Exam Report: B.4 Network+ Certification Practice Exam

Date: 12/4/2019 6:38:11 pm
Time Spent: 01:07:43 of 01:30:00

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 53%

Passing Score: 95%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following is a policy that defines appropriate and inappropriate activities and usage for company resources, assets, and communications?

- Disaster recovery plan (DRP)
- Business impact analysis (BIA)
- Acceptable use policy (AUP)
- Business continuity plan (BCP)

Explanation

An acceptable use policy defines appropriate and inappropriate activities and usage for company resources, assets, and communications.

The business impact analysis (BIA) identifies critical processes/assets and the effect of their loss on the company. The disaster recovery plan (DRP) addresses how the corporation will respond to a disaster. The business continuity plan (BCP) addresses how the corporation will respond to the disruption of critical systems.
[netpro18v5_all_questions_en.exm SSCP-7 NEW [7]]

Question 2: Correct

How can an organization help prevent social engineering attacks? (Select two.)

- [x] Publish and enforce clearly written security policies
- [ ] Implement IPsec on all critical systems
- [ ] Utilize 3DES encryption for all user sessions
- [x] Educate employees on the risks and countermeasures

Explanation

User training and policy enforcement are the keys to preventing social engineering attacks. Many users are not aware of social engineering risks. Training raises awareness, provides clear instructions for dealing with and reporting suspicious activity, and directly supports all published security policies.

Technical countermeasures protect against automated attacks. Social engineering seeks to gain access by exploiting human nature.
[netpro18v5_all_questions_en.exm SSCP-4 SP [352]]

Question 3: Incorrect

You were recently hired by a small start-up company. The company is in a small office and has several remote employees.

You have been asked to find a business service that would accommodate the current size of the company, but would also be able to scale as the company grows. The service needs to provide adequate storage, as well as additional computing power.

Which cloud service model should you use?

IaaS

~~PaaS~~

DaaS

SaaS

Explanation

Infrastructure as a service (IaaS) delivers infrastructure to the client, such as processing, storage, networks, and virtualized environments. The client deploys and runs software without purchasing servers, data center space, or network equipment.

Software as a service (SaaS) delivers software applications to the client either over the internet or on a local area network. Platform as a service (PaaS) delivers everything a developer needs to build an application onto the cloud infrastructure. The deployment comes without the cost and complexity of buying and managing the underlying hardware and software layers. Data as a service (DaaS) stores and provides data from a centralized location without requiring local collection and storage.
[netpro18v5_all_questions_en.exm NP15_CLOUD_COMPUTING_05]

Question 4: Correct

Why should you store backup media off site?

To make the restoration process more efficient.

To reduce the possibility of theft.

To comply with government regulations.

To prevent the same disaster from affecting both the network and the backup media.

Explanation

Backup media should be stored off site to prevent the same disaster from affecting the network and the backup media. If your primary facility is destroyed by fire, your only hope of recovery is off site data storage.

Off site storage does not significantly reduce the possibility of media theft because it can be stolen while in transit or at your storage location. Off site storage is not a government regulation. Off site storage does not make the restoration process more efficient because additional time is spent retrieving backup media from its off site storage location.
[netpro18v5_all_questions_en.exm CISSP-1016 SP [15]]

Question 5: Correct

You have just downloaded a file. You create a hash of the file and compare it to the hash posted on the website. The two hashes match. What do you know about the file?

You will be the only one able to open the downloaded file.

No one has read the file contents as it was downloaded.

Your copy is the same as the copy posted on the website.

You can prove the source of the file.

Explanation

A hash is a function that takes a variable-length string (message) and compresses and transforms it into a fixed-length value. Hashes ensure the data integrity of files and messages in transit. The sender and the receiver use the same hashing algorithm on the original data. If the hashes match, then the data can be assumed to be unmodified.

Hashes do not ensure confidentiality (in other words, hashes are not used to encrypt data). Non-repudiation proves the source of a file and is accomplished using digital signatures.
[netpro18v5_all_questions_en.exm SP08_5-2 2]

Question 6: Incorrect

What is another name for a logic bomb?

Pseudo flaw

Asynchronous attack

DNS poisoning

~~Trojan horse~~

Explanation

A logic bomb is a specific example of an asynchronous attack. An asynchronous attack is a form of malicious attack where actions taken at one time do not cause their intended, albeit negative, action until a later time.

A pseudo flaw is a form of IDS to detect when an intruder attempts to perform a common but potentially dangerous administrative task. DNS poisoning is the act of inserting incorrect domain name or IP address mapping information into a DNS server or a client's cache. A Trojan horse is any malicious code embedded inside of a seemingly benign carrier. None of these issues is a synonym for a logic bomb.
[netpro18v5_all_questions_en.exm SSCP-4 CP [278]]

Question 7: Correct

You want to reduce collisions by creating separate collision domains and virtual LANs. Which of the following devices should you choose?

Router

Switch

Bridge

Active hub

Explanation

Use a switch to create additional collision domains on a LAN. A switch filters an entire network and creates virtual LANs inside it rather than dividing it into separate internetworks as a router does.
[netpro18v5_all_questions_en.exm NP05_1-6 #36]

Question 8: Correct

Which of the following enterprise wireless deployment models uses access points with enough intelligence to allow the creation of guest WLANs for keeping public wireless traffic separate from private traffic?

Hub-and-spoke infrastructure

Distributed wireless mesh infrastructure

Independent access points

Lightweight access point (LWAP) with wireless controller infrastructure

Explanation

A distributed wireless mesh architecture moves some of the network intelligence from the controller out to the individual access points. In this configuration, the controller is no longer a bottleneck. The APs are smart enough to communicate directly with each other to create more efficient data paths for network traffic.

With the hub-and-spoke infrastructure, the individual access points contain very little embedded intelligence and are sometimes referred to as lightweight access points (LWAPs). Independent access points offer limited mobility and require the individual configuration of each AP.
[netpro18v5_all_questions_en.exm *NP15_WIRELESS_NETWORK_IMPLEMENTATION_01]

Question 9: Correct

Your company is a small start-up that has leased office space in a building shared by other businesses. All businesses share a common network infrastructure. A single switch connects all devices in the building to the router that provides internet access.

You would like to make sure that your computers are isolated from computers used by other companies. Which feature should you request to have implemented?

VPN

Spanning tree

Port security

VLAN

Explanation

Define virtual LANs (VLANs) on the switch. A port on the switch is associated with a VLAN. Only devices connected to ports that are members of the same VLAN can communicate with each other. Routers are used to allow communication between VLANs if necessary.

Use virtual private network (VPN) to securely connect two hosts through an unsecured network (such as the internet). VPN tunneling protocols protect data as it travels through the unsecured network. Spanning tree is a switch feature that allows redundant paths between switches. Port security is a method of requiring authentication before a network connection is allowed.
[netpro18v5_all_questions_en.exm NP09 2-7 2]

Question 10: Correct

Which technologies are used by the 802.11ac standard to increase network bandwidth? (Select two.)

- [ ] Data compression
- [ ] Four MIMO radio streams
- [x] Eight MIMO radio streams
- [ ] 40 MHz bonded channels
- [x] 160 MHz bonded channels

Explanation

To increase network bandwidth, the 802.11ac standard uses:

- Eight MIMO radio streams
- 160 MHz wide bonded channels

[netpro18v5_all_questions_en.exm RT NP15_5.3-4]

Question 11: Correct

You are the administrator of your company's network. You want to prevent unauthorized access to your intranet from the internet. Which of the following should you implement?

- Proxy server
- Firewall
- ICS
- Packet Internet Groper

Explanation

A firewall allows you to filter unwanted traffic from the internet to your network. Packet internet groper is better known by its acronym, PING, a TCP/IP command. A proxy server caches web pages. ICS allows you to connect a small network to the internet through a single connection.
[netpro18v5_all_questions_en.exm NP05_3-5 #32]

Question 12: Incorrect

What is the main difference between vulnerability scanning and penetration testing?

- ~~The goal of vulnerability scanning is to identify potential weaknesses; the goal of penetration testing is to attack a system.~~
- Vulnerability scanning is performed with a detailed knowledge of the system; penetration testing starts with no knowledge of the system.
- Vulnerability scanning is performed within the security perimeter; penetration testing is performed outside of the security perimeter.
- Vulnerability scanning uses approved methods and tools; penetration testing uses hacking tools.

Explanation

Penetration testing simulates an actual attack on the network and is conducted from outside the organization's security perimeter. Vulnerability scanning is typically performed internally by users with administrative access to the system.
The goal of both vulnerability scanning and penetration testing is to identify the effectiveness of security measures and identify weaknesses that can be fixed. While some penetration testing is performed with no knowledge of the network, penetration testing could be performed by testers with detailed information about the systems. Both vulnerability scanning and penetration testing can use similar tools, although illegal tools should be avoided in both activities.
[netpro18v5_all_questions_en.exm SP08_4-3 3]

Question 13: Correct

Which of the following functions can a port scanner provide?

- (selected) Determining which ports are open on a network.
- Auditing IPsec encryption algorithm configuration.
- Automatically close open ports on the network.
- Testing virus definition design for false positives.

Explanation

Port scanners can determine which TCP/UDP ports are open on a network . Many port scanners provide additional information, including the host operating system and version of any detected servers. Hackers use port scanners to gather valuable information about a target. System administrators should use the same tools for proactive penetration testing and to ensure compliance with all corporate security policies.
[netpro18v5_all_questions_en.exm SP02_1-7 84]

Question 14: Incorrect

A user reports that she can't connect to the Internet. After some investigation, you find that the wireless router has been misconfigured. You are responsible for managing and maintaining the wireless access point.

What should you do next?

- ~~Document the problem.~~
- (selected) Create an action plan.
- Determine if escalation is needed.
- Fix the problem.

Explanation

At this point, you should create an action plan and account for side effects of the proposed plan. Identifying the affects ahead of time helps you put measures into place to eliminate or reduce any potential negative consequences.

Escalation is not necessary because you are already in charge of managing the wireless access point, and the problem is isolated to that device. Fix the problem only after creating the action plan and identifying possible effects. Document the problem and the solution after the problem has been fixed and the solution has been verified.
[netpro18v5_all_questions_en.exm NP09_4-6 #MCS3]

Question 15: Correct

You have a web server that will be used for secure transactions for customers who access the website over the internet. The web server requires a certificate to support SSL.

Which method would you use to get a certificate for the server?

- Create your own internal PKI to issue certificates.
- (selected) Obtain a certificate from a public PKI.
- Run a third-party tool to generate the certificate.
- Have the server generate its own certificate.

Explanation

Computers must trust the CA that issues a certificate. For computers that are used on the internet and accessible to public users, obtain a certificate from a public CA such as VeriSign. By default, most computers trust well-known public CAs.

Use a private PKI to issue certificates to computers and users within your own organization. You configure computers to trust your own PKI, so certificates issued by your internal CAs are automatically trusted. A certificate generated by a server is called a self-signed certificate. A self-signed certificate provides no proof of identity because any other server can claim to be that server just by issuing itself a certificate.

