Chapter 1
Network Fundamentals (Domain 1)

THE CCNA EXAM TOPICS COVERED IN THIS PRACTICE TEST INCLUDE THE FOLLOWING:

- **1.0 Network Fundamentals (ICND1)**
  - 1.1 Compare and contrast OSI and TCP/IP models (ICND1)
  - 1.2 Compare and contrast TCP and UDP protocols (ICND1)
  - 1.3 Describe the impact of infrastructure components in an enterprise network (ICND1)
  - 1.4 Describe the effects of cloud resources on enterprise network architecture (ICND2)
  - 1.5 Compare and contrast collapsed core and three-tier architectures (ICND1)
  - 1.6 Compare and contrast network topologies (ICND1)
  - 1.7 Select the appropriate cabling type based on implementation requirements (ICND1)
  - 1.8 Apply troubleshooting methodologies to resolve problems (ICND1)
  - 1.9 Configure, verify, and troubleshoot IPv4 addressing and subnetting (ICND1)
  - 1.10 Compare and contrast IPv4 address types (ICND1)
  - 1.11 Describe the need for private IPv4 addressing (ICND1)
  - 1.12 Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment (ICND1)
  - 1.13 Configure, verify, and troubleshoot IPv6 addressing (ICND1)
  - 1.14 Configure and verify IPv6 Stateless Address Autoconfiguration (ICND1)
  - 1.15 Compare and contrast IPv6 address types (ICND1)

1. Which statement is a valid reason the OSI reference model was created?

Technet24.ir

A. It encourages vendors to create proprietary standards for any component of the OSI.

B. It allows for changes on one layer to apply to another layer so they can work together.

C. It prevents industry standardization of network processes.

D. It divides network communication into smaller components for design and troubleshooting.

2. When a program uses encryption such as SSL, which layer is responsible?

A. Presentation layer

B. Transport layer

C. Data Link layer

D. Session layer

3. Which device would primarily function at the Data Link layer?

A. Routers

B. Firewalls

C. Gateways

D. Switches

4. Which is the proper order of the OSI layers?

A. Application, Transport, Session, Presentation, Network, Data Link, Physical

B. Presentation, Application, Session, Transport, Network, Data Link, Physical

C. Application, Presentation, Session, Transport, Network, Data Link, Physical

D. Application, Presentation, Transport, Network, Session, Data Link, Physical

5. Which OSI layer is responsible for logical addressing?

A. Transport layer

B. Network layer

C. Application layer

D. Data Link layer

6. Which OSI layer is responsible for connection-oriented communication?

A. Transport layer

B. Presentation layer

C. Data Link layer

D. Application layer

7. Which layer is responsible for compression and decompression?

A. Application layer

B. Physical layer

C. Session layer

D. Presentation layer

8. Which layer of the OSI is responsible for dialog control of applications?

A. Application layer

B. Physical layer

C. Session layer

D. Network layer

9. At which layer of the OSI can you find DTE and DCE interfaces?

A. Application layer

B. Physical layer

C. Session layer

D. Transport layer

10. At which DoD model layer does Telnet, TFTP, SNMP, and SMTP function?

Technet24.ir

A. Host-to-Host layer

B. Process/Application layer

C. Internet layer

D. Network Access layer

11. An administrator is checking to make sure that SNMP is working properly. Which is the highest layer checked in the OSI if it is working successfully?

A. Application layer

B. Presentation layer

C. Session layer

D. Network layer

12. The receiving computer checked the checksum of a frame. It had been damaged during transfer, so it is discarded. At which layer of the OSI did this occur?

A. Physical layer

B. Data Link layer

C. Network layer

D. Session layer

13. Which layer in the DoD model is responsible for routing?

A. Host-to-Host layer

B. Process/Application layer

C. Internet layer

D. Network Access layer

14. Which devices create collision domains, raising effective bandwidth?

A. Firewalls

B. Hubs

C. Routers

D. Switches

15. Which device acts like a multiport repeater?

A. Firewall
B. Hub
C. Router
D. Switch

16. Which layer of the OSI defines the PDU, or protocol data unit, of segments?

A. Application layer
B. Session layer
C. Network layer
D. Transport layer

17. Which device will create broadcast domains and raise effective bandwidth?

A. Firewall
B. Hub
C. Router
D. Switch

18. Which is a correct statement about MAC addresses?

A. Organizationally unique identifiers (OUIs) create a unique MAC address.
B. The first 24 bits of a MAC address is specified by the vendor.
C. The IEEE is responsible for MAC address uniqueness.
D. If the I/G bit is set to 1, then the frame identifies a broadcast or multicast.

19. Which access/contention method is used for Ethernet?

Technet24.ir

A. CSMA/CA

B. CSMA/CD

C. 802.2

D. Token passing

20. What is the correct order of encapsulation?

A. User datagrams, packets, segments, frames, bits

B. User datagrams, sessions, segments, packets, frames, bits

C. User datagrams, segments, packets, frames, bits

D. Bits, frames, sessions, packets, user datagrams

21. Which application provides terminal emulation over a network?

A. SNMP

B. Telnet

C. HTTP

D. TFTP

22. Which protocol is responsible for identifying upper-layer network protocols at the Data Link layer?

A. LLC logical link control

B. MAC

C. 802.3

D. FCS

23. The translation of ASCII to EBCDIC is performed at which layer of the OSI?

A. Application layer

B. Session layer

C. Presentation layer

D. Data Link layer

24. Which is not a common cause for LAN congestion?

A. Broadcasts

B. Multicasts

C. Adding switches for connectivity

D. Using multiple hubs for connectivity

25. Flow control can be found at which layer of the OSI?

A. Transport layer

B. Network layer

C. Data Link layer

D. Session layer

26. Which protocol requires the programmer to deal with lost segments?

A. SSL

B. TCP

C. UDP

D. NMS

27. Which is a correct statement about the Transmission Control Protocol (TCP)?

A. TCP is a connectionless protocol.

B. TCP allows for error detection and correction.

C. TCP is faster than UDP.

D. TCP allows for retransmission of lost segments.

28. Which statement correctly describes what happens when a web browser initiates a request to a web server?

Technet24.ir

A. The sender allocates a port dynamically above 1024 and associates it with the request.

B. The receiver allocates a port dynamically above 1024 and associates it with the request.

C. The sender allocates a port dynamically below 1024 and associates it with the request.

D. The receiver allocates a port dynamically below 1024 and associates it with the request.

29. Which protocol and port number is associated with SMTP?

A. UDP/69

B. UDP/25

C. TCP/69

D. TCP/25

30. How does TCP guarantee delivery of segments to the receiver?

A. Via the destination port

B. TCP checksums

C. Window size

D. Sequence and acknowledgment numbers

31. When a programmer decides to use UDP as a transport protocol, what is a decision factor?

A. Redundancy of acknowledgment is not needed.

B. Guaranteed delivery of segments is required.

C. Windowing flow control is required.

D. A virtual circuit is required.

32. Which mechanism allows for programs running on a server (daemons) to listen for requests through the process called binding?

A. Headers

B. Port numbers

C. MAC address

D. Checksums

33. Which is a correct statement about sliding windows used with TCP?

A. The window size is established during the three-way handshake.

B. Sliding windows allow for data of different lengths to be padded.

C. It allows TCP to indicate which upper-layer protocol created the request.

D. It allows the router to see the segment as urgent data.

34. Why does DNS use UDP?

A. DNS requires acknowledgment of the request for auditing.

B. The requests require flow control of UDP.

C. DNS requests are usually small and do not require connections setup.

D. DNS requires a temporary virtual circuit.

35. What is required before TCP can begin sending segments?

A. Three-way handshake

B. Port agreement

C. Sequencing of segments

D. Acknowledgment of segments

36. Which term describes what it is called when more than one wireless access point (WAP) covers the same SSID?

A. Broadcast domain

B. Basic service set

C. Extended server set

D. Wireless mesh

Technet24.ir

37. Which protocol allows a Lightweight AP (LWAP) to forward data to the wired LAN?

A. Spanning Tree Protocol (STP)
B. Bridge protocol data units (BPDUs)
C. Orthogonal Frequency Division Multiplexing (OFDM)
D. Control and Provisioning of Wireless Access Points (CAPWAP)

38. Which component allows wireless clients to roam between access points and maintain authentication?

A. Basic service set
B. Extended service set
C. Wireless LAN controller
D. Service set ID

39. Which is a valid reason to implement a wireless LAN controller (WLC)?

A. Centralized authentication
B. The use of autonomous WAPs
C. Multiple SSIDs
D. Multiple VLANs

40. You require a density of 100 wireless clients in a relatively small area. Which design would be optimal?

A. Autonomous WAPs with a WLC
B. Lightweight WAPs with a WLC
C. Autonomous WAPs without a WLC
D. Lightweight WAPs without a WLC

41. When designing a wireless network, which would be a compelling reason to use 5 GHz?

A. 5 GHz can go further.

B. 5 GHz allows for more clients.

C. There are 24 non-overlapping channels.

D. There is less interference on 5 GHz.

42. Which allows for seamless wireless roaming between access points?

A. Single SSID

B. Single service set

C. 802.11ac

D. Wireless LAN controller

43. In the 2.4 GHz spectrum for 802.11, which channels are non-overlapping?

A. Channels 1, 3, and 11

B. Channels 1, 3, and 6

C. Channels 1, 6, and 11

D. Channels 1 through 6

44. Which is one of the critical functions that a wireless LAN controller performs?

A. Allows autonomous WAPs

B. Synchronizes the WAPs with the same IOS

C. Triangulates users for location lookups

D. Allows for the use of all frequency channels

45. Which is the contention method 802.11 wireless uses?

A. CSMA/CA

B. CSMA/CD

C. BSSS

D. OFDM

46. When firewalls are placed in a network, which zone contains Internet-

Technet24.ir

facing services?

A. Outside zone
B. Enterprise network zone
C. Demilitarized zone
D. Inside zone

47. According to best practices, what is the proper placement of a firewall?

A. Only between the internal network and the Internet
B. At key security boundaries
C. In the DMZ
D. Only between the DMZ and the Internet

48. Which is a false statement about firewalls?

A. Firewalls can protect a network from external attacks.
B. Firewalls can protect a network from internal attacks.
C. Firewalls can provide stateful packet inspection.
D. Firewalls can control application traffic.

49. Which of the following options is not a consideration for the management of a firewall?

A. All physical access to the firewall should be tightly controlled.
B. All firewall policies should be documented.
C. Firewall logs should be regularly monitored.
D. Firewalls should allow traffic by default and deny traffic explicitly.

50. What is the reason firewalls are considered stateful?

A. Firewalls keep track of the zone states.
B. Firewalls keep accounting on the state of packets.
C. Firewalls track the state of a TCP conversation.
D. Firewalls transition between defense states.

51. You have an Adaptive Security Appliance (ASA) and two separate

Internet connections via different providers. How could you apply the same policies to both connections?

A. Place both connections into the same zone.
B. Place each connection into an ISP zone.
C. Apply the same ACL to both of the interfaces.
D. Each connection must be managed separately.

52. Why should servers be placed in the DMZ?

A. So that Internet clients can access them
B. To allow access to the Internet and the internal network
C. To allow the server to access the Internet
D. To restrict the server to the Internet

53. Which type of device will detect but not prevent unauthorized access?

A. Firewall
B. IPS
C. IDS
D. Honey pots

54. When a firewall matches a URI, it is operating at which layer?

A. Layer 7
B. Layer 5
C. Layer 4
D. Layer 3

55. In which zone should an email server be located?

A. Inside zone
B. Outside zone
C. DNS zone
D. DMZ

56. Amazon Web Services (AWS) and Microsoft Azure are examples of

Technet24.ir

what?

A. Public cloud providers
B. Private cloud providers
C. Hybrid cloud providers
D. Dynamic cloud providers

57. You are looking to create a fault tolerant colocation site for your servers at a cloud provider. Which type of cloud provider would you be searching for?

A. PaaS
B. IaaS
C. SaaS
D. BaaS

58. Which allows for the distribution of compute resources such as CPU and RAM to be distributed over several operating systems?

A. Physical server
B. Hypervisor
C. Virtual machine
D. Virtual network

59. Which option describes a virtual machine (VM) best?

A. An operating system that is running directly on hardware
B. An operating system that is running with dedicated hardware
C. An operating system that is running on reduced hardware features
D. An operating system that is decoupled from the hardware

60. What is the physical hardware used in virtualization called?

A. Host

B. VM

C. Hypervisor

D. Guest

61. Which component connects the virtual machine NIC to the physical network?

A. vNIC

B. Trunk

C. Virtual switch

D. NX-OS

62. Which component acts as a distribution switch for the physical data center?

A. Top of Rack switch

B. End of Row switch

C. Core switch

D. Virtual switch

63. Which is not a NIST criteria for cloud computing?

A. Resource pooling

B. Rapid elasticity

C. Automated billing

D. Measured service

64. Which term describes an internal IT department hosting virtualization for a company?

A. Public cloud

B. Elastic cloud

C. Private cloud

D. Internal cloud

Technet24.ir

65. What is the role of a cloud services catalog?

A. It defines the capabilities for the cloud.

B. It defines the available VMs for creation in the cloud.

C. It defines the available VMs running in the cloud.

D. It defines the drivers for VMs in the cloud.

66. A hosted medical records service is an example of which cloud model?

A. PaaS

B. IaaS

C. SaaS

D. BaaS

67. A hosted environment that allows you to write and run programs is an example of which cloud model?

A. PaaS

B. IaaS

C. SaaS

D. BaaS

68. Which cloud connectivity method allows for seamless transition between public clouds?

A. MPLS VPN

B. Internet VPN

C. Intercloud exchange

D. Private WAN

69. Which statement is not a consideration when converting to an email SaaS application if the majority of users are internal?

