N10-006 comptia

http://www.gratisexam.com/

Sections
1. Network architecture
2. Network operations
3. Network security
4. Troubleshooting
5. Industry standards, practices, and network theory
6. Mix questions

Exam A

QUESTION 1
A technician needs to limit the amount of broadcast traffic on a network and allow different segments to communicate with each other. Which of the following options would satisfy these requirements?

A. Add a router and enable OSPF.

B. Add a layer 3 switch and create a VLAN.

C. Add a bridge between two switches.

D. Add a firewall and implement proper ACL.

Correct Answer: B
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

We can limit the amount of broadcast traffic on a switched network by dividing the computers into logical network segments called VLANs.
A virtual local area network (VLAN) is a logical group of computers that appear to be on the same LAN even if they are on separate IP subnets. These logical subnets are configured in the network switches. Each VLAN is a broadcast domain meaning that only computers within the same VLAN will receive broadcast traffic.

To allow different segments (VLAN) to communicate with each other, a router is required to establish a connection between the systems. We can use a network router to route between the VLANs or we can use a 'Layer 3' switch. Unlike layer 2 switches that can only read the contents of the data-link layer protocol header in the packets they process, layer 3 switches can read the (IP) addresses in the network layer protocol header as well.

QUESTION 2
The network install is failing redundancy testing at the MDF. The traffic being transported is a mixture of multicast and unicast signals. Which of the following would BEST handle the rerouting caused by the disruption of service?

A. Layer 3 switch

B. Proxy server

C. Layer 2 switch

D. Smart hub

Correct Answer: A
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

The question states that the traffic being transported is a mixture of multicast and unicast signals. There are three basic types of network transmissions: broadcasts, which are packets transmitted to every node on the network; unicasts, which are packets transmitted to just one node; and multicasts, which are packets transmitted to a group of nodes. Multicast is a layer 3 feature of IPv4 & IPv6. Therefore, we would need a layer 3 switch (or a router) to reroute the traffic. Unlike layer 2 switches that can only read the contents of the data-link layer protocol header in the packets they process, layer 3 switches can read the (IP) addresses in the network layer protocol header as well.

QUESTION 3
A technician needs to set aside addresses in a DHCP pool so that certain servers always receive the same address. Which of the following should be configured?

A. Leases

B. Helper addresses

C. Scopes

D. Reservations

Correct Answer: D
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

A reservation is used in DHCP to ensure that a computer always receives the same IP address. To create a reservation, you need to know the hardware MAC address of the network interface card that should receive the IP address.
For example, if Server1 has MAC address of 00:A1:FB:12:45:4C and that computer should always get 192.168.0.7 as its IP address, you can map the MAC address of Server1 with the IP address to configure reservation.

QUESTION 4
Joe, a network technician, is setting up a DHCP server on a LAN segment. Which of the following options should Joe configure in the DHCP scope, in order to allow hosts on that LAN segment using dynamic IP addresses, to be able to access the Internet and internal company servers? (Select THREE).

A. Default gateway

B. Subnet mask

C. Reservations

D. TFTP server

E. Lease expiration time of 1 day

F. DNS servers

G. Bootp

Correct Answer: ABF
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

The question states that the client computers need to access the Internet as well as internal company servers. To access the Internet, the client computers need to be configured with an IP address with a subnet mask (answer B) and the address of the router that connects the company network to the Internet. This is known as the 'default gateway' (answer A).
To be able to resolve web page URLs to web server IP addresses, the client computers need to be configured with the address of a DNS server (answer F).

QUESTION 5
A technician just completed a new external website and setup access rules in the firewall. After some testing, only users outside the internal network can reach the site. The website responds to a ping from the internal network and resolves the proper public address. Which of the following could the technician do to fix this issue while causing internal users to route to the website using an internal address?

A. Configure NAT on the firewall

B. Implement a split horizon DNS

C. Place the server in the DMZ

D. Adjust the proper internal ACL

Correct Answer: B
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

Split horizon DNS (also known as Split Brain DNS) is a mechanism for DNS servers to supply different DNS query results depending on the source of the request. This can be done by hardware-based separation but is most commonly done in software.
In this question, we want external users to be able to access the website by using a public IP address. To do this, we would have an external facing DNS server

hosting a DNS zone for the website domain. For the internal users, we would have an internal facing DNS server hosting a DNS zone for the website domain. The external DNS zone will resolve the website URL to an external public IP address. The internal DNS server will resolve the website URL to an internal private IP address.

QUESTION 6
When configuring a new server, a technician requests that an MX record be created in DNS for the new server, but the record was not entered properly. Which of the following was MOST likely installed that required an MX record to function properly?

A. Load balancer
B. FTP server
C. Firewall DMZ
D. Mail server

Correct Answer: D
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

A mail exchanger record (MX record) is a DNS record used by email servers to determine the name of the email server responsible for accepting email for the recipient's domain.
For example a user sends an email to recipient@somedomain.com. The sending user's email server will query the somedomain.com DNS zone for an MX record for the domain. The MX record will specify the hostname of the email server responsible for accepting email for the somedomain.com domain, for example, mailserver.somedomain.com. The sending email server will then perform a second DNS query to resolve mailserver.somedomain.com to an IP address. The sending mail server will then forward the email to the destination mail server.

QUESTION 7
Which of the following protocols uses label-switching routers and label-edge routers to forward traffic?

A. BGP
B. OSPF
C. IS-IS
D. MPLS

Correct Answer: D
Section: Network architecture
Explanation

Explanation/Reference:

Explanation:

In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself.

MPLS works by prefixing packets with an MPLS header, containing one or more labels.

An MPLS router that performs routing based only on the label is called a label switch router (LSR) or transit router. This is a type of router located in the middle of a MPLS network. It is responsible for switching the labels used to route packets. When an LSR receives a packet, it uses the label included in the packet header as an index to determine the next hop on the label-switched path (LSP) and a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is routed forward.

A label edge router (LER) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERs respectively, add an MPLS label onto an incoming packet and remove it off the outgoing packet.

When forwarding IP datagrams into the MPLS domain, an LER uses routing information to determine appropriate labels to be affixed, labels the packet accordingly, and then forwards the labelled packets into the MPLS domain. Likewise, upon receiving a labelled packet which is destined to exit the MPLS domain, the LER strips off the label and forwards the resulting IP packet using normal IP forwarding rules.

QUESTION 8
Which of the following is MOST likely to use an RJ-11 connector to connect a computer to an ISP using a POTS line?

A. Multilayer switch
B. Access point
C. Analog modem
D. DOCSIS modem

Correct Answer: C
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

Before ADSL broadband connections became the standard for Internet connections, computers used analog modems to connect to the Internet. By today's standards, analog modems are very slow typically offering a maximum bandwidth of 56Kbps.

An analog modem (modulator/demodulator) converts (modulates) a digital signal from a computer to an analog signal to be transmitted over a standard (POTS) phone line. The modem then converts (demodulates) the incoming analog signal to digital data to be used by the computer.

An analog modem uses an RJ-11 connector to connect to a phone line (POTS) in the same way a phone does.

QUESTION 9
An administrator notices an unused cable behind a cabinet that is terminated with a DB-9 connector. Which of the following protocols was MOST likely used on this cable?

A. RS-232

B. 802.3

C. ATM

D. Token ring

Correct Answer: A
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

A DB-9 connector is used on serial cables. Serial cables use the RS-232 protocol which defines the functions of the 9 pins in a DB-9 connector. The RS-232 standard was around long before computers. It's rare to see a new computer nowadays with a serial port but they were commonly used for connecting external analog modems, keyboards and mice to computers.

QUESTION 10
Which of the following connection types is used to terminate DS3 connections in a telecommunications facility?

A. 66 block

B. BNC

C. F-connector

D. RJ-11

Correct Answer: B
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

A DS3 (Digital Signal 3) is also known as a T3 line with a maximum bandwidth of 44.736 Mbit/s. DS3 uses 75 ohm coaxial cable and BNC connectors.

QUESTION 11
An F-connector is used on which of the following types of cabling?

A. CAT3

B. Single mode fiber

C. CAT5

D. RG6

Correct Answer: D
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

An F connector is a coaxial RF connector commonly used for terrestrial television, cable television and universally for satellite television and cable modems, usually with RG-6/U cable or, in older installations, with RG-59/U cable.

QUESTION 12
A network technician must utilize multimode fiber to uplink a new networking device. Which of the following Ethernet standards could the technician utilize? (Select TWO).

A. 1000Base-LR
B. 1000Base-SR
C. 1000Base-T
D. 10GBase-LR
E. 10GBase-SR
F. 10GBase-T

Correct Answer: BE
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

1000BASE-SX is a fiber optic Gigabit Ethernet standard for operation over multi-mode fiber with a distance capability between 220 meters and 550 meters.
10Gbase-SR is a 10 Gigabit Ethernet LAN standard for operation over multi-mode fiber optic cable and short wavelength signaling.

QUESTION 13

CORRECT TEXT
SIMULATION
You have been tasked with testing a CAT5e cable. A summary of the test results can be found on the screen.
Step 1: Select the tool that was used to create the cable test results.
Step 2: Interpret the test results and select the option that explains the results. After you are done with your analysis, click the 'Submit Cable Test Analysis' button.

Cable Test

Step 1: Select the tool that was used to create the cable test results.

Cable Test Result		
1, 2	Open	7ft
3, 6	Short	7ft
4, 5	Open	7ft
7, 8	Open	7ft

Tool Choices
- [ ] Crimper
- [ ] Cable Certifier
- [ ] Multimeter
- [ ] Punch Down Tool
- [ ] Protocol Analyzer
- [ ] OTDR
- [ ] Toner Probe

Correct Answer: Here is the solution below
Section: Network architecture

Explanation

Explanation/Reference:
Explanation:

A Cable Certifier provides "Pass" or "Fail" information in accordance with industry standards but can also show detailed information when a "Fail" occurs. This includes shorts, the wire pairs involved and the distance to the short. When a short is identified, at the full length of the cable it means the cable has not been crimped correctly.

QUESTION 14
A network engineer needs to set up a topology that will not fail if there is an outage on a single piece of the topology. However, the computers need to wait to talk on the network to avoid congestions. Which of the following topologies would the engineer implement?

A. Star
B. Bus
C. Ring
D. Mesh

Correct Answer: C
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

Token Ring networks are quite rare today. Token Ring networks use the ring topology. Despite being called a Ring topology, the ring is logical and the physical network structure often forms a 'star' topology with all computers on the network connecting to a central multistation access unit (MAU). The MAU implements the logical ring by transmitting signals to each node in turn and waiting for the node to send them back before it transmits to the next node. Therefore, although the cables are physically connected in a star, the data path takes the form of a ring. If any computer or network cable fails in a token ring network, the remainder of the network remains functional. The MAU has the intelligence to isolate the failed segment.
To ensure that the computers need to wait to talk on the network to avoid congestions, a Token Ring network uses a 'token'. The token continually passes around the network until a computer needs to send data. The computer then takes the token and transmits the data before releasing the token. Only a computer in possession of the token can transmit data onto the network.

QUESTION 15
A network topology that utilizes a central device with point-to-point connections to all other devices is which of the following?

A. Star
B. Ring
C. Mesh
D. Bus

Correct Answer: A
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

A Star network is the most common network in use today. Ethernet networks with computers connected to a switch (or a less commonly a hub) form a star network. The switch forms the central component of the star. All network devices connect to the switch. A network switch has a MAC address table which it populates with the MAC address of every device connected to the switch. When the switch receives data on one of its ports from a computer, it looks in the MAC address table to discover which port the destination computer is connected to. The switch then unicasts the data out through the port that the destination computer is connected to.

QUESTION 16
Which of the following network topologies has a central, single point of failure?

A. Ring
B. Star
C. Hybrid
D. Mesh

Correct Answer: B
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

A Star network is the most common network in use today. Ethernet networks with computers connected to a switch (or a less commonly a hub) form a star network. The switch forms the central component of the star. All network devices connect to the switch. A network switch has a MAC address table which it populates with the MAC address of every device connected to the switch. When the switch receives data on one of its ports from a computer, it looks in the MAC address table to discover which port the destination computer is connected to. The switch then unicasts the data out through the port that the destination computer is connected to. The switch that forms the central component of a star network is a single point of failure. If the switch fails, no computers will be able to communicate with each other.

QUESTION 17
Which of the following refers to a network that spans several buildings that are within walking distance of each other?

A. CAN
B. WAN
C. PAN
D. MAN

Correct Answer: A
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

CAN stands for Campus Area Network or Corporate Area Network. Universities or colleges often implement CANs to link the buildings in a network. The range of CAN is 1KM to 5KM. If multiple buildings have the same domain and they are connected with a network, then it will be considered as a CAN.

QUESTION 18
Which of the following network infrastructure implementations would be used to support files being transferred between Bluetooth-enabled smartphones?

A. PAN
B. LAN
C. WLAN
D. MAN

Correct Answer: A
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

PAN stands for Personal Area Network. It is a network of devices in the area of a person typically within a range of 10 meters and commonly using a wireless technology such as Bluetooth or IR (Infra-Red).

QUESTION 19
Which of the following describes an IPv6 address of ::1?

A. Broadcast
B. Loopback
C. Classless
D. Multicast

Correct Answer: B
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

The loopback address is a special IP address that is designated for the software loopback interface of a computer. The loopback interface has no hardware

associated with it, and it is not physically connected to a network. The loopback address causes any messages sent to it to be returned to the sending system. The loopback address allows client software to communicate with server software on the same computer. Users specify the loopback address which will point back to the computer's TCP/IP network configuration.
In IPv4, the loopback address is 127.0.0.1.
In IPv6, the loopback address is 0:0:0:0:0:0:0:1, which can be shortened to ::1

QUESTION 20
Which of the following is an example of an IPv4 address?

A. 192:168:1:55

B. 192.168.1.254

C. 00:AB:FA:B1:07:34

D. ::1

Correct Answer: B
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

An IPv4 address is notated as four decimal numbers each between 0 and 255 separated by dots (xxx.xxx.xxx.xxx). Each number is known as an octet as it represents eight binary bits. All four octets make up a 32-bit binary IPv4 address.
In this question, 192.168.1.254 is a valid IPv4 address.

QUESTION 21
A technician, Joe, needs to troubleshoot a recently installed NIC. He decides to ping the local loopback address. Which of the following is a valid IPv4 loopback address?

A. 10.0.0.1

B. 127.0.0.1

C. 172.16.1.1

D. 192.168.1.1

Correct Answer: B
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

The loopback address is a special IP address that is designated for the software loopback interface of a computer. The loopback interface has no hardware associated with it, and it is not physically connected to a network. The loopback address causes any messages sent to it to be returned to the sending system. The loopback address allows client software to communicate with server software on the same computer. Users specify the loopback address which will point back to the computer's TCP/IP network configuration.
In IPv4, the loopback address is 127.0.0.1.
In IPv6, the loopback address is 0:0:0:0:0:0:0:1, more commonly notated as follows. ::1

QUESTION 22
A technician, Joe, has been tasked with assigning two IP addresses to WAN interfaces on connected routers. In order to conserve address space, which of the following subnet masks should Joe use for this subnet?

A. /24
B. /32
C. /28
D. /29
E. /30

Correct Answer: E
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

An IPv4 address consists of 32 bits. The first x number of bits in the address is the network address and the remaining bits are used for the host addresses. The subnet mask defines how many bits form the network address and from that, we can calculate how many bits are used for the host addresses.
In this question, the /30 subnet mask dictates that the first 30 bits of the IP address are used for network addressing and the remaining 2 bits are used for host addressing. The formula to calculate the number of hosts in a subnet is 2n - 2. The "n" in the host's formula represents the number of bits used for host addressing. If we apply the formula (22 – 2), a /30 subnet mask will provide 2 IP addresses.

QUESTION 23
HOTSPOT
Corporate headquarters provided your office a portion of their class B subnet to use at a new office location. Allocate the minimum number of addresses (using CIDR notation) needed to accommodate each department.

Range Given: 172.30.232.0/24

- Sales   57 devices
- HR   23 devices
- IT   12 devices
- Finance   32 devices
- Marketing   9 devices

After accommodating each department, identify the unused portion of the subnet by responding to the question on the graphic. All drop downs must be filled.
Instructions: When the simulation is complete, please select the Done button to submit.

All Networks have the range from /0 to/32

Hot Area:

CIDR Notation

Instructions: When the simulation is complete, please select the Done button to submit.

Sales Network [dropdown]

/0 /1 /2 /3 /4 /5 /6 /7 /8 /9 /10 /11 /12 /13 /14 /15 /16 /17 /18 /19 /20 /21 /22 /23 /24 /25 /26 /27 /28 /29 /30 /31 /32

HR Network [dropdown]

/0 /1 /2 /3 /4 /5 /6 /7 /8 /9 /10 /11 /12 /13 /14 /15 /16 /17 /18 /19 /20 /21 /22 /23 /24 /25 /26 /27 /28 /29 /30 /31 /32

Layer 3 Switch

Finance Network [dropdown]

/0 /1 /2 /3 /4 /5 /6 /7 /8 /9 /10 /11 /12 /13 /14 /15 /16 /17 /18 /19 /20 /21 /22 /23 /24 /25 /26 /27 /28 /29 /30 /31 /32

Marketing Network [dropdown]

/0 /1 /2 /3 /4 /5 /6 /7 /8 /9 /10 /11 /12 /13 /14 /15 /16 /17 /18 /19 /20 /21 /22 /23 /24 /25 /26 /27 /28 /29 /30 /31 /32

IT Network [dropdown]

/0 /1 /2 /3 /4 /5 /6 /7 /8 /9 /10 /11 /12 /13 /14 /15 /16 /17 /18 /19 /20 /21 /22 /23 /24 /25 /26 /27 /28 /29 /30 /31 /32

Which of the following would represent the LARGEST possible contiguous block of remaining addresses? [dropdown]

/0 /1 /2 /3 /4 /5 /6 /7 /8 /9 /10 /11 /12 /13 /14 /15 /16 /17 /18 /19 /20 /21 /22 /23 /24 /25 /26 /27 /28 /29 /30 /31 /32

http://www.gratisexam.com/

Correct Answer:

CIDR Notation

Instructions: When the simulation is complete, please select the Done button to submit.
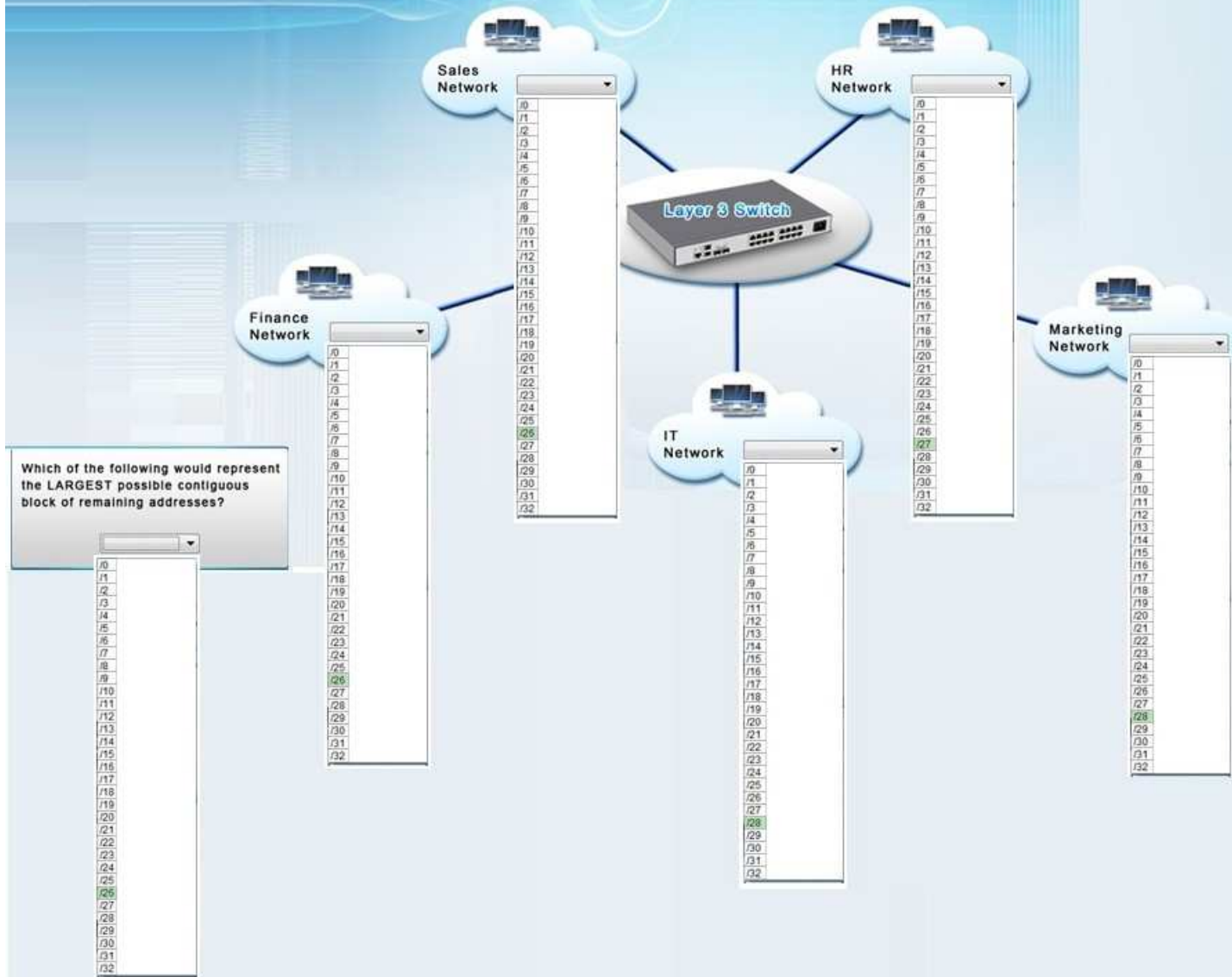
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

An IPv4 address consists of 32 bits. The first x number of bits in the address is the network address and the remaining bits are used for the host addresses. The subnet mask defines how many bits form the network address and from that, we can calculate how many bits are used for the host addresses.
The formula to calculate the number of hosts in a subnet is 2n - 2. The "n" in the host's formula represents the number of bits used for host addressing. If we apply the formula (22 – 2), we can determine that the following subnets should be configured:

Sales network – /26 – This will provide up to 62 usable IP addresses (64-2 for subnet and broadcast IP)
HR network - /27 – This will provide for up to 30 usable IP's (32-2)
IT - /28 – This will provide for up to 14 usable IP's (16-2)
Finance - /26 – Note that a /27 is 32 IP addresses but 2 of those are reserved for the network and broadcast IP's and can't be used for hosts.
Marketing - /28
If we add up how many IP blocks are used that is 64+32+16+64+16=192.
A /24 contains 256 IP addresses, so 256-192=64.
So the last unused box should be a /26, which equates to 64 addresses

QUESTION 24
A host has been assigned the address 169.254.0.1. This is an example of which of the following address types?

