CompTIA

N10-008

Network+

Question: 80

Which of the following types of networking devices can split a single network into multiple collision domains while maintaining a single broadcast domain? (Choose all that apply.)

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

Answer: A, B

A bridge can split a single network into two collision domains, because it forwards only the packets that are destined for the other side of the bridge
A switch creates a separate collision domain for each port
Both bridges and switches forward all broadcast packets, so they maintain a single broadcast domain for the entire network
A hub maintains a single collision domain and a single broadcast domain
A router creates two collision domains, but it does not forward broadcasts, so it creates two broadcast domains as well

Question: 81

You have just finished installing a web server farm on your company's network, along with a router to create a screened subnet (perimeter network) on which the web servers are located. However, you now cannot access the web servers from your workstation on the internal network. Which of the following is not one of the tasks you will have to complete before you can access the screened subnet from the internal network?

A. Change MAC addresses
B. Change IP addresses
C. Update the DNS records
D. Change default gateway addresses

Answer: A

Media Access Control (MAC) addresses are hard-coded into network interface adapters and are not easily changeable
There is also no need to change them for this purpose
First, you will have to change IP addresses of the web servers

This is because the computers on the other side of the router, on the screened subnet, must use an IP network address that is different from the internal network’s address

Next, you will have to change the default gateway address setting on the internal network computers to the address of the router on the internal network so that traffic can be forwarded to the screened subnet

Finally, you will have to update the resource records on your Domain Name System (DNS) server to reflect the IP address changes

Question: 82

You are testing a twisted-pair cable run using a tone generator and locator. When you apply the tone generator to a particular pin at one end of the cable, you detect a tone on two pins at the other end. Which of the following faults have you discovered?

A. Split pair
B. Open
C. Short
D. Crosstalk

Answer: C

A short is when a wire is connected to two or more pins at one end of the cable or when the conductors of two or more wires are touching inside the cable

This would cause a tone applied to a single pin at one end to be heard on multiple pins at the other end

The other three options would not cause this to occur

An open circuit would manifest as a failure to detect a tone on a wire, indicating that there is either a break in the wire somewhere inside the cable or a bad connection with the pin in one or both connectors

A split pair is a connection in which two wires are incorrectly mapped in exactly the same way on both ends of the cable

Crosstalk is a type of interference caused by signals on one wire bleeding over to other wires

Question: 83

Your network has been experiencing intermittent service slowdowns and outages ever since the company moved into their new building. You have tried every troubleshooting modality you can think of, but you have not been able to determine the cause. One particular user, perhaps hoping to be the squeaky wheel that gets the grease, has taken to calling you every time he experiences a problem. One day, as you are working in the datacenter, you notice that the user calls every time you hear an additional humming noise. After examining the doors in the hallway, you realize that the racks containing the network switches are located right next to the elevator machinery room. Which of the following conditions is probably causing this intermittent network communication problem?

A. Bottleneck
B. EMI
C. Latency
D. Crosstalk

Answer: B

Elevator machinery, fluorescent light fixtures, and other electrical devices in an office environment can generate magnetic fields, resulting in electromagnetic interference (EMI)

When copper-based cables are located too near to such a device, the magnetic fields can generate an electric current on the cable that interferes with the signals exchanged by network devices

If the network users experience a problem every time the elevator machinery switches on, EMI is a likely cause of the problem

Crosstalk and attenuation can both cause intermittent network communication problems, but they cannot be caused by elevator machinery

Latency describes a generalized delay in network transmissions, not intermittent packet delays

Question: 84

Ralph is installing a pair of redundant servers and must choose whether to run them in an active-active or active-passive configuration. Running the servers in an active-active configuration provides which of the following advantages that the same servers in an active-passive configuration do not? (Choose all that apply.)

A. Fault tolerance
B. Load balancing
C. Data encapsulation
D. Increased performance

Answer: B, D
In an active-active configuration, servers can balance the incoming client load between them
Because the active servers are all servicing clients, the overall performance of the cluster is increased
Both active-active and active-passive configurations provide fault tolerance
Data encapsulation is not a factor in either configuration

Question: 85

You are starting work at a new company, and on your first day, you ask about wireless access for your laptop. You are given a Service Set Identifier (SSID) and a WiFi Protected Access II (WPA2) passphrase. Later, in the lunchroom, when you try to connect your laptop to the network, you cannot see the SSID you were given in the list of available networks, although you can see other networks. What should you do next to try to resolve the problem?
A. Move closer to the Wireless Access Point (WAP).
B. Move away from the microwave in the lunchroom.
C. Type in the WPA2 passphrase.
D. Type the SSID in manually.

