Question 1:

Skipped

A store owner would like to have secure wireless access available for both business equipment and patron use.

Which of the following features should be configured to allow different wireless access through the same equipment?

- **SSID**

  (Correct)

- **TKIP**

- **LTE**

- **MIMO**

Explanation

With multiple SSIDs operating on top of one physical device, different wireless accesses can be served for different purposes and user groups.

Question 2:

Skipped

Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

- **MAC spoofing**

- **DDoS**

-

Ransomware

(Correct)

- **Phishing**

Explanation
Crypto-malware uses some form of encryption to lock a user out of a system. Once the crypto-malware encrypts the computer, usually encrypting the boot drive, in most cases the malware then forces the user to pay money to get the system decrypted. When any form of malware makes you pay to get the malware to go away, we call that malware *ransomware*. If a crypto-malware uses a ransom, we commonly call it *crypto-ransomware*.

To recover from this attack, proper backup implementation is mandatory.

Question 3:
Skipped
A technician is troubleshooting a wireless connectivity issue in a small office located in a high-rise building. Several APs are mounted in this office. The users report that the network connections frequently disconnect and reconnect throughout the day.

Which of the following is the MOST likely cause of this issue?

- **The RSSI is misreported**
- **EIRP needs to be boosted**
- **Channel overlap is occurring**
- **The AP association time is set too low**

(Correct)

Explanation
If AP association time is too long, the DHCP pool might be exhaustive soon and there will be no available IP addresses for new clients.

If AP association time is too short, clients have to reconnect to the AP more often, causing frustration for end users.

In this situation, the MOST likely cause of the mentioned issue is that the AP association time is set too low.

Question 4:
Skipped
A technician needs to configure a Linux computer for network monitoring. The technician has the following information: Linux computer details:

Interface	IP address	MAC address
eth0	10.1.2.24	A1:B2:C3:F4:E5:D6

Switch mirror port details:

Interface	IP address	MAC address
eth1	10.1.2.3	A1:B2:C3:D4:E5:F6

After connecting the Linux computer to the mirror port on the switch, which of the following commands should the technician run on the Linux computer?

- **ifconfig eth1 up**
- **ifconfig eth0 promisc**

  (Correct)
- **ifconfig eth0 10.1.2.3**
- **ifconfig eth1 hw ether A1:B2:C3:D4:E5:F6**

Explanation
Generally speaking, "promiscuous mode" means that a network interface card will pass all frames received up to the operating system for processing, versus the traditional mode of operation wherein only frames destined for the NIC's MAC address or a broadcast address will be passed up to the OS. Generally, promiscuous mode is used to "sniff" all traffic on the wire.

To enable the promiscuous mode on the physical NIC, run the following command on the server text console:
 # ifconfig eth0 promisc

Question 5:
Skipped
An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt.

Which of the following attack types BEST describes this action?

- **Rainbow table attack**
- **Dictionary attack**
- **Pass-the-hash attack**
- **Brute-force attack**

(Correct)

Explanation
***Brute-force password attack*:** In this type of attack, the attacker tries all possible password combinations until a match is made. For example, a brute-force attack might start with the letter a and go through the letter z, and then the attacker might attempt the letters aa through zz, continuing to try combinations until the password is determined. Using complicated passwords—with a mixture of upper- and lowercase letters as well as special characters and numbers—can help prevent brute-force attacks.
Question 6:

Skipped

Access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time.

Which of the following allows the enforcement of this policy?

- **Cameras**
- **Smart lockers**
- **Motion detection**
- **Access control vestibules**

  (Correct)

Explanation

An *access control vestibule*—traditionally called a *mantrap*—is an entryway with two successive locked doors and a small space between them providing one-way entry or exit. After entering the first door, the second door cannot be unlocked until the first door is closed and secured. Access to the second door may be a simple key or may require approval by someone else who watches the trap space on video. Unauthorized persons remain trapped until they are approved for entry, let out the first door, or held for the appropriate authorities.

With access control vestibule, even though multiple employees enter the facility at the same time, the card reader can record the access individually.

Question 7:

Skipped

Which of the following devices would be used to manage a corporate WLAN?

- **A wireless router**

- **A wireless NAS**
- **A wireless bridge**
- **A wireless controller**

  (Correct)

Explanation
In larger enterprise environments, wireless LAN controllers (WLCs) often provide the control plane intelligence that APs lack.

Question 8:

Skipped

A company requires a disaster recovery site to have equipment ready to go in the event of a disaster at its main datacenter. The company does not have the budget to mirror all the live data to the disaster recovery site.

