CS Exit Ethiopia

Questions & Worked Answers

Computer Science Exit Examination

101 complete questions

1 selected course | 18 November 2026

Selected courses

01. Network and System Administration

https://csexitethiopia.com

abelasnake2003@gmail.com | Telegram: @Abechu7

Course contents

Each course begins on a new page. PDF bookmarks provide question, study-note section and revision-topic navigation.

Network and System Administration 3

Reading the answers

Every question includes its answer, explanation, choice-by-choice contrasts and available evidence. Primary note proof quotes the study notes. Related reading and module passages are labelled separately; a module reference is not presented as primary note proof.

Network and System Administration

Questions & Worked Answers

101 questions

Question 1 | Q00011

You administer a network and need to display active connections with their protocol, local address and port, foreign address and port, and connection state. Which command provides this connection table?

A. traceroute

B. ipconfig

C. netstat

D. nslookup

Hint

Match the requested observation to the tool’s actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer C: netstat.

NSA07 identifies netstat as the tool that displays connections, protocol names, local and foreign endpoints, and TCP connection states. That is the complete set of information requested, so option C is right. Numeric-output flags can keep addresses and ports numeric; the Windows form netstat -ano also includes process IDs.

Why each choice is right or wrong

A - Incorrect: Traceroute reports responding hops on a network path, not a connection table with local/foreign ports and TCP states.

B - Incorrect: Ipconfig reports adapter addressing and configuration, not active transport connections and their remote endpoints.

C - Correct: Netstat displays the requested protocol, endpoint and connection-state information.

D - Incorrect: Nslookup queries DNS records rather than listing active connections or TCP states.

Primary note proof

Study-note section NSA07

> netstat displays connections/endpoints/protocols and TCP states; netstat -ano displays numeric addresses/ports and PIDs. Use the exact command name netstat rather than netstart. ping probes IP reachability; traceroute/tracert reveals responding hops using TTL/hop-limit expiry. ICMP filtering can prevent replies without proving the service is down. nslookup inspects DNS.

Study-note section NSA07

> Windows ipconfig shows addresses, mask and gateway; ipconfig /all adds complete adapter configuration including physical/MAC address, DHCP and DNS information. /renew requests renewal, /release releases a dynamic address and /flushdns clears the client DNS cache. Linux ip addr and ip route show interface addresses and routes; exact persistent configuration varies by distribution.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 2-7

> TCP and UDP must use port numbers to communicate with the upper layers, because they‘re what keep track of different conversations crossing the network simultaneously. These port numbers identify the source and destination application or process in the TCP segment. There are 216 = 65,536 ports available.

Data Communication and Computer Networking module | PDF page 27 | lines 29-31

> Traceroute Using ICMP timeouts, Traceroute is used to discover the path a packet takes as it traverses an Internetwork.

Question sources

MOE Computer Science Exit Exam · 2016 · Question 11

Question 2 | Q00077

Which statements about ordinary dynamic DHCP allocation are incorrect? Select all that apply.

A. An IP leased by the DHCP for a host is permanent

B. DHCP assures connectivity ever users move from location to location

C. The IP address are chosen from a predetermined range of address

D. DHCP allows a host to acquire an IP address automatically

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A, B: An IP leased by the DHCP for a host is permanent; DHCP assures connectivity ever users move from location to location

A dynamic DHCP lease lasts for a specified interval and must be renewed; it is not a permanent assignment. DHCP can automate address configuration after moving, but connectivity also depends on a reachable server or relay, a suitable scope and a working network. The server selects addresses from its configured pool. Thus the permanence and guaranteed-connectivity claims are false, while pool selection and automatic acquisition are true.

Why each choice is right or wrong

A - Correct: A leased dynamic address is time-limited and can become reusable after expiration; it is not permanent.

B - Correct: DHCP alone cannot assure connectivity after every location change; server, relay and network conditions matter.

C - Incorrect: A DHCP server manages an address scope/pool, supporting selection from a predetermined range.

D - Incorrect: Automatic acquisition of an address and options is a supported DHCP function.

Primary note proof

Study-note section NSA04

> DHCP supplies addresses and configuration options. Typical initial IPv4 allocation is Discover→Offer→Request→ACK. The server manages its scope/pool, allocated leases, exclusions and reservations; options may include mask, gateway and DNS servers. A dynamic lease lasts for a specified interval, not forever.

Study-note section NSA05

> Use a scope matching the subnet, exclude manually assigned server/router addresses, set correct options and provide a relay when client broadcasts must cross a router. Static assignments and DHCP can coexist; avoid address conflicts. DHCP lowers repetitive administration but availability/security depend on deployment and protection from rogue replies. It does not guarantee connectivity whenever a device changes location.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

> The Process/Application Layer Protocols
> • Telnet
> • File Transfer Protocol (FTP)
> • Network File System (NFS).
> • Simple Mail Transfer Protocol (SMTP
> • POP3 is used to receive mail.
> • Simple Network Management Protocol (SNMP)
> • Domain Name Service (DNS)
> • Dynamic Host Configuration Protocol (DHCP)

Question sources

MOE Computer Science Exit Exam · 2016 · Question 77

Question 3 | Q00091

Which listed operation is not a DHCP server function?

A. It grants an IP address when receives a request from a client.

B. It maintains the information about client configuration parameters.

C. It maintains a database of available IP addresses.

D. Resolve hostnames to IP addresses using DNS records.

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: Resolve hostnames to IP addresses using DNS records.

A DHCP server manages address pools, lease allocations and configuration parameters supplied to clients. It may allocate an address in response to a client exchange and retain information about availability and options. Hostname-to-address resolution is a DNS function instead. Repairing the duplicated malformed option supplies a distinct nonfunction while preserving the original distinction between automatic configuration and other network services.

Why each choice is right or wrong

A - Incorrect: Allocating an address in response to client requests is a DHCP server function.

B - Incorrect: The server manages lease and configuration parameters, so this is not a nonfunction.

C - Incorrect: Maintaining scope/pool availability is explicitly part of DHCP server management.

D - Correct: Hostname-to-address resolution belongs to DNS rather than DHCP allocation.

Primary note proof

Study-note section NSA04

> DHCP supplies addresses and configuration options. Typical initial IPv4 allocation is Discover→Offer→Request→ACK. The server manages its scope/pool, allocated leases, exclusions and reservations; options may include mask, gateway and DNS servers. A dynamic lease lasts for a specified interval, not forever.

Study-note section NSA06

> Forward resolution obtains an address from a name, using A for IPv4 and AAAA for IPv6. Reverse lookup uses a PTR record in the reverse namespace to obtain a name from an address. CNAME aliases a name, MX identifies mail exchangers and NS identifies authoritative name servers. Forward and reverse records need not both exist or be perfect inverses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

MOE Computer Science Exit Exam · 2016 · Question 91

Question 4 | Q00185

Based on the predefined policy of Network management, controlling access to the network is the task of

A. Fault Management

B. Performance Management

C. Security Management

D. Configuration Management

E. None

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer C: Security Management

PDF p.30 places restricting access to authorized users under security procedures. The requested access-control responsibility therefore matches Security Management.

Why each choice is right or wrong

A - Incorrect: Fault management concerns failures rather than the access authorization described on p.30.

B - Incorrect: Capacity/performance is a different responsibility (p.29), not authorization.

C - Correct: Security procedures explicitly ensure only authorized users have network access (p.30).

D - Incorrect: Configuration management is not the named access-security responsibility.

E - Incorrect: The security alternative directly matches the stated responsibility.

Primary note proof

Study-note section NSA01

Use documentation, standardization, least privilege, automation and measured change. Record the current state, intended change, rollback and validation. Schedule maintenance according to service impact and urgency, not merely because a calendar date arrived. Fault management restores failures; performance management measures service behavior; configuration management tracks settings; security management controls access; accounting tracks usage.

Study-note section NSA26

A security policy states required behavior, scope, accountable roles and enforcement. Begin with assets/service objectives, assess threats and weaknesses, choose controls, define exceptions/incident procedures, approve/communicate, monitor and periodically review. CIA means confidentiality, integrity and availability; neither sensitive-data protection nor availability alone is the universal primary goal.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Question sources

Addis Ababa University mock exam · Question 87

Question 5 | Q00186

A Unix utility which used for checking and repairing file system inconsistencies.

A. init

B. halt

C. inittab

D. fsck

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: fsck

NSA20 directly defines fsck as the filesystem-checking and optional repair utility. Repairs must follow the filesystem's supported safe or offline procedure. The alternatives refer to initialization/shutdown or an initialization configuration file, not the checking-and-repair role stated in the question.

Why each choice is right or wrong

A - Incorrect: Init concerns system initialization/service management rather than the filesystem-checking utility defined in NSA20.

B - Incorrect: Halt stops a system; it is not the utility for checking and repairing filesystem inconsistencies.

C - Incorrect: Inittab is an initialization configuration file, not the filesystem-checking command.

D - Correct: Fsck checks filesystems and can invoke filesystem-specific repair tools under supported safe conditions.

Primary note proof

Study-note section NSA20

> ext2 is a Linux filesystem; ext4 is a later filesystem; HPFS is historically associated with OS/2, while swap is backing space rather than an ordinary user-file filesystem. fsck checks and optionally repairs filesystems through filesystem-specific tools; it is not init, halt or an inittab file. Repairs require the filesystem's supported offline/safe procedure. Mount attaches a filesystem to a directory; partitioning, mounting, quotas and capacity belong to storage administration.

Study-note section NSA-S03

> In a traditional SysV-style system, init starts and supervises configured processes; /etc/inittab is its configuration file. The halt command stops the system through the supported shutdown procedure. Neither initialization, shutdown nor their configuration file is a filesystem-consistency check; fsck supplies that separate checking and optional repair role.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 61 | lines 26-36

> What is Unix/Linux?
> The Unix OS is a set of programs that act as a link between the computer and the user. The computer program that allocates the system resources and coordinates all the details of the computer‘s internals is called the operating system or the kernel. Users communicate with the kernel through a program known as the shell. The shell is a command line interpreter; it translates commands entered by the user and converts them into a language that is understood by the kernel.

Data Communication and Computer Networking module | PDF page 64 | lines 8-12

> /lost+found: Every partition has a lost+found for files
> that were saved during failures are here.
> /misc: For miscellaneous purposes.
> /mnt: Standard mount point for external file systems,
> e.g. a CD-ROM or a digital camera.

Question sources

Addis Ababa University mock exam · Question 88

Question 6 | Q00188

A PC obtains its IP address from a DHCP server. If the PC is taken off the network for repair, what happens to the IP address configuration?

A. The address is returned to the pool for reuse when the lease expires

B. The address lease is automatically renewed until the PC is returned

C. The configuration is held by the server to be reissued when the PC is returned

D. The configuration is permanent and nothing changes

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: The address becomes reusable when its lease expires

Taking the PC offline does not make the dynamic assignment permanent or cause endless automatic renewal. NSA04 says a disconnected client's lease can expire and the address then becomes eligible for reuse. On return, the client must validate, renew or obtain new configuration rather than assume it still owns its former address.

Why each choice is right or wrong

A - Correct: After expiry the address becomes eligible for return to the available pool, subject to server policy.

B - Incorrect: A disconnected client does not automatically renew indefinitely while it remains off the network.

C - Incorrect: The server need not hold the old address for that client after lease expiry without a reservation.

D - Incorrect: A dynamic lease has a finite interval and is not an unchanging permanent assignment.

Primary note proof

Study-note section NSA04

A client renews before expiry; it later tries rebinding if renewal fails. A disconnected host does not automatically renew forever. On lease expiry the address becomes eligible for reuse, subject to server policy. Reconnection normally triggers validation/renewal/new allocation, so an expired lease alone does not prove persistent failure. A reservation gives a predictable address to a known client while retaining DHCP configuration.

Study-note section NSA04

DHCP supplies addresses and configuration options. Typical initial IPv4 allocation is Discover→Offer→Request→ACK. The server manages its scope/pool, allocated leases, exclusions and reservations; options may include mask, gateway and DNS servers. A dynamic lease lasts for a specified interval, not forever.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Addis Ababa University mock exam · Question 90

Computer Science Exit Exam · Sene 2016 · Question 4-2

Computer Science Exit Exam practice collection · Question 161

Question 7 | Q00189

Which command in Microsoft Windows allows you to verify your IP address, subnet mask, default gateway, and MAC address?

A. C:\>ipconfig/all

B. C:\>ping

C. C:\>ipconfig

D. C:\>ipstatus

Hint

Match the requested observation to the tool's actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer A: ipconfig /all

The distinguishing requirement is the MAC address as well as IP, mask and gateway. NSA07 assigns this complete adapter detail to ipconfig /all; basic ipconfig covers the ordinary addressing summary. A displays the command with its /all switch. Ping tests reachability and ipstatus is not the defined Windows diagnostic.

Why each choice is right or wrong

A - Correct: The /all switch supplies the detailed adapter information, including the physical/MAC address requested.

B - Incorrect: Ping probes reachability rather than reporting the adapter's complete IP and MAC configuration.

C - Incorrect: Basic ipconfig reports IP, mask and gateway but omits the requested detailed physical/MAC information.

D - Incorrect: Ipstatus is not the Windows adapter-configuration command established by the complete note.

Primary note proof

Study-note section NSA07

> Windows ipconfig shows addresses, mask and gateway; ipconfig /all adds complete adapter configuration including physical/MAC address, DHCP and DNS information. /renew requests renewal, /release releases a dynamic address and /flushdns clears the client DNS cache. Linux ip addr and ip route show interface addresses and routes; exact persistent configuration varies by distribution.

Study-note section NSA07

> netstat displays connections/endpoints/protocols and TCP states; netstat -ano displays numeric addresses/ports and PIDs. Use the exact command name netstat rather than netstart. ping probes IP reachability; traceroute/tracert reveals responding hops using TTL/hop-limit expiry. ICMP filtering can prevent replies without proving the service is down. nslookup inspects DNS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 65 | lines 39-47

> Network configuration commands
> The ip Command
> The distribution-specific scripts and graphical tools
> are front-ends to ip (or ifconfig and route on older
> systems) to display and configure the kernel‘s
> networking configuration. The ip command is used for
> assigning IP addresses to interfaces, for setting up routes
> to the Internet and to other networks, for displaying
> TCP/IP

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

Ping (Packet Internet Groper) uses ICMP echo messages to check the physical and logical connectivity of machineson a network.