A. APIPA
B. MAC
C. Static
D. Public

Correct Answer: A
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

APIPA stands for Automatic Private IP Addressing and is a feature of Windows operating systems. When a client computer is configured to use automatic addressing (DHCP), APIPA assigns a class B IP address from 169.254.0.0 to 169.254.255.255 to the client when a DHCP server is unavailable.
When a client computer configured to use DHCP boots up, it first looks for a DHCP server to provide the client with IP address and subnet mask. If the client is unable to contact a DHCP server, it uses APIPA to automatically configure itself with an IP address from a range that has been reserved especially for Microsoft. The client also configures itself with a default class B subnet mask of 255.255.0.0. The client will use the self-configured IP address until a DHCP server becomes available.

QUESTION 25
A company wants to create highly available datacenters. Which of the following will allow the company to continue to maintain an Internet presence at all sites in the event that a WAN circuit at one site goes down?

A. Load balancer
B. VRRP
C. OSPF
D. BGP

Correct Answer: D
Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

A collection of networks that fall within the same administrative domain is called an autonomous system (AS). In this question, each datacenter will be an autonomous system.
The routers within an AS use an interior gateway protocol, such as the Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) protocol, to exchange routing information among themselves. At the edges of an AS are routers that communicate with the other AS's on the Internet, using an exterior gateway protocol such as the Border Gateway Protocol (BGP).
If a WAN link goes down, BGP will route data through another WAN link if redundant WAN links are available.

QUESTION 26
A technician is connecting a NAS device to an Ethernet network. Which of the following technologies will be used to encapsulate the frames?

A. HTTPS
B. Fibre channel
C. iSCSI
D. MS-CHAP

Correct Answer: C

Section: Network architecture
Explanation

Explanation/Reference:
Explanation:

A NAS or a SAN will use either iSCSI or Fiber Channel. In this question, the NAS is connected to an Ethernet network. Therefore, iSCSI will most likely be used (Fiber Channel over Ethernet (FCoE) can be used but is less common). ISCSI means Internet SCSI. ISCSI uses TCP (Transmission Control Protocol) which enables it to be used over TCP/IP networks such as Ethernet.
For Fiber channel, a separate Fiber Channel network would be required unless FCoE is used.

QUESTION 27
Company policies require that all network infrastructure devices send system level information to a centralized server. Which of the following should be implemented to ensure the network administrator can review device error information from one central location?

A. TACACS+ server
B. Single sign-on
C. SYSLOG server
D. Wi-Fi analyzer

Correct Answer: C
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

Syslog is a protocol designed to send log entries generated by a device or process called a facility across an IP network to a message collector, called a syslog server. A syslog message consists of an error code and the severity of the error. A syslog server would enable the network administrator to view device error information from a central location.

QUESTION 28
After a recent breach, the security technician decides the company needs to analyze and aggregate its security logs. Which of the following systems should be used?

A. Event log
B. Syslog
C. SIEM
D. SNMP

Correct Answer: C
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

Using a Security information and event management (SIEM) product, the security logs can be analyzed and aggregated.
SIEM is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM is sold as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes.
SIEM capabilities include Data aggregation; Log management aggregates data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events.

QUESTION 29
A technician would like to track the improvement of the network infrastructure after upgrades. Which of the following should the technician implement to have an accurate comparison?

A. Regression test
B. Speed test
C. Baseline
D. Statement of work

Correct Answer: C
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

In networking, baseline can refer to the standard level of performance of a certain device or to the normal operating capacity for your whole network. High-quality documentation should include a baseline for network performance, because you and your client need to know what "normal" looks like in order to detect problems before they develop into disasters.
A network baseline delimits the amount of available bandwidth available and when. For networks and networked devices, baselines include information about four key components:
Processor
Memory
Hard-disk (or other storage) subsystem
Network adapter or subsystem

QUESTION 30

It has been determined by network operations that there is a severe bottleneck on the company's mesh topology network. The field technician has chosen to use log management and found that one router is making routing decisions slower than others on the network. This is an example of which of the following?

A. Network device power issues
B. Network device CPU issues
C. Storage area network issues
D. Delayed responses from RADIUS

Correct Answer: B
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

Network processors (CPUs) are used in the manufacture of many different types of network equipment such as routers. Such a CPU on a router could become bottleneck for the network traffic. The routing through that device would then slow down.

QUESTION 31
A network technician receives the following alert from a network device:

"High utilizations threshold exceeded on gi1/0/24 : current value 9413587.54"

Which of the following is being monitored to trigger the alarm?

A. Speed and duplex mismatch
B. Wireless channel utilization
C. Network device CPU
D. Network device memory
E. Interface link status

Correct Answer: E
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

This is an error message that indicates that threshold of high utilization of network interface, in this case interface gi1/0/24, has been exceeded. The message has been triggered on the interface link status.

Note: gi1/0 would be a gigabyte interface.

QUESTION 32
The administrator's network has OSPF for the internal routing protocol. One port going out to the Internet is congested. The data is going out to the Internet, but queues up before sending. Which of the following would resolve this issue?

Output:
Fast Ethernet 0 is up, line protocol is up
Int ip address is 10.20.130.5/25
MTU 1500 bytes, BW10000 kbit, DLY 100 usec
Reliability 255/255, Tx load 1/255, Rx load 1/255
Encapsulation ospf, loopback not set
Keep alive 10
Half duplex, 100Mb/s, 100 Base Tx/Fx
Received 1052993 broadcasts
0 input errors
983881 packets output, 768588 bytes
0 output errors, 0 collisions, 0 resets

A. Set the loopback address
B. Change the IP address
C. Change the slash notation
D. Change duplex to full

Correct Answer: D
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

From the output we see that the half-duplex is configured. This would not use the full capacity of ports on the network. By changing to full duplex the throughput would be doubled.
Note: All communications are either half-duplex or full-duplex. During half-duplex communication, a device can either send communication or receive communication, but not both at the same time. In full-duplex communication, both devices can send and receive communication at the same time. This means that the effective throughput is doubled and communication is much more efficient.

QUESTION 33
The RAID controller on a server failed and was replaced with a different brand. Which of the following will be needed after the server has been rebuilt and joined to the domain?

A. Vendor documentation

B. Recent backups

C. Physical IP address

D. Physical network diagram

Correct Answer: B
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

If the RAID controller fails and is replaced with a RAID controller with a different brand the RAID will break. We would have to rebuild a new RAID disk, access and restore the most recent backup to the new RAID disk.
Note: RAID controller is a hardware device or software program used to manage hard disk drives (HDDs) or solid-state drives (SSDs) in a computer or storage array so they work as a logical unit. In hardware-based RAID, a physical controller is used to manage the RAID array.

QUESTION 34
An administrator reassigns a laptop to a different user in the company. Upon delivering the laptop to the new user, the administrator documents the new location, the user of the device and when the device was reassigned. Which of the following BEST describes these actions?

A. Network map

B. Asset management

C. Change management

D. Baselines

Correct Answer: B
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

Documenting the location, the user of the device and the date of the reassignment would be part of the asset management.
The best way to keep track of your computers and their configurations is to document them yourself. Large enterprise networks typically assign their own identification numbers to their computers and other hardware purchases as part of an asset management process that controls the entire life cycle of each device, from recognition of a need to retirement or disposal.

QUESTION 35
A network technician is diligent about maintaining all system servers' at the most current service pack level available. After performing upgrades, users experience

issues with server-based applications. Which of the following should be used to prevent issues in the future?

A. Configure an automated patching server
B. Virtualize the servers and take daily snapshots
C. Configure a honeypot for application testing
D. Configure a test lab for updates

Correct Answer: D
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

To prevent the service pack issues make sure, before going ahead and applying a new Service Pack in your production environment, to validate them in a test/lab environment first.

QUESTION 36
A system administrator has been tasked to ensure that the software team is not affecting the production software when developing enhancements. The software that is being updated is on a very short SDLC and enhancements must be developed rapidly. These enhancements must be approved before being deployed. Which of the following will mitigate production outages before the enhancements are deployed?

A. Implement an environment to test the enhancements.
B. Implement ACLs that only allow management access to the enhancements.
C. Deploy an IPS on the production network.
D. Move the software team's workstations to the DMZ.

Correct Answer: A
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

Environments are controlled areas where systems developers can build, distribute, install, configure, test, and execute systems that move through the Software Development Life Cycle (SDLC). The enhancements can be deployed and tested in a test environment before they are installed in the production environment.

QUESTION 37
A system administrator wants to update a web-based application to the latest version. Which of the following procedures should the system administrator perform FIRST?

A. Remove all user accounts on the server
B. Isolate the server logically on the network
C. Block all HTTP traffic to the server
D. Install the software in a test environment

Correct Answer: D
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

We should test the new version of the application in a test/lab environment first. This way any potential issues with the new software would not affect the production environment.
Set up a test lab on an isolated network in your organization. Do not set up your test lab in your production environment.

QUESTION 38
Network segmentation provides which of the following benefits?

A. Security through isolation
B. Link aggregation
C. Packet flooding through all ports
D. High availability through redundancy

Correct Answer: A
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

Network segmentation in computer networking is the act or profession of splitting a computer network into subnetworks, each being a network segment. Advantages

of such splitting are primarily for boosting performance and improving security through isolation.
Advantages of network segmentation:
Improved security: Broadcasts will be contained to local network. Internal network structure will not be visible from outside
Reduced congestion: Improved performance is achieved because on a segmented network there are fewer hosts per subnetwork, thus minimizing local traffic
Containing network problems: Limiting the effect of local failures on other parts of network

QUESTION 39
After a company rolls out software updates, Ann, a lab researcher, is no longer able to use lab equipment connected to her PC. The technician contacts the vendor and determines there is an incompatibility with the latest IO drivers. Which of the following should the technician perform so that Ann can get back to work as quickly as possible?

A. Reformat and install the compatible drivers.

B. Reset Ann's equipment configuration from a backup.

C. Downgrade the PC to a working patch level.

D. Restore Ann's PC to the last known good configuration.

E. Roll back the drivers to the previous version.

Correct Answer: E
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

By rolling back the drivers Ann would be able to use her lab equipment again.
To roll back a driver in Windows means to return the driver to the version that was last installed for the device. Rolling back a driver is an easy way to return a driver to a working version when a driver update fails to fix a problem or maybe even causes a new problem. Think of rolling back a driver as a quick and easy way to uninstall the latest driver and then reinstall the previous one, all automatically.

QUESTION 40
Which of the following requires the network administrator to schedule a maintenance window?

A. When a company-wide email notification must be sent.

B. A minor release upgrade of a production router.

C. When the network administrator's laptop must be rebooted.

D. A major release upgrade of a core switch in a test lab.

Correct Answer: B
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

During an update of a production router the router would not be able to route packages and the network traffic would be affected. It would be necessary to announce a maintenance window.
In information technology and systems management, a maintenance window is a period of time designated in advance by the technical staff, during which preventive maintenance that could cause disruption of service may be performed.

QUESTION 41
A company has implemented the capability to send all log files to a central location by utilizing an encrypted channel. The log files are sent to this location in order to be reviewed. A recent exploit has caused the company's encryption to become unsecure. Which of the following would be required to resolve the exploit?

A. Utilize a FTP service

B. Install recommended updates

C. Send all log files through SMTP

D. Configure the firewall to block port 22

Correct Answer: B
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

If the encryption is unsecure then we must look for encryption software updates or patches. If they are available we must install them.
As vulnerabilities are discovered, the vendors of the operating systems or applications often respond by releasing a patch. A patch is designed to correct a known bug or fix a known vulnerability in a piece of software.
A patch differs from an update, which, in addition to fixing a known bug or vulnerability, adds one or more features to the software being updated.

QUESTION 42
An outside organization has completed a penetration test for a company. One of the items on the report is reflecting the ability to read SSL traffic from the web server. Which of the following is the MOST likely mitigation for this reported item?

A. Ensure patches are deployed

B. Install an IDS on the network

C. Configure the firewall to block traffic on port 443

D. Implement a VPN for employees

Correct Answer: A

Section: Network operations
Explanation

Explanation/Reference:
Explanation:

As vulnerabilities are discovered, the vendors of the operating systems or applications often respond by releasing a patch. A patch is designed to correct a known bug or fix a known vulnerability, such as in this case to be able to read SSL traffic, in a piece of software.
A patch differs from an update, which, in addition to fixing a known bug or vulnerability, adds one or more features to the software being updated.

QUESTION 43
A company has had several virus infections over the past few months. The infections were caused by vulnerabilities in the application versions that are being used. Which of the following should an administrator implement to prevent future outbreaks?

A. Host-based intrusion detection systems
B. Acceptable use policies
C. Incident response team
D. Patch management

Correct Answer: D
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

As vulnerabilities are discovered, the vendors of the operating systems or applications often respond by releasing a patch. A patch is designed to correct a known bug or fix a known vulnerability, such as in this case to be vulnerable to virus infections, in a piece of software.
A patch differs from an update, which, in addition to fixing a known bug or vulnerability, adds one or more features to the software being updated.

QUESTION 44
Which of the following protocols must be implemented in order for two switches to share VLAN information?

A. VTP
B. MPLS
C. STP
D. PPTP

Correct Answer: A
Section: Network operations

Explanation

Explanation/Reference:
Explanation:

The VLAN Trunking Protocol (VTP) allows a VLAN created on one switch to be propagated to other switches in a group of switches (that is, a VTP domain).

QUESTION 45
A technician is setting up a new network and wants to create redundant paths through the network. Which of the following should be implemented to prevent performance degradation?

A. Port mirroring
B. Spanning tree
C. ARP inspection
D. VLAN

Correct Answer: B
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

QUESTION 46
A training class is being held in an auditorium. Hard-wired connections are required for all laptops that will be used. The network technician must add a switch to the room through which the laptops will connect for full network access. Which of the following must the technician configure on a switch port, for both switches, in order to create this setup?

A. DHCP
B. Split horizon
C. CIDR
D. TRUNK

Correct Answer: D
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

We should use trunk ports to set up a VLAN for the laptops that will be used in the auditorium.
A trunk port is a port that is assigned to carry traffic for all the VLANs that are accessible by a specific switch, a process known as trunking. Trunk ports mark frames with unique identifying tags – either 802.1Q tags or Interswitch Link (ISL) tags – as they move between switches. Therefore, every single frame can be directed to its designated VLAN.

QUESTION 47
A desktop computer is connected to the network and receives an APIPA address but is unable to reach the VLAN gateway of 10.10.100.254. Other PCs in the VLAN subnet are able to reach the Internet. Which of the following is MOST likely the source of the problem?

A. 802.1q is not configured on the switch port

B. APIPA has been misconfigured on the VLAN

C. Bad SFP in the PC's 10/100 NIC

D. OS updates have not been installed

Correct Answer: A
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

APIPA addresses are self-configured and are used when the client is unable to get proper IP configuration from a DHCP server. One possible source of this problem is that switch port, to which the computer is connected, is misconfigured. The 802.1q protocol is used to configure VLAN trunking on switch ports.

QUESTION 48
Which of the following communication technologies would MOST likely be used to increase bandwidth over an existing fiber optic network by combining multiple signals at different wavelengths?

A. DWDM

B. SONET

C. ADSL

D. LACP

Correct Answer: A
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

Dense wavelength-division multiplexing (DWDM) is a high-speed optical network type commonly used in MANs (metropolitan area networks). DWDM uses as many as 32 light wavelengths on a single fiber, where each wavelength can support as many as 160 simultaneous transmissions using more than eight active wavelengths per fiber.

QUESTION 49
When two or more links need to pass traffic as if they were one physical link, which of the following would be used to satisfy the requirement?

A. Port mirroring

B. 802.1w

C. LACP

D. VTP

Correct Answer: C
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

The Link Aggregation Control Protocol (LACP) enables you to assign multiple physical links to a logical interface, which appears as a single link to a route processor.

QUESTION 50
A technician is configuring a managed switch and needs to enable 802.3af. Which of the following should the technician enable?

A. PoE

B. Port bonding

C. VLAN

D. Trunking

Correct Answer: A
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

Power over Ethernet (PoE) is defined by the IEEE 802.3af and 802.3at standards.
PoE allows an Ethernet switch to provide power to an attached device (for example, a wireless access point, security camera, or IP phone) by applying power to the same wires in a UTP cable that are used to transmit and receive data.

QUESTION 51
A technician has finished configuring AAA on a new network device. However, the technician is unable to log into the device with LDAP credentials but is able to do so with a local user account. Which of the following is the MOST likely reason for the problem?

A. Username is misspelled is the device configuration file
B. IDS is blocking RADIUS
C. Shared secret key is mismatched
D. Group policy has not propagated to the device

Correct Answer: C
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

AAA through RADIUS uses a Server Secret Key (a shared secret key). A secret key mismatch could cause login problems.
Authentication, authorization, and accounting (AAA) allows a network to have a single repository of user credentials. A network administrator can then, for example, supply the same credentials to log in to various network devices (for example, routers and switches). RADIUS and TACACS+ are protocols commonly used to communicate with an AAA server.

QUESTION 52
Multiple students within a networking lab are required to simultaneously access a single switch remotely. The administrator checks and confirms that the switch can be accessed using the console, but currently only one student can log in at a time. Which of the following should be done to correct this issue?

A. Increase installed memory and install a larger flash module.
B. Increase the number of VLANs configured on the switch.
C. Decrease the number of VLANs configured on the switch.
D. Increase the number of virtual terminals available.

Correct Answer: D
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

You can set a limit of how many virtual terminals that can simultaneously be connected to a switch. Here the limit is set to one, and we should increase it.
For a Cisco network device:
You can use virtual terminal lines to connect to your Cisco NX-OS device, for example a switch. Secure Shell (SSH) and Telnet create virtual terminal sessions. You can configure an inactive session timeout and a maximum sessions limit for virtual terminals.
session-limit sessions
Example:
switch(config-line)# session-limit 10
Configures the maximum number of virtual sessions for the Cisco NX-OS device. The range is from 1 to 64.

QUESTION 53
A company is experiencing very slow network speeds of 54Mbps. A technician has been hired to perform an assessment on the existing wireless network. The technician has recommended an 802.11n network infrastructure. Which of the following allows 802.11n to reach higher speeds?

A. MU-MIMO
B. LWAPP
C. PoE
D. MIMO

Correct Answer: D
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

One way 802.11n achieves superior throughput is through the use of a technology called multiple input, multiple output (MIMO). MIMO uses multiple antennas for transmission and reception.

QUESTION 54
A network technician must create a wireless link between two buildings in an office park utilizing the 802.11ac standard. The antenna chosen must have a small physical footprint and minimal weight as it will be mounted on the outside of the building. Which of the following antenna types is BEST suited for this solution?

A. Yagi

B. Omni-directional

C. Parabolic

D. Patch

Correct Answer: D
Section: Network operations
Explanation

Explanation/Reference:
Explanation:

A patch antenna is a type of radio antenna with a low profile, which can be mounted on a flat surface. A patch antenna is typically mounted to a wall or a mast and provides coverage in a limited angle pattern.

QUESTION 55
An attacker has connected to an unused VoIP phone port to gain unauthorized access to a network. This is an example of which of the following attacks?

A. Smurf attack

B. VLAN hopping

C. Bluesnarfing

D. Spear phishing

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:

The VoIP phone port can be used to attack a VLAN on the local network.
VLAN hopping is a computer security exploit, a method of attacking networked resources on a Virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible.

QUESTION 56
Packet analysis reveals multiple GET and POST requests from an internal host to a URL without any response from the server. Which of the following is the BEST explanation that describes this scenario?

A. Compromised system

B. Smurf attack

C. SQL injection attack

D. Man-in-the-middle

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:

As the extra unexplainable traffic comes from an internal host on your network we can assume that this host has been compromised.
If your system has been compromised, somebody is probably using your machine--possibly to scan and find other machines to compromise

QUESTION 57
A technician needs to ensure that new systems are protected from electronic snooping of Radio Frequency emanations. Which of the following standards should be consulted?

A. DWDM
B. MIMO
C. TEMPEST
D. DOCSIS

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:

Tempest was the name of a government project to study the ability to understand the data over a network by listening to the emanations. Tempest rooms are designed to keep emanations contained in that room to increase security of data communications happening there.

QUESTION 58
A company has decided to update their usage policy to allow employees to surf the web unrestricted from their work computers. Which of the following actions should the IT security team implement to help protect the network from attack as a result of this new policy?

