DUMPSARENA

Network Technology Associate

CIW 1D0-61C

Version Demo

Total Demo Questions: 9

Total Premium Questions: 92

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Networking Fundamentals	15
Topic 2, Networking Hardware	11
Topic 3, Networking Protocols and Services	11
Topic 4, Network Security	21
Topic 5, Wireless Networking	16
Topic 6, Emerging Technologies	17
Topic 7, Mix Questions	1
Total	92

QUESTION NO: 1

Jenny recently switched from broadband cable Internet to ADSL service with her local phone company. To economize, she chose the self-installation option. It appears that her ADSL modem is not allowing her to connect to the Internet.

Which setting should she check first?

A. Loopback address

B. Software version

C. Default gateway

D. Device name

ANSWER: C

Explanation:

The **Default gateway** setting should be checked first. A default gateway is the local router or modem interface to which a host sends traffic intended for networks outside its own local IP subnet. In a typical self-installed ADSL connection, the ADSL modem/router provides this gateway function for the home computer or LAN. If the computer has an incorrect gateway address, or no gateway configured, it may still communicate with devices on the local network but will have no route for Internet-bound packets. Confirming that the gateway address matches the ADSL modem/router's LAN address is therefore a fundamental early troubleshooting step. The setting can be supplied manually or automatically through DHCP, so checking the current network configuration also helps establish whether the computer successfully received usable settings from the modem/router. Microsoft's TCP/IP troubleshooting guidance identifies the default gateway as a key configuration value to verify when diagnosing network connectivity: TCP/IP addressing and subnetting. The IETF's IPv4 host requirements likewise defines the default gateway as the router used for forwarding packets beyond the local network: RFC 1122.

QUESTION NO: 2

The Internet has enabled many new anti-social activities, such as online stalking, cyberbullying, and addiction to solitary online activities.

Which choice is the most feasible way for schools and parents to reduce cyberbullying?

A. Monitor, track and record all online activity conducted by students.

B. Teach teens that the use of online communication is a freedom of expression.

C. Prevent students from accessing the Internet while at school so that they learn good habits.

D. Educate students about cyber-ethics and the consequences of questionable online behavior.

ANSWER: D

Explanation:

Educate students about cyber-ethics and the consequences of questionable online behavior is the most feasible approach because it addresses cyberbullying at its source: the choices students make when communicating online. Effective education helps learners recognize harmful conduct, understand that online actions can have real-world effects, develop empathy for others, and know how to report bullying safely. It can also establish clear expectations for respectful digital communication and reinforce that school conduct standards apply in online environments connected to the school community.

Schools and parents can support this approach through age-appropriate digital-citizenship lessons, discussions of privacy and responsible posting, clear anti-bullying policies, and consistent guidance on preserving evidence and seeking help. This is a practical, sustainable strategy because it builds judgment and responsible habits that students can apply across devices, platforms, and settings—not only on a particular network. The U.S. government's StopBullying.gov guidance emphasizes educating students and creating a safe, respectful environment as part of preventing cyberbullying. The Cybersecurity and Infrastructure Security Agency also provides digital-citizenship resources that promote safe and responsible technology use. See StopBullying.gov: Prevent Cyberbullying and CISA: K-12 Cybersecurity.

QUESTION NO: 3

Wireless networks are subject to more security issues than standard wired networks.

Which wireless security protocol can prevent unauthorized devices from connecting to the wireless network?

A. WPA2

B. RSA

C. AES

D. DES

ANSWER: A

Explanation:

WPA2 is the correct wireless security protocol because it controls access to a Wi-Fi network through authentication and encryption. A wireless client must successfully complete the WPA2 authentication process—typically by supplying the configured pre-shared key in a personal network or valid enterprise credentials in an enterprise deployment—before it can join the protected wireless network. This prevents devices that do not possess the required credentials from associating and gaining normal network access.

WPA2 uses the IEEE 802.11i security framework and is commonly implemented with AES-based CCMP protection. Its role is broader than merely encrypting individual data; it establishes a security mechanism for authenticating clients and protecting traffic after association. For a WPA2 deployment to provide meaningful access control, administrators should use a strong, unique passphrase for WPA2-Personal or centrally managed authentication for WPA2-Enterprise, and should disable insecure legacy modes. NIST wireless-security guidance describes the importance of using robust WLAN authentication and cryptographic protections: NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks. The Wi-Fi Alliance also identifies WPA2 as a Wi-Fi security certification based on strong authentication and data protection mechanisms: Wi-Fi Alliance: Wi-Fi Security.

QUESTION NO: 4

Configuring a wireless network involves several steps. Which of the following is a task that should be performed to configure and connect to a wireless network?

A. Configure a certificate authority and configure the trust settings.

B. Configure the wireless AP's SSID, encryption level and shared key.

C. Connect your computer to the same network hub as the wireless AP.

D. Connect your computer to the same network switch as the wireless AP.

ANSWER: B

Explanation:

Configuring the wireless AP's SSID, encryption level and shared key is the essential task for establishing a usable and protected wireless LAN. The SSID is the network name that identifies the WLAN to client devices. A wireless client must select or be configured with the appropriate SSID before it can attempt to join that WLAN. The access point's security configuration also determines how clients authenticate and protect traffic over the radio link. For a shared-key wireless deployment, the same pre-shared key must be configured on the access point and supplied to authorized client devices. The encryption/security mode and key must be compatible on both sides; otherwise, a client cannot successfully authenticate and connect. Current security guidance favors WPA3-Personal where available, or WPA2-Personal with AES/CCMP for compatible environments, using a strong unique passphrase. Cisco's wireless documentation describes configuring an SSID and assigning security settings as core WLAN configuration activities, while the National Institute of Standards and Technology provides wireless security guidance for protecting WLAN access and communications. See Cisco WLAN configuration documentation and NIST SP 800-153: Guidelines for Securing Wireless LANs.

QUESTION NO: 5

You are distributing a large video game file using BitTorrent. First, you upload the initial file and make it available via a central server called a tracker. Other users can then connect to the tracker and download the file. Each user who downloads the file makes it available to other users to download. The use of BitTorrent significantly reduces the original provider's hardware and bandwidth resource costs.

BitTorrent is an example of what type of network?

A. Centralized network

B. Client-server network

C. Peer-to-peer (P2P) network

D. Virtual private network

ANSWER: C

Explanation:

Peer-to-peer (P2P) network is correct because BitTorrent distributes content among participating users, called peers, rather than requiring the original publisher to deliver the complete file separately to every downloader. A file is divided into smaller pieces, and peers in the same torrent swarm can download pieces from multiple peers while simultaneously uploading pieces they have already obtained. As additional users participate, they contribute upload capacity, which spreads the bandwidth demand across the community and substantially reduces the bandwidth and hardware burden on the original content provider.

A tracker may assist peers in locating other participants in a swarm, but it does not change the fundamental P2P nature of the file-transfer model. Modern BitTorrent systems can also use decentralized peer-discovery mechanisms, such as Distributed Hash Tables. The defining characteristic remains that endpoint systems act in both roles: they consume data and provide data to others. This cooperative sharing model is particularly useful for large, popular files because availability and aggregate transfer capacity can grow as more peers join. The BitTorrent specification describes peers exchanging file pieces within a swarm: BitTorrent Protocol Specification (BEP 3). Additional protocol specifications, including decentralized tracker alternatives, are maintained at BEP 5: DHT Protocol.

QUESTION NO: 6

A network administrator wants workstations to receive an IP address, subnet mask, default gateway, and DNS server addresses automatically when they connect to the network.

Which service should the administrator configure?

A. DHCP

B. DNS

C. NAT

D. SMTP

ANSWER: A

Explanation:

DHCP is designed to automatically provide TCP/IP configuration settings to client devices. A DHCP server can lease an IP address and provide related options, including the subnet mask, default gateway, and DNS server addresses. This reduces manual configuration work and helps prevent addressing errors on networks with many clients.

DHCP leases are temporary assignments, allowing addresses to be reused when devices disconnect or no longer require them. DNS resolves names to IP addresses, but it does not normally assign IP configuration to clients. The DHCP protocol is defined in RFC 2131.

QUESTION NO: 7

Which port number is used by Secure Shell (SSH) by default?

A. 21

B. 22

C. 23

D. 443

ANSWER: B

Explanation:

Port 22 is correct. Secure Shell (SSH) is a protocol used to establish encrypted remote command-line sessions and to securely transfer files through related tools such as SCP and SFTP. Administrators commonly use SSH to manage network devices and servers remotely while protecting credentials and session data from interception.

SSH normally listens on TCP port 22, although an administrator can configure a service to use a different port. Port 23 is traditionally associated with Telnet, which does not encrypt its traffic. The Internet Assigned Numbers Authority lists SSH as using TCP port 22 in its Service Name and Transport Protocol Port Number Registry.

QUESTION NO: 8

ABC Company develops its own database applications. ABC is considering migrating to cloud services to accommodate the company's growth.

What strategy should ABC use to ensure continuous data protection if it begins using cloud services?

A. Cloud-only solution

B. Regional systems solution

C. Location systems solution

D. Multiple cloud-service providers

ANSWER: D

Explanation:

Multiple cloud-service providers is the appropriate strategy because it can provide independent redundancy for ABC's database data and recovery services. A resilient multi-cloud design copies data and maintains recoverable workloads in more than one provider environment, so protection does not depend solely on one provider's infrastructure, regional availability, account access path, or service outage response. For continuous protection, ABC should configure automated replication or frequent immutable backups, encrypt data in transit and at rest, define recovery-point and recovery-time objectives, and regularly test restoration from the alternate provider. Merely subscribing to more than one provider is not sufficient; the protection comes from deliberately maintaining independent, current, and tested copies of the database and the configuration needed to restore it. NIST emphasizes that cloud customers retain important responsibilities for data protection, availability planning, and understanding provider controls in cloud deployments. CISA likewise recommends resilience planning, including backups and tested recovery capabilities, to reduce the impact of disruptions. See NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing and CISA Cloud Security Technical Reference Architecture.

QUESTION NO: 9

Virtualization software transforms the hardware resources of a physical computer to create a fully functional virtual computer that can run its own operating systems and applications.

In addition to the CPU and RAM, which hardware resources are used by virtualization software?

A. Hard disk and USB devices

B. Hard disk and network devices

C. Virtual hard disk and network devices

D. Network devices and secondary storage devices

ANSWER: B

Explanation:

Hard disk and network devices is correct because a hypervisor must present more than processing and memory for a virtual machine to operate as a usable computer. It virtualizes storage by exposing virtual disks to the guest operating system. Those virtual disks are backed by physical storage on the host, such as internal disks, SAN storage, or other configured storage locations. The guest can then partition, format, and use its virtual disk in much the same way it would use a physical hard drive.

Virtualization software also provides virtual network adapters and virtual switches. These let a guest operating system communicate with other virtual machines, the host, and external networks while the hypervisor maps that traffic to available physical network interfaces. Together, virtual storage and virtual networking allow the guest to install an operating system, retain files and application data, and participate in network communications. Microsoft's Hyper-V documentation describes virtual machines as using virtual hard disks and virtual network adapters, while VMware's documentation explains that virtual machines use virtual hardware backed by host resources. See Microsoft Hyper-V overview and VMware virtual machine hardware documentation.