[netpro18v5_all_questions_en.exm NP09_6-4 #MCS3]

Question 16: Correct

You are building a new network for a small startup financial services company. Security is paramount, so each organization within the company will have its own network segment separated by a router. However, funds are limited, and you have been asked to keep costs to a minimum.

You have acquired a used fiber optic switch and want to use it to create a fiber optic backbone that interconnects all of the routers. You purchased several used single-mode GBIC modules on eBay that you will install in each router to allow them to connect to the switch.

Both the switch and the GBIC modules use MTRJ connectors. You connect each module to the switch with 1-meter multimode patch cables.

Will this implementation work?

- (●) No. You shouldn't use multi-mode patch cables with single-mode GBIC modules.
- ( ) No. You should not use standard fiber optic switches to create a backbone network for routers.
- ( ) No. You should purchase fiber optic equipment that use FC connectors.
- ( ) Yes,. All of the requirements for implementing a fiber optic network have been met.

Explanation

Some GBIC/SFP modules use multi-mode fiber, while others use single-mode. You must use the correct type of fiber optic cable and connector required by the specific adapter. You cannot mix and match different types of cable. In this scenario, connecting a single-mode GBIC to multi-mode fiber will introduce a catastrophic signal loss of up to 99%.

[netpro18v5_all_questions_en.exm RT NP15_4.5-2]

Question 17: Incorrect

Drag the broadcast domain property on the left to the appropriate network device(s) on the right. Each property can be used more than once.

Single broadcast domain	Hub
~~Multiple broadcast domains~~	Unmanaged switch
Single broadcast domain	
~~Multiple broadcast domains~~	802.11n wireless access point
Single broadcast domain	
Multiple broadcast domains	Router
Single broadcast domain	Bridge
Single broadcast domain	Repeater
Multiple broadcast domains	Layer 3 switch

Explanation

A broadcast domain is a logical division of a network. All network hosts within the same broadcast domain can reach each other using broadcasts at the Data Link layer. All network hosts connected to the following Layer 2 network devices are members of the same broadcast domain:

- Hubs
- Unmanaged switches (because they do not support VLANs)
- 802.11 wireless access points
- Bridges
- Repeaters

Layer 3 devices are used to define boundaries between broadcast domains, such as a router or a layer 3 switch. A managed switch with VLANs implemented also creates separate broadcast domain for each VLAN.
[netpro18v5_all_questions_en.exm D&D1]

Question 18: Incorrect

Which of the following is a feature of MS-CHAP v2 that is not included in CHAP?

- Certificate-based authentication
- Hashed shared secret
- ~~Three-way handshake~~
- Mutual authentication

Explanation

MS-CHAP v2 allows for mutual authentication, where the server authenticates to the client.

Both CHAP and MS-CHAP use a three-way handshake process for authenticating users with usernames and passwords. The password (or shared secret) value is hashed, and the hash, not the shared secret, is sent for authentication.
[netpro18v5_all_questions_en.exm NP09_6-4 #MCS9]

Question 19: Incorrect

To answer this question, complete the lab using information below.
You have completed this lab and may go on to the next question.

Launch Lab

You did not complete the lab correctly.

Close Lab Report

Performance

Your Score: 0 of 2 (0%)
Elapsed Time: 3 minutes 3 seconds

Task Summary

Actions you were required to perform:

- ✗ Enable all of the ports to other devices Show Details
- ✗ Enable the link between two of the three switches to prevent a switching loop

[np18v5_typnet.exm NETWORKPERFQ]

Question 20: Incorrect

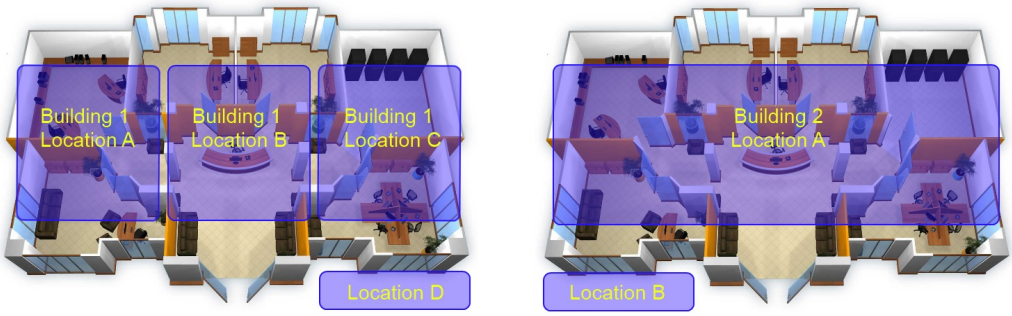
You are building a wireless network within and between two buildings. The buildings are separated by more than 3000 feet. The wireless network should meet the following requirements:

- Wireless data within Building 1 should be protected with the highest degree of security.
- Wireless data within Building 2 should be accessible and permitted by any wireless client.
- Wireless signals between Buildings 1 and 2 should be protected with the highest degree of security.
- Wireless signals within Buildings 1 and 2 should cover the whole structure, but not extend to the outside.

For each location on the image below, you need to select the following:

- Antenna option
- Security option

Drag the items from the list on the left to the location identifier on the right. Items may be used more than once. Not all items will be used.



Building 1 - Location A

Right-facing directional antenna	~~WPA2 with TKIP~~
	WPA2 with CCMP

Building 1 - Location B

Omni-directional antenna	~~WPA2 with TKIP~~
	WPA2 with CCMP

Building 1 - Location C

Left-facing directional antenna	~~WPA2 with TKIP~~
	WPA2 with CCMP

Building 1 - Location D

Right-facing high-gain directional antenna	WPA2 with CCMP

Building 2 - Location A

Omni-directional antenna	WEP with open authentication

Building 2 - Location B

Left-facing high-gain directional antenna	WPA2 with CCMP

Explanation

To answer this question correctly, you should choose the following:

Building 1 - Location A = Right-facing directional antenna, WPA2- CCMP
Building 1 - Location B = Omni-directional antenna, WPA2- CCMP
Building 1 - Location C = Left-facing directional antenna, WPA2- CCMP
Building 1 - Location D = Right-facing parabolic antenna, WPA2- CCMP
Building 2 - Location A = Omni-directional antenna, WEP with open authentication
Building 2 - Location B = Left-facing parabolic antenna, WPA2- CCMP

Be aware of the following types of antennas:

- Directional antenna:
  - Creates a narrow, focused signal in a particular direction.
  - Focuses the signal to provide greater signal strength, thus increasing the transmission distance.
  - Provides a stronger point-to-point connection, better equipping them to handle obstacles. A *parabolic* directional antenna is highly focused, sending and receiving signals in far greater distances than achieved with a typical directional antenna.
- Omni-directional antenna:
  - Disperses the RF wave in an equal 360-degree pattern.
  - Provides access to many clients in a radius.

Be aware of the following types of security:

- Wired Equivalent Privacy (WEP) is an optional component of the 802.11 specifications, but is easily broken. When using WEP, use open authentication.
- Wi-Fi Protected Access 2 (WPA2) resolves the weaknesses inherent in WEP. WPA2 uses counter mode with the CBC-MAC protocol (CCMP), also known as AES-CCMP. Note that WPA2 does not use TKIP.

[netpro18v5_all_questions_en.exm PERF-BASED#2]

Question 21: Correct

Which network component connects a device to transmission media and allows the device to send and receive messages?

- Client
- Network interface card
- Peripheral
- Protocol
- Server

Explanation

The network interface card (NIC) allows a device to send and receive messages over the transmission media.

[netpro18v5_all_questions_en.exm NP05_1-6 #67]

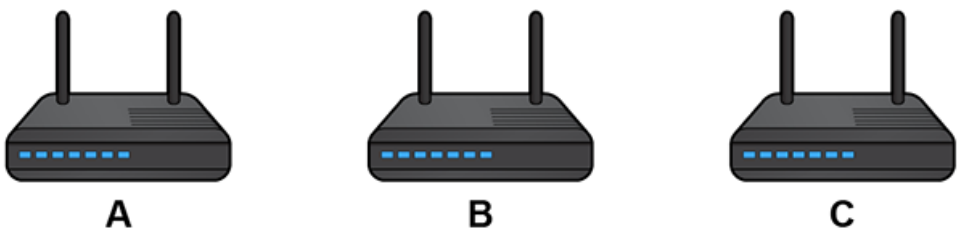
Question 22: Correct

Mobile devices in your organization use the access points shown in the figure below to connect to your wireless network.

Recently, a catastrophic early morning power surge occurred. It was followed by an outage that lasted longer than your backup equipment could supply temporary power.

After you powered the equipment back on, everything initially appeared to work correctly. However, ever since this event, some mobile users report that wireless network connections sometimes get dropped or perform very poorly.

What should you do? (Select two.)



• SSID: WestSimWireless • Mode: 802.11n • Security: WPA2-PSK • Channel: 1 • Frequency: 2.4 GHz • Admin username: @dM1n • Admin password: p@$$w0rd • IP address: 192.168.0.1	• SSID: WestSimWireless • Mode: 802.11b • Security: WPA2-PSK • Channel: 4 • Frequency: 2.4 GHz • Admin username: @dM1n • Admin password: p@$$w0rd • IP address: 192.168.0.2	• SSID: WestSimWireless • Mode: 802.11n • Security: WPA2-PSK • Channel: 6 • Frequency: 2.4 GHz • Admin username: @dM1n • Admin password: p@$$w0rd • IP address: 192.168.0.3

- [x] Set the channel used by access point B to 11.
- [ ] Set the channel used by access point B to 8.
- [ ] Configure each access point to use a different SSID.
- [ ] Set access points A and C to use 802.11b wireless networking.
- [ ] Set the channel used by access point A to 5.
- [ ] Set the channel used by access point C to 7.
- [ ] Configure each access point to use 802.1x authentication.
- [x] Set access point B to use 802.11n wireless networking.

Explanation

During the power surge and/or power outage, some of the configuration settings on access point B were lost or reset to default values. To fix the issues users are experiencing, you need to:

- Set access point B to use 802.11n wireless networking. This will rectify the poor performance users are experiencing while accessing the wireless network through access point B.
- Set the channel used by access point B to 11. 2.4 GHz channels overlap. In this scenario, the channel used by access point B (4) overlaps with the channels used by access points A (1) and C (6). This will rectify the dropped connections users are experiencing.

Channels 5, 7, and 8 overlap with channel 6, so setting any access point to these channels will cause a conflict with access point C. Using the same SSID on all access points allows users to roam about the facility and stay connected to the same wireless network. While using 802.1x authentication would make the wireless network more secure, it will not address the issues users are experiencing. Configuring access points A and C to use 802.11b will cause all users to experience poor network performance.
[netpro18v5_all_questions_en.exm MCS9]

Question 23: Correct

Your manager has asked you to implement a network infrastructure that will accommodate failed connections.

Which of the following network topologies provides redundancy for a failed link?

- (•) Mesh
- ( ) Bus
- ( ) Star
- ( ) Ring

Explanation

In a mesh topology, each network device is interconnected to all other network nodes. This creates multiple data paths. If a link fails, the data has an alternate route to its destination.

