



CompTIA

Exam RC0-N06

CompTIA Network+ Recertification Exam for Continuing Education

Version: 7.0

[Total Questions: 470]

Topic break down

Topic	No. of Questions
Topic 1: Network architecture	39
Topic 2: Network operations	29
Topic 3: Network security	29
Topic 4: Troubleshooting	31
Topic 5: Industry standards, practices, and network theory	26
Topic 6: Mix questions	316

Topic 1, Network architecture

Question No : 1 - (Topic 1)

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

Answer: D

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 No : 2 - (Topic 1)

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

Answer: A

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 1KMto 5KM. If multiple buildings have the same domain and they are connected with a network, then it will be considered as a CAN.

Question No : 3 - (Topic 1)

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

Answer: B

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 No : 4 CORRECT TEXT - (Topic 1)

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.

Dumps with PDF and VCE (+Free VCE Software)

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



Explanation:

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

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.

- Correctly crimped cable
- Incorrectly crimped cable

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 No : 5 - (Topic 1)

When convergence on a routed network occurs, which of the following is true?

- A. All routers are using hop count as the metric
- B. All routers have the same routing table
- C. All routers learn the route to all connected networks

D. All routers use route summarization

Answer: C

Explanation:

Routers exchange routing topology information with each other by using a routing protocol. When all routers have exchanged routing information with all other routers within a network, the routers are said to have converged. In other words: In a converged network all routers "agree" on what the network topology looks like.

Question No : 6 - (Topic 1)

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

Answer: C

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 No : 7 - (Topic 1)

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

Answer: A,B,F

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 No : 8 - (Topic 1)

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

Answer: B

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 No : 9 - (Topic 1)

Which of the following would be used in an IP-based video conferencing deployment? (Select TWO).

- A. RS-232
- B. 56k modem
- C. Bluetooth
- D. Codec
- E. SIP

Answer: D,E

Explanation:

The term "codec" is a concatenation of "encoder" and "decoder". In video conferencing, a codec is software (or can be hardware) that compresses (encodes) raw video data before it is transmitted over the network. A codec on the receiving video conferencing device will then decompress (decode) the video signal for display on the conferencing display. The Session Initiation Protocol (SIP) is a protocol for initiating an interactive user session that involves multimedia elements such as voice, chat, gaming, or in this case video.

Question No : 10 - (Topic 1)

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

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

Answer: B

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 No : 11 - (Topic 1)

Which of the following is used to define how much bandwidth can be used by various protocols on the network?

- A. Traffic shaping
- B. High availability
- C. Load balancing
- D. Fault tolerance

Answer: A

Explanation:

If a network connection becomes saturated to the point where there is a significant level of contention, network latency can rise substantially.

Traffic shaping is used to control the bandwidth used by network traffic. In a corporate environment, business-related traffic may be given priority over other traffic. Traffic can be prioritized based on the ports used by the application sending the traffic. Delayed traffic is stored in a buffer until the higher priority traffic has been sent.

Question No : 12 - (Topic 1)

Which of the following provides accounting, authorization, and authentication via a centralized privileged database, as well as, challenge/response and password encryption?

- A. Multifactor authentication
- B. ISAKMP
- C. TACACS+
- D. Network access control

Answer: C

Explanation:

TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol that handles authentication, authorization, and accounting (AAA) services. Similar to RADIUS, TACACS+ is a centralized authentication solution used to provide access to network resources. TACACS+ separates the authentication, authorization, and accounting services enabling you to host each service on a separate server if required.

Question No : 13 HOTSPOT - (Topic 1)

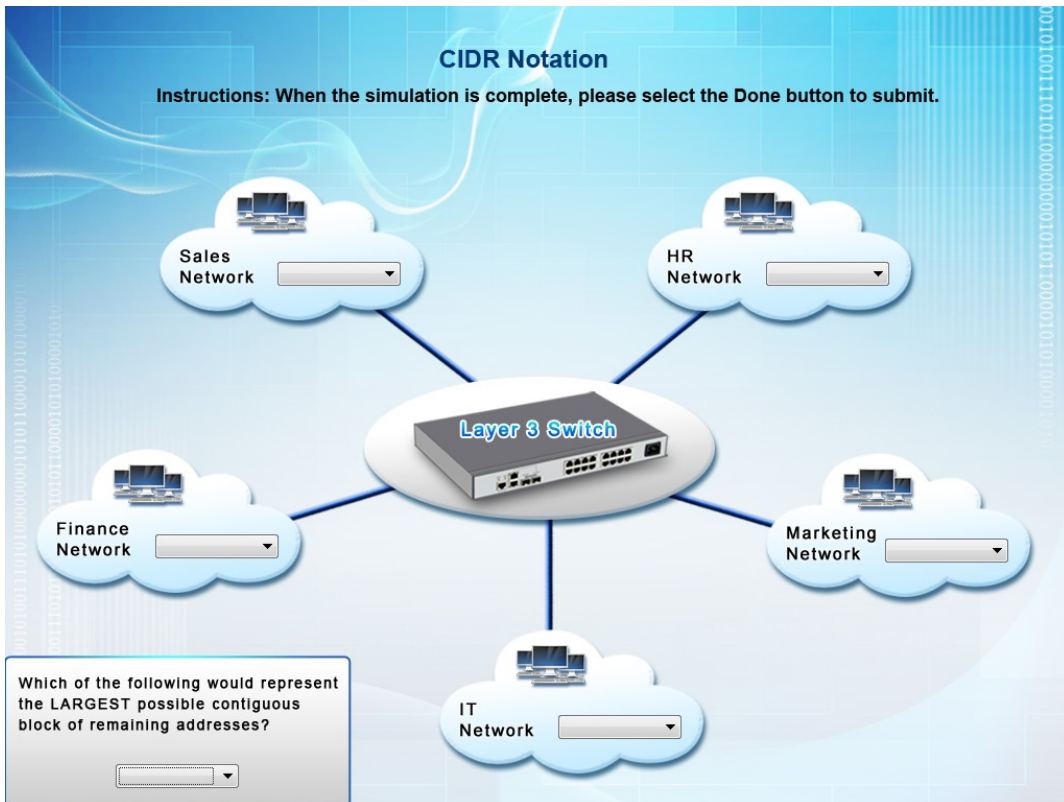
Corporate headquarters provided your office a portion of their class B subnet to use at a new office location. Allocate the minimum number of addresses (using CIDR notation) needed to accommodate each department.