A. Install host-based anti-malware software
B. Implement MAC filtering on all wireless access points
C. Add an implicit deny to the core router ACL
D. Block port 80 outbound on the company firewall
E. Require users to utilize two-factor authentication

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:

To protect the computers from employees installing malicious software they download on the internet, antimalware should be run on all systems.
After a single machine in a company is compromised and is running malicious software (malware), the attacker can then use that single computer to proceed further into the internal network using the compromised host as a pivot point. The malware may have been implemented by an outside attacker or by an inside disgruntled employee.

QUESTION 59
Which of the following would be the result of a user physically unplugging a VoIP phone and connecting it into another interface with switch port security enabled as the default setting?

A. The VoIP phone would request a new phone number from the unified communications server.
B. The VoIP phone would cause the switch interface, that the user plugged into, to shutdown.
C. The VoIP phone would be able to receive incoming calls but will not be able to make outgoing calls.
D. The VoIP phone would request a different configuration from the unified communications server.

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:

Without configuring any other specific parameters, the switchport security feature will only permit one MAC address to be learned per switchport (dynamically) and use the shutdown violation mode; this means that if a second MAC address is seen on the switchport the port will be shutdown and put into the err-disabled state.

QUESTION 60
A network technician has been tasked to configure a new network monitoring tool that will examine interface settings throughout various network devices. Which of the following would need to be configured on each network device to provide that information in a secure manner?

A. S/MIME
B. SYSLOG
C. PGP
D. SNMPv3
E. RSH

Correct Answer: D
Section: Network security
Explanation

Explanation/Reference:
Explanation:

The network monitoring need to use a network management protocol. SNMP has become the de facto standard of network management protocols. The security weaknesses of SNMPv1 and SNMPv2c are addressed in SNMPv3.

QUESTION 61
A technician wants to securely manage several remote network devices. Which of the following should be implemented to securely manage the devices?

A. WPA2
B. IPv6
C. SNMPv3
D. RIPv2

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:

To manage the remote network devices we need to use a network management protocol. SNMP has become the de facto standard of network management protocols. The security weaknesses of SNMPv1 and SNMPv2c are addressed in SNMPv3.

QUESTION 62
A technician needs to secure web traffic for a new e-commerce website. Which of the following will secure traffic between a web browser and a website?

A. SSL

B. DNSSEC
C. WPA2
D. MTU

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:

Secure Sockets Layer (SSL) provides cryptography and reliability for upper layers (Layers 5–7) of the OSI model. SSL (and TLS) provide secure web browsing (web traffic) via Hypertext Transfer Protocol Secure (HTTPS).

QUESTION 63
A company has seen an increase in ransomware across the enterprise. Which of the following should be implemented to reduce the occurrences?

A. ARP inspection
B. Intrusion detection system
C. Web content filtering
D. Port filtering

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:

Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.
The best way to avoid ransomware include proactive measures like the following:
Don't click on any URL or open an attachment you are not expecting.
Implement an email content filtering service
Install a web content filtering service
Invest in leading end point security software solutions

QUESTION 64
A company wants to make sure that users are required to authenticate prior to being allowed on the network. Which of the following is the BEST way to accomplish this?

A. 802.1x
B. 802.1p
C. Single sign-on
D. Kerberos

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:

For security purposes, some switches require users to authenticate themselves (that is, provide credentials, such as a username and password, to prove who they are) before gaining access to the rest of the network. A standards-based method of enforcing user authentication is IEEE 802.1X.

QUESTION 65
A wireless network technician for a local retail store is installing encrypted access points within the store for real-time inventory verification, as well as remote price checking capabilities, while employees are away from the registers. The store is in a fully occupied strip mall that has multiple neighbors allowing guest access to the wireless networks. There are a finite known number of approved handheld devices needing to access the store's wireless network. Which of the following is the BEST security method to implement on the access points?

A. Port forwarding
B. MAC filtering
C. TLS/TTLS
D. IP ACL

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:

MAC filtering allows traffic to be permitted or denied based on a device's MAC address. We make a MAC filtering which contains the MAC addresses of all approved devices that need to access the wireless network. This ensures that only approved devices are given access to the network.

QUESTION 66
A network technician has set up an FTP server for the company to distribute software updates for their products. Each vendor is provided with a unique username and password for security. Several vendors have discovered a virus in one of the security updates. The company tested all files before uploading them but retested

the file and found the virus. Which of the following could the technician do for vendors to validate the proper security patch?

A. Use TFTP for tested and secure downloads
B. Require biometric authentication for patch updates
C. Provide an MD5 hash for each file
D. Implement a RADIUS authentication

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:

If we put an MD5 has for each file we can see if the file has been changed or not.
MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual.

QUESTION 67
During a check of the security control measures of the company network assets, a network administrator is explaining the difference between the security controls at the company. Which of the following would be identified as physical security controls? (Select THREE).

A. RSA
B. Passwords
C. Man traps
D. Biometrics
E. Cipher locks
F. VLANs
G. 3DES

Correct Answer: CDE
Section: Network security
Explanation

Explanation/Reference:
Explanation:

Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.
C: A mantrap is a mechanical physical security devices for catching poachers and trespassers. They have taken many forms, the most usual being like a large

foothold trap, the steel springs being armed with teeth which met in the victim's leg.
D: Biometric authentication is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems. Biometric authentication is a physical security device.
E: Cipher locks are used to control access to areas such as airport control towers, computer rooms, corporate offices, embassies, areas within financial institutions, research and development laboratories, and storage areas holding weapons, controlled substances, etc. Cipher locks are physical security devices.

QUESTION 68
Which of the following physical security controls prevents an attacker from gaining access to a network closet?

A. CCTVs
B. Proximity readers
C. Motion sensors
D. IP cameras

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:

A proximity card is a physical card which used to get access to a physical area such as a network closet.
It is a "contactless" smart card which can be read without inserting it into a reader device, as required by earlier magnetic stripe cards such as credit cards and "contact" type smart cards. The proximity cards are part of the Contactless card technologies. Held near an electronic reader for a moment they enable the identification of an encoded number.
Note: Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

QUESTION 69
A technician needs to install software onto company laptops to protect local running services, from external threats. Which of the following should the technician install and configure on the laptops if the threat is network based?

A. A cloud-based antivirus system with a heuristic and signature based engine
B. A network based firewall which blocks all inbound communication
C. A host-based firewall which allows all outbound communication
D. A HIDS to inspect both inbound and outbound network communication

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:

A host-based firewall is a computer running firewall software that can protect the computer itself. For example, it can prevent incoming connections to the computer and allow outbound communication only.

QUESTION 70
A technician is setting up a computer lab. Computers on the same subnet need to communicate with each other using peer to peer communication. Which of the following would the technician MOST likely configure?

A. Hardware firewall
B. Proxy server
C. Software firewall
D. GRE tunneling

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:

A host-based firewall is a computer running firewall software that can protect the computer itself. A software firewall would be the most cost effective in a lab scenario.

QUESTION 71
A firewall ACL is configured as follows:

10. Deny Any Trust to Any DMZ eq to TCP port 22
11. Allow 10.200.0.0/16 to Any DMZ eq to Any
12. Allow 10.0.0.0/8 to Any DMZ eq to TCP ports 80, 443
13. Deny Any Trust to Any DMZ eq to Any

A technician notices that users in the 10.200.0.0/16 network are unable to SSH into servers in the DMZ. The company wants 10.200.0.0/16 to be able to use any protocol, but restrict the rest of the 10.0.0.0/8 subnet to web browsing only. Reordering the ACL in which of the following manners would meet the company's objectives?

A. 11, 10, 12, 13
B. 12, 10, 11, 13
C. 13, 10, 12, 11

D. 13, 12, 11, 10

Correct Answer: A
Section: Network security
Explanation

Explanation/Reference:
Explanation:

ACL are processed in TOP DOWN process in routers or switches. This means that when a condition in the ACL is met, all processing is stopped.
We start by allowing any protocol on the 10.200.0.0/16 subnet:11. Allow 10.200.0.0/16 to Any DMZ eq to Any
We then deny any traffic on TCP port 22:10. Deny Any Trust to Any DMZ eq to TCP port 22
We allow browsing (port 80 and 443) on the 10.0.0.0/8 subnet:Allow 10.0.0.0/8 to Any DMZ eq to TCP ports 80, 443
Finally we deny all other traffic:13. Deny Any Trust to Any DMZ eq to Any

QUESTION 72
A technician is installing a surveillance system for a home network. The technician is unsure which ports need to be opened to allow remote access to the system.
Which of the following should the technician perform?

A. Disable the network based firewall
B. Implicit deny all traffic on network
C. Configure a VLAN on Layer 2 switch
D. Add the system to the DMZ

Correct Answer: D
Section: Network security
Explanation

Explanation/Reference:
Explanation:

By putting the system in the DMZ (demilitarized zone) we increase the security, as the system should be opened for remote access.
A DMZ is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. A DMZ often contains servers that should be accessible from the public Internet.

QUESTION 73
The ability to make access decisions based on an examination of Windows registry settings, antivirus software, and AD membership status is an example of which of the following NAC features?

A. Quarantine network
B. Persistent agents
C. Posture assessment
D. Non-persistent agents

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:

Network Admission Control (NAC) can permit or deny access to a network based on characteristics of the device seeking admission, rather than just checking user credentials. For example, a client's OS, Windows Registry settings, AD membership status, and version of antivirus software could be checked against a set of requirements before allowing the client to access a network.
This process of checking a client's characteristics is called posture assessment.

QUESTION 74
Which of the following types of network would be set up in an office so that customers could access the Internet but not be given access to internal resources such as printers and servers?

A. Quarantine network
B. Core network
C. Guest network
D. Wireless network

Correct Answer: C
Section: Network security
Explanation

Explanation/Reference:
Explanation:

A wireless guest network could be set up so that it has limited access (no access to local resources) but does provide Internet access for guest users.

QUESTION 75
Which of the following is a security benefit gained from setting up a guest wireless network?

A. Optimized device bandwidth
B. Isolated corporate resources
C. Smaller ACL changes
D. Reduced password resets

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:

A wireless guest network could be set up so that it has limited access (no access to local resources) but does provide Internet access for guest users. The corporate resources would be inaccessible (isolated) from the guest network.

QUESTION 76
Ann, a network technician, was asked to remove a virus. Issues were found several levels deep within the directory structure. To ensure the virus has not infected the .mp4 files in the directory, she views one of the files and believes it contains illegal material. Which of the following forensics actions should Ann perform?

A. Erase the files created by the virus
B. Stop and escalate to the proper authorities
C. Check the remaining directories for more .mp4 files
D. Copy the information to a network drive to preserve the evidence

Correct Answer: B
Section: Network security
Explanation

Explanation/Reference:
Explanation:

Computer forensics is about legal evidence found in computers and digital storage.
A plan should include first responders securing the area and then escalating to senior management and authorities when required by policy or law.

QUESTION 77
A network technician was tasked to respond to a compromised workstation. The technician documented the scene, took the machine offline, and left the PC under a cubicle overnight. Which of the following steps of incident handling has been incorrectly performed?

A. Document the scene

B. Forensics report

C. Evidence collection

D. Chain of custody

Correct Answer: D
Section: Network security
Explanation

Explanation/Reference:
Explanation:

To verify the integrity of data since a security incident occurred, you need to be able to show a chain of custody.
A chain of custody documents who has been in possession of the data (evidence) since a security breach occurred. A well-prepared organization will have process and procedures that are used when an incident occurs.
A plan should include first responders securing the area and then escalating to senior management and authorities when required by policy or law. The chain of custody also includes documentation of the scene, collection of evidence, and maintenance, e-discovery (which is the electronic aspect of identifying, collecting, and producing electronically stored information), transportation of data, forensics reporting, and a process to preserve all forms of evidence and data when litigation is expected. The preservation of the evidence, data, and details is referred to as legal hold.

QUESTION 78
A network technician is using a network monitoring system and notices that every device on a particular segment has lost connectivity. Which of the following should the network technician do NEXT?

A. Establish a theory of probable cause.

B. Document actions and findings.

C. Determine next steps to solve the problem.

D. Determine if anything has changed.

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The technician has already identified the symptom: Loss of connectivity on a specific network segment. The next step in identifying the problem is to "Determine if anything has changed".
Common troubleshooting steps and procedures:

1. Identify the problem.
Information gathering.
Identify symptoms.
Question users.
Determine if anything has changed.
2. Establish a theory of probable cause.
Question the obvious.
3. Test the theory to determine cause:
When the theory is confirmed, determine the next steps to resolve the problem.
If theory is not confirmed, re-establish a new theory or escalate.
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 preventive measures.
7. Document findings, actions, and outcomes.

QUESTION 79
A user calls the help desk and states that he was working on a spreadsheet and was unable to print it. However, his colleagues are able to print their documents to the same shared printer. Which of the following should be the FIRST question the helpdesk asks?

A. Does the printer have toner?

B. Are there any errors on the printer display?

C. Is the user able to access any network resources?

D. Is the printer powered up?

Correct Answer: C
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The user has already provided you with the information relevant to the first step in the 7-step troubleshooting process. The next step is to "Question the obvious."
The user has stated: "…his colleagues are able to print their documents to the same shared printer." The obvious question in this instance is whether the user can access any network resources.
1. Identify the problem.
Information gathering.
Identify symptoms.
Question users.
Determine if anything has changed.
2. Establish a theory of probable cause.
Question the obvious.

3. Test the theory to determine cause:
When the theory is confirmed, determine the next steps to resolve the problem.
If theory is not confirmed, re-establish a new theory or escalate.
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 preventive measures.
7. Document findings, actions, and outcomes.

QUESTION 80
A network technician has detected duplicate IP addresses on the network. After testing the behavior of rogue DHCP servers, the technician believes that the issue is related to an unauthorized home router. Which of the following should the technician do NEXT in the troubleshooting methodology?

A. Document the findings and action taken.

B. Establish a plan to locate the rogue DHCP server.

C. Remove the rogue DHCP server from the network.

D. Identify the root cause of the problem.

Correct Answer: B
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

By testing the behavior of rogue DHCP servers and determining that the issue is related to an unauthorized home router, the technician has completed the third step in the 7-step troubleshooting process. The next step is to establish a plan of action to resolve the problem and identify potential effects. Establishing a plan to locate the rogue DHCP server meets the requirements of this step.
1. Identify the problem.
Information gathering.
Identify symptoms.
Question users.
Determine if anything has changed.
2. Establish a theory of probable cause.
Question the obvious.
3. Test the theory to determine cause:
When the theory is confirmed, determine the next steps to resolve the problem.
If theory is not confirmed, re-establish a new theory or escalate.
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 preventive measures.
7. Document findings, actions, and outcomes.

QUESTION 81
A technician is troubleshooting a client's connection to a wireless network. The client is asked to run a "getinfo" command to list information about the existing condition.

myClient$ wificard --getinfo
agrCtlRSSI:-72
agrExtRSSI:0
state:running
op mode: station
lastTxRate:178
MaxRate:300
802.11 auth:open
link auth:wpa2-psk
BSSID:0F:33:AE:F1:02:0A
SSID:CafeWireless
Channel:149,1

Given this output, which of the following has the technician learned about the wireless network? (Select TWO).

A. The WAP is using RC4 encryption
B. The WAP is using 802.11a
C. The WAP is using AES encryption
D. The WAP is using the 2.4GHz channel
E. The WAP is using the 5GHz channel
F. The WAP is using 802.11g

Correct Answer: CE
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

WPA2 makes use of the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption protocol, which is an AES based protocol.
The output shows that the wireless network operates on channel 149, which is a channel in the 5GHz band.

QUESTION 82
An administrator only has telnet access to a remote workstation. Which of the following utilities will identify if the workstation uses DHCP?

A. tracert
B. ping
C. dig
D. ipconfig
E. netstat

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The ipconfig command displays the TCP/IP configuration of a Windows system. The ipconfig /all command displays the system's TCP/IP configuration in detail. This output includes whether DHCP is enabled or not.

QUESTION 83
A network technician is performing a tracert command to troubleshoot a website-related issue. The following output is received for each hop in the tracert:
1 * * * Request timed out.
2 * * * Request timed out.
3 * * * Request timed out.

The technician would like to see the results of the tracert command. Which of the following will allow the technician to perform tracert on external sites but not allow outsiders to discover information from inside the network?

A. Enable split horizon to allow internal tracert commands to pass through the firewall
B. Enable IGMP messages out and block IGMP messages into the network
C. Configure the firewall to allow echo reply in and echo request out of the network
D. Install a backdoor to access the router to allow tracert messages to pass through

Correct Answer: C
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

Tracert makes use of ICMP echo packets to trace the route between two hosts. For the command to be successful, the firewall has to allow incoming echo replies and outgoing echo requests.

QUESTION 84
A network technician has received comments from several users that cannot reach a particular website. Which of the following commands would provide the BEST information about the path taken across the network to this website?

A. ping
B. netstat
C. telnet
D. tracert

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The tracert command is used to determine the amount of hops a packet takes to reach a destination. It makes use of ICMP echo packets to report information at every step in the journey. This is how the path taken across the network is obtained.

QUESTION 85
After connecting a workstation directly to a small business firewall, a network administrator is trying to manage it via HTTPS without losing its stored configuration. The only two pieces of information that the network administrator knows about the firewall are the management interface MAC address, which is 01:4a:d1:fa:b1:0e, and the administrator's password. Which of the following will allow the administrator to log onto the firewall via HTTPS if the management's IP address is unknown and the administrator's workstation IP address is 192.168.0.10/23?

A. Use the reset button on the back of the firewall to restore it to its factory default, and then log onto
B. Run the following command on the administrator's workstation: arp –s 192.168.1.200 01:4a:d1:fa:b1:0e
C. Use an SNMP tool to query the firewall properties and determine the correct management IP address
D. Use a crossover cable to connect to the console port and reconfigure the firewall management IP to 192.168.0.1

Correct Answer: B
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

Address Resolution Protocol (ARP) is used to resolve IP addresses to MAC addresses. The arp –s command adds a static permanent address to the ARP cache. This will allow the administrator to access the firewall.

QUESTION 86
A network technician has detected a personal computer that has been physically connected to the corporate network. Which of the following commands would the network technician use to locate this unauthorized computer and determine the interface it is connected to?

A. nbtstat –a
B. show mac address-table
C. show interface status
D. show ip access-list
E. nslookup hostname

Correct Answer: B
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The show mac address-table command is used to view the ageing timer, and also the unicast and multicast MAC addresses stored in the MAC address table by the switch. Furthermore, you can view all of the addresses in the table or only the addresses learned or specified on a particular port or VLAN.

QUESTION 87
A technician has verified that a recent loss of network connectivity to multiple workstations is due to a bad CAT5 cable in the server room wall. Which of the following tools can be used to locate its physical location within the wall?

A. Cable certifier
B. Multimeter
C. Cable tester
D. Toner probe

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:

Explanation:

Toner probes are specifically used to trace cables hidden in floors, ceilings, or walls. They can also be used to track cables from the patch panels to their destinations.

QUESTION 88
A user connects to a wireless network at the office and is able to access unfamiliar SMB shares and printers. Which of the following has happened to the user?

A. The user is connected using the wrong channel.
B. The user is connected to the wrong SSID.
C. The user is experiencing an EMI issue.
D. The user is connected to the wrong RADIUS server.

Correct Answer: B
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The user is connecting to an SSID assigned to a different subnet. Therefore, the user has access to SMB shares and printers that are not recognizable.

QUESTION 89
A technician is troubleshooting a wired device on the network. The technician notices that the link light on the NIC does not illuminate. After testing the device on a different RJ-45 port, the device connects successfully. Which of the following is causing this issue?

A. EMI
B. RFI
C. Cross-talk
D. Bad wiring

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The question states that the device worked on a different port. This indicates that the wiring is faulty.

QUESTION 90
A technician is tasked with connecting a router to a DWDM. The technician connects the router to the multiplexer and confirms that there is a good signal level. However, the interface on the router will not come up. Which of the following is the MOST likely cause?

A. The wrong wavelength was demuxed from the multiplexer.
B. The SFP in the multiplexer is malfunctioning.
C. There is a dirty connector on the fiber optic cable.
D. The fiber optic cable is bent in the management tray.

Correct Answer: A
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

A multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A demultiplexer (or demux) is a device taking a single input signal and selecting one of many data-output-lines, which is connected to the single input. Since the signal going in is good, the problem must be with the signal output. If the correct wavelength was demultiplexed, the interface will be displayed on the router.

QUESTION 91
While troubleshooting a network outage, a technician finds a 100-meter fiber cable with a small service loop and suspects it might be the cause of the outage. Which of the following is MOST likely the issue?

A. Maximum cable length exceeded
B. Dirty connectors
C. RF interference caused by impedance mismatch
D. Bend radius exceeded

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The excessive bending of fiber-optic cables can increase microbending and macrobending losses. Microbending causes light attenuation induced by deformation of the fiber, while macrobending causes the leakage of light through the fiber cladding and this is more likely to happen where the fiber is excessively bent.

QUESTION 92

A network technician has been assigned to install an additional router on a wireless network. The router has a different SSID and frequency. All users on the new access point and the main network can ping each other and utilize the network printer, but all users on the new router cannot get to the Internet. Which of the following is the MOST likely cause of this issue?

A. The gateway is misconfigured on the new router.
B. The subnet mask is incorrect on the new router.
C. The gateway is misconfigured on the edge router.
D. The SSID is incorrect on the new router.

Correct Answer: A
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

A missing or incorrect default gateway parameter limits communication to the local segment.
The question states: "All users on the new access point and the main network can ping each other and utilize the network printer, but all users on the new router cannot get to the Internet".