The star topology connects network devices to the network with a single patch cable. A patch cable failure makes the connected device unavailable. The bus topology has a single point of failure. If there is a break in the network media, the network becomes unavailable. A single break in a physical ring topology disables the network.
[netpro18v5_all_questions_en.exm NP05_4-7 #43]

Question 24: Incorrect

You have a network that occupies all three floors of a building. The WAN service provider has installed the

line for the WAN service into the building in a wiring closet on the main floor. You have a wiring closet on the two remaining floors directly above the wiring closet on the main floor.

What would you use to connect the wiring closets together?

- Demarc extension
- Smart jack
- ~~Horizontal cross connect~~
- Vertical cross connect

Explanation

A vertical cross connect joins the main distribution frame (MDF) on the main floor to intermediate distribution frames (IDFs) on upper floors. Cabling runs vertically (up and down) between the MDF and the IDFs.

A horizontal cross connect joins IDFs on the same floor. Cabling runs horizontally (sideways) between the IDFs. A smart jack is a special loopback plug installed at the demarcation point for a WAN service. Technicians at the central office can send diagnostic commands to the smart plug to test connectivity between the central office and the demarc.

A demarc extension extends the demarcation point from its original location to another location within the building. The demarc extension typically consists of a single wire bundle that attaches to the existing demarc and supplies a termination point to a different location. You might need a demarc extension if your network occupies an upper floor of a building. The LEC will typically install the demarc into the MDF on the bottom floor, and you will need to install an extension to place the demarc into the IDF on your floor.

[netpro18v5_all_questions_en.exm NP09_2-8 #MCS4]

Question 25: Incorrect

Match the wireless signaling method on the left with its definition on the right. (Not all of the signaling methods match a definition.)

Uses a narrow frequency band and hops data signals in a predictable sequence

~~CDMA~~ FHSS

Breaks data into pieces and sends the pieces across multiple frequencies in a defined range.

✓ DSSS

Breaks data into very small data streams in order to send the information across long distances.

~~FHSS~~ OFDM

Explanation

The following table describes the most common signaling methods used by wireless networks.

Method	Description
Frequency Hopping Spread Spectrum (FHSS)	FHSS uses a narrow frequency band and hops data signals in a predictable sequence from frequency to frequency over a wide band of frequencies.
Direct-Sequence Spread Spectrum (DSSS)	DSSS uses a transmitter that breaks data into pieces and sends the pieces across multiple frequencies in a defined range. DSSS is more susceptible to interference and less secure then FHSS.
Orthogonal Frequency-Division Multiplexing (OFDM)	OFDM breaks data into very small data streams in order to send the information across long distances where environmental obstacles may be an issue.

[netpro18v5_all_questions_en.exm *NP15_WIRELESS_CONCEPTS_01]

Question 26: Correct


This question includes an image to help you answer the question. Close

```
switch2# show interfaces fa0/1
```

```
FastEthernet0/13 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is c0c1.c09b.acf5 (bia c0c1.c09b.acf5)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     12347 packets input, 853952 bytes, 0 no buffer
     Received 7244 broadcasts (234 multicasts)
     154 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 234 multicast, 0 pause input
     0 input packets with dribble condition detected
     40733 packets output, 3197652 bytes, 0 underruns
     0 output errors, 1015 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 113 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Review the output from the show interfaces fa0/1 command on the switch2 switch in the exhibit.

What is wrong with the fa0/1 interface in this example?

- ◯ The cable connecting the fa0/1 interface with the device on the other end is a straight-through cable, but needs to be crossed-over.
- ➡ ◉ A duplex mismatch exists with the device on the other end of the connection.
- ◯ The line status is administratively down.
- ◯ The protocol status is down.

Explanation

In this example, the following statistics indicate that a duplex mismatch error has occurred:

- Duplexing is set to half.
- There are a significant number of runts.
- There are a significant number of collisions.
- There are a significant number of late collisions.

[netpro18v5_all_questions_en.exm *NP15_WAN_TROUBLESHOOTING_03]

Question 27: Correct

Which of the following protocols includes extensive error checking to ensure that a transmission is sent and received without mistakes?

- ◯ UDP
- ◯ UDB
- ◯ UCP
- ➡ ◉ TCP

Explanation

The TCP protocol includes error checking.
[netpro18v5_all_questions_en.exm NP05_2-10 #113]

Question 28: Incorrect

Match the firewall type on the right with the OSI layer at which it operates.

Each OSI Layer may be used once, more than once, or not at all.

Packet filtering firewall	Circuit-level proxy	Application-level gateway	Routed firewall	Transparent firewall
~~OSI Layer 2~~	~~OSI Layer 1~~	✓ OSI Layer 7	✓ OSI Layer 3	~~OSI Layer 6~~
OSI Layer 3	OSI Layer 5			OSI Layer 2

Explanation

Each firewall type operate at a specific layer of the OSI model.

- Packet filtering firewalls operate at Layer 3.
- Circuit-level proxies operate at Layer 5.
- Application-level gateways operate at Layer 7.
- Routed firewalls operate at Layer 3.
- Transparent firewalls operate at Layer 2.

[netpro18v5_all_questions_en.exm *NP15_FIREWALLS_03]

Question 29: Incorrect

Which of the following locations creates the greatest amount of interference for a wireless access point? (Select two.)

- [x] ~~In the top floor of a two-story building~~
- [ ] Near backup generators
- [ ] Near cordless phones
- [ ] Near DCHP servers

Explanation

Other wireless transmitting devices (such as cordless phones or microwaves) and generators cause interference for wireless access points.

In general, place access points higher up to avoid interference problems caused by going through building foundations. DHCP servers provide IP information for clients and do not cause interference.
[netpro18v5_all_questions_en.exm AP09PA_3-2 #16]

Question 30: Correct

You manage a firewall that connects your private network to the internet. You would like to see a record of every packet that has been rejected by the firewall in the past month.

Which tool should you use?

- ( ) Packet sniffer
- (•) Event log
- ( ) Throughput tester
- ( ) Load tester

Explanation

Use the event logs to see a record of past events. Logging capabilities are built into operating systems, services, and applications. Log entries are generated in response to configuration changes or actions taken by the system. Depending on the device, there might be multiple logs with different names, so the exact log you consult might vary depending on the device.

A packet sniffer is special software that captures (records) frames that are transmitted on the network. A packet sniffer would tell you the frames and packets sent to the device, but would not identify the actions the firewall took in response to those packets.

A load tester simulates a load on a server or service. A throughput tester measures the amount of data that can be transferred through a network or processed by a device (such as the amount of data that can be retrieved from disk in a specific period of time).
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS7]

Question 31: Correct

Examine the following output.

Reply from 64.78.193.84: bytes=32 time=86ms TTL=115
Reply from 64.78.193.84: bytes=32 time=43ms TTL=115