Question sources

Addis Ababa University mock exam · Question 91

Computer Science Exit Exam · Sene 2016 · Question 29-2

Computer Science Exit Exam practice collection · Question 160

Question 8 | Q00191

You are the administrator of an active directory domain. A user complains to you that he is unable to change his password. No other users have this issue. What is the most likely cause of the problem?

A. Insufficient login credentials

B. He is a member of the Administrators group

C. He is not a member of the domain

D. The property "User cannot change password" has been enabled when it was created

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: The account’s User cannot change password property

A failure isolated to one domain user favors inspecting that user’s permissions and cannot-change-password setting. D is the specific account control matching the symptom, and NSA17 explicitly identifies it as a plausible exam cause. It remains a most-likely option among these choices, not proof of its actual state: password age/rules and other account conditions would require real diagnosis.

Why each choice is right or wrong

A - Incorrect: Generic insufficient credentials gives no specific cause for this domain user’s isolated password-change restriction.

B - Incorrect: Administrators membership does not inherently prohibit users from changing their own passwords.

C - Incorrect: The scenario concerns a domain user; lacking domain membership is not the specific account restriction supported here.

D - Correct: The cannot-change-password setting directly blocks the operation and matches the isolated account symptom.

Primary note proof

Study-note section NSA17

If only one domain user cannot change a password, inspect that account's cannot-change-password setting and relevant policy/permission before blaming all directory infrastructure. Other possibilities include minimum password age, password rules or account state; the setting is a plausible exam cause, not a conclusion from failure alone. Membership in Administrators does not inherently prohibit changing one's password. Privileged reset and user-initiated password change are different operations.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 42 | lines 36-49

All user accounts have specific capabilities, privileges, and rights. When you create a user account, you can grant the user specific capabilities by making the user a member of one or more groups. This gives the user the capabilities of these groups. You then assign additional capabilities by making a user a member of the appropriate groups or withdraw capabilities by removing a user from a group. An important part of an administrator‘s job is being able to determine and set permissions, privileges, and logon rights as necessary. Although you can‘t change a group‘s built-in capabilities, you can change a group‘s default privileges and logon rights. For example, you could revoke network access to a computer by removing agroup‘s right to access the computer from the network.

Data Communication and Computer Networking module | PDF page 34 | lines 7-14

Domain Controllers
A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing end devices to access shared domain resources. It authenticates users, stores user account information and enforces security policy for a domain. It is most commonly implemented in Microsoft

Question sources

Addis Ababa University mock exam · Question 93

Question 9 | Q00353

Which is the most specific DNS term for obtaining an IP address from a hostname?

A. Forward resolution

B. Backward resolution

C. Binding

D. Resolving

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: Forward resolution

Forward resolution names the specific direction from a hostname to an address record. Resolving is a broader term that also includes this operation, so it is less specific than the requested answer. Reverse lookup goes from an address to a name, and binding is not the DNS operation defined here. Asking for the most specific term makes the overlapping general description a meaningful distractor.

Why each choice is right or wrong

A - Correct: Forward resolution is the precise name-to-address operation defined by NSA06.

B - Incorrect: Reverse lookup runs in the opposite direction, obtaining a name from an address.

C - Incorrect: Binding is not the note's term for the DNS name-to-address operation; LDAP bind authenticates a session.

D - Incorrect: Resolving includes forward lookup but is broader than the most specific term requested.

Primary note proof

Study-note section NSA06

> Forward resolution obtains an address from a name, using A for IPv4 and AAAA for IPv6. Reverse lookup uses a PTR record in the reverse namespace to obtain a name from an address. CNAME aliases a name, MX identifies mail exchangers and NS identifies authoritative name servers. Forward and reverse records need not both exist or be perfect inverses.

Study-note section NSA06

> Resolvers cache answers for their TTL. Query nslookup name or specify the DNS server explicitly; compare the configured resolver with the authoritative answer when appropriate. A successful ping by address but failed name lookup suggests naming/configuration trouble. Ping by name may display a resolved address, but nslookup is the direct DNS diagnostic. "Resolving" is a general term that includes forward resolution.

Study-note section NSA14

LDAP accesses directory entries/attributes identified by distinguished names. Bind authenticates a session; search retrieves matching entries; compare tests an attribute value; add/delete/modify change entries; modify-DN renames or moves; unbind ends the session. StartTLS upgrades a connection to TLS where supported; LDAPS uses TLS from connection setup. Protect credentials and verify server identity.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP
address, 127.0.0.1, which is
usedfor interprocess communication.
Never remove this line! Sometimes contains
addresses of additional hosts, whichcan be contacted
without using an external naming service such as
DNS (the Domain Name Server).

Question sources

Computer Science model exam · Question 84

University of Gondar model exam · Question 83

Question 10 | Q00354

You know a server hostname and want to query its DNS address records directly, optionally choosing the DNS server. Which listed diagnostic tool is designed for that task?

A. Nslookup

B. Ping command

C. Traceroute

D. Netstat

Hint

Match the requested observation to the tool’s actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer A: Nslookup

Nslookup directly queries DNS for the address records associated with a name and can use a specified DNS server. Ping may display a resolved address, but its principal task is testing IP reachability. Traceroute examines responding path hops, while netstat exposes endpoints and connection state. The direct-DNS-query requirement identifies the intended diagnostic without relying on incidental address displays from other commands.

Why each choice is right or wrong

A - Correct: Nslookup directly queries DNS records for the known name and is the conventional diagnostic here.

B - Incorrect: Ping primarily tests reachability; displaying a resolved address is not the direct DNS-record query requested.

C - Incorrect: Traceroute inspects responding hops rather than directly querying DNS address records.

D - Incorrect: Netstat reports existing endpoints/connections and is not a direct lookup for an arbitrary server name.

Primary note proof

Study-note section NSA06

> Resolvers cache answers for their TTL. Query nslookup name or specify the DNS server explicitly; compare the configured resolver with the authoritative answer when appropriate. A successful ping by address but failed name lookup suggests naming/configuration trouble. Ping by name may display a resolved address, but nslookup is the direct DNS diagnostic. “Resolving” is a general term that includes forward resolution.

Study-note section NSA07

> netstat displays connections/endpoints/protocols and TCP states; netstat -ano displays numeric addresses/ports and PIDs. Use the exact command name netstat rather than netstart. ping probes IP reachability; traceroute/tracert reveals responding hops using TTL/hop-limit expiry. ICMP filtering can prevent replies without proving the service is down. nslookup inspects DNS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

> Ping (Packet Internet Groper) uses ICMP echo
> messages to check the physical and logical
> connectivity of machineson a network.

Data Communication and Computer Networking module | PDF page 27 | lines 29-31

> Traceroute Using ICMP timeouts, Traceroute is
> used to discover the path a packet takes as it
> traverses an Internetwork.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

> /etc/hosts
> The /etc/hosts file always contains the localhost IP
> address, 127.0.0.1, which is
> usedfor interprocess communication.
> Never remove this line! Sometimes contains
> addresses of additional hosts, whichcan be contacted
> without using an external naming service such as
> DNS (the Domain Name Server).

Question sources

Computer Science model exam · Question 85

University of Gondar model exam · Question 84

Question 11 | Q00355

LAN clients must reach public IPv4 destinations through a gateway with working routes. Which listed address situation commonly calls for source NAT at that gateway?

A. Default gateway of LAN isn't configured

B. Global IP address is used in the LAN

C. He/she don't know type of IP address used in the LAN

D. Private IP address is used in the LAN

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: Private IP address is used in the LAN

Private IPv4 addresses are not directly routed as public Internet destinations. A gateway can translate those source addresses, often using port bindings so several clients share a public address. This works together with valid routing and the external connection. A missing default gateway must be repaired separately, and public addressing or uncertainty about the current configuration is not by itself a reason to enable NAT.

Why each choice is right or wrong

A - Incorrect: A missing gateway requires routing configuration; address translation is not a replacement for it.

B - Incorrect: Public addressing in a LAN does not automatically require address translation.

C - Incorrect: Not knowing the address type calls for inspecting configuration, not blindly enabling NAT.

D - Correct: Private IPv4 clients commonly need source translation when reaching public destinations through this gateway.

Primary note proof

Study-note section NSA03

An IPv4 address is 32 bits; a CIDR prefix determines its network. Compute network=address AND mask; devices use a route/gateway for remote subnets. Private ranges are 10/8,172.16/12 and 192.168/16; private addresses are not directly Internet-routable. Neither IP alone nor a class label determines today's subnet.

Study-note section NSA11

Routing selects a next hop using a destination prefix; NAT rewrites addresses. Many-to-one address-and-port translation (PAT/NAPT) maps internal flows to one public address using distinct port bindings. For example, two private client sockets can appear as public-address ports 40001 and 40002, with replies translated back to the correct clients.

Study-note section NSA11

NAT is often used when private IPv4 clients access public networks; it does not itself replace a gateway, route, firewall or authentication. One-to-one NAT and destination translation are other forms, so NAT does not always mean many hosts share one address. Public addressing inside a LAN does not automatically require NAT. Unsolicited inbound service access may require explicit mapping and filtering.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Computer Science model exam · Question 86

University of Gondar model exam · Question 85

Question 12 | Q00356

Which single option gives the complete set of scenarios where DHCP can meet the stated address-management goal, assuming a correctly deployed service?

A. A small network needing automatic host address configuration.

B. Fixed-purpose devices needing predictable addresses through DHCP reservations.

C. A large device population needing centrally managed address configuration.

D. All are correct

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: All are correct

DHCP can reduce repetitive configuration in small as well as large networks. Reservations allow a known device to receive a predictable address while retaining centrally supplied options. A complex population of clients may also benefit from centrally managed scopes and configuration. The scenarios state these goals rather than treating size or complexity alone as a mandate. Each individual option is valid but incomplete as the requested complete set.

Why each choice is right or wrong

A - Incorrect: DHCP can automate this small network, but A alone omits the other qualifying scenarios.

B - Incorrect: Reservations meet the predictable-address goal, but B alone is incomplete.

C - Incorrect: Centralized DHCP management can meet this goal, but C alone is incomplete.

D - Correct: All three stated goals can be met by an appropriately configured DHCP service.

Primary note proof

Study-note section NSA04

> A client renews before expiry; it later tries rebinding if renewal fails. A disconnected host does not automatically renew forever. On lease expiry the address becomes eligible for reuse, subject to server policy. Reconnection normally triggers validation/renewal/new allocation, so an expired lease alone does not prove persistent failure. A reservation gives a predictable address to a known client while retaining DHCP configuration.

Study-note section NSA05

> Use a scope matching the subnet, exclude manually assigned server/router addresses, set correct options and provide a relay when client broadcasts must cross a router. Static assignments and DHCP can coexist; avoid address conflicts. DHCP lowers repetitive administration but availability/security depend on deployment and protection from rogue replies. It does not guarantee connectivity whenever a device changes location.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

> The Process/Application Layer Protocols
> • Telnet
> • File Transfer Protocol (FTP)
> • Network File System (NFS).
> • Simple Mail Transfer Protocol (SMTP
> • POP3 is used to receive mail.
> • Simple Network Management Protocol (SNMP)
> • Domain Name Service (DNS)
> • Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science model exam · Question 87

University of Gondar model exam · Question 86

Question 13 | Q00550

A disconnected client returns after its old DHCP lease expired. The correct scope has 20 assignable addresses, all now leased to other active clients; the server and relay are reachable. What best explains why the returning client cannot obtain an address?

A. the IP address lease has expired on the DHCP server.

B. the DHCP scope needs to be redefined.

C. the DHCP pool limit has been reached.

D. the DHCP server needs to be restarted.

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C: the DHCP pool limit has been reached.

A reachable DHCP service still needs an available address in the correct pool. Here all twenty assignable addresses are already leased to other active clients, so the returning client cannot receive a free dynamic allocation. Its expired lease permits reuse but does not alone explain persistent failure after reconnection. The pool-capacity observation supplies the diagnosis; it does not establish a need to redefine the scope or restart the server.

Why each choice is right or wrong

A - Incorrect: The old lease expired, but normal reacquisition would succeed if pool capacity remained; expiry alone is insufficient.

B - Incorrect: The scope is correct; the evidence identifies exhausted capacity rather than an incorrect subnet definition.

C - Correct: All assignable pool addresses are leased, so the pool limit prevents a new allocation.

D - Incorrect: The server is reachable and processing requests; a restart does not create free pool capacity.

Primary note proof

Study-note section NSA04

A client renews before expiry; it later tries rebinding if renewal fails. A disconnected host does not automatically renew forever. On lease expiry the address becomes eligible for reuse, subject to server policy. Reconnection normally triggers validation/renewal/new allocation, so an expired lease alone does not prove persistent failure. A reservation gives a predictable address to a known client while retaining DHCP configuration.

Study-note section NSA05

For a returning client, inspect current lease/address, reachable server/relay, free pool capacity and logs. New devices can exhaust a pool, but absent observations this is only a hypothesis. Some clients self-configure IPv4 link-local addresses such as 169.254.2.33 after DHCP failure; these support same-link communication, not ordinary routed Internet access. 0.0.0.0 is unspecified and 255.255.255.255 is limited broadcast.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science model exam · 2015 · Question 19

Question 14 | Q00563

After a NIC replacement, the adapter is recognized and enabled in firmware and Device Manager, but there is no link light. On the same switch port, replacing only the CAT5 cable with a known-good cable restores connectivity. Which listed fault is isolated?

A. the CAT5 cable is defective

B. the NIC is disabled in BIOS

C. The NIC is disabled in Device Manager

D. The RJ11 jack is defective

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: the CAT5 cable is defective

The test changes one relevant factor while keeping the adapter and switch port unchanged. Connectivity returns with a known-good cable, which isolates the original cable or its terminations as the failing component. The explicit enabled-state checks exclude the two disabling explanations. RJ11 is a telephone connector rather than the Ethernet connection being tested, so it does not describe the observed fault.

Why each choice is right or wrong

A - Correct: Replacing only the cable restores the link, isolating the original CAT5 cable or its terminations.