QUESTION 93
While troubleshooting a connectivity issue, a network technician determines the IP address of a number of workstations is 169.254.0.0/16 and the workstations cannot access the Internet. Which of the following should the technician check to resolve the problem?

A. Default gateway address
B. Misconfigured DNS
C. DHCP server
D. NIC failure

Correct Answer: C
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

If a DHCP server fails, the workstations are assigned an address from the 169.254.0.0 address range by Automatic Private IP Addressing (APIPA). APIPA also configures a suitable subnet mask, but it doesn't configure the system with a default gateway address. This allows communication on the local network, but not externally.

QUESTION 94
A network engineer is troubleshooting an issue with a computer that is unable to connect to the Internet. The network engineer analyzes the following output from a command line utility:

Network DestinationNetmaskGatewayInterface
192.168.1.0 255.255.255.0192.168.1.254eth0
192.168.1.10255.255.255.255192.168.1.10eth0
127.0.0.1255.0.0.0On-Linlo
127.0.0.0255.0.0.0On-Linklo
255.255.255.255255.255.255.255102.168.1.10eth0

Which of the following is the reason for the computer issue, given the above output?

A. Wrong default gateway netmask
B. Incorrect default gateway address
C. Default gateway on the wrong interface
D. Missing default gateway

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The output appears to be a result of running the netstat –r command. If the default gateway was present, the first line would show the Network Destination as 0.0.0.0 and the Netmask as 0.0.0.0.

QUESTION 95
A company has changed ISPs for their office and ordered a new 250 Mbps symmetrical Internet connection. As a result, they have been given a new IP range. The ISP has assigned the company 10.10.150.16 /28. The company gateway router has the following interface configuration facing the ISP:

Interface A:
IP address: 10.10.150.16
Subnet mask: 255.255.255.240
Default gateway: 10.10.150.32
Speed: 1000 Mbps
Duplex: Auto
State: No Shutdown

None of the workstations at the company are able to access the Internet. Which of the following are the reasons? (Select TWO).

A. There is a duplex mismatch between the router and ISP.

B. The router interface is turned off.

C. The interface is set to the incorrect speed.

D. The router is configured with the incorrect subnet mask.

E. The router interface is configured with the incorrect IP address.

F. The default gateway is configured incorrectly.

Correct Answer: EF
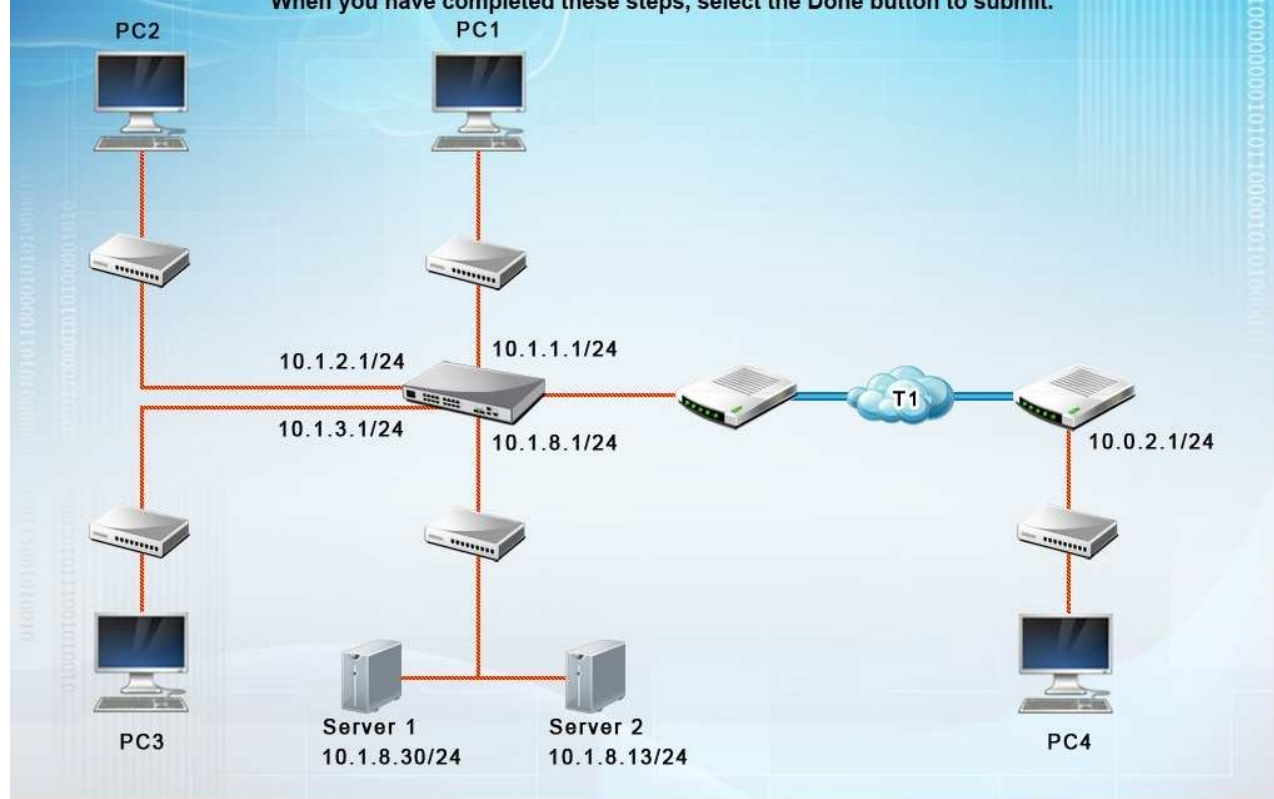**Section: Troubleshooting**
Explanation

Explanation/Reference:
Explanation:

According to the IP Address Range Calculator, for the given subnet mask and the IP range address range assigned by the ISP, the first host address should be 10.10.150.17 and the broadcast address should be 10.10.150.31. Therefore, the router interface is configured with the incorrect IP address and the default gateway is configured incorrectly.

QUESTION 96
CORRECT TEXT
SIMULATION
After recent changes to the pictured network, several users are unable to access the servers. Only PC1, PC2, PC3, and PC4 are clickable and will give you access to the command prompt and the adapter configuration tabs.
Instructions: Verify the settings by using the command prompt, after making any system changes. Next, restore connectivity by making the appropriate changes to the infrastructure. When you have completed these steps, select the Done button to submit.

Network Diagram

Instructions: Verify the settings by using the command prompt, after making any system changes.
Next, restore connectivity by making the appropriate changes to the infrastructure.
When you have completed these steps, select the Done button to submit.

PC2

PC1

10.1.2.1/24

10.1.1.1/24

T1

10.1.3.1/24

10.1.8.1/24

10.0.2.1/24

PC3

Server 1
10.1.8.30/24

Server 2
10.1.8.13/24

PC4

ADAPTER CONFIGURATION | COMMAND PROMPT | PC 1 | (X)

You can get IP settings assigned automatically if your network supports this capability.Otherwise,you need to ask your network administrator for the appropriate IP settings.

- Obtain an IP address automatically
- Use the following IP address

IP address: 10 . 1 . 1 . 129

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 1 . 1 . 1

- Obtain DNS server address automatically
- Use the following DNS server addresses

Perferred DNS server: 10 . 1 . 8 . 13

Alternate DNS server: .   .   .

☐ Validate settings upon exit   Advanced...

Apply   Cancel

You can get IP settings assigned automatically if your network supports this capability.Otherwise,you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
◉ Use the following IP address

IP address: 10 . 1 . 2 . 129
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 1 . 2 . 1

○ Obtain DNS server address automatically
◉ Use the following DNS server addresses

Perferred DNS server: 10 . 1 . 8 . 13
Alternate DNS server: .   .   .

☐ Validate settings upon exit   Advanced...

Apply   Cancel

ADAPTER CONFIGURATION   COMMAND PROMPT   PC 3

You can get IP settings assigned automatically if your network supports this capability.Otherwise,you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address

IP address: 10 . 1 . 3 . 129

Subnet mask: 255 . 255 . 255 . 128

Default gateway: 10 . 1 . 3 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses

Perferred DNS server: 10 . 1 . 8 . 13

Alternate DNS server: .   .   .

☐ Validate settings upon exit   Advanced...

Apply   Cancel

ADAPTER CONFIGURATION **COMMAND PROMPT** PC 4 ⊗

You can get IP settings assigned automatically if your network supports this capability.Otherwise,you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
◉ Use the following IP address

IP address:	10 . 0 . 2 . 129
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 1 . 2 . 1

○ Obtain DNS server address automatically
◉ Use the following DNS server addresses

| Perferred DNS server: | 10 . 1 . 8 . 13 |
| Alternate DNS server: | . . . |

☐ Validate settings upon exit   Advanced...

Apply   Cancel

Correct Answer: Here is the solution below
Section: Troubleshooting

Explanation

Explanation/Reference:
Explanation:

The default gateway must be on the same network as the nodes that use it. Therefore, the subnet on PC3 and the default gateway on PC4 must be modified.

References:
Dulaney, Emmett and Mike Harwood, CompTIA Network+ Authorized Exam Cram, Fourth Edition, Pearson, Indianapolis, 2012, p 101.
http://www.subnetonline.com/pages/subnet-calculators/ip-subnet-calculator.php

QUESTION 97
A PC technician has installed a new network printer that was preconfigured with the correct static IP address, subnet mask, and default gateway. The printer was installed with a new cable and appears to have link activity, but the printer will not respond to any network communication attempts. Which of the following is MOST likely the cause of the problem?

A. Damaged cable
B. Duplex mismatch
C. Incorrect VLAN assignment
D. Speed mismatch

Correct Answer: C
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

If a port is accidentally assigned to the wrong VLAN in a switch, it's as if that client was magically transported to another place in the network. This would explain the inability to communication with the printer, as it is on a different VLAN.

QUESTION 98
A network administrator recently installed a web proxy server at a customer's site. The following week, a system administrator replaced the DNS server overnight. The next day, customers began having issues accessing public websites. Which of the following will resolve the issue?

A. Update the DNS server with the proxy server information.

B. Implement a split horizon DNS server.

C. Reboot the web proxy and then reboot the DNS server.

D. Put the proxy server on the other side of the demarc.

Correct Answer: A
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

Proxy servers act as an intermediary for requests from clients seeking resources from other servers. If the DNS server is not communicating with the proxy server, these requests are not forwarded. Therefore, updating the DNS server with the proxy server information will solve the problem.

QUESTION 99
Two weeks after installation, a network technician is now unable to log onto any of the newly installed company switches. The technician suspects that a malicious user may have changed the switches' settings before they were installed in secure areas. Which of the following is the MOST likely way in which the malicious user gained access to the switches?

A. Via SSH using the RADIUS shared secret

B. Via HTTP using the default username and password

C. Via console using the administrator's password

D. Via SNMP using the default RO community

Correct Answer: B
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

A new network switch is accessed via HTTP to perform the initial configuration. The username and password used is a factory default.

QUESTION 100
A network technician is troubleshooting a problem at a remote site. It has been determined that the connection from router A to router B is down. The technician at the remote site re-terminates the CAT5 cable that connects the two routers as a straight through cable. The cable is then tested and is plugged into the correct interface. Which of the following would be the result of this action?

A. The normal amount of errors and the connection problem has been resolved.

B. The interface status will indicate that the port is administratively down.

C. The traffic will flow, but with excessive errors.

D. The interface status will show line protocol down.

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

Devices of different types are connected with a straight through cable (patch cable). In this case, it is used to connect two devices of the same type. It is for this reason that the interface will display the line protocol down status.

QUESTION 101
Which of the following helps prevent routing loops?

A. Routing table

B. Default gateway

C. Route summarization

D. Split horizon

Correct Answer: D
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

Routing loops occur when the routing tables on the routers are slow to update and a redundant communication cycle is created between routers. Split horizon, which prevents the router from advertising a route back to the other router from which it was learned, can be used to resist routing loops. Poison reverse, also known as split horizon with poison reverse, is also used to resist routing loops.

QUESTION 102
After repairing a computer infected with malware, a technician determines that the web browser fails to go to the proper address for some sites. Which of the following should be checked?

A. Server host file

B. Subnet mask

C. Local hosts file

D. Duplex settings

Correct Answer: C
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

The local hosts file is a text file that contains hostname-to-IP address mappings. By default, host to IP address mappings that are configured in the Hosts file supersede the information in DNS. If there is an entry for a domain name in the Hosts file, then the server will not attempt to query DNS servers for that name. Instead, the IP address that is configured in the Hosts file will be used. If the IP address corresponding to a name changes and the Hosts file is not updated, you may be unable to connect to the host.

QUESTION 103
Which of the following WAN technologies is associated with high latency?

A. T1
B. Satellite
C. Cable
D. OCx

Correct Answer: B
Section: Troubleshooting
Explanation

Explanation/Reference:
Explanation:

Latency in this instance is the time it takes for the signal to and from the satellite. Since signal has to travel to the satellite, then from the satellite to the ground station, and then out to the Internet (or IP WAN). Not forgetting the return trip, and processing delays.

QUESTION 104
When a client calls and describes a problem with a computer not being able to reach the Internet, in which of the following places of the OSI model would a technician begin troubleshooting?

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

Correct Answer: B
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

The bottom layer of the OSI reference model is Layer 1, the physical layer.
The physical layer is the layer that defines the hardware elements of a network.
These elements include:
Network Interface Cards
Network topology
Network cabling
The type of signals used for data transmissions

When troubleshooting a network connectivity issue, the first thing you would check is the computer's network cabling, the network card etc. In other words, the computer's physical connection to the network.

QUESTION 105
A network engineer is dispatched to an employee office to troubleshoot an issue with the employee's laptop. The employee is unable to connect to local and remote resources. The network engineer flips the laptop's wireless switch on to resolve the issue. At which of the following layers of the OSI model was the issue resolved?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4
E. Layer 7

Correct Answer: A
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

The bottom layer of the OSI reference model is Layer 1, the physical layer.
The physical layer is the layer that defines the hardware elements of a network.
These elements include:
Network Interface Cards
Network topology

Network cabling
The type of signals used for data transmittions

In this question, the network engineer flipped the laptop's wireless switch on to resolve the issue. The laptop was unable to connect to the wireless network because the wireless network interface card was switched off. Switching the wireless network interface card on enabled the laptop to connect to the wireless network. The wireless network interface card is a physical layer device.

QUESTION 106
When troubleshooting a network problem, browsing through the log of a switch, it is discovered that multiple frames contain errors. In which of the following layers does the problem reside? (Select TWO).

A. Layer 2
B. Layer 3
C. Layer 5
D. Transport layer
E. Data link
F. Physical layer

Correct Answer: AE
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

Layer 2 of the OSI reference model is the data-link layer. Components of the data-link layer include frame-format, Media Access Control (MAC) addressing, protocol identification and error detection.
When data is being sent, it is split into protocol data units (PDUs) as it passes through the layers of the OSI model. The PDUs have different names as they are passed through the layers of the OSI model. In layer 2, the PDU is called a 'Frame'.
The most common protocol specified in the data-link layer is Ethernet and the most common network component in the data-link layer is a network switch.
In this question, problems are discovered with Ethernet frames by examining the logs in a network switch. Therefore, for this question, we are working in Layer 2, the data-link layer.

QUESTION 107
A network administrator is using a packet analyzer to determine an issue on the local LAN. Two separate computers are showing an error message on the screen and are unable to communicate with other computers in the same lab. The network administrator looks at the following output:

SRC MACSRC IPDST MACDST IP
00:1D:1F:AB:10:7D192.168.1.10:200015:BE:9F:AB:10:1D192.168.1.14:1200
05:DD:1F:AB:10:27192.168.1.10:100022:C7:2F:AB:10:A2192.168.1.15:1300

Given that all the computers in the lab are directly connected to the same switch, and are not using any virtualization technology, at which of the following layers of the OSI model is the problem occurring?

A. Network
B. Application
C. Data link
D. Transport

Correct Answer: A
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

If we look at the Source Mac column, we can see two different MAC addresses. Every network interface card has a unique MAC address. These are the network cards in the two separate computers.
If we look in the Source IP column, we can see that the two network cards have been assigned the same IP address (192.168.1.10). This is the problem in this question. The error message on the screens will be saying that "An IP conflict exists". Every network card connected to the network needs to be configured with a different IP address.
As the problem is with the IP address configuration of the two computers, we know that the problem is occurring at the Network layer (layer 3) of the OSI model. The network layer is responsible for Internet Protocol (IP) addressing and routing.

QUESTION 108
Which of the following will negotiate standoff timers to allow multiple devices to communicate on congested network segments?

A. CSMA/CD
B. OSPF
C. DOCSIS
D. BGP

Correct Answer: A
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

Carrier Sense Multiple Access/Collision Detect (CSMA/CD) is used by devices in an Ethernet network for transmitting data on the network.
Any device on an Ethernet network can send data at any time. The network devices sense when the line is idle and therefore available for the transmission of data.

The network device then transmits a data frame onto the network. If another device sends a frame at exactly the same time, a collision occurs and the frames are discarded. The network devices will then wait for a random period of time before attempting to send the frame again.

QUESTION 109
Which of the following devices implements CSMA/CA virtually through the RTS/CTS protocols?

A. Firewall
B. Router
C. 802.11 AP
D. Switch

Correct Answer: C
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

802.11 AP is a Wireless Access Point used in a wireless network.
If two computers on a network send data frames at the same time, a collision between the frames can occur. The frames are then discarded and the sending computers will attempt to send the data again.
Carrier sense multiple access with collision avoidance (CSMA/CA) is a protocol used in wireless networks where computers connected to the wireless network attempt to avoid collisions by transmitting data only when the channel is sensed to be "idle". Carrier Sense Multiple Access/Collision Detect (CSMA/CD) is unreliable in wireless networks because computers connected to the wireless network often cannot see each other so CSMA/CA is a better option for avoiding collisions.
Request to Send/Clear to Send (RTS/CTS) can also be used to mediate access to the wireless network. This goes some way to alleviating the problem of computers not being able to see each other because in a wireless network, the Wireless Access Point only issues a "Clear to Send" to one node at a time.
With RTS/CTS, a Request to Send (RTS) packet is sent by the sending computer, and a Clear to Send (CTS) packet is sent by the intended receiver. This will alert all computers within range of the sender, receiver or both, to not transmit for the duration of the transmission. This is known as the IEEE 802.11 RTS/CTS exchange.

QUESTION 110
The management team wants to set up a wireless network in their office but all of their phones operate at the 2.4 GHz frequency. They need a wireless network that would be able to operate at a higher frequency than their phones. Which of following standards should be used?

A. 802.11a
B. 802.11b
C. 802.11g
D. 802.1x

Correct Answer: A

Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

In this question, we need a wireless network that operates at a frequency higher than the 2.4GHz frequency.
802.11 is a set of IEEE standards that govern wireless networking transmission methods. The 802.11 standards commonly used today to provide wireless connectivity in home or office wireless networks are 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac.
The 802.11a standard supports speeds up to 54Mbps and uses the 5-GHz band.

QUESTION 111
A user with an 802.11n WLAN card is connected to a SOHO network and is only able to connect at 11 Mbps with full signal strength. Which of the following standards is implemented on the network?

A. 802.11a
B. 802.11ac
C. 802.11b
D. 802.11g

Correct Answer: C
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

802.11 is a set of IEEE standards that govern wireless networking transmission methods. The 802.11 standards commonly used today to provide wireless connectivity in home or office wireless networks are 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac.
802.11b supports speeds up to 11Mbps and uses the 2.4GHz frequency.
In this question, the user is using an 802.11n WLAN card. Although the 802.11n WLAN card can support speeds up to 300Mbps, the user is only able to connect at 11Mbps because the user is connected to a wireless network configured to use 802.11b.

QUESTION 112
A network technician has been tasked with designing a WLAN for a small office. One of the requirements of this design is that it is capable of supporting HD video streaming to multiple devices. Which of the following would be the appropriate wireless technology for this design?

A. 802.11g
B. 802.11ac
C. 802.11b

D. 802.11a

Correct Answer: B
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

In this question, we need a wireless network capable of supporting HD video streaming to multiple devices. We therefore need the fastest wireless network speed available.
802.11 is a set of IEEE standards that govern wireless networking transmission methods. The 802.11 standards commonly used today to provide wireless connectivity in home or office wireless networks are 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac.
The 802.11ac standard is the fastest wireless network supporting speeds of over 3Gbps and uses the 5-GHz band.

QUESTION 113
A company is deploying a new wireless network and requires 800Mbps network throughput. Which of the following is the MINIMUM configuration that would meet this need?

A. 802.11ac with 2 spatial streams and an 80MHz bandwidth

B. 802.11ac with 3 spatial streams and a 20MHz bandwidth

C. 802.11ac with 3 spatial streams and a 40MHz bandwidth

D. 802.11ac with 4 spatial streams and a 160MHz bandwidth

Correct Answer: A
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

Spatial streaming is used in wireless communications where multiple-input-multiple-output (MIMO) is being used. With MIMO, multiple antennas are used for transmission and reception. MIMO was available in 802.11n but its capabilities have been extended in 802.11ac.
802.11ac supports a mandatory 80 MHz channel bandwidth for stations (vs. 40 MHz maximum in 802.11n), 160 MHz available optionally and more (up to 8) special streams.
A single antenna and 80 MHz channel bandwidth provides a bandwidth of 433Mbps. In this question, we need a minimum bandwidth of 800Mbps. Two antennas and 80 MHz channel bandwidth provides a bandwidth of 867Mbps and therefore meets the requirement.

QUESTION 114
A network technician is attempting to connect a new host to existing manufacturing equipment on an Ethernet network. The technician is having issues trying to establish communication between the old equipment and the new host. The technician checks the cabling for breaks and finds that the CAT3 cable in use is in

perfect condition. Which of the following should the technician check to ensure the new host will connect?