A. Internal bandwidth usage

B. External bandwidth usage

C. Location of the users

D. Branch office connectivity to the Internet

70. Which of the following is a virtual network function (VNF) device?

A. Virtual switch

B. Virtual firewall

C. Database server

D. File server

71. You purchase a VM on a public cloud and plan to create a VPN tunnel to the cloud provider. Your IP network is 172.16.0.0/12, and the provider has assigned an IP address in the 10.0.0.0/8 network. What VNF will you need from the provider to communicate with the VM?

A. Virtual switch

B. Virtual firewall

C. Virtual router

D. Another IP scheme at the provider

72. Which protocol would you use to synchronize the VM in the public cloud with an internal time source at your premise?

A. DNS

B. rsync

C. NTP

D. VPN

73. You need to scale out some web servers to accommodate load. Which method would you use?

Technet24.ir

A. Add vCPUs.

B. Add vRAM.

C. Add DNS.

D. Add SLBaaS.

74. You have several VMs in a public cloud. What is a benefit of creating NTP VNF in the public cloud for the VMs?

A. Better time synchronization

B. Better response time from the VMs

C. Lower bandwidth utilization from your premises

D. Overcoming different time zones

75. When deciding to move DNS into the cloud for an application on the public cloud, what is the primary decision factor?

A. Bandwidth

B. Response time

C. Proper DNS resolution

D. The cloud provider's requirements

76. Access layer switches in the three-tier design model perform which task?

A. Connect to other switches for redundancy

B. Connect to users

C. Connect campuses

D. Connect to the Internet

77. Distribution layer switches in the three-tier design model perform which task?

A. Connect to other switches for redundancy

B. Connect to users

C. Connect campuses

D. Connect to the Internet

78. Core layer switches in the three-tier design model perform which task?

A. Connect to other switches for redundancy
B. Connect to users
C. Connect campuses
D. Connect to the Internet

79. The two-tier design model contains which layer switches?

A. Core, distribution, and access
B. Core and distribution
C. Distribution and access
D. Internet, core, distribution, and access

80. You have one campus, which contains 2,000 PCs, and each edge switch will contain 25 to 40 PCs. Based on this layout, which design model should be used?

A. Collapsed-core model
B. Three-tier model
C. DOD model
D. Access model

81. You have four campuses, each containing 500 PCs, and each edge switch will contain 20 to 30 PCs. Based on this layout, which design model should be used?

A. Collapsed-core model
B. Three-tier model
C. DOD model
D. Access model

82. Which should only be performed at the core layer?

Technet24.ir

A. Routing

B. Supporting clients

C. Configuring ACLs

D. Switching

83. Which layer in the three-tier model is where redistribution of routing protocols should be performed?

A. Core layer

B. Distribution layer

C. Access layer

D. Routing layer

84. Which layer in the three-tier model is where collision domains should be created?

A. Core layer

B. Distribution layer

C. Access layer

D. Routing layer

85. Which is an accurate statement about the collapsed-core design concept?

A. It is best suited for large-scale networks.

B. It allows for better bandwidth.

C. It is best suited for small enterprises.

D. It bottlenecks bandwidth.

86. Which network topology design has a centralized switch connecting all of the devices?

A. Star topology

B. Full mesh topology

C. Partial mesh topology

D. Hybrid topology

87. Which is a direct benefit of a full mesh topology?

A. Increased bandwidth

B. Increased redundancy

C. Decreased switch count

D. Increased complexity

88. Where is the hybrid topology most commonly seen in the three-tier design model?

A. Core layer

B. Distribution layer

C. Access layer

D. Routing layer

89. Where is the full mesh topology commonly seen in the three-tier design model?

A. Core layer

B. Distribution layer

C. Access layer

D. Routing layer

90. Where is the star topology most commonly seen in the three-tier design model?

A. Core layer

B. Distribution layer

C. Access layer

D. Routing layer

91. Which topology does the collapsed core layer switch use in a two-tier design model?

Technet24.ir

A. Star topology

B. Full mesh topology

C. Partial mesh topology

D. Hybrid topology

92. Define a full mesh topology design.

A. All links from the central switch connect to the edge switches.

B. All links between switches are connected to each other redundantly.

C. Only links between similar switch types are connected to each other redundantly.

D. All ports are used for connecting only other switches.

93. Define a star topology design.

A. All links from the central switch connect to the edge switches.

B. All links between switches are connected to each other redundantly.

C. Only links between similar switch types are connected to each other redundantly.

D. All ports are used for connecting other switches.

94. Which topology does an autonomous WAP use?

A. Star topology

B. Full mesh topology

C. Partial mesh topology

D. Hybrid topology

95. If you had limited cable access for the distribution switches, which topology would you need to plan for?

A. Star topology

B. Full mesh topology

C. Partial mesh topology

D. Hybrid topology

96. Which cable standard delivers 1 Gb/s using four pairs of CAT5e?

A. 1000Base-T
B. 1000Base-SX
C. 1000Base-LX
D. 1000Base-X

97. Which fiber optic standard uses a 9 micron core and can span up to 10km?

A. UTP
B. Multi-mode
C. Single-mode
D. STP

98. Which cable type would you use to connect a router to a switch?

A. Straight-through cable
B. Crossover cable
C. Rolled cable
D. Shielded cable

99. What is the maximum distance you can run 1000Base-T?

A. 100 meters
B. 1,000 meters
C. 100 feet
D. 1,000 feet

100. What is the terminal specification to connect to a Cisco router or switch via serial cable?

A. 9600 baud 8-N-0
B. 9600 baud 8-N-1
C. 2400 baud 8-N-1
D. 115,200 baud 8-N-1

Technet24.ir

101. Which cable type would you use to connect a switch to a switch?

A. Straight-through cable
B. Crossover cable
C. Rolled cable
D. Shielded cable

102. Which fiber optic standard utilizes a 50 micron core?

A. UTP
B. Multi-mode
C. Single-mode
D. STP

103. Which type of cable would be used to connect a computer to a switch for management of the switch?

A. Straight-through cable
B. Crossover cable
C. Rolled cable
D. Shielded cable

104. Which specification for connectivity is currently used in data centers for cost and simplicity?

A. 10GBase-T
B. 40GBase-T
C. 10GBase-CX
D. 100GBase-TX

105. If you had an existing installation of Cat5e on your campus, what is the highest speed you could run?

A. 10 Mb/s

B. 100 Mb/s

C. 1 Gb/s

D. 10 Gb/s

106. You get a call that the Internet is down. When you investigate the Internet router and perform a `show interface serial 0/0`, you see the following status. What might be the problem?

```
Serial0/0 is administratively down, line protocol is up
  Hardware is MCI Serial
```

A. The serial line connecting to the ISP is down.

B. Someone accidentally shut down the serial interface.

C. Routing to the ISP is not set correctly.

D. The clocking from the ISP has stopped.

107. When performing troubleshooting for a routing issue, which method should be used first to isolate the problem?

A. Pinging the destination IP back to the originating IP

B. Pinging the originating IP to the destination IP

C. Traceroute from the originating IP to the destination IP

D. Traceroute from the destination IP to the originating IP

108. Which command would you run to diagnose a possible line speed or duplex issue?

A. Switch#`show speed`

B. Switch#`show duplex`

C. Switch#`show interface status`

D. Switch#`show diagnostics`

109. Which command would you use, to diagnose a problem with frames that are not getting forwarded to the destination node on a switch?

Technet24.ir

A. Switch#`show route`

B. Switch#`show mac address-table`

C. Switch#`show mac table`

D. Switch#`show interface`

110. Which command should you start with when trying to diagnose port security issues?

A. Switch#`show port-security`

B. Switch#`show mac address-table`

C. Switch#`show interface`

D. Switch#`show security`

111. After solving the root cause of a problem, what should be done?

A. Isolate the problem.

B. Perform root cause analysis.

C. Escalate the problem.

D. Monitor the solution.

112. What is the first step to troubleshooting a problem?

A. Isolate the problem.

B. Perform root cause analysis.

C. Escalate the problem.

D. Monitor the solution.

113. Which command should be used to verify that a VLAN is defined on a switch to troubleshoot a VLAN forwarding issue?

A. Switch#`show interfaces fast 0/0 switchport`

B. Switch#`show vlan`

C. Switch#`show vlans`

D. Switch#`show vtp`

114. It is reported that users cannot reach an internal server. You only

have access to the local switches at your facility. You perform a `show interface fast 0/23` on the user reporting the problem and the status of the switch is up/up. What should you do next?

A. Isolate the problem.

B. Perform root cause analysis.

C. Escalate the problem.

D. Monitor the solution.

115. You just installed a new switch and you cannot get traffic forwarded to a remote VLAN. You believe there is a problem with trunking. Which command will you start with to verify trunking.

A. Switch#`show interfaces fast 0/0 switchport`

B. Switch#`show vlan`

C. Switch#`show vlans`

D. Switch#`show trunks`

116. Which class is the IP address 172.23.23.2?

A. Class A

B. Class B

C. Class C

D. Class D

117. Which is the default subnet mask for a Class A address?

A. 255.0.0.0

B. 255.255.0.0

C. 255.255.255.0

D. 255.255.255.255

118. Which address is a multicast IP address?

Technet24.ir

A. 221.22.20.2

B. 223.3.40.2

C. 238.20.80.4

D. 240.34.22.12

119. Which is true of an IP address of 135.20.255.255?

A. It is a Class A address.

B. It is a broadcast address.

C. It is the default gateway address.

D. It has a default mask of 255.0.0.0

120. What is the CIDR notation for a subnet mask of 255.255.240.0?

A. /19

B. /20

C. /22

D. /28

121. You have been given an IP address network of 203.23.23.0. You are asked to subnet it for two hosts per network. What is the subnet mask you will need to use to maximize networks?

A. 255.255.255.252

B. 255.255.255.248

C. 255.255.255.240

D. 255.255.255.224

122. You have been given an IP address network of 213.43.53.0. You are asked to subnet it for 22 hosts per network. What is the subnet mask you will need to use to maximize networks?

A. 255.255.255.252

B. 255.255.255.248

C. 255.255.255.240

D. 255.255.255.224

123. Which valid IP is in the same network as 192.168.32.61/26?

A. 192.168.32.59
B. 192.168.32.63
C. 192.168.32.64
D. 192.168.32.72

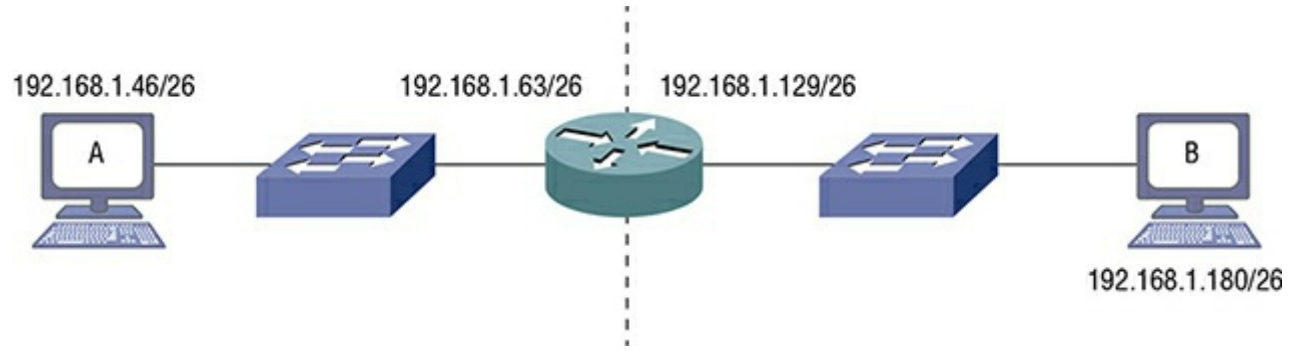
124. You are setting up a network in which you need 15 routed networks. You have been given a network address of 153.20.0.0, and you need to maximize the number of hosts in each network. Which subnet mask will you use?

A. 255.255.224.0
B. 255.255.240.0
C. 255.255.248.0
D. 255.255.252.0

125. An ISP gives you an IP address of 209.183.160.45/30 to configure your end of the serial connection. Which IP address will be on the side at the ISP?

A. 209.183.160.43/30
B. 209.183.160.44/30
C. 209.183.160.46/30
D. 209.183.160.47/30

126. In the following exhibit, what needs to be changed for Computer A to successfully communicate with Computer B (assume the least amount of effort to fix the problem)?



Technet24.ir

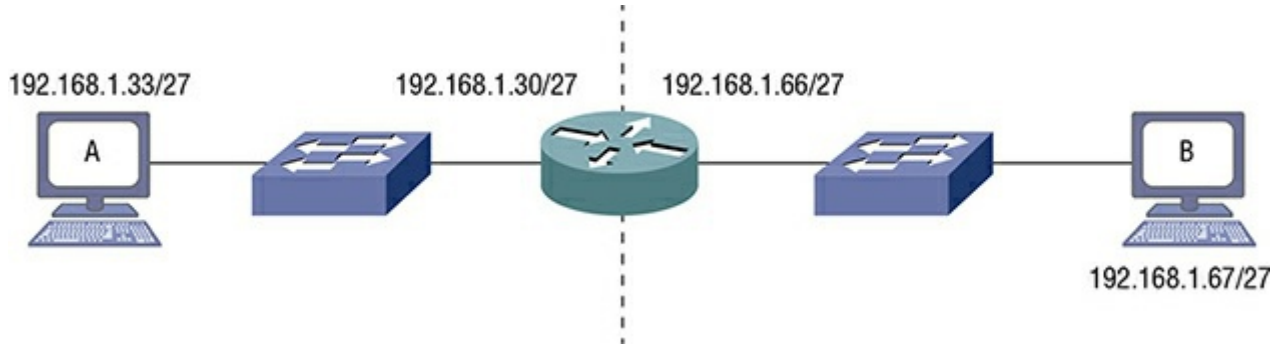
A. Computer A needs to have its IP address changed.