Answer: D
It is possible that the WAP has been configured to not broadcast the network’s SSID as a security measure, so you should first attempt to access it by typing the SSID in manually
You cannot type in the WPA2 passphrase until you are in the process of connecting to the SSID
Moving the laptop closer to the access point or away from possible sources of electromagnetic interference might be solutions to the problem, but they should not be the first thing you try in this case

Question: 86

You are responsible for a Wireless Local Area Network (WLAN) that consists of an 802.11n 2x2 access point and laptop computers with a variety of network adapters. Some of the laptops support 802.11n, most support 802.11g, and a few older models have 802.11b adapters. The WLAN is located in a large office building with many other wireless networks, and you are having trouble finding a channel on the 2.4 GHz band that is not congested with traffic. Scanning the 5 GHz band, you find relatively little traffic, so you reconfigure the access point to use a 5 GHz channel. The result is that some of the laptops are able to connect to the network, whereas others are not. What is the most likely reason for the connection failures, and what must you do to enable all the laptops to connect to the wireless network?

A. The 802.11b standard does not support communication using the 5 GHz band. You must replace the network adapters in those laptops with newer models for them to connect successfully.

B. The 5 GHz band does not support automatic channel selection. You must configure each laptop to use the same channel as the access point for all the laptops to connect successfully.

C. The 5 GHz band does not support Multiple Input, Multiple Output (MIMO) communications, so the 802.11n laptops are unable to connect to the network. You must replace the access point with an 802.11g unit for all the laptops to connect successfully.

D. The 802.11g and 802.11b standards do not support communication using the 5 GHz band. You must configure the access point to support 2.4 GHz for all the laptops to connect successfully.

Answer: D

The 802.11b and 802.11g standards do not support 5 GHz communications

Configuring the access point to support 2.4 GHz is the only way for the 802.11b and 802.11g computers to connect to the network

The 5 GHz band does support automatic channel selection, so there is no need to configure the channel on each laptop manually

The 5 GHz band does support MIMO, and the 802.11n laptops should be able to connect

The 802.11b standard does support the 2.4 GHz band

Question: 87

In the Domain Name System (DNS), a zone is a contiguous area of the DNS namespace for which authority is delegated to one or more DNS servers. Which of the following DNS resource record types specifies the IP addresses of the authoritative DNS servers for a particular zone?

A. PTR

B. SRV

C. MX

D. NS

Answer: D
The Name Server (NS) resource record identifies the authoritative servers for a particular DNS zone
Pointer Records (PTRs) are used to resolve IP addresses into hostnames
Mail Exchange (MX) records identify the mail servers for a particular domain
Service Records (SRVs) identify the designated servers for a particular application
None of these other options identify the authoritative servers for a zone

Question: 88

You are experiencing poor performance on your home 802.11n wireless network. You live in a large apartment complex, and when you run a WiFi analyzer, you see many other nearby networks using the often-recommended channels 1, 6, and 11 on the 2.4 GHz frequency. Using the 5 GHz frequency is not an option for your equipment. What should you do to improve the network's performance?

A. Configure your equipment to use channel 10.
B. Configure your equipment to use channel 9.
C. Configure your equipment to use channel 5.
D. Configure your equipment to use channel 2.

Answer: B
The 2.4 GHz band used by Wireless Local Area Networks (WLANs) consists of channels that are 20 (or 22) MHz wide
However, the channels are only 5 MHz apart, so there is channel overlap that can result in interference
Channels 1, 6, and 11 are the only channels that are far enough apart from each other to avoid any overlap with the adjacent channels
This is why they are often recommended
However, in this scenario, these channels are too crowded with other networks
You should therefore use a channel that is as far as possible from the crowded ones
Channels 2, 5, and 10 are all immediately adjacent to a crowded channel, but channel 9 is at least two channels away from the nearest crowded channel
Therefore, you should configure your equipment to use channel 9

Question: 89

Your company’s office building is having a fire inspection, and you are the only person on duty in the datacenter. The inspector from the fire department asks you where they can find documentation about all chemicals and equipment used in the company’s datacenter. You lead the inspector to the director’s office, but you are not sure what the documents he needs are called. Which of the following document types contains this information?

A. MSDS
B. NDA
C. BYOD
D. ESD

Answer: A

Material Safety Data Sheets (MSDSs) are documents created by manufacturers of chemical, electrical, and mechanical products that specify the potential risks and dangers associated with them, particularly in regard to flammability and the possibility of toxic out-gassing

A properly documented network should have MSDS documents on file for all of the chemical and hardware products used to build and maintain it

MSDSs can be obtained from manufacturers or the Environmental Protection Agency (EPA)

Electrostatic discharges (ESDs), Nondisclosure Agreements (NDAs), and Bring Your Own Device (BYOD) policies are not concerned with the dangers inherent in building contents

Question: 90

Which of the following Power over Ethernet (PoE) specifications supplies power to devices using the spare wire pair on a 10Base-T or 100Base-TX twisted-pair network?

A. 4PPoE
B. Alternative A
C. Alternative B
D. All of the above

Answer: C

The Alternative B PoE variant can use the spare wire pair in a CAT 5 or better 10Base-T or 100Base-TX cable to supply power to connected devices
The Alternative A and 4PPoE variants cannot use the spare wire pair in this manner; they supply power using the wire pairs that carry data at the same time
For Gigabit Ethernet or faster installations, Alternative B is also capable of using the data wire pairs

Question: 91

The iSCSI storage area networking protocol uses clients called initiators and servers called targets. However, on many Storage Area Networks (SANs), there needs to be a way for the initiators to locate the targets. Which of the following technologies do iSCSI initiators use to locate iSCSI targets on the network?

A. ICMP
B. DNS
C. iDNS
D. iSNS

Answer: D
The Internet Storage Name Service (iSNS) is an application that provides iSCSI initiators with automated discovery of targets located on the network
iSNS can also function as a discovery service for Fibre Channel devices
Internet Control Message Protocol (ICMP) and Domain Name System (DNS) are not capable of registering iSCSI targets
iDNS does not exist

Question: 92

You are deploying an 802.11n wireless network for a client that is asking for the best possible security you can provide without deploying additional servers. When setting up the Wireless Access Point (WAP), you disable Service Set Identifier (SSID) broadcasts, select WiFi Protected Access with Pre-Shared Keys (WPA-PSKs), and configure Media Access Control (MAC) address filtering. Which of the following statements about the security of this arrangement is true?

A. You should not disable SSID broadcasts since this prevents users from connecting to the network.

B. The configuration is as secure as you can make it with the specified equipment.
C. You should use WiFi Protected Access II (WPA2) instead of WPA, since it is more resistant to certain types of attacks.
D. You should not use MAC address filtering since it exposes MAC addresses to possible attacks.

Answer: C
WPA has been found to be vulnerable, and WPA2 was designed to address those vulnerabilities, so you should use WPA2 instead of WPA
Suppressing SSID broadcasts does not prevent users from connecting to the network, and MAC filtering strengthens security without exposing MAC addresses to undue risk

Question: 93

Which of the following connector types are used with fiber-optic cables? (Choose all that apply.)
A. DB-9
B. SC
C. BNC

D. ST
E. MTRJ
F. RJ11

Answer: B, D, E
Subscriber Connector (SC), Mechanical Transfer - Registered Jack (MT-RJ), and Straight Tip (ST) are all types of fiber-optic connectors
DB-9 is a D-shell connector used for serial ports
Bayonet-Neill-Concelman (BNC) is a type of connector used with coaxial cable
RJ11 is used with twisted-pair cable for telephone connections

Question: 94

Which of the following are available as Internet of Things (IoT) devices?
A. Refrigerators
B. Doorbells

C. Thermostats
D. Speakers
E. All of the above

Answer: E
The IoT consists of devices that are ordinarily passive, but which have been made intelligent by installing a network client configuring them to participate on an IP network
All of the devices listed are available as “smart” devices that enable remote users to interact with them over the Internet

Question: 95

You are designing an Ethernet network for your company’s newest branch office. Your current task is to decide which Ethernet specification to use for the network, a decision that you know will determine what type of cabling you need to purchase and the topology with which the cable will be installed. Which layers of the Open Systems Interconnection (OSI) reference model apply to the cabling and topology elements of a network?
A. The application and transport layers
B. The transport and network layers
C. The network and data link layers
D. The data link and physical layers

Answer: D
The physical layer defines the mechanical and electrical characteristics of the cables used to build a network
The data link layer defines specific network (LAN or WAN) topologies and their characteristics
The physical layer specification you will implement is dependent on the data link layer protocol you select
The network, transport, and application layers are not concerned with cables and topologies

Question: 96

You are troubleshooting a workstation that cannot access the network. The workstation is plugged into a wall plate that should provide it with access to a

DHCP-equipped network using the 192.168.4.0/24 network address. No one else on that network is reporting a problem. You check that the patch cable is properly plugged into the workstation and the wall plate, which they are, and then run ipconfig /all on the workstation and examine the output. Which of the statements could be the explanation for the workstation's problem, based on the following ipconfig results?

```
Windows IP Configuration
 Host Name . . . . . . . . . . . . : Client12
 Primary Dns Suffix . . . . . . . :
 Node Type . . . . . . . . . . . . : Hybrid
 IP Routing Enabled. . . . . . . . : No
 WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
 Description . . . . . . . . . . . : PCIe Family Controller
   Physical Address. . . . . . . . . : 60-EB-69-93-5E-E5
 DHCP Enabled. . . . . . . . . . . : Yes
 Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c955:c944:acdd:3fcb%2
 IPv4 Address. . . . . . . . . . . : 169.254.203.42
 Subnet Mask . . . . . . . . . . . : 255.255.0.0
 Lease Obtained. . . . . . . . . . : Monday, October 23, 2017 6:23:47 PM
 Lease Expires . . . . . . . . . . : Saturday, November 18, 2017 9:49:24 PM
 Default Gateway . . . . . . . . . :
 DHCPv6 IAID . . . . . . . . . . . : 241232745
 DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-18-10-22-0D-60-EB-69-93-5E-E5
 DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
 fec0:0:0:ffff::2%1
 fec0:0:0:ffff::3%1
 NetBIOS over Tcpip. . . . . . . . : Enabled
```

A. The DNS server addresses are incorrect.
B. The Default Gateway address is missing.
C. The Subnet Mask value is incorrect.
D. The DHCP scope is exhausted.

Answer: D

The 169.254.203.42 address assigned to the workstation is from the 169.254.0.0/16 network address assigned to Automatic Private IP Addressing (APIPA), a standard for the assignment of IP addresses to Dynamic Host

Configuration Protocol (DHCP) clients when they cannot obtain an address from a DHCP server
The workstation’s DHCP client is activated, and since no one else is experiencing a problem, you can assume that the DHCP server is functioning
The Subnet Mask value is correct for an APIPA address, and APIPA does not provide Default Gateway or Domain Name System (DNS) server addresses
Therefore, an exhausted DHCP scope is the only one of the explanations provided that could be the cause of the problem

Question: 97

A user calls you at the IT help desk and reports that she is having intermittent problems accessing both local servers and internet websites. Which of the following potential problems can you rule out immediately?

A. Malfunctioning Domain Name System (DNS) server
B. Duplicate Media Access Control (MAC) addresses
C. Duplicate IP addresses
D. Malfunctioning router

Answer: C
Operating systems detect duplicate IP addresses immediately and display error messages or notifications on the computers involved
Therefore, the user with the problem would have been informed immediately if another system was using her IP address
All of the other options are possible causes of the problem that are more difficult to troubleshoot

Question: 98

You have recently discovered a rogue Dynamic Host Configuration Protocol (DHCP) server on your network. After disabling the rogue server, you now need to terminate all of the rogue IP address leases currently held by DHCP clients on the network and then have them request new leases from the authorized DHCP server. Which of the following commands must you run on each client to do this? (Choose all that apply.)

A. ipconfig /dump
B. ipconfig /lease
C. ipconfig /release

D. ipconfig /renew
E. ipconfig /discard

Answer: C, D
The ipconfig /release command terminates the current DHCP address lease
Then, the ipconfig /renew command causes the client to begin the process of negotiating a new lease, this time with the authorized DHCP server
dump, lease, and discard are not valid ipconfigparameters

Question: 99

Ralph is reading an article about datacenter design, and he is puzzled by references to east-west and north-south traffic. Which of the following statements best describes the difference between east-west and north-south traffic in a datacenter?
A. East-west is switch-to-switch traffic, while north-south is switch-to-router traffic.
B. East-west describes traffic between devices at the same layer of the Open Systems Interconnection (OSI) reference model, while north-south describes traffic between OSI model layers.
C. East-west traffic stays within the datacenter, while north-south traffic does not.
D. East-west is backbone traffic among switches and routers, while north-south is traffic to end systems, such as servers.

Answer: C
East-west traffic describes traffic flow within the datacenter, while north-south is traffic between devices inside the datacenter and outside devices
The terms east-west and north-south do not pertain to the OSI model layers or to the specific devices used

Question: 100

Which of the following attack types involves the modification of a legitimate software product?
A. War driving
B. Logic bomb
C. Evil twin

D. Social engineering

Answer: B

A logic bomb is a code insert placed into a legitimate software product that triggers a malicious event when certain conditions are met, such as when a specific time or date arrives. All of the other options do not involve software products. Social engineering is the practice of obtaining sensitive data by contacting users and pretending to be someone with a legitimate need for that data. War driving is an attack method that consists of driving around a neighborhood with a computer, scanning for unprotected wireless networks. An evil twin is a fraudulent access point on a wireless network that mimics the Service Set Identifier (SSID) of a legitimate access point, in the hope of luring in users.

KILL EXAMS
Questions & Answ
Killexams Inc
Test Engine V.5.3
Killexams Inc