```
Reply from 64.78.193.84: bytes=32 time=44ms TTL=115
Reply from 64.78.193.84: bytes=32 time=47ms TTL=115
Reply from 64.78.193.84: bytes=32 time=44ms TTL=115
Reply from 64.78.193.84: bytes=32 time=44ms TTL=115
Reply from 64.78.193.84: bytes=32 time=73ms TTL=115
Reply from 64.78.193.84: bytes=32 time=46ms TTL=115
```

Which of the following utilities produced this output?

- **ping**
- **ifconfig**
- **tracert**
- **nslookup**

Explanation

The output shown was produced by the **ping** utility. Specifically, the information output was created using the**ping -t** command. The **-t** switch causes packets to be sent to the remote host continuously until stopped manually. **ping** is a useful tool for testing connectivity between devices on a network. Using the **-t** switch with **ping** can be useful in determining whether the network is congested, as such a condition will cause sporadic failures in the **ping** stream.

tracert is similar to **ping** in that it tests connectivity between two hosts on the network. The difference is that **tracert** reports information on all intermediate devices between the host system and the target system. **ping**, on the other hand, does not report information on intermediate devices.

nslookup is a tool provided on Linux, Unix and Windows systems that allows manual name resolution requests to be made to a DNS server. This can be useful when troubleshooting name resolution problems. **ifconfig** is a tool used on Unix, Linux and Macintosh systems to view the configuration of network interfaces, including TCP/IP network settings.
[netpro18v5_all_questions_en.exm NP05_4-2 #86]

Question 32: Correct

Match each troubleshooting command on the left with its function on the right. Each utility may be used once, more than once, or not at all.

Tests connectivity between two network hosts by sending IPv4 ICMP Echo Request packets without modifying the TTL parameter.

- ping

Computes lost/sent packet statistics for each hop in the route between two hosts.

- pathping

Used on Linux systems to identify the route between two IPv6 hosts.

- traceroute6

Used on Windows systems to identify the route between two IPv4 hosts.

- tracert

Tests connectivity between two network hosts by sending IPv6 ICMP Echo Request packets without modifying the TTL parameter.

- ping -6

Explanation

Several commonly used network troubleshooting commands include the following:

- The **pathping** command combines the tracert and ping utilities to identify problems at a router or a network link. Unlike tracert or traceroute, pathping can track lost/sent packet statistics for each hop in the route between two hosts. The pathping command is only available on Windows.
- The **ping** command sends an IPv4 ICMP echo request/reply packet to a remote host. A response from the remote host indicates that both hosts are correctly configured and a connection exists between them. The ping command is available on Windows and Linux.
- The **ping -6** command sends an IPv6 ICMP echo request/reply packet to a remote host. A response from the remote host indicates that both hosts are correctly configured and a connection exists between them. The ping -6 command is only available on Windows. On Linux, you would use **ping6** instead.

- The **tracert** command uses ICMP packets to test the path between two IPv4 networks. Responses from each hop on the route are measured three times to provide an accurate representation of how long the packet takes to reach, and be returned by, the destination device. The tracert command is only available on Windows. On Linux, you would use **traceroute** instead.
- The **traceroute6** command is used on Linux systems to identify the route between two IPv6 hosts.

[netpro18v5_all_questions_en.exm RT NP15_4.2-1]

Question 33: Incorrect

Which of the following devices operate at the Data Link layer of the OSI model? (Select three.)

- [x] Network interface cards (NICs)
- [ ] Routers
- [x] ~~Hubs~~
- [x] ~~Repeaters~~
- [ ] Switches
- [ ] Bridges

Explanation

Network interface cards (NICs), bridges, and switches all operate at the OSI Data Link layer. They use the physical device address (MAC address) to identify packets. Hubs and repeaters operate at the Physical layer--they simply repeat packets without regard to addresses. Routers function at the Network layer--they examine the logical device and network address to perform routing tasks.
[netpro18v5_all_questions_en.exm NP05_2-3 #7]

Question 34: Correct

When recovery is being performed due to a disaster, which services are to be stabilized first?

- ( ) Least business critical
- ( ) Outside communications
- (•) Mission critical
- ( ) Financial support

Explanation

Restore mission critical services first. If mission critical services are not restored within their maximum tolerable downtime, the organization is no longer viable.

Restore the least critical services last. Financial support and outside communications are restored only after all other services with a higher level of criticality have been restored.
[netpro18v5_all_questions_en.exm CISSP-803 NEW [71]]

Question 35: Correct

Your computer is sharing information with a remote computer using the TCP/IP protocol. Suddenly, the connection stops working and appears to hang. Which command can you use to check the connection?

- (•) **netstat**
- ( ) **ipconfig**
- ( ) **ping**
- ( ) **arp**
- ( ) **nbtstat**

Explanation

Use the **netstat** command to check the status of a TCP connection.
[netpro18v5_all_questions_en.exm NP05_4-1 #31]

Question 36: Correct

You work in an office that uses Linux servers and Windows servers. The network uses the TCP/IP protocol.

You are sitting at a workstation that uses Windows 10. An application you are using is unable to contact a Windows server named FileSrv2.

Which command can you use to determine whether your computer can still contact the server?

- **tracert**
- **nwlookup**
- **arp**
- **ping**

Explanation

On a TCP/IP-based network, you can use the **ping** command to check connectivity between a source and destination computer.
[netpro18v5_all_questions_en.exm NP05_4-1 #15]

Question 37: Incorrect

You have installed a new application on a network device. During testing, it appears as if the software is causing other services running on the device to stop responding.

Which tool should you consult to identify the problem?

- Application log
- Load tester
- Packet sniffer
- ~~Throughput tester~~

Explanation

Logs contain a record of events that have happened on a system. Logging capabilities are built into operating systems, services, and applications. Log entries are generated in response to configuration changes, changes in system state, or network condition variations.

A packet sniffer is special software that captures (records) frames that are transmitted on the network. A load tester simulates a load on a server or service. A throughput tester measures the amount of data that can be transferred through a network or processed by a device (such as the amount of data that can be retrieved from disk in a specific period of time).
[netpro18v5_all_questions_en.exm NP09_4-4 #MCS6]

Question 38: Correct

Which of the following terms identifies the wiring closet in the basement or a ground floor that typically includes the demarcation point?

- Horizontal cross connect
- IDF
- MDF
- 110 block
- Smart jack

Explanation

The main distribution frame (MDF) is the main wiring point for a building. The MDF is typically located on the bottom floor or basement. The LEC typically installs the demarc to the MDF. An intermediate distribution frame (IDF) is a smaller wiring distribution point within a building. IDFs are typically located on each floor directly above the MDF, but you can place additional IDFs on each floor as necessary.

A horizontal cross connect joins wiring closets on the same floor. A smart jack is a special loopback plug installed at the demarcation point for a WAN service. Technicians at the central office can send diagnostic commands to the smart plug to test connectivity between the central office and the demarc.

Use 66 and 110 blocks to connect individual wires within a wiring closet.
[netpro18v5_all_questions_en.exm NP09_2-8 #MCS6]

Question 39: Incorrect

Users report that the network is down. As a help desk technician, you investigate and determine that a specific router is configured so that a routing loop exists.

What should you do next?

- Document the problem.
- Create an action plan.
- ~~Fix the problem.~~
- Determine if escalation is needed.

Explanation

After identifying the most probable cause, escalate the problem if it is beyond your ability to fix or if it is out of your scope of management. For example, the problem might be in a router configuration that you are not authorized to correct. When forwarding the problem on to someone else, be sure to describe the nature of the problem, the actions you have already taken, and the symptoms that lead you to believe the problem is outside of your area of responsibility.

If you decide that escalation is not necessary, you can then create an action plan that includes the fix and identifying possible effects of implementing the fix. After the solution has been implemented, verify that it works and that there were no unforeseen consequences. Finally, document the problem and the solution.
[netpro18v5_all_questions_en.exm NP09_4-6 #MCS2]

Question 40: Incorrect

You manage a server at work that has just been configured with a new application. Consequently, the server has crashed several times during the last week. You think you have resolved the problem, but you would like to be able to manage the server remotely just in case more issues occur.

Which of the following protocols would you use for remote management? (Select two.)

- [ ] ICA
- [ ] PPPoE
- [ ] PPP
- [x] VNC
- [x] ~~L2TP~~
- [ ] PPTP

Explanation

Use a remote desktop protocol to remotely manage devices. The remote desktop protocol allows you to interact with the computer's desktop without being present at the console. There are multiple protocols that you can use for remote desktop connections.

- Virtual Network Computing (VNC) was originally developed for UNIX. Applications using VNC include RealVNC, TightVNC, UltraVNC, and Vine Server.
- Independent Computing Architecture (ICA) is the protocol used by Citrix products (WinFrame and MetaFrame/XenApp).
- The Remote Desktop Protocol (RDP) is the protocol developed by Microsoft and used in Microsoft's Terminal Services, Remote Desktop, and Remote Assistance solutions. Aqua Connect has licensed RDP and created a version for Mac OS X as a server.

PPP and PPPoE are protocols that are used to control remote access. Both allow the authentication, authorization, and accounting of remote access connections. PPTP and L2TP are VPN protocols that provide a secure connection to a destination host or network through the internet .
[netpro18v5_all_questions_en.exm NP09_6-3 #MCM1]

Question 41: Incorrect

You are reviewing the output of the **show interfaces** command for the Gi0/1 interface on a switch. You notice a significant number of CRC errors displayed.

What are the most likely causes? (Select two. Each response is a complete solution.)

- [ ] The cable connected to this interface is a cross-over cable, but should be a straight-through cable.
- [x] ~~The cable connected to this interface is a straight-through cable, but should be a cross-over cable.~~
- [x] Collisions.
- [ ] EMI or cross-talk on the cable connected to the interface.
- [ ] The device on the other end of the cable is powered off or the other interface is administratively shutdown.

Explanation

CRC errors are received frames that did not pass the FCS check. These are usually caused by collisions, but they can also be caused by EMI or cross-talk on UTP cabling. All of these conditions can damage frames on the wire, causing a CRC error.

Using the wrong type of cabling would cause the link to go down. A disabled interface on the other end of the cable would also cause the link to go down.
[netpro18v5_all_questions_en.exm *NP15_WAN_TROUBLESHOOTING_05]

Question 42: Correct

In virtualization, what is the role of the hypervisor?

- ( ) A hypervisor has the actual hardware in place on the machine, such as the hard disk drive(s), optical drive, RAM, and motherboard.
- ( ) A hypervisor is created within the host operating system and simulates a hard disk for the virtual machine.
- ( ) A hypervisor is a software implementation that executes programs like a physical machine.
- (•) A hypervisor allows virtual machines to interact with the hardware without going through the host operating system.

Explanation

A hypervisor is a thin layer of software that resides between the virtual operating system(s) and the hardware. A hypervisor allows virtual machines to interact with the hardware without going through the host operating system. A hypervisor manages access to system resources such as:

- CPU
- Storage
- RAM