B. Computer B needs to have its IP address changed.

C. The default gateway IP address for Computer A needs to be changed.

D. The default gateway IP address for Computer B needs to be changed.

127. In the following exhibit, what needs to be changed for Computer A to successfully communicate with Computer B (assume the least amount of effort to fix the problem)?



A. Computer A needs to have its IP address changed.

B. Computer B needs to have its IP address changed.

C. The default gateway IP address for Computer A needs to be changed.

D. The default gateway IP address for Computer B needs to be changed.

128. Which subnet does host 131.50.39.23/21 belong to?

A. 131.50.39.0/21

B. 131.50.32.0/21

C. 131.50.16.0/21

D. 131.50.8.0/21

129. A computer has an IP address of 145.50.23.1/22. What is the broadcast address for that computer?

A. 145.50.254.255

B. 145.50.255.255

C. 145.50.22.255

D. 145.50.23.255

130. What is the valid IP address range for the network of 132.59.34.0/23?

A. 132.59.34.1 to 132.59.36.254
B. 132.59.34.1 to 132.59.35.254
C. 132.59.34.1 to 132.59.34.254
D. 132.59.34.1 to 132.59.35.255

131. What is the subnet mask for a CIDR notation of /20?

A. 255.255.224.0
B. 255.255.240.0
C. 255.255.248.0
D. 225.225.252.0

132. What is the number of subnets which you can have for a mask of 255.255.255.248?

A. 8
B. 16
C. 32
D. 64

133. What is the valid number of hosts for a network with a subnet mask of 255.255.255.224?

A. 16
B. 32
C. 14
D. 30

134. You have been given the network of 141.23.64.0/19. What is a valid host in this network?

Technet24.ir

A. 141.23.120.5/19

B. 141.23.96.12/19

C. 141.23.97.45/19

D. 141.23.90.255/19

135. You have four networks of 141.24.4.0, 141.24.5.0, 141.24.6.0, and 141.24.7.0 that you need to super-net together so you can write one ACL in your firewall. What is the super-netted address you will use?

A. 141.24.4.0/20

B. 141.24.4.0/21

C. 141.24.4.0/22

D. 141.24.4.0/23

136. You have eight consecutive networks of 132.22.24.0 to 123.22.31.0, which you need to super-net together so you can write one ACL in your firewall. What is the super-netted address you will use?

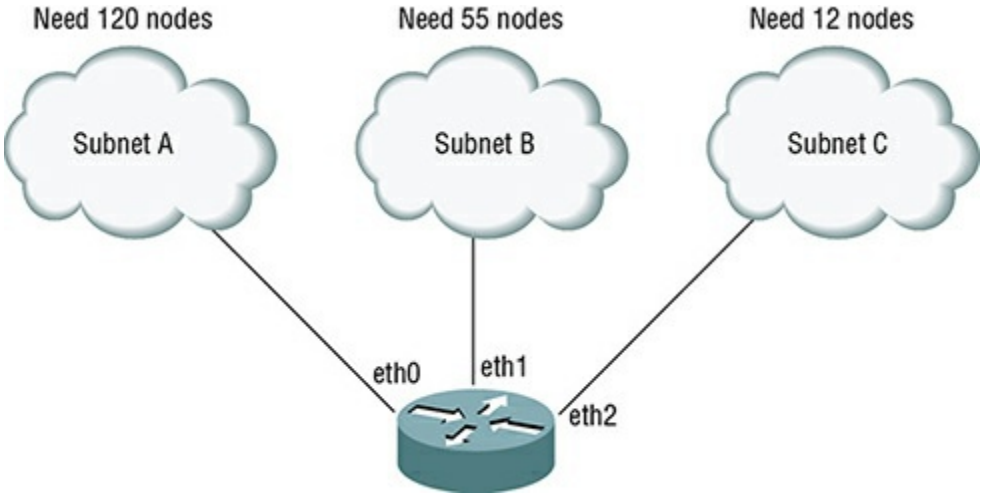
A. 132.22.24.0/20

B. 132.22.24.0/21

C. 132.22.24.0/22

D. 132.22.24.0/23

137. You need to use the IP address space of 198.33.20.0/24 and create a VLSM subnet scheme for the network in the following exhibit. What is the network ID for Subnet A?



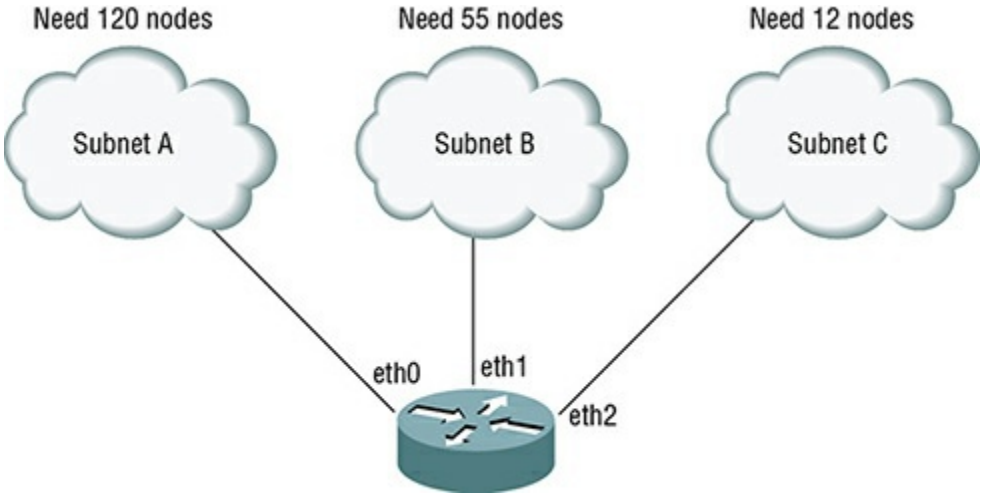
A. 198.33.20.0/25

B. 198.33.20.0/24

C. 198.33.20.0/26

D. 198.33.20.0/28

138. You need to use the IP space of 198.33.20.0/24 and create a VLSM subnet scheme for the network in the following exhibit. What is the network ID for Subnet B?



A. 198.33.20.0/25

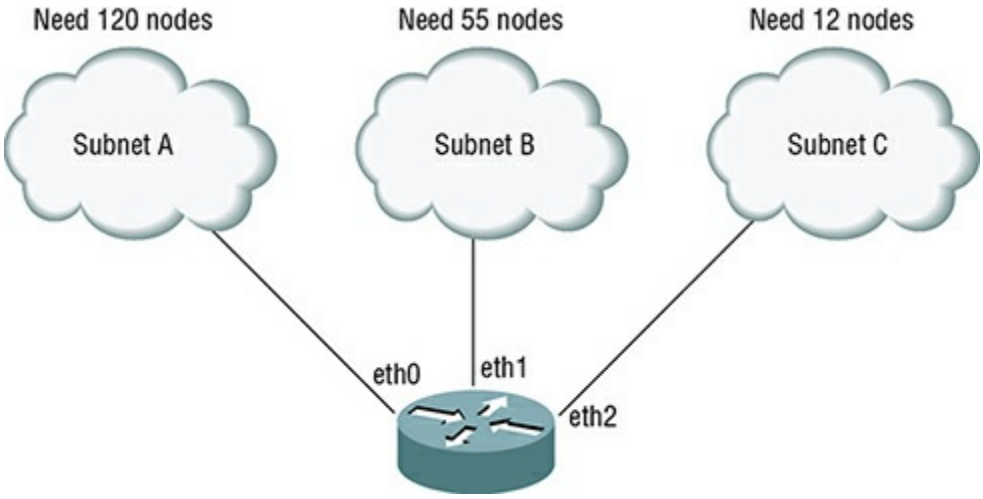
B. 198.33.20.0/24

C. 198.33.20.0/26

D. 198.33.20.0/28

139. You need to use the IP space of 198.33.20.0/24 and create a VLSM subnet scheme for the network in the following exhibit. What is the network ID for Subnet C?

Technet24.ir



A. 198.33.20.0/25
B. 198.33.20.0/24
C. 198.33.20.0/26
D. 198.33.20.0/28

140. A computer with an IP address of 172.18.40.5/12 is having trouble getting to an internal server at an IP address of 172.31.2.4. The default gateway of the computer is 172.16.1.1. What is the problem?

A. The IP address of the computer is wrong.
B. The IP address of the default gateway is wrong.
C. The IP address of the internal server is wrong.
D. The problem is not the networking configuration.

141. A computer has an IP address of 192.168.1.6/24, and its gateway address is 192.168.1.1. It is trying to reach a server on an IP address of 127.20.34.4. The server is not responding. What is the problem?

A. The IP address of the computer is wrong.
B. The IP address of the default gateway is wrong.
C. The IP address of the internal server is wrong.
D. The problem is not the networking configuration.

142. Which is true about a layer 3 broadcast?

A. All of the network bits are ones.

B. The destination MAC in the frame is always all *F*s.

C. The broadcast can be segmented by switches.

D. The IP address is always 255.255.255.255.

143. Which method is used to direct communications to a single host?

A. Unicast

B. Broadcast

C. Multicast

D. Anycast

144. Which method is used to direct communications to the closest IP address to the source?

A. Unicast

B. Broadcast

C. Multicast

D. Anycast

145. Which method is used to direct communications to a group of computers that subscribe to the transmission?

A. Unicast

B. Broadcast

C. Multicast

D. Anycast

146. What is the multicast address range?

A. 224.0.0.0/7

B. 224.0.0.0/6

C. 224.0.0.0/5

D. 224.0.0.0/4

147. Which protocol allows multicast switches to join computers to the

Technet24.ir

multicast group?

A. ICMP
B. IGMP
C. IPMI
D. IPGRP

148. Which protocol uses broadcasting at layer 3?

A. ARP
B. DHCP
C. IGMP
D. SNMP

149. Which method is used to direct communications to all computers in a subnet?

A. Unicast
B. Broadcast
C. Multicast
D. Anycast

150. Which of the following is an example of a multicast address?

A. 192.168.1.224
B. 240.23.4.224
C. 239.45.32.1
D. 244.23.43.11

151. Which RFC defines private IP addresses?

A. RFC 1819
B. RFC 1911
C. RFC 1918
D. RFC 3030

152. What is a major reason to use private IP addressing?

A. It allows for the conservation of public IP addresses.

B. Since they are non-routable on the Internet, they are secure.

C. It keeps communications private.

D. They allow easier setup than public IP addresses.

153. What is required when using private IP addresses to communicate with Internet hosts?

A. Internet router

B. IPv4 tunnel

C. VPN tunnel

D. Network Address Translation

154. Which is the Class A private IP address range?

A. 10.0.0.0/8

B. 10.0.0.0/12

C. 172.16.0.0/12

D. 10.0.0.0/10

155. Which is the Class B private IP address range?

A. 10.0.0.0/8

B. 10.0.0.0/12

C. 172.16.0.0/12

D. 10.0.0.0/10

156. Which is the Class C private IP address range?

A. 192.168.1.0/24

B. 192.168.0.0/24

C. 192.168.0.0/16

D. 192.168.0.0/12

157. You plug a laptop into a network jack. When you examine the IP address, you see 169.254.23.43. What can you conclude?

Technet24.ir

A. The network jack is not working.

B. Your laptop has a static IP address configured.

C. The network is configured properly.

D. The DHCP server is down.

158. You plug a laptop into a network jack. When you examine the IP address, you see 10.23.2.3. What can you conclude?

A. The network jack is not working.

B. Your laptop has a static IP address configured.

C. The network is configured properly.

D. The DHCP server is down.

159. You want to put a web server online for public use. Which IP address would you use?

A. 192.168.34.34

B. 172.31.54.3

C. 10.55.33.32

D. 198.168.55.45

160. Who is the governing body that distributes public IP address?

A. IANA

B. RFC

C. IAB

D. IETF

161. Why is IPv6 needed in the world today?

A. It does not require NAT to operate.

B. The IPv4 address space is exhausted.

C. IPv4 is considered legacy, and IPv6 is the replacement.

D. IPv6 does not require subnetting.

162. How many bits is an IPv6 address?

A. 32 bits

B. 64 bits

C. 128 bits

D. 256 bits

163. You have two facilities and both use IPv6 addressing internally. However, both facilities are connected to the Internet via IPv4. What is one recommended method you can use to communicate between the facilities over the Internet?