Which of the following concepts should the company select?

- **Hot site**
- **Cold site**
- **Warm site**

  (Correct)
- **Cloud site**

Explanation
A *cold site* is a location that consists of a building, facilities, desks, toilets, parking—everything that a business needs…except computers. A cold site generally takes more than a few days to bring online.

A *warm site* starts with the same components as a cold site, but adds computers loaded with software and functioning servers—a complete hardware infrastructure. A warm site lacks current data and may not have functioning Internet/network links. Bringing this site up to speed may start with activating your network links, and it most certainly requires loading data from recent backups. A warm site should only take a day or two to bring online.

A *hot site* has everything a warm site does, but also includes very recent backups. It might need just a little data restored from a backup to be current, but in many cases a hot site is a complete duplicate of the primary site. A proper hot site should only take a few hours to bring online.

In this situation, warm site should be selected to satisfy company's requirements.

Question 9:
Skipped
An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex.

Which of the following is the MOST likely cause of this issue?

- **One of the devices has a hardware issue**
- **One of the devices is misconfigured**
- **The cable length is excessive**
- **The link is improperly terminated**

  (Correct)

Explanation
Late Collision is a collision on an Ethernet network that is detected late in the transmission of the packet. Late collisions can result from defective Ethernet transceivers, from having too many repeaters between stations, or from exceeding Ethernet specifications for maximum node-to-node distances.

In this situation, the most likely cause is "the link is improperly terminated".

Question 10:
Skipped
A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light.

According to troubleshooting methodology, this is an example of:

- **using a bottom-to-top approach.**

  (Correct)

- **questioning the obvious.**

- **documenting a finding.**

- **establishing a plan of action.**

Explanation
Checking the link light first meaning checking Layer 1 first. This is the first step in bottom-to-top approach when the technician will check all possible issues at each OSI Layers from Layer 1 to Layer 7.
Question 11:
Skipped
A network administrator is troubleshooting an issue with a new Internet connection. The ISP is asking detailed questions about the configuration of the router that the network administrator is troubleshooting.

Which of the following commands is the network administrator using? (Selected TWO).

- **show ip arp**
- **show route**

  (Correct)
- **tcpdump**
- **netstat**
- **show config**

  (Correct)
- **hostname**

Explanation
The configuration of the router can be displayed with SHOW commands.

Of the three show commands, *show ip arp* displays Address Resolution Protocol (ARP) cache, not the configuration of the devices.

Hence, two appropriate answers are:

1. show config

The **show config** command (or some variation of it) is used to examine the configuration of a network device. For example, on a Cisco router, the **show running-configuration** command permits you to see the current configuration of the device, which is stored in the RAM of the device. To view the saved configuration that is loaded when the system is rebooted, you can use the **show startup-configuration** command.

2. show route

The **show route** command (or some variation of it) is used to view the routing table configuration of the network device. On a Cisco router, you can use **show ip route** to view the IPv4 routing table.

Question 12:

Skipped

A network administrator is installing a wireless network at a client's office.

Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

- **GSM**
- **CSMA/CD**
- **CSMA/CA**

  (Correct)
- **CDMA**

Explanation

CDMA and GSM are for mobile network.

CSMA/CD is for wired Ethernet network.

CSMA/CA is for wireless network.

Question 13:

Skipped

A network administrator is configuring a load balancer for two systems.

Which of the following must the administrator configure to ensure connectivity during a failover?

- **Broadcast IP**
- **NAT**
- **VIP**

  (Correct)
- **IPv6 tunneling**
- **APIPA**

Explanation
If the systems are in different subnets, the virtual IP address can be set at the level of a load balancer. The load balancer is configured with the two physical IP addresses of the two systems in their respective subnets. And the load balancer routes the traffic according a health check to systems.

Question 14:
Skipped
Which of the following services can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices?

- **DaaS**
- **SaaS**

- **PaaS**
- **IaaS**

  (Correct)

Explanation
Saas, PaaS and DaaS do not provide hardware options. Only IaaS provides to customers the options to pick their desired hardware types.

Question 15:
Skipped
Branch users are experiencing issues with videoconferencing.

Which of the following will the company MOST likely configure to improve performance for these applications?

- **Quality of service**

  (Correct)
- **Network load balancer**
- **Dynamic routing**
- **Link Aggregation Control Protocol**
- **Static IP addresses**

Explanation

If you need to control how much of your bandwidth is used for certain devices or applications, quality of service (QoS) policies should be used to prioritize traffic based on certain rules. These rules control how much bandwidth a protocol, application PC, user, VLAN, or IP address may use.