A physical machine (also known as the host operating system) has the actual hardware in place on the machine, such as the hard disk drive(s), optical drive, RAM, motherboard, etc. A virtual machine is a software implementation that executes programs like a physical machine. A virtual machine appears to be a self-contained and autonomous system. A virtual hard disk (VHD) is a file that is created within the host operating system and simulates a hard disk for the virtual machine.
[netpro18v5_all_questions_en.exm NP15_VIRTUALIZATION_01]

Question 43: Incorrect

Match the EtherChannel protocol on the left with its characteristics on the right. Each protocol may be used once, more than once, or not at all.

Desirable mode places the port in a negotiating state.	Based on the 802.3ad standard.
~~Link Aggregation Control Protocol (LACP)~~	✓ Link Aggregation Control Protocol (LACP)
Port Aggregation Protocol (PAgP)	
Passive mode places the port into a passive negotiating state.	Auto mode places the port into a passive negotiating state.
~~Port Aggregation Protocol (PAgP)~~	✓ Port Aggregation Protocol (PAgP)
Link Aggregation Control Protocol (LACP)	

Active mode places the port in a negotiating state.

✓ Link Aggregation Control Protocol (LACP)

Explanation

Cisco switches can use the following protocols for EtherChannel configuration:

Port Aggregation Protocol (PAgP)

Port Aggregation Protocol prevents loops, limits packet loss due to misconfigured channels, and aids in network reliability. PAgP operates in the following modes:

- Auto places the port into a passive negotiating state and forms an EtherChannel if the port receives PAgP packets. While in this mode, the port does not initiate the negotiation.
- Desirable places the port in a negotiating state to form an EtherChannel by sending PAgP packets. A channel is formed with another port group in either the auto or desirable mode.

Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol is based on the 802.3ad standard and has similar functions to PAgP. LACP is used when configuring EtherChannel between Cisco switches and non-Cisco switches that support 802.3ad. LACP operates in the following modes:

- Passive places the port into a passive negotiating state and forms an EtherChannel if the port receives LACP packets. While in this mode, the port does not initiate the negotiation.
- Active places the port in a negotiating state to form an EtherChannel by sending LACP packets. A channel is formed with another port group in either the active or passive mode.

[netpro18v5_all_questions_en.exm RT NP15_2.6-2]

Question 44: Correct

You have been struggling to keep the temperature in your server room under control. To address this issue, you have decided to reconfigure the room to create hot and cold aisles.

Which of the following are true concerning this configuration? (Select two.)

- ☐ The hot aisle should face the air conditioner's output ducts.
- ➡ ☑ The rear of your servers should face the hot aisle.
- ➡ ☑ The front of your servers should face the cold aisle.
- ☐ The rear of your servers should face the cold aisle.
- ☐ The cold aisle should face the air conditioner's return duct.
- ☐ The front of your servers should face the hot aisle.

Explanation

The use of hot and cold aisles within the server room is an effective method for reducing the temperature. The front of your servers should face the cold aisle. This allows them to draw in cooler air to reduce the temperature of system components. The rear of your servers should face the hot aisle. This ensures the hot air is directed away from other server systems. The hot aisle should face the air conditioner's return duct. This allows the heated air to be cooled by the AC system. The cold aisle should face the air conditioner's output ducts. This ensures cool air is drawn into servers to cool their components.

[netpro18v5_all_questions_en.exm RT NP15_5.7-6]

Question 45: Incorrect

Which of the following describe the channels and data transfer rates used for ISDN BRI? (Select two.)

- ➡ ☐ Two B channels operating at 64 Kbps each
- ☑ ~~One D channel operating at 64 Kbps~~
- ➡ ☐ One D channel operating at 16 Kbps
- ☑ ~~23 B channels operating at 64 Kbps each~~

Explanation

ISDN BRI uses two B channels operating at 64 Kbps each and one D channel operating at 16 Kbps. It is often called 2B + 1D.

ISDN PRI uses 23 B channels (at 64 Kbps) and one D channel (at 64 Kbps). It is also called 23B + 1D.
[netpro18v5_all_questions_en.exm *NP15_WAN_CONCEPTS_14]

Question 46: Incorrect

Which port does Telnet use?

- 23
- ~~34~~
- 25
- 80

Explanation

Telnet uses port 23.
[netpro18v5_all_questions_en.exm NP05_2-12 #41]

Question 47: Correct

Which of the following statements about SSL VPN are true? (Select two.)

- [ ] Uses pre-shared keys for authentication.
- [x] Encrypts the entire communication session.
- [ ] Uses UDP port 500.
- [x] Uses port 443.
- [ ] Provides message integrity using HMAC.
- [ ] Encapsulates packets by adding a GRE header.

Explanation

SSL VPN uses the SSL protocol to secure communications. SSL VPN:

- Authenticates the server to the client using public key cryptography and digital certificates.
- Encrypts the entire communication session.
- Uses port 443, which is already open on most firewalls.

Pre-shared keys are used by IPsec to provide authentication with other protocols. IPsec also uses HMAC to provide message integrity checks. GRE headers are used exclusively by the GRE tunneling protocol. UDP port 500 is used by the Layer 2 tunneling protocol (L2TP).
[netpro18v5_all_questions_en.exm *NP15_REMOTE_ACCESS_SECURITY_01]

Question 48: Incorrect

The media access control method of all Ethernet networks is _____.

- Polling
- ~~CSMA/CA~~
- CSMA/CD
- Token passing

Explanation

Carrier sense multiple access with collision detection (CSMA/CD) is the media access control method of all Ethernet networks.
[netpro18v5_all_questions_en.exm NP05_1-2 #23]

Question 49: Correct

A user from the sales department calls to report that he is experiencing problems connecting to the sales file server. All users in the sales department connect to the sales server through a single Ethernet switch. No other users have reported problems connecting to the sales server.

Which of the following troubleshooting actions are you most likely to perform first?

- Replace the Ethernet switch in the sales department.
- Replace the network card in the sales server.
- Reinstall the network card drivers on the sales server.
- Replace the network card in the user's computer.

Explanation

In this scenario, you are most likely to replace the network card in the user's computer.

As there is only one user experiencing a problem, you are unlikely to replace the network card in the server or replace the Ethernet switch. For the same reason, you are also unlikely to replace the network card drivers on the server. If more than one user were experiencing the problem, any of the options could be a valid troubleshooting step.
[netpro18v5_all_questions_en.exm NP05_4-8 #95]

Question 50: Correct

Assuming the network is indicated by the default portion of the IP address, which three of the following IP addresses belong to the Class A network 114.0.0.0? (Select three.)

- [ ] 115.88.0.55
- [ ] 115.77.89.4
- [x] 114.122.66.12
- [ ] 115.0.0.66
- [x] 114.0.0.15
- [x] 114.58.12.0

Explanation

With a Class A network, the first octet indicates the network address. All hosts on the network must have the same value in the first octet (114).
[netpro18v5_all_questions_en.exm NP05_2-6 #76]

Question 51: Incorrect

When troubleshooting network issues, it's important to carry out tasks in a specific order.

Drag the trouble shooting task on the left to the correct step on the right.

Step 1	
✓ Identify the problem.	
Step 2	
✓ Establish a theory of probable cause.	
Step 3	
✓ Test the theory to determine the cause.	
Step 4	
~~Document findings, actions, and outcomes.~~	Establish a plan of action.
Step 5	
~~Establish a plan of action.~~	Implement the solution or escalate.
Step 6	

~~Implement the solution or escalate.~~	Verify full system functionality.

Step 7

~~Verify full system functionality.~~	Document findings, actions, and outcomes.

Explanation

The following is a general approach to network troubleshooting:

1. Identify the problem.
2. Establish a theory of probable cause.
3. Test the theory to determine the cause.
4. Establish a plan of action to resolve the problem and identify potential effects.
5. Implement the solution or escalate as necessary.
6. Verify full system functionality and, if applicable, implement preventative measures.
7. Document findings, actions, and outcomes.

[netpro18v5_all_questions_en.exm *NP15_PERF-BASED_01]

Question 52: Incorrect

Your wireless network consists of multiple 802.11n access points that are configured as follows:

- SSID (hidden): CorpNet
- Security: WPA2-PSK using AES
- Frequency: 5.75 GHz
- Bandwidth per channel: 40 MHz

Because of the unique construction of your organization's facility, there are many locations that do not have a clear line of sight between network clients and access points. As a result, radio signals are reflected along multiple paths before finally being received. The result is distorted signals that interfere with each other.

What should you do?

- Reduce the power of the access point radio signals.
- ~~Install directional access points.~~
- Implement antenna diversity.
- Switch to RADIUS authentication for wireless clients.

Explanation

Antenna diversity implements two or more radio antennae to improve the quality and reliability of a wireless link. In environments where there is no clear line of sight between transmitter and receiver, the radio signal is reflected along multiple paths before finally being received. This can introduce phase shifts, time delays, attenuation, and distortion that interfere with each another on the receiving antenna.

You can rectify the situation by implementing antenna diversity two ways:

- *Spatial diversity* uses multiple antennas that are physically separated from one another.
- *Pattern diversity* uses two or more co-located antennas with different radiation patterns.

Using a RADIUS authentication solution increases wireless network security, but it doesn't address the issue of multipath interference. Reducing radio power could help solve multipath interference issues in some situations, but it may make it worse in others. This is also true of directional access points.

[netpro18v5_all_questions_en.exm MCS4]

Question 53: Correct

Your company uses VoIP for phone calls. Recently, employees have been complaining about phone calls with unusual sound effects.

Which type of problem is occurring on the VoIP system?

- Packet loss
- Latency
- Jitter
- Echo

Explanation

Because VoIP transmits call data using IP packets over a packet-switched network, VoIP is susceptible to the following problems:

- Latency occurs when data takes a long time to arrive at the receiving device. Delays cause long pauses between speaking and receiving and can result in callers continually interrupting each other.
- Jitter is a variation in the delay of individual packets. Jitter causes strange sound effects as the delay of packets fluctuates.
- Packet loss occurs when packets do not arrive at all. Packet loss causes drop-outs in the conversation.
- Echo occurs when you hear your own voice in the telephone receiver while you are talking. Excessive delay can cause unacceptable levels of echo.

[netpro18v5_all_questions_en.exm *NP15_VOICE_OVER_IP_04]

Question 54: Correct

What is the minimum cable specification that supports 1000 Mbps Ethernet?

- ○ Cat 3
- ○ Cat 4
- ○ Cat 5
- ➡ ◉ Cat 5e
- ○ Cat 6
- ○ Cat 7

Explanation

1000 Mbps Ethernet (Gigabit Ethernet) requires at least Cat 5e cables.

Cat 3 and Cat 4 only support 10 Mbps Ethernet. Cat 5 cable only supports up to 100 Mbps. Cat 6 or Cat 7 is required for bandwidth up to 10 Gbps Ethernet.

[netpro18v5_all_questions_en.exm NP09_2-1 #1]

Question 55: Incorrect

Which of the following are solutions that address physical security? (Select two.)

- ☐ Implement complex passwords.
- ➡ ☐ Escort visitors at all times.
- ➡ ☑ Require identification and name badges for all employees.
- ☐ Scan all floppy disks before use.
- ☑ ~~Disable guest accounts on computers.~~

Explanation

Physical security controls physical access to the network or its components. Physical security controls include:

- Requiring identification or key cards before entry is permitted.
- Escorting visitors at all times.
- Keeping doors and windows locked.
- Keeping devices with sensitive information out of view of public users.
- Keeping the server room locked and locking computers to racks or tables to prevent theft.

[netpro18v5_all_questions_en.exm NP09 6-5 MCM2]

Question 56: Correct

Which of the following strategies are used to prevent duplicate IP addresses being used on a network? (Select two.)

- ➡ ☑ Use Automatic Private IP Addressing.
- ☐ Set the Windows network-monitoring utility to identify potential IP conflicts.
- ☐ Install the DHCP client on all workstations.

- [x] Install a DHCP server on the network.
- [ ] Configure client systems to use static IP assignment.
- [ ] Configure a HOSTS file for local IP resolution.

