP

* 1. Step 1 is enabling PAP

Step 2 is ‘assigning the credentials’

Step 3 is ‘creating the account’

* 1. Step 1 is ‘assigning the credentials’

Step 2 is enabling PAP

Step 3 is ‘creating the account’

* 1. Step 1 is enabling PAP

Step 2 is ‘creating the account’

Step 3 is ‘assigning the credentials’

1. In Point-to-Point Protocols, which authentication protocol is encrypted one:
   1. PAP
   2. CHAP
   3. PaGP
   4. LACP
2. In Dynamic Trunking Protocol, which of the following settings on the two connecting switches will not result in a TRUNK port?
   1. S1: Dynamic desirable, S2: Dynamic desirable
   2. S1: Dynamic Auto, S2: Access
   3. S1: Dynamic Auto, S2: Trunk
   4. S1: Dynamic Auto, S2: Dynamic desirable
3. The device router, bridge, Gateway are used in which of the following layers of OSI reference model:

a) Layer -2, Layer-1 and Layer-5

b) Layer-3, Layer-2, Layer-7

c) Layer-1,Layer-3,Layer-5

d) Layer-7, Layer-2,Layer-3

1. To deliver a message to the correct application program running on a host, the \_\_\_\_\_\_\_ address must be consulted.

a. port

b. IP

c. physical

d. None of the above

1. Transmission media lie below the \_\_\_\_\_\_\_ layer.

a. physical

b. network

c. transport

d. application

1. One of the responsibilities of the transport layer protocol is to create a \_\_\_\_\_\_ communication.

a. host-to-host

b. process-to-process

c. node-to-node

d. none of the above

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a method of implementing a telecommunication network in which two network nodes establish a dedicated communication channel before the nodes communicate with each other
   1. Packet switching
   2. Message switching
   3. Circuit Switching
   4. End-to-end transmission
2. What is the size of MAC Address?

a) 16-bits

b) 32-bits

c) 48-bits

d) 64-bits

1. The 8-bit field in IPv4 header which controls the maximum number of routers visited by the datagram during its lifetime
2. VER
3. Header length
4. Payload
5. Time to live (TTL)
6. Which of the following is a wireless LAN standards?

a) IEEE 802.11

b) IEEE 609.12

c) IEEE 803.14

d) IEEE 809.10

1. Which of the following is a wireless WAN standard?

a) IEEE 802.11

b) IEEE 609.12

c) IEEE 803.14

d) IEEE 802.16

40. Authentication mechanisms use \_\_\_\_\_\_\_\_\_\_ qualities to confirm a user's identity

* 1. Something the **user knows**.
  2. Something the **user has**
  3. Something the **user is**
  4. All of the above

1. During computer communication in a network the following two key words are transmitted: 1 1 0 1 0 1 1 0 and 0 0 0 0 1 1 0 0.

After Mod 2 operation what is the final key word received is \_\_\_\_\_\_\_\_\_\_\_\_\_

1. Bit stuff the following payload:

100000111111111110000010101010101111111111000111111111111111000

42) A class A network on the internet has a subnet mask of 255.255.224.0. What is the maximum number of subnets connected

a) 4 b)6 **c) 8** d) 10

43) In the label header of MPLS the no.of bits allocated for TTL are:

**a)8** b)6 c)16 d)32

44) VPN stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

45) DNS uses port no. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_during internet operations

a)50 b)25 c)80 **d)53**

46) DHCPv4 assigns IPv4 addresses and other network configuration information \_\_\_\_\_\_\_\_\_\_\_

**a) Dynamically** b) Static c)both static & dynamic d)None of the above

47) DHCPv4 server sends the binding \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_message to the requesting client as a unicast.

a)DHCPDISCOVER b)DHCPREQUEST **c) DHCPOFFER** d)DHCPACK

48) OSI reference model follows which type of approach:\_\_\_\_\_\_\_\_\_\_

**a) Top to bottom** b) Bottom to top c) Horizontal d) Vertical

1.

Which of the following is not a characteristic of a VPN?