A. Dedicated leased line

B. Frame Relay

C. Dual stack

D. 6to4 tunnel

164. Which command is required on a router to support IPv6 static addressing?

A. Router(config)#`ipv6 address`

B. Router(config)#`ipv6 routing`

C. Router(config)#`ipv6 enable`

D. Router(config)#`ipv6 unicast-routing`

165. Which command would you use on an interface to set the IPv6 address?

A. Router(config-if)#`ip address`
`2001:0db8:85aa:0000:0000:8a2e:1343:1337`

B. Router(config-if)#`ipv6 address`
`2001:0db8:85aa:0000:0000:8a2e:1343:1337`

C. Router(config-if)#`ip address`
`2001:0db8:85aa:0000:0000:8a2e:1343:1337/64`

D. Router(config-if)#`ipv6 address`
`2001:0db8:85aa:0000:0000:8a2e:1343:1337/64`

166. Which field of the IPv6 header allows for a dual-stack host to decide which stack to process the packet in?

Technet24.ir

A. Version field

B. Flow label

C. Source address

D. Destination address

167. Which command would set the IPv6 default route for a router to interface s0/0?

A. Router(config)#`ip route 0.0.0.0/0 s0/0`

B. Router(config)#`ipv6 route 0.0.0.0/0 s0/0`

C. Router(config)#`ipv6 unicast-route ::0/0 s0/0`

D. Router(config)#`ipv6 route ::0/0 s0/0`

168. You want to see all of the interfaces on a router configured with IPv6. Which command would you use?

A. Router#`show ipv6 interfaces brief`

B. Router#`show ip interfaces brief`

C. Router#`show interfaces status`

D. Router#`show ip addresses`

169. Which dynamic routing protocol(s) can be used with IPv6?

A. RIPng

B. OSPFv3

C. EIGRPv6

D. All of the above

170. You need to see all routes in the routing table for only IPv6. Which command will achieve this?

A. Router#`show route`

B. Router#`show ip route`

C. Router#`show ipv6 route`

D. Router#`show route ipv6`

171. Which is a valid shortened IPv6 address for 2001:0db8:0000:0000:0000:8a2e:0000:1337?

A. 2001:db8:0000::8a2e::1337
B. 2001:db8:::8a2e:0000:1337
C. 2001:db8::8a2e::1337
D. 2001:db8::8a2e:0:1337

172. Which is the correct expanded IPv6 address of 2001::456:0:ada4?

A. 2001:0000:0000:0456:0000:ada4
B. 2001:0000:0000:0000:456:0000:ada4
C. 2001:0000:0000:0000:0000:0456:0000:ada4
D. 2001:0000:0000:0000:0456:0000:0000:ada4

173. In the IPv6 address of 2001.0db8:1234:0016:0023:8080:2345:88ab/64, what is the subnet quartet?

A. 1234
B. 0016
C. 0023
D. 8080

174. What is the network prefix for the IPv6 address of 2001.db8::8080:2345:88ab/64?

A. 2001:db8::/64
B. 2001:0db8:8080:2345/64
C. 2001:0db8:0000:8080/64
D. 2001:0db8:0000:2345/64

175. You need to verify connectivity to an IPv6 address of fc00:0000:0000:0000:0000:0000: 0000:0004. Which command would you use?

Technet24.ir

A. Router#`ping fc00::4`

B. Router#`ping fc::4`

C. Router#`ping6 fc00::4`

D. Router#`ping6 fc::4`

176. Which address is a valid IPv6 host address?

A. fe8::1

B. 2001:db8::2435

C. ff02::1

D. ::1

177. Which statement is true of an IPv6 address?

A. The first 48 bits is the subnet ID.

B. All IPv6 addresses have a built-in loopback.

C. A single interface can be assigned multiple IPv6 addresses.

D. The IPv6 address plan allows for doubling the amount of IPv4 addresses.

178. You have been given an IPv6 prefix of 2001:0db8:aabb:5/52. How many subnets can you have from this address?

A. 8,192

B. 4,096

C. 1,024

D. 512

179. You work for an ISP. The American Registry for Internet Numbers (ARIN) has given you the 2001:0db8:8/34 IP address block. You need to figure out how many /48 blocks you can assign to your customers.

A. 32,768

B. 16,384

C. 8,192

D. 4,096

180. How many bits are contained in each field of an IPv6 address between the colons?

A. 8 bits
B. 32 bits
C. 4 bits
D. 16 bits

181. Which command would be used inside of an interface to configure SLAAC?

A. Router(config-if)#`enable slaac`
B. Router(config-if)#`ipv6 address slaac`
C. Router(config-if)#`ipv6 address dhcp`
D. Router(config-if)#`ipv6 address autoconfig`

182. Which address is used for RS (Router Solicitation) messages?

A. ff00::2
B. ff02::2
C. ff00::1
D. ff02::1

183. Which address is used for RA (Router Advertisement) messages?

A. ff00:2
B. ff02:2
C. ff00:1
D. ff02:1

184. What protocol/process in IPv6 replaces the IPv4 ARP process?

A. NDP (NS/NA)
B. DAD (NS/NA)
C. SLAAC (RS/RA)
D. ARPv6(NS/NA)

Technet24.ir

185. Which layer 3 protocol allows for NDP to process SLAAC?

A. IGMP
B. ICMP
C. ICMPv6
D. IGMPv6

186. What are stateless DHCPv6 servers used for?

A. Configuring the default gateway
B. Configuring the IPv6 address
C. Configuring the IPv6 prefix length
D. Configuring the DNS server address

187. Which command will configure an IPv6 DHCP relay agent for an interface?

A. Router(config-if)#`ipv6 helper 2001:db8:1234::1`
B. Router(config-if)#`ipv6 dhcp helper 2001:db8:1234::1`
C. Router(config-if)#`ipv6 dhcp 2001:db8:1234::1`
D. Router(config-if)#`ipv6 dhcp relay destination 2001:db8:1234::1`

188. Which mechanism in IPv6 allows for SLAAC to avoid duplicating an IPv6 address?

A. NDP (NS/NA)
B. DAD (NS/NA)
C. SLAAC (RS/RA)
D. ARPv6(NS/NA)

189. What is the process of stateful DHCPv6 for IPv6?

A. Discover, Offer, Request, Acknowledge
B. Solicit, Advertise, Request, Reply
C. Neighbor Solicitation, Neighbor Advertisement
D. Router Solicitation, Router Advertisement

190. When SLAAC is performed on an IPv6 host, which process happens first?

A. A Router Solicitation message is sent from the client.
B. A Router Advertisement message is sent from the router.
C. A link-local address is auto-configured on the client.
D. DAD is performed on the IPv6 address.

191. Which address is a global unicast address?

A. fe80:db80:db01:ada0:1112::1
B. 2005:acd:234:1132::43
C. fd00:ac34:34b:8064:234a::7
D. ff00:101:4ab0:3b3e::10

192. Which address is a link-local address?

A. fe80:db80:db01:ada0:1112::1
B. 2005:acd:234:1132::43
C. fd00:ac34:34b:8064:234a::7
D. ff00:101:4ab0:3b3e::10

193. For global unicast addresses, which part of the address is allotted by the RIR, or Regional Internet Registry?

A. First 23 bits
B. First 32 bits
C. First 48 bits
D. First 64 bits

194. Which address is a unique-local address?

A. fe80:db80:db01:ada0:1112::1
B. 2005:acd:234:1132::43
C. fd00:ac34:34b:8064:234a::7
D. ff00::10

Technet24.ir

195. Which address is a multicast address?

A. fe80:db80:db01:ada0:1112::1
B. 2005:acd:234:1132::43
C. fd00:ac34:34b:8064:234a::7
D. ff00::10

196. Which IPv6 address type is similar to IPv4 RFC 1918 addresses?

A. Link-local addresses
B. Global unicast addresses
C. EUI-64 addresses
D. Anycast addresses

197. Which command would configure a single anycast address on a router's interface?

A. Router(config-if)#`ip address 2001:db8:1:1:1::12/64`
B. Router(config-if)#`ipv6 address 2001:db8:1:1:1::12/64 anycast`
C. Router(config-if)#`ipv6 anycast address 2001:db8:1:1:1::12/128`
D. Router(config-if)#`ipv6 address 2001:db8:1:1:1::12/128 anycast`

198. You are using the EUI-64 method of allocating the host portion of the IPv6 addresses. The MAC address of the host is f423:5634:5623. Which is the correct IP address that will be calculated for a network ID of fd00:1:1::?

A. fd00:0001:0001:0000:f623:56ff:fe34:5623/64
B. fd00:0001:0001:0000:f423:56ff:fe34:5623/64
C. fd00:0001:0001:0000:fffe:f623:5634:5623/64
D. fd00:0001:0001:0000:f623:56ff:ff34:5623/64

199. Which address is a EUI-64 generated address?

A. 2001:db8:33::f629:58fe:ff35:5893/64

B. fd00:4:33::f680:45ca:ac3b:5a73/64

C. 2001:db8:aa::f654:56ff:fe34:a633/64

D. 2001:db8:17:fffe:f623::ff34:5623/64

200. Which command would use the MAC address for the host portion of the IPv6 address on a router interface?

A. Router(config-if)#`ip address eui-64 2001:db8:1234::/64`

B. Router(config-if)#`ip address 2001:db8:1234::/64 mac-address`

C. Router(config-if)#`ipv6 address 2001:db8:1234::/64 eui-64`

D. Router(config-if)#`ipv6 address 2001:db8:1234::/64 mac`

201. You are using the EUI-64 method of allocating the host portion of the IPv6 addresses. The MAC address of the host is e5ee:f556:2434. What is the correct IP address that will be calculated for a network ID of fd00:2:2::?

A. fd00:2:2::e9ee:f5ff:fe56:2434/64

B. fd00:2:2::fffe:e5ee:f556:2434/64

C. fd00:2:2::e7ee:f5ff:fe56:2434/64

D. fd00:2:2::e2ee:f5ff:fe56:2434/64

202. Which command would you use to find the joined multicast groups for an IPv6 interface?

A. Router#`show ipv6 multicast`

B. Router#`show ipv6 interface gi 0/1`

C. Router#`show ipv6 routes`

D. Router#`show mutlicast`

203. Which type of IPv6 addressing allows for a one-to-many address for IP services?

Technet24.ir

A. Multicast address

B. Anycast address

C. Unicast address

D. Localcast address

204. What type of address is ::1/128?

A. Multicast address

B. Anycast address

C. Unicast address

D. Loopback address

205. Which type of IPv6 addressing allows for a one-to-closest address for IP services?

A. Multicast address

B. Anycast address

C. Unicast address

D. Loopback address

206. Which type of automatic address assignment will not allow for EUI-64 addressing?

A. Static addressing

B. SLAAC addressing

C. Stateful DHCPv6 addressing

D. Stateless DHCPv6 addressing

207. Which type of address always uses the EUI-64 addressing mechanism?

A. Link-local addresses

B. Global unicast addresses

C. SLAAC addresses

D. Anycast addresses

208. You have been given an IPv6 address of 2030:3454:aabb::/64. What can you conclude?

A. The IP address is a unique-local address.

B. The IP has been given to you by the Regional Internet Registry.

C. The IP has been given to you by the Internet service provider.

D. The IP has been given to you by IANA.

209. You are using the EUI-64 method of allocating the host portion of the IPv6 addresses. The MAC address of the host is 401e:32e4:ff03. What is the correct IP address that will be calculated for a network ID of fd00:3:3::?

A. fd00:3:3::fffe:421e:32e4:ff03/64

B. fd00:3:3::421e:32ff:fee4:ff03/64

C. fd00:3:3::401e:32ff:fee4:ff03/64

D. fd00:3:3::421e:32ff:ffe4:ff03/64

210. Which is a valid unique-local address?

A. fec0:1111:2e3c:eab3::5/64

B. fe80:d2e1:e24:63::25/64

C. fd00:1edc:bae:eea4::2478/64

D. fc00:4fec:ecf2:343::e44/64

Technet24.ir

Chapter 1: Network Fundamentals (Domain 1)

1. D. The OSI reference model was created to divide the network communication process into smaller components for standardization, design, and troubleshooting purposes. It also allows for a nonproprietary standardization of components and prevents a change at one layer from affecting other layers.

2. A. The Presentation layer is responsible for encryption and decryption. Web servers use SSL to encrypt data and the client uses SSL to decrypt the data. SSL processing for both server and client is done at the Presentation layer.

3. D. Switches primarily function at the Data Link layer. They inspect frames to direct traffic to the appropriate port by employing source MAC address learning and forward/filter decisions.

4. C. A simple way of remembering the order of the OSI layers is with a mnemonic such as All People Seem To Need Drinking Parties or All People Seem To Need Data Processing.

5. B. The Network layer is responsible for logical addressing. Routers use logical addressing for path determination to remote networks the same way the post office uses zip codes and street addresses to route mail.

6. A. Connection-oriented communication happens at the Transport layer with TCP. TCP uses a three-way handshake to establish a connection. Once it is established, sequences and acknowledgments make sure that data is delivered. Both server and client have a virtual circuit during the establishment.

7. D. The Presentation layer is responsible for compression and decompression. Compression methods can be MP3, JPG, and ZIP, which reduce the number of bits that need to be transmitted over the network. Often web servers use gzip to speed up page delivery. One end compresses and the other end decompresses the data.

8. C. Applications are found in the upper three layers and dialog control is found in the session layer. An example of dialog control is how an application such as instant

messaging sends messages with half-duplex conversations like a walkie-talkie.

9. B. DTE and DCE interfaces are defined at the Physical layer. The original interfaces referred to computers and modems, respectively. However, today the DTE and DCE interfaces define the equipment such as hosts and switches, respectively.

10. B. Telnet, TFTP, SNMP, and SMTP all function at the Process/Application layer according to the DoD model. The Process/Application layer is a macro layer combining the Application, Presentation, and Session layers of the OSI model.

11. A. Since SNMP is an application, if it returns back successfully, then we can conclude that the Application layer on the client successfully made a connection to the Application layer on the server.

12. B. The Data Link layer is responsible for checking the FCS, or Frame Checking Sequence, which is a checksum of the frame. This occurs on the MAC sublayer of the Data Link layer.

13. C. The Internet layer of the DoD model maps to the Network layer of the OSI model. The Network layer is where routing occurs.

14. D. Switches create collision domains by isolating the possibility of a collision to the segment it is transmitting to or receiving frames from. This in turn raises effective bandwidth for the rest of the segments.

15. B. A hub is a multiport repeater. When a hub receives a frame, it will repeat the frame on all other ports, regardless of whether or not the port is the destination host.

16. D. The segment PDU is found at the Transport layer of the OSI. TCP/IP comprises two protocols at this layer: TCP and UDP, which create segments.

17. C. A router will stop broadcasts by default. If you add a router to a flat network, which is a single broadcast domain, you effectively raise bandwidth by reducing the number of broadcasts.

18. D. When the Individual/Group (I/G) high order bit is set to 1, the frame is a broadcast or a multicast transmission. The OUI assigned by the IEEE is only partially responsible for MAC uniqueness. The vendor is responsible for the last 24 bits of a MAC address.

19. B. Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is a contention method that allows multiple devices to share the access media and detect collisions of frames.

Technet24.ir

20. C. The correct order of encapsulation starting with the Application layer is user datagrams, segments, packets, frames, and bits.

21. B. Telnet is used for terminal emulation over a network to a device expecting terminal emulation, such as a router or switch.

22. A. Logical Link Control (LLC) is responsible for identifying network protocols at the Data Link layer. This allows the Data Link layer to forward the packet to the appropriate upper-layer protocol.

23. C. The Presentation layer is responsible for translation such as ASCII to EBCDIC. All translation, encryption/decryption, and compression/decompression happens at the Presentation layer.

24. C. Broadcasts, multicasts, and multiple hubs for connectivity are all common causes of LAN congestion. Adding switches for connectivity has no direct relationship to LAN congestion, since switches create collision domains and raise effective bandwidth.

25. A. The Transport layer is responsible for flow control via the TCP/IP protocols of TCP and UDP.

26. C. User Datagram Protocol (UDP) does not guarantee segments are delivered. Therefore, the programmer must account for segments that are never received or out of order.

27. D. TCP is a connection-based protocol via the three-way handshake. It is not faster than UDP. However, it allows for the retransmission of lost segments because of sequences and acknowledgments.

28. A. The sender allocates a port dynamically above 1024 and associates it with the request through a process called a handle. This way if a web browser creates three requests for three different web pages, the pages are loaded to their respective windows.

29. D. The Simple Mail Transfer Protocol (SMTP) uses TCP port 25 to send mail.

30. D. TCP guarantees delivery of segments with sequence and acknowledgment numbers. At the Transport layer, each segment is given a sequence number that is acknowledged by the receiver.

31. A. When a programmer decides to use UDP, it is normally because the programmer is sequencing and acknowledging datagrams already. The redundancy of acknowledgments at the Transport layer is not needed.

32. B. When a daemon or server process starts, it binds to a port number on which to listen for a request. An example is when a web server binds to the port number of TCP/80.

33. A. The window size, which is a buffer, is established and agreed upon by the sender and receiver during the three-way handshake.

34. C. DNS requests are usually small and do not require the overhead of sequence and acknowledgment of TCP. If a segment is dropped, the DNS protocol will ask again.

35. A. A three-way handshake is required between sender and receiver before TCP can begin sending traffic. During this three-way handshake, the sender's window buffer size is synchronized with the receiver's window buffer size.

36. C. When more than one WAP covers the same SSID, it is called an extended service set (ESS). A wireless LAN (WLAN) controller coordinates the cell or coverage area so the same SSID is on two different channels.

37. D. Control and Provisioning of Wireless Access Points is a protocol that's responsible for provisioning of LWAPs and forwarding of data to the wireless LAN controller.

38. C. The wireless LAN controller (WLC) is responsible for centralized authentication of users and/or computers on a wireless network. When a wireless device is roaming, the WLC is responsible for maintaining the authentication between access points.

39. A. Centralized authentication of clients is a valid reason to implement a WLC. Although a WLC makes it easier to implement multiple SSIDs and VLANs, this task can be performed with autonomous WAPs, each performing its own authentication.

40. **B.** To achieve density and/or bandwidth in a relatively small area, you will need to deploy lightweight WAPS with a WLC. Although autonomous WAPS without a WLC would work, it would be problematic due to frequency coordination and roaming.

41. C. The 5 GHz band for 802.11 a/n/ac has 24 non-overlapping channels. The 2.4 GHz band for 802.11 b/g/n has only 3 non-overlapping channels. If the clients are compatible with 802.11 a/n/ac, it is desirable to use 5 GHz.

Technet24.ir

42. D. A wireless LAN controller keeps track of which LWAP a client has associated to and centrally forwards the packets to the appropriate LWAP.

43. C. In the 2.4 GHz spectrum for 802.11, there are three non-overlapping channels-1, 6, and 11, each of which is 22 MHz wide. Although channel 14 technically is non-overlapping, it is only allowed in Japan.

44. B. When WAPs are introduced to the wireless LAN controller, the WLC is responsible for synchronizing the WAPS to a standardized IOS. This allows for uniform support and features of the wireless system and is dependent on the model of WAP.

45. A. 802.11 uses a contention method of Carrier Sense Multiple Access/Collision Avoidance. 802.11 implements a Request to Send/Clear to Send mechanism that avoids collisions.

46. C. The demilitarized zone (DMZ) is where Internet-facing servers/services are placed.

47. B. Firewalls should always be placed at key security boundaries, which can be the Internet and your internal network. However, proper placement is not exclusive to the boundaries of the Internet and internal networks. For example, it could be placed between two internal networks, such as R&D and guest networks.

48. B. Firewalls cannot provide protection from internal attacks on internal resources. They are designed to protect networks from external attacks or attacks emanating from the outside or directed toward the Internet.

49. A. All physical access to a firewall should be controlled tightly so that it is not tampered with, which could allow external threats to enter the network. This control should include vendors and approved administrators. Physical access to the firewall is a security principal and therefore not a consideration for the management of a firewall.

50. C. Firewalls keep track of the TCP conversation via the SYN-SYN/ACK- ACK three-way handshake. This is done so that a DoS attack such as a SYN flood can be mitigated.

51. A. ASA allow for zones to be created and the connections applied to the zones. This methodology allows for security rules to be applied uniformly to the outside zone.

52. B. Servers should be placed in the DMZ so they can access both the inside zone and outside zone. This will allow a server such as a web server to allow client access from the Web (outside). Rules could also be applied so that the server (for example, a database server) could allow access to data from within the internal network (inside).

53. C. An IDS, or intrusion detection system, will detect unauthorized access. However, it will not prevent unauthorized access. It is a form of audit control in a network.

54. A. When a firewall matches a Uniform Resource Identifier (URI), such as a URL, it is

operating at layer 7. This is known as a web application firewall, or WAF.

55. D. Since the email server needs access to the Internet to send and receive mail, it should be placed in the demilitarized zone (DMZ). This will also allow access to internal clients in the inside zone.

56. A. AWS and Microsoft Azure are examples of public cloud providers. Private clouds are internally created, and hybrid clouds are a combination of services between your private cloud and the public cloud.

57. B. If you were looking to create a fault tolerant colocation site as a cloud provider, you would be searching for an Infrastructure as a Service provider. This would allow you to install your own operation system and applications.

58. B. The hypervisor allows for multiple operating systems to share CPUS, RAM, network, and storage of a physical server.

59. D. A virtual machine, or VM, is an operating system that is running on hardware but is not directly attached to the hardware. It is decoupled from the hardware through the use of a hypervisor. The hypervisor creates an abstraction layer between the hardware and the operating system.

60. A. The physical hardware (such as a server) used in virtualization is the host.

61. C. A virtual switch connects the virtual machine NIC to the physical network.

62. B. The End of Row (EOR) switch acts as a distribution switch for the Top of Rack (TOR) switches.

63. C. Automated billing is not a NIST criteria for cloud computing. It is

Technet24.ir

essential for the cloud computing vendor, but is not relevant if you are hosting it yourself. The five NIST criteria for cloud computing are on- demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

64. C. When an internal IT department hosts the virtualization for a company,

it is called a private cloud.

65. B. A cloud services catalog satisfies the self-service aspect of cloud computing. It does this by listing all of the available VMs that can be created in the cloud environment, such as web servers, application server, databases, and so on.

66. C. A hosted medical records service is an example of a SaaS, or Software as a Service, model. The customer cannot choose variables such as vCPU or RAM. The cloud provider is responsible for the delivery of the software, maintenance of the OS, and maintenance of the hardware.

67. A. A hosted service that allows you to develop upon it is an example of the Platform as a Service (PaaS) model. The cloud provider is responsible for the delivery of APIs that developers can use to create programs. 68. C. An intercloud exchange is a service that connects multiple public clouds through a common private WAN connection. This allows a network engineer to configure the private WAN once and be able to transition between the public clouds on the service side without reconfiguration of the private WAN.

69. A. Internal bandwidth usage is not a consideration after conversion to a SaaS application. External bandwidth should be considered since internal users will access the application through the Internet. Location of the users should also be a deciding factor in moving to a SaaS model. Branch office connectivity to the Internet should be considered also when converting.

70. B. A virtual firewall or virtual router is an example of a VNF. These devices are typically network functions that are found in internal networks such as firewalls and routers**.** These devices perform basic network functionality and run as a virtual machine or virtual instance.

71. C. You will need a virtual router running static NAT to translate the two different IP networks. This type of service is called a virtual network function, or VNF.
72. C. Network Time Protocol (NTP) is a standardized protocol for network time synchronization.

73. D. If you wanted to scale a web server out to several other web servers, you would use Server Load Balancing as a Server (SLBaaS) from your

cloud provider.

74. C. Lowering bandwidth between the premises and your VMs on the public cloud is a direct benefit if locating NTP on the public cloud for VM time synchronization.

75. A. Bandwidth is the primary decision factor for moving DNS closer to the application in the public cloud. However, if the majority of DNS users are on premises, then it should remain on premises for bandwidth reasons.

76. B. Access layer switches connect to users and are edge network devices.

77. A. Distribution layer switches connect to access layer switches and core switches to provide redundancy.

78. C. Core layer switches connect campuses together via the distribution layer switches.

79. C. The two-tier, or collapsed-core, model contains only the distribution and access layer switches.

80. A. Based on the layout of your network, the collapsed-core model is the most appropriate model to design. If at a later time other campuses are joined to the network, the core layer can be added.

81. B. Based on the layout of your network the three-tier model is the most appropriate model to design. Since there are four campuses, the core layer is recommended for connectivity.

82. D. Only switching between campus (distribution) switches should be performed at the core layer. Nothing should be done to slow down forwarding of traffic, such as using ACLs, supporting clients, or routing between VLANs.

83. B. The distribution layer is where redistribution of routing protocols should be performed. It should never be performed at the core or access layer.

84. C. The access layer is where collision domains should be created. This

is called network segmentation.

85. C. The collapsed-core design model is best suited for small enterprises. It can later be expanded out to a three-tier model as an enterprise grows in size. It has no effect on bandwidth if designed right.

86. A. A star topology has a centralized switch connecting all of the devices outward like a star.

87. B. Increased redundancy of connections is a direct benefit of a full mesh topology. Although bandwidth will increase because of multiple paths, additional dynamic routing protocols will need to be implemented to achieve this.

88. C. The hybrid topology is most often seen at the access layer. The devices are connected in a star topology and the access layer switches are partially meshed to the distribution layer switches.

89. B. Distribution layer switches are fully meshed for redundancy. The number of links can be calculated with the formula of N(N − 1). So if you had four distribution switches, the ports required for a full mesh would be 4(4 − 1) = 4 × 3 12 ports among the four switches. The formula of N (N - 1) / 2 would give you the number of links (connected ports): 4(4 − 1) / 2 = 4×3/2=6 links.

90. A. Core layer switches are commonly set up in a star topology. This is because core layer switches connect multiple campuses via distribution layer switches.

91. A. The collapsed core layer switch uses a star topology connecting outward to the access layer switches. This design is often found in small enterprise and single campus design.

92. B. All links between switches are connected redundantly. This allows for both the forwarding plane and control plane to have multiple paths and redundancy. The forwarding plane forwards traffic, and the control plane controls routing between VLANs.

93. A. In a star topology, the central switch is connected outward to all edge switches. This is commonly seen at the core layer switch.

94. A. An autonomous WAP acts similarly to an access layer switch. However, WAPs normally do not have redundant links back to the distribution switches. So it acts more like a star topology, connecting the Ethernet and wireless clients together.

95. C. Generally, office buildings do not have direct runs to each switch closet from the other closets. Although a full mesh is desirable, sometimes only a partial mesh is achievable.

96. A. 1000Base-T is short for 1000 Baseband - Twisted pair. 1000Base-T utilizes all four pairs over standard Cat5e, whereas 100Base-T utilizes only two pairs of Cat5.

97. C. Single-mode fiber is 9 microns at its core. With proper transceivers, the signal can span 10 km to 70 km without needing to be retransmitted.

98. A. A straight-through cable would be used since routers are DTE, or data terminal equipment, and switches are DCE, or data communications equipment. DTE to DCE requires a straight-through cable.

99. A. 1000Base-T can be run up to 100 meters, or 328 feet, per its specification.

100. B. You connect to Cisco switches and routers via 900 baud, 8 data bits, no parity, and 1 stop bit.

101. B. You would use a crossover cable because a switch is a DCE device. When connecting DCE to DCE, you would need to cross the connection with a crossover cable. Newer switches have MDI-X capabilities to detect the need for a crossover cable and will automatically switch the cable over if a straight-through cable is used.

102. B. Multi-mode fiber can be either 50 microns or 62.5 microns at its core. The maximum distance for 50 micron fiber is 550 meters utilizing the 1000Base-LX specification.

103. C. Although operation of computers connected to a switch uses a straight-through cable, management via the console port requires a rolled cable and an EIA/TIA 232

adapter.

104. C. 10GBase-CX is commonly used in data centers. It is referred to by its nickname of Twinax. It is a fixed, balanced coaxial pair that can be run up to 25 meters.

105. C. Cat5e can support up to 1 Gb/s via the 1000Base-T specification. Since 10Base-T, 100Base-T, and 1000Base-T can be run up to 100 meters in length, it allows for interchangeability with speeds. It was very common when Cat5e came out 16 years ago for installers to future-proof wiring

Technet24.ir

installations with it.

106. B. It is most likely, since the interface was working before, that someone "shut down" the interface with the `shutdown` command. This can be seen in the `show interface serial 0/0` command; the interface is reporting it is administratively shut down.

107. C. Traceroute should be used from the originating IP when the problem is to the destination IP. When the traceroute times out is most likely where the problem is located.

108. C. When you're checking for speed and/or duplex issues, the `show interface status` command will detail all of the ports with their negotiated speed and duplex.

109. B. When you're diagnosing frame forwarding on a switch, the MAC address table needs to be inspected to see if the switch has learned the destination MAC address.

110. A. When you're trying to diagnose port security, the first command should be `show port-security`. This will detail all of the ports with port security and their expected behavior when port security is violated.

111. D. After isolating the problem, performing root cause analysis, and ultimately solving the problem, the implemented solution should be monitored or verified.

112. A. The first step to troubleshooting a problem is isolating the problem. This can be done various ways and can sometime include documenting the problem to understand the root cause.

113. B. The first command used to diagnose a VLAN forwarding issue is the `show vlan` command. This command will show all of the VLANs that are defined on the switch either manually or dynamically through the VLAN Trunking Protocol (VTP).

114. C. Since you only have access to the local switches at your facility and you have checked the local user's connection status, your only option is to escalate the problem.

115. A. The command that you should begin with is `show interfaces fast 0/0 switchport`. This command will show the trunk status of the port as well as the operational status.

116. B. The IP address of 172.23.23.2 is a Class B address.
117. A. The default subnet mask of a Class A address is 255.0.0.0.

118. C. The multicast range begins with 224 to 239 in the first octet. Therefore, only the IP address 238.20.80.4 is correct.

119. B. The IP address 135.20.255.255 is a Class B broadcast address.

120. B. The CIDR notation for 255.255.240.0 is /20. The first two subnets are 8 bits (8 × 2 = 16), and the 240 is 4 more bits (16 + 4 = 20).

121. A. The mask you will need to use is 255.255.255.252. This will allow for two hosts per network for a total of 64 networks. The formula for solving for hosts is: 2X – 2 is equal to or greater than 2(hosts), which in this case is (22 − 2) = (4 − 2) = 2. So 2 bits are used for the host side, leaving 6 bits for the subnet side. 6 bits + 24 bits (original subnet mask) = /30, or 255.255.255.252.

122. D. The mask you will need to use is 255.255.255.224. This will allow for 30 hosts per network for a total of eight networks. The formula for solving for hosts is: 2X – 2 is equal to or greater than 22 hosts, which in this case is (25 − 2) = (32 − 2) = 30. So 5 bits are used for the host side, leaving 3 bits for the subnet

side. 3 bits + 24 bits (original subnet mask) /27, or 255.255.255.224.

123. A. The valid IP address range for the 192.168.32.0/26 network is 192.168.32.1 to 192.168.32.62, 192.168.32.65 to 192.168.32.126, etc. Therefore, 192.168.32.59 is within the valid IP range of 192.168.32.61/26.

124. B. The subnet mask will be 255.255.240.0. Since you need to solve for the number of networks, the equation is: 2o is equal to or greater than 15 networks. 24 16 completed the equation; the 4 bits represent the subnet side; you add the 4 bits to the 16 bits of the class B subnet mandated by the IETF. 16 + 4 = /20 = 255.255.240.0.

125. C. The valid IP address range for 209.183.160.45/30 is 209.183.160.45-209.183.160.46. Both IP addresses are part of the 209.183.160.44/30 network. 209.183.160.47/30 is the broadcast address for the network.

126. C. Computer A's default gateway address is 192.168.1.63. This address is the broadcast address for the 192.168.1.0/26 network and cannot be used as that network's gateway.

Technet24.ir

127. A. Computer A needs to have its IP address changed to align with the network that its gateway is in. Computer A is in the 192.168.1.32/27 network, while its gateway address is in the 192.168.1.0/27 network. Although changing the gateway address would work, the least amount of effort needs to be done. Changing the gateway address, which is a valid IP address, would create more work for other clients.

128. B. The /21 subnet mask has subnets in multiples of 8. So the networks would be 131.50.8.0/21, 131.50.16.0/21, 131.50.32.0/21, and 131.50.40.0/21. The IP address of 131.50.39.23/21 would belong to the 131.50.32.0/21 network with a valid range

of 131.50.32.1 to 131.50.39.254.

129. D. The network for the computer with an IP address of 145.50.23.1/22 is 145.50.20.0/22. Its valid range is 145.50.20.1 to 145.50.23.254; the broadcast address for the range is 145.50.23.255.

130. B. The valid IP address range for the network of 132.59.34.0/23 is 132.59.34.1 to 132.59.35.254. The first address of 132.59.34.0/23 is the network ID and the last address of 132.59.35.255 is the broadcast ID.

131. B. The /20 CIDR notation written out is 255.255.240.0. The first two 8 bits are 255.255, and the last 4 bits make up the subnet mask of 250 to make a complete mask of 255.255.240.0.

132. C. The network mask of 255.255.255.248 borrows 5 bits for the network mask. Using the formula of 2o = subnets, 25 = 32 subnets.

133. D. The valid number of hosts for a network with a subnet mask of 255.255.255.224 is 30. If 224 uses 3 bits of the 8 bits available for the network ID, then 5 bits remain for the host portion of the IP address. Using the formula of 2× - 2 = valid hosts, 25 − 2 = 32 − 2 = 30 valid hosts.

134. D. The valid IP range for the network of 141.23.64.0/19 is 141.23.64.1 to 141.23.95.254. The IP address of 141.23.90.255/19 is a valid IP address within this range.

135. C. Summarization is similar to subnetting, with the exception that you are grouping IP addresses together. Think of it as reverse subnetting. Since /22 is multiples of 4, the statement of 141.24.4.0/22 would give the following range of IP addresses to be blocked: 141.24.4.1 to 141.24.7.254.

136. B. Summarization is similar to subnetting, with the exception that you are grouping IP addresses together. Think of it as reverse subnetting.
Since /21 is multiples of 8, the statement of 132.22.24.0/21 would give the following range of IP addresses to be blocked: 132.22.24.1 to 132.22.31.254.

137. A. Using the subnet of 198.33.20.0/25 will give you 126 nodes. Since you are

using 1 bit of the 8 bits in the 4th octet for the network ID, you have 7 bits left for the hosts. Using the formula of 2o − 2 = valid hosts, 27 - 21282 = 126 valid hosts.

138. C. Using the subnet of 198.33.20.0/26 will give you 62 nodes. Since you are using 2 bits of the 8 bits in the 4th octet for the network ID, you have 6 bits left for the hosts. Using the formula of 2* − 2 = valid hosts, 26 -2=642 = 62 valid hosts.

139. D. Using the subnet of 198.33.20.0/28 will give you 16 nodes. Since you are using 4 bits of the 8 bits in the 4th octet for the network ID, you have 4 bits left for the hosts. Using the formula of 2 − 2 = valid hosts, 24 -2=16 2= 14 valid hosts.

140. D. The computer had an IP address of 172.18.40.5/12 and it belongs to the 172.16.0.0/12 network, which has a range of 172.16.0.1 to 172.31.255.254. Therefore, the internal server is within the same network as the computer, and the default gateway has no effect on the problem. The conclusion is that the network is not the problem.

141. C. The computer and the gateway address are correct; the IP address of the remote server is wrong. It is a loopback address and can only be internally used by the local computer. The valid range for loopback is 127.0.0.1 to 127.255.255.254.

142. B. A layer 3 broadcast is always all ones in the host portion of the IP address. When the IP stack see this, it puts all *Fs* in the destination Ethernet MAC address.

143. A. A unicast address is a single valid IP address for direct communications purposes between two hosts.

144. D. Anycast is a way of allowing the same IP address on multiple machines in different geographical areas. The routing protocol is used to advertise in routing tables the closest IP by the use of metrics. Currently this is how DNS root servers work.

145. C. Multicast is used to allow computers to opt into a transmission. Examples

of uses for multicast are imaging of computers, video, and

Technet24.ir

routing protocols, to name a few.

146. D. The multicast address range is 224.0.0.0 to 239.255.255.255. The /4 depicts a subnet of 16.

147. B. IGMP, or Internet Group Messaging Protocol, allows switches to join computers to the multicast group table. This allows the selective process of snooping to occur when a transmission is sent.

148. B. DHCP uses a packet called a Discover packet. This packet is addressed to 255.255.255.255. Although ARP uses a broadcast, it is a layer 2 broadcast, not a layer 3 broadcast.

149. B. A broadcast will forward a message to all computers in the same subnet.

150. C. The multicast address range is 224.0.0.0 to 239.255.255.255.

151. C. RFC 1918 defines three private address ranges, which are not routable on the Internet.

152. A. The private IP address space was created to preserve the number of public IP addresses.

153. D. Network Address Translation (NAT) is required to communicate over the Internet with private IP addresses.

154. A. The Class A private IP address range is defined as 10.0.0.0/8. The address range is 10.0.0.0 to 10.255.255.255.

155. C. The Class **B** private IP address range is defined as 172.16.0.0/12. The address range is 172.16.0.0 to 172.31.255.255.

156. C. Although a Class C address has a classful subnet mask of 255.255.255.0, the private IP address range put aside for Class C addresses is 192.168.0.0 to 192.168.255.255, written in CIDR notation as 192.168.0.0/16.

157. D. Any address in the range of 169.254.0.0/16 is a link-local address. It means that the computer has sensed that a network connection is present, but no DHCP is present. The network only allows local communications and no routing. Microsoft refers to this as an APIPA address.

158. C. The network seems to be configured properly. You have received a valid address in the Class A space of the RFC 1918 private address range.

159. D. 198.168.55.45 is a valid IPv4 public address. All of the other addresses are RFC 1918 compliant and thus non-routable on the Internet.

160. A. IANA, or the Internet Assigned Numbers Authority, is the governing body, which distributes public IP addresses and registers them to ISPs.

161. B. IPv4 allows for 232 = 4.3 billion addresses. However, only 3.7 billion are usable, because of reservations and classful addressing. The current IPv4 address space is exhausted and IPv6 allows for 2128 = 3.4 × 1038.

162. C. An IPv6 address is 128 bits: 64 bits is the network ID, and 64 bits is the host ID.

163. D. A 6to4 tunnel can be achieved between the routers. This encapsulates the IPv6 header in an IPv4 header so that it can be routed across the Internet.

164. D. In order to enable IPv6 on a router, you must globally configure the router with the command `ipv6 unicast-routing`. Although `ipv6 enable` will work, it will allow only link-local addressing.

165. D. When you configure routers, always use the rule of major/minor. The major protocol is `ipv6`, and the minor command is `address`. So the correct command is `ipv6 address 2001:0db8:85aa: 0000:0000:8a2e:1343:1337/64`. The additional rule is to specify the network portion with a `/64`.

166. A. The first 4 bits of an IPv6 header contain the version number. In an IPv4 packet, this

is set to 0100, but in an IPv6 packet, this number is set to 0110. This allows for the host to decide which stack to process the packet in.

167. D. When you configure routers, always use the rule of major/minor. The major protocol is `ipv6` and the minor command is route. So the correct command is `ipv6 route ::0/0 0/0`, specifying the `::0/0 s0/0` to mean everything out of the existing interface of so/o.

168. A. When you use a `show` command, always follow it with the major protocol and then the parameters. The `show ipv6 interfaces brief` command would show all of the interfaces configured with an IPv6 address.

169. D. RIPng, OSPFv3, and EIGRPv6 are all dynamic routing protocols

Technet24.ir

that work with IPv6.

170. C. The command `show ipv6 route` will display only the IPv6 routes in the routing table.

171. D. You can remove leading os in the quartet, and you can condense four zeros to one zero. However, you can use the :: to remove zeros only once.

172. C. Expanding out the IP of 2001::0456:0:ada4, you first expand the :0: to four zeros. Then expand the remainder of the quartets to Os to make a 32-digit number again.

173. B. The first 48 bits of an IPv6 address is the global prefix; the next 16 bits is the subnet portion of the IPv6 address. 48 bits + 16 bits = 64 bits for the network ID.

174. A. The network prefix is 2001:db8::/64. Expanded it is written as 2001:0db8:0000:0000/64. However, the condensed version written in the answer is valid.

175. C. The command to ping an IPv6 address is `ping6`. The valid condensed address for fc00:0000:0000:0000:0000:0000:0000:0004 is fco0::4. You cannot

condense trailing zeros such as fcoo. You can only condense leading zeros.

176. **B.** The address 2001:db8::2435 is a valid IP address. It is shortened by removing leading zeros and condensed. You cannot clip off the trailing zeros in an address like fe80::1. Also, ffo2::1 is a multicast address and cannot be used for host addressing.

177. C. A single interface can be configured with multiple addresses. Most host interfaces will have a link-local address for duplicate address detection.

178. B. The answer is 4,096 subnets. You have been given the first 52 bits from your ISP. However, the complete network ID is 64 bits. You subtract 52 bits from 64 bits = 12 bits, then 212 = 4,096.

179. B. The answer is 16,384 networks. You subtract 34 bits from 48 bits 14 bits, then 214 = 16384.

180. D. In between each set of colons or field there are four hex numbers, and each hex number represents 4 bits. Four numbers × 4 bits = 16 bits. In an IPv6 address, there are eight fields of 16 bits. Eight fields x 16 bits bit address.

128

181. D. The correct command to configure Stateless Address Autoconfiguration is `ipv6 address autoconfig`. Although `ipv6 address dhcp` is a valid command, it requires a stateful DHCP server.

182. B. Router solicitations are sent on a multicast address of ffo2:2. This address is a local scope multicast to all IPv6 routers.

183. D. Router advertisements are sent on a multicast address of ffo2:1. This address is a local scope multicast to all IPv6 hosts.

184. A. The Neighbor Discovery Protocol uses Neighbor Solicitation and Neighbor Advertisements messages to look up an IP address from a MAC address through the use of multicast.

185. C. The layer 3 protocol that Neighbor Discovery Protocol uses to process Stateless Address Autoconfiguration are ICMPv6 messages.

186. D. Stateless DHCPv6 servers are used to configure DHCP options only. The one option that all clients need is the DNS server.

187. D. You can set the IPv6 DHCP relay agent on the interface for a stateful DHCPv6 server using the command `ipv6 dhcp relay destination 2001: db8:1234::1`.

188. **B.** Duplicate Address Detection, or DAD, uses Neighbor Solicitation and Neighbor Advertisement messages to avoid duplicate addresses when SLAAC is being used.

189. B. Stateful DHCPv6 uses a process similar to DORA for IPv4. However, IPv6 uses multicast in lieu of broadcasts via the DHCPv6 Solicit multicast address.

190. C. Before a host can communicate via an RS packet, it first needs a valid IP address. The first address is a link-local address so that it can send an RS packet and receive an RA packet. The client performs DAD on both the link-local address and the proposed address.

191. B. The global unicast address is defined as 2000::/3. This provides a valid range of 2000:: to 3fff::.

192. A. The link-local address is defined as fe80::/10. Any address starting with fe80 is non-routable.

Technet24.ir

193. A. The first 23 bits are allotted to the ISP by the RIR for the region of the world for which the ISP is requesting the prefix.

194. C. The unique-local address is defined as fcoo::/7. Unique-local addresses have replaced site-local addresses as of 2004 and are non- routable. The valid IPv6 range is fcoo:: to fdoo:: despite IANA reserving fcoo::/7 as the fcoo:: range. The range

should not be used since the 8th bit is considered the "local bit" and is required to be a 1, as in, for example, 1111 1101 = fd.

195. D. The multicast address is defined as ffoo::/8. Multicast addresses always start with *ff*.

196. A. IPv4 RFC 1918 addresses are defined as private non-routable IP addresses. In IPv6, link-local addresses are the equivalent to RFC 1918 addresses and are non-routable.

197. D. The command to configure an anycast address on an interface would be `ipv6 address 2001:db8:1:1:1::12/128 anycast`. The /128 defines a single IP to advertise in routing tables.

198. A. When converting a MAC address to an EUI-64 host address, the first step is to split the MAC address into 6-byte sections of f42356 and 345623 and place *fffe* in between them, f423:56ff:fe34:5623. This gives you a 64-bit value comprised of a 48-bit MAC address and a 16-bit filler. You must then invert "flip" the 7th bit. Example: f4 = 1111 010 = flipped 1111 0110 = f6.

199. C. The EUI-64 address can always be found by looking at the last 64 bits. In between the last 64 bits of the address, you will always find *fffe*.

200. C. The command to set an EUI-64 address for the host portion of the IPv6 address on an interface is `ipv6 address 2001: db8:1234::/64 eui-64`.

201. C. When converting a MAC address to an EUI-64 host address, the first step is to split the MAC address into 6-byte sections of e5eef5 and 562434 and place *fffe* in between them: e5ee:f5ff:fe56:2434. This gives you a 64-bit value comprised of a 48-bit MAC address and a 16-bit filler. You must then invert "flip" the 7th bit. Example: e5 = 1110 011 = flipped 1110 0111 = e7.

202. B. The output of `show ipv6 interface gi 0/1` shows the

multicast groups the interface has joined.

203. A. A one-to-many IPv6 address is a multicast address. One multicast address will allow many IPv6 clients to receive the transmission.

204. D. The ::1 address is a special address called a loopback address, similar to 127.0.0.1 in IPv4.

205. B. A one-to-closest IPv6 address is an anycast address. Many routers or services can have the same address. However, routing protocols allow for the client to be directed to the closest resource.

206. C. Stateful DHCPv6 addressing will not allow EUI-64 addressing. This is because the DHCPv6 server is responsible for allocating an IPv6 address from a predefined pool.

207. A. Link-local addresses starting with fe80::/10 always configure the host portion of the address with an EUI-64 address. Note that Microsoft products default to a random host ID and can be configured to generate the host ID with EUI-64.

208. C. The IPv6 address has been given to you by the ISP with your company's unique identifier. The first 32 bits are allocated to the ISPs, and they in turn add a unique 16-bit address for your company. This makes 32 bits + 16 bits = 48 bits. You have 16 bits for subnetting after the first 48 bits to make a full 64-bit network ID.

209. B. When converting a MAC address to an EUI-64 host address, the first step is to split the MAC address into 6-byte sections of 401e32 and e4ff03 and place *fffe* in between them: 401e:32ff:fee4:ff03. This gives you a 64-bit value comprised of a 48 bit MAC address and a 16 bit filler. You must then invert "flip" the 7th bit. Example: 40 = 0100 000 = flipped

0100 0010 = 42.

210. C. Although the unique-local address scope is defined as fcoo::/7, RFC 4193 states that the 8th bit must equal a one for the local (L) bit. This requires the address to always start with fd which in binary is 1111 =

= f and

1101 = d or 1111 1101 =
fd.

Technet24.ir

CCE 313 – VIVA QS

1. What Is the Internet?
   Ans: The Internet is **a global network of billions of computers and other electronic devices**. With the Internet, it's possible to access almost any information, communicate with anyone else in the world, and do much more. You can do all of this by connecting a computer to the Internet, which is also called going online.

2. What is a network in a computer?
   Ans: A computer network is **a system that connects two or more computing devices for transmitting and sharing information**. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also be wireless.

3. What is the purpose of nuts and bolts?
   Ans: Bolts and nuts are used to permanently or semi-permanently fasten materials, usually metal. A nut is an attachment that fits the end of a bolt and strengthens its holding power. The bolt, which is non-tapered, then holds the part fastened with the nut.

4. What is SMTP?
   Ans: SMTP - Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers.

5. What do you know about DNS?
   Ans: The DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites. DNS implements a distributed database to store this name and address information for all public hosts on the Internet.

6. Tell me something about Telnet?
   Ans: Telnet is the main Internet protocol for creating a connection to a remote server.

7. Can you explain Application layer?
   Ans: The application layer is located at the top of the TCP/IP protocol layers. This one contains the network applications which make it possible to communicate using the lower layers. The software in this layer therefore communicates using one of the two protocols of the layer below (the transport layer), i.e. TCP or UDP. In computer networking, an application layer firewall is a firewall operating at the application layer of a protocol stack. Generally it is a host using various forms of proxy servers to proxy traffic instead of routing it. As it works on the application layer, it may inspect the contents of the traffic, blocking what the firewall administrator views as inappropriate content, such as certain websites, viruses, and attempts to exploit known logical flaws in client software, and so forth. An application layer firewall does not route traffic on the network layer. All traffic stops at the firewall which may initiate its own connections if the traffic satisfies the rules.

8. What is Brute force attack?
   Ans: In cryptography, a brute force attack is a strategy used to break the encryption of data. It involves traversing the search space of possible keys until the correct key is found. The selection of an appropriate key length depends on the practical feasibility of performing a brute force attack. By obfuscating the data to be encoded, brute force attacks are made less effective as it is more difficult to determine when one has succeeded in breaking the code.

9. Explain FTP Spoofing attack?
   Ans: In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

10. Explain FTP bounce attack?
    Ans: FTP bounce attack is an exploit of the FTP protocol whereby an attacker is able to use the PORT command to request access to ports indirectly through the use of the victim machine as a middle man for the request.

11. What is NAT traversal?
    Ans: The representation of the IP addresses and port numbers in the PORT command and PASV reply poses a challenge to FTP in traversing Network address translators (NAT). The NAT device must alter these values, so that they contain the IP address of the NAT ed client, and a port chosen by the NAT device for the data connection. The new address and port will probably differ in length in their decimal representation from the original address and port. Such translation is not usually performed in most NAT devices, but special application layer gateways exist for this purpose.

12. Explain Remote FTP or FTPmail?
    Ans: Where FTP access is restricted, a remote FTP or FTPmail service can be used to circumvent the problem. An email containing the FTP commands to be performed is sent to a remote FTP server, which is a mail server that parses the incoming email, executes the FTP commands, and sends back an email with any downloaded files as an attachment. Obviously this is less flexible than an FTP client, as it is not possible to view directories interactively or to modify commands, and there can also be problems with large file attachments in the response not getting through mail servers. As most internet users these days have ready access to FTP, this procedure is no longer in everyday use.

13. Explain security concerns of FTP?
    Ans: The original FTP specification has many security concerns. In May 1999, the following flaws were addressed:
        - ► Bounce Attacks
        - ► Spoof Attacks
        - ► Brute Force Attacks
        - ► Sniffing

- ► Username Protection
- ► Port Stealing

14. What is File Transfer Protocol (FTP)?
    Ans: FTP (File Transfer Protocol) is a standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server applications, which solves the problem of different end host configurations (i.e., Operating System, file names). File Transfer Protocol is used with user-based password authentication or with anonymous user access.

15. Describe the different roles of HTTP?
    Ans: In HTTP, there are two different roles: server and client. In general, the client always initiates the conversation; the server replies. HTTP is text based; that is, messages are essentially bits of text, although the message body can also contain other media. Text usage makes it easy to monitor an HTTP exchange.

16. What is the mean of GET?
    Ans: GET is the simplest type of HTTP request method; the one that browsers use each time you click a link or type a URL into the address bar. It instructs the server to transmit the data identified by the URL to the client. Data should never be modified on the server side as a result of a GET request. In this sense, a GET request is read-only, but of course, once the client receives the data, it is free to do any operation with it on its own side - for instance, format it for display.

17. What are response codes in HTTP?
    Ans: HTTP response codes standardize a way of informing the client about the result of its request.
    You might have noticed that the example application uses the PHP header(), passing some strange looking strings as arguments. The header() function prints the HTTP headers and ensures that they are formatted appropriately. Headers should be the first thing on the response, so you shouldn't output anything else before you are done with the headers. Sometimes, your HTTP server may be configured to add other headers, in addition to those you specify in your code.

18. Explain about persistent connections?
    Ans:In HTTP/0.9 and 1.0, the connection is closed after a single request/response pair. In HTTP/1.1 a keep-alive-mechanism was introduced, where a connection could be reused for more than one request.

19. Explain secure HTTP?
    Ans: There are currently two methods of establishing a secure HTTP connection: the https URI scheme and the HTTP 1.1 Upgrade header, introduced by RFC 2817. Browser support for the Upgrade header is, however, nearly non-existent, so HTTPS is still the dominant method of establishing a secure HTTP connection. Secure HTTP is notated by the prefix https:// instead of http:// on web URIs.

20. What is Idempotent methods and web applications?
    Ans: Methods PUT and DELETE are defined to be idempotent, meaning that multiple identical requests should have the same effect as a single request. Methods GET, HEAD, OPTIONS and TRACE, being prescribed as safe, should also be idempotent, as HTTP is a stateless protocol.

21. Tell me what happens to an undeliverable datagram?
    Ans: An undeliverable datagram is discarded and an ICMP error message is sent to the source host.

22. When IP is a best-effort protocol in HTTP?
    Ans: IP is a best-effort protocol, because it will make every effort to always transmit a datagram and also datagrams will not be just discarded. However, the delivery of the datagram to the destination is not guaranteed.

23. Which OSI layer does IP belong?
    Ans: IP belongs to the Network Layer (layer 3) in the OSI model. Internet protocol is working in network layer of osi model in congection with tcp tx layer protocol.

24. What is the meaning of PUT?
    Ans: A PUT request is used when you wish to create or update the resource identified by the URL. For example, 1 PUT /clients/robin might create a client, called Robin on the server. You will notice that REST is completely backend agnostic; there is nothing in the request that informs the server how the data should be created - just that it should. This allows you to easily swap the backend technology if the need should arise. PUT requests contain the data to use in updating or creating the resource in the body. In cURL, you can add data to the request with the -d switch.
    1 curl -v -X PUT -d "some text"

25. What is the mean of 500 Internal Server Error HTTP response codes?
    Ans: When all else fails; generally, a 500 response is used when processing fails due to unanticipated circumstances on the server side, which causes the server to error out.

26. What is the mean of 409 Conflict HTTP response codes?
    Ans: This indicates a conflict. For instance, you are using a PUT request to create the same resource twice.

27. What is the mean of 405 Method Not Allowed HTTP response codes?
    Ans: The HTTP method used is not supported for this resource.

28. What is the mean of 401 Unauthorized HTTP response codes?
    Ans: This error indicates that you need to perform authentication before accessing the resource.

29. What is the mean of 404 Not Found HTTP response codes?

Ans: This response indicates that the required resource could not be found. This is generally returned to all requests which point to a URL with no corresponding resource.

30. What is the mean of 400 Bad Request HTTP response codes?
    Ans: The request was malformed. This happens especially with POST and PUT requests, when the data does not pass validation, or is in the wrong format.

31. What is the mean of 201 Created HTTP response codes?
    Ans: This indicates the request was successful and a resource was created. It is used to confirm success of a PUT or POST request.

32. What is 200 OK HTTP response codes?
    Ans: This response code indicates that the request was successful.

33. What are the safe and unsafe methods of HTTP?
    Ans: safe methods are those that never modify resources. The only safe methods, from the four listed above, is GET. The others are unsafe, because they may result in a modification of the resources.

34. For what purposes POST is used?
    Ans: POST is used when the processing you wish to happen on the server should be repeated, if the POST request is repeated (that is, they are not idempotent; more on that below). In addition, POST requests should cause processing of the request body as a subordinate of the URL you are posting to.

35. What is the mean of URLS in HTTP?
    Ans: URLs are how you identify the things that you want to operate on. We say that each URL identifies a resource. These are exactly the same URLs which are assigned to web pages. In fact, a web page is a type of resource.

36. What is cURL in HTTP?
    Ans: cURL is a command line tool that is available on all major operating systems.

37. What are request methods?
    Ans: HEAD: Asks for the response identical to the one that would correspond to a GET request, but without the response body. This is useful for retrieving meta-information written in response headers, without having to transport the entire content.

    GET: Requests a representation of the specified resource. Requests using GET (and a few other HTTP methods) "SHOULD NOT have the significance of taking an action other than retrieval". The W3C has published guidance principles on this distinction, saying, "Web application design should be informed by the above principles, but also by the relevant limitations." See safe methods below.

POST: Submits data to be processed (e.g., from an HTML form) to the identified resource. The data is included in the body of the request. This may result in the creation of a new resource or the updates of existing resources or both.

PUT: Uploads a representation of the specified resource.

DELETE: Deletes the specified resource.

TRACE: Echoes back the received request, so that a client can see what (if any) changes or additions have been made by intermediate servers.

OPTIONS: Returns the HTTP methods that the server supports for specified URL. This can be used to check the functionality of a web server by requesting '*' instead of a specific resource.

CONNECT: Converts the request connection to a transparent TCP/IP tunnel, usually to facilitate SSL-encrypted communication (HTTPS) through an unencrypted HTTP proxy.

PATCH: Is used to apply partial modification

38. Explain How Does SMTP Work?
    Ans: SMPT is responsible for transmitting email across Internet networks (IPs). This technology is used specifically for sending outgoing email. Clients typically use applications such as Internet Message Access Protocol (IMAP) or Post Office Protocol (POP) to access to their email box. For example, if you send an email it goes to a mail server using SMTP. The mail client will then deliver it to the user's mailbox.

39. Explain Address Resolution Protocol ARP?
    Ans: Address Resolution Protocol ARP, is responsible for mapping an IP address to its corresponding physical network address. It is mostly seen on Ethernet network.

40. Do you know Maximum Transfer Unit, MTU?
    Ans: MTU specifies the largest amount of data that can be transferred across a network.

41. What is a Loopback Address?
    Ans: A loopback address is the one, which normally used internally by the system to point to itself. This is different from another Public or Private IP Address. This is mostly used to call the local system and for troubleshooting purposes. The default Loopback IP Address is 127.0.0.1

42. What is Default Gateway?
    Ans: A Default Gateway is an address to which all the packets to which there is no known Route is available is been sent. In other words, if the system doesn't know where to send a set of packets, it will forward it to this address which then takes care of routing to appropriate destinations.

43. What is IPV6?
    Ans: As the Internet is flooded with more and more networks and computers, the system is now slowly running out of available addresses to fit in more networks or computers. For this reason, IPV6 is being designed. This is a new version of the IP protocol addressing method (V6 is Version 6) which is to slowly and steadily replace the existing IPV4 (V4 is version 4).

44. What is a Subnet mask?
    Ans: A Subnet Mask is an address mask that allows, systems to differentiate between the Network ID from that that of the Host Ids in a IP Address. This is represented very much as how an Ip address is represented.

45. Explain the concept of TCP/IP
    Ans: The primary purpose of TCP/IP is to deliver data packets between the source application or the device and the destination using different methods and structures that place tags such as address information within data packets. TCP/IP helps connect devices over the Internet and to transmit data from one device to another.

46. What is the difference between flow control and error control?
    Ans: Flow control is a method that maintains proper data transmission from the sender to the receiver. Error control ensures the delivery of error-free data from the sender to the receiver. Flow control avoids overrunning and prevents data loss. In contrast, error control detects and corrects the errors which may have occurred during transmission.

47. What is a socket?
    Ans: A socket programming interface offers the routines required for interprocess communication between programs on the local system or spread throughout a distributed TCP/IP-based network environment. Once a connection gets established, a socket descriptor specifically identifies a peer-to-peer connection.
    Example: "A TCP/IP socket often communicates between two computers. It includes the IP address and the host that those computers use to transmit data. All the applications in the transmission use the socket to send and receive information.

48. What is the function of a router?
    Ans: The router is a networking device that can forward data packets between computer networks and perform traffic-directing functions on the Internet. You can mention a few of its functions in your answer to this question.

49. What are Pvt. IP address?
    Ans: The private IP address of a system is the IP address that is used to communicate within the same network. Using private IP data, information can be sent or received within the same network. For more details please refer difference between private and public IP addresses.

50. How TCP protocol provides reliability?

Ans:TCP is reliable as it uses checksum for error detection, attempts to recover lost or corrupted packets by re-transmission, acknowledgment policy, and timers. It uses features like byte numbers and sequence numbers and acknowledgment numbers so as to ensure reliability.

51. Write down the name of services provided by TCP?
    Ans: Process to process communication
    Stream orientation
    Full duplex service
    Multiplexing
    Reliability
52. The name of all TCP “Flag”?

ans: A TCP Flag field contains 6 different flags, namely:
URG: Urgent pointer is valid
ACK: Acknowledgement number is valid(used in case of cumulative acknowledgment)
PSH: Request for push
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: Terminate the connection

53. Explain how is the TTL field used to prevent indefinite looping of IP datagrams?

    Ans: The TTL field contains a counter value set by the source host. Each gateway that processes this datagram, decreases the TTL value by one. When the TTL value reaches zero, the datagram is discarded.

54. What is the byte order used for transmitting datagram headers in the TCP/IP protocol suite?

    Ans: All the datagram headers in the TCP/IP protocol suite are transmitted in the "big endian" byte order. i.e. The most significant byte is transmitted first. This is also called as "network byte order".

55. Why there are two length fields (IP header length, IP datagram length) in the IP header?

    Ans: The size of the IP header is not fixed. Depending on the IP options present, the size of the IP header will vary. A separate field for the IP header length is added, so that the destination system can separate the IP datagram header from the payload.

56. What is the typical value for the TTL field?
    Ans: The typical value for a TTL field is 32 or 64.

57. Which RFC discusses the Type Of Service (TOS) field?
    Ans: RFC 1349 discusses the Type Of Service (TOS) field.

58. What is the use of the Time To Live (TTL) field in the IP header?

Ans: The TTL field is used to limit the lifetime of a IP datagram and to prevent indefinite looping of IP datagrams. Time To Live is used to limit the period of time of transmission of network technology.

59. Is the datagram identifier field unique for each IP datagram?
    Ans: Yes. The IP datagram identifier field is different for each IP datagram transmitted. The fragments of an IP datagram will have the same identifier value.

60. Explain congestion?

    Ans: A state occurring in the network layer when the message traffic is so heavy that it slows down network response time is known as congestion. For more details please read TCP congestion control article.

61. What is UDP protocol?

    Ans: User Data Protocol is a communication protocol. It is normally used as an alternative for TCP/IP. However there are a number of differences between them. UDP does not divide data into packets. Also, UDP does not send data packets in sequence. Hence, the application program must ensure the sequencing. UDP uses port numbers to distinguish user requests. It also has a checksum capability to verify the data.

62. What is TCP windowing concept?

    Ans: TCP windowing concept is primarily used to avoid congestion in the traffic. It controls the amount of unacknowledged data a sender can send before it gets an acknowledgement back from the receiver that it has received it.

63. Which is the faster protocol either UDP or TCP?

    UDP is the faster protocol as it doesn't wait for acknowledgement so it is not at all having reliability as compared to TCP.

64. Is the ip address of computer and modems is same or not?

    No. The IP address of a system is the logical address whereas the address of the MODEM is the MAC(Media Access Control) adderess, it is the physical address provided by the vendor.

65. What is throjan?

    Named after the Trojan Horse of ancient Greek history, a trojan is a network software application designed to remain hidden on an installed computer. Trojans generally serve maliciious purposes and are therefore a form of malware, like viruses. Trojans sometimes, for example, access

personal information stored locally on home or business computers, then send these data to a remote party via the Internet.

66. What do you mean about isp, and what is work?

    ISP: (internet service providers)who provides internet services work of ISP:
    1) providing internet services i.e ips
    2) web server sevices
    3) Virtual hosting (manage web server ,domain and users intenet related works)

67. Can SSL support UDP, as SSL support TCP?

    Ans: No SSL cannot support in UDP beacuse in UDP is a connectionless protocol it is focused on the speed than the security.

68. What is a peer-to-peer process?
    Ans: A peer-to-peer process refers to all processes on a machine that communicates at a given layer.

69. Define network topology.
    Ans: Network topology refers to the network's physical structure that defines how nodes or computers will be connected.

70. What is a firewall?
    Ans: A firewall is a security system concept that helps in protecting computers from any cyber-attack or unauthorized access.

71. What is meant by clustering support?
    Ans: Clustering support is the ability of a network operating system in a fault-tolerant group to connect multiple servers. The primary purpose of clustering is that if one server fails, the processing can continue with the next server in the cluster.

72. How does dynamic host configuration protocol help in network administration?
    Ans: The network administrator applies the dynamic host configuration protocol to create a pool of IP addresses instead of visiting each client computer to configure a static IP address. This pool is known as the scope that can be assigned to clients dynamically.

73. Explain Proxy Server and its function.
    Ans: IP addresses are required for data transmission and are even used by DNS to route to the correct website. Without knowledge of the actual and correct IP address, it is not possible to identify the network's physical location. Proxy servers prevent unauthorized access of IP addresses and make the computer network virtually invisible to external users.

74. What are the characteristics of networking?

Ans: The characteristics of networking are:

Medium- the channel used by computers for communication
Topology- the way computers are arranged in the network physically or logically
Protocols- deals with how computers communicate with one another.

75. What do you understand by beaconing?
Ans: When a network self-repair its issues, then it is known as beaconing. It is mainly used in Fiber Distributed Data Interface (FDDI) and token ring networks. If a device in the network faces any problem, then the devices that are not receiving any signal are notified. This way, the problem gets repaired within the network.

76. What is SLIP?
Ans: SLIP refers to Serial Line Interface Protocol. It is used for transmitting IP datagrams over a serial line. SLIP, or Serial Line Interface Protocol, is an old protocol developed during the early UNIX days. This is one of the protocols that are used for remote access.

77. What LAN is?
Ans: LAN refers to Local Area Network. It is the network between devices located in a remote physical location. It can be either wired or wireless. LANs differ from each other based on given factors:

Protocol - rules for data transfer
Media - medium for connecting like twisted pair wires and optic fibers
Topology - arrangement of nodes in the network

78. What is meant by NOS?
Ans: NOS or Network Operating System is an operating system designed to support databases, workstations, personal computers, and networks. For example, Linux, MAC OS X, Windows Server 2008. These OS provide functionalities such as multiprocessing support, processor support, web services, authentication, etc.

79. Explain piggybacking.
Ans: In two-way communication, the receiver sends an acknowledgment to the sender on receiving the data packets. Suppose the receiver does not send the acknowledgment immediately and waits till the network layer passes in the following data packet. In that case, an acknowledgment is attached to the outgoing data frame. This process is known as piggybacking.

80. What do you understand by DHCP?
Ans: Dynamic Host Configuration Protocol or DHCP is a network management protocol. DHCP automatically assigns IP addresses to the devices on the network and is used on the UDP/IP networks. In turn, it reduces the need for a network admin to assign IP addresses manually; this further reduces errors.

81. What is the best place to install an antivirus program in a network containing twenty workstations and two servers?
    Ans: The best option is to install antivirus on all the computers of the network. This will protect all devices from others in case there is a virus inserted into the server.

82. Tell us about IPv6.
    Ans: IPv6 refers to the Internet Protocol version 6. This is the latest version of the Internet Protocol. Its IP address length is 128 bits which resolve the issue of approaching network addresses shortage.

83. What do you understand by sneakernet?
    Ans: Sneakernet refers to the unofficial term for transferring electronic information by physically moving media like the USB flash, Floppy disk, optical disks, etc.

84. What is a Link?
    Ans: A link refers to the connectivity between two devices. It includes the type of cables and protocols used for one device to be able to communicate with the other.

85. What is the maximum length allowed for a UTP cable?
    Ans: A single segment of UTP cable has an allowable length of 90 to 100 meters. This limitation can be overcome by using repeaters and switches.

86. What is data encapsulation?
    Ans: Data encapsulation is the process of breaking down information into smaller, manageable chunks before it is transmitted across the network. In this process that the source and destination addresses are attached to the headers, along with parity checks.

87. What is a VPN?
    Ans: VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.

88. What is NIC?
    Ans: NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to connect to a network. Every NIC has its own MAC address that identifies the PC on the network.

89. What is the importance of implementing a Fault Tolerance System?
    Ans: A fault tolerance system ensures continuous data availability. This is done by eliminating a single point of failure.

90. What does 10Base-T mean?
    Ans: The 10 refers to the data transfer rate. In this case, it is 10Mbps. The word Base refers to baseband, as opposed to broadband.

91. What is tracert?
    Ans: Tracert is a Windows utility program that can use to trace the route taken by data from the router to the destination network. It also shows the number of hops taken during the entire transmission route.

92. What is the proper termination rate for UTP cables?
    Ans: The proper termination for unshielded twisted pair network cable is 100 ohms.

93. What is netstat?
    Ans: Netstat is a command-line utility program. It provides useful information about the current TCP/IP settings of a connection.

94. What is ICMP?
    Ans: ICMP is an Internet Control Message Protocol. It provides messaging and communication for protocols within the TCP/IP stack. This is also the protocol that manages error messages that are used by network tools such as PING.

95. What is ipconfig?
    Ans: Ipconfig is a utility program that is commonly used to identify the addresses information of a computer on a network. It can show the physical address as well as the IP address.

96. What is the difference between a straight-through and crossover cable?
    Ans: A straight-through cable is used to connect computers to a switch, hub, or router. A crossover cable is used to connect two similar devices, such as a PC to PC or Hub, to the Hub.

97. What is the client/server?
    Ans: Client/server is a type of network wherein one or more computers act as servers. Servers provide a centralized repository of resources such as printers and files. Clients refer to a workstation that accesses the server.