Explanation

To avoid duplicate IP addresses being used by network systems, automatic IP assignment is used. Both the DHCP service and APIPA can automatically assign addresses to client systems.

Clients configured to use static IP addressing may inadvertently have duplicate IP addresses assigned to them. In such a case, one of the systems will not be able to log on to the network.
[netpro18v5_all_questions_en.exm NP05_2-9 #61]

Question 57: Correct

Which component of a change and configuration management policy identifies technical and budgetary considerations associated with a proposed change and also identifies any potential impacts to the network?

- ( ) Change request
- (•) Feasibility analysis
- ( ) Authorized downtime
- ( ) Rollback

Explanation

A feasibility analysis identifies technical and budgetary considerations associated with a proposed change. It should also identify any potential impacts to the network.

In the event that a change unintentionally causes problems, your change and configuration management process should include provisions for a rollback. A rollback makes it possible to revert the system back to the state it was in before the change was put into effect. Authorized downtime defines a maintenance window during which the system will be unavailable while the change is made. A change request identifies the need for a change.
[netpro18v5_all_questions_en.exm RT NP15_5.8-3]

Question 58: Incorrect

In business continuity planning, what is the primary focus of the scope?

- ( ) Business processes
- ( ) Company assets
- (•) ~~Recovery time objective~~
- ( ) Human life and safety

Explanation

Business processes are the primary focus of the scope of BCP.

Company assets are the focus of risk assessment for security policy development, not BCP. Human life and safety are considerations for emergency response, but are not the focus of the BCP scope. Recovery time objective is a consideration in the development of emergency response, not an aspect of BCP scope.
[netpro18v5_all_questions_en.exm SSCP-7 CP [198]]

Question 59: Incorrect

You want to use CCTV to increase your physical security. You want to be able to remotely control the camera position. Which camera type should you choose?

- ( ) PTZ
- ( ) Bullet
- (•) ~~C-mount~~
- ( ) Dome

Explanation

A pan tilt zoom (PTZ) camera lets you dynamically move the camera and zoom in on specific areas (cameras without PTZ capabilities are manually set looking a specific direction). Automatic PTZ mode automatically moves the camera between several preset locations; manual PTZ lets an operator remotely control the camera positon.

A bullet camera has a built-in lens and is long and round in shape. Most bullet cameras can be used indoors or outdoors. A c-mount camera has interchangeable lenses and is typically rectangular in shape. Most c-mount cameras require a special housing to be used outdoors. A dome camera is a camera protected with a plastic or glass dome. These cameras are more vandal-resistant than other cameras.

PTZ cameras can be bullet, c-mount, or dome cameras.
[netpro18v5_all_questions_en.exm SP08_3-9 1]

Question 60: Incorrect

After installing a new 2.4Ghz cordless phone system in your office, you notice that wireless network performance is adversely affected. Which of the following wireless networking standards are you most likely using? (Select two.)

- [x] 802.11b
- [ ] 802.11g
- [ ] 802.11a
- [ ] Bluetooth

Explanation

Both the 802.11b and 802.11g wireless networking standards use the 2.4Ghz frequency range. A cordless phone system on the same frequency range may affect the performance of the wireless network.

802.11a uses the 5Ghz frequency range, so it would not be affected by a cordless phone system that uses the 2.4Ghz frequency range. Bluetooth does use the 2.4Ghz frequency range, but is used more widely as a mechanism to connect consumer electronic devices like personal digital assistants (PDAs), cameras, and phones, rather than as a wireless local area networking (LAN) method.
[netpro18v5_all_questions_en.exm NP05_4-8 #87]

Question 61: Correct

When a malicious user captures authentication traffic and replays it against the network later, what is the security problem you are most concerned about?

- (•) An unauthorized user gaining access to sensitive resources
- ( ) Denial of service
- ( ) Spam
- ( ) Bandwidth consumption

Explanation

When a malicious user captures authentication traffic and replays it against the network later, the security problem you are most concerned about is an unauthorized user gaining access to sensitive resources. Once a replay attack has been successful, the attacker has the same access to the system as the user from whom the authentication traffic was captured.
[netpro18v5_all_questions_en.exm CISSP-102 SP [23]]

Question 62: Incorrect

Which type of internet service uses the DOCSIS specification?

- (•) ~~Fiber optic~~
- ( ) Unshielded twisted pair
- ( ) Coaxial cable
- ( ) Shielded twisted pair

Explanation

The Data Over Cable Service Interface Specification (DOCSIS) defines coaxial cable networking specifications. It is used by cable TV providers to provide internet access over their existing coaxial cable infrastructure. It specifies channel widths and modulation techniques. It also defines the manner in which the core components of the network communicate.
[netpro18v5_all_questions_en.exm RT NP15_5.4-1]

Question 63: Correct

A user on your network has been moved to another office down the hall. After the move, she calls you complaining that she has only occasional network access through her wireless connection. Which of the following is most likely the cause of the problem?

- The client system has moved too far away from the access point.
- The encryption level has been erroneously set back to the default setting.
- The client has incorrect WEP settings.
- An SSID mismatch between the client and the WAP.
- An SSID mismatch between the client and the server.

Explanation

In this case, the wireless client system has had no problems accessing the wireless access point until she moves to the new office. In some cases, moving a system will cause signal loss either from the increased distance away from the WAP or from unexpected interference by such things as concrete walls or steel doors. There are several ways to correct the problem, including reducing the physical distance to the client, using a wireless amplifier, upgrading the antennae on the wireless devices, or adding another WAP to the infrastructure.

Because the client could previously access the WAP and still has occasional access, it is likely that the move was the cause of the problem and not any configuration setting on the client system.
[netpro18v5_all_questions_en.exm NP05_4-8 #23]

Question 64: Incorrect

You are considering using Wi-Fi triangulation to track the location of wireless devices within your organization. However, you have read on the internet that this type of tracking can produce inaccurate results.

What is the most important consideration for getting reliable results when implementing this type of system?

- Wireless encryption in use
- Signal strength
- Wireless standard in use
- ~~WAP placement~~

Explanation

Wi-Fi triangulation works by configuring wireless devices to sniff for wireless networks in range and then measuring each network's signal strength. The results are compared with a signal strength database, and basic geometry identifies the device's location. The wireless device doesn't actually have to connect to any of these networks; it simply scans them to determine their signal strength. For this to work, the administrators of all Wi-Fi networks used for triangulation must perform periodic site surveys to populate and maintain the signal strength database.

WAP placement is a consideration in Wi-Fi triangulation, but the signal strength database is the key to determining a device's location. Only a small amount of physical displacement between access points is necessary to triangulate. The wireless standard or encryption in use has little effect on Wi-Fi triangulation.
[netpro18v5_all_questions_en.exm MCS8]

Question 65: Incorrect

You are traveling throughout North America to many metropolitan and rural areas.

Which single form of internet connectivity provides the greatest potential connectivity wherever you travel?

- ~~Broadband cable~~

- DSL
- PSTN
- ISDN

Explanation

Network access using a modem over the telephone company network (PSTN) is not the fastest method for internet connectivity. However, it has the advantage of being available virtually anywhere that regular voice-grade communications are available.

Broadband cable is dependent on service offerings from the regional cable television company, which does not have as great a presence as the telephone company. To use broadband cable, the service must be added to the cable TV lines. DSL and ISDN are offered through the telephone company; however, they are not available in all service areas. And even when available, they require that the subscriber be within a certain proximity of telephone company equipment.
[netpro18v5_all_questions_en.exm *NP15_WAN_CONCEPTS_18]

Question 66: Incorrect

You are adding a new rack to your data center, which will house two new blade servers and a new switch. The new servers will be used for file storage and a database server.

The only space you have available in the data center is on the opposite side of the room from your existing rack, which already houses several servers, a switch, and a router. You plan to configure a trunk port on each switch and connect them with a cross-over UTP plenum cable that will run through the suspended tile ceiling of the data center.

To provide power for the new devices, you had an electrician install several new 20-amp wall outlets near the new rack. Each device in the rack will be plugged directly into one of these new wall outlets.

What is wrong with this configuration? (Select two.)

- [x] You should implement a UPS between the wall outlet and the network devices.
- [ ] You should implement redundant power supplies for the network devices.
- [ ] You should not run a plenum cable through a suspended tile ceiling.
- [x] ~~You should not connect networking equipment to a 20-amp wall circuit.~~
- [ ] You must use a straight-through cable to connect the two switches together.

Explanation

In this scenario, all devices in the new rack will go down if the power from the wall outlet fails for some reason (such as a power outage). To prevent this from happening, a UPS should be implemented between the wall outlets and the network devices. In addition, the power supplies used by computing equipment have finite life spans and fail frequently. Because these are mission-critical devices, you should consider implementing redundant power supplies.

Plenum network cabling is specifically designed to run through a suspended tile ceiling. The space between the suspended tile and the physical ceiling is called a ceiling plenum. In the early days of networking, cross-over cables were required to uplink two hubs or switches together. Most modern switches implement Auto MDI-X, which detects whether cross-over is required and automatically configures the interface, allowing you to use either a cross-over or straight-through cable. Using a 20-amp circuit for networking equipment is considered a data center best practice. Connecting too many devices to a standard 15-amp wall circuit can overload it and trip its breaker.
[netpro18v5_all_questions_en.exm RT NP15_5.7-5]

Question 67: Correct

How can QoS be configured so that large data transfers will not block VoIP calls by using too much network bandwidth?

- QoS can be configured on network devices to only allow network protocols that throttle network bandwidth usage.
- QoS can be configured on network devices to limit the size of a file that can be transferred on the network.
- QoS can be configured on network devices to set a bandwidth threshold on selected ports.

- [x] QoS can be configured on network devices to give priority to VoIP traffic.

Explanation

Network devices can examine the type of service or precedence bits in the header of an IP packet to determine the type of traffic. QoS settings can be configured on a network devices to give VoIP traffic priority over normal computer traffic.
[netpro18v5_all_questions_en.exm MCS7]

Question 68: Correct

Which organization is responsible for allocating public IP addresses?

- [ ] CompTIA
- [ ] IETF
- [ ] IEEE
- [x] IANA

Explanation

The Internet Assigned Numbers Authority (IANA) is responsible for allocating IP addresses used on the internet. When you want to obtain a public IP address, you would typically get the address from your ISP. The ISP has received addresses from a Regional Internet Registry (RIR), which was previously assigned a block of addresses from IANA. IANA is operated by the Internet Corporation for Assigned Names and Numbers (ICANN), so you might also see that ICANN is responsible for assigning public IP addresses.