A.It is a secure network

B.It is deployed over a shared infrastructure

C.It may use tunneling techniques

D.It does not provide any cost savings to alternate connectivity options

Correct Answer

D. It does not provide any cost savings to alternate connectivity options

Explanation

A VPN is a secure network that allows users to access and transmit data over a shared infrastructure. It achieves this by using tunneling techniques, which encapsulate data packets within another protocol. One of the advantages of using a VPN is that it can provide cost savings compared to alternate connectivity options, such as leased lines or dedicated networks. Therefore, the statement "It does not provide any cost savings to alternate connectivity options" is not a characteristic of a VPN.

2. What would be a good characterization of a VPN tunnel established between a telecommuter's PC using a VPN client software and a VPN Concentrator at the HQ location?

A.Remote access VPN

B.Site to site VPN

C.Extranet VPN

D.LAN to LAN VPN

Correct Answer

A. Remote access VPN

A good characterization of a VPN tunnel established between a telecommuter's PC using a VPN client software and a VPN Concentrator at the HQ location would be a remote access VPN. This type of VPN allows remote users to securely connect to a private network over the internet, providing them with access to resources and services as if they were directly connected to the network at the HQ location.

3. Which of the following may be used as a terminating point for a site to site VPN tunnel?

A.Router

B.Firewall

C.Concentrator

D.All of the above

Correct Answer

D. All of the above

Explanation

All of the above options, including router, firewall, and concentrator, can be used as terminating points for a site-to-site VPN tunnel. A router is commonly used to establish VPN connections between two networks, while a concentrator is a specialized device designed for managing multiple VPN connections. Therefore, any of these options can serve as a termination point for a site-to-site VPN tunnel.

4. Which of the following is not a Layer 2 tunneling protocol?

A.PPTP

B.IPSEC

C.L2TP

D.L2F

Correct Answer

B. IPSEC

Explanation

IPSEC is not a Layer 2 tunneling protocol. It is actually a Layer 3 protocol that provides secure communication over the Internet. Layer 2 tunneling protocols, on the other hand, are used to create virtual tunnels for transmitting data between two network endpoints. PPTP, L2TP, and L2F are all examples of Layer 2 tunneling protocols that are commonly used for VPN (Virtual Private Network) connections.

5. Which of the following security techniques provide confidentiality (data privacy) service?

A.Key exchange

B.Encryption

C.All of the above

D.Hashing

Correct Answer

B. Encryption

Explanation

Encryption is a security technique that provides confidentiality or data privacy service. It involves converting plain text into cipher text using an algorithm and a key. This ensures that only authorized individuals can access and understand the information, as the cipher text is unreadable without the key. Encryption is widely used to protect sensitive data during transmission or storage, preventing unauthorized access and maintaining the confidentiality of the information.

6. DES, 3DES, and AES are examples of encryption algorithms that use the same key for encryption and decryption. Such encryption algorithms are categorized as:

A.Asymmetrical encryption

B.Symmetrical encryption

C.Secure Hash Function

D.Public Key Infrastructure

Correct Answer

B. Symmetrical encryption

Explanation

Symmetrical encryption algorithms, such as DES, 3DES, and AES, use the same key for both encryption and decryption processes. In symmetrical encryption, the sender and receiver share a common secret key, which is used to encrypt the data at the sender's end and decrypt it at the receiver's end. This type of encryption is efficient and faster compared to asymmetrical encryption, where different keys are used for encryption and decryption. Therefore, the given answer categorizing these encryption algorithms as symmetrical encryption is correct.

7. Which of the following is not true about DES, 3DES and AES?

A.DES has the least cryptographic strength

B.3DES is strong but has high CPU overhead

C.AES offers a good balance of cryptographic strength and CPU overhead

D.AES has export restrictions associated with it

Correct Answer

D. AES has export restrictions associated with it

Explanation

AES does not have export restrictions associated with it. This means that AES can be freely used and distributed without any limitations or restrictions imposed by governments or regulatory bodies. DES, on the other hand, has the least cryptographic strength, meaning it is the least secure among the three encryption algorithms mentioned. 3DES is strong but has high CPU overhead, which means it requires more computational resources to perform encryption and decryption compared to AES.