A. Confirm the new host is using 10GBaseSR due to the manufacturing environment
B. Confirm the new host is compatible with 10BaseT Ethernet
C. Confirm the existing 10Base2 equipment is using the proper frame type
D. Confirm that CSMA/CD is disabled on the Ethernet network

Correct Answer: B
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

The question states that the equipment is old and that CAT3 cabling is being used.
10BaseT Ethernet networks are old and slow by today's standards. 10BaseT Ethernet networks use CAT3 UTP cabling and offer a maximum bandwidth of just 10Mpbs.
A new host computer nowadays will have a network card that supports 1000Mpbs to be used with CAT5, CAT5e or CAT6 network cables in a 1000BaseT network.
In this question, we need to check that the network card on the new host computer is backward-compatible with the old 10BaseT network.

QUESTION 115
Before logging into the company network, users are required to sign a document that is to be stored in their personnel file. This standards and policies document is usually called which of the following?

A. SOP
B. BEP
C. AUP
D. SLA

Correct Answer: C
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

AUP stands for Acceptable Use Policy. An Acceptable Use Policy defines what a user can or cannot do with his or her computer during business hours. For example, using the company's Internet connection to look at the sports scores on a sports website may be deemed inappropriate or unacceptable during business hours. Other examples include the use of social media websites such as Facebook or using Instant Messaging clients to chat to your friends.

QUESTION 116
A service provider is unable to maintain connectivity to several remote sites at predetermined speeds. The service provider could be in violation of the:

A. MLA.
B. SLA.
C. SOW.
D. MOU.

Correct Answer: B
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

SLA stands for Service Level Agreement. This is a common document in business used to define a minimum standard of service that a customer can expect from a supplier. SLA's are particularly common in the I.T. sector where a service provider is offering a service to a customer. As a customer, you want your hosted services and Internet or WAN connections to be available all the time. SLAs often guarantee 99.9% uptime for a service.
In this question, the service provider is providing WAN links to remote sites with a guaranteed bandwidth on the WAN links. A failure to maintain the connectivity to the remote sites would be a violation of the Service Level Agreement (SLA).

QUESTION 117
A customer has engaged a company to improve the availability of all of the customer's services and applications, enabling the customer to minimize downtime to a few hours per quarter. Which of the following will document the scope of the activities the company will provide to the customer, including the intended outcomes?

A. MLA
B. MOU
C. SOW
D. SLA

Correct Answer: C
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

SOW stands for Statement of Work. When a company has been hired for a project that involves many tasks, a statement of work is often issued at the start of the project.
The SOW will outline the tasks or activities in a project, their costs and the timelines for deliverables within the project. In an IT project, the SOW would define what tasks will be performed (hardware and software upgrades etc.), why the work is being done and how long each stage of the project will take.

QUESTION 118
A technician has prolonged contact with a thermal compound. Which of the following resources should be consulted?

A. HCL
B. MSDS
C. SLA
D. HVAC

Correct Answer: B
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

MSDS stands for Material Safety Data Sheet. An MSDS is a health and safety document that contains information on the potential hazards of working with a chemical product and how to work safely with the chemical product.
In this question, the thermal compound is a chemical product so the MSDS will provide information about the effects of prolonged contact with the thermal compound.

QUESTION 119
An organization is moving to a new datacenter. During the move, several technicians raise concerns about a system that could potentially remove oxygen from the server room and result in suffocation. Which of the following systems are they MOST likely discussing?

A. Fire suppression
B. Mantraps at the entry
C. HVAC
D. UPS and battery backups

Correct Answer: A
Section: Industry standards, practices, and network theory

Explanation

Explanation/Reference:
Explanation:

Fire suppression systems are often deployed in server rooms to prevent a fire destroying all the I.T. equipment. Different fire suppression systems work in different ways. Obviously a fire suppression system that sprays water onto the fire is no good for a server room as the water would do as much damage as the fire. A common fire suppression system used in server rooms is one that suppresses the fire by starving it of oxygen. One way the oxygen can be removed from the server room is to fill the server room with an inert gas such as carbon dioxide.

QUESTION 120
Which of the following describes an area containing a rack that is used to connect customer equipment to a service provider?

A. 110 block
B. MDF
C. DSU
D. CSU

Correct Answer: B
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

MDF stands for Main Distribution Frame. A Main Distribution Frame is a commonly a long steel rack accessible from both sides. On one side of the rack is cabling that connects the service provider's network. The other side of the rack is for the connections to the customer's equipment.

QUESTION 121
Which of the following PDUs is used by a connectionless protocol?

A. Frames
B. Segments
C. Streams
D. Datagram

Correct Answer: D
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

UDP is a connectionless transport protocol that operates in the transport layer of the OSI model. UDP stands for User Datagram Protocol. PDUs (Protocol Data Units) used by UDP are known as Datagrams.

QUESTION 122
A network technician is utilizing a network protocol analyzer to troubleshoot issues that a user has been experiencing when uploading work to the internal FTP server. Which of the following default port numbers should the technician set the analyzer to highlight when creating a report? (Select TWO).

A. 20
B. 21
C. 22
D. 23
E. 67
F. 68
G. 69

Correct Answer: AB
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

FTP (File Transfer Protocol) is used for transferring files between an FTP client and an FTP server. FTP uses TCP Ports 20 and 21.

QUESTION 123
A network technician has just installed a TFTP server on the administrative segment of the network to store router and switch configurations. After a transfer attempt to the server is made, the process errors out. Which of the following is a cause of the error?

A. Only FTP can be used to copy configurations from switches
B. Anonymous users were not used to log into the TFTP server
C. An incorrect password was used and the account is now locked
D. Port 69 is blocked on a router between the network segments

Correct Answer: D
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

The question states that the TFTP server is installed on the "administrative segment of the network". This implies that the network has multiple segments (subnets) and TFTP server is on a different network segment to other computers.
For a computer on one subnet to connect to a computer on a different subnet, a router is required to route traffic between the two subnets. Routers often include firewalls so they can be configured to allow specific traffic to be routed between the subnets and block unwanted traffic.
TFTP uses UDP port 69. The most likely cause of the connection timeout error in the question is that the firewall has not been configured to allow traffic using UDP port 69.

QUESTION 124
A network administrator has created a virtual machine in the cloud. The technician would like to connect to the server remotely using RDP. Which of the following default ports needs to be opened?

A. 445
B. 3389
C. 5004
D. 5060

Correct Answer: B
Section: Industry standards, practices, and network theory
Explanation

Explanation/Reference:
Explanation:

RDP (Remote Desktop Protocol) is used for connecting to a remote Windows computer. When using RDP to connect to a remote Windows computer, you can view and control the desktop of the remote computer. RDP uses TCP port 3389.

QUESTION 125
CORRECT TEXT
SIMULATION

After recent changes to the pictured network, several users are unable to access the servers. Only PC1, PC2, PC3, and PC4 are configurable. You can only change the adapter configurations to each PC.

Restore connectivity by making the appropriate changes to the infrastructure.

Use these options to change the IP Address Settings on each PC to fix the issue

0	1	2	3
128	192	224	240
248	250	252	255

PC 2
IP address: 10 . 1 . 2 . 129
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 1 . 2 . 1
DNS server: 10 . 1 . 8 . 13

PC 1
IP address: 10 . 1 . 1 . 129
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 1 . 1 . 1
DNS server: 10 . 1 . 8 . 13

PC 3
IP address: 10 . 1 . 3 . 129
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 1 . 3 . 1
DNS server: 10 . 1 . 8 . 1

PC 4
IP address: 10 . 0 . 2 . 129
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 0 . 2 . 1
DNS server: 10 . 1 . 8 . 1

10.1.2.1/24
10.1.1.1/24
10.1.3.1/24
10.1.8.1/24
WAN
10.0.2.1/24

Server1
10.1.8.30/24

Server2
10.1.8.13/24

Correct Answer: Here is the solution below
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

On PC3, change the subnet mask to 255.255.255.0. When it is set to 255.255.255.128, then the PC with a .129 address will not be on the same subnet as the default gateway which is .1
On PC4, change the default gateway to 10.0.2.1. It has been incorrectly set as 10.1.2.1.

On this simulation, you will be asked to test connectivity after fixing the issues. You MUST ping the other three computers on EACH computer (i.e. from PC1, ping PC2, PC3, PC4, and from PC2, ping PC1, PC3 and PC4, etc)

QUESTION 126
DRAG DROP
Your company recently purchased a new building down the street from the existing office.

For each of the tasks below, select the appropriate antenna type and encryption object for all wireless access point (AP).
1. Create an encrypted wireless connection between the two buildings that BEST controls signal propagation, while maximizing security.
2. Restrict the wireless signal generated by the access points (AP's) inside Building 1, so that it minimizes broadcast beyond the building.
3. Maximize wireless coverage inside Building 1.
4. Building 1's internal wireless network is for visitors only and must not require any special configuration on the visitor's device to connect.

Select and Place:

Correct Answer:
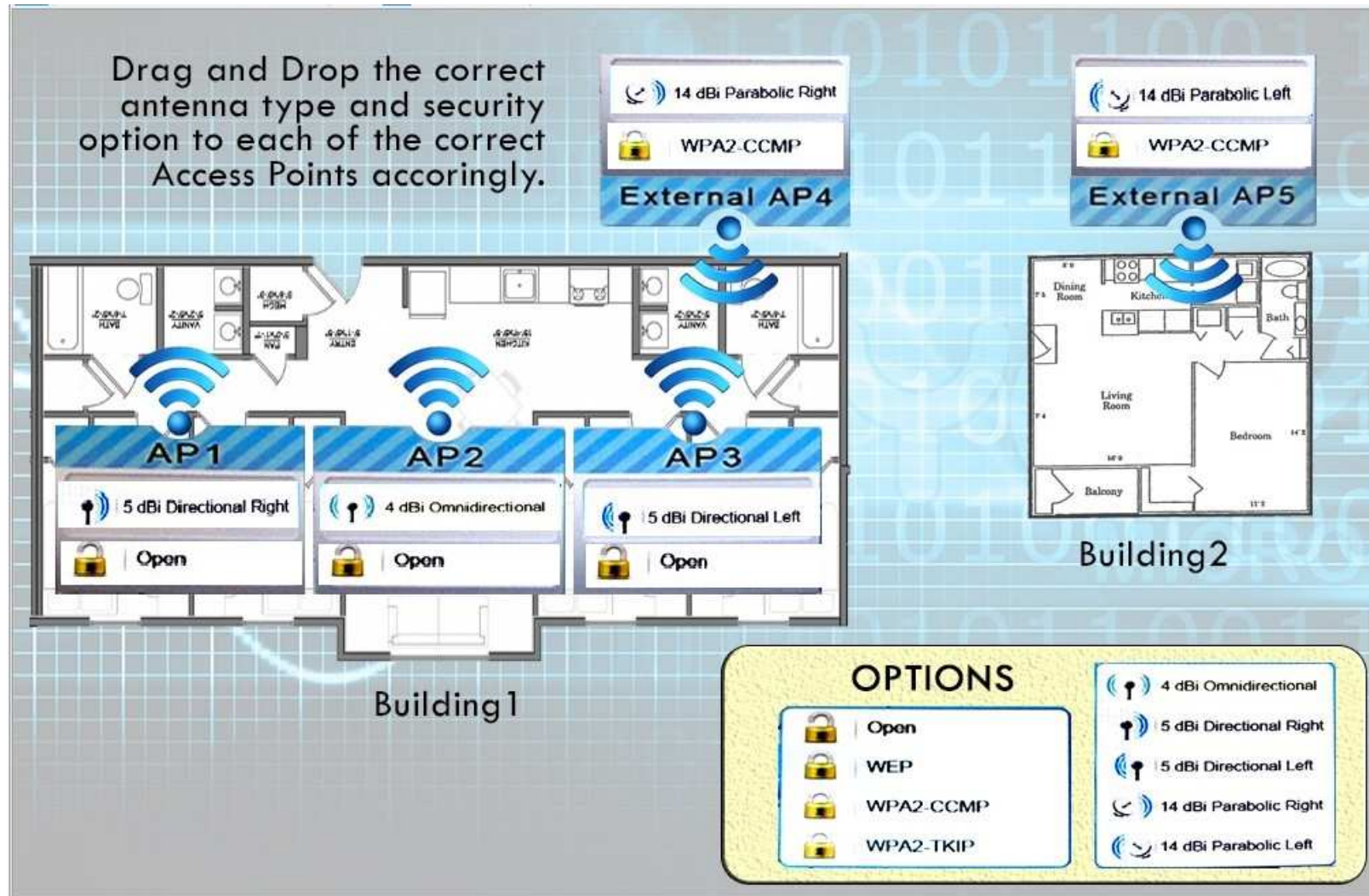
Section: Mix questions
Explanation

Explanation/Reference:

QUESTION 127
DRAG DROP
Wireless network users recently began experiencing speed and performance issues after access point 2 (AP2) was replaced due to faulty hardware. The original network was installed according to a consultant's specifications and has always worked without a problem.

You a network technician, have been tasked with evaluating the situation and resolving the issues to improve both performance and connectivity. Refer to the following exhibits and perform any necessary changes to the wireless and wired infrastructure by adjusting devices. Note: Adjust the LEAST number of devices needed to fix the issue.

Select and Place:

OPTIONS

Note: Adjust the LEAST number of devices needed to fix the issue.

IP Addresses:
192.168.100.151 192.168.100.152
192.168.100.153 192.168.100.1

Wireless Name: CorpNET
New Router password: 123456789b

Available WiFi Channels:
01 02 03 04 05 06 07 08 09 10 11

CIDR Options: WiFi Mode:
24 25 26 27 28 29 30   A B G N

Speed   Duplex
Auto 100 1000   Auto Half Full

Available Security Types: Submit?
OPEN WEP WPA WPA2   (Save)

Access Point 1
IP Address: 192.168.100.151
Subnet CIDR: 24
Gateway: 192.168.100.1
SSID: CorpNET
Wireless Channel: 01
Speed: 100
Duplex: Full
Wireless Mode: G
Security Setting: WPA
Password: 123456789b

Access Point 2
IP Address: 192.168.100.152
Subnet CIDR: 24
Gateway: 192.168.100.1
SSID: CorpNET
Wireless Channel: 01
Speed: Auto
Duplex: Auto
Wireless Mode: B
Security Setting: WPA
Password: 123456789b

Access Point 3
IP Address: 192.168.100.153
Subnet CIDR: 24
Gateway: 192.168.100.1
SSID: CorpNET
Wireless Channel: 11
Speed: 100
Duplex: Full
Wireless Mode: G
Security Setting: WPA
Password: 123456789b

AP1   AP2   AP3   Switch1

Correct Answer:

Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

After you fix AP2, you must click on the switch, which will bring up the switch interface. Type in the two commands that they show there, to prove the fix. Do not

worry that interface 4 is down, there is no interface 4 for you to do

QUESTION 128
DRAG DROP
A customer's email server is not sending emails. Arrange the troubleshooting steps in the order the technician should perform them:

Select and Place:

1	Implement the solution
2	Verify full system functionality
3	Establish a theory of probable cause
4	Determine if any recent changes have been made to the server
5	Document findings, actions, and outcomes
6	Establish a plan of action to resolve the problem
7	Test the theory to determine cause
8	Implement preventative measures

Correct Answer:

1. Determine if any recent changes have been made to the server
2. Establish a theory of probable cause
3. Test the theory to determine cause
4. Establish a plan of action to resolve the problem
5. Implement the solution
6. Verify full system functionality
7. Implement preventative measures
8. Document findings, actions, and outcomes

Section: Mix questions
Explanation

Explanation/Reference:

QUESTION 129
DRAG DROP

Drag and drop the fiber cable connection types to the appropriate image.

Select and Place:

| FC | LC(single) | LC(duplex) | SC | ST |

Correct Answer:

ST	SC	LC(single)	LC(duplex)	FC
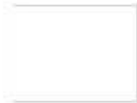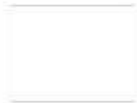
QUESTION 130
DRAG DROP
Build a T-658A Connection

Select and Place:
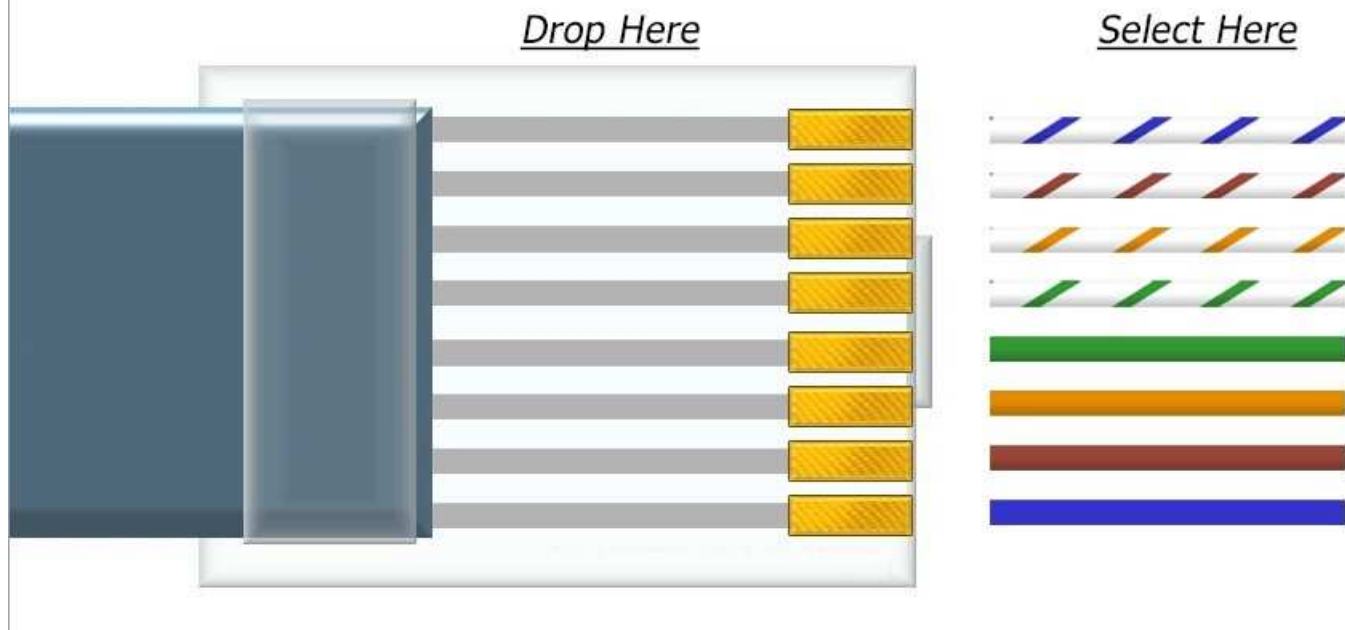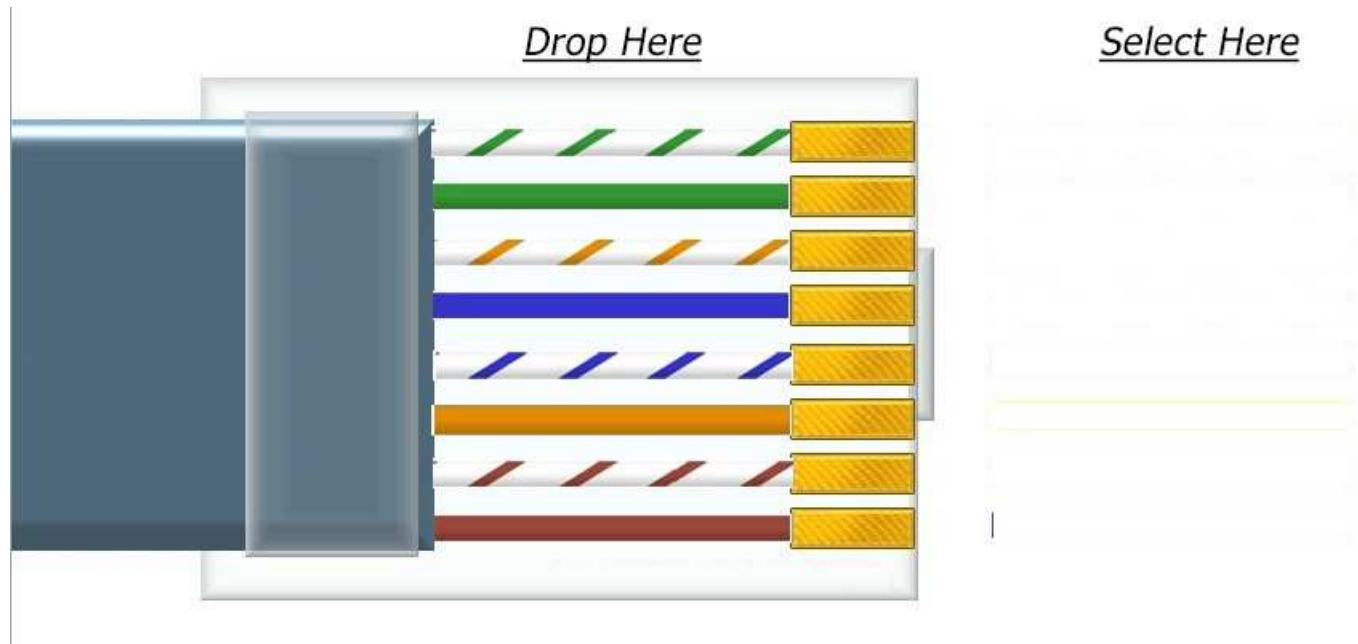
Drop Here   Select Here

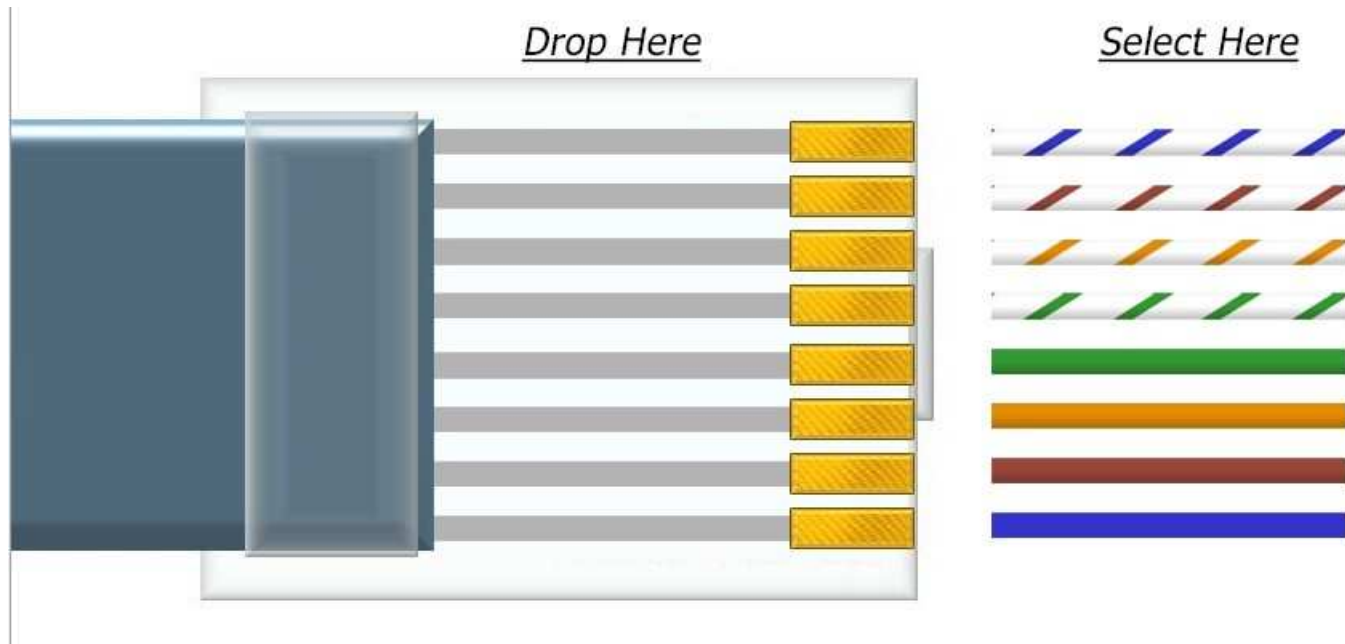**Correct Answer:**

Drop Here   Select Here

Section: Mix questions
Explanation

Explanation/Reference:
Cat5/6 Cable Pinouts

QUESTION 131
DRAG DROP
Build a T-658B Connection

Select and Place:
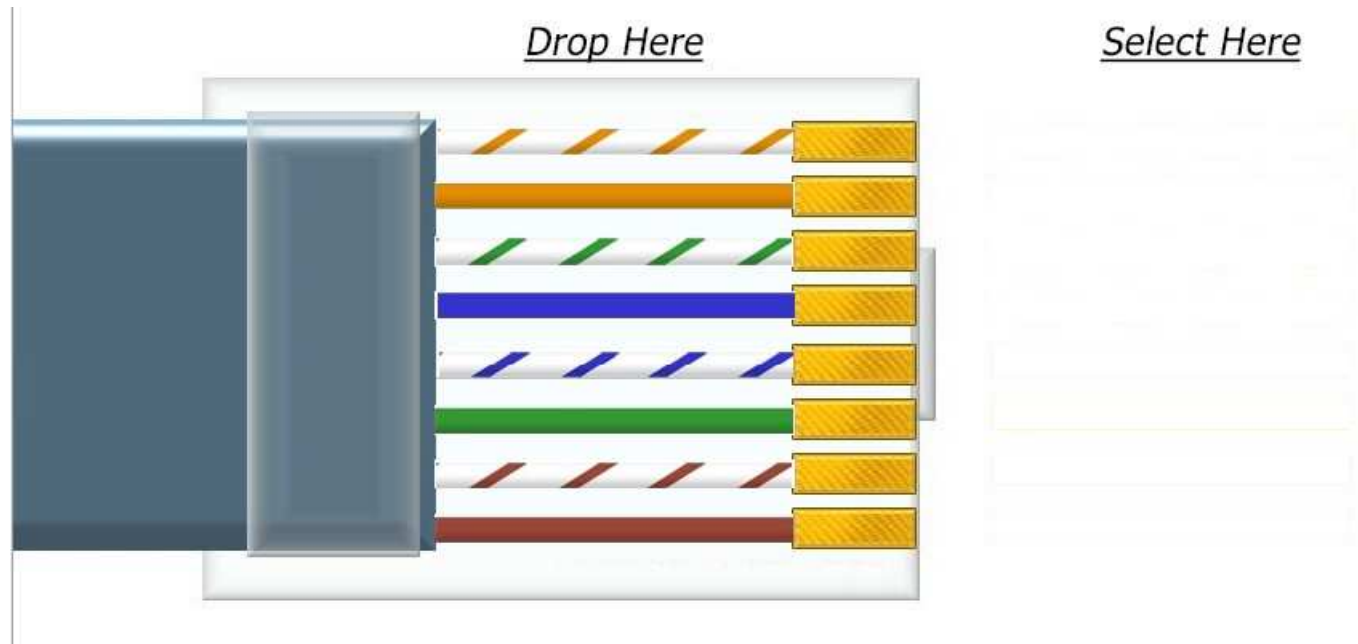
Drop Here
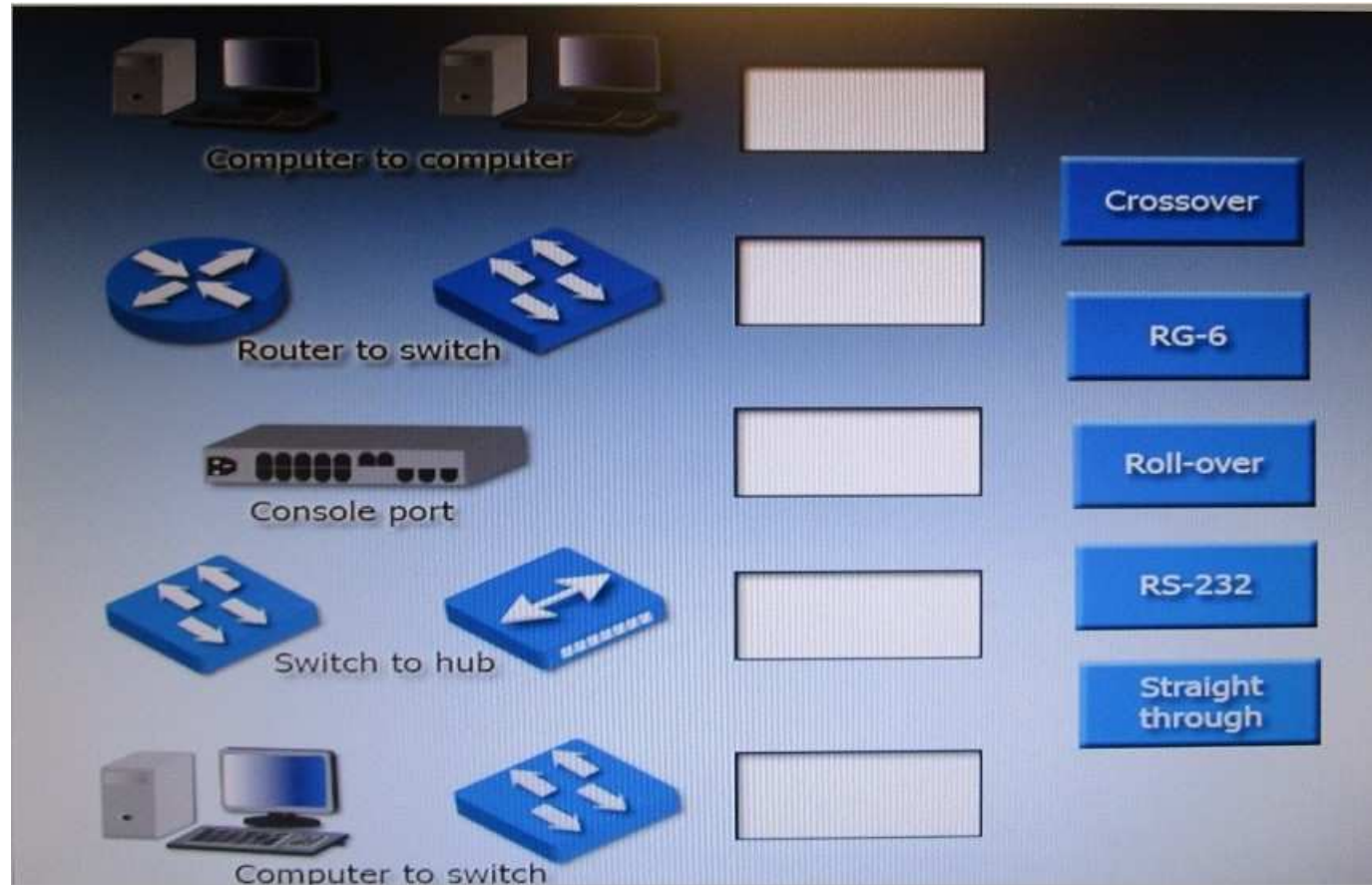
Select Here

Correct Answer:

Drop Here
Select Here

Section: Mix questions
Explanation

Explanation/Reference:
Cat5/6 Cable Pinouts

QUESTION 132
DRAG DROP

Select and Place:

Computer to computer

Router to switch

Console port

Switch to hub

Computer to switch

Crossover

RG-6

Roll-over

RS-232

Straight through
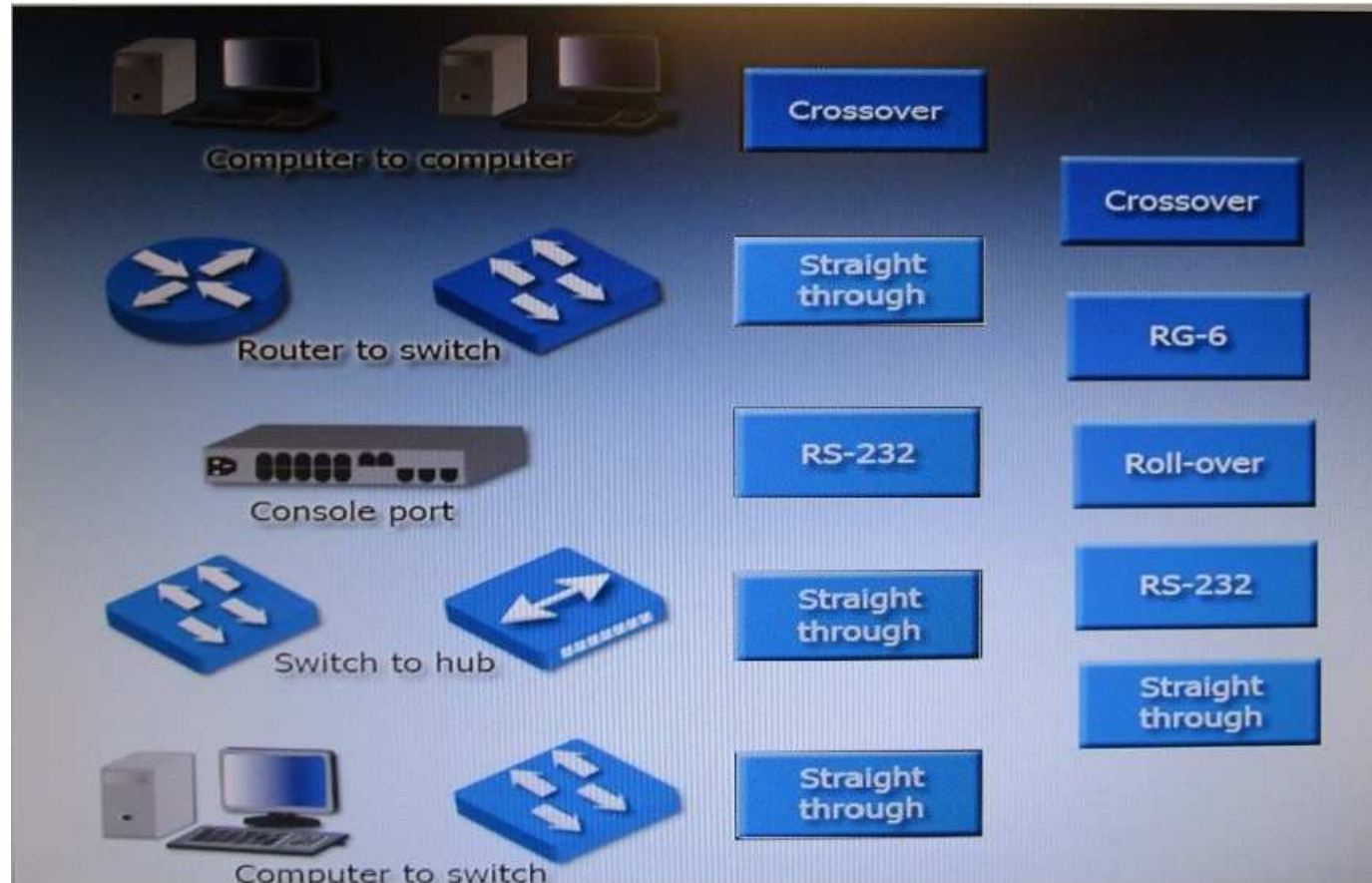
Correct Answer:

Section: Mix questions
Explanation

Explanation/Reference:

QUESTION 133
DRAG DROP

Select and Place:

Correct Answer:

Section: Mix questions
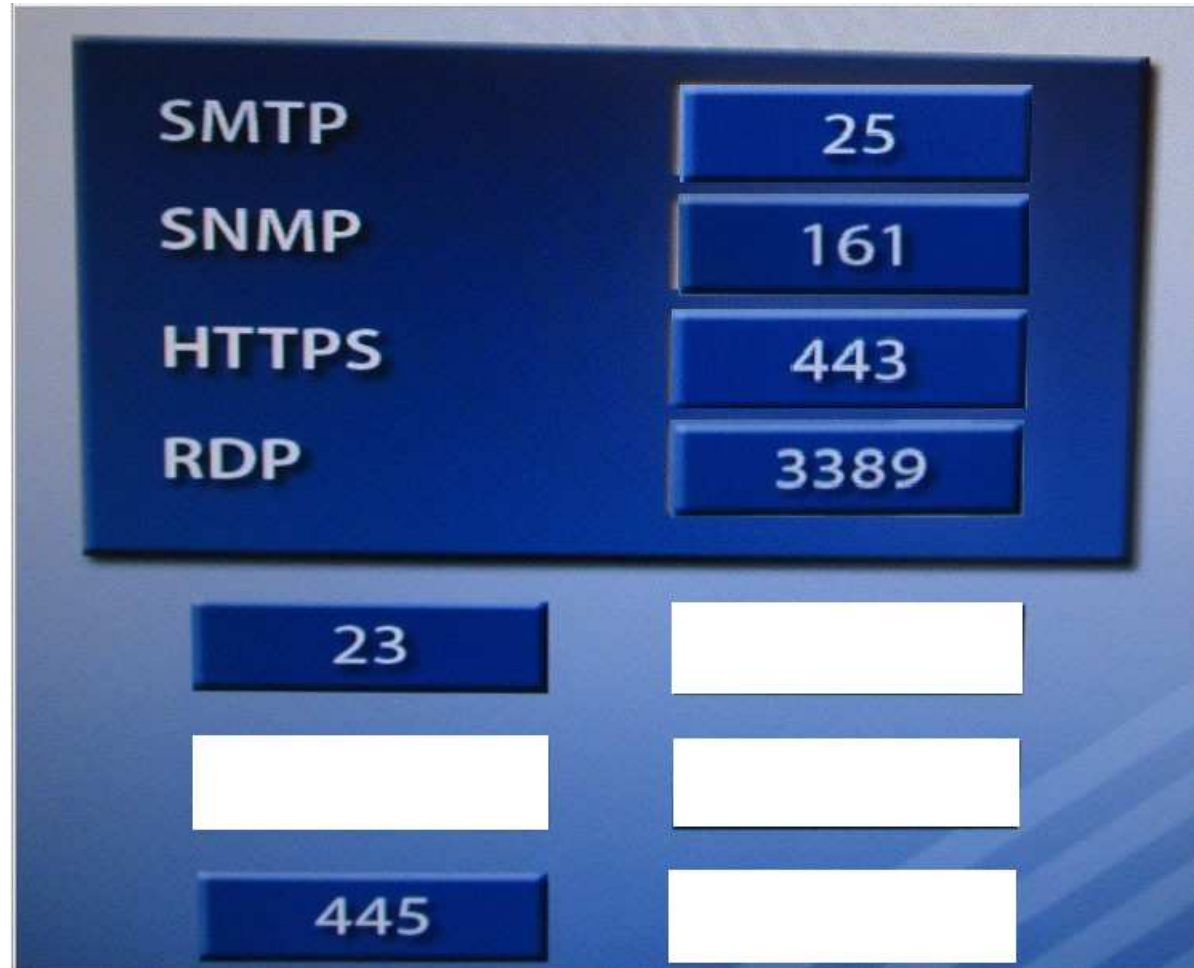**Explanation**

Explanation/Reference:

QUESTION 134
DRAG DROP

You are tasked with creating a network that will accomplish the following requirements

Requirements:

1) The remote sales team must be able to connect to the corporate network
2) Each department must have ONLY two PCs and a server
3) Each department must be segmented from each other
4) The following VLANs have been designated:
a) VLAN 2- Finance
b) VLAN 12- Sales
c) VLAN 22- Human Resources (HR)

Complete the network by dragging the required objects into the diagram

INSTRUCTIONS: Objects can be used multiple times and not all placeholders need to be filled

Select and Place:

Network Diagram

Instructions: Objects can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

Correct Answer:
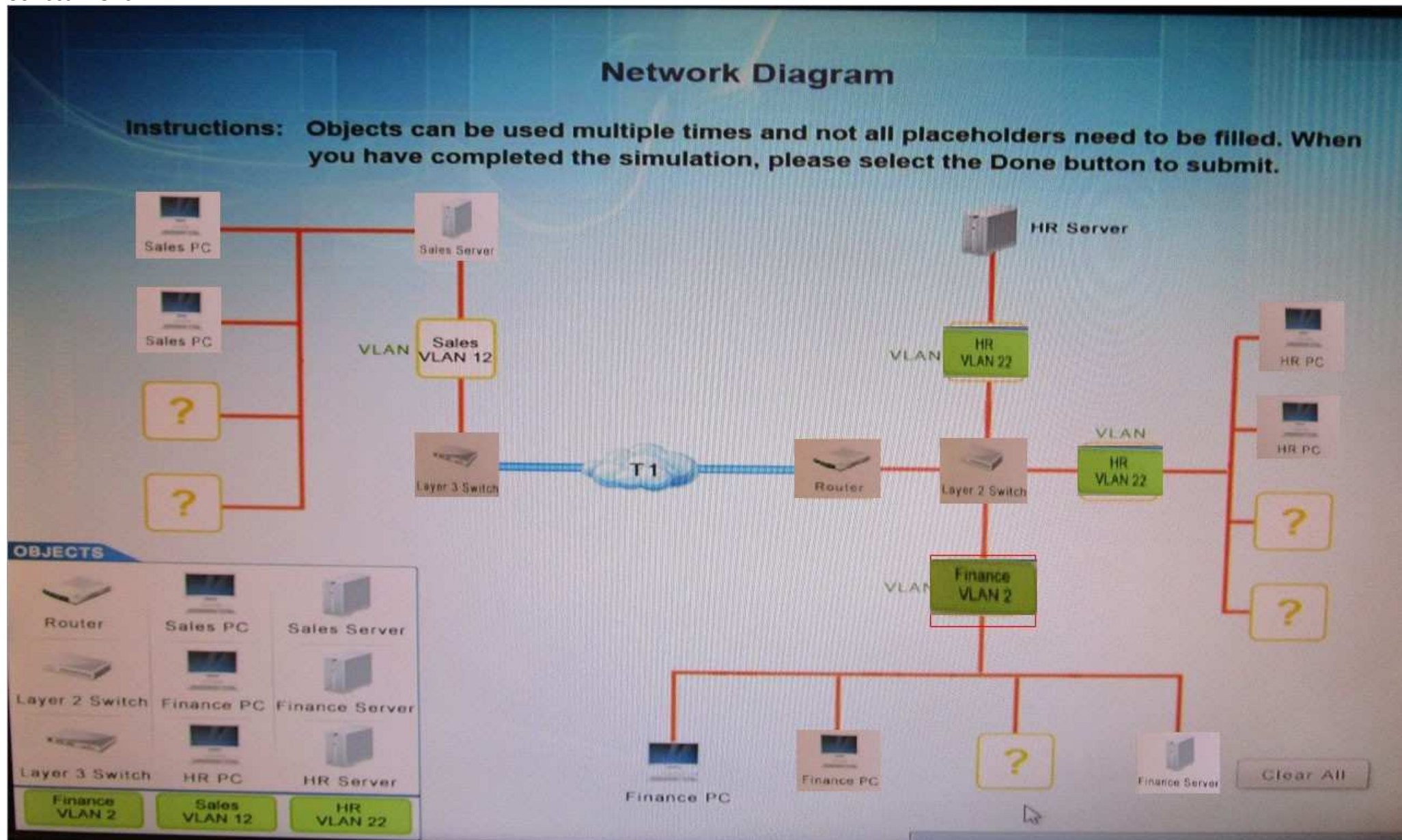

Network Diagram

Instructions: Objects can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.
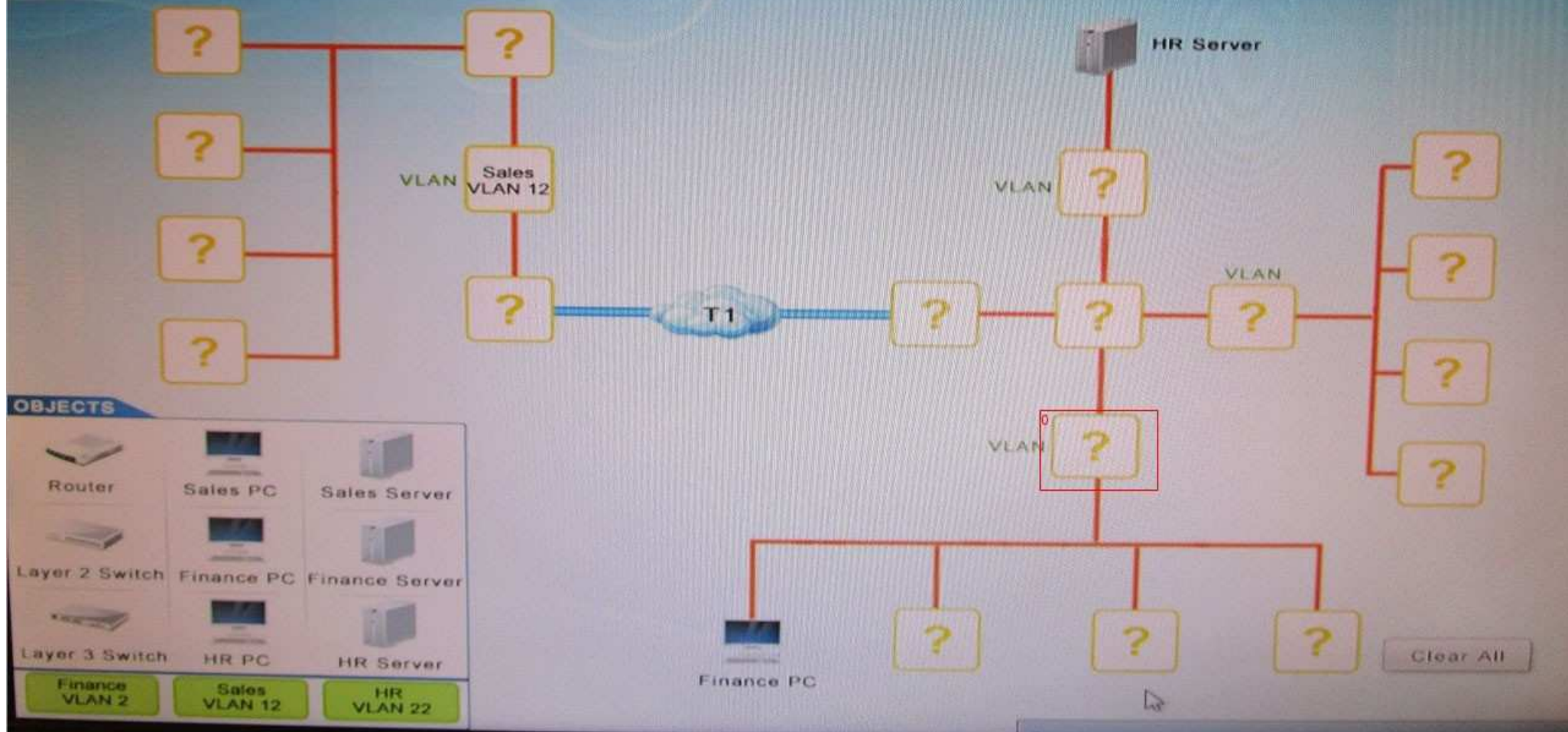
QUESTION 135
CORRECT TEXT
SIMULATION
You have been tasked with setting up a wireless network in an office. The network will consist of 3 access points and a single switch. The network must meet the following parameters.
The SSIDs need to be configured as corpnet with a key of S3cr3t!
The wireless signals should not interfere with each other
The subnet the Access points and Switch are on should only support 30 devices maximum
The access Points should be configured to only support TKIP clients at a maximum speed

Instructions: Click on the devices to review their information and adjust the setting of the APs to meet the given requirements.

Network Diagram

Instructions: Perform changes to the wireless and wired infrastructure by adjusting the devices.

AP Physical Locations
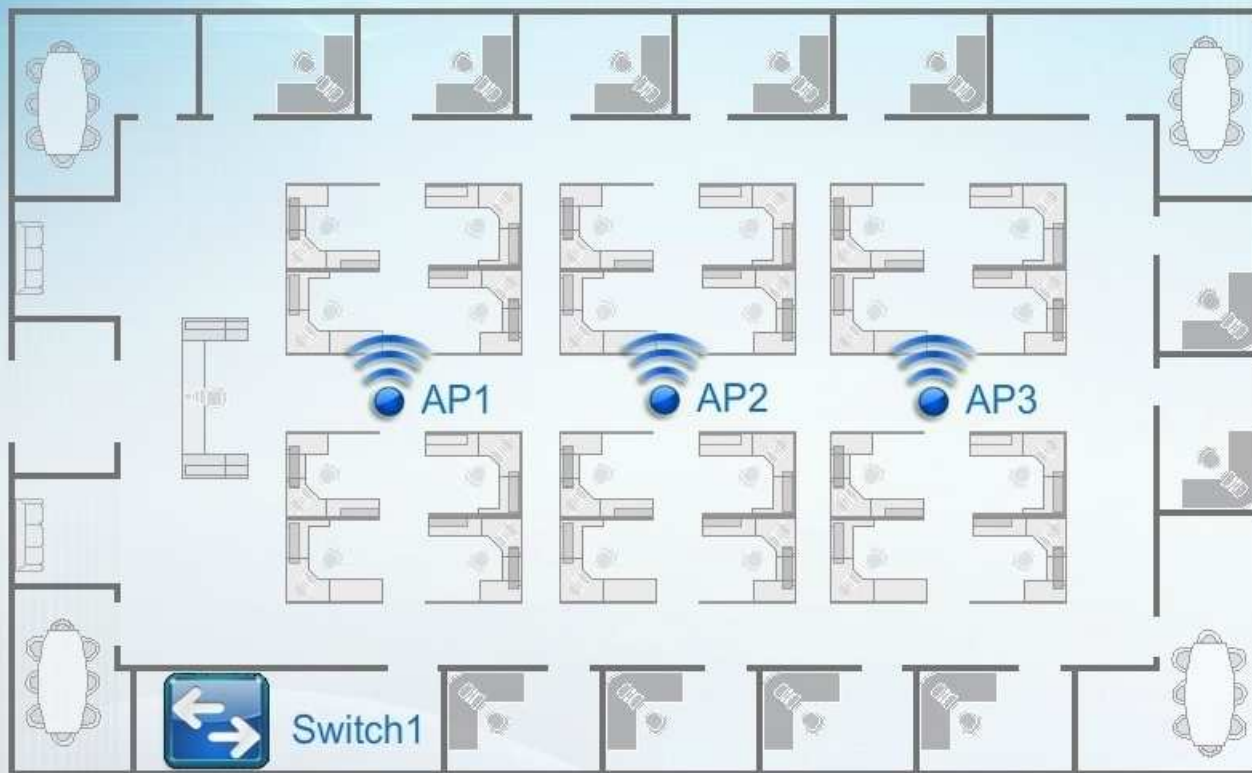
AP1

AP2

AP3

Switch1

Correct Answer: Here is the solution below
Section: Mix questions

Explanation

Explanation/Reference:
Explanation:

This simulation is still under construction. On the first exhibit, the layout should be as follows

Access Point Name AP1
IP Address 192.168.1.3
Gateway 192.168.1.2
SSID corpnet
SSID Broadcast yes

Mode G
Channel 1

Speed Auto
Duplex Auto

WPA
Passphrase S3cr3t!

Exhibit 2 as follows

Access Point Name AP2
IP Address 192.168.1.4
Gateway 192.168.1.2
SSID corpnet
SSID Broadcast yes

Mode G
Channel 6

Speed Auto
Duplex Auto

WPA
Passphrase S3cr3t!

Exhibit 3 as follows

Access Point Name AP3

IP Address 192.168.1.5
Gateway 192.168.1.2
SSID corpnet
SSID Broadcast yes

Mode G
Channel 11

Speed Auto
Duplex Auto

WPA
Passphrase S3cr3t!

QUESTION 136
A company installs a new mail server. Which of the following DNS records need to be configured to allow the organization to receive email?

A. CNAME
B. MX
C. PTR
D. A

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 137
The administrator modifies a rule on the firewall, and now all the FTP users cannot access the server any longer. The manager calls the administrator and asks what caused the extreme downtime for the server. In regards to the manager's inquiry, which of the following did the administrator forget to do FIRST?

A. Submit a change request
B. Schedule a maintenance window
C. Provide notification of change to users
D. Document the changes

Correct Answer: A
Section: Mix questions

Explanation

Explanation/Reference:
Explanation:

QUESTION 138
A network administrator noticed that when one computer goes down, all the other computers in the office will not work. Which of the following topologies is in use?

A. Star
B. Ring
C. Hybrid
D. Bus
E. Mesh

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 139
There has been an increased amount of successful social engineering attacks at a corporate office. Which of the following will reduce this attack in the near future?

A. Helpdesk training
B. Appropriate use policy
C. User awareness training
D. Personal Identifiable Information

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 140
The human resource department has been moved to an area which is more than 60 meters away from the nearest IDF. In order to comply with the SLA which requires that 10Gb speeds be provided, which of the following media will need to utilized?

A. CAT6e
B. CAT5e
C. 802.11n
D. 802.11ac

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 141
While troubleshooting, a technician notices that some clients using FTP still work and that pings to the local router and servers are working. The technician tries to ping all known nodes on the network and they reply positively, except for one of the servers. The technician notices that ping works only when the host name is used but not when FQDN is used. Which of the following servers is MOST likely down?

A. WINS server
B. Domain controller
C. DHCP server
D. DNS server

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 142
An area to which access is controlled by retina scan is protected by which of the following security measure types?

A. Two-factor authentication
B. Biometric
C. Cipher locks
D. Optical reader
E. Proximity reader

Correct Answer: B

QUESTION 143
Which of the following ports should be allowed to provide access to certain VoIP applications?

A. 110
B. 139
C. 1720
D. 5060

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 144
Which of the following should be used to ensure a specific device always receives the same IP address?

A. IP helper
B. Reservation
C. Address lease
D. DHCP scope
E. DHCP relay

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 145
Users connecting to an SSID appear to be unable to authenticate to the captive portal. Which of the following is the cause of this issue?

A. WPA2 security key

B. SSL certificates

C. CSMA/CA

D. RADIUS

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 146
A company owns four kiosks that are in close proximity within a shopping center. The owner is concerned about someone accessing the internet via the kiosk's wireless network. Which of the following should be implemented to provide wireless access only to the employees working at the kiosk?

A. Firewall

B. Web filtering

C. MAC filtering

D. Host-based antivirus

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 147
Which of the following applies to data as it travels from Layer 1 to Layer 7 of the OSI model?

A. Tagging

B. Encapsulation

C. Tunneling

D. De-encapsulation

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 148
A T1 line has lost connectivity to the ISP. The ISP has instructed the technician to place a loopback on a device connecting the T1 line to their central office. On which of the following devices will the technician implement the loopback?

A. Channel remote module

B. Fiber optic modem

C. Channel service unit

D. Digital subscriber line modem

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 149
Routing prefixes which are assigned in blocks by IANA and distributed by the Regional Internet Registry (RIR) are known as which of the following?

A. Network handle

B. Autonomous system number

C. Route aggregation

D. Top level domain

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 150
QoS operates at which of the following OSI model layers? (Select TWO)

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 5
E. Layer 7

Correct Answer: BC
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 151
A client reports that half of the marketing department is unable to access network resources. The technician determines that the switch has failed and needs to replace it. Which of the following would be the MOST helpful in regaining connectivity?

A. VLAN configuration
B. Network diagram
C. Configuration backup
D. Router image

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 152
Ann, a system administrator, is troubleshooting an issue with a DNS server. She notices that the security logs have filled up and that they need to be cleared from the event viewer. She recalls this being a daily occurrence. Which of the following solutions would BEST resolve this problem?

A. Increase the maximum log size

B. Log into the DNS server every hour to check if the logs are full
C. Install an event management tool
D. Delete the logs when full

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 153
Which of the following protocols were designed to avoid loops on a Layer 2 network? (Select TWO)

A. OSPF
B. RIPv2
C. 802.1q
D. Spanning tree
E. 802.1d
F. QoS

Correct Answer: DE
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 154
While implementing wireless access points into the network, one building is having connectivity issues due to light fixtures being replaced in the ceiling, while all other buildings' connectivity is performing as expected. Which of the following should be exchanged on the access points installed in the building with connectivity issues?

A. UTP patch cables
B. Antenna
C. Power adapter
D. Security standard

Correct Answer: B

QUESTION 155
A technician is attempting to resolve an issue with users on the network not being able to access websites. The technician pings the default gateway and DNS servers successfully. Pinging a website by URL is unsuccessful but using a known IP address is successful. Which of the following will resolve the issue?

A. Update the HOST file with the URLs for all websites
B. Use NSLOOKUP to resolve URLs
C. Ensure ICMP messages can pass through the firewall
D. Enable port 53 on the firewall

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 156
The Chief Information Officer (CIO) of an organization is concerned that the current locally-hosted, software threat solution is not agile enough. The CIO points to specific examples of zero-day threats that have recently taken a day or more to receive patches. The IT team is tasked with finding a solution that has a better chance of stopping emerging threats and stopping zero-day threats more quickly. Which of the following solutions would have the BEST chance of meeting these goals?

A. Stateful firewall
B. Premise-based IDS
C. Host-based IDS
D. Cloud-based anti-malware

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 157
A network technician was tasked to install a network printer and share it to a group of five human resource employees. The technician plugged the device into a LAN jack, but was unable to obtain an IP address automatically. Which of the following is the cause of the problem?

A. DNS
B. Wrong TCP port
C. Split horizon
D. DHCP scope

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 158
A technician is configuring a computer lab at a school. The computers need to be able to communicate with each other, but students using the computers should not be able to access the internet. Which of the following rules on the firewall should the technician configure for the lab computers?

A. Block all LAN to LAN traffic
B. Block all LAN to WAN traffic
C. Block all WAN to LAN traffic
D. Block all WLAN to WAN traffic

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 159
A network administrator is noticing slow responds times from the server to hosts on the network. After adding several new hosts, the administrator realizes that CSMA/CD results in network slowness due to congestion at the server NIC. Which of the following should the network administrator do to correct the issue?

A. Add a honeypot to reduce traffic to the server
B. Update the Ethernet drivers to use 802.3
C. Add additional network cards to the server

D. Disable CSMA/CD on the network

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 160
A technician wants to update the organization's disaster recovery plans. Which of the following will allow network devices to be replaced quickly in the event of a device failure?

A. Vendor documentation
B. Archives/backups
C. Proper asset tagging and labeling
D. Network Baseline

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 161
A user is unable to connect to a server in another building. A technician is troubleshooting the issue and determines the following:

1)Client PC 1 has an IP address if 192.168.10.25/25
2)PC 1 can successfully ping its gateway of 192.168.10.1/25 which is an interface of router A
3)Server A is named 'BLDGBFILESRVR01' and has an IP address of 192.168.10.145/25
4) PC 2 with an IP address of 192.168.10.200/25 can successfully ping server A
However, when PC 1 pings server A, it receives a destination host unreachable responds. Which of the following is the MOST likely cause?

A. Link from touter A to PC 1 are on different subnets
B. Link from router A to server A is down
C. Link from PC 1 to router A has duplex issues
D. Link from server A top PC 2 is down

Correct Answer: B

Explanation/Reference:
Explanation:
PC 1 cannot connect to Server A. PC 1 and Server A are on different subnets that are connected by Router A. PC 1 can connect to Router A; therefore there is no problem with the link or IP address configuration between PC 1 and Router A.

PC 2, which is on the same subnet as Server A, can connect to Server A; therefore Server A is up.

As PC 1 can connect to Router A but cannot connect to Server A, and Server A is up; the problem must be the connection (link) between Router A and Server A.

QUESTION 162
A company is having a new T1 line installed. Which of the following will the connection MOST likely terminate to?

A. Core switch
B. MDF
C. Ethernet router
D. IDF

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 163
A technician wants to implement a network for testing remote devices before allowing them to connect to the corporate network. Which of the following could the technician implement?

A. High availability
B. MAN network
C. Quarantine
D. Honeynet

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 164
Which of the following broadband WAN technologies would MOST likely be used to connect several remote branches that have no fiber or satellite connections?

A. OC12
B. POTS
C. WiMax
D. OC3

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 165
A technician is troubleshooting a PC that is having intermittent connectivity issues. The technician notices that the STP cables pairs are not completely twisted near the connector. Which of the following is the issue?

A. Cross-talk
B. 568A/568B mismatch
C. Tx/Rx reverse
D. Split pairs

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 166
Which of the following can be issued from the command line to find the layer 3 hops to a remote destination?

A. traceroute
B. nslookup
C. ping
D. netstat

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 167
A administrator's network has OSPF for the internal routing protocol and has two interfaces that continue to flap. The administrator reviews the following output:
Fast ethernet 0 is up, line protocol is up
Int ip address is 10.20.130.5/25
MTU 1500 bytes, BW10000 kbit, DLY 100 usec
Reliability 255/255, Tx load 1/255, Rx load 1/255
Encapsulation ospf, loopback not set
Keep alive 10
Full duplex, 100Mb/s, 100Base Tx/Fx
Received 1052993 broadcasts
1258 input errors
983881 packet output, 768588 bytes
1747 output errors, 0 collisions, 423 resets
Which of the following problems would cause the interface flap?

A. Wrong IP address
B. Loopback not set
C. Bad wire
D. Incorrect encapsulation
E. Duplex mismatch

Correct Answer: E
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 168
Which of the following allows a telecommunication company to test circuits to customers remotely?

A. VLAN
B. Toner Probe
C. RDP
D. Smart Jack
E. VPN

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 169
A single mode fiber is no longer providing network connectivity to a remote site. Which of the following would be used to identify the location of the break?

A. MT-RJ
B. OTDR
C. Media converter
D. Cable certifier

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 170
Users are reporting extreme slowness across the network every Friday. Which of the following should the network technician review first to narrow down the root cause of the problem?

A. Baseline

B. Bottleneck

C. Utilization

D. Link status

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 171
A contractor was hired to troubleshoot congestion issues on the network. After a few of the switches have been reconfigured/upgraded by the contractor, congestion worsens and collisions increase. Which of the following is the BEST action to alleviate the situation?

A. Allow the contractor to reset switches to factory defaults

B. Check the cabling on all switches for improper crossover use

C. Document the changes that were made

D. Downgrade firmware and restore backup configuration

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 172
An organization is involved in a civil court action and needs to ensure email messages are retained. Which of the following describes the requirement to archive and retain email traffic and other correspondence?

A. Chain of custody

B. Legal hold

C. Divide and conquer

D. Persistent agents

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 173
In the past, a company has experienced several network breaches as a result of end-user actions. To help mitigate future breaches, which of the following documents should the security team ensure are up-to-date and enforced for all employees? (Select TWO)

A. Memorandum of understanding
B. Data classification document
C. Service level agreement
D. Interconnection security agreement
E. Consent to monitor
F. Acceptable use policy

Correct Answer: AF
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 174
The Chief Information Officer (CIO) wants to improve the security of the company's data. Which of the following is a management control that should be implemented to ensure employees are using encryption to transmit sensitive information?

A. Policies
B. VPN
C. HTTPS
D. Standards

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 175
A client reports that half of the office is unable to access a shared resource. Which of the following should be used to troubleshoot the issue?

A. Data backups

B. Network diagrams

C. Baseline information

D. Vendor documentation

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 176
An administrator needs to set up a space in the office where co-workers can relax. The administrator sets up several TV's with interconnected gaming systems in the office. Which of the following did the administrator set up?

A. CAN

B. MAN

C. WAN

D. LAN

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 177
Channel bonding will improve which of the following wireless characteristics?

A. Signal strength

B. Encryption strength

C. Coverage area

D. Connection speed

Correct Answer: D
Section: Mix questions

Explanation

Explanation/Reference:
Explanation:

QUESTION 178
Users have reported poor network performance. A technician suspects a user may have maliciously flooded the network with ping request. Which of the following should the technician implement to avoid potential occurrences from happening in the future?

A. Block all ICMP request
B. Update all antivirus software
C. Remove all suspected users from the network
D. Upgrade firmware on all network cards

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 179
A network technician is troubleshooting a network connection error, when pinging the default gateway no reply is received. The default gateway is found to be functioning properly but cannot connect to any workstations. At which of the following OSI layers could the problem exist? (Select TWO)

A. Presentation
B. Transport
C. Session
D. Data link
E. Application
F. Physical

Correct Answer: DF

Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 180
A technician has determined the most likely cause of an issue and implement a solution. Which of the following is the NEXT step that should be taken?

A. Document the findings, actions, and outcomes
B. Duplicate the problem if possible
C. Verify system functionality
D. Make an archival backup

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 181
An administrator has a physical server with a single NIC. The server needs to deploy two virtual machines. Each virtual machine needs two NIC's, one that connects to the network, and a second that is a server to server heartbeat connection between the two virtual machines. After deploying the virtual machines, which of the following should the administrator do to meet these requirements?

A. The administrator should create a virtual switch for each guest. The switches should be configured for inter-switch links and the primary NIC should have a NAT to the corporate network
B. The administrator should create a virtual switch that is bridged to the corporate network and a second virtual switch that carries intra-VM communication only
C. The administrator should create a virtual switch to bridge all of the connections to the network. The virtual heartbeat NICs should be set to addresses in an unused range
D. The administrator should install a second physical NIC onto the host, and then connect each guest machine's NICs to a dedicated physical NIC

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 182
A network technician is asked to redesign an Ethernet network before new monitoring software is added to each host on the network. The new software will broadcast statistics from each host to a monitoring host for each of the five departments in the company. The added network traffic is a concern of management that must be addressed. Which of the following solutions should the technician design into the new network?

A. Place each department in a separate VLAN
B. Add a router and create a segment for all the monitoring host stations
C. Increase the number of switches on the network to reduce broadcasts
D. Increase the collision domain to compensate for the added broadcasts

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 183
A company has added several new employees, which has caused the network traffic to increase by 200%. The network traffic increase from the new employees was only expected to be 20% to 30%. The administration suspects that the network may have been compromised. Which of the following should the network administrator have done previously to minimize the possibility of a network breach?

A. Create VLANs to segment the network traffic
B. Place a network sniffer on segments with new employees
C. Provide end user awareness and training for employees
D. Ensure best practices were implemented when creating new user accounts

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 184
A network technician discovers an issue with spanning tree on the core switch. Which of the following troubleshooting steps should the network technician perform NEXT to resolve the issue?

A. Test a theory to determine the cause
B. Escalate to a senior technician

C. Identify the symptoms
D. Establish a theory of probable cause
E. Establish a plan of action

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 185
Which of the following would be the BEST addition to a business continuity plan that would protect business from a catastrophic event such as a fire, tornado, or earthquake?

A. UPS and battery backups
B. Fire suppression systems
C. Building generator
D. Hot sites or cold sites
E. NAS and tape backups

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 186
A network technician has created a network consisting of an external internet connection, a DMZ, an internal private network, and an administrative network. All routers and switches should be configured to accept SSH connections from which of the following network segments?

A. The internal network since it is private
B. The admin private network allowing only admin access
C. The DMZ only allowing access from the segment with the servers
D. The internet connection to allow admin access from anywhere

Correct Answer: B
Section: Mix questions

Explanation

Explanation/Reference:
Explanation:

QUESTION 187
A network technician needs to monitor the network to find a user that is browsing inappropriate websites. Which of the following would the technician use to view the website and find the user browsing it?

A. An SNMP GET
B. A top listener tool
C. An intrusion detection system
D. A packet sniffer

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 188
A network administrator receives a call asking for assistance with connecting to the network. The user asks for the IP address, subnet class, and VLAN required to access the network. This describes which of the following attacks?

A. Social engineering
B. Spoofing
C. Zero-day attack
D. VLAN hopping

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 189
Which of the following cloud infrastructure designs includes on premise servers utilizing a centralized syslog server that is hosted at a third party organization for review?

A. Hybrid

B. Public

C. Community

D. Private

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 190
A new threat is hiding traffic by sending TLS-encrypted traffic outbound over random ports. Which of the following technologies would be able to detect and block this traffic?

A. Intrusion detection system

B. Application aware firewall

C. Stateful packet inspection

D. Stateless packet inspection

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 191
The network administrator is configuring a switch port for a file server with a dual NIC. The file server needs to be configured for redundancy and both ports on the NIC need to be combined for maximum throughput. Which of the following features on the switch should the network administrator use?

A. BPDU

B. LACP

C. Spanning tree

D. Load balancing

Correct Answer: B

Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 192
A network technician is using telnet to connect to a router on a network that has been compromised. A new user and password has been added to the router with full rights. The technician is concerned that the regularly used administrator account has been compromised. After changing the password on all networking devices, which of the following should the technician perform to prevent the password for the administrator account from being sniffed on the network?

A. Use SNMPv1 for all configurations involving the router
B. Ensure the password is 10 characters, containing letter and numbers
C. Copy all configurations to routers using TFTP for secuirty
D. Only allow administrators to access routers using port 22

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 193
A network technician has configured a point-to-point interface on a router, however, once the fiber optic cables have been run, the interface will not come up. The technician has cleaned the fiber connectors and used an optical power meter to confirm that light is passing in both directions without excessive loss. Which of the following is the MOST likely cause?

A. Distance limitation
B. Wavelength mismatch
C. cross-talk
D. EMI
E. Macro bend

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 194
A network administrator wants to deploy a wireless network in a location that has too much RF interference at 2.4 GHz. Which of the following standards requires the use of 5 GHz band wireless transmissions? (Select TWO)

A. 802.11a
B. 802.11ac
C. 802.11b
D. 802.11g
E. 802.11n

Correct Answer: AB
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 195
Upon arrival at work, an administrator is informed that network users cannot access the file server. The administrator logs onto the server and sees the updates were automatically installed and the network connection shows limited and no availability. Which of the following needs to be rolled back?

A. The browser on the server
B. The server's NIC drivers
C. The server's IP address
D. The antivirus updates

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 196
A network engineer is conducting an assessment for a customer that wants to implement an 802.11n wireless network. Before the engineer can estimate the number of WAPs needed, it is important to reference which of the following?

A. Network diagram
B. Site survey
C. Network topology
D. PoE requirements

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 197
Which of the following default ports is associated with protocols that are connectionless?

A. 80
B. 443
C. 2427
D. 3389

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 198
A company is implementing enhanced user authentication for system administrators accessing the company's confidential servers. Which of the following would be the BEST example of two-factor authentication?

A. ID badge and keys
B. Password and key fob
C. fingerprint scanner and retina scan

D. Username and password

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 199
A company that was previously running on a wired network is performing office-wide upgrades. A department with older desktop PC's that do not have wireless capabilities must be migrated to the new network, ensuring that all computers are operating on a single network. Assuming CAT5e cables are available, which of the following network devices should a network technician use to connect all the devices to the wireless network?

A. Wireless bridge
B. VPN concentrator
C. Default WAP
D. Wireless router

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 200
Which of the following integrity security mechanisms ensures that a sent message has been received intact, by the intended receiver?

A. IPSEC
B. SHA
C. DES
D. CRC

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 201

A technician installs a new piece of hardware and now needs to add the device to the network management tool database. However, when adding the device to the tool using SNMP credentials, the tool cannot successfully interpret the results. Which of the following would need to be added to the network management tool to allow it to interpret the new device and control it using SNMP?

A. TRAP
B. GET
C. MIB
D. WALK

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 202

Which of the following communication technologies is used by video conferencing systems to synchronize video streams, and reduce bandwidth, sent by a central location to subscribed devices?

A. Anycast
B. Unicast
C. CoS
D. QoS
E. Multicast

Correct Answer: E
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 203

Which of the following is a UC application?

A. Softphone

B. Intranet

C. Proxy

D. Facsimile

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 204
A company is installing several APs for a new wireless system that requires users to authenticate to the domain. The network technician would like to authenticate to a central point. Which of the following would work BEST to achieve these results?

A. A TACACS+ device and a RADIUS server

B. A TACACS and a proxy server

C. A RADIUS server and an access point

D. A RADIUS server and a network controller

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 205
A network technician is replacing security devices that protect the DMZ for a client. The client has an application that allows external users to access the application remotely. After replacing the devices, the external users are unable to connect remotely to the application. Which of the following is MOST likely misconfigured?

A. Content filter

B. Firewall

C. DNS

D. DHCP

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 206
A technician is dispatched to investigate sporadic network outages. After looking at the event logs of the network equipment, the technician finds that all of the equipment is restarting at the same time every day. Which of the following can the technician deploy to correct this issue?

A. Grounding bar
B. Rack monitoring
C. UPS
D. Air flow management
E. Surge protector

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 207
A network technician needs to protect IP based servers in the network DMZ from being discovered by an intruder utilizing a ping sweep. Which of the following should the technician do to protect the network from ping sweeps?

A. Block echo replies inbound to the DMZ
B. Disable UDP on the servers
C. Block ICMP at the firewall
D. Disable TCP/IP on the server

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 208
Which of the following 802.11g antennas broadcast an RF signal in a specific direction with a narrow path?

A. Omni-direction
B. Unidirectional
C. Patch
D. Yagi

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 209
A network administrator notices that the border router is having high network capacity loads during non-working hours which is causing web services outages.
Which of the following is the MOST likely cause?

A. Evil twin
B. Session hijacking
C. Distributed DoS
D. ARP cache poisoning

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 210
A client is receiving certificate errors in other languages when trying to access the company's main intranet site. Which of the following is MOST likely the cause?

A. DoS
B. Reflective DNS
C. Man-in-the-middle
D. ARP poisoning

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 211
A technician add memory to a router, but that memory is never recognized by the router. The router is then powered down, and the technician relocates all of the memory to different modules. On startup, the router does not boot and displays memory errors. Which of the following is MOST likely the cause?

A. VTP
B. Driver update
C. ESD
D. Halon particles

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 212
An additional network segment is urgently needed for QA testing on the external network. A software release could be impacted id this change is not immediate. The request come directly from management, and there is no time to go through the emergency change control process. Given this scenario, which of the following is the BEST course of action for the network administrator to take?

A. Wait until the maintenance window, and make the requested change
B. First document the potential impacts and procedures related to the change
C. Send out a notification to the company about the change
D. Make the change, noting the requester, and document all network changes

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 213
A technician who is working with a junior member of the team is called away for another issue. The junior technician orders an SC 80/125 fiber cable instead of an ST 80/125. Which of the following will MOST likely be an issue with the new cable?

A. Wavelength mismatch
B. Distance limitations
C. Connector mismatch
D. Attenuation/Db loss:

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 214
Which of the following is a document that is used in cyber forensics that lists everywhere evidence has been?

A. Warrant
B. Legal document
C. Chain of custody
D. Forensic report
E. Documentation of the scene

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 215
QoS operates at which of the following OSI model layers? (Select TWO)

A. Layer 1

B. Layer 2
C. Layer 3
D. Layer 4
E. Layer 5

Correct Answer: BC
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 216
Which of the following is considered a classless routing protocol?

A. IGRP
B. IS-IS
C. RIPv1
D. STP

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 217
A network technician needs to set up two public facing web servers and watns to ensure that if they are compromised the intruder cannot access the intranet. Which of the following security techniques should be used?

A. Place them behind honeypots
B. Place them in a separate subnet
C. Place them between two internal firewalls
D. Place them in the demilitarized zone

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 218
A company has a network with three switches, each one with eight ports. The switch is connected to a router that has a hub with four computers plugged into one of its interfaces. How many broadcast domains are present in this company's network

A. 1
B. 2
C. 5
D. 16
E. 28

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 219
A company plan established to resume normal system operations following a disruption in business would be described as which of the following?

A. First responders
B. User awareness training
C. Disaster recovery
D. Business continuity

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 220
A client is concerned about a hacker compromising a network in order to gain access to confidential research data. Which of the following could be implemented to redirect any attackers on the network?

A. DMZ

B. Content Filter

C. Botnet

D. Honeypot

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 221
A technician installs a new WAP and users in the area begin to report poor performance. The technician uses a ping and 3 of 5 packets respond. Testing from a wired connection shows 5 of 5 packets respond. Which of the following tools should be used to discover the cause of the poor performance?

A. Port scanner tool

B. Interface monitoring tool

C. Packet capture tool

D. Spectrum Analyzer tool

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 222
A network technician has just received an email regarding a security issue detected on the company's standard web browser. Which of the following will MOST likely fix the issue?

A. Firmware update

B. OS update

C. Vulnerability patch

D. Driver update

Correct Answer: C
Section: Mix questions

Explanation

Explanation/Reference:
Explanation:

QUESTION 223
There is a network looping problem after installing some switches. The switch vendor suggested the use of 802.1d. Which of the following is the MOST probable reason the vendor made this suggestion?

A. It is a rapid version of spanning tree that uses BPDU to detect problems
B. It is a regular version of port mirroring that uses hellow packets to detect loops
C. It is a simple version of spanning tree that uses BPDU to detect problems
D. It is a rapid version of port mirroring that uses BPDU to detect problems

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 224
A NAC service has discovered a virus on a client laptop. In which of the following locations would the NAC service place the laptop?

A. On the DMZ network
B. On the sandbox network
C. On the honeypot
D. On the quarantine network

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 225
A company utilizes a patching server to regularly update their PC's. After the latest round of patching all of the older PCs with non-gigabit Ethernet cards become disconnected from the network and now require a technician to fix the issue locally at each PC. Which of the following should be done to prevent this issue in the future?

A. Enable automatic rebooting of the pCs after patching is completed

B. Require the patching server to update the oldest PCs off hours

C. Disable automatic driver updates to PCs on the patching server

D. Throttle the connection speed of the patching server to match older PCs

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 226
A technician has punched down only the middle two pins (pins 4 and 5) on an ethernet patch panel. The technician has cabled this port to be used with which of the following?

A. 10baseT

B. POTS

C. 568B

D. 568A

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 227
Which of the following protocols is used to encapsulate other network layer protocols such as multicast and IPX over WAN connections?

A. MPLS

B. ESP

C. GRE

D. PPP

Correct Answer: C
Section: Mix questions

Explanation

Explanation/Reference:
Explanation:

QUESTION 228
A network technician is tasked with designing a firewall to improve security for an existing FTP server that is on the company network and is accessible from the internet. The security concern is that the FTP server is compromised it may be used as a platform to attack other company servers. Which of the following is the BEST way to mitigate this risk?

A. Add an outbound ACL to the firewall
B. Change the FTP server to a more secure SFTP
C. Use the implicit deny of the firewall
D. Move the server to the DMZ of the firewall

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 229
A network administrator received the following email from a user:
From: user@company.com
To: abuse@company.com
Subject: Free smart phone
Dear, user, please click the following link to get your free smart phone http://www.freesmartphone.it:8080/survey.php

Which of of the following should the administrator do to prevent all employees from accessing the link in the above email, while still allowing Internet access to the freesmartphone.it domain?

A. Add http://www.freesmartphone.it:8080/survey.php to the browser group policy block list.
B. Add DENY TCP http://www.freesmartphone.it ANY EQ 8080 to the firewall ACL

C. Add DENY IP ANY ANY EQ 8080 to the intrusion detection system filter
D. Add http://www.freesmartphone.it:8080/survey.php to the load balancer

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 230
Which of the following types of equipment should be used for telecommunications equipment and have an open design?

A. 2/4 post racks
B. Rail Racks
C. Vertical frame
D. Ladder racks

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 231
A facility would like to verify each individual's identity prior to allowing access to the datacenter. Additionally,the facility would like to ensure that users do not tailgate behind other users. Which of the following would BEST meet these goals?

A. Implement a biometric reader at the datacenter entrance and require passage through a mantrap
B. Implement a security guard at the facility entrance and a keypad on the datacenter entrance
C. Implement a CCTV camera and a proximity reader on the datacenter entrance
D. Implement a biometric reader at the facility entrance and a proximity card at the datacenter entrance

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:

Explanation:

QUESTION 232
A network technician needs to connect two switches. The technician needs a link between them which is capable of handling 10gb. Which of the following media would be optimal for this application?

A. CAT5e cable
B. Coax cable
C. Fiber Optic cable
D. CAT6 cable

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 233
Joe, and administrator, is setting up three more switches in the test lab and is configuring the switches. He is verifying the connectivity but when he pings one of the switches he receives "Destination Unreachable". Which of the following issues could this be?

A. Denial of service attack
B. Misconfigured DNS settings
C. Misconfigured Split Horizon
D. RADIUS authentication errors

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 234
A company is selecting a fire suppression system for their new datacenter and wants to minimize the IT system recovery period in the event of a fire. Which of the following is the best choice for the fire suppression system?

A. Portable extinguishers
B. Wet Pipe

C. Clean Gas
D. Dry Pipe

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 235
Which of the following BEST describes the process of documenting everyone who has physical access or possession of evidence

A. Legal hold
B. Chain of custody
C. Secure copy protocol
D. Financial responsiblity

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 236
A network technician must allow use of HTTP from the internet to an internal resource running HTTP. This is an example of which of the following?

A. Dynamic DNS
B. Virtual Private networking (VPN)
C. Dynamic NAT
D. Port Forwarding

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 237
A network topology in which all nodes have point to point connections to all other nodes is known as which of the following?

A. Mesh
B. Ring
C. Bus
D. Star

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 238
A technician needs to install a server to authenticate remote users before they have access to corporate network resources when working from home. Which of the following servers should the technician implement?

A. DNSSEC
B. PPP
C. RAS
D. VLAN
E. NAT

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 239
While monitoring the network, a technician notices that the network traffic to one of the servers is extremely high. Which of the following should the technician use to verify if this is a concern?

A. Log management
B. Network diagram

C. Network baseline

D. Real time monitor

Correct Answer: C
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 240
A network administrator is tasked with building a wireless network in a new adjacent building. Wireless clients should not have visibility to one another but should have visibility to the wired users. Users must seamlessly migrate between the two buildings while maintaining a connection to the LAN. Which of the following is the BEST way to configure the new wireless network in the new building?

A. Use the same SSIDs on different channels and AP isolation

B. Use different SSIDs on different channels and VLANs

C. Use different SSIDs on the same channels with VLANs

D. Use the same SSIDs on same channels with AP isolation

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 241
A customer is attempting to download a file from a remote FTP server, but receives an error that a connection cannot be opened. Which of the following should be one FIRST to resolve the problem?

A. Ensure that port 20 is open

B. Ensure that port 161 is open

C. Flush the DNS cache on the local workstation

D. Validate the security certificate from the host

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 242
OFDM, QAM and QPSK are all examples of which of the following wireless technologies?

A. Frequency
B. Modulation
C. RF interference
D. Spectrum

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 243
A network administrator is following best practices to implement firewalls, patch management and policies on the network. Which of the following should be performed to verify the security controls in place?

A. Penetration testing
B. AAA authentication testing
C. Disaster recovery testing
D. Single point of failure testing

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 244
Which of the following is a connectionless protocol? (Select TWO)

A. ICMP
B. SSL

C. TCP
D. SSH
E. HTTP
F. UDP

Correct Answer: AF
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 245
Ann, a network technician is preparing to configure a company's network. She has installed a firewall to allow for an internal DMZ and external network. No hosts on the internal network should be directly accessible by IP address from the internet, but they should be able to communicate with remote networks after receiving a proper IP address. Which of the following is an addressing scheme that will work in this situation?

A. Teredo tunneling
B. Private
C. APIPA
D. Classless

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 246
A company has just implemented VoIP. Prior to the implementation, all of the switches were upgraded to layer 3 capable in order to more adequately route packages. This is an example of which of the following network segmentation techniques?

A. Compliance implementation
B. Separate public/private newtorking
C. Honeypot implementation
D. Performance optimization

Correct Answer: D

QUESTION 247
A malicious student is blocking mobile devices from connecting to the internet when other students are in the classroom. Which of the following is the malicious student implementing?

http://www.gratisexam.com/

A. Removing the AP from the classroom
B. ACL
C. Jamming
D. Firewall
E. IPS

Correct Answer: C

QUESTION 248
A technician configures a firewall in the following manner in order to allow HTTP traffic
Source IPZone Dest IPZonePortAction
AnyUntrustAnyDMZ80Allow
The organization should upgrade to which of the following technologies to prevent unauthorized traffic from traversing the firewall?

A. HTTPS
B. Stateless packet inspection
C. Intrusion detection system
D. Application aware firewall

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 249
Exploiting a weakness in a user's wireless headset to compromise the mobile device is known as which of the following?

A. Multiplexing
B. Zero-day attack
C. Smurfing
D. Bluejacking

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 250
A technician is concerned about security and is asked to set up a network management protocol. Which of the following is the best option?

A. SLIP
B. SNMPv3
C. TKIP
D. SNMPv2

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 251
A network technician wants to allow HTTP traffic through a stateless firewall. The company uses the 192.168.0.0/24 network. Which of the following ACL should the technician configure? (Select TWO)

A. PERMIT SRCIP 192.168.0.0/24 SPORT:80 DSTIP:192.168.0.0/24 DPORT:80

B. PERMIT SRCIP 192.168.0.0/24 SPORT:ANY DSTIP:ANY DPORT 80

C. PERMIT SRCIP:ANY SPORT:80 DSTIP:192.168.0.0/24 DPORT ANY

D. PERMIT SRCIP: ANY SPORT:80 DSTIP:192.168.0.0/24 DPORT:80

E. PERMIT SRCIP:192.168.0.0/24 SPORT:80 DSTIP:ANY DPORT:80

Correct Answer: B
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 252
A network technician has been asked to make the connections necessary to add video transported via fiber optics to the LAN within a building. Which of the following is the MOST common connector that will be used on the switch to connect the media converter?

A. FDDI

B. Fiber coupler

C. MT-RJ

D. ST

Correct Answer: D
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 253
A technician is troubleshooting a newly installed WAP that is sporadically dropping connections to devices on the network. Which of the following should the technician check FIRST?

A. WAP placement

B. Encryption type

C. Bandwidth saturation

D. WAP SSID

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 254
Which of the following ports is used to provide secure sessions over the web by default?

A. 22
B. 25
C. 80
D. 5004

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 255
An attack where the potential intruder tricks a user into providing sensitive information is known as which of the following?

A. Social engineering
B. Bluesnarfing
C. Man-in-the-middle
D. Evil Twin

Correct Answer: A
Section: Mix questions
Explanation

Explanation/Reference: