

➤ **Vendor: CompTIA**

➤ **Exam Code: N10-006**

➤ **Exam Name: CompTIA Network+ Certification Exam**

➤ **Question 201 -- Question 300**

[Visit PassLeader and Download Full Version N10-006 Exam Dumps](#)

QUESTION 201

Which of the following provides secure access to a network device?

- A. SNMPv2
- B. FTP
- C. RSH
- D. SSH

Answer: D

Explanation:

Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client (running SSH server and SSH client programs, respectively).

QUESTION 202

Which of the following uses distance vector algorithms to determine the BEST network route to a destination address?

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

Answer: D

Explanation:

Here the term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network

QUESTION 203

Which of the following uses classless subnet masks across a network?

- A. Subnetting

- B. CIDR
- C. Supernetting
- D. Summarization

Answer: B

Explanation:

Classless Inter-Domain Routing is based on variable-length subnet masking (VLSM), which allows a network to be divided into variously sized subnets, providing the opportunity to size a network more appropriately for local needs and also CIDR allows an address or routing prefix to be written with a suffix indicating the number of bits of the prefix, such as 192.168.2.0/24.

QUESTION 204

Enterprise IP routing policy is MOST clearly depicted in which of the following configuration management documents?

- A. Logical network diagrams
- B. Physical network diagrams
- C. Wiring schematics
- D. Group security role assignments

Answer: A

Explanation:

A logical network diagram illustrates the network architecture of a group of interconnected computers and other devices, such as printers, modems, switches, routers, and even mobile devices. These electronic components form the physical network that provides local area network (LAN) and wide area network (WAN) access to users. Once you know the layout and you have an idea about the packet flow then your job becomes easy and you can create an action plan to go for the implementation.

QUESTION 205

While preparing to replace an old CAT3 cable with a CAT6 cable to implement VoIP, a facilities employee mistakenly disconnects the entire patch panel, including valid wiring to live workstations. Which of the following should an administrator use in order to connect those ports FIRST?

- A. Toner
- B. Multimeter
- C. Reflectometer
- D. Cable tester

Answer: A

Explanation:

Toner connects to any voice, data, or video cable to detect open/short circuits, continuity, AC/DC voltage* and dial tone* all while protecting up to 52 volt.

QUESTION 206

Which of the following methods would be implemented to correct a network slowdown caused by excessive video streaming?

- A. Traffic shaping
- B. Proxy server
- C. VPN concentrator
- D. High availability

Answer: A

Explanation:

As traffic shaping will prioritize the video packets over another packets and then video packets will travel fast on bandwidth.

QUESTION 207

While working on a PC, a technician notices 0.0.0.0 in the routing table. Which of the following does this indicate?

- A. It is the default route.
- B. This is the address for the DHCP server.
- C. The PC has not been assigned an IP address.
- D. The firewall is down.

Answer: A

Explanation:

The address 0.0.0.0 generally means "any address". If a packet destination doesn't match an individual address in the table, it must match a 0.0.0.0 gateway address. In other words, default gateway is always pointed by 0.0.0.0

QUESTION 208

Users inform an administrator that the network is slow. The administrator notices the bulk of the traffic is SIP and RTP traffic. Which of the following could the administrator do to help BEST alleviate the traffic congestion for the users?

- A. Create an ACL on the switches and routers that are dropping SIP and RTP packets.
- B. Create a QoS policy prioritizing users over RTP and SIP traffic.
- C. Create another VLAN for SIP and RTP traffic.
- D. Create a rule to throttle SIP and RTP to 10Kbps or less.

Answer: C

Explanation:

As if we will create a vlan for sip and rtp traffic only this traffic will flow from the ports then.

QUESTION 209

If a NIC does not have a link light, there is a failure at which of the following OSI layers?

- A. Physical
- B. Session
- C. Data link
- D. Presentation

Answer: A

Explanation:

The NIC does not have light refers to a situation that there could be a fault in the LAN cable or the ports are down and all of these fall under the physical layer. To make it simple, it falls in physical layer because blinking lights refers to the physical connectivity.

QUESTION 210

Which of the following is the control when observing network bandwidth patterns over time?

- A. Network log

- B. Baseline
- C. Flow data
- D. Interface statistics

Answer: B

Explanation:

To successfully baseline a network it is important to consider two functions; performance at protocol level and performance at application level. There are many significant metrics to consider at the protocol level, but only a few which are critical. The most important is bandwidth utilization compared with bandwidth availability. The most likely cause of poor network performance is insufficient bandwidth. Trending bandwidth utilization allows you to recognize problem areas, provide enough bandwidth to reach performance objectives, and predict future capacity requirements. Changes in bandwidth utilization patterns also provide a clear indication of network usage alterations, such as a change in end-user behavior, or the unauthorized addition of an application.

QUESTION 211

Which of the following technologies is used on cellular networks?

- A. Ethernet
- B. CDMA
- C. CSMA/CA
- D. POTS

Answer: B

Explanation:

CDMA is an example of multiple access, which is where several transmitters can send information simultaneously over a single communication channel. This allows several users to share a band of frequencies (see bandwidth). To permit this to be achieved without undue interference between the users CDMA employs spread-spectrum technology and a special coding scheme

QUESTION 212

Which of the following technologies allows multiple staff members to connect back to a centralized office?

- A. Peer to Peer
- B. VPN
- C. PKI
- D. VLAN

Answer: B

Explanation:

VPN enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

QUESTION 213

Which of the following is the MOST secure way to prevent malicious changes to a firewall?

- A. SNMPv2 access only
- B. TELNET access only
- C. SSH access only

D. Console access only

Answer: D

Explanation:

As SSH is secure than any other option because it provide encryption. So we use SSH to remotely access.

QUESTION 214

Which of the following allows a malicious attacker to view network traffic if the attacker is on the same network segment as Joe, an administrator?

- A. DoS attack
- B. Man-in-the-middle attack
- C. Smurf attack
- D. Xmas attack

Answer: B

Explanation:

An attack where a user gets between the sender and receiver of information and sniffs any information being sent. In some cases, users may be sending unencrypted data, which means the man-in-the-middle (MITM) can obtain any unencrypted information. In other cases, a user may be able to obtain information from the attack, but have to unencrypt the information before it can be read.

QUESTION 215

Which of the following OSI layers allows users to access network services such as file sharing?

- A. Layer 1
- B. Layer 3
- C. Layer 4
- D. Layer 7

Answer: D

Explanation:

Basically File Transfer protocol (FTP) is responsible for file transfer which lies under Application layer (Layer 7) of OSI layers.

QUESTION 216

Which of the following can function in an unsecure mode?

- A. SNMPv3
- B. SSH
- C. SSL
- D. SCP

Answer: A

Explanation:

SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, it looks much different due to new textual conventions, concepts, and terminology. SNMPv3 primarily added security and remote configuration enhancements to SNMP

QUESTION 217

Which of the following is used to register and resolve IP addresses with their plain language

equivalents?

- A. Proxy server
- B. DNS server
- C. Brouter equipment
- D. DHCP server

Answer: B

Explanation:

DNS server translate (resolution) the human-memorable domain names and hostnames into the corresponding numeric Internet Protocol (IP) addresses.

QUESTION 218

An administrator determines there are an excessive number of packets being sent to a web server repeatedly by a small number of external IP addresses. This is an example of which of the following attacks?

- A. DDoS
- B. Viruses
- C. Worms
- D. Man-in-the-middle

Answer: A

Explanation:

DDoS attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols

QUESTION 219

Which of the following features will a firewall MOST likely use to detect and prevent malicious traffic on the network?

- A. Zone filtering
- B. Signature identification
- C. Port identification
- D. Port scanner

Answer: B

Explanation:

Signature-based detection really is more along the lines of intrusion detection than firewalls. However, many personal firewalls and some corporate firewalls contain this functionality. Essentially, the system can be configured to look for specific patterns, known to be malicious, and block the traffic

QUESTION 220

Which of the following protocols is MOST commonly associated with VoIP?

- A. LDAP
- B. HTTPS
- C. SIP
- D. SCP

Answer: C

Explanation:

The Session Initiation Protocol (SIP) is a signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks.

QUESTION 221

Stateful packet inspection is a security technology used by which of the following devices?

- A. Unmanaged switch
- B. Hardware firewall
- C. Bridge
- D. IDS

Answer: B

Explanation:

With Stateful Packet Inspection (SPI), every time a packet is sent out of the computer, the firewall keeps track of it. When a packet comes back to the firewall, the firewall can tell whether or not the in-bound packet is a reply to the packet that was sent out. This way, the firewall can handle most network traffic safely without a complex configuration of firewall rules.

QUESTION 222

Which of the following commands will provide an administrator with the number of hops a packet takes from host to host?

- A. nslookup
- B. ping
- C. traceroute
- D. route

Answer: C

Explanation:

In computing, traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection.

QUESTION 223

Which of the following is needed when using WPA2-Enterprise wireless encryption?

- A. TFTP
- B. RADIUS
- C. LDAP
- D. IPSec

Answer: B

Explanation:

The WPA2 standard supports two different authentication mechanisms: one using standard RADIUS servers and the other with a shared key, similar to how WEP works.

QUESTION 224

Which of the following technologies is used to connect public networks using POTS lines?

- A. OC3
- B. OC12
- C. PSTN
- D. Cable

Answer: C

Explanation:

The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing any telephone in the world to communicate with any other

QUESTION 225

An administrator would like to inspect all traffic flowing over the SMTP protocol on a given network. Which of the following tools would accomplish this? (Select TWO).

- A. Packet sniffer
- B. Honeypot
- C. Port mirroring
- D. IPS
- E. Port scanner
- F. IDS

Answer: AC

Explanation:

(IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

And we use packet sniffer to detect the types of packet.

QUESTION 226

Which of the following switch features allows for both incoming and outgoing data across physical ports at the same time?

- A. Burst-frame
- B. Full-duplex
- C. Half-duplex
- D. VoIP

Answer: B

Explanation:

Full-duplex (FDX), or sometimes double-duplex system, allows communication in both directions, and, unlike half-duplex, allows this to happen simultaneously. Land-line telephone networks are full-duplex, since they allow both callers to speak and be heard at the same time

QUESTION 227

Which of the following is a common physical network topology?

- A. Cross-over
- B. Loopback
- C. Star

D. Straight

Answer: C

Explanation:

A star network consists of one central switch, hub or computer, which acts as a conduit to transmit messages. This consists of a central node, to which all other nodes are connected; this central node provides a common connection point for all nodes through a hub. In star topology, every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

QUESTION 228

PKI is a method of user authentication which uses which of the following?

- A. Various router commands
- B. Access control lists
- C. Certificate services
- D. A RADIUS server

Answer: C

Explanation:

A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally

QUESTION 229

A technician has a network with a mix of newer and older equipment. Which of the following settings would dynamically configure whether to use full or half duplex?

- A. Transmission speed
- B. Frequency
- C. Auto-negotiate
- D. Distance

Answer: C

Explanation:

Autonegotiation is an Ethernet procedure by which two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control. In this process, the connected devices first share their capabilities regarding these parameters and then choose the highest performance transmission mode they both support.

QUESTION 230

An administrator needs to install a WAP in a location where there is no electrical wiring. Which of the following should the administrator use to complete a successful installation?

- A. Coaxial
- B. Wireless bridge
- C. PoE
- D. Multimode fiber

Answer: C

Explanation:

PoE provides both data and power connections in one cable, so equipment doesn't require a separate cable for each need.

QUESTION 231

Which of the following is always true when a router selects a destination?

- A. The default gateway is selected over any other static or dynamic route.
- B. The shortest route is always selected.
- C. The most specific route is selected over the default gateway.
- D. A dynamic route is selected over a directly attached network.

Answer: C

Explanation:

Router always looks for the most closely matched route for forwarding the packet. For example if there are two routes in your router and you have to send a packet to a host with an ip 10.10.10.10 then it will forward packet to 192.168.1.10 rather than 192.168.1.1:

Network	Destination	Netmask	Gateway
0.0.0.0	0.0.0.0	0.0.0.0	192.168.1.1
10.10.10.0	255.255.255.0	192.168.1.10	

QUESTION 232

A proxy server would MOST likely be installed to provide which of the following functions? (Select TWO).

- A. Combined DNS and DHCP hosting
- B. Encryption
- C. Content filtering
- D. Fault tolerance
- E. Website caching

Answer: CE

Explanation:

A content-filtering web proxy server provides administrative control over the content that may be relayed in one or both directions through the proxy. A caching proxy server accelerates service requests by retrieving content saved from a previous request made by the same client or even other clients.

QUESTION 233

Which of the following would the telecommunications carrier use to segregate customer traffic over long fiber links?

- A. VLAN
- B. MPLS
- C. VPN
- D. PSTN

Answer: B

Explanation:

MPLS is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints

QUESTION 234

Drag and Drop Question

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

FC LC (single) LC (duplex) SC ST

Answer:



QUESTION 235

An administrator notices SMTP traffic is being blocked by the company firewall. Which of the following ports should be opened?

- A. 25
- B. 53
- C. 110
- D. 443

Answer: A

Explanation:

SMTP is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks. SMTP uses TCP port 25.

QUESTION 236

Which of the following network topologies would be separated into two networks if a client in the middle is removed or the cable is cut?

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

Answer: C

Explanation:

A bus network topology is a network topology in which a set of clients are connected via a shared

communications line/cables, called a bus.

QUESTION 237

Which of the following is an example of a Class C address?

- A. 10.19.0.79
- B. 127.34.8.197
- C. 176.96.1.222
- D. 192.168.1.105

Answer: D

Explanation:

Class C address range varies from 192.0.0.0 to 223.255.255.255.

QUESTION 238

Drag and Drop Question

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

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

Answer:

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

QUESTION 239

Drag and Drop Question

GigSwitch1 is currently configured with a speed of 100 and Duplex is set to Auto on all interfaces. Interface 2 will be connected to GigSwitch2 which is used for all departments. Interface 1 will be used for HR traffic only.

GigSwitch1 needs to be configured with the following parameters:

- * Configure the necessary protocol to prevent switching loops
- * Configure GigSwitch1 with a /24 IP address for management
- * Traffic across Interface 1 needs to be forced to accept and receive up to 100Mbps data at the same time
- * Traffic across Interface 2 needs to be forced to use Gigabit speeds and maximum performance

Drag and drop the appropriate configurations to their corresponding requirements. All placeholders must be filled. Not all configurations will be used.

The image shows a network configuration simulator interface with three main columns: **Global Switch Configuration**, **Interface 1**, and **Interface 2**. Each column contains two input fields labeled '1' and '2'. Below these are several configuration buttons:

- Global Switch Configuration:**
 - 100/Full
 - 100/Auto
 - Auto/Full
 - Auto/Half
- Interface 1:**
 - 1000/Full
 - 1000/Auto
 - IP Address 192.168.1.1 255.255.240.0
 - IP Address 192.168.1.1 255.255.240.0
 - IP Address 192.168.1.1 255.255.255.0
- Interface 2:**
 - VLAN trunking/multiplexing
 - VLAN 10 HR
 - VLAN 20 Sales
 - VLAN 30 OPS
 - Enable STP
 - Enable AAA
 - Enable SNMPv3

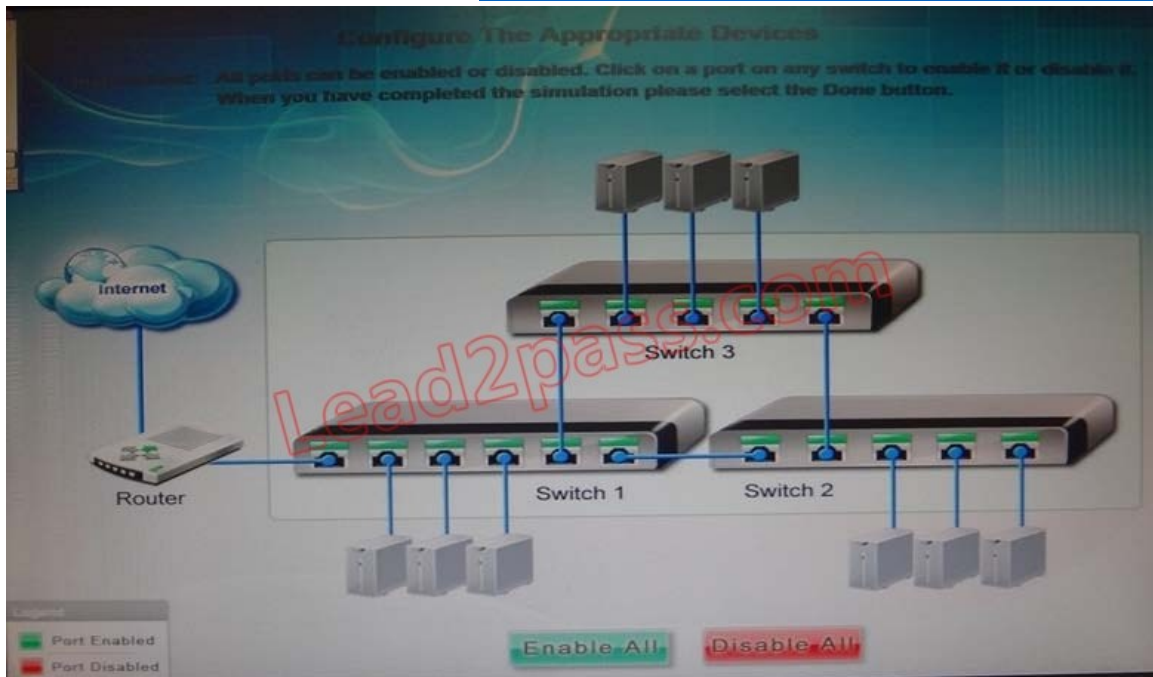
Answer:

Global Switch Configuration	Interface 1	Interface 2
1 IP Address 192.168.1.1 255.255.255.240	1 VLAN 10 HR	1 VLAN trunking/ multiplexing
2 Enable STP	2 100/Full	2 1000/Full
100/Full	1000/Full	IP Address 192.168.1.1 255.255.255.240
100/Auto	1000/Auto	VLAN 10 HR
Auto/Full	IP Address 192.168.1.1 255.255.240.0	VLAN 20 Sales
Auto/Half	IP Address 192.168.1.1 255.255.255.0	VLAN 30 OPS
		Enable STP
		Enable AAA
		Enable SNMPv3

QUESTION 240

Lab Simulation

Workstations are unable to access the internet after a recent power outage. Configure the appropriate devices to ensure All workstations have internet connectivity.



Answer:

The switches are not connected properly.

Connect Switch 1 to switch three on the last port and then connect the last port of the switch 3 to the first port of switch 2. In this way the switches will be connected properly. Click Enable All to enable the switches.

QUESTION 241

Lab Simulation

You have been tasked with testing a CAT5e cable.

A summary of the test results can be found on the screen.

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

Step 2: Interpret the test results and select the option that explains the results.

After you are done with your analysis, click the 'Submit Cable Test Analysis' button.

Cable Test

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

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

→

Tool Choices	
<input type="checkbox"/>	Crimper
<input type="checkbox"/>	Cable Certifier
<input type="checkbox"/>	Multimeter
<input type="checkbox"/>	Punch Down Tool
<input type="checkbox"/>	Protocol Analyzer
<input type="checkbox"/>	OTDR
<input type="checkbox"/>	Toner Probe

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

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

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.

Correct voltage on the cable
 Incorrect voltage on the cable

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	
<input type="checkbox"/>	Crimper
<input type="checkbox"/>	Cable Certifier
<input type="checkbox"/>	Multimeter
<input checked="" type="checkbox"/>	Punch Down Tool
<input type="checkbox"/>	Protocol Analyzer
<input type="checkbox"/>	OTDR
<input type="checkbox"/>	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 punched cable
 Incorrectly punched cable

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	
<input type="checkbox"/>	Crimper
<input type="checkbox"/>	Cable Certifier
<input type="checkbox"/>	Multimeter
<input type="checkbox"/>	Punch Down Tool
<input checked="" type="checkbox"/>	Protocol Analyzer
<input type="checkbox"/>	OTDR
<input type="checkbox"/>	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.

Correct captured packets
 Incorrect captured packets

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.

Correct length cable
 Incorrect length cable

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 toned cable
 Incorrectly toned cable

Answer: Cable certifier - incorrectly crimped cable

QUESTION 242

Lab Simulation

Wireless network users recently began experiencing speed and performance issues after access point 2 (AP2) was replaced due to faulty hardware.

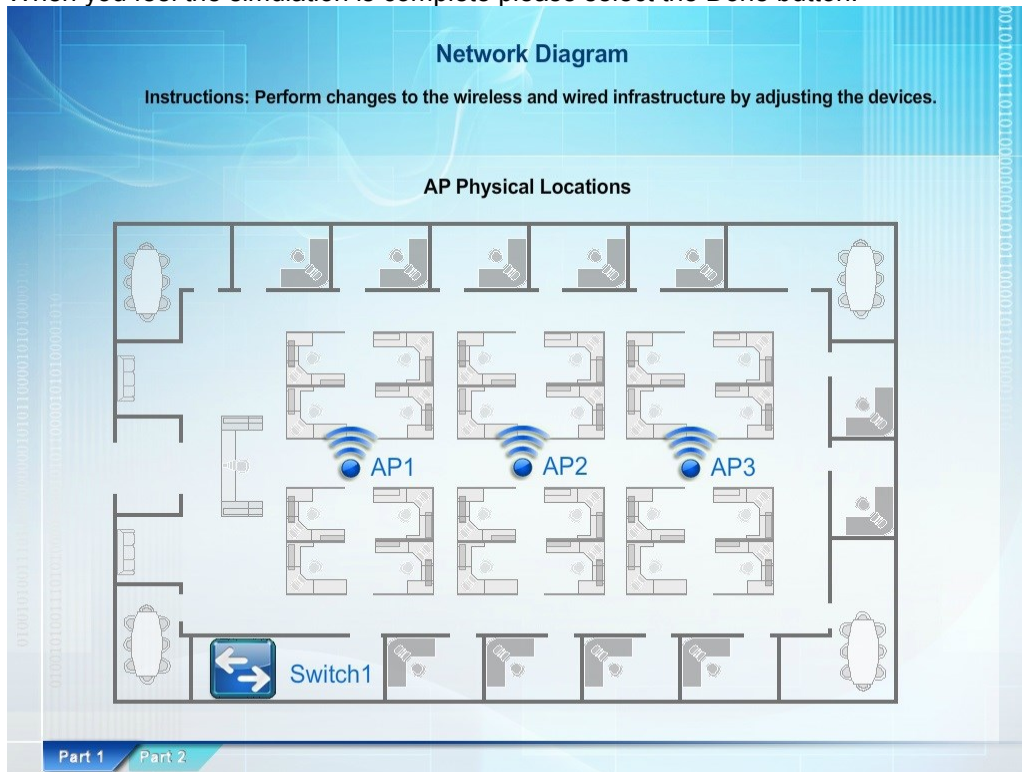
The original network was installed according to a consultant's specifications and has always worked without a problem.

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 100n 1000n

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: AP2
IP Address: 192.168.100.152 / 24
Gateway: 192.168.100.1
SSID: CorpNET
SSID Broadcast: Yes No

Wireless

Mode: B
Channel: 1

Wired

Speed: AUT 1U 10U
Duplex: AUT Half Full

Security

Security Settings: None WEP WPA
Key or Passphrase: 123456789b

Reset Submit

Wireless AP3 Settings

http://ap3.setup.do

Wireless AP Configuration Settings

Basic Configuration

Access Point Name: AP3
IP Address: 192.168.100.153 / 24
Gateway: 192.168.100.1
SSID: CorpNET
SSID Broadcast: Yes No

Wireless

Mode: G
Channel: 11

Wired

Speed: AUT 1U 10U
Duplex: AUT Half Full

Security

Security Settings: None WEP WPA
Key or Passphrase: 123456789b

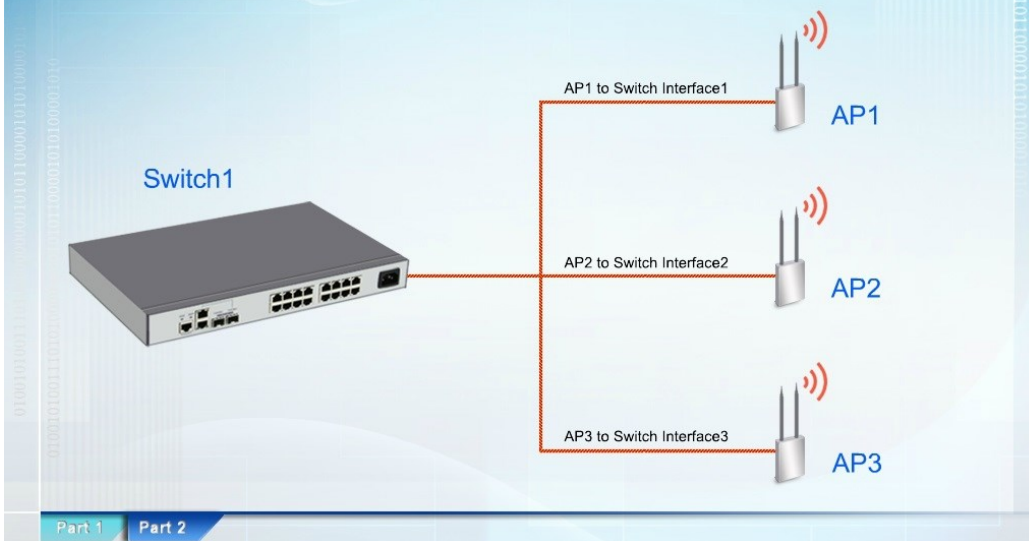
Reset Submit

```
SWITCH 1
SW1# help
sh[ow] int[erfaces]
sh[ow] run[ning] int[erfaces]
SW1# _
```

Network Diagram

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

Logical Network Diagram



Answer:

- Change the speed and duplex settings on AP2 only to 100 and full.
- Change the mode to G on AP2
- Change the channel to 6 on AP2

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.

QUESTION 243

A user's laptop is unable to keep a stable network connection. Which of the following measures would MOST likely need to be configured?

- A. SSID name
- B. WAP encryption strength
- C. WAP radio power
- D. Channel overlay

Answer: C

Explanation:

WAP radio power is the signal strength through which you can specify the range from which you can stay connected to the network and access internet. Here, when the user is not able to maintain a stable connection then it is a problem with the signal strength for sure so you can try to increase the signal strength by increasing the radio power.

QUESTION 244

The security administrator needs to restrict specific devices from connecting to certain WAPs. Which of the following security measures would BEST fulfill this need?

- A. WAP placement
- B. MAC address filtering
- C. Content filtering
- D. Encryption type and strength

Answer: B

Explanation:

MAC Filtering (or EUI filtering, or layer 2 address filtering) is a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

QUESTION 245

Which of the following performs authentication and provides a secure connection by using 3DES to encrypt all information between two systems?

- A. HTTPS
- B. SSH
- C. RSA
- D. SSL

Answer: B

Explanation:

DES encryption algorithm encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).

QUESTION 246

The Network Interface Layer of the TCP/IP model corresponds to which of the following layers of the OSI model? (Select TWO).

- A. Network
- B. Session
- C. Transport
- D. Physical
- E. Data link

Answer: DE

Explanation:

The network layer is responsible for packet forwarding including routing through intermediate routers, whereas the data link layer is responsible for media access control, flow control and error checking.

QUESTION 247

In which of the following layers of the OSI model would MAC addressing be found?

- A. Network
- B. Application
- C. Data Link
- D. Transport

Answer: C

Explanation:

The ITU-T G.703 standard, which provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes a complete data link layer which provides both error correction and flow control by means of a selective repeat Sliding Window Protocol.

QUESTION 248

Several users from the finance department report that they are able to access the Internet, but unable to connect to their financial applications. The network technician is unable to ping the finance server. The technician decides to check the switch and determines that Internet access is working. Which of the following is a possible cause of the access issues?

- A. Faulty cable
- B. Remote management disabled
- C. Improper VLAN assignment
- D. Mismatched duplex

Answer: C

Explanation:

Finance Server is placed in same VLAN which is assigned to finance users if they are able to access internet that's means connectivity to switch is good, so we have to check the VLAN assigned to users.

QUESTION 249

A technician needs to ensure that traffic from a specific department is separated within several switches. Which of the following needs to be configured on the switch to separate the traffic?

- A. Duplex settings
- B. SNMP string
- C. VLAN assignments
- D. Spanning tree

Answer: C

Explanation:

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

QUESTION 250

Several users are reporting connectivity issues with their laptops. Upon further investigation, the network technician identifies that their laptops have been attacked from a specific IP address outside of the network. Which of the following would need to be configured to prevent any further attacks from that IP address?

- A. Port security
- B. IDS
- C. Firewall rules
- D. Switch VLAN assignments

Answer: C

Explanation:

Firewall rules block or allow specific traffic passing through from one side of the router to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

QUESTION 251

The company is setting up a new website that will be requiring a lot of interaction with external users. The website needs to be accessible both externally and internally but without allowing access to internal resources. Which of the following would MOST likely be configured on the firewall?

- A. PAT
- B. DHCP
- C. DMZ
- D. NAT

Answer: C

Explanation:

DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

QUESTION 252

Which of the following attacks would allow an intruder to do port mapping on a company's internal server from a separate company server on the Internet?

- A. SYN flood
- B. Teardrop
- C. Smurf
- D. FTP bounce

Answer: D

Explanation:

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

QUESTION 253

Which of the following would be used to check whether a DoS attack is taking place from a specific remote subnet?

- A. Syslog files
- B. Honeypot
- C. Network sniffer
- D. tracer

Answer: C

Explanation:

A network sniffer monitors data flowing over computer network links. It can be a self-contained software program or a hardware device with the appropriate software or firmware programming.

QUESTION 254

A network technician has just upgraded a switch. The new switch's IP range and subnet mask correctly match other network devices. The technician cannot ping any device outside of the switch's own IP subnet. The previous switch worked correctly with the same settings. Which of the following is MOST likely the problem?

- A. The proxy server is set incorrectly.
- B. The Ethernet cable is pinched.
- C. The network gateway is set incorrectly.
- D. The IP address is set incorrectly.

Answer: C

Explanation:

When user is able to ping everything in its own subnet that means that all the hosts are reachable however when you are not able to ping anything outside of this subnet then please check if the device is sending traffic to the correct host who should forward it to the further devices.

QUESTION 255

Joe has a small office and is looking to replace his phone system with a lower cost solution that requires minimal in-house support. Which of the following is the BEST choice?

- A. Wide Area Network
- B. NAT
- C. Virtual PBX
- D. Virtual LAN

Answer: C

Explanation:

Virtual PBX, a business phone system providing call routing, follow-me calling, voice-mail, fax-mail, and ACD queues with no customer installed equipment.

QUESTION 256

An unusual amount of activity is coming into one of the switches in an IDF. A malware attack is suspected. Which of the following tools would appropriately diagnose the problem?

- A. Cable tester
- B. Protocol analyzer
- C. Load balancer
- D. OTDR

Answer: B

Explanation:

A packet analyzer is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content.

QUESTION 257

Joe, a user, has a computer that has a link light on his network interface card (NIC); however, Joe is unable to access the Internet. Which of the following is the cause of this issue?

- A. Faulty GBIC
- B. Faulty SFP
- C. Cable is a crossover
- D. VLAN mismatch

Answer: D

Explanation:

As user has link light on NIC that means he has connectivity with switch so he need to check his vlan assignment.

QUESTION 258

Which of the following can a network technician change to help limit war driving?

- A. Signal strength
- B. SSID
- C. Frequency
- D. Channel

Answer: A

Explanation:

War driving is a term used to describe the process of a hacker who, armed with a laptop and a wireless adapter card and traveling via a car, bus, subway train, or other form of mechanized transport, goes around sniffing for WLANs. Over time, the hacker builds up a database comprising the network name, signal strength, location, and ip/namespace in use..

QUESTION 259

Which of the following is an example of a CSMA/CD medium?

- A. WEP

- B. SONET
- C. Token ring
- D. Ethernet

Answer: D

Explanation: CSMA/CD is a Media Access Control method in which a carrier sensing scheme is used and also a transmitting data station that detects another signal while transmitting a frame, stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame

QUESTION 260

Which of the following performance optimization techniques would be MOST beneficial for a network-wide VoIP setup? (Select TWO).

- A. Proxy server
- B. Traffic shaping
- C. Caching engines
- D. Load balancing
- E. Quality of service

Answer: BE

Explanation:

Traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time. The result of traffic shaping is a smoothed packet output rate. QoS (Quality of Service) is a major issue in VOIP implementations. The issue is how to guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due to interference from other lower priority traffic.

Things to consider are:

Latency: Delay for packet delivery

Jitter: Variations in delay of packet delivery

Packet loss: Too much traffic in the network causes the network to drop packets
Burstiness of Loss and Jitter: Loss and Discards (due to jitter) tend to occur in bursts

QUESTION 261

A network technician is troubleshooting signal problems with certain WAPs in an office and finds consistently high ping times across the units. Such an issue is called which of the following?

- A. Latency
- B. Attenuation
- C. Crosstalk
- D. Frequency hopping

Answer: A

Explanation:

During the high ping time users are using most of the bandwidth that causes latency so signal strength gets affected by this.

QUESTION 262

A customer has requested a solution using multiple WAPs for wireless access. Which of the following should be different on each WAP to prevent wireless problems?

- A. Firewalls
- B. VLANs

- C. Channels
- D. Antenna types

Answer: C

Explanation:

Protocol requires 16.25 to 22 MHz of channel separation (as shown above), adjacent channels overlap and will interfere with each other.

Channels 1, 6, and 11 are the most common channels to choose, and most routers will use one of them as the default channel--but the general idea is to be as far away from everybody else as you can.

QUESTION 263

Which of the following ports would have to be allowed through a firewall for POP3 traffic to pass on its default port?

- A. 110
- B. 123
- C. 143
- D. 443

Answer: A

Explanation:

Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. POP3 server listens on well-known port 110.

QUESTION 264

Which of the following copper cable types should be chosen to run gigabit speeds through a dropped ceiling that returns airflow?

- A. Non-Plenum CAT5
- B. Non-Plenum CAT5e
- C. Plenum CAT5
- D. Plenum CAT5e

Answer: D

Explanation:

Cat 5e is a twisted pair cable for carrying signals. This type of cable is used in structured cabling for computer networks such as Ethernet. The cable standard provides performance of up to 100 MHz and is suitable for 10BASE-T, 100BASE-TX (Fast Ethernet), and 1000BASE-T (Gigabit Ethernet).

QUESTION 265

Management has decided that they want a high level of security. They do not want Internet requests coming directly from users. Which of the following is the BEST recommendation?

- A. Content filter
- B. Proxy server
- C. Layer 3 switch
- D. Firewall

Answer: B

Explanation:

A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

QUESTION 266

Management wants to be sure that the existing wiring infrastructure conforms to CAT5e standards. Which of the following is the correct tool?

- A. Cable certifier
- B. Cable tester
- C. OTDR
- D. Protocol analyzer

Answer: A

Explanation:

A cable certifier is used to verify that a cable meets its specifications such as the bandwidth and frequency. For example, it can verify a CAT 5e cable meets specifications and supports speeds of 1000Mbps.

QUESTION 267

A company wants to secure its WAPs from unauthorized access. Which of the following is the MOST secure wireless encryption method?

- A. SSID disable
- B. SNMPv3
- C. WEP
- D. WPA2

Answer: D

Explanation:

WPA2 improves security of Wi-Fi connections by not allowing use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes (limitations) in the original WPA implementation.

QUESTION 268

Which of the following will allow a technician to monitor all network traffic when connected to a mirror port?

- A. VLAN tags
- B. SNMP
- C. Packet sniffer
- D. Syslog

Answer: C

Explanation:

Mirror port just send the packet to the port which is selected to grab the packet of any destination port to capture that packets we need packet sniffer.

QUESTION 269

A customer wants to increase firewall security. Which of the following are common reasons for implementing port security on the firewall? (Select TWO).

- A. Preventing dictionary attacks on user passwords

- B. Reducing spam from outside email sources
- C. Shielding servers from attacks on internal services
- D. Blocking external probes for vulnerabilities
- E. Directing DNS queries to the primary server

Answer: CD

Explanation:

Port security is required because if we keep the ports unsecure then hackers can do port scanning and can compromise the internal secured network so we will have to shield servers to avoid attacks from outside and we need to block incoming scanning request coming from outside.

QUESTION 270

A user reports that some normally accessible external sites are not responding, but most other sites are responding normally. Which of the following is MOST likely the cause?

- A. VLAN tag mismatch
- B. Wrong subnet mask
- C. Smurf attack
- D. Faulty routing rule

Answer: D

Explanation:

This happens when the DNS server is able to resolve the URL but there can be a conflicting route pointing to somewhere else rather than to the correct device who is responsible for routing traffic to the internet.

QUESTION 271

The security measure used to reduce vulnerabilities for MOST network devices that require regular application and monitoring is:

- A. patch management.
- B. security limitations.
- C. documentation.
- D. social engineering.

Answer: A

Explanation:

A patch is a piece of software designed to fix security vulnerabilities and other bugs, and improving the usability or performance.

QUESTION 272

A user wants to connect seven PCs together for a game night. Which of the following should the user install to help with this task?

- A. Media convertor
- B. Switch
- C. Firewall
- D. Bridge

Answer: B

Explanation:

They connect multiple PCs, printers, servers and other hardware. Switches allow you to send

information, such as email, and access shared resources, including printers, in a smooth, efficient, and transparent manner.

QUESTION 273

Which of the following defines the amount of time a host retains a specific IP address before it is renewed or released?

- A. DHCP lease
- B. DNS suffix
- C. Subnet mask
- D. DHCP reservation

Answer: A

Explanation:

By default, each IP address assigned by a DHCP Server comes with a one-day lease, which is the amount of time that the address is valid.

QUESTION 274

Which of the following appliances creates and manages a large number of secure remote-access sessions, and also provides a high availability solution?

- A. Media converter
- B. Proxy server
- C. VPN concentrator
- D. Load balancer

Answer: C

Explanation:

The VPN Concentrator is used for Remote Access VPN's that allows users to use an encrypted tunnel to securely access a corporate or other network via the Internet.

QUESTION 275

A customer wants to keep cost to a minimum and has only ordered a single static IP address from the ISP. Which of the following must be configured on the router to allow for all the computers to share the same public IP address?

- A. VLANs
- B. PoE
- C. PAT
- D. VPN

Answer: C

Explanation:

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

QUESTION 276

After a technician has identified the problem and its impact, which of the following steps should be performed NEXT?

- A. Implement preventative measures.

- B. Establish a plan of action to resolve the problem.
- C. Establish a theory of probable cause.
- D. Implement the solution or escalate as necessary.

Answer: C

Explanation:

By sorting out the probable causes and establishing a theory on them he will come to know whether it is right cause or not.

QUESTION 277

Which of the following wireless standards has a MAXIMUM transfer rate of 11Mbps?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11n

Answer: B

Explanation:

The 802.11b standard allows for a maximum data transfer speed of 11 Mbps, at a range of about 100 m indoors and up to 200 metres outdoors (or even beyond that, with directional antennas.)

Hypothetical speed

Range(indoors)

Range(outdoors)

11 Mbits/s

50 m

200 m

5.5 Mbits/s

75 m

300 m

2 Mbits/s

100 m

400 m

1 Mbit/s

150 m

500 m

QUESTION 278

A technician tests a cable going to the patch panel and notices the following output from the cable tester:

```
1-----1
2-----2
3-----3
4-----4
5-----5
6-----6
7-----7
8-----8
```

On a T568A standard CAT5e cable, which of the following wire strands is the cause of this connectivity issue?

- A. White Orange
- B. Solid Brown

- C. Solid Orange
- D. White Green

Answer: D

Explanation:

T568A Wiring

Pin

Pair

Wire

Color



white/green



green



white/orange



blue



white/blue



orange



white/brown



brown

QUESTION 279

Which of the following monitoring devices are used only to recognize suspicious traffic from specific software?

- A. Signature based IPS
- B. Application based IDS
- C. Anomaly based IDS
- D. Application based IPS

Answer: B

Explanation:

An APIDS monitors the dynamic behavior and state of the protocol and will typically consist of a system or agent that would typically sit between a process, or group of servers, monitoring and analyzing the application protocol between two connected devices.

QUESTION 280

Which of the following security appliances are used to only identify traffic on individual systems?

- A. Host based IPS
- B. Application based IPS
- C. Network based IDS
- D. Host based IDS

Answer: D

Explanation:

A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyzes the internals of a computing system as well as the network packets on its network interfaces.

QUESTION 281

Which of the following components of wiring distribution is referred to as the core communications closet for an organization?

- A. MDF
- B. Smart jack
- C. IDF
- D. Demarc extension

Answer: A

Explanation:

MDF stands for Main Distribution Frame and is the main computer room for servers, hubs, routers, DSL's, etc. to reside.

QUESTION 282

Which of the following LAN technologies is used to provide a MAXIMUM bandwidth of 1Gbps through singlemode fiber?

- A. 10GBaseLR
- B. 100BaseFX
- C. 100BaseTX
- D. 1000BaseX

Answer: D

Explanation:

1000BaseX identifies various Gigabit Ethernet physical layer standards as defined in IEEE802.3z, such as 1000BaseLX, 1000BaseSX, 1000BaseCX and 1000BaseLH. Basically, all standards included in 1000BaseX uses 8B/10B coding scheme with 8 bits of data and 2 bits of error-correction data. Each specification allows various cable (fiber or copper) lengths, and uses different cable media.

QUESTION 283

Which of the following does Kerberos provide?

- A. Non-repudiation
- B. Accounting
- C. Exchange
- D. Authentication

Answer: D

Explanation:

Kerberos is a trusted third-party authentication service based on the model presented by Needham and Schroeder. It is trusted in the sense that each of its clients believes Kerberos' judgment as to the identity of each of its other clients to be accurate.

QUESTION 284

Which of the following does Kerberos use to authenticate?

- A. Tickets

- B. Servers
- C. Users
- D. Clients

Answer: A

Explanation:

Kerberos keeps a database of its clients and their private keys. The private key is a large number known only to Kerberos and the client it belongs to. In the case that the client is a user, it is an encrypted password. Network services requiring authentication register with Kerberos, as do clients wishing to use those services. The private keys are negotiated at registration.

QUESTION 285

After a network technician has added a new workstation and cabling to the network, users report the network is very slow. The activity lights on all switches are blinking rapidly, showing large amounts of traffic. Which of the following is the BEST explanation for the traffic?

- A. The new user is downloading large files.
- B. The router failed, flooding the network with beacons.
- C. The new user's IP address is a duplicate.
- D. A switching loop was created.

Answer: D

Explanation:

A Switching loop or Bridge loop occurs in computer networks when there is more than one Layer 2 (OSI model) path between two endpoints (e.g. multiple connections between two network switches or two ports on the same switch connected to each other). The loop creates broadcast radiation as broadcasts and multicasts are forwarded by switches out every port, the switch or switches will repeatedly rebroadcast the broadcast messages flooding the network.

QUESTION 286

Users have reported choppy audio in phone conversations since the implementation of SIP phones on the network. Which of the following should be implemented to alleviate the delays?

- A. Caching
- B. VoIP
- C. QoS
- D. SMTP

Answer: C

Explanation:

By QoS we can prioritize the voice packets over data network. So delay and latency will get reduce.

QUESTION 287

A company has recently allowed its employees to telecommute two days a week. The employees MUST have a minimum of 1Mbps non-shared connection to the Internet. Which of the following MUST the employees have at their home in order to connect to the Internet?

- A. ISDN
- B. Cable modem
- C. DSL
- D. Dial-up networking

Answer: C

Explanation:

Digital subscriber line (DSL, originally digital subscriber loop) is a family of technologies that provide Internet access by transmitting digital data over the wires of a local telephone network.

QUESTION 288

A customer with a SOHO requires fast, secure, cost-effective access to the Internet. Which of the following would be the MOST appropriate solution? (Select TWO).

- A. OC3 line with built-in firewall
- B. DS3 line with a separate firewall
- C. Cable modem with a separate firewall
- D. Dial-up modem with separate firewall
- E. DSL router with firewall capabilities

Answer: CE

QUESTION 289

At which of the following layers do frames exist? (Select TWO).

- A. OSI model Data link layer
- B. TCP/IP model Network Interface layer
- C. OSI model Physical layer
- D. OSI model Network layer
- E. TCP/IP model Internet layer

Answer: AB

Explanation:

The data link layer is concerned with local delivery of frames between devices on the same LAN. Data-link frames, as these protocol data units are called, do not cross the boundaries of a local network. Inter-network routing and global addressing are higher layer functions, allowing data-link protocols to focus on local delivery, addressing, and media arbitration. In this way, the data link layer is analogous to a neighborhood traffic cop; it endeavors to arbitrate between parties contending for access to a medium, without concern for their ultimate destination.

QUESTION 290

A user is unable to access any network resources. The IP configuration of the workstation is as follows:

IP Address: 192.168.10.32
Subnet Mask: 255.255.255.240
Default Gateway: 192.168.10.46

Which of the following would allow the user to connect to network resources?

- A. Change the default gateway to 192.168.10.1
- B. Change the default gateway to 192.168.10.254
- C. Change the IP address to 192.168.10.31
- D. Change the IP address to 192.168.10.33

Answer: D

Explanation:

The given ip address is network id which we don't assign to the host so the next ip is applicable to this.

QUESTION 292

A technician has replaced the Internet gateway router, and now no users can reach the Internet. The technician can ping the router Ethernet port but not the ISP's router IP address. Which of the following is the MOST likely problem?

- A. Faulty crossover cable
- B. DNS server is down
- C. Switching loop
- D. Outside interface shutdown

Answer: D

QUESTION 293

Which of the following commands will display the associated IP address of a network adapter in Windows and Linux environments? (Select TWO).

- A. dig
- B. nslookup
- C. nbstat
- D. ifconfig
- E. ipconfig

Answer: DE

QUESTION 294

A router operates at which of the following layers of the OSI model?

- A. Layer 2
- B. Layer 3
- C. Layer 4
- D. Layer 5

Answer: B

QUESTION 295

When querying a DNS server for an AAAA record, which of the following is an appropriate response?

- A. 192.168.2.1
- B. 00:f3:82:99:a2:b8
- C. 61.23.168.192.in-addr.arpa
- D. 3ffe:1900:4545:3:200:f8ff:fe21:67cf

Answer: D

QUESTION 296

A computer on VLAN 10 with the IP address of 192.168.1.45/27 cannot ping a computer on VLAN 20 with the IP address of 192.168.1.65/27. Which configuration change will allow the PING to be successful?

- A. Replace the router with a Layer 2 switch that supports VLANs

- B. Change VLAN 20 computers Default Gateway to 192.168.1.127/27
- C. Change VLAN 10 computers Default Gateway to 192.168.1.32/27
- D. Allow ICMP to pass through the Router

Answer: D

QUESTION 297

Which of the following network devices restricts traffic based on words, signatures, and URLs?

- A. Layer 2 switch
- B. Content filter
- C. Load balancer
- D. Traffic analyzer

Answer: B

QUESTION 298

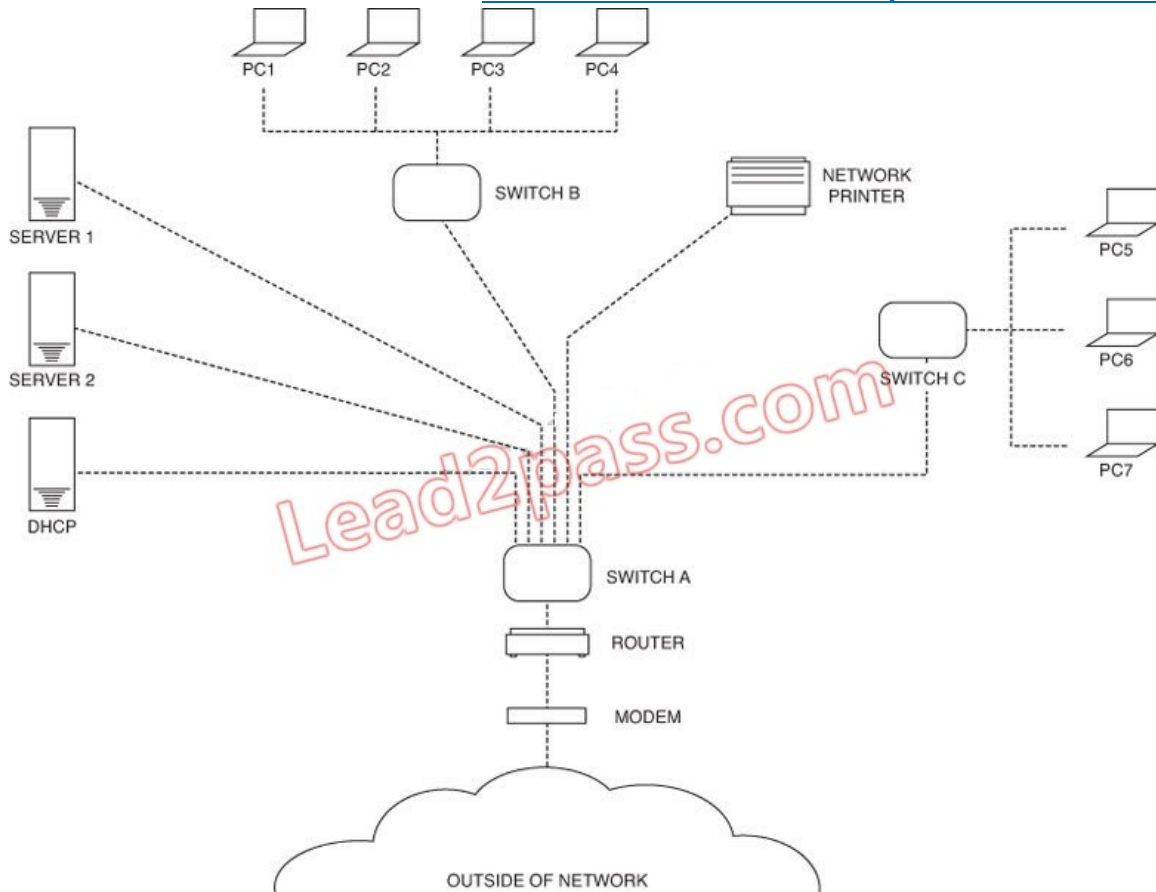
A new firewall was recently installed blocking SMTP traffic. As a result, no one has Internet access. Which of the following has MOST likely occurred?

- A. Port security is blocking all traffic.
- B. An IDS is blocking all traffic.
- C. Implicit deny is blocking all traffic.
- D. SMTP is blocking all traffic.

Answer: C

QUESTION 299

Please refer to the attached exhibit. Which of the following types of configuration management documentation is represented?



- A. Network security policy
- B. Network baseline
- C. Logical network diagram
- D. Wiring schematic

Answer: C

QUESTION 300

Which of the following is the only standard that can operate at either frequency?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11n

Answer: D

Explanation:

Only 802.11n can operate at 2.4Ghz and 5Ghz

[Visit PassLeader and Download Full Version N10-006 Exam Dumps](#)