B - Incorrect: The adapter is explicitly enabled in firmware.

C - Incorrect: The adapter is explicitly enabled in Device Manager.

D - Incorrect: RJ11 is a telephone connector, not the expected Ethernet RJ45 connection in this NIC scenario.

Primary note proof

Study-note section NSA09

> Check power, cable/connector and link state, then NIC/driver state, VLAN membership, address/prefix, local gateway, route, DNS and finally application port/authentication. A recognized NIC makes a missing driver less likely, not proof of a working physical link. Ethernet commonly uses RJ45 connectors; an RJ11 telephone jack is not the expected Ethernet connection.

Study-note section NSA09

> If same-subnet traffic works but remote traffic fails, compare gateway/routes and filtering. If ping fails but the application connection works, ICMP filtering is plausible. If an application port is refused, the destination is reachable enough to reject it; inspect service/listener policy. A timeout can result from loss, filtering or a down host and needs more evidence.

Study-note section NSA08

Define the symptom, scope, time and recent changes; gather the configuration, baseline and logs. Form a testable hypothesis, test the least disruptive explanation, isolate the failing component, apply a targeted fix, verify the user service and document the result. Change one relevant factor at a time when possible. A reboot can hide evidence and is not a diagnosis by itself.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 16-18

• Diagnosing and troubleshooting problems on the network and determining the best course of action to take to solve them.

Question sources

Computer Science model exam · 2015 · Question 32

Question 15 | Q00586

Permissions of a file are represented by which of the following characters?

A. r,w,x

B. w,x

C. x,w,e

D. x,w

Hint

Identify the platform and permission model; for an rwx string, separate owner/group/other triplets and use the stated bit weights.

Answer A: r, w and x

NSA19 groups ordinary Unix permission bits into owner/group/other triplets, each containing read, write and execute. Their conventional letters are r, w and x, with numeric weights 4, 2 and 1 respectively. Only A contains the complete set; the alternatives omit read or substitute a nonpermission letter.

Why each choice is right or wrong

A - Correct: r, w and x denote the complete read, write and execute permission set.

B - Incorrect: This omits r, the read bit, and therefore is not the full ordinary permission-letter set.

C - Incorrect: The letter e is not an ordinary Unix rwx permission bit and read is missing.

D - Incorrect: This lists execute and write but omits the read permission represented by r.

Primary note proof

Study-note section NSA19

The nine ordinary permission bits are owner, group and other triplets. In each triplet read=4,write=2,execute=1; sum enabled bits to get an octal digit. A leading ls -l character denotes file type, not another permission bit. For directories, read lists names, execute permits traversal/search, and write changes entries subject to other checks. File deletion usually depends on parent directory permissions, with sticky-bit/ACL rules also possible.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 43 | lines 19-35

In Windows, a user account or a user group can receive one of the following permissions to any file or folder:
Read: allows the viewing and listing of a file or folder. When viewing a folder, you can view all its files and subfolders.
Write: allows writing to a file or adding files and subfolders to a folder.
List folder contents: this permission can be assigned only to folders. It permits the viewing and listing of files and subfolders, as well as executing files that are found inthat folder.
Read & execute: permits the reading and accessing of a file‘s contents as well as its execution. When dealing withfolders, it allows the viewing and listing of files and subfolders, as well as the execution of files.

Data Communication and Computer Networking module | PDF page 63 | lines 8-16

Sorts of Files
Most files are just files, called regular files; they contain normal data, for example text files, executable files or programs, input for or output from a program and so on. The -l option to ls displays the file type, using the first character of each input line:
The following table gives an overview of the characters determining the file type:

Question sources

Computer Science model exam · 2015 · Question 55

Question 16 | Q00633

In a centralized client-server deployment, where must centralized file/directory service software be installed at minimum? Client networking support is a separate component.

A. Server

B. every system in the network

C. both server and every system in the network

D. None

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: Server

The question distinguishes server-side service software from the networking support required on every participant. A centralized service runs on a server that provides it; clients need their own networking support but do not all need the server component installed. Options requiring deployment on every system therefore exceed the minimum location asked for. This does not imply that client operating systems lack networking capabilities.

Why each choice is right or wrong

A - Correct: The server hosts the centralized server-side component.

B - Incorrect: Installing the server component on every system is not the minimum required deployment.

C - Incorrect: Requiring every client as well as the server exceeds the minimum server-side placement.

D - Incorrect: A centralized service does require a host, so none is false.

Primary note proof

Study-note section NSA02

> Clients request services; servers provide them. Peer-to-peer systems can do both. A server can also be a client of DNS or backups, so dedicated role does not mean it never makes requests. A network OS is not universally installed only on a dedicated server: clients also require networking support. Specify centralized service software versus the OS on all participants.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 32 | lines 23-30

> Windows workgroup
> A Windows workgroup is a group of standalone
> computers in a peer-to-peer network. Each computer in
> the workgroup uses its own local accounts database to

authenticate resource access. The computers in a workgroup also do not have a common authentication process. The default-networking environment for a clean windows load is workgroup

Data Communication and Computer Networking module | PDF page 34 | lines 7-14

Domain Controllers
A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing end devices to access shared domain resources. It authenticates users, stores user account information and enforces security policy for a domain. It is most commonly implemented in Microsoft

Question sources

Computer Science model exam · 2015 · Question 102

Question 17 | Q00635

Which listed item is a native Linux filesystem for ordinary user files, rather than a foreign-origin filesystem or paging area?

A. ext2

B. hpfs

C. swap

D. All

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: ext2

Ext2 is a Linux filesystem used for ordinary files. HPFS has its historical origin in OS/2, although Linux can access it when the appropriate driver is available. Swap supplies paging backing space rather than an ordinary user-file filesystem. The native-origin scope therefore identifies ext2 without incorrectly denying Linux support for foreign filesystems or treating swap as a conventional file-storage format.

Why each choice is right or wrong

A - Correct: Ext2 is the native Linux filesystem listed.

B - Incorrect: HPFS is historically associated with OS/2, so it is not the native Linux example requested.

C - Incorrect: Swap is paging backing space, not an ordinary filesystem for storing user files.

D - Incorrect: The all option includes swap as a filesystem, contrary to the note's explicit distinction.

Primary note proof

Study-note section NSA20

ext2 is a Linux filesystem; ext4 is a later filesystem; HPFS is historically associated with OS/2, while swap is backing space rather than an ordinary user-file filesystem. fsck checks and optionally repairs filesystems through filesystem-specific tools; it is not init, halt or an inittab file. Repairs require the filesystem's supported offline/safe procedure. Mount attaches a filesystem to a directory; partitioning, mounting, quotas and capacity belong to storage administration.

Study-note section NSA20

Linux can access some foreign-origin filesystems, including HPFS when its driver is available. Filesystem origin and Linux driver support are different questions. Swap is a paging area rather than an ordinary user-file filesystem. ext2 is a native Linux-filesystem example; broader Linux filesystem support can also include HPFS, so distinguish origin from driver support.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 63 | lines 8-16

Sorts of Files
Most files are just files, called regular files; they
contain normal data, for example text files,
executable files or programs, input for or output
from a program and so on. The -l option to ls
displays the file type, using the first character of
each input line:
The following table gives an overview of the
characters determining the file type:

Data Communication and Computer Networking module | PDF page 64 | lines 8-12

/lost+found: Every partition has a lost+found for files
that were saved during failures are here.
/misc: For miscellaneous purposes.
/mnt: Standard mount point for external file systems,
e.g. a CD-ROM or a digital camera.

Question sources

Computer Science model exam · 2015 · Question 104

Question 18 | Q00650

The top-level directory on a Linux system is represented as _____

A. /

B. $

C. *

D. #

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: /

PDF p.63 states that the tree begins at a forward slash and calls that directory root. Thus the top-level directory is /.

Why each choice is right or wrong

A - Correct: The forward slash is explicitly the root directory (p.63).

B - Incorrect: The cited root symbol is /, not $.

C - Incorrect: The cited root symbol is /, not *.

D - Incorrect: The cited root symbol is /, not #.

Primary note proof

Study-note section NSA20

> / is the filesystem root; /root is the administrative user’s home. /etc stores configuration, /home ordinary user homes, /var variable data/logs, /dev device nodes, /proc kernel/process information, /boot boot material and /tmp temporary files. Cleanup/mount layouts vary; do not assume every partition has lost+found or every reboot erases every temporary directory.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 63 | lines 19-22

> The tree of the file system starts at the trunk or slash, indicated by a forward slash (/). This directory, containingall underlying directories and files, is also called root directory or —the root‖ of the file system.

Question sources

Computer Science model exam · 2015 · Question 119

Question 19 | Q00900

Which listed item is a traffic-prioritization mechanism that can operate across layers, rather than an application mediator or service installation/configuration activity?

A. Proxies and agents

B. Installing a new service

C. .
E-mail configuration

D. Quality of service

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: Quality of service

Quality of service classifies, queues and prioritizes traffic to meet performance objectives such as low delay or limited loss. It can span layers while supporting applications. Proxies and agents are mediating components, and installing a service or configuring email are administrative activities. The revised question uses those explicit functional categories, so it does not require an unsupported taxonomy that labels every item an application-layer service.

Why each choice is right or wrong

A - Incorrect: Proxies and agents mediate requests as components rather than naming the traffic-prioritization mechanism.

B - Incorrect: Installing a service is an administrative activity, not a traffic-prioritization mechanism.

C - Incorrect: Email configuration is an administrative activity rather than cross-layer traffic prioritization.

D - Correct: QoS classifies and prioritizes traffic and can operate across layers.

Primary note proof

Study-note section NSA12

> A proxy acts on behalf of a client or backend service and can cache, filter or mediate application requests. A default IP gateway is a next-hop router; an application gateway may translate protocols. It need not be a modem/router combination. These terms describe functions that can coexist on one machine.

Study-note section NSA12

> QoS classifies, queues and prioritizes traffic to meet performance objectives such as low delay or limited loss. It can operate across layers and support applications, so it is not exclusively an application-layer service. Installing a new service is an administrative action; email configuration is another action and proxies/agents are components. Distinguish service-management actions from components using a stated taxonomy.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 48 | lines 41-47

Proxies and Gateways
What is proxy server?
A proxy server acts as a gateway between you and the Internet. It‘s an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

Question sources

Computer Science Exit Exam · 2018 · Question 13

Question 20 | Q00924

A data-center volume has exactly two equal disks and must retain service after either disk fails. One disk’s usable capacity is sufficient. Which listed RAID level meets these requirements?

A. RAID level 3

B. RAID level 1

C. .

RAID level 2

D. RAID level 0

Hint

Compare striping granularity, redundancy placement, usable capacity and required disk-failure tolerance.

Answer B: RAID level 1

With exactly two equal disks, RAID1 mirrors the data and leaves one disk's usable capacity while tolerating either disk failing. RAID0 provides no disk-failure tolerance. RAID2 and RAID3 rely on different striping and redundancy layouts rather than the two-disk mirrored arrangement that meets these requirements. The choice follows the stated disk count, capacity and failure goal rather than the institution's size or industry.

Why each choice is right or wrong

A - Incorrect: RAID3 uses byte striping with dedicated parity, not the required two-disk fault-tolerant layout.

B - Correct: A two-disk RAID1 mirror has one disk's capacity and survives either disk failing.

C - Incorrect: RAID2 uses bit striping with Hamming redundancy, rather than the two-disk solution meeting this requirement.

D - Incorrect: RAID0 has no disk-failure tolerance.

Primary note proof

Study-note section NSA25

> RAID0 stripes for capacity/throughput with no disk-failure tolerance. RAID1 mirrors; a two-disk mirror has one disk's usable capacity and survives one disk failure. RAID2 uses bit striping/Hamming-code redundancy, RAID3 byte striping with dedicated parity, RAID4 block striping with dedicated parity and RAID5 block striping with distributed parity. RAID6 distributes dual parity and tolerates two disk failures. RAID10 stripes mirrored pairs; survival depends on which disks fail.

Study-note section NSA25

> With N equal disks of capacity D, RAID0 usable=ND, paired RAID1/10≈ND/2, RAID5=(N−1)D and RAID6=(N−2)D. Hardware RAID may offload work to controller resources/cache but does not universally outperform software RAID. Rebuilds consume bandwidth; parity writes have overhead. A large university/bank alone does not select a level. Striping plus parity is not uniquely RAID5 unless distributed block parity is specified.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 59 | lines 14-24

> Data is distributed across the drives in one of several ways, referred to as RAID levels, depending on the required level of redundancy and performance. The different schemes, or data distribution layouts, are namedby the word —RAID‖ followed by a number, for example RAID 0 or RAID 1. Each scheme, or RAID level, provides a different balance among the key goals: reliability, availability, performance, and capacity. RAIDlevels greater than RAID 0 provide

protection against unrecoverable sector read errors,
as well as against failures of whole physical drives.

Data Communication and Computer Networking module | PDF page 59 | lines 46-52

RAID 1 consists of data mirroring, without parity or striping . Data is written identically to two or more drives,thereby producing a —mirrored set‖ of drives. Thus, any read request can be serviced by any drive in the set. If a request is broadcast to every drive in the set, it can be serviced by the drive that accesses the data first (depending on its seek time and rotational latency),

Data Communication and Computer Networking module | PDF page 60 | lines 12-26

RAID 2 consists of bit-level striping with dedicated Hamming-code parity. All disk spindle rotation is synchronized and data is striped such that each sequential bit is on a different drive. Hamming-code parity is calculated across corresponding bits and stored on at least one parity drive. This level is of historical significance only; as of 2014 it is not used by any commercially available system.
RAID 3 consists of byte-level striping with dedicated parity. All disk spindle rotation is synchronized and data is striped such that each sequential byte is on a different drive. Parity is calculated across corresponding bytes and stored on a dedicated parity drive. Although implementations exist, RAID 3 is not commonly used in practice.

Data Communication and Computer Networking module | PDF page 59 | lines 33-45

RAID 0 consists of striping, but no mirroring or parity. Compared to a spanned volume, the capacity of a RAID 0 volume is the same; it is the sum of the capacities of the drives in the set. But because striping distributes the contents of each file among all drives in the set, the failure of any drive causes the entire RAID 0 volume and all files to be lost. In comparison, a spanned volume preserves thefiles on the unfailing drives. The benefits of RAID 0 is that the throughput of read and write operations to any file is multiplied by the number of drives because, unlike spanned volumes, reads and writes are done concurrently.