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.



CIDR Notation

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

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

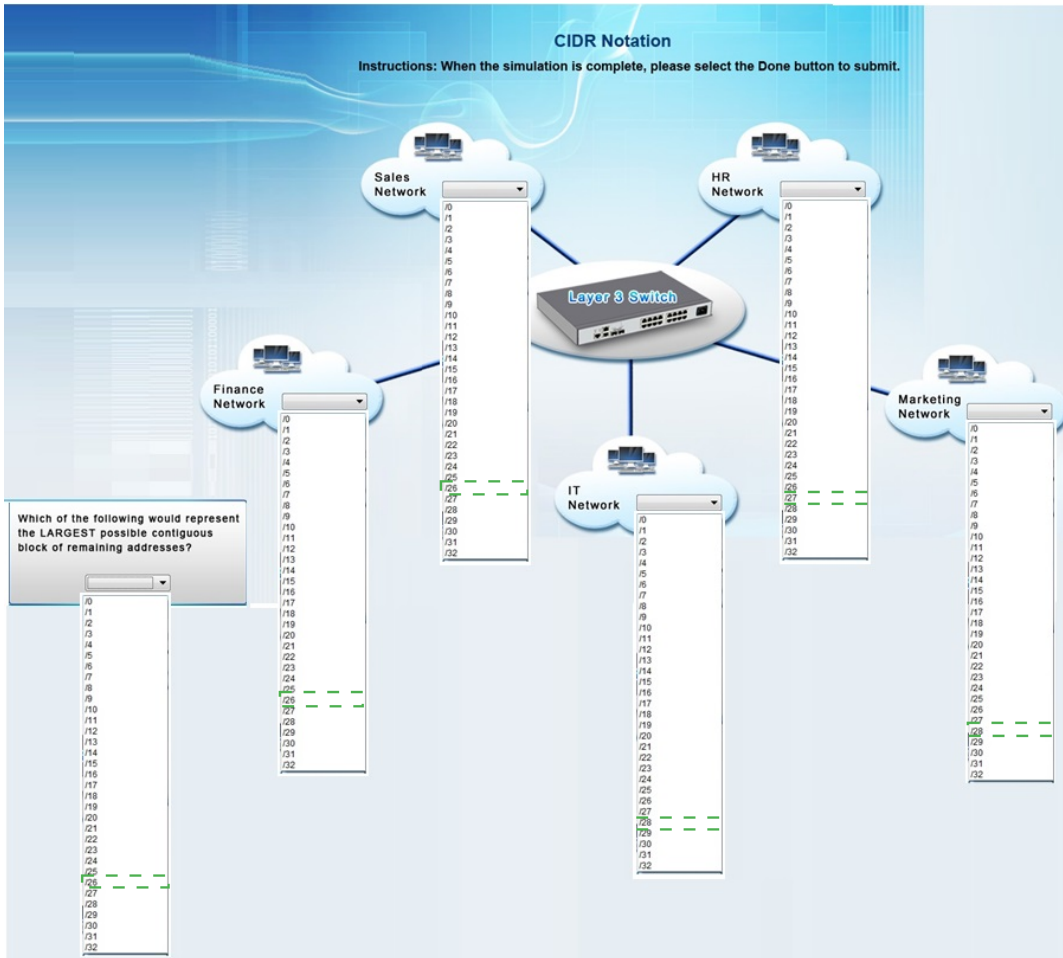
CIDR Notation

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

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

All Networks have the range from /0 to/32

Answer:



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 $2^n - 2$. 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 No : 14 - (Topic 1)

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. Tokenring

Answer: A

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 No : 15 - (Topic 1)

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

Answer: C

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 No : 16 - (Topic 1)

An administrator has a virtualization environment that includes a vSAN and iSCSI switching. Which of the following actions could the administrator take to improve the performance of data transfers over iSCSI switches?

- A.** The administrator should configure the switch ports to auto-negotiate the proper Ethernet settings.
- B.** The administrator should configure each vSAN participant to have its own VLAN.
- C.** The administrator should connect the iSCSI switches to each other over inter-switch links (ISL).
- D.** The administrator should set the MTU to 9000 on the each of the participants in the vSAN.

Answer: D

Explanation:

When using an iSCSI SAN (with iSCSI switching), we can improve network performance by enabling 'jumbo frames'. A jumbo frame is a frame with an MTU of more than 1500. By setting the MTU to 9000, there will be fewer but larger frames going over the network. Enabling jumbo frames can improve network performance by making data transmissions more efficient. The CPUs on switches and routers can only process one frame at a time. By putting a larger payload into each frame, the CPUs have fewer frames to process.

Question No : 17 - (Topic 1)

A SQL server needs several terabytes of disk space available to do an uncompressed backup of a database. Which of the following devices would be the MOST cost efficient to use for this backup?

- A. iSCSI SAN
- B. FCoE SAN
- C. NAS
- D. USB flash drive

Answer: C

Explanation:

A NAS is a Network Attached Storage device; typically a bunch of cheap hard disks, usually arranged in a Raid and consisting of either SAS (serial attached SCSI) or Sata disks just like the ones in most desktops.