In this situation, configuring QoS to assign higher priority to video conferencing traffic will help improve its performance.

Question 16:

Skipped

A network engineer is investigating reports of poor network performance. Upon reviewing a device configuration, the engineer finds that duplex settings are mismatched on both ends.

Which of the following would be the MOST likely result of this finding?

- **Increased device temperature**
- **Increased CRC errors**

  (Correct)
- **Increased switching loops**
- **Increased giants and runts**

Explanation

On an Ethernet connection, a **duplex mismatch** is a condition where two connected devices operate in different duplex modes, that is, one operates in half duplex while the other one operates in full duplex. The effect of a duplex mismatch is a link that operates inefficiently.

Communication *is* possible over a connection in spite of a duplex mismatch. Single packets are sent and acknowledged without problems. As a result, a simple ping command fails to detect a duplex mismatch because single packets and their resulting acknowledgments at 1-second intervals do not cause any problem on the network. A

terminal session which sends data slowly (in very short bursts) can also communicate successfully. However, as soon as either end of the connection attempts to send any significant amount of data, the network suddenly slows to very low speed. Since the network is otherwise working, the cause is not so readily apparent.

A duplex mismatch causes problems when both ends of the connection attempt to transfer data at the same time. This happens even if the channel is used (from a high-level or user's perspective) in one direction only, in case of large data transfers. Indeed, when a large data transfer is sent over a TCP, data is sent in multiple packets, some of which will trigger an acknowledgment packet back to the sender. This results in packets being sent in both directions at the same time.

In such conditions, the full-duplex end of the connection sends its packets while receiving other packets; this is exactly the point of a full-duplex connection. Meanwhile, the half-duplex end cannot accept the incoming data while it is sending – it will sense it as a collision. The half-duplex device ceases its current data transmission, sends a jam signal instead and then retries later as per CSMA/CD. This results in the full-duplex side receiving an incomplete frame with CRC error or a runt frame. It does not detect any collision since CSMA/CD is disabled on the full-duplex side. As a result, when both devices are attempting to transmit at (nearly) the same time, the packet sent by the full-duplex end will be discarded and lost due to an assumed collision and the packet sent by the half duplex device will be delayed or lost due to a CRC error in the frame.

Question 17:

Skipped

A network requirement calls for segmenting departments into different networks. The campus network is set up with users of each department in multiple buildings.

Which of the following should be configured to keep the design simple and efficient?

- **MDIX**
- **Flow control**
- **Jumbo frames**
-

Port tagging

(Correct)

Explanation
A Virtual Local Area Network is a method used to segment networks without the need to physically run cables to separate hardware. In this situation, VLAN is the best solution to meet the requirement.

One of the mechanism to enable VLAN is port tagging which indicates the VLAN a port belongs to.

Question 18:
Skipped
Which of the following protocols will a security appliance that is correlating network events from multiple devices MOST likely rely on to receive event messages?

- **Secure File Transfer Protocol**
- **Syslog**

  (Correct)
- **Server Message Block**
- **Session Initiation Protocol**

Explanation
The security appliance that is correlating network events from multiple devices is normally called SIEM (security information and event management).

Syslog is a widely used logging standard that is applicable to most SIEM systems, such as IBM QRadar and HP ArcSight.

Question 19:
Skipped

An engineer is configuring redundant network links between switches.

Which of the following should the engineer enable to prevent network stability issues?

- **Flow control**
- **CSMA/CD**
- **802.1Q**
- **STP**

(Correct)

Explanation
Redundant network links between switches might cause layer 2 loop that can be prevented by Spanning Tree Protocol (STP).

The Ethernet standards body adopted the *Spanning Tree Protocol (STP)* to eliminate the problem of accidental switching loops. For decades, switches have had STP enabled by default, and can detect potential loops before they happen. Using special STP frames known as *bridge protocol data units (BPDUs)*, switches communicate with other switches to prevent loops from happening in the first place.

Question 20:
Skipped
A network engineer configured new firewalls with the correct configuration to be deployed to each remote branch. Unneeded services were disabled, and all firewall rules were applied successfully.

Which of the following should the network engineer perform NEXT to ensure all the firewalls are hardened successfully?

- **Update the firewalls with current firmware and software**

- **Configure the log settings on the firewalls to the central syslog server**

  (Correct)

- **Use the same complex passwords on all firewalls**

- **Ensure an implicit permit rule is enabled**

Explanation
Implicit permit rule is not appropriate for firewalls. Rule should be implicit deny.

Since new firewalls with the correct configuration has been configured, so it implies that the password, firmware and software have been configured properly already.

Hence, the next thing the administrator should do is to configure the log settings on the firewalls to the central syslog server.

Question 21:
Skipped
A network administrator is talking to different vendors about acquiring technology to support a new project for a large company.

Which of the following documents will MOST likely need to be signed before information about the project is shared?

- **MOU**

- **NDA**

  (Correct)

-

SLA

- **BYOD policy**

Explanation
To protect the confidential of the new project and its purposes, NDA should be signed with external vendors.

A **non-disclosure agreement** (**NDA**), also known as a **confidentiality agreement** (**CA**), **confidential disclosure agreement** (**CDA**), **proprietary information agreement** (**PIA**), **secrecy agreement** (**SA**), or **non-disparagement agreement**, is a legal contract or part of a contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to.

Question 22:
Skipped
A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection.

Which of the following access methods would provide the BEST security for this new datacenter?

- **Virtual network computing**
- **In-band connection**
- **Secure Socket Shell**
- **Site-to-site VPN**

(Correct)

Explanation

In-band connection manages the network through the network itself. Management traffic and data traffic share the same infrastructure. This has lower security posture than out of band connection.

Secure Shell (SSH) is a cryptographic protocol that provides communications security over a computer network, connecting an SSH client application with an SSH server. SSH is not used for connecting two datacenters.

Virtual networking is not appropriate here. The company aims to connect two physical datacenters, so it should use "physical" networking.

Site-to-site VPN refers to a connection set up between multiple sites (networks/datacenters). This is the most appropriate solution for this situation.

Question 23:

Skipped

An administrator would like to create a fault-tolerant ring between three switches within a Layer network.

Which of the following Ethernet features should the administrator employ?

- **Port mirroring**
- **Open Shortest Path First**
- **An interior gateway protocol**
- **Spanning Tree Protocol**

  (Correct)

Explanation

Fault-tolerant ring between three switches creates Layer 2 loop (switching loop) within this network segment.

In the early days of switches, making a Layer 2 loop in a network setup would bring the network crashing down. A frame could get caught in the loop, so to speak, and not reach its destination.

The Ethernet standards body adopted the *Spanning Tree Protocol (STP)* to eliminate the problem of accidental switching loops. For decades, switches have had STP enabled by default, and can detect potential loops before they happen

Question 24:

Skipped

A fiber link connecting two campus networks is broken.

Which of the following tools should an engineer use to detect the exact break point of the fiber link?

- **Cable tester**
- **PoE injector**
- **Tone generator**
- **OTDR**

  (Correct)
- **Fusion splicer**

Explanation

An optical time domain reflectometer (OTDR) is a device used to precisely detect faults in an optical fiber link of a communication network. Its function includes generation and transmission of a series of high-speed optical pluses within the fiber.

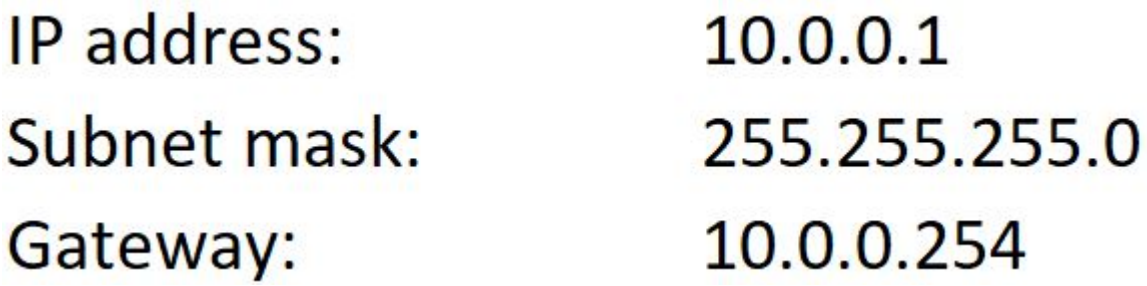
Fiber communication system maintenance depends on optical time domain reflectometers. An OTDR simply generates a pulse inside a fiber to be tested for faults

or defects. Different events within the fiber create a Rayleigh back scatter. Pulses are returned to the OTDR and their strengths are then measured and calculated as a function of time and plotted as a function of fiber stretch. The strength and returned signal tell about the location and intensity of the fault present.

Question 25:

Skipped

The following configuration is applied to a DHCP server connected to a VPN concentrator:



There are 300 non-concurrent sales representatives who log in for one hour a day to upload reports, and 252 of these representatives are able to connect to the VPN without any Issues. The remaining sales representatives cannot connect to the VPN over the course of the day.

Which of the following can be done to resolve the issue without utilizing additional resources?

- **Decrease the lease duration**

  (Correct)

- **Reboot the DHCP server**

- **Configure a new router**

- **Install a new VPN concentrator**

Explanation
With the network 10.0.0.0/24, there are 252 available addresses for VPN clients. Rebooting DHCP server, installing new VPN concentrator, or configurating new router do not change this limitation. There are maximum 252 VPN sessions at any moment. However, since the connections from sale reps are non-concurrent, the issue can be fixed by reducing the lease duration of IP.

Question 26:

Skipped

A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port.

Which of the following commands should the administrator use to accomplish this goal?

- **arp -a**
- **nslookup**
- **netstat -a**

  (Correct)
- **ipconfig /a**

Explanation
The quickest way to get an overview of the ports used by the system and their status is to issue the **netstat -a** command from the command line.

Question 27:

Skipped

A technician is writing documentation regarding a company's server farm. The technician needs to confirm the server name for all Linux servers.

Which of the following commands should the technician run?

-

route

- **nslookup**

  (Correct)

- **arp**

- **ipconfig**

Explanation
With nslookup, you can (assuming you have the permission) query all types of information from a DNS server and change how your system uses DNS. You can run nslookup in noninteractive or interactive mode. If you just want a quick query, use the former. Type `nslookup` followed by the desired IP address or name; if you want to, you can specify a DNS server by adding that after.

Question 28:

Skipped

A network administrator redesigned the positioning of the APs to create adjacent areas of wireless coverage. After project validation, some users still report poor connectivity when their devices maintain an association to a distanced AP.

Which of the following should the network administrator check FIRST?

- **Check to see if MU-MIMO was properly activated on the APs**

- **Verify that the AP antenna type is correct for the new layout**

- **Validate the roaming settings on the APs and WLAN clients**

  (Correct)

- **Deactivate the 2.4GHz band on the APs**

Explanation
With multiple WAPs in an ESS, clients connect to whichever WAP has the strongest signal. As clients move through the space covered by the broadcast area, they change WAP connections seamlessly, a process called *roaming*.

After creating adjacent areas of wireless coverage, users still have access to distanced AP is the signal of suboptimal roaming configuration. Hence, the administrator should validate the roaming settings on the APs and WLAN clients.

Question 29:
Skipped
A technician is installing multiple UPS units in a major retail store. The technician is required to keep track of all changes to new and old equipment.

Which of the following will allow the technician to record these changes?

- **Asset tags**

  (Correct)

- **A camera**

- **A smart locker**

- **An access control vestibule**

Explanation
Many companies employ RFID and other electronic devices as *asset tags* for inventory control purposes. In this situation, asset tags should be utilized to keep track of all UPS units.
Question 30:
Skipped

After the A record of a public website was updated, some visitors were unable to access the website.

Which of the following should be adjusted to address the issue?

- **SOA**
- **TTL**

  (Correct)
- **MX**
- **TXT**

Explanation
SOME, not ALL users report the issue. So MX, TXT and SOA records are less likely the one that should be adjusted.

“How do all these DNS servers know to refresh the records they store in their cache with fresh information from the authoritative name servers?” That is controlled by a *time to live (TTL)* field on every DNS record. This field indicates the number of seconds that administrators want DNS resolvers to hold records in their caches before removing the cached record.

A short TTL time means that people will see DNS record updates faster (for instance, if you have moved your Web site to a new server). A longer TTL means the records will be held in caches longer. If TTL is too long, some users will not be able to access the website with new address.

Question 31:
Skipped
A network administrator wants to analyze attacks directed toward the company's network.

Which of the following must the network administrator implement to assist in this goal?

- **A honeypot**

  (Correct)

- **A screened subnet**

- **Network segmentation**

- **Antivirus**

Explanation
When we talk about network security, honeypots and honeynets are often mentioned. Honeypots are a rather clever approach to network security but perhaps a bit expensive. A *honeypot* is a system set up as a decoy to attract and deflect attacks from hackers. The server decoy appears to have everything a regular server does—OS, applications, and network services. The attacker thinks she is accessing a real network server, but she is in a network trap.