Question sources

Computer Science Exit Exam · 2018 · Question 37

Question 21 | Q00937

Which listed RAID layout uses block-level striping with distributed parity and tolerates one disk failure?

A. RAID 2

B. RAID 1

C. RAID 5

D. RAID 0

Hint

Compare striping granularity, redundancy placement, usable capacity and required disk-failure tolerance.

Answer C: RAID 5

RAID5 distributes parity across disks while striping data at block level. That distinguishes it from RAID2's bit striping and Hamming-code redundancy. RAID1 mirrors copies instead of organizing the array as distributed-parity striping, while RAID0 adds no redundancy. The explicit granularity and parity placement identify the intended layout rather than treating every form of redundant striping as equivalent.

Why each choice is right or wrong

A - Incorrect: RAID2 uses bit striping with Hamming redundancy, not distributed block parity.

B - Incorrect: RAID1 mirrors data rather than using the specified striping-with-parity organization.

C - Correct: RAID5 uses block striping with distributed parity and one-disk failure tolerance.

D - Incorrect: RAID0 stripes without redundant parity and provides no disk-failure tolerance.

Primary note proof

Study-note section NSA25

> RAID0 stripes for capacity/throughput with no disk-failure tolerance. RAID1 mirrors; a two-disk mirror has one disk's usable capacity and survives one disk failure. RAID2 uses bit striping/Hamming-code redundancy, RAID3 byte striping with dedicated parity, RAID4 block striping with dedicated parity and RAID5 block striping with distributed parity. RAID6 distributes dual parity and tolerates two disk failures. RAID10 stripes mirrored pairs; survival depends on which disks fail.

Study-note section NSA25

> With N equal disks of capacity D, RAID0 usable=ND, paired RAID1/10≈ND/2, RAID5=(N−1)D and RAID6=(N−2)D. Hardware RAID may offload work to controller resources/cache but does not universally outperform software RAID. Rebuilds consume bandwidth; parity writes have overhead. A large university/bank alone does not select a level. Striping plus parity is not uniquely RAID5 unless distributed block parity is specified.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 60 | lines 12-26

RAID 2 consists of bit-level striping with dedicated Hamming-code parity. All disk spindle rotation is synchronized and data is striped such that each sequential bit is on a different drive. Hamming-code parity is calculated across corresponding bits and stored on at least one parity drive. This level is of historical significance only; as of 2014 it is not used by any commercially available system.
RAID 3 consists of byte-level striping with dedicated parity. All disk spindle rotation is synchronized and data is striped such that each sequential byte is on a different drive. Parity is calculated across corresponding bytes and stored on a dedicated parity drive. Although implementations exist, RAID 3 is not commonly used in practice.

Data Communication and Computer Networking module | PDF page 60 | lines 35-46

RAID 5 consists of block-level striping with distributed parity. Unlike RAID 4, parity information is distributed among the drives, requiring all drives but one to be present to operate. Upon failure of a single drive, subsequent reads can be calculated from the distributed parity such that no data is lost. RAID 5 requires at least three disks. Like all single-parity concepts, large RAID 5 implementations are susceptible to system failures because of trends regarding array rebuild time and the chance of drive failure during rebuild. Rebuilding an array requires reading all data from all disks, opening a chance for a second drive failure and the loss of the entire array.

Data Communication and Computer Networking module | PDF page 59 | lines 46-52

RAID 1 consists of data mirroring, without parity or striping . Data is written identically to two or more drives,thereby producing a —mirrored set‖ of drives. Thus, any read request can be serviced by any drive in the set. If a request is broadcast to every drive in the set, it can be serviced by the drive that accesses the data first (depending on its seek time and rotational latency),

Data Communication and Computer Networking module | PDF page 59 | lines 33-45

RAID 0 consists of striping, but no mirroring or parity. Compared to a spanned volume, the capacity of a RAID 0 volume is the same; it is the sum of the

capacities of the drives in the set. But because striping distributes the contents of each file among all drives in the set, the failure of any drive causes the entire RAID 0 volume and all files to be lost. In comparison, a spanned volume preserves thefiles on the unfailing drives. The benefits of RAID 0 is that the throughput of read and write operations to any file is multiplied by the number of drives because, unlike spanned volumes, reads and writes are done concurrently.

Question sources

Computer Science Exit Exam · 2018 · Question 50

Question 22 | Q00954

Which tool directly sends ICMP echo probes to test IP reachability?

A. Ipconfig

B. Ping

C. Encryption

D. Firewall

Hint

Match the requested observation to the tool’s actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer B: Ping

Ping sends ICMP echo requests and observes replies to test IP reachability. A reply confirms that the path and target support that exchange. A missing reply may reflect filtering or loss, so it does not alone prove disconnection. Interface configuration inspection, confidentiality protection and traffic-policy enforcement serve different purposes from sending this diagnostic probe.

Why each choice is right or wrong

A - Incorrect: Ipconfig displays local adapter configuration; it does not send the requested echo probes.

B - Correct: Ping sends ICMP echo requests and checks for replies.

C - Incorrect: Encryption protects confidentiality rather than generating an echo reachability test.

D - Incorrect: A firewall permits or blocks traffic according to policy rather than being the echo-probe utility.

Primary note proof

Study-note section NSA07

Windows ipconfig shows addresses, mask and gateway; ipconfig /all adds complete adapter configuration including physical/MAC address, DHCP and DNS information. /renew requests renewal, /release releases a dynamic address and /flushdns clears the client DNS cache. Linux ip addr and ip route show interface addresses and routes; exact persistent configuration varies by distribution.

Study-note section NSA-S04

Ping uses ICMP echo messages to test IP reachability. A reply shows that the addressed host and path support that exchange; no reply alone does not prove the host is disconnected, because filtering or loss can suppress responses. Traceroute instead discovers responding intermediate hops through packet-lifetime expiry; it is a path-discovery diagnostic, not the same question as an end-to-end echo test.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

Ping (Packet Internet Groper) uses ICMP echo
messages to check the physical and logical
connectivity of machineson a network.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Computer Science Exit Exam · 2018 · Question 67

Question 23 | Q01003

Suppose you are network administrator, you want to determine the path between two connections, often a connection to another device will have to go through multiple routers. Which command would you use?

A. ping

B. nslookup

C. traceroute

D. All of the above

Hint

Match the requested observation to the tool's actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer C: traceroute

Traceroute discovers responding intermediate hops by using packet-lifetime expiry. That provides evidence about the multi-router path toward a destination. Ping instead tests an end-to-end echo exchange, and nslookup asks DNS questions. Neither produces the requested hop sequence, so combining all the tools is not the correct description of the specific path-discovery command. Some routers may suppress responses, leaving gaps in the trace.

Why each choice is right or wrong

A - Incorrect: Ping probes end-to-end reachability, not the intermediate-hop sequence.

B - Incorrect: Nslookup inspects DNS name-resolution information, not router hops.

C - Correct: Traceroute discovers responding intermediate hops toward the destination.

D - Incorrect: Not all listed commands perform hop discovery.

Primary note proof

Study-note section NSA07

> netstat displays connections/endpoints/protocols and TCP states; netstat -ano displays numeric addresses/ports and PIDs. Use the exact command name netstat rather than netstart. ping probes IP reachability; traceroute/tracert reveals responding hops using TTL/hop-limit expiry. ICMP filtering can prevent replies without proving the service is down. nslookup inspects DNS.

Study-note section NSA06

> Resolvers cache answers for their TTL. Query nslookup name or specify the DNS server explicitly; compare the configured resolver with the authoritative answer when appropriate. A successful ping by address but failed name lookup suggests naming/configuration trouble. Ping by name may display a resolved address, but nslookup is the direct DNS diagnostic. "Resolving" is a general term that includes forward resolution.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

> Ping (Packet Internet Groper) uses ICMP echo messages to check the physical and logical connectivity of machineson a network.

Data Communication and Computer Networking module | PDF page 27 | lines 29-31

> Traceroute Using ICMP timeouts, Traceroute is used to discover the path a packet takes as it traverses an Internetwork.

Question sources

National Exit Exam practice questions · Question 17

Question 24 | Q01191

In a deployment with one unprotected DHCP server, which statements are not actual disadvantages of DHCP? Select all that apply.

A. Fault on the DHCP server can affect the whole network

B. It is not a secured way of assigning IP addresses

C. Static IP address assignment can't be used.

D. It minimizes the load of network admin

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C, D: Static IP address assignment can't be used.; It minimizes the load of network admin

A single DHCP service can become an availability dependency for clients needing configuration, and rogue replies are a risk in an unprotected deployment. However, DHCP does not prohibit static assignments: administrators can exclude manually used addresses to avoid conflicts. Reducing repetitive administration is also an advantage. Therefore the false limitation about static addressing and the genuine administrative benefit are the requested exceptions.

Why each choice is right or wrong

A - Incorrect: Depending on deployment, DHCP-server failure can impair clients needing leases, so this can be a disadvantage.

B - Incorrect: Rogue replies and insecure deployment are genuine risks, although DHCP security depends on protections.

C - Correct: This alleged disadvantage is false: static assignments and DHCP can coexist safely with exclusions.

D - Correct: Reducing repetitive administrator work is an advantage rather than a disadvantage.

Primary note proof

Study-note section NSA05

> Use a scope matching the subnet, exclude manually assigned server/router addresses, set correct options and provide a relay when client broadcasts must cross a router. Static assignments and DHCP can coexist; avoid address conflicts. DHCP lowers repetitive administration but availability/security depend on deployment and protection from rogue replies. It does not guarantee connectivity whenever a device changes location.

Study-note section NSA04

> DHCP supplies addresses and configuration options. Typical initial IPv4 allocation is Discover→Offer→Request→ACK. The server manages its scope/pool, allocated leases, exclusions and reservations; options may include mask, gateway and DNS servers. A dynamic lease lasts for a specified interval, not forever.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

> The Process/Application Layer Protocols
> • Telnet
> • File Transfer Protocol (FTP)
> • Network File System (NFS).
> • Simple Mail Transfer Protocol (SMTP
> • POP3 is used to receive mail.
> • Simple Network Management Protocol (SNMP)
> • Domain Name Service (DNS)
> • Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science model exam 2 · Question 12

Question 25 | Q01210

Which listed address is the conventional IPv4 loopback address normally chosen to test the local IP stack? Select one.

A. 127.0.0.1

B. 1.0.0.127

C. 127.0.0.0

D. 127.0.0.255

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: 127.0.0.1

The whole 127/8 range is reserved for loopback, but 127.0.0.1 is the conventional address normally used for this test. The other 127-prefixed choices belong to the broader reserved block without being the conventional address requested. The reversed-looking 1.0.0.127 is outside loopback space. A successful loopback probe tests local protocol processing and does not establish that cables or remote devices work.

Why each choice is right or wrong

A - Correct: 127.0.0.1 is the conventional IPv4 loopback address explicitly named in the note.

B - Incorrect: 1.0.0.127 is outside the reserved 127/8 loopback block.

C - Incorrect: This belongs to loopback-reserved 127/8, but is not the conventional address requested.

D - Incorrect: This also lies in 127/8, but is not the conventional loopback address requested.

Primary note proof

Study-note section NSA03

> 127.0.0.1 conventionally names the local IPv4 loopback interface; 127/8 is reserved for loopback. Loopback tests local protocol processing, not cable, switch or remote reachability. Programs can use it for local services. Several loopback descriptions or several 127/8 addresses may be valid; compare each with the stated role.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

> /etc/hosts
> The /etc/hosts file always contains the localhost IP
> address, 127.0.0.1, which is
> usedfor interprocess communication.
> Never remove this line! Sometimes contains
> addresses of additional hosts, whichcan be contacted
> without using an external naming service such as
> DNS (the Domain Name Server).

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

> Ping (Packet Internet Groper) uses ICMP echo
> messages to check the physical and logical
> connectivity of machineson a network.

Question sources

Computer Science model exam 2 · Question 31

Question 26 | Q01216

Most of the time, it is recommended to apply a Hardware RAID into your system in terms of system performance. Why? Because Hardware RAID:

A. A physical storage device that is built into a system

B. Can appear as a single hard disk in the system

C. There is no difference between regular hardware and the RAID devices

D. Can use its own resources

Hint

Compare striping granularity, redundancy placement, usable capacity and required disk-failure tolerance.

Answer D: Hardware RAID can use its own controller resources

NSA25 supports controller resources/cache as a reason hardware RAID may offload work from the host. D directly states that relevant mechanism. Appearing as one disk is a presentation property rather than the performance explanation, and neither simply being physical nor denying differences explains offload. The note also rejects any universal claim that hardware RAID always performs better.

Why each choice is right or wrong

A - Incorrect: Being a physical device alone does not explain any RAID performance advantage or computation offload.

B - Incorrect: A single logical-disk presentation does not establish that host processing work is offloaded.

C - Incorrect: Denying differences provides no performance mechanism and ignores dedicated controller resources.

D - Correct: Dedicated controller resources/cache can perform RAID work rather than relying entirely on the host CPU.

Primary note proof

Study-note section NSA25

> With N equal disks of capacity D, RAID0 usable=ND, paired RAID1/10≈ND/2, RAID5=(N−1)D and RAID6=(N−2)D. Hardware RAID may offload work to controller resources/cache but does not universally outperform software RAID. Rebuilds consume bandwidth; parity writes have overhead. A large university/bank alone does not select a level. Striping plus parity is not uniquely RAID5 unless distributed block parity is specified.

Study-note section NSA25

RAID0 stripes for capacity/throughput with no disk-failure tolerance. RAID1 mirrors; a two-disk mirror has one disk's usable capacity and survives one disk failure. RAID2 uses bit striping/Hamming-code redundancy, RAID3 byte striping with dedicated parity, RAID4 block striping with dedicated parity and RAID5 block striping with distributed parity. RAID6 distributes dual parity and tolerates two disk failures. RAID10 stripes mirrored pairs; survival depends on which disks fail.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 59 | lines 14-24

Data is distributed across the drives in one of several ways, referred to as RAID levels, depending on the required level of redundancy and performance. The different schemes, or data distribution layouts, are namedby the word —RAID‖ followed by a number, for example RAID 0 or RAID 1. Each scheme, or RAID level, provides a different balance among the key goals: reliability, availability, performance, and capacity. RAIDlevels greater than RAID 0 provide protection against unrecoverable sector read errors, as well as against failures of whole physical drives.