A NAS is essentially a file server that connects to an Ethernet network and is configured with a TCP/IP address. A NAS supports Windows networking and works at the file level as opposed to a SAN (Storage Area Network) which works at the block level when dealing with data. You can access file shares on a NAS in the same way that you would access file shares on a file server.

A NAS is a much cheaper option than a SAN.

Question No : 18 - (Topic 1)

Which of the following is used to authenticate remote workers who connect from offsite?
(Select TWO).

- A. OSPF
- B. VTP trunking
- C. Virtual PBX
- D. RADIUS
- E. 802.1x

Answer: D,E

Explanation:

D: A RADIUS (Remote Authentication Dial-in User Service) server is a server with a database of user accounts and passwords used as a central authentication database for users requiring network access. RADIUS servers are commonly used by ISP's to authenticate their customer's Internet connections.

Remote users connect to one or more Remote Access Servers. The remote access servers then forward the authentication requests to the central RADIUS server.

E: 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a network.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client that wishes to attach to the network. The authenticator is a network device, such as an Ethernet switch, wireless access point or in this case, a remote access server and the authentication server is the RADIUS server.

Question No : 19 - (Topic 1)

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

Answer: C

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.

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

Answer: A

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 No : 21 - (Topic 1)

A company has a new offering to provide access to their product from a central location rather than clients internally hosting the product on the client network. The product contains sensitive corporate information that should not be accessible from one client to another. This is an example of which of the following?

- A. Public SaaS
- B. Private SaaS
- C. Hybrid IaaS
- D. Community IaaS

Answer: B

Explanation:

SaaS stands for Software as a Service. This is a cloud model whereby a service provider provides a software service and makes the service available to customers over the Internet. Examples of SaaS include Microsoft Office 365, Microsoft Exchange Online, Microsoft Lync Online etc.

Advantages of SaaS include ease of administration: no need to install and configure local servers, no need to configure backups, no need to keep the software patched, no need to worry about system recovery, lower costs: saving on the purchase of server hardware and software; with SaaS, you lease the service paying either monthly or yearly and compatibility by ensuring that all users are using the same version of software.

There are two types of SaaS: public and private. With public SaaS, multiple customers (usually companies) share the same servers running the software. With private SaaS, the servers running the software are dedicated to a single customer which provides the isolation and extra security required when dealing with sensitive information.

Question No : 22 - (Topic 1)

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

Answer: E

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 $2^n - 2$. The "n" in the host's formula represents the number of bits used for host addressing. If we apply the formula $(2^2 - 2)$, a /30 subnet mask will provide 2 IP addresses.

Question No : 23 - (Topic 1)

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

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

Answer: B

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 No : 24 - (Topic 1)

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

Answer: A

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 No : 25 - (Topic 1)

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

Answer: B,E

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 No : 26 - (Topic 1)

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

Answer: A

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 No : 27 - (Topic 1)

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

- A. CAT3
- B. Single mode fiber
- C. CAT5
- D. RG6

Answer: D

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 No : 28 - (Topic 1)

Which of the following network elements enables unified communication devices to connect to and traverse traffic onto the PSTN?

- A. Access switch
- B. UC gateway
- C. UC server
- D. Edge router

Answer: B

Explanation:

People use many methods of communication nowadays such as voice, email, video and instant messaging. People also use many different devices to communicate such as smart phones, PDAs, computers etc. Unified Communications (UC) enables people using different modes of communication, different media, and different devices to communicate with anyone, anywhere, at any time.

Many communication methods use digital signals. To send a digital signal over the analog PSTN, you need a gateway (in this case a UC Gateway) to convert the digital signals into an analog format that can be sent over the PSTN.

Question No : 29 - (Topic 1)

Which of the following network devices use ACLs to prevent unauthorized access into company systems?

- A. IDS
- B. Firewall
- C. Content filter
- D. Load balancer

Answer: B

Explanation:

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. Firewalls use ACLs (access control lists) to determine which traffic is allowed through the firewall. All traffic entering or leaving the intranet passes through the firewall, which examines each message and blocks or allows the message depending on rules specified in the ACL. The rules in the ACL specify which combinations of source IP address, destination address in IP port numbers are allowed.

Question No : 30 - (Topic 1)

A technician has been given a list of requirements for a LAN in an older building using CAT6 cabling. Which of the following environmental conditions should be considered when deciding whether or not to use plenum-rated cables?

- A. Workstation models
- B. Window placement
- C. Floor composition
- D. Ceiling airflow condition

Answer: D

Explanation:

In a large building, the 'plenum' is the space between floors used to circulate air through the building. This space is also an ideal place to run computer network cabling. However, in the event of fire in the building, the network cables can be very hazardous because when they burn, the cable insulation gives off a poisonous smoke that gets circulated around the building. Furthermore, the burning cables help to spread the fire.

Plenum-rated cables are designed to be cabled through the plenum in a building. Plenum-rated cables are covered in fire-retardant plastic jacket to avoid the risk of toxic smoke being circulated around the building.

QUESTIONNO: 40

A VLAN with a gateway offers no security without the addition of:

- A. An ACL.
- B. 802.1w.
- C. A RADIUS server.
- D. 802.1d.

Answer: A

A gateway in a VLAN connects to another network. The other network can be the Internet, another subnet on the network or another VLAN. The gateway will be a router and for security, it should also be a firewall.

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from

accessing private networks connected to the Internet, especially intranets. Firewalls use ACLs (access control lists) to determine which traffic is allowed through the firewall. All traffic entering or leaving the intranet passes through the firewall, which examines each message and blocks or allows the message depending on rules specified in the ACL. The rules in the ACL specify which combinations of source IP address, destination address in IP port numbers are allowed.

Question No : 31 - (Topic 1)

An organization requires a second technician to verify changes before applying them to network devices. When checking the configuration of a network device, a technician determines that a coworker has improperly configured the AS number on the device. This would result in which of the following?

- A. The OSPF not-so-stubby area is misconfigured
- B. Reduced wireless network coverage
- C. Spanning tree ports in flooding mode
- D. BGP routing issues

Answer: D

Explanation:

BGP (Border Gateway Protocol) is used to route data between autonomous systems (AS's) A collection of networks that fall within the same administrative domain is called an autonomous system (AS).

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).

Question No : 32 - (Topic 1)

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

Answer: A

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 No : 33 - (Topic 1)

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

Answer: B

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 No : 34 - (Topic 1)

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

Answer: B

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 No : 35 - (Topic 1)

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

Answer: D

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 No : 36 - (Topic 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.

Answer: B

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 No : 37 - (Topic 1)

A technician is helping a SOHO determine where to install the server. Which of the following should be considered FIRST?

- A. Compatibility requirements
- B. Environment limitations
- C. Cable length
- D. Equipment limitations

Answer: B

Explanation:

SOHO stands for Small Office / Home Office. A SOHO network is typically a small network. Being a small network, it is unlikely that it will have a datacenter or even a dedicated server room. Any servers installed in the network will still have the same environmental requirements as servers in a large network. The servers should be in a secure isolated

area if required. The servers also need to be kept cool and dry. Therefore, the first consideration in a SOHO office is “Environment limitations”: where the servers and other network hardware will be located.

Question No : 38 - (Topic 1)

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

Answer: D

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 No : 39 - (Topic 1)

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

Answer: D

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 mailserver will then forward the email to the destination mail server.

Topic 2, Network operations

Question No : 40 - (Topic 2)

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.

Answer: A

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 No : 41 - (Topic 2)

A company is experiencing accessibility issues reaching services on a cloud-based system. Which of the following monitoring tools should be used to locate possible outages?

- A. Network analyzer
- B. Packet analyzer
- C. Protocol analyzer
- D. Network sniffer

Answer: A

Explanation:

A network analyzer is a useful tool, helping you do things like track traffic and malicious usage on the network.

Question No : 42 - (Topic 2)

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.

Answer: B

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 No : 43 - (Topic 2)

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

Answer: D

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 No : 44 - (Topic 2)

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

Answer: A

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 No : 45 - (Topic 2)

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.

Answer: D

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 No : 46 - (Topic 2)

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

Answer: C

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 No : 47 - (Topic 2)

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

Answer: D

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 No : 48 - (Topic 2)

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

Answer: A

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 No : 49 - (Topic 2)

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

Answer: C

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 No : 50 - (Topic 2)

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 havenot been installed

Answer: A

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 No : 51 - (Topic 2)

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

Answer: C

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 No : 52 - (Topic 2)

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

Answer: B

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 No : 53 - (Topic 2)

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

Answer: B

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 No : 54 - (Topic 2)

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

Answer: D

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 No : 55 - (Topic 2)

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

Answer: C

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 No : 56 - (Topic 2)

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

Answer: B

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 No : 57 - (Topic 2)

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.

Answer: E

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 No : 58 - (Topic 2)

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

Answer: D

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 No : 59 - (Topic 2)

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

Answer: D

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 No : 60 - (Topic 2)

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

Answer: D

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 No : 61 - (Topic 2)

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

Answer: A

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 No : 62 - (Topic 2)

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

Answer: A

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 No : 63 - (Topic 2)

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

Answer: C

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 No : 64 - (Topic 2)

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

Answer: E

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 No : 65 - (Topic 2)

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

Answer: B

Explanation:

If the encryption is unsecure then we must look forencryption 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 No : 66 - (Topic 2)

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

Answer: A

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 No : 67 - (Topic 2)

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

Answer: B

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 No : 68 - (Topic 2)

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

Answer: D

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.

Topic 3, Network security

Question No : 69 - (Topic 3)

Which of the following concepts are MOST important for a company's long term health in the event of a disaster? (Select TWO).

- A. Redundancy
- B. Implementing acceptable use policy
- C. Offsite backups
- D. Uninterruptable power supplies
- E. Vulnerability scanning

Answer: A,C

Explanation:

In case of disaster you must protect your data. Some of the most common strategies for data protection include:

backups made to tape and sent off-site at regular intervals

backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk

the use of high availability systems which keep both the data and system replicated off-site (making the main site redundant), enabling continuous access to systems and data, even after a disaster.

Question No : 70 - (Topic 3)

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

Answer: C

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 No : 71 - (Topic 3)

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

Answer: B

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 No : 72 - (Topic 3)

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

Answer: C

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 No : 73 - (Topic 3)

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

Answer: A

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 No : 74 - (Topic 3)

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

Answer: C

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 No : 75 - (Topic 3)

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

Answer: B

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 No : 76 - (Topic 3)

A malicious user floods a switch with frames hoping to redirect traffic to the user's server. Which of the following attacks is the user MOST likely using?

- A. DNS poisoning
- B. ARP poisoning
- C. Reflection
- D. SYN attack

Answer: B

Explanation:

Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised.

Question No : 77 - (Topic 3)

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

Answer: C,D,E

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 accessto 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 No : 78 - (Topic 3)

A network technician is assisting the company with developing a new business continuity plan. Which of the following would be an appropriate suggestion to add to the plan?

- A. Build redundant links between core devices
- B. Physically secure all network equipment
- C. Maintain up-to-date configuration backups
- D. Perform reoccurring vulnerability scans

Answer: A

Explanation:

The business continuity plan focuses on the tasks carried out by an organization to ensure that critical business functions continue to operate during and after a disaster.

By keeping redundant links between core devices critical business services can be kept running if one link is unavailable during a disaster.

Question No : 79 - (Topic 3)

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

Answer: C

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 No : 80 - (Topic 3)

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

Answer: A

Explanation:

To protect the computers from employees installing malicious software they download on the internet, anti-malware 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 No : 81 - (Topic 3)

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

Answer: B

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 No : 82 - (Topic 3)

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

Answer: C

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 No : 83 - (Topic 3)

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

Answer: C

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 No : 84 - (Topic 3)

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

Answer: A

Explanation:

Secure SocketsLayer (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 No : 85 - (Topic 3)

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

Answer: D

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 No : 86 - (Topic 3)

Which of the following technologies is designed to keep systems uptime running in the

event of a disaster?

- A. High availability
- B. Load balancing
- C. Quality of service
- D. Caching engines

Answer: A

Explanation:

If a network switch or router stops operating correctly (meaning that a network fault occurs), communication through the network could be disrupted, resulting in a network becoming unavailable to its users. Therefore, network availability, called uptime, is a major design consideration.

Question No : 87 - (Topic 3)

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

Answer: B

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 No : 88 - (Topic 3)

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.

Answer: B

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 No : 89 - (Topic 3)

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

Answer: A

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 AnyDMZ 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 No : 90 - (Topic 3)

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 hashfor each file
- D. Implement a RADIUS authentication

Answer: C

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 No : 91 - (Topic 3)

Which of the following describes a smurf attack?

- A. Attack on a target using spoofed ICMP packets to flood it
- B. Intercepting traffic intended for a target and redirecting it to another
- C. Spoofed VLAN tags used to bypass authentication
- D. Forging tags to bypass QoS policies in order to steal bandwidth

Answer: A

Explanation:

The Smurf Attack is a distributed denial-of-service attack in which largenumbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address.

Most devices on a network will, by default, respond to this by sending a reply to the source

IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

Question No : 92 - (Topic 3)

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

Answer: A

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 No : 93 - (Topic 3)

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

Answer: D

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 No : 94 - (Topic 3)

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

Answer: D

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 No : 95 - (Topic 3)

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

Answer: C

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 No : 96 - (Topic 3)

An organization notices a large amount of malware and virus incidents at one satellite office, but hardly any at another. All users at both sites are running the same company image and receive the same group policies. Which of the following has MOST likely been implemented at the site with the fewest security issues?

- A. Consent to monitoring
- B. Business continuity measures
- C. Vulnerability scanning
- D. End-user awareness training

Answer: D

Explanation:

Users should have security awareness training and should have all accepted and signed

acceptable use policy (AUP) agreements. User awareness training is one of the most significant countermeasures the company can implement.

Question No : 97 - (Topic 3)

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

Answer: B

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.

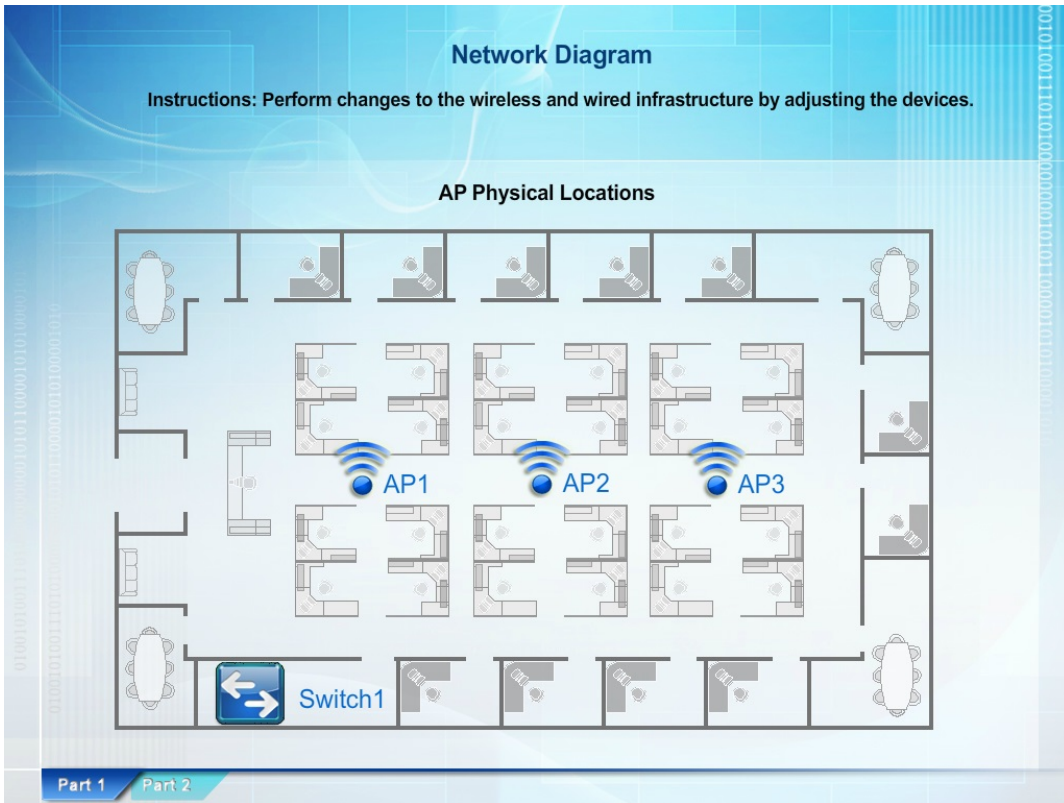
Topic 4, Troubleshooting

Question No : 98 CORRECT TEXT - (Topic 4)

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 diagram 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, all blue icons in the image are clickable. When you feel the simulation is complete please select the Done button.



Wireless AP1 Settings

http://ap1.setup.do

Wireless AP Configuration Settings

Basic Configuration

Access Point Name:

IP Address: /

Gateway:

SSID:

SSID Broadcast: Yes No

Wireless

Mode:

Channel:

Wired

Speed: AUT 10 100

Duplex: AUT Half Full

Security

Security Settings: None WEP WPA

Key or Passphrase:

Wireless AP2 Settings

http://ap2.setup.do

Wireless AP Configuration Settings

Basic Configuration

Access Point Name:

IP Address: /

Gateway:

SSID:

SSID Broadcast: Yes No

Wireless

Mode:

Channel:

Wired

Speed: AUT 10 100

Duplex: AUT Half Full

Security

Security Settings: None WEP WPA

Key or Passphrase:

Dumps with PDF and VCE (+Free VCE Software)

Wireless AP3 Settings

http://ap3.setup.do

Wireless AP Configuration Settings

Basic Configuration

Access Point Name:

IP Address: /

Gateway:

SSID:

SSID Broadcast: Yes No

Wireless

Mode:

Channel:

Wired

Speed: AUT 100n 100n

Duplex: AUT Half Full

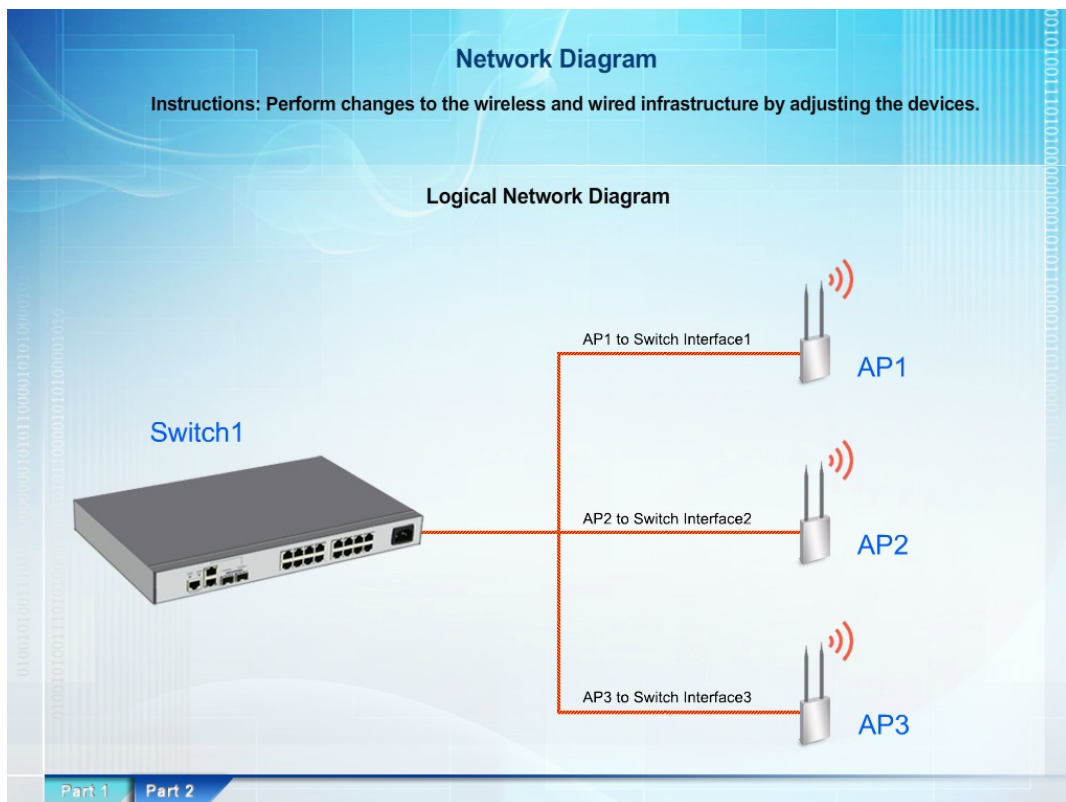
Security

Security Settings: None WEP WPA

Key or Passphrase:

```
SW1# help
sh[ow] int[erfaces]
sh[ow] run[ning] int[erfaces]

SW1#
```



Answer: Here is the solution below.

Explanation:

Since we know that the network was running perfectly before replacing AP2 we should start by looking at this new device that was used to replace the old one. Here we see that the other AP's have hard coded the speed and duplex settings to 100/full, while AP2 is set to auto/auto.

Also, the other AP's have been configured to use 802.11G, while AP2 is using 802.11B.

Finally the channel that AP2 is using overlaps with AP1 which can cause problems.

Channels 1, 6, and 11 are spaced far enough apart that they don't overlap. On a non-MIMO setup (i.e. 802.11 a, b, or g) you should always try to use channel 1, 6, or 11. Since AP1 is using 1, and AP3 is using 11, AP2 should be using 6.

References:

Dulaney, Emmett and Mike Harwood, CompTIA Network+ Authorized Exam Cram, Fourth Edition, Pearson, Indianapolis, 2012, p 269.

Lammle, Todd, CompTIA Network+ Deluxe Study Guide, Deluxe Edition, Wiley Publishing,

Inc., Indianapolis, 2009, pp 676, 677.

http://en.wikipedia.org/wiki/List_of_WLAN_channels#2.4GHz_28802.11b.2Fg.2Fn.2

9

Question No : 99 - (Topic 4)

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

Answer: C

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 No : 100 - (Topic 4)

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?

Answer: C

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 No : 101 - (Topic 4)

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

Answer: B

Explanation:

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

Microsoft Exams List

70-246 Dump PDF VCE	70-485 Dump PDF VCE	70-742 Dump PDF VCE	98-366 Dump PDF VCE
70-247 Dump PDF VCE	70-486 Dump PDF VCE	70-743 Dump PDF VCE	98-367 Dump PDF VCE
70-331 Dump PDF VCE	70-487 Dump PDF VCE	70-744 Dump PDF VCE	98-368 Dump PDF VCE
70-332 Dump PDF VCE	70-488 Dump PDF VCE	70-761 Dump PDF VCE	98-369 Dump PDF VCE
70-333 Dump PDF VCE	70-489 Dump PDF VCE	70-762 Dump PDF VCE	98-372 Dump PDF VCE
70-334 Dump PDF VCE	70-490 Dump PDF VCE	70-765 Dump PDF VCE	98-373 Dump PDF VCE
70-339 Dump PDF VCE	70-491 Dump PDF VCE	70-768 Dump PDF VCE	98-374 Dump PDF VCE
70-341 Dump PDF VCE	70-492 Dump PDF VCE	70-980 Dump PDF VCE	98-375 Dump PDF VCE
70-342 Dump PDF VCE	70-494 Dump PDF VCE	70-981 Dump PDF VCE	98-379 Dump PDF VCE
70-345 Dump PDF VCE	70-496 Dump PDF VCE	70-982 Dump PDF VCE	MB2-700 Dump PDF VCE
70-346 Dump PDF VCE	70-497 Dump PDF VCE	74-343 Dump PDF VCE	MB2-701 Dump PDF VCE
70-347 Dump PDF VCE	70-498 Dump PDF VCE	74-344 Dump PDF VCE	MB2-702 Dump PDF VCE
70-348 Dump PDF VCE	70-499 Dump PDF VCE	74-409 Dump PDF VCE	MB2-703 Dump PDF VCE
70-354 Dump PDF VCE	70-517 Dump PDF VCE	74-678 Dump PDF VCE	MB2-704 Dump PDF VCE
70-383 Dump PDF VCE	70-532 Dump PDF VCE	74-697 Dump PDF VCE	MB2-707 Dump PDF VCE
70-384 Dump PDF VCE	70-533 Dump PDF VCE	77-420 Dump PDF VCE	MB2-710 Dump PDF VCE
70-385 Dump PDF VCE	70-534 Dump PDF VCE	77-427 Dump PDF VCE	MB2-711 Dump PDF VCE
70-410 Dump PDF VCE	70-640 Dump PDF VCE	77-600 Dump PDF VCE	MB2-712 Dump PDF VCE
70-411 Dump PDF VCE	70-642 Dump PDF VCE	77-601 Dump PDF VCE	MB2-713 Dump PDF VCE
70-412 Dump PDF VCE	70-646 Dump PDF VCE	77-602 Dump PDF VCE	MB2-714 Dump PDF VCE
70-413 Dump PDF VCE	70-673 Dump PDF VCE	77-603 Dump PDF VCE	MB2-715 Dump PDF VCE
70-414 Dump PDF VCE	70-680 Dump PDF VCE	77-604 Dump PDF VCE	MB2-716 Dump PDF VCE
70-417 Dump PDF VCE	70-681 Dump PDF VCE	77-605 Dump PDF VCE	MB2-717 Dump PDF VCE
70-461 Dump PDF VCE	70-682 Dump PDF VCE	77-881 Dump PDF VCE	MB2-718 Dump PDF VCE
70-462 Dump PDF VCE	70-684 Dump PDF VCE	77-882 Dump PDF VCE	MB5-705 Dump PDF VCE
70-463 Dump PDF VCE	70-685 Dump PDF VCE	77-883 Dump PDF VCE	MB6-700 Dump PDF VCE
70-464 Dump PDF VCE	70-686 Dump PDF VCE	77-884 Dump PDF VCE	MB6-701 Dump PDF VCE
70-465 Dump PDF VCE	70-687 Dump PDF VCE	77-885 Dump PDF VCE	MB6-702 Dump PDF VCE
70-466 Dump PDF VCE	70-688 Dump PDF VCE	77-886 Dump PDF VCE	MB6-703 Dump PDF VCE
70-467 Dump PDF VCE	70-689 Dump PDF VCE	77-887 Dump PDF VCE	MB6-704 Dump PDF VCE
70-469 Dump PDF VCE	70-692 Dump PDF VCE	77-888 Dump PDF VCE	MB6-705 Dump PDF VCE
70-470 Dump PDF VCE	70-695 Dump PDF VCE	77-891 Dump PDF VCE	MB6-884 Dump PDF VCE
70-473 Dump PDF VCE	70-696 Dump PDF VCE	98-349 Dump PDF VCE	MB6-885 Dump PDF VCE
70-480 Dump PDF VCE	70-697 Dump PDF VCE	98-361 Dump PDF VCE	MB6-886 Dump PDF VCE
70-481 Dump PDF VCE	70-698 Dump PDF VCE	98-362 Dump PDF VCE	MB6-889 Dump PDF VCE
70-482 Dump PDF VCE	70-734 Dump PDF VCE	98-363 Dump PDF VCE	MB6-890 Dump PDF VCE
70-483 Dump PDF VCE	70-740 Dump PDF VCE	98-364 Dump PDF VCE	MB6-892 Dump PDF VCE
70-484 Dump PDF VCE	70-741 Dump PDF VCE	98-365 Dump PDF VCE	MB6-893 Dump PDF VCE

Cisco Exams List

010-151 Dump PDF VCE	350-018 Dump PDF VCE	642-737 Dump PDF VCE	650-667 Dump PDF VCE
100-105 Dump PDF VCE	352-001 Dump PDF VCE	642-742 Dump PDF VCE	650-669 Dump PDF VCE
200-001 Dump PDF VCE	400-051 Dump PDF VCE	642-883 Dump PDF VCE	650-752 Dump PDF VCE
200-105 Dump PDF VCE	400-101 Dump PDF VCE	642-885 Dump PDF VCE	650-756 Dump PDF VCE
200-120 Dump PDF VCE	400-151 Dump PDF VCE	642-887 Dump PDF VCE	650-968 Dump PDF VCE
200-125 Dump PDF VCE	400-201 Dump PDF VCE	642-889 Dump PDF VCE	700-001 Dump PDF VCE
200-150 Dump PDF VCE	400-251 Dump PDF VCE	642-980 Dump PDF VCE	700-037 Dump PDF VCE
200-155 Dump PDF VCE	400-351 Dump PDF VCE	642-996 Dump PDF VCE	700-038 Dump PDF VCE
200-310 Dump PDF VCE	500-006 Dump PDF VCE	642-997 Dump PDF VCE	700-039 Dump PDF VCE
200-355 Dump PDF VCE	500-007 Dump PDF VCE	642-998 Dump PDF VCE	700-101 Dump PDF VCE
200-401 Dump PDF VCE	500-051 Dump PDF VCE	642-999 Dump PDF VCE	700-104 Dump PDF VCE
200-601 Dump PDF VCE	500-052 Dump PDF VCE	644-066 Dump PDF VCE	700-201 Dump PDF VCE
210-060 Dump PDF VCE	500-170 Dump PDF VCE	644-068 Dump PDF VCE	700-205 Dump PDF VCE
210-065 Dump PDF VCE	500-201 Dump PDF VCE	644-906 Dump PDF VCE	700-260 Dump PDF VCE
210-250 Dump PDF VCE	500-202 Dump PDF VCE	646-048 Dump PDF VCE	700-270 Dump PDF VCE
210-255 Dump PDF VCE	500-254 Dump PDF VCE	646-365 Dump PDF VCE	700-280 Dump PDF VCE
210-260 Dump PDF VCE	500-258 Dump PDF VCE	646-580 Dump PDF VCE	700-281 Dump PDF VCE
210-451 Dump PDF VCE	500-260 Dump PDF VCE	646-671 Dump PDF VCE	700-295 Dump PDF VCE
210-455 Dump PDF VCE	500-265 Dump PDF VCE	646-985 Dump PDF VCE	700-501 Dump PDF VCE
300-070 Dump PDF VCE	500-275 Dump PDF VCE	648-232 Dump PDF VCE	700-505 Dump PDF VCE
300-075 Dump PDF VCE	500-280 Dump PDF VCE	648-238 Dump PDF VCE	700-601 Dump PDF VCE
300-080 Dump PDF VCE	500-285 Dump PDF VCE	648-244 Dump PDF VCE	700-602 Dump PDF VCE
300-085 Dump PDF VCE	500-290 Dump PDF VCE	648-247 Dump PDF VCE	700-603 Dump PDF VCE
300-101 Dump PDF VCE	500-801 Dump PDF VCE	648-375 Dump PDF VCE	700-701 Dump PDF VCE
300-115 Dump PDF VCE	600-199 Dump PDF VCE	648-385 Dump PDF VCE	700-702 Dump PDF VCE
300-135 Dump PDF VCE	600-210 Dump PDF VCE	650-032 Dump PDF VCE	700-703 Dump PDF VCE
300-160 Dump PDF VCE	600-211 Dump PDF VCE	650-042 Dump PDF VCE	700-801 Dump PDF VCE
300-165 Dump PDF VCE	600-212 Dump PDF VCE	650-059 Dump PDF VCE	700-802 Dump PDF VCE
300-180 Dump PDF VCE	600-455 Dump PDF VCE	650-082 Dump PDF VCE	700-803 Dump PDF VCE
300-206 Dump PDF VCE	600-460 Dump PDF VCE	650-127 Dump PDF VCE	810-403 Dump PDF VCE
300-207 Dump PDF VCE	600-501 Dump PDF VCE	650-128 Dump PDF VCE	820-424 Dump PDF VCE
300-208 Dump PDF VCE	600-502 Dump PDF VCE	650-148 Dump PDF VCE	840-425 Dump PDF VCE
300-209 Dump PDF VCE	600-503 Dump PDF VCE	650-159 Dump PDF VCE	
300-210 Dump PDF VCE	600-504 Dump PDF VCE	650-281 Dump PDF VCE	
300-320 Dump PDF VCE	640-692 Dump PDF VCE	650-393 Dump PDF VCE	
300-360 Dump PDF VCE	640-875 Dump PDF VCE	650-472 Dump PDF VCE	
300-365 Dump PDF VCE	640-878 Dump PDF VCE	650-474 Dump PDF VCE	
300-370 Dump PDF VCE	640-911 Dump PDF VCE	650-575 Dump PDF VCE	
300-375 Dump PDF VCE	640-916 Dump PDF VCE	650-621 Dump PDF VCE	
300-465 Dump PDF VCE	642-035 Dump PDF VCE	650-663 Dump PDF VCE	
300-470 Dump PDF VCE	642-732 Dump PDF VCE	650-665 Dump PDF VCE	
300-475 Dump PDF VCE	642-747 Dump PDF VCE	650-754 Dump PDF VCE	

HOT EXAMS

Cisco

[100-105 Dumps VCE PDF](#)
[200-105 Dumps VCE PDF](#)
[300-101 Dumps VCE PDF](#)
[300-115 Dumps VCE PDF](#)
[300-135 Dumps VCE PDF](#)
[300-320 Dumps VCE PDF](#)
[400-101 Dumps VCE PDF](#)
[640-911 Dumps VCE PDF](#)
[640-916 Dumps VCE PDF](#)

Microsoft

[70-410 Dumps VCE PDF](#)
[70-411 Dumps VCE PDF](#)
[70-412 Dumps VCE PDF](#)
[70-413 Dumps VCE PDF](#)
[70-414 Dumps VCE PDF](#)
[70-417 Dumps VCE PDF](#)
[70-461 Dumps VCE PDF](#)
[70-462 Dumps VCE PDF](#)
[70-463 Dumps VCE PDF](#)
[70-464 Dumps VCE PDF](#)
[70-465 Dumps VCE PDF](#)
[70-480 Dumps VCE PDF](#)
[70-483 Dumps VCE PDF](#)
[70-486 Dumps VCE PDF](#)
[70-487 Dumps VCE PDF](#)

CompTIA

[220-901 Dumps VCE PDF](#)
[220-902 Dumps VCE PDF](#)
[N10-006 Dumps VCE PDF](#)
[SY0-401 Dumps VCE PDF](#)