The honeypot has two key purposes. It can give administrators valuable information on the types of attacks being carried out. In turn, the honeypot can secure the real production servers according to what it learns. Also, the honeypot deflects attention from working servers, allowing them to function without being attacked.

Question 32:
Skipped
Which of the following technologies provides a failover mechanism for the default gateway?

- **OSPF**

- **STP**

- **LACP**
- **FHRP**

  (Correct)

Explanation
Building with high availability in mind extends to more than just servers; a default gateway, for example, is a critical node that can be protected by adding redundant backups. Protocols that support HA and redundancy are referred to as *first hop redundancy protocols (FHRPs)* and include the open standard *Virtual Router Redundancy Protocol (VRRP)* and the Cisco-proprietary *Hot Standby Router Protocol (HSRP)* and *Gateway Load Balancing Protocol (GLBP)*. The nice thing about VRRP, HSRP, and GLBP is that, conceptually, they perform the same function. They take multiple routers and gang them together into a single virtual router with a single *virtual IP (VIP)* address that clients use as a default gateway. This includes making redundant firewalls on the redundant routers! GLBP takes things a step further, providing full load balancing as well.

Question 33:

Skipped

An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch.

Which of the following command-line tools should the technician use to determine where the incident is occurring?

- **show config**
- **show counters**
- **netstat**
-

nslookup

- **show interface**

  (Correct)

Explanation
Show interface command lists out current status of a interface. If connection between the interface and core switch has been broken, output of this command will clearly show that information.

Question 34:
Skipped
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds that jitter at the office is greater than 10ms on the only WAN connection available.

Which of the following would be MOST affected by this statistic?

- **An in-office video call with a coworker**
- **A VoIP sales call with a customer**

  (Correct)
- **Firewall CPU processing time**
- **Routing table from the ISP**

Explanation
High jitter does not significantly impact the convergent time of routing protocol or CPU processing time of firewall.

In-office video call will not be impact since the video call is between endpoints within the same office that do not run over WAN link.

VoIP call with external customer will be impacted seriously with this high jitter.

Question 35:

Skipped

Several WIFI users are reporting the inability to connect to the network. WLAN users on the guest network are able to access all network resources without any performance issues. The following table summarizes the findings after a site survey of the area in question:

Location	AP 1	AP 2	AP 3	AP 4
SSID	Corp1	Corp1	Corp1/Guest	Corp1/Guest
Channel	2	1	5	11
RSSI	-81dBm	-82dBm	-44dBm	-41dBm
Antenna type	Omni	Omni	Directional	Directional

Which of the following should a wireless technician do NEXT to troubleshoot this issue?

- **Reconfigure the channels to reduce overlap**

  (Correct)

- **Decrease power in AP 3 and AP 4**

- **Update the SSIDs on all the APs**

- **Replace the omni antennas with directional antennas**

Explanation

With the results of site survey, it is obvious that there are two possible reasons of the inability tonaccess issue. First is the low signal from AP 1 and AP 2. Second is the channel interefence of AP 1 and AP 2.

Of the four answers, reconfiguring channels to reduce overlap should be the one to do next. It is easy to do and does not require to replace hardware (comparing to the option of replacing omni antennas with directional antennas).

Question 36:

Skipped

Which of the following routing protocols is used to exchange route information between public autonomous systems?

- **OSPF**
- **EIGRP**
- **BGP**

  (Correct)
- **RIP**

Explanation

When routers in one AS need to communicate with routers in another AS, they use an Exterior Gateway Protocol (EGP). The network or networks within an AS communicate with protocols as well: Interior Gateway Protocols (IGPs).

OSPF, EIGRP and RIP are all IGPs.

BGP is EGP.

The easy way to keep these terms separate is to appreciate that although many protocols can be used within each Autonomous System, the Internet uses a single protocol for AS-to-AS communication: the Border Gateway Protocol (BGP). BGP is the glue of the Internet, connecting all of the Autonomous Systems

Question 37:

Skipped

A technician is connecting DSL for a new customer. After installing and connecting the on-premises equipment, the technician verifies DSL synchronization. When connecting to a workstation, however, the link LEDs on the workstation and modem do not light up.

Which of the following should the technician perform during troubleshooting?

- **Look for a rogue DHCP server on the network.**
- **Replace the cable connecting the modem and the workstation.**

  (Correct)
- **Identify the switching loops between the modem and the workstation.**
- **Check for asymmetrical routing on the modem.**

Explanation
The link LEDs on the workstation and modem do not light up indicates Layer 1 issue that should be troubleshooted by checking and replacing the cable connecting the modem and the workstation.

Question 38:

Skipped

Which of the following transceiver types can support up to 40Gbps?

- **QSFP**
- **SFP**
- **QSFP+**

  (Correct)
- **SFP+**

Explanation
Way back in 2010, the IEEE 802.3ba committee approved standards for 40- and 100-Gb Ethernet, 40 Gigabit Ethernet (40 GbE) and 100 Gigabit Ethernet (100 GbE), respectively. Both standards, in their many varieties, use the same frame as the slow-by-comparison earlier versions of Ethernet, so with the right switches, you've got perfect interoperability. The 40 GbE and 100 GbE standards are primarily used when lots of bandwidth is needed, such as connecting servers, switches, and routers.

Common 40 GbE runs on OM3 or better multimode fiber, uses laser light, and uses various four-channel connectors. A typical connector is called an enhanced quad small form-factor pluggable (QSFP+), essentially taking four SFP+ transceivers and squashing them into a single, wider transceiver. Other 40 GbE standards run on single-mode fiber and can do distances up to 10 km. Still other 40 GbE connections run on Cat 8 UTP for an underwhelming 30 meters.

Question 39:
Skipped
Which of the following systems would MOST likely be found in a screened subnet?

- **RADIUS**
- **LDAP**
- **FTP**

  (Correct)
- **SQL**

Explanation
A ***screened subnet***—previously called a ***demilitarized zone (DMZ)***—often contains servers that should be accessible from the public Internet. With a screened subnet, for example, you could allow users on the Internet to initiate an email or web session coming into your organization's email or web server; however, you could block other protocols for those users.

Of those 4 server types, FTP or shared file server is the one should be put into this screened subnet or DMZ, enabling external users can send/receive files.

Question 40:

Skipped

A technician is connecting multiple switches to create a large network for a new office. The switches are unmanaged Layer 2 switches with multiple connections between each pair. The network is experiencing an extreme amount of latency.

Which of the following is MOST likely occurring?

- **A broadcast storm**

  (Correct)

- **Routing loops**

- **Ethernet collisions**

- **A DDoS attack**

Explanation

When an abnormally high number of broadcast packets are sent across the network within a short period of time, this is known as a *broadcast storm*, and it can degrade network performance as switches become overwhelmed with trying to keep up with the flood of packets.

A *switching loop* can occur any time there are multiple paths between two endpoints: more than one connection between two switches, for example. When there is a loop, it creates broadcast storms as broadcasts and multicasts are forwarded by switches out every port (the switches will repeatedly rebroadcast the messages, thus flooding the network). Layer 2 headers do not support a time to live (TTL) value, so a frame sent into a looped topology can loop forever.

Question 41:

Skipped

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- **Reservation**

  (Correct)

- **Dynamic assignment**

- **Exclusion**

- **Scope options**

- **Static assignment**

Explanation
MAC ***reservations*** is to enable DHCP to lease the same address to the same host each time. From then on, any time the system with that MAC address makes a DHCP Request, the reservation guarantees that that system will get the same IP address.
Question 42:
Skipped
A network technician needs to ensure outside users are unable to telnet into any of the servers at the datacenter.

Which of the following ports should be blocked when checking firewall configuration?

- **8080**

- **23**

(Correct)

- 80
- 3389
- 22

Explanation
Telnet uses port 23 that should be blocked in this situation.
Question 43:
Skipped
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

- Intrusion prevention
- Next-generation firewall

(Correct)

- Proxy server
- VPN headend
- Layer 3 switch

Explanation
Next Generation Firewall (NGFW) such as Cisco FTD (Firepower Threat Defense) can filter content, perform threat protection, and manage multiple IPSec site-to-site connections.

Question 44:

Skipped

A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

Software on the workstation needs to send a query to the local subnet broadcast address.

To which of the following addresses should the software be configured to send the query?

- **10.1.2.255**
- **10.1.2.0**
- **10.1.2.23**
- **10.1.2.1**
- **10.1.2.31**

(Correct)

Explanation
Network 10.1.2.0/27 has broadcast address of 10.1.2.31

Question 45:

Skipped

A network technician is installing new software on a Windows-based server in a different geographical location.

Which of the following would be BEST for the technician to use to perform this task?

- **RDP**

  (Correct)

- **SSH**

- **DNS**

- **FTP**

Explanation
To remotely control Windows-based server, RDP is the best choice.

For more information - Remote terminal programs all require a server and a client. The server is the computer to be controlled. The client is the computer from which you do the controlling. Citrix created a standard called Independent Computing Architecture (ICA) that defined how terminal information was passed between the server and the client. Citrix made a breakthrough product—so powerful that Microsoft licensed the Citrix code and created its own product called Windows Terminal Services. Not wanting to pay Citrix any more money, Microsoft then created its own standard called Remote Desktop Protocol (RDP) and unveiled a new remote terminal called Remote Desktop Connection (RDC) starting with Windows XP (so it's been around a long time).

Question 46:

Skipped

Which of the following TCP ports is used by the Windows OS for file sharing?

- **445**
- **53**

  (Correct)
- **1443**
- **389**

Explanation
TCP port 445 is used by SMB protocol in Windows systems for file sharing.
Question 47:
Skipped
Which of the following ports is commonly used by VoIP phones?

- **20**
- **5060**

  (Correct)
- **445**
- **143**

Explanation

Port 20 is for FTP.

Port 143 is for IMAP.

Port 445 is for SMB.

Port 5060 is for SIP, a telephony protocol.

Question 48:

Skipped

Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site.

Which of the following will BEST provide this functionality?

- **Split-tunnel VPN**
- **Client-to-site VPN**
- **Third-party VPN service**
- **Site-to-site VPN**

  (Correct)

Explanation

A site-to-site virtual private network (VPN) is a connection between two or more networks, such as a corporate network and a branch office network. Many organizations use site-to-site VPNs to leverage an internet connection or untrustworthy WAN for private traffic.

Question 49:

Skipped

Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

-

Zero Trust

- **TACACS+**

  (Correct)

- **Multifactor authentication**

- **Separation of duties**

- **SSO**

Explanation
Routers and switches need administration. In a simple network, you can access the administration screen for each router and switch by entering a username and password for each device. When a network becomes complex, with many routers and switches, logging into each device separately starts to become administratively messy. The answer is to make a single server store the ACL for all the devices in the network. To make this secure, you need to follow the AAA principles.

Terminal Access Controller Access Control System Plus (TACACS+) is a protocol developed by Cisco to support AAA in a network with many routers and switches. TACACS+ is very similar to RADIUS in function, but uses TCP port 49 by default and separates authorization, authentication, and accounting into different parts. TACACS+ uses PAP, CHAP, and MD5 hashes, but can also use Kerberos as part of the authentication scheme

Question 50:
Skipped
Which of the following connector types would have the MOST flexibility?

- **RJ45**

- **BNC**
- **LC**
- **SFP**

  (Correct)

Explanation
When you want to uplink one Ethernet switch to another, you might need different connectors (for example, for MMF, SMF, or UTP) for different installations. Fortunately, some Ethernet switches have one or more empty slots in which you can insert a gigabit interface converter (GBIC). GBICs are interfaces that have a bandwidth capacity of 1Gbps and are available with MMF, SMF, and UTP connectors. **This allows you to have flexibility in the uplink technology you use in an Ethernet switch.**

A smaller variant of a regular GBIC is the ***small form-factor pluggable (SFP)***, which is sometimes called a *mini-GBIC*. And to show the variety of *transceivers* you might encounter today, even this SFP has many variations, including the following:

Enhanced form-factor pluggable (SFP+)

Quad small form-factor pluggable (QSFP)

Enhanced quad small form-factor pluggable (QSFP+)

Of the four connector types, the one has the MOST flexibility is SFP

Question 51:
Skipped
At which of the following OSI model layers would a technician find an IP header?

- **Layer 3**

  (Correct)

- **Layer 1**
- **Layer 4**
- **Layer 2**

Explanation
IP header is a component of Internet Protocol (IP) that works at Network Layer (Layer 3).

Question 52:
Skipped
A technician is implementing a new wireless network to serve guests at a local office. The network needs to provide Internet access but disallow associated stations from communicating with each other.

Which of the following would BEST accomplish this requirement?

- **Port security**
- **DHCP snooping**
- **Device geofencing**
- **Wireless client isolation**

(Correct)

Explanation

You can set up *wireless client isolation* or *guest network isolation* on better wireless access points to protect the rest of your network. Both features work similarly, blocking access to other wireless clients and the wired network, while allowing Internet access. In a typical Wi-Fi setup, every wireless client is part of the same WLAN and can communicate with each other. Isolation blocks this feature, making it ideal for the public portion of a wireless network.