Question sources

Computer Science model exam 2 · Question 37

Question 27 | Q01271

All of the following are the roles of a system admin related to the file system and disk space management EXCEPT?

A. Assigning user ID and User name for system users

B. Determining desk usage and quota

C. Creating a Mounting point

D. Partition disk space

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: Assigning user ID and User name for system users

PDF p.42 assigns account permissions and capabilities to user administration, p.53 monitors free disk space, and p.64 identifies a mount point. Assigning a username/ID is the account task, while the other options concern storage organization or capacity.

Why each choice is right or wrong

A - Correct: This belongs to account administration (p.42), making it the requested exception.

B - Incorrect: Disk usage and quota concern the storage capacity being monitored on p.53.

C - Incorrect: A mounting point belongs to the filesystem organization illustrated by /mnt (p.64).

D - Incorrect: Partitioning concerns organizing disk space, within the storage subject rather than naming users.

Primary note proof

Study-note section NSA20

> ext2 is a Linux filesystem; ext4 is a later filesystem; HPFS is historically associated with OS/2, while swap is backing space rather than an ordinary user-file filesystem. fsck checks and optionally repairs filesystems through filesystem-specific tools; it is not init, halt or an inittab file. Repairs require the filesystem's supported offline/safe procedure. Mount attaches a filesystem to a directory; partitioning, mounting, quotas and capacity belong to storage administration.

Study-note section NSA17

> Create named accounts, assign only needed groups/rights, disable departed users and audit privileged activity. Authentication verifies the account; authorization permits operations. A user right such as remote logon differs from a permission on one file. Group-based administration is easier to review than many hidden individual grants.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 42 | lines 36-49

> All user accounts have specific capabilities, privileges,
> and rights. When you create a user account, you can grant
> the user specific capabilities by making the user a member
> of one or more groups. This gives the user the capabilities
> of these groups. You then assign additional capabilities by
> making a user a member of the appropriate groups or
> withdraw capabilities by removing a user from a group.
> An important part of an administrator‘s job is being able
> to determine and set permissions, privileges, and logon
> rights as necessary. Although you can‘t change a group‘s
> built-in capabilities, you can change a group‘s default
> privileges and logon rights. For example, you could
> revoke network access to a computer by removing agroup‘s
> right to access the computer from the network.

Data Communication and Computer Networking module | PDF page 53 | lines 2-20

> Monitoring storage normally takes place at two
> different levels:
> • Monitoring for sufficient disk space
> • Monitoring for storage-related

performanceproblems
The reason for this is that it is possible to have dire problems in one area and no problems whatsoever in the other. For example, it is possible to cause a disk drive to run out of disk space without once causing any kind of performance-related problems. Likewise, it is possible tohave a disk drive that has 99% free space, yet is being pushed past its limits in terms of performance.
In any case, the following statistics are useful for monitoring storage:
• Free Space
• File System-Related Statistics
• Transfers per Second
• Reads/Writes per Second

Data Communication and Computer Networking module | PDF page 64 | lines 8-12

/lost+found: Every partition has a lost+found for files that were saved during failures are here.
/misc: For miscellaneous purposes.
/mnt: Standard mount point for external file systems, e.g. a CD-ROM or a digital camera.

Question sources

Computer Science model exam 2 · Question 92

Question 28 | Q01307

In the ordinary Unix owner/group/other rwx permission-bit model, which operation has no separate file permission bit?

A. Read

B. Write

C. Execute

D. Delete

Hint

Identify the platform and permission model; for an rwx string, separate owner/group/other triplets and use the stated bit weights.

Answer D: Delete

Each ordinary Unix permission triplet contains read, write and execute bits. There is no fourth delete bit in that model. Deletion generally depends on permissions on the parent directory, with other mechanisms such as sticky bits or ACLs able to add restrictions. Windows can have an explicit delete permission, so naming the Unix rwx model is essential to make the exception accurate.

Why each choice is right or wrong

A - Incorrect: Read is a recognized permission in both Windows and ordinary Unix permission models.

B - Incorrect: Write is a recognized access permission, not the requested generic exception.

C - Incorrect: Execute/read-execute permissions exist in the models described in the note.

D - Correct: Unix rwx has no separate delete bit; deletion usually depends on the parent directory.

Primary note proof

Study-note section NSA19

> The nine ordinary permission bits are owner, group and other triplets. In each triplet read=4,write=2,execute=1; sum enabled bits to get an octal digit. A leading ls -l character denotes file type, not another permission bit. For directories, read lists names, execute permits traversal/search, and write changes entries subject to other checks. File deletion usually depends on parent directory permissions, with sticky-bit/ACL rules also possible.

Study-note section NSA18

> Deleting can be an explicit permission in Windows; specify the operating system before comparing permission names. Modify and full control are not identical: full control includes changing permission/ownership capabilities. Separate data access from logon rights. A user allowed to read a file is not necessarily allowed to write it or administer its parent folder.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 43 | lines 19-35

> In Windows, a user account or a user group can receive one of the following permissions to any file or folder:
> Read: allows the viewing and listing of a file or folder. When viewing a folder, you can view all its files and subfolders.
> Write: allows writing to a file or adding files and subfolders to a folder.
> List folder contents: this permission can be assigned only to folders. It permits the viewing and listing of files and subfolders, as well as executing files that are found inthat folder.

> Read & execute: permits the reading and accessing of a file‘s contents as well as its execution. When dealing withfolders, it allows the viewing and listing of files and subfolders, as well as the execution of files.

Data Communication and Computer Networking module | PDF page 43 | lines 36-44

> Modify: when dealing with files, it allows their reading, writing and deletion. When dealing with folders, it allowsthe reading and writing of files and subfolders, plus the deletion of the folder.
> Full control: it allows reading, writing, changing and deleting of any file and subfolder. Generally, files inheritthe permissions of the folder where they are placed, but users can also define specific permissions that are assigned only to a specific file.

Question sources

Operating Systems practice questions · Question 25

Question 29 | Q01495

After DHCP fails at startup, a client self-configures an IPv4 link-local interface address for same-link communication. Which address could it assign?

A. 255.255.255.255

B. 127.0.0.1

C. 169.254.2.33

D. 0.0.0.0

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C: 169.254.2.33 as an IPv4 link-local fallback

An IPv4 link-local fallback uses the 169.254 range; 169.254.2.33 is a usable example. This can permit communication with peers on the same link, but does not provide ordinary routed Internet connectivity. The other values serve special broadcast, loopback or unspecified-address roles. In particular, 0.0.0.0 may appear before configuration but is not the assigned link-local address requested here.

Why each choice is right or wrong

A - Incorrect: This is the limited-broadcast destination, not an assigned host address.

B - Incorrect: Loopback addresses the local host, not its link-local interface.

C - Correct: 169.254.2.33 is an IPv4 link-local fallback address.

D - Incorrect: The unspecified address is not a configured link-local host address.

Primary note proof

Study-note section NSA05

> For a returning client, inspect current lease/address, reachable server/relay, free pool capacity and logs. New devices can exhaust a pool, but absent observations this is only a hypothesis. Some clients self-configure IPv4 link-local addresses such as 169.254.2.33 after DHCP failure; these support same-link communication, not ordinary routed Internet access. 0.0.0.0 is unspecified and 255.255.255.255 is limited broadcast.

Study-note section NSA03

> 127.0.0.1 conventionally names the local IPv4 loopback interface; 127/8 is reserved for loopback. Loopback tests local protocol processing, not cable, switch or remote reachability. Programs can use it for local services. Several loopback descriptions or several 127/8 addresses may be valid; compare each with the stated role.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

> The Process/Application Layer Protocols
> • Telnet
> • File Transfer Protocol (FTP)
> • Network File System (NFS).
> • Simple Mail Transfer Protocol (SMTP
> • POP3 is used to receive mail.
> • Simple Network Management Protocol (SNMP)
> • Domain Name Service (DNS)
> • Dynamic Host Configuration Protocol (DHCP)

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

> /etc/hosts
> The /etc/hosts file always contains the localhost IP
> address, 127.0.0.1, which is
> usedfor interprocess communication.
> Never remove this line! Sometimes contains
> addresses of additional hosts, whichcan be contacted
> without using an external naming service such as
> DNS (the Domain Name Server).

Question sources

Mock exam 1 · Question 11

Question 30 | Q01592

Which action is not sound OS hardening when required services must remain available?

A. Remove unnecessary applications and services

B. Install patches

C. Configure users and permissions

D. Block every port, including ports required by legitimate services.

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: Block every port, including ports required by legitimate services.

Hardening reduces unnecessary exposure while preserving the services the system must provide. Removing unused software, deploying supported patches and restricting accounts or permissions all support that goal. Filtering unused ports can help too, but indiscriminately blocking ports required by legitimate services destroys availability. The port option states that harmful action explicitly rather than treating every form of port filtering as inappropriate.

Why each choice is right or wrong

A - Incorrect: Removing unnecessary applications/services reduces attack surface and is an explicit hardening action.

B - Incorrect: Supported patches repair known weaknesses and are part of hardening.

C - Incorrect: Restricting users and permissions is an explicit hardening measure.

D - Correct: Blocking ports required by legitimate services defeats availability rather than sound hardening.

Primary note proof

Study-note section NSA27

> Hardening reduces exposure through unnecessary-service removal, supported patches, restricted accounts/permissions and appropriate port filtering. Blocking an unused known port can be hardening; blocking every useful port merely destroys availability. Weak passwords and unpatched exploitable software are vulnerabilities; attacks exploit weaknesses, and risk combines likelihood with impact.

Study-note section NSA01

> Use documentation, standardization, least privilege, automation and measured change. Record the current state, intended change, rollback and validation. Schedule maintenance according to service impact and urgency, not merely because a calendar date arrived. Fault management restores failures; performance management measures service behavior; configuration management tracks settings; security management controls access; accounting tracks usage.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 19-33

Although the specifics of being a system administrator may change from platform to platform, there are underlying themes that do not. These themes make up the philosophy of system administration. The themes are:
• Automate everything
• Document everything
• Communicate as much as possible
• Know your resources
• Know your users
• Know your business
• Security cannot be an afterthought
• Plan ahead
• Expect the unexpected
• Backup and disaster recovery planning
• Patching

Data Communication and Computer Networking module | PDF page 58 | lines 33-40

Disadvantages of Remote Administration
Remote administration has many disadvantages too apart from its advantages. The first and foremost disadvantage is the security. Generally, certain ports to be open at Server level to do remote administration. Due to open ports, the hackers/attackers takes advantage to compromise the system. It is advised that remote administration to be used only in emergency or essential

Data Communication and Computer Networking module | PDF page 42 | lines 36-49

All user accounts have specific capabilities, privileges, and rights. When you create a user account, you can grant the user specific capabilities by making the user a member of one or more groups. This gives the user the capabilities of these groups. You then assign additional capabilities by making a user a member of the appropriate groups or withdraw capabilities by removing a user from a group. An important part of an administrator‘s job is being able to determine and set permissions, privileges, and logon rights as necessary. Although you can‘t change a group‘s built-in capabilities, you can change a group‘s default privileges and logon rights. For example, you could revoke network access to a computer by removing agroup‘s right to access the computer from the network.

Data Communication and Computer Networking module | PDF page 59 | lines 2-4

situations only to do administration remotely. In normal situations, it is ideal to block the ports to avoid remote administration.

Question sources

Mock exam 3 · Question 24

Question 31 | SM0028

You know the upstairs computer's IP address and want a basic end-to-end ICMP echo reachability test, rather than a router-hop trace. Which command should you use?

A. nslookup

B. ping

C. DHCP discover

D. traceroute

Hint

Match the requested observation to the tool's actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer B: ping

Ping directly tests whether the addressed computer and path support an ICMP echo exchange. A reply is useful reachability evidence; absence of a reply may result from filtering or loss. Nslookup tests DNS, DHCP discovery seeks configuration service, and traceroute identifies responding intermediate hops. These answer different operational questions from the basic echo test requested.

Why each choice is right or wrong

A - Incorrect: Nslookup queries DNS, which is unnecessary for the specified known-IP echo test.

B - Correct: Ping performs the requested end-to-end ICMP echo test.

C - Incorrect: DHCP discovery locates configuration service rather than testing this remote host.

D - Incorrect: Traceroute probes the hop path rather than performing the requested basic echo test.

Primary note proof

Study-note section NSA-S04

Ping uses ICMP echo messages to test IP reachability. A reply shows that the addressed host and path support that exchange; no reply alone does not prove the host is disconnected, because filtering or loss can suppress responses. Traceroute instead discovers responding intermediate hops through packet-lifetime expiry; it is a path-discovery diagnostic, not the same question as an end-to-end echo test.

Study-note section NSA07

netstat displays connections/endpoints/protocols and TCP states; netstat -ano displays numeric addresses/ports and PIDs. Use the exact command name netstat rather than netstart. ping probes IP reachability; traceroute/tracert reveals responding hops using TTL/hop-limit expiry. ICMP filtering can prevent replies without proving the service is down. nslookup inspects DNS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

Ping (Packet Internet Groper) uses ICMP echo
messages to check the physical and logical
connectivity of machineson a network.

Data Communication and Computer Networking module | PDF page 27 | lines 29-31

Traceroute Using ICMP timeouts, Traceroute is
used to discover the path a packet takes as it
traverses an Internetwork.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

MOE Computer Science Exit Exam · Question 8-3

National Computer Science Exit Exam · Question 28

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 186

Question 32 | SM0084

Which one of the following is correct about human role in system administration?

A. Ethics is not a requirement to manage computers

B. It requires patience, understanding and knowledge

C. It doesn't need organizational skills

D. System administrator is not expected to have skills and confidence

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer B: Patience, understanding and knowledge

NSA01 includes human abilities and responsible conduct in administration: patience, communication, ethics, technical understanding and organization. B agrees with that account. The other statements deny ethics, organization or expected competence, directly contradicting the note’s description of the role rather than identifying a valid human requirement.