8. What do you call a cryptographic function that has the following features: - Takes a variable-sized message as input and produces a fixed-length output - The output will be identical for an identical input - A one-way function that is difficult to reverse (invert)

A.Encryption

B.Key Exchange

C.Hashing

D.Scrambling

Correct Answer

C. Hashing

Explanation

A cryptographic function that takes a variable-sized message as input and produces a fixed-length output is called hashing. The output of the hashing function will always be the same for an identical input, making it useful for verifying data integrity. Additionally, hashing is a one-way function that is difficult to reverse or invert, providing security for sensitive information.

9. Hashing functions like MD5 and SHA are used in IPSEC to provide which of the following services:

A.Data confidentiality (privacy from eavesdropping)

B.Data Integrity (data protected from being changed during transit)

C.Securely negotiating a key over a unsecure media

D.Anti replay protection

Correct Answer

B. Data Integrity (data protected from being changed during transit)

Explanation

Hashing functions like MD5 and SHA are used in IPSEC to provide data integrity. These functions generate a unique hash value for a given set of data. This hash value acts as a digital signature for the data, ensuring that it has not been altered during transit. By comparing the received hash value with the calculated hash value, the recipient can verify the integrity of the data. Therefore, the use of hashing functions in IPSEC helps protect the data from being changed or tampered with during transmission.

10. Which of the following processes is used in IPSEC to negotiate symmetric keys securely between endpoints over an unsecured intermediate media?

A.Diffie-Hellman Key Exchange

B.Advanced Encryption Standard (AES)

C.Secure Hashing Algorithm (SHA)

D.None of the above

Correct Answer

A. Diffie-Hellman Key Exchange

Explanation

The correct answer is Diffie-Hellman Key Exchange. This process is used in IPSEC to negotiate symmetric keys securely between endpoints over an unsecured intermediate media. Diffie-Hellman allows two parties to establish a shared secret key over an insecure channel without actually transmitting the key. This key can then be used for symmetric encryption and decryption of IPSEC traffic.

11. Which of the following services is not provided by an IPSEC tunnel?

A.Data Confidentiality

B.Origin Authentication

C.Data Integrity

D.Protection from Spyware

Correct Answer

D. Protection from Spyware

Explanation

An IPSEC tunnel provides services such as Data Confidentiality, Origin Authentication, and Data Integrity. These services ensure that the data transmitted through the tunnel is secure, authenticated, and not tampered with. However, Protection from Spyware is not a service provided by an IPSEC tunnel. Spyware refers to malicious software that is designed to gather information without the user's knowledge or consent. While an IPSEC tunnel can provide security for data transmission, it does not specifically protect against spyware threats.

12. Which of the following services is not provided by AH?

A.Data Confidentiality (encryption)

B.Origin Authentication

C.Data Integrity

D.Protection against Anti Replay attacks

Correct Answer

A. Data Confidentiality (encryption)

Explanation

AH (Authentication Header) is a protocol used in IPsec (Internet Protocol security) to provide authentication and integrity of IP packets. It does not provide data confidentiality or encryption. Instead, AH focuses on verifying the authenticity of the source of the IP packet and ensuring the integrity of the data within the packet. Data confidentiality, which involves encrypting the data to protect it from unauthorized access, is typically provided by another IPsec protocol called ESP (Encapsulating Security Payload). Therefore, the correct answer is Data Confidentiality (encryption).

13. Which protocol number is associated with ESP?

A.51

B.53

C.50

D.500

Correct Answer

C. 50

Explanation

The correct answer is 50. ESP (Encapsulating Security Payload) is a protocol used in IPsec (Internet Protocol Security) to provide confidentiality, integrity, and authentication for data packets. It operates at the network layer (Layer 3) of the OSI model. Protocol numbers are used to identify different protocols in IP networks, and the protocol number 50 is specifically associated with ESP.

14. Which of the following is not performed during Phase 1 of ISAKMP?

A.Negotiate ISAKMP SAs

B.Negotiate IPSEC SAs

C.Perform peer authentication

D.Perform initial Diffie-Hellman Key Exchange

Correct Answer

B. Negotiate IPSEC SAs

Explanation

During Phase 1 of ISAKMP, the following tasks are performed: negotiate ISAKMP SAs, perform peer authentication, and perform initial Diffie-Hellman Key Exchange. However, negotiating IPSEC SAs is not performed during Phase 1. IPSEC SAs are negotiated during Phase 2 of ISAKMP.

15. The end result of Phase 1 of ISAKMP is an interim secure channel over which Phase II of ISAKMP is performed. What does Phase II do?

A.Negotiate ISAKMP SAs

B.Negotiate IPSEC SAs

C.Perform peer authentication

D.Perform initial Diffie-Hellman Key Exchange

Correct Answer

B. Negotiate IPSEC SAs

Explanation

Phase II of ISAKMP negotiates IPSEC SAs (Security Associations). IPSEC SAs define the parameters for securing the actual data traffic between two peers. This phase establishes the necessary keys and algorithms for encryption, authentication, and integrity, allowing secure communication between the peers. Phase II builds upon the secure channel established in Phase I to enable the secure exchange of IPSEC SAs.

16. What is the end result of Phase II of ISAKMP?

A.The IPSEC tunnel is established

B.Phase III of ISAKMP commences

C.The IPSEC tunnel is torn down and renegotiated

D.An interim secure channel is established

Correct Answer

A. The IPSEC tunnel is established

Explanation

Phase II of ISAKMP is responsible for establishing the IPSEC tunnel. ISAKMP (Internet Security Association and Key Management Protocol) is a protocol used for establishing security associations and exchanging keys for IPsec (Internet Protocol Security) encryption. Phase II specifically deals with negotiating the IPSEC parameters such as encryption algorithms, session keys, and security policies. Once Phase II is successfully completed, the IPSEC tunnel is established, allowing secure communication between the two endpoints.

17. Which of the following is NOT a value add of the companion protocol ISAKMP for IPSEC?

A.It automates the IPSEC tunnel establishment process

B.It allows symmetric keys used by encryption and hashing algorithms to be negotiated dynamically

C.It gives a lifetime to the tunnel, after which the tunnel expires and is reestablished

D.It reduces the overheads associated with IPSEC tunnel establishment

Correct Answer

D. It reduces the overheads associated with IPSEC tunnel establishment

Explanation

The companion protocol ISAKMP for IPSEC does not reduce the overheads associated with IPSEC tunnel establishment.

18. Where does ISAKMP reside in the TCP/IP protocol stack?

A.Directly above IP with protocol number 50

B.Above UDP with port number 500

C.Above TCP with port number 500

D.Over AH/ESP with port number 500

Correct Answer

B. Above UDP with port number 500

Explanation

ISAKMP (Internet Security Association and Key Management Protocol) resides above UDP with port number 500 in the TCP/IP protocol stack. ISAKMP is a key management protocol used for establishing and negotiating security associations (SA) between devices in a network. It operates at the transport layer and uses UDP as its transport protocol. By residing above UDP with port number 500, ISAKMP ensures that it can communicate securely with other devices in the network.

19. Which of the following approaches may be used to do peer authentication during Phase 1 of ISAKMP?

A.Pre-Shared Keys

B.Digital Certificates

C.All the above

D.Peer authentication is not performed during Phase 1 of ISAKMP

Correct Answer

C. All the above

Explanation

Both pre-shared keys and digital certificates can be used for peer authentication during Phase 1 of ISAKMP. Pre-shared keys involve sharing a secret key between the peers, while digital certificates use a public key infrastructure to verify the identity of the peers. Using both approaches provides an added layer of security and flexibility in choosing the authentication method. Therefore, the correct answer is "All the above."

20. Which of the following is a proprietary extension to IPSEC that is not defined in the RFC specifications for IPSEC?

A.Peer Authentication using digital certificates during Phase 1 of ISAKMP

B.Per User Authentication when connecting from VPN client to VPN concentrator

C.AES encryption for confidentiality

D.An IPSEC tunnel operating in transport mode

Correct Answer

B. Per User Authentication when connecting from VPN client to VPN concentrator

Explanation

Per User Authentication when connecting from VPN client to VPN concentrator is a proprietary extension to IPSEC that is not defined in the RFC specifications for IPSEC. The RFC specifications for IPSEC do not include any specific authentication mechanism for individual users connecting from a VPN client to a VPN concentrator. Therefore, the option of per user authentication in this context would be considered a proprietary extension.

21. Which of the following describes the capability for a VPN terminating interface to simultaneously send IPsec protected traffic and regular unprotected traffic?

A.

Split tunneling

B.

Load Balancing

C.

Firewalling

D.

Dual Stack tunneling

Correct Answer

A. Split tunneling

Explanation

Split tunneling describes the capability for a VPN terminating interface to simultaneously send IPsec protected traffic and regular unprotected traffic. This means that the VPN can route some traffic through the encrypted tunnel while allowing other traffic to bypass the tunnel and use the regular internet connection. This can be useful in situations where certain traffic, such as accessing local resources, does not need to be encrypted and can be routed directly.

1.

198.2.2.1 IP address belongs to which IP class?

A.Class A

B.Class B

C.Class C

D.Class D

Correct Answer

C. Class C

Explanation

The IP address 198.2.2.1 belongs to Class C. In Class C, the first octet ranges from 192 to 223, which falls within the range of 198. Therefore, the given IP address is in Class C.

2. What is the acronym for LAN?

A.

Local Area Network

B.

Local Access Network

C.

Line And Networking

D.

Line-less Networking

Correct Answer

A. Local Area Network

Explanation

The correct answer is Local Area Network. LAN stands for Local Area Network, which refers to a network that connects computers and devices within a limited area, such as a home, office, or building. It allows for the sharing of resources, such as files, printers, and internet connections, among the connected devices.

3.

Define what a LAN is?

A.

Connected devices share the resources of a single processor or server within a small geographic area

B.

Normally found within a business and school

C.

These are computers that share resources over a large area

D.

None of the above

Correct Answer

A. Connected devices share the resources of a single processor or server within a small geographic area

Explanation

A LAN, or Local Area Network, refers to a network of connected devices that share resources, such as a processor or server, within a small geographic area. This type of network is typically found within businesses and schools. It allows for efficient sharing of resources and enables communication and data transfer between connected devices.

4.

Mr. John is a small businessman who runs Hardware. He has been experiencing problems with his small accounting department, which he depends on to provide sales reports. Mr. John wants to share information between his 7 computer stations and have on central printing area. What type of network would you recommend to Mr. John?

A.MAN

B.LAN

C.WAN

D.SAN

Correct Answer

B. LAN

Explanation

Based on the given scenario, a Local Area Network (LAN) would be the most suitable network type for Mr. John. A LAN is a network that connects computers and devices within a limited area, such as a small office or building. It allows for the sharing of resources, such as printers and files, among the connected computers. Since Mr. John wants to share information between his 7 computer stations and have a central printing area, a LAN would provide the necessary connectivity and functionality for his small business.

5.

What covers a larger geographical area than MAN?

A.WAN

B.LAN

C.Both A and B

D.None of the above

Correct Answer

A. WAN

Explanation

A WAN (Wide Area Network) covers a larger geographical area than a MAN (Metropolitan Area Network). While a MAN typically covers a city or a metropolitan area, a WAN can span across multiple cities, countries, or even continents. Therefore, WAN is the correct answer as it encompasses a larger geographical area compared to a MAN.

6. Which type of network consists of both LANs and MANs?

A.Wide Area Network

B.Local Area Network

C.Both A and B

D.None of the above

Correct Answer

A. Wide Area Network

Explanation

A Wide Area Network (WAN) consists of both Local Area Networks (LANs) and Metropolitan Area Networks (MANs). LANs are used to connect devices within a small geographical area, such as an office or a building, while MANs connect multiple LANs within a larger geographical area, such as a city. Therefore, a WAN includes both LANs and MANs, making "Both A and B" the correct answer.

7. Arrange the Following Types of Networks according to their size, from largest to smallest?

A.LAN, WAN, MAN

B.WAN, LAN, MAN

C.MAN, LAN, WAN

D.WAN, MAN, LAN

Correct Answer

D. WAN, MAN, LAN

Explanation

In this question, we are asked to arrange the types of networks according to their size, from largest to smallest. LAN stands for Local Area Network, which is the smallest network that covers a limited geographical area, such as a home, office, or building. MAN stands for Metropolitan Area Network, which covers a larger area, such as a city or town. WAN stands for Wide Area Network, which is the largest network that covers a wide geographical area, such as multiple cities or even countries. Therefore, the correct arrangement from largest to smallest is WAN, MAN, LAN.

8. You are a member of a club that deals with computer networks. The club has to take a project to build a MAN. Where would this project likely take place?

A.A small building/organization

B.University or college

C.Home

D.None of the above

Correct Answer

B. University or college

Explanation

This project would likely take place in a university or college because these institutions typically have the resources, infrastructure, and expertise to undertake such a project. They often have dedicated departments or research centers focused on computer networks and would have the necessary equipment, funding, and personnel to successfully build a Metropolitan Area Network (MAN). Additionally, universities and colleges often engage in research and development activities, making them suitable environments for this type of project.

9. What does the acronym MAN stand for?

A.Magnetic Access Network

B.Metropolitan Area Network

C.Multi-Area Network

D.Multi-Access Net

Correct Answer

B. Metropolitan Area Network

Explanation

A Metropolitan Area Network (MAN) is a network that covers a larger geographical area than a Local Area Network (LAN) but smaller than a Wide Area Network (WAN). It connects multiple LANs within a city or metropolitan area, providing high-speed communication and data transfer between different locations. MANs are typically owned and operated by telecommunications companies or internet service providers, and they are used to connect businesses, government agencies, educational institutions, and other organizations within a specific region.

10. In your school there is a library, and you can use the internet to do research, this library will most likely be a \_\_\_\_\_\_\_ network.

A.MAN

B.LAN

C.WAN

D.All of the above

Correct Answer

C. WAN

Explanation

Since the question mentions using the internet to do research, it suggests that the library is connected to a wide area network (WAN). A wide area network is a network that connects multiple local area networks (LANs) over a large geographical area, such as different schools or offices in different locations. Therefore, the library in the school would most likely be a WAN network.

11. Which network topologies have the highest transmission speed?

A.LAN

B.WAN

C.MAN

D.All of the above

Correct Answer

A. LAN

Explanation

LAN (Local Area Network) has the highest transmission speed among the given network topologies. LANs are typically confined to a small geographical area, such as a building or campus, and are designed for high-speed data transmission within that area. They use technologies like Ethernet or Wi-Fi, which offer fast and reliable connections. In contrast, WANs (Wide Area Networks) cover larger areas and are often slower due to the limitations of long-distance transmission. MANs (Metropolitan Area Networks) fall in between LANs and WANs in terms of size and transmission speed. Therefore, LAN is the correct answer as it provides the highest transmission speed.

12. IPv6 addresses have a size of:

A.64 bits

B.128 bits

C.256 bits

D.512 bits

Correct Answer

B. 128 bits

Explanation

IPv6 addresses have a size of 128 bits. This means that an IPv6 address is composed of 128 binary digits, allowing for a much larger address space compared to IPv4. The increased address space in IPv6 allows for the creation of more unique addresses to support the growing number of devices connected to the internet.

<https://nesoacademy.org/cs/06-computer-networks/ppts/01-introduction-to-computer-networks>

<https://cspages.ucalgary.ca/~cwill/CPSC441/slides.html>

<https://www.webasha.com/blog/ccna-interview-questions-on-nat>

<https://www.examveda.com/networking/practice-mcq-question-on-network-address-translation/>