The IETF is an organization that is responsible for settings standards used on the internet. For example, the IETF has defined the standards for NAT as well as other protocols. The IEEE is an organization that sets networking standards for technologies such as Ethernet or wireless networking. CompTIA is a professional organization that represents computing technology companies and individuals.
[netpro18v5_all_questions_en.exm NP09_1-4 #9]

Question 69: Incorrect

You have been hired to design a wireless network for a SOHO environment. You are currently in the process of gathering network requirements from management.

Which of the following questions should you ask? (Select three.)

- [x] What type of data will be transmitted on the network?
- [x] Is the size of the business expected to grow in the future?
- [ ] Are there microwaves or cordless phones that can cause interference?
- [x] ~~Where can network hardware be mounted in the building?~~
- [x] How many devices will need to be supported?

Explanation

The first thing you do when designing a wireless network is gather network requirements. Meet with all stakeholders and decision-makers to discuss the implementations and gather detailed information. For example, you should:

- Identify the intended use of the wireless network.
- Identify the location of wireless service areas.
- Anticipate the number of wireless devices that need to be supported in each area.
- Discuss future network needs so that you can plan for expansion.
- Discuss data encryption and network security requirements.

Mounting points or sources of interference should be considered in the network design phase, after all requirements have been gathered.
[netpro18v5_all_questions_en.exm *NP15_WIRELESS_NETWORK_DESIGN]

Question 70: Incorrect

Match each type of access point on the left with the wireless network architecture where it is commonly used on the right. Each type of access point may be used once, more than once, or not at all.

Independent access point infrastructure

~~Lightweight AP~~ Intelligent AP

Hub-and-spoke infrastructure

~~Intelligent AP~~ Lightweight AP

Distributed wireless mesh infrastructure

✓ Intelligent AP

Explanation

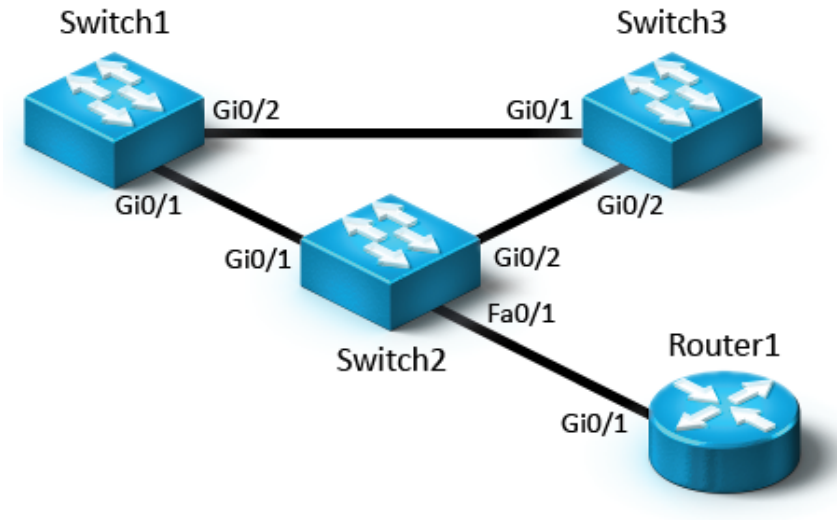
Different types of access points are used in different wireless network architectures, as described in the following table:

Architecture	Description
Independent Access Points	In the early days of wireless networking, large organizations implemented independent access points throughout their facilities. Each AP stood alone, providing separate wireless networks using its own independent configuration.
Hub-and-Spoke Infrastructure	In a hub-and-spoke configuration, a wireless controller is connected to all access points using wired links. The individual access points contain very little embedded intelligence and are sometimes referred to as lightweight access points (LWAPs).
Distributed Wireless Mesh Infrastructure	Newer wireless networks can be deployed using a distributed wireless mesh architecture. These networks still use a controller, but they move some of the network intelligence from the controller out to the individual access points. In this configuration, the controller is no longer a bottleneck. The APs are smart enough to communicate directly with each other to create more efficient data paths for network traffic.

[netpro18v5_all_questions_en.exm RT NP15_4.3-2]

Question 71: Correct

This question includes an image to help you answer the question. Close



Consider the network shown in the exhibit.

You have been experiencing intermittent connectivity issues with switch2. To check the status of the interfaces, you run the following commands:

switch2# show interfaces fa0/1 status
Port Name Status Vlan Duplex Speed Type
Fa0/1 connected 3 a-half a-100 10/100BaseTX

switch2# show interfaces Gi0/1 status
Port Name Status Vlan Duplex Speed Type
Gi0/1 connected trunk a-full a-1000 1000BaseTX

switch2# show interfaces Gi0/2 status
Port Name Status Vlan Duplex Speed Type
Gi0/2 connected trunk a-full a-1000 1000BaseTX

What is the issue with this network?

- The device connected to the Fa0/1 interface has auto-negotiation disabled.
- The device connected to the Gi0/1 interface has auto-negotiation disabled.
- There is a link speed mismatch on the Gi0/1 interface.
- There is a duplex mismatch on the Gi0/2 interface.
- There is a link speed mismatch on the Gi0/2 interface.

Explanation

A duplex mismatch probably exists on the Fa0/1 interface. Note that duplexing has been automatically set to half, which is the default behavior for Cisco devices when auto-negotiation fails. To fix the issue, check the Gi0/1 interface on router1 to see if auto-negotiation has been disabled. You could manually configure the Fa0/1 interface on switch2 to use the same duplexing and link speed settings as the interface on the router, or you could re-enable auto-negotiation on the router interface.

The Gi0/1 and Gi0/2 interfaces on switch2 appear to be functioning correctly with full duplexing and full link speed automatically configured.
[netpro18v5_all_questions_en.exm *NP15_WAN_TROUBLESHOOTING_08]

Question 72: Correct

You want to know what protocols are being used on your network. You'd like to monitor network traffic and sort traffic based on protocol.

Which tool should you use?

- Packet sniffer
- IDS
- Throughput tester
- IPS
- Port scanner

Explanation

A packet sniffer is special software that captures (records) frames that are transmitted on the network. Use a packet sniffer to:

- Identify the types of traffic on a network.
- View the exchange of packets between communicating devices. For example, you can capture frames related to DNS and view the exact exchange of packets for a specific name resolution request.
- Analyze packets sent to and from a specific device.
- View packet contents.

Use a port scanner to identify protocol ports that are opened in a firewall or active on a device. A port scanner checks individual systems, while a packet sniffer watches traffic on the network. A throughput tester measures the amount of data that can be transferred through a network or processed by a device (such as the amount of data that can be retrieved from disk in a specific period of time).

An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. A passive IDS monitors, logs, and detects security breaches, but takes no action to stop or prevent the attack. An active IDS (also called an intrusion protection system or IPS) performs the functions of an IDS, but can also react when security breaches occur.
[netpro18v5_all_questions_en.exm NP09_5-2 #MCS1]

Question 73: Incorrect

You want to implement 802.1x authentication on your wireless network. Which of the following will be

required?

- ~~WPA2~~
- RADIUS
- TKIP
- WPA

Explanation

802.1x authentication uses usernames and passwords, certificates, or devices such as smart cards to authenticate wireless clients. 802.1x authentication requires the following components:

- A RADIUS server to centralize user account and authentication information. A centralized database for user authentication is required to allow wireless clients to roam between cells and authenticate using the same account information.
- A PKI for issuing certificates. At a minimum, the RADIUS server must have a server certificate. To support mutual authentication, each client must also have a certificate.

You can use 802.1x authentication with both WPA and WPA2, and even with WEP with some devices and operating systems. TKIP is an encryption method used with WPA.
[netpro18v5_all_questions_en.exm NP09_1-7 #6]

Question 74: Incorrect

Members of the sales team use laptops to connect to the company network. While traveling, they connect their laptops to the internet through airport and hotel networks.

You are concerned that these computers will pick up viruses that could spread to your private network. You would like to implement a solution that prevents the laptops from connecting to your network unless anti-virus software and the latest operating system patches have been installed.

Which solution should you use?

- NAT
- NIDS
- NAC
- ~~VLAN~~
- DMZ

Explanation

Network Access Control (NAC) controls access to the network by not allowing computers to access network resources unless they meet certain predefined security requirements. Conditions that can be part of the connection requirements include requiring that computers have:

- Anti-virus software with up-to-date definition files
- An active personal firewall
- Specific operating system critical updates and patches

A client that is determined by the NAC agent to be healthy is given access to the network. An unhealthy client who has not met all the checklist requirements is either denied access or can be given restricted access to a remediation network, where remediation servers can be contacted to help the client to become compliant.

A demilitarized zone (DMZ) is a buffer network (or subnet) that sits between the private network and an untrusted network (such as the internet). A virtual LAN (VLAN) is a logical grouping of computers based on switch port. VLAN membership is configured by assigning a switch port to a VLAN. An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. A network-based IDS (NIDS) scans network traffic to look for intrusion attempts.

Network address translation (NAT) modifies the IP addresses in packets as they travel from one network (such as a private network) to another (such as the internet). NAT allows you to connect a private network to the internet without obtaining registered addresses for every host. Hosts on the private network share the registered IP addresses.
[netpro18v5_all_questions_en.exm SP08_2-2 2]

Question 75: Incorrect

You are configuring a network firewall to allow SMTP outbound email traffic and POP3 inbound email

traffic.

Which of the following TCP/IP ports should you open on the firewall? (Select two.)

- [x] ~~143~~
- [ ] 443
- [x] 110
- [ ] 25
- [ ] 21

Explanation

The simple mail transfer protocol (SMTP) uses TCP/IP port 25. The post office protocol version 3 (POP3) uses TCP/IP port 110.

The file transfer protocol (FTP) uses TCP/IP Port 21. The internet message access protocol (IMAP) uses TCP/IP port 143. TCP/IP port 443 is used by the secure sockets layer (SSL) protocol.
[netpro18v5_all_questions_en.exm NP05_2-12 #49]

Question 76: Incorrect

You are concerned about protecting your network from network-based attacks from the internet. Specifically, you are concerned about zero day attacks (attacks that have not yet been identified or that do not have prescribed protections).

Which type of device should you use?

- ( ) Host-based firewall
- (•) ~~Network-based firewall~~
- ( ) Anti-virus scanner
- ( ) Signature-based IDS
- ( ) Anomaly-based IDS

Explanation

An anomaly-based intrusion detection system (IDS) can recognize and respond to some unknown attacks. Signature recognition, also referred to as pattern matching or dictionary recognition, looks for patterns in network traffic and compares them to known attack patterns called signatures. Signature-based recognition cannot detect unknown attacks; they can only detect attacks identified by published signature files.

Anti-virus software is a form of signature-based IDS. A network-based firewall filters packets for a network, while a host-based firewall filters packets for a host. Firewalls are typically configured using access control lists that identify specific traffic that is allowed or denied.
[netpro18v5_all_questions_en.exm NP09_6-2 #MCS4]

Question 77: Correct

Which of the following tests can be performed by a TDR? (Select two.)

- [ ] Identify split pairs and miswires.
- [x] Identify the location of a fault on a cable.
- [x] Measure the length of a cable.
- [ ] Measure near end and far end crosstalk.
- [ ] Verify that the cable meets Cat5e, Cat6, or Cat7 standards.

Explanation

A TDR is a special device that sends electrical pulses on a wire in order to discover information about the cable. The TDR measures impedance discontinuities, the echo received on the same wire in response to a signal on the wire. The results of this test can be used to:

- Estimate the length of a wire.
- Measure the cable impedance.
- Identify the locations of splices and connectors on the wire.
- Identify shorts and open circuits and the location of the fault.

Use a cable certifier to verify that a cable meets Cat5e, Cat6, or Cat6e standards, especially to make sure that crosstalk is within acceptable levels. Use a cable tester to check for miswires and split pairs. Many cable certifiers and some cable testers also include a TDR.
[netpro18v5_all_questions_en.exm NP09_5-3 #MCM1]

Question 78: Incorrect

You use Cat5e twisted pair cable on your network. Cables are routed through walls and the ceiling.

A user puts a screw in the wall to hang a picture and pierces the cable so that a signal sent on pin 1 arrives on the cable connected to pin 7.

Which term describes this condition?

- Attenuation
- ~~Split pair~~
- Open circuit
- Short circuit
- Crosstalk

Explanation

An electrical short occurs when electrical signals take a path other than the intended path. In the case of twisted pair wiring, a short means that a signal sent on one wire might arrive on a different wire. Shorts are caused by worn wire jackets, crushed wires that touch, and pierced wire that touches metal. If an open circuit is a cut in the wire that prevents the original signal from reaching the end of the wire, you will have a short.

If you have a short, the signal travels a different path. If you have an open circuit, the signal does not travel anywhere (electricity cannot flow because the path is disconnected).

Crosstalk is interference that is caused by signals within the twisted pairs of wires. Attenuation is the loss of signal strength from one end of a cable to the other caused by distance. A split pair condition is where a single wire in two different pairs is reversed at both ends. For example, instead of matching the green and green/white wires in pins 1 and 2, you swap the solid green wire with the solid brown wire.
[netpro18v5_all_questions_en.exm NP09_4-7 #MCS7]

Question 79: Incorrect

The Data Link Layer of the OSI model is comprised of two sublayers. What are they? (Select two.)

- [x] LLC
- [ ] LAT
- [x] MAC
- [ ] SAN
- [x] ~~DLC~~

Explanation

The Data Link layer is split into the following sublayers:

- The Logical Link Control (LLC) Sublayer, which provides the operating system link to the device driver.
- The Media Access Control (MAC) Sublayer, which translates generic network requests into device-specific terms.

[netpro18v5_all_questions_en.exm NP05_2-2 #139]

Question 80: Incorrect

You've decided to use a subnet mask of 255.255.192.0 on the 172.17.0.0 network to create four separate subnets.

Which network IDs will be assigned to these subnets in this configuration? (Select two.)

- [x] ~~172.17.96.0~~
- [ ] 172.17.128.0
- [ ] 172.17.0.0
- [ ] 172.17.16.0
- [x] ~~172.17.32.0~~

Explanation

The subnet mask used for the 172.17.0.0 network can be viewed in binary notation as 11111111.11111111.11000000.000000. Because the first two bits of the third octet are used for the network portion of the address, four subnets are possible:

- 172.17.0.0
- 172.17.64.0
- 172.17.128.0
- 172.17.192.0

[netpro18v5_all_questions_en.exm RT-SP-6.1-1]

Question 81: Incorrect

You have implemented a network where hosts are assigned specific roles, such as file sharing and printing roles. Other hosts access those resources, but do not host services of their own.

What type of network do you have?

- (•) ~~Peer-to-peer~~
- ( ) Intranet
- ( ) Client-server
- ( ) Extranet

Explanation

In a client-server network, hosts have specific roles. For example, some hosts are assigned server roles, which allow them to provide network resources to other hosts. Other hosts are assigned client roles, which allow them to consume network resources.

In a peer-to-peer network, each host can provide network resources to other hosts or access resources located on other hosts, and each host is in charge of controlling access to those resources.

An *intranet* is a private network that uses internet technologies. Services on an intranet are only available to hosts that are connected to the private network. An *extranet* is a private network that uses internet technologies, but whose resources are made available to external (but trusted) users. For example, you might create a website on a private network that only users from a partner company can access.

[netpro18v5_all_questions_en.exm NP09_2-7 #MCS4]

Question 82: Correct

A router is connected to network 192.168.1.0/24 and network 192.168.2.0/24. The router is configured to use RIP and has learned of networks 192.168.3.0/24 and 192.168.4.0/24.

The next hop router for network 192.168.3.0 has changed. You need to make the change with the least amount of effort possible.

What should you do?

- ( ) Manually reconfigure the default route to point to the new next hop router.
- (•) Wait for convergence to take place.
- ( ) Force RIP to perform an immediate update.
- ( ) Stop and restart the RIP protocol on the router.

Explanation

When using a routing protocol, changes in routing information take some time to be propagated to all routers on the network. The term "convergence" is used to describe the condition when all routers have the same (or correct) routing information.

Static routes in the routing table must be updated manually. Restarting RIP might actually increase the time required for changes to be learned. Forcing an update (if the router supports it) is not a requirement, as the periodic sharing of routes will eventually update the routing table entry.
[netpro18v5_all_questions_en.exm NP09_1-6 #MCS7]

Question 83: Correct

You manage a network that uses switches. In the lobby of your building are three RJ45 ports connected to a switch.

You want to make sure that visitors cannot plug in their computers into the free network jacks and connect to the network, but you want employees who plug into those same jacks should be able to connect to the network.

What feature should you configure?

- VLANs
- Port authentication
- Bonding
- Spanning tree
- Mirroring

Explanation

Use port authentication to prevent unauthorized access through switch ports. Port authentication is provided by the 802.1x protocol and allows only authenticated devices to connect to the LAN through the switch. Authentication uses usernames and passwords, smart cards, or other authentication methods.

- When a device first connects, the port is set to an unauthorized state. Ports in unauthorized states can only be used for 802.1x authentication traffic.
- After the server authenticates the device or the user, the switch port is placed in an authorized state, and access to other LAN devices is allowed.

With a VLAN, you assign each port to a VLAN. If the ports in the lobby were assigned to one VLAN, you could control the type of access through the switch for those ports, but could not modify the access based on user. If you use a VLAN, both visitors and employees would have the same access through those ports.

Spanning tree is a protocol on a switch that allows the switch to maintain multiple paths between switches within a subnet. The spanning tree protocol runs on each switch and is used to select a single path between any two switches. Mirroring sends traffic from all switch ports to a switch port you designate as the mirrored port. Bonding allows multiple switch ports to be used at the same time to reach a specific destination.
[netpro18v5_all_questions_en.exm NP09_3-3 12]

Question 84: Correct

Which type of denial of service (DoS) attack occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses?

- ARP poisoning
- Spam
- DNS poisoning
- SYN flood

Explanation

DNS poisoning occurs when a name server receives malicious or misleading data that incorrectly maps host names and IP addresses. In a DNS poisoning attack:

- Incorrect DNS data is introduced into a primary DNS server.
- The incorrect mapping is made available to client applications through the resolver.
- Traffic is directed to incorrect sites.

ARP poisoning corrupts the ARP cache or sends incorrect ARP data that spoofs MAC addresses, causing devices to send frames to the wrong host or an unreachable host. Spam sent in such great amounts can consume bandwidth or fill a mailbox, leaving no room for legitimate traffic. The SYN flood exploits the TCP three-way handshake.
[netpro18v5_all_questions_en.exm SSCP-4 NEW [173]]

Question 85: Incorrect

Which of the following are valid IPv6 IP addresses? Select all that apply.

- [x] ~~165.15.78.53.100.1~~
- [x] ~~343F:1EEE:ACDD:2034:1FF3:5012~~
- [ ] 141:0:0:0:15:0:0:1
- [ ] 6384:1319:7700:7631:446A:5511:8940:2552
- [ ] 127.0.0.1
- [ ] 192.168.2.15

Explanation

An IPv6 IP address is a 128-bit address listed as eight 16-bit hexadecimal sections. Leading zeros can be omitted in each section. Therefore, 6384:1319:7700:7631:446A:5511:8940:2552 and 141:0:0:0:15:0:0:1 are both valid IPv6 IP addresses. A single set of all-zero sections can be abbreviated with two colons (::). Therefore, 141::15:0:0:1 is also a valid address.

127.0.0.1 and 192.168.2.15 are IPv4 IP address.

343F:1EEE:ACDD:2034:1FF3:5012 is a 48 bit MAC address.

[netpro18v5_all_questions_en.exm NP05_2-5 #77||/]

Question 86: Correct

Which of the following protocols or services would you associate with Window's Remote Desktop Services network traffic?

- (•) RDP
- ( ) NNTP
- ( ) WPA
- ( ) WTSP

Explanation

The Remote Desktop Protocol (RDP) is used by Window's Remote Desktop Services applications, including Remote Desktop Connection.

WTSP is not a recognized protocol used on networks. The network news transport protocol (NNTP) is used to access newsgroups and download messages. It is not associated with Windows Terminal Services. Wi-Fi Protected Access (WPA) is a security mechanism designed to provide protection on wireless networks. It is not associated with Windows Terminal Services.
[netpro18v5_all_questions_en.exm NP05_2-16 #84]

Question 87: Correct

Which of the following uses hacking techniques to proactively discover internal vulnerabilities?

- ( ) Reverse engineering
- ( ) Passive reconnaissance
- (•) Penetration testing
- ( ) Inbound scanning

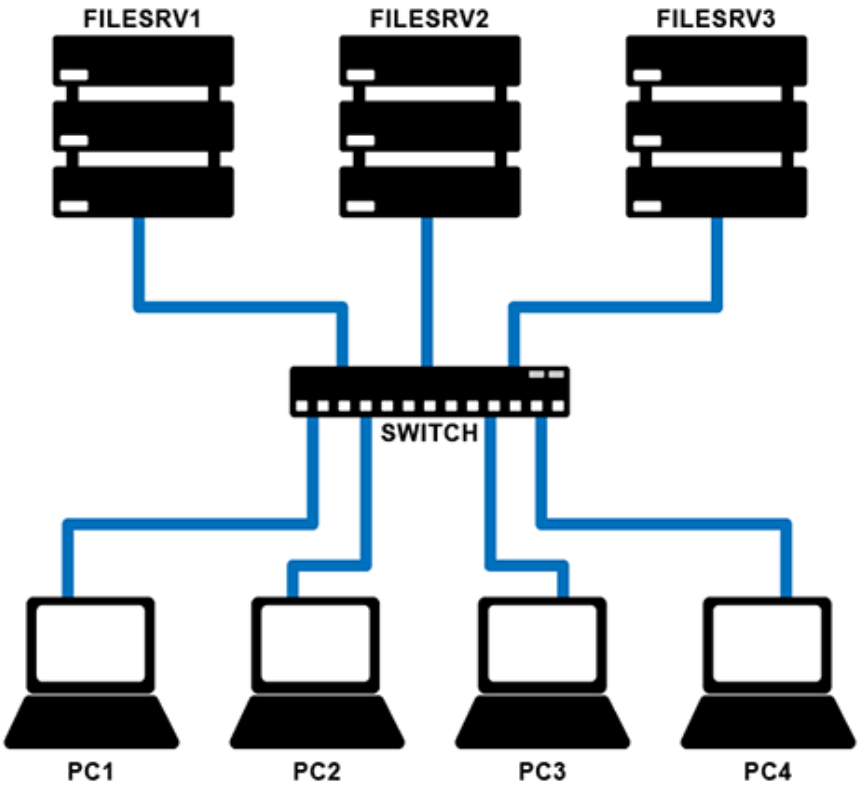
Explanation

Penetration testing is the practice of proactively testing systems and policies for vulnerabilities. This

approach seeks to identify vulnerabilities internally before a malicious individual can take advantage of them. Common techniques are identical to those used by hackers and include network/target enumeration and port scanning.
[netpro18v5_all_questions_en.exm CISSP-104 SP [23]]

Question 88: Correct

This question includes an image to help you answer the question. Close



You manage a network with three dedicated storage devices, as shown in the diagram. Users on the network see only a single file server.

Which network-based storage technology is being used?

- iSCSI SAN with clustering
- NAS
- Fibre channel SAN
- NAS with clustering

Explanation

NAS with clustering is being used. A NAS device is an appliance that is dedicated to file storage. With clustering, multiple NAS devices are grouped together to provide a degree of fault tolerance. To users on the network, the cluster appears as a single file server. Without clustering, the NAS devices would appear as three separate file servers.

Because client devices are connected directly to the switch, it cannot be an iSCSI or Fiber Channel SAN implementation. iSCSI and Fibre Channel SANs both use special switches to create the SAN fabric that client systems are not connected to directly.
[netpro18v5_all_questions_en.exm *NP15_NETWORK-BASED_STORAGE_04]

Question 89: Correct

Which component is most likely to allow physical and virtual machines to communicate with each other?

- Host operating system
- Virtual switch

- VHD
- Virtual desktop

Explanation

Virtual switches allow multiple virtual servers and/or desktops to communicate on virtual network segments and/or the physical network. Virtual switches are often configured in the hypervisor.

A virtual hard disk (VHD) is a file that is created within the host operating system and simulates a hard disk for the virtual machine. A physical machine (also known as the host operating system) has the actual hardware in place on the machine, such as the hard disk drive(s), optical drive, RAM, motherboard, etc. A virtual desktop is a virtual machine in a software implementation of a computer that executes programs like a physical machine.
[netpro18v5_all_questions_en.exm NP15_VIRTUAL_NETWORKING_02]

Question 90: Correct

All of the 802.11 standards for wireless networking support which type of communication path sharing technology?

- Token passing
- CSMA/CD
- CSMA/CA
- Polling

Explanation

802.11x standards for wireless networking all support the CSMA/CA (carrier sense multiple access with collision avoidance) type of communication path sharing technology. This CSMA/CA allows multiple baseband clients to share the same communication medium. CSMA/CA works as follows:

1. The system asks for permission to transmit.
2. A designated authority (such as a hub, router, or access point), grants access when the communication medium is free.
3. The system transmits data and waits for an ACK (acknowledgment).
4. If no ACK is received, the data is retransmitted.

Polling is a mechanism where one system is labeled as the primary system. The primary system polls each secondary system in turn to inquire whether they have data to transmit. Token passing is a mechanism that uses a digital pass card. Only the system holding the token is allowed to communicate. CSMA/CD is the technology used by Ethernet. CSMA/CD works as follows:

1. The system listens for traffic. If the line is clear, the system begins transmitting.
2. During the transmission, the system listens for collisions.
3. If no collisions are detected, the communication succeeds. If collisions are detected, an interrupt jam signal is broadcast to stop all transmissions. Each system waits a random amount of time before starting over at step 1.

[netpro18v5_all_questions_en.exm NP05_1-7 #39]