Why each choice is right or wrong

A - Incorrect: NSA01 explicitly includes ethics among the qualities required for responsible administration.

B - Correct: Patience and technical understanding/knowledge agree directly with the human qualities listed in NSA01.

C - Incorrect: Organization is explicitly important, so denying organizational skills contradicts the note.

D - Incorrect: The role requires technical understanding and competent administration rather than an absence of skills.

Primary note proof

Study-note section NSA01

> System administrators maintain hosts, accounts, storage, software and availability; network administrators maintain connectivity, addressing, routes, network devices and performance. Security administrators coordinate controls and policy. These duties overlap, so account management, testing patches and training users are not exclusive to one job title. Patience, communication, ethics, technical understanding and organization matter alongside command knowledge.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 29 | lines 16-20

> It‘s about hardware, software, user support,
> diagnosis, repair and prevention. System

administrators need to know a bit of everything: the skills are technical, administrative and socio-psychological.

Question sources

MOE Computer Science Exit Exam · Question 24-1

National Computer Science Exit Exam · Question 83

National Computer Science Exit Exam

MOE Computer Science Exit Exam

Computer Science Exit Exam practice collection · Question 187

Question 33 | SM0270

A planned hardware upgrade requires the system to be powered off, and an acceptable maintenance window and rollback are arranged. Which listed circumstance justifies the planned shutdown?

A. Using regular schedules

B. For maintenance and upgrade

C. To check for security alerts

D. When there is a failure

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer B: For maintenance and upgrade

A shutdown is justified when the required procedure needs it and its service impact has been planned. Here the hardware upgrade explicitly requires power-off and an acceptable window has been arranged. A calendar schedule alone is insufficient, checking alerts ordinarily requires no shutdown, and no failure is described. The decision therefore follows the actual maintenance requirement rather than a universal rule that systems should stop periodically.

Why each choice is right or wrong

A - Incorrect: A regular calendar schedule alone does not justify shutting down a service without considering impact and necessity.

B - Correct: The stated maintenance/upgrade procedure requires a planned power-off.

C - Incorrect: Checking alerts does not ordinarily require stopping the system and supplies no shutdown justification here.

D - Incorrect: No failure is described; the shutdown is required for the planned upgrade.

Primary note proof

Study-note section NSA01

Use documentation, standardization, least privilege, automation and measured change. Record the current state, intended change, rollback and validation. Schedule maintenance according to service impact and urgency, not merely because a calendar date arrived. Fault management restores failures; performance management measures service behavior; configuration management tracks settings; security management controls access; accounting tracks usage.

Study-note section NSA08

Define the symptom, scope, time and recent changes; gather the configuration, baseline and logs. Form a testable hypothesis, test the least disruptive explanation, isolate the failing component, apply a targeted fix, verify the user service and document the result. Change one relevant factor at a time when possible. A reboot can hide evidence and is not a diagnosis by itself.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Question sources

Computer Science Exit Exam · Sene 2016 · Question 23-1

Computer Science Exit Exam practice collection · Question 192

Question 34 | SM0287

Which one of the following is NOT a reason for the need of backups?

A. Security incidents

B. Upgrades and migrations

C. Hardware failures

D. Authorization

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: Authorization

Backups preserve recoverable earlier data after hardware loss, compromise, corruption or failed upgrades and migrations. These events can destroy or damage the live copy, so independent protected copies and tested restores address their consequences. Authorization instead decides who may access current resources. It is essential security policy, but is a separate function from preserving copies for recovery.

Why each choice is right or wrong

A - Incorrect: Compromise can damage or delete data, creating a restoration need.

B - Incorrect: Failed upgrades or migrations can require restoring the previous valid data.

C - Incorrect: Hardware failure can destroy the live copy and require recovery.

D - Correct: Authorization governs current access rights; it is not a data-loss recovery reason.

Primary note proof

Study-note section NSA24

> Backups recover previous data after deletion, compromise, corruption, failed upgrades/migrations or hardware loss. Authorization controls current access, a different function. A mirror/replica also copies deletions or corruption and does not replace versioned independent backups. Keep protected copies in separate failure domains, define retention and test restores.

Study-note section NSA17

> Create named accounts, assign only needed groups/rights, disable departed users and audit privileged activity. Authentication verifies the account; authorization permits operations. A user right such as remote logon differs from a permission on one file. Group-based administration is easier to review than many hidden individual grants.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 6-8

> • Backing up the network software and data
> regularly to protect against the failure of network
> or any of its components

Data Communication and Computer Networking module | PDF page 46 | lines 19-22

> that the user profile data is not being automatically backed
> up by the server. Since most users rarely back up their
> computers, if a hard drive fails, any data that is stored
> within local profiles on that machine would be lost.

Data Communication and Computer Networking module | PDF page 42 | lines 36-49

> All user accounts have specific capabilities, privileges, and rights. When you create a user account, you can grant the user specific capabilities by making the user a member of one or more groups. This gives the user the capabilities of these groups. You then assign additional capabilities by making a user a member of the appropriate groups or withdraw capabilities by removing a user from a group. An important part of an administrator‘s job is being able to determine and set permissions, privileges, and logon rights as necessary. Although you can‘t change a group‘s built-in capabilities, you can change a group‘s default privileges and logon rights. For example, you could revoke network access to a computer by removing agroup‘s right to access the computer from the network.

Question sources

Computer Science Exit Exam · Sene 2016 · Question 28-3

Computer Science Exit Exam practice collection · Question 190

Question 35 | SS099

The ordinary file permission string -rwxr--r-- is represented by which octal mode?

A. 744

B. 700

C. 755

D. 766

Hint

Identify the platform and permission model; for an rwx string, separate owner/group/other triplets and use the stated bit weights.

Answer A: 744.

The leading hyphen identifies an ordinary file and is not a permission bit. Split the remaining characters as rwx | r-- | r--. The owner has 4+2+1=7, the group has read only (4), and others have read only (4). Writing those three octal digits in order gives 744, so A is correct.

Why each choice is right or wrong

A - Correct: 744 exactly represents owner rwx, group r-- and others r--.

B - Incorrect: 700 would deny both group and others all permissions, unlike the two read permissions shown.

C - Incorrect: 755 would give group and others execute permission as well as read permission; those execute bits are absent.

D - Incorrect: 766 would give group and others write permission; neither triplet contains w.

Primary note proof

Study-note section NSA19

The nine ordinary permission bits are owner, group and other triplets. In each triplet read=4,write=2,execute=1; sum enabled bits to get an octal digit. A leading ls -l character denotes file type, not another permission bit. For directories, read lists names, execute permits traversal/search, and write changes entries subject to other checks. File deletion usually depends on parent directory permissions, with sticky-bit/ACL rules also possible.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 63 | lines 8-16

Sorts of Files
Most files are just files, called regular files; they contain normal data, for example text files, executable files or programs, input for or output from a program and so on. The -l option to ls displays the file type, using the first character of each input line:
The following table gives an overview of the characters determining the file type:

Data Communication and Computer Networking module | PDF page 43 | lines 19-35

In Windows, a user account or a user group can receive one of the following permissions to any file or folder:
Read: allows the viewing and listing of a file or folder. When viewing a folder, you can view all its files and subfolders.
Write: allows writing to a file or adding files and subfolders to a folder.
List folder contents: this permission can be assigned only to folders. It permits the viewing and listing of files and subfolders, as well as executing files that are found inthat folder.
Read & execute: permits the reading and accessing of a file‘s contents as well as its execution. When dealing withfolders, it allows the viewing and listing of files and subfolders, as well as the execution of files.

Question sources

Computer Science model exam collection · Question 6

Question 36 | AM0564

What is the primary role of a system administrator?

A. Designing computer networks

B. Developing software applications

C. Managing and maintaining computer systems

D. Providing technical support to end-users

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C: Managing and maintaining computer systems

PDF p.28 describes getting computer systems running and keeping them running; p.29 calls system administration the management of computers. C captures that broad primary role rather than one subtask.

Why each choice is right or wrong

A - Incorrect: Network design is one challenge (p.30), narrower than maintaining computer systems.

B - Incorrect: The definition is operational management, not developing applications (p.28).

C - Correct: Managing and maintaining systems directly matches pp.28-29.

D - Incorrect: User support is included (p.29), but is only part of the broader role.

Primary note proof

Study-note section NSA01

> System administrators maintain hosts, accounts, storage, software and availability; network administrators maintain connectivity, addressing, routes, network devices and performance. Security administrators coordinate controls and policy. These duties overlap, so account management, testing patches and training users are not exclusive to one job title. Patience, communication, ethics, technical understanding and organization matter alongside command knowledge.

Study-note section NSA01

> Use documentation, standardization, least privilege, automation and measured change. Record the current state, intended change, rollback and validation. Schedule maintenance according to service impact and urgency, not merely because a calendar date arrived. Fault management restores failures; performance management measures service behavior; configuration management tracks settings; security management controls access; accounting tracks usage.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 46-53

> Philosophy of System Administration
> Network and system administration is a branch of engineering that concerns the operational management of human-computer systems. It is about putting together a network of computers (workstations, PCs and supercomputers), getting them running and then keeping them running in spite of the activities of users who tend to cause the systems to fail.

Data Communication and Computer Networking module | PDF page 29 | lines 25-36

> System administration is the term used traditionally by mainframe and Unix engineers to describe the management of computers whether they are coupled by a network or not. To this community, network administration means the management of network infrastructure devices (routers and switches). The world of personal computers (PCs) has no tradition of managingindividual computers and their subsystems, and thus doesnot speak of system administration, per se. To this community, network administration is the management ofPCs in a network. In this material, we shall take the first view, since this is more precise.

Question sources

Computer Science MCQ practice collection · Question 564

Question 37 | AM0565

Under the note’s primary division of administrative responsibilities, which listed task directly concerns ongoing network connectivity, performance and protection?

A. Installing and configuring operating systems

B. Monitoring network performance and security

C. Developing software applications

D. Providing end-user training

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer B: Monitoring network performance and security

Network administrators primarily maintain connectivity, addressing, routes, devices and performance. Monitoring network performance and security directly matches that operational scope. Operating-system installation and user training may be shared administrative duties, but they do not directly describe the ongoing network-monitoring task asked for. Developing software applications has a different primary purpose. The scope selects the core network responsibility without claiming exclusive job boundaries.

Why each choice is right or wrong

A - Incorrect: OS installation can overlap with administrative work, but is not the ongoing network-monitoring task requested.

B - Correct: Monitoring network performance and security directly matches network-administration responsibilities.

C - Incorrect: Developing application software is not a network-administration responsibility established by this note.

D - Incorrect: User training may be shared, but does not directly name monitoring network operation.

Primary note proof

Study-note section NSA01

> System administrators maintain hosts, accounts, storage, software and availability; network administrators maintain connectivity, addressing, routes, network devices and performance. Security administrators coordinate controls and policy. These duties overlap, so account management, testing patches and training users are not exclusive to one job title. Patience, communication, ethics, technical understanding and organization matter alongside command knowledge.

Study-note section NSA22

> Measure a baseline, sample over an interval, compare with workload and correlate symptoms before changing hardware. CPU utilization/run queues identify processing pressure; low free memory alone is weak evidence because cache may be reclaimable. Persistent paging with high latency indicates memory pressure. Storage capacity and I/O latency are separate: a disk can be nearly empty but saturated, or nearly full while lightly loaded.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 29 | lines 44-56

> Scope of Network administration
> The management of a network, usually called network administration, consists of procedures and services that keep the network running properly. An important part of network management entails making sure that the network is available (or up and

running as IT professionals say) when employees and managers need it.Other admin activities are:
• Monitoring the network capacity to ensure that alltransmission requirements can be met.
• Adding capacity to the network by increasing band width interconnecting additional modes, or creating and interconnecting additional networks.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 30 | lines 41-51

The challenges of system administration
System administration is not just about installing operating systems. It is about planning and designing an efficient community of computers so that real users will be able to get their jobs done. That means:
• Designing a network which is logical and efficient.
• Deploying large numbers of machines which can be easily upgraded later.
• Deciding what services are needed.
• Planning and implementing adequate security.
• Providing a comfortable environment for users.

Data Communication and Computer Networking module | PDF page 30 | lines 2-5

• Training people to use the network effectively
• Assisting IT professionals in organizational applications that will make good use of the network‘s capabilities.

Question sources

Computer Science MCQ practice collection · Question 565

Question 38 | AM0566

What is the purpose of system administration?

A. Managing software development projects

B. Ensuring the availability and reliability of computer systems

C. Managing user accounts and permissions

D. Designing computer networks

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer B: Ensuring the availability and reliability of computer systems

Keeping systems running (PDF p.28) and seeking predictability as the basis of reliability (p.31) support availability and reliability as the purpose. User permissions are a means of administration (p.42), not its full goal.

Why each choice is right or wrong

A - Incorrect: Software-project management is not the system-operation goal defined on p.28.

B - Correct: Availability follows from keeping systems running; reliability is explicitly tied to predictability (pp.28,31).

C - Incorrect: Account and permission management is a narrower activity (p.42).

D - Incorrect: Design is one planning task, narrower than the operational goal (pp.28,30).

Primary note proof

Study-note section NSA01

> System administrators maintain hosts, accounts, storage, software and availability; network administrators maintain connectivity, addressing, routes, network devices and performance. Security administrators coordinate controls and policy. These duties overlap, so account management, testing patches and training users are not exclusive to one job title. Patience, communication, ethics, technical understanding and organization matter alongside command knowledge.

Study-note section NSA01

> Use documentation, standardization, least privilege, automation and measured change. Record the current state, intended change, rollback and validation. Schedule maintenance according to service impact and urgency, not merely because a calendar date arrived. Fault management restores failures; performance management measures service behavior; configuration management tracks settings; security management controls access; accounting tracks usage.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 46-53

Philosophy of System Administration
Network and system administration is a branch of engineering that concerns the operational management of human-computer systems. It is about putting together a network of computers (workstations, PCs and supercomputers), getting them running and then keeping them running in spite of the activities of users who tend to cause the systems to fail.

Data Communication and Computer Networking module | PDF page 31 | lines 30-35

Principle 2 (Predictability)
The highest level aim in system administration is to work towards a predictable system. Predictability has limits. It is the basis of reliability, hence trust and therefore security.

Data Communication and Computer Networking module | PDF page 42 | lines 36-49

All user accounts have specific capabilities, privileges, and rights. When you create a user account, you can grant the user specific capabilities by making the user a member of one or more groups. This gives the user the capabilities of these groups. You then assign additional capabilities by making a user a member of the appropriate groups or withdraw capabilities by removing a user from a group. An important part of an administrator‘s job is being able to determine and set permissions, privileges, and logon rights as necessary. Although you can‘t change a group‘s built-in capabilities, you can change a group‘s default privileges and logon rights. For example, you could revoke network access to a computer by removing agroup‘s right to access the computer from the network.

Question sources

Computer Science MCQ practice collection · Question 566

Question 39 | AM0567

What is a key principle of system administration?

A. Least privilege

B. Agile development

C. Object-oriented programming

D. Cloud computing

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: Least privilege

NSA01 explicitly identifies least privilege among administration principles: give accounts and processes only the access required for their work. Agile development and object-oriented programming are development approaches; cloud computing is a computing/deployment model. They may occur in administered systems but are not the administration access principle asked for.

Why each choice is right or wrong

A - Correct: Least privilege is explicitly named as a system-administration principle in NSA01.

B - Incorrect: Agile development organizes software work rather than specifying the administration access principle in the note.

C - Incorrect: Object-oriented programming structures software; it is not the stated system-administration principle.

D - Incorrect: Cloud computing is a delivery/deployment model, not the access-control principle listed in NSA01.

Primary note proof

Study-note section NSA17

> Create named accounts, assign only needed groups/rights, disable departed users and audit privileged activity. Authentication verifies the account; authorization permits operations. A user right such as remote logon differs from a permission on one file. Group-based administration is easier to review than many hidden individual grants.

Study-note section NSA-S01

> Least privilege limits an account or process to the rights its task needs. Agile development instead organizes frequent delivery and adaptation of software. Object-oriented programming organizes software around objects with state and behavior. Cloud computing supplies on-demand access to a shared pool of configurable computing resources. A development approach or hosting model does not itself define an access-rights principle.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 31 | lines 17-29

> Principle 1 (Policy is the foundation)
> System administration begins with a
> policy - adecision about what we want
> and what should be, in relation to what we
> can afford.
> Policy speaks of what we wish to

accomplish with the system, and what we
are willing to tolerate of behavior within it.
It must refer to both the component parts and
to the environmentwith which the system
interacts. If we cannot secure predictability,
then we cannot expect
long-term conformance with a policy.

Data Communication and Computer Networking module | PDF page 31 | lines 30-35

Principle 2 (Predictability)
The highest level aim in system
administration is to work towards a
predictable system. Predictability has limits.
It is the basis of reliability, hence trust and
therefore security.

Data Communication and Computer Networking module | PDF page 43 | lines 47-52

Assigning User Rights
The most efficient way to assign user rights is to make the
user a member of a group that already has the right. In
some cases, however, you might want a user to have a
particular right but not have all the other rights of the
group. One way to resolve this problem is to give the user

Question sources

Computer Science MCQ practice collection · Question 567

Question 40 | AM0568

Using the note’s primary role division, which role is responsible for host-local accounts together with host storage, software and availability?

A. Network administrator

B. Database administrator

C. Security administrator

D. System administrator

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: System administrator

System administrators maintain hosts, accounts, storage, software and availability. Network administrators focus on connectivity and routes, while security administrators coordinate controls and policy. Database administration concerns a different resource scope. Responsibilities can overlap, but the stated question asks for the primary host-level role associated with the complete stated set of duties rather than implying that no other administrator ever manages accounts.

Why each choice is right or wrong

A - Incorrect: The primary network role concerns connectivity, addressing and routing rather than this host-level bundle.

B - Incorrect: Database-account administration is a narrower resource scope than the host-level duties listed.

C - Incorrect: Security administration coordinates controls and policy rather than the complete host-maintenance bundle.

D - Correct: System administration is assigned hosts, accounts, storage, software and availability.

Primary note proof

Study-note section NSA01

> System administrators maintain hosts, accounts, storage, software and availability; network administrators maintain connectivity, addressing, routes, network devices and performance. Security administrators coordinate controls and policy. These duties overlap, so account management, testing patches and training users are not exclusive to one job title. Patience, communication, ethics, technical understanding and organization matter alongside command knowledge.

Study-note section NSA17

> Create named accounts, assign only needed groups/rights, disable departed users and audit privileged activity. Authentication verifies the account; authorization permits operations. A user right such as remote logon differs from a permission on one file. Group-based administration is easier to review than many hidden individual grants.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 42 | lines 36-49

> All user accounts have specific capabilities, privileges,
> and rights. When you create a user account, you can grant
> the user specific capabilities by making the user a member
> of one or more groups. This gives the user the capabilities
> of these groups. You then assign additional capabilities by
> making a user a member of the appropriate groups or
> withdraw capabilities by removing a user from a group.
> An important part of an administrator‘s job is being able

> to determine and set permissions, privileges, and logon rights as necessary. Although you can‘t change a group‘s built-in capabilities, you can change a group‘s default privileges and logon rights. For example, you could revoke network access to a computer by removing agroup‘s right to access the computer from the network.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

> • Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
> • Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Question sources

Computer Science MCQ practice collection · Question 568

Question 41 | AM0569

What is the purpose of network administration?

A. Managing computer hardware

B. Managing computer software

C. Managing network infrastructure

D. Managing user accounts

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C: Managing network infrastructure

PDF p.29 distinguishes the management of computers from management of network infrastructure devices, explicitly adopting the latter meaning for network administration. C is the direct match.

Why each choice is right or wrong

A - Incorrect: General hardware management is broader than the infrastructure-device definition on p.29.

B - Incorrect: General software management is not the adopted network-administration definition.

C - Correct: The module defines network administration as managing routers, switches and network infrastructure (p.29).

D - Incorrect: Account management is an administration subtask but not the adopted infrastructure-focused definition.

Primary note proof

Study-note section NSA01

System administrators maintain hosts, accounts, storage, software and availability; network administrators maintain connectivity, addressing, routes, network devices and performance. Security administrators coordinate controls and policy. These duties overlap, so account management, testing patches and training users are not exclusive to one job title. Patience, communication, ethics, technical understanding and organization matter alongside command knowledge.

Study-note section NSA02

Switching normally forwards frames using MAC addresses within a LAN; routing forwards IP packets between networks. TCP supplies an ordered reliable byte stream, while UDP preserves datagrams without that guarantee. Ports distinguish application endpoints, not physical connectors. Draw switches, links, subnets, gateways, service hosts and dependencies in a network diagram. A topology's shape alone does not guarantee security.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 29 | lines 25-36

System administration is the term used traditionally by mainframe and Unix engineers to describe the management of computers whether they are coupled by a network or not. To this community, network administration means the management of network infrastructure devices (routers and switches). The world of personal computers (PCs) has no tradition of managingindividual computers and their subsystems, and thus doesnot speak of system administration, per se. To this community, network administration is the management ofPCs in a network. In this material, we shall take the first view, since this is more precise.

Question sources

Computer Science MCQ practice collection · Question 569

Question 42 | AM0570

What is the role of a security administrator in system administration?

A. Monitoring network performance

B. Managing user accounts and permissions

C. Enforcing security policies and procedures

D. Configuring network devices

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer C: Enforcing security policies and procedures

PDF p.30 requires putting security procedures in place and ensuring they are followed; p.34 says domain controllers enforce security policy. Enforcing policies and procedures is therefore the best statement of the security role, without assuming exclusive staffing boundaries.

Why each choice is right or wrong

A - Incorrect: Performance monitoring is separately discussed as capacity management (p.29).

B - Incorrect: Account permissions contribute to access security but are narrower than enforcing security procedures.

C - Correct: The duty to ensure security procedures are followed is explicit on p.30.

D - Incorrect: Configuring devices is not by itself the policy-enforcement purpose described on p.30.

Primary note proof

Study-note section NSA26

> A security policy states required behavior, scope, accountable roles and enforcement. Begin with assets/service objectives, assess threats and weaknesses, choose controls, define exceptions/incident procedures, approve/communicate, monitor and periodically review. CIA means confidentiality, integrity and availability; neither sensitive-data protection nor availability alone is the universal primary goal.

Study-note section NSA01

> System administrators maintain hosts, accounts, storage, software and availability; network administrators maintain connectivity, addressing, routes, network devices and performance. Security administrators coordinate controls and policy. These duties overlap, so account management, testing patches and training users are not exclusive to one job title. Patience, communication, ethics, technical understanding and organization matter alongside command knowledge.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

> • Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
> • Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 34 | lines 7-14

> Domain Controllers
> A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing end devices to access shared domain resources. It authenticates users, stores user account information and enforces security policy for a domain. It is most commonly implemented in Microsoft

Question sources

Computer Science MCQ practice collection · Question 570

Question 43 | AM0571

Which concept in system administration emphasizes the importance of regularly backing up data?

A. Redundancy

B. Fault tolerance

C. Disaster recovery

D. Load balancing

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C: Disaster recovery

PDF p.30 explicitly pairs “Backup and disaster recovery planning.” Its backup duty protects against network/component failure. Disaster recovery is therefore the choice directly connected to regular data backup in the module.

Why each choice is right or wrong

A - Incorrect: Redundancy can protect operation but is not the theme explicitly paired with backups on p.30.

B - Incorrect: Fault tolerance is not the module's named backup-planning concept here.

C - Correct: Backup and disaster recovery planning are explicitly paired (p.30).

D - Incorrect: Load balancing is not connected to backup planning in this passage.

Primary note proof

Study-note section NSA-S02

> Disaster recovery planning prepares for restoring systems and data after disruptive loss. Regular protected backups and tested restoration are part of that plan. Continuing operation despite a component failure is a fault-tolerance objective; possessing extra components alone does not establish that older valid data can be recovered.

Study-note section NSA24

> Backups recover previous data after deletion, compromise, corruption, failed upgrades/migrations or hardware loss. Authorization controls current access, a different function. A mirror/replica also copies deletions or corruption and does not replace versioned independent backups. Keep protected copies in separate failure domains, define retention and test restores.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 19-33

> Although the specifics of being a system administrator
> may change from platform to platform, there are
> underlying themes that do not. These themes make up the
> philosophy of system administration. The themes are:
> • Automate everything
> • Document everything
> • Communicate as much as possible
> • Know your resources
> • Know your users
> • Know your business
> • Security cannot be an afterthought
> • Plan ahead
> • Expect the unexpected
> • Backup and disaster recovery planning
> • Patching

Data Communication and Computer Networking module | PDF page 30 | lines 6-8

> • Backing up the network software and data
> regularly to protect against the failure of network
> or any of its components

Question sources

Computer Science MCQ practice collection · Question 571

Question 44 | AM0572

Which skill describes the general process of diagnosing faults and selecting fixes across system-administration tasks, rather than a specialized design, database or cabling task?

A. Graphic design

B. Database query optimization

C. Troubleshooting and problem-solving

D. Network cable installation

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C: Troubleshooting and problem-solving

Troubleshooting and problem-solving cover defining symptoms, gathering evidence, forming testable hypotheses, isolating causes, applying targeted fixes and verifying service. This process applies across many administration duties. Graphic design, query optimization and cable installation may be useful specialized activities, but none names the broad diagnostic process requested. The scope does not imply that administrators never perform those other tasks.

Why each choice is right or wrong

A - Incorrect: Graphic design concerns visual communication rather than the general diagnostic process.

B - Incorrect: Query optimization improves database query behavior, a specialized task.

C - Correct: Troubleshooting and problem-solving name the requested cross-task diagnostic skill.

D - Incorrect: Cable installation is a physical infrastructure task rather than the general reasoning process.

Primary note proof

Study-note section NSA08

> Define the symptom, scope, time and recent changes; gather the configuration, baseline and logs. Form a testable hypothesis, test the least disruptive explanation, isolate the failing component, apply a targeted fix, verify the user service and document the result. Change one relevant factor at a time when possible. A reboot can hide evidence and is not a diagnosis by itself.

Study-note section NSA09

> Check power, cable/connector and link state, then NIC/driver state, VLAN membership, address/prefix, local gateway, route, DNS and finally application port/authentication. A recognized NIC makes a missing driver less likely, not proof of a working physical link. Ethernet commonly uses RJ45 connectors; an RJ11 telephone jack is not the expected Ethernet connection.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 29 | lines 16-20

> It‘s about hardware, software, user support, diagnosis, repair and prevention. System administrators need to know a bit of everything: the skills are technical, administrative and socio-psychological.

Data Communication and Computer Networking module | PDF page 30 | lines 16-18

> • Diagnosing and troubleshooting problems on the network and determining the best course of action to take to solve them.

Data Communication and Computer Networking module | PDF page 31 | lines 7-14

> Some system administrators are responsible for both the hardware of the network and the computers which it connects, i.e. the cables as well as the computers. Some are only responsible for the computers. Either way, an understanding of how data flow from machine to machineis essential as well as an understanding of how each machine affects every other.

Question sources

Computer Science MCQ practice collection · Question 572

Question 45 | AM0573

Which tasks belong to administrator-side software update and patch management, rather than authoring the software patch? Select all that apply.

A. Developing software patches

B. Testing software updates

C. Installing and deploying software updates

D. Analyzing software vulnerabilities

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer B, C, D: Testing software updates; Installing and deploying software updates; Analyzing software vulnerabilities

Patch administration includes assessing relevant weaknesses, testing or staging an update, preparing rollback, deploying it and verifying the result. These steps help choose and safely apply the appropriate repair. Writing the vendor's software patch is a development activity rather than the operational workflow being classified. The multiple-selection instruction retains the complementary assessment, testing and deployment responsibilities instead of forcing an installation-only answer.

Why each choice is right or wrong

A - Incorrect: Writing the software patch is a development responsibility, not the patch-administration workflow stated here.

B - Correct: Testing/staging updates before deployment is an explicit administrator duty.

C - Correct: Deploying and verifying software updates is also an explicit administrator duty.

D - Correct: Assessing known weaknesses helps prioritize relevant patches and is part of the stated vulnerability-management workflow.

Primary note proof

Study-note section NSA27

> Hardening reduces exposure through unnecessary-service removal, supported patches, restricted accounts/permissions and appropriate port filtering. Blocking an unused known port can be hardening; blocking every useful port merely destroys availability. Weak passwords and unpatched exploitable software are vulnerabilities; attacks exploit weaknesses, and risk combines likelihood with impact.

Study-note section NSA27

> Preventive controls restrict harmful actions, detective controls expose them and recovery controls restore service. Account lifecycle, backup procedures, device configuration and traffic analysis can all be security controls under a stated objective. A vulnerability scan checks known weakness patterns, not bandwidth. Test/stage patches, prepare rollback, deploy and verify; testing and installation are both legitimate administrator duties.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 19-33

> Although the specifics of being a system administrator
> may change from platform to platform, there are
> underlying themes that do not. These themes make up the
> philosophy of system administration. The themes are:
> • Automate everything
> • Document everything
> • Communicate as much as possible
> • Know your resources

• Know your users
• Know your business
• Security cannot be an afterthought
• Plan ahead
• Expect the unexpected
• Backup and disaster recovery planning
• Patching

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Question sources

Computer Science MCQ practice collection · Question 573

Question 46 | AM0574

Which listed protocol sends or relays email messages between mail systems?

A. FTP

B. HTTP

C. SMTP

D. DHCP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C: SMTP

SMTP is the mail sending and relay protocol. HTTP serves web resources, so a webmail interface can use HTTP without making it the mail-transfer protocol requested here. FTP transfers files as its named service, and DHCP supplies host configuration. Distinguishing the mail transport role from a user-facing web interface removes the broad interpretation of providing email services.

Why each choice is right or wrong

A - Incorrect: FTP is a file-transfer protocol, not the listed mail relay protocol.

B - Incorrect: HTTP serves web resources; webmail access is distinct from mail-system relay.

C - Correct: SMTP sends and relays email messages.

D - Incorrect: DHCP supplies host configuration rather than transferring email.

Primary note proof

Study-note section NSA10

> DNS resolves names; DHCP supplies host configuration. SMTP sends/relays mail, while IMAP/POP retrieve it. FTP is a named file-transfer protocol; HTTP also transfers files, so “transfers files” is not an exclusive FTP description. HTTP/HTTPS serve web resources. SSH provides encrypted remote login; SFTP transfers files over SSH and differs from FTP or FTPS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

> Application Layer
> The Application Layer is a combination of Session,
> Presentation & Application Layers of OSI models and defines
> high level protocols like File Transfer (FTP), Electronic Mail
> (SMTP), Virtual Terminal (TELNET), Domain Name Service
> (DNS), etc.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

> The Process/Application Layer Protocols
> • Telnet
> • File Transfer Protocol (FTP)
> • Network File System (NFS).
> • Simple Mail Transfer Protocol (SMTP
> • POP3 is used to receive mail.
> • Simple Network Management Protocol (SNMP)
> • Domain Name Service (DNS)
> • Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science MCQ practice collection · Question 574

Question 47 | AM0575

Which service translates domain names into IP addresses?

A. DNS

B. DHCP

C. FTP

D. HTTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: DNS

Name-to-address translation is forward DNS resolution. NSA06 specifies A records for IPv4 and AAAA for IPv6. DHCP instead provides host configuration, while FTP and HTTP provide application data-transfer services. Those functions are distinct from resolving a domain name into its address records.

Why each choice is right or wrong

A - Correct: DNS forward resolution maps names to address records, using A or AAAA as appropriate.

B - Incorrect: DHCP supplies client addresses and options rather than translating arbitrary domain names.

C - Incorrect: FTP transfers files and does not provide the domain-name resolution service.

D - Incorrect: HTTP exchanges web resources rather than serving as the name-to-address directory service.

Primary note proof

Study-note section NSA06

> Forward resolution obtains an address from a name, using A for IPv4 and AAAA for IPv6. Reverse lookup uses a PTR record in the reverse namespace to obtain a name from an address. CNAME aliases a name, MX identifies mail exchangers and NS identifies authoritative name servers. Forward and reverse records need not both exist or be perfect inverses.

Study-note section NSA10

> DNS resolves names; DHCP supplies host configuration. SMTP sends/relays mail, while IMAP/POP retrieve it. FTP is a named file-transfer protocol; HTTP also transfers files, so “transfers files” is not an exclusive FTP description. HTTP/HTTPS serve web resources. SSH provides encrypted remote login; SFTP transfers files over SSH and differs from FTP or FTPS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP
address, 127.0.0.1, which is
usedfor interprocess communication.
Never remove this line! Sometimes contains
addresses of additional hosts, whichcan be contacted
without using an external naming service such as
DNS (the Domain Name Server).

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science MCQ practice collection · Question 575

Question 48 | AM0576

Which listed protocols transfer file content from a server to a client as part of their ordinary service? Select all that apply.

A. SMTP

B. DNS

C. FTP

D. HTTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C, D: FTP; HTTP

FTP is specifically a file-transfer protocol, while HTTP also transfers file resources through web request and response exchanges. Their service semantics differ, but the broad content-transfer capability applies to both. SMTP is classified here as mail submission and relay, and DNS as name resolution. The revised selection instruction recognizes the two qualifying services without pretending that file transfer is exclusive to one protocol.

Why each choice is right or wrong

A - Incorrect: SMTP is identified with mail submission/relay rather than the file-transfer service in this comparison.

B - Incorrect: DNS resolves names and is not the offered file-content transfer service.

C - Correct: FTP is explicitly a named protocol for client/server file transfer.

D - Correct: HTTP also transfers file resources, so the general function is not exclusive to FTP.

Primary note proof

Study-note section NSA10

> DNS resolves names; DHCP supplies host configuration. SMTP sends/relays mail, while IMAP/POP retrieve it. FTP is a named file-transfer protocol; HTTP also transfers files, so “transfers files” is not an exclusive FTP description. HTTP/HTTPS serve web resources. SSH provides encrypted remote login; SFTP transfers files over SSH and differs from FTP or FTPS.

Study-note section NSA06

> Forward resolution obtains an address from a name, using A for IPv4 and AAAA for IPv6. Reverse lookup uses a PTR record in the reverse namespace to obtain a name from an address. CNAME aliases a name, MX identifies mail exchangers and NS identifies authoritative name servers. Forward and reverse records need not both exist or be perfect inverses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

> Application Layer
> The Application Layer is a combination of Session,
> Presentation & Application Layers of OSI models and defines
> high level protocols like File Transfer (FTP), Electronic Mail
> (SMTP), Virtual Terminal (TELNET), Domain Name Service
> (DNS), etc.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

> The Process/Application Layer Protocols
> • Telnet
> • File Transfer Protocol (FTP)
> • Network File System (NFS).
> • Simple Mail Transfer Protocol (SMTP

- POP3 is used to receive mail.
- Simple Network Management Protocol (SNMP)
- Domain Name Service (DNS)
- Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science MCQ practice collection · Question 576

Question 49 | AM0577

Which service is responsible for assigning IP addresses to devices on a network?

A. DNS

B. DHCP

C. FTP

D. HTTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer B: DHCP

NSA04 assigns host-address configuration to DHCP, including a server-managed scope and time-limited leases. DNS resolves names, while FTP and HTTP transfer application content. Therefore DHCP is the network service responsible for automatically supplying a device's IP configuration among these options.

Why each choice is right or wrong

A - Incorrect: DNS resolves names into records; it does not lease the device's own network address.

B - Correct: DHCP supplies addresses and configuration options to clients from a managed scope.

C - Incorrect: FTP transfers files rather than assigning network addresses to devices.

D - Incorrect: HTTP provides web request/response services and not host-address allocation.

Primary note proof

Study-note section NSA04

DHCP supplies addresses and configuration options. Typical initial IPv4 allocation is Discover→Offer→Request→ACK. The server manages its scope/pool, allocated leases, exclusions and reservations; options may include mask, gateway and DNS servers. A dynamic lease lasts for a specified interval, not forever.

Study-note section NSA10

DNS resolves names; DHCP supplies host configuration. SMTP sends/relays mail, while IMAP/POP retrieve it. FTP is a named file-transfer protocol; HTTP also transfers files, so “transfers files” is not an exclusive FTP description. HTTP/HTTPS serve web resources. SSH provides encrypted remote login; SFTP transfers files over SSH and differs from FTP or FTPS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science MCQ practice collection · Question 577

Question 50 | AM0578

Which protocol is used for secure remote login and file transfer?

A. SSH

B. DNS

C. FTP

D. HTTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: SSH, with SFTP for file transfer over SSH

NSA10 assigns protected remote login to SSH and file transfer over that protected connection to SFTP. Thus SSH is the underlying secure protocol family among these options. DNS provides naming; ordinary FTP and HTTP do not by themselves provide the protected remote-login capability in the stem.

Why each choice is right or wrong

A - Correct: SSH protects remote login and supports the SFTP file-transfer service over SSH.

B - Incorrect: DNS resolves names and supplies neither remote terminal login nor a secure file-transfer session.

C - Incorrect: Ordinary FTP transfers files but is distinct from SFTP and does not supply encrypted remote login.

D - Incorrect: Ordinary HTTP supplies web exchange semantics, not the SSH remote-login and SFTP functions.

Primary note proof

Study-note section NSA10

DNS resolves names; DHCP supplies host configuration. SMTP sends/relays mail, while IMAP/POP retrieve it. FTP is a named file-transfer protocol; HTTP also transfers files, so “transfers files” is not an exclusive FTP description. HTTP/HTTPS serve web resources. SSH provides encrypted remote login; SFTP transfers files over SSH and differs from FTP or FTPS.

Study-note section NSA30

Use authenticated protected remote administration such as SSH or properly secured management services, with restricted source access and auditing. VPNs provide protected connectivity under their defined security model; they are not packet analyzers. Firewall filtering permits/blocks traffic according to policy; it is not inherently encryption. Losing remote connectivity while changing a management route/firewall is an operational risk to plan for.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 58 | lines 22-32

The following are some of proprietary and open source
applications that can be used to achieve this.
• SSH (Secure Shell)
• OpenSSH (OpenBSD Secure Shell)
• Telnet
• rlogin
• rsh
• VNC (Virtual Network Computing)
• FreeNX
• Wireless Remote Administration
• Remote Desktop Connection (RDC)

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

Application Layer
The Application Layer is a combination of Session,
Presentation & Application Layers of OSI models and defines
high level protocols like File Transfer (FTP), Electronic Mail
(SMTP), Virtual Terminal (TELNET), Domain Name Service
(DNS), etc.

Question sources

Computer Science MCQ practice collection · Question 578

Question 51 | AM0579

Which service is used for translating private IP addresses to public IP addresses?

A. NAT

B. DNS

C. FTP

D. HTTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: NAT

NAT rewrites network addresses, commonly translating private internal IPv4 addresses for access to a public network. Routing still selects the path and NAT does not replace firewall or authentication policy. DNS resolves names, FTP transfers files, and HTTP serves web resources. Those application services may run through a translating router, but they do not perform the address-rewriting function themselves.

Why each choice is right or wrong

A - Correct: NAT performs the requested address translation.

B - Incorrect: DNS maps names and related records rather than rewriting packet addresses.

C - Incorrect: FTP transfers files rather than translating network addresses.

D - Incorrect: HTTP serves web resources rather than rewriting IP addresses.

Primary note proof

Study-note section NSA11

> Routing selects a next hop using a destination prefix; NAT rewrites addresses. Many-to-one address-and-port translation (PAT/NAPT) maps internal flows to one public address using distinct port bindings. For example, two private client sockets can appear as public-address ports 40001 and 40002, with replies translated back to the correct clients.

Study-note section NSA11

> NAT is often used when private IPv4 clients access public networks; it does not itself replace a gateway, route, firewall or authentication. One-to-one NAT and destination translation are other forms, so NAT does not always mean many hosts share one address. Public addressing inside a LAN does not automatically require NAT. Unsolicited inbound service access may require explicit mapping and filtering.

Study-note section NSA06

Forward resolution obtains an address from a name, using A for IPv4 and AAAA for IPv6. Reverse lookup uses a PTR record in the reverse namespace to obtain a name from an address. CNAME aliases a name, MX identifies mail exchangers and NS identifies authoritative name servers. Forward and reverse records need not both exist or be perfect inverses.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Computer Science MCQ practice collection · Question 579

Question 52 | AM0580

Which protocol is used for web browsing?

A. SMTP

B. DNS

C. FTP

D. HTTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: HTTP

Web browsing obtains resources through web request/response exchanges. NSA10 identifies HTTP/HTTPS for these resources, making HTTP the offered protocol. SMTP handles mail submission/relay, DNS handles name resolution and FTP handles its own file-transfer service; they may assist applications but do not define the web exchange asked for.

Why each choice is right or wrong

A - Incorrect: SMTP submits and relays email rather than serving browser web resources.

B - Incorrect: DNS resolves server names and is a supporting service rather than the web resource-transfer protocol.

C - Incorrect: FTP is a separate file-transfer protocol, not the normal web-browsing exchange named in the note.

D - Correct: HTTP supplies web-resource request/response exchanges and is explicitly named for web services.

Primary note proof

Study-note section NSA10

> DNS resolves names; DHCP supplies host configuration. SMTP sends/relays mail, while IMAP/POP retrieve it. FTP is a named file-transfer protocol; HTTP also transfers files, so “transfers files” is not an exclusive FTP description. HTTP/HTTPS serve web resources. SSH provides encrypted remote login; SFTP transfers files over SSH and differs from FTP or FTPS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

> Application Layer
> The Application Layer is a combination of Session,
> Presentation & Application Layers of OSI models and defines
> high level protocols like File Transfer (FTP), Electronic Mail
> (SMTP), Virtual Terminal (TELNET), Domain Name Service
> (DNS), etc.

Data Communication and Computer Networking module | PDF page 28 | lines 2-7

> TCP and UDP must use port numbers to communicate
> with the upper layers, because they‘re what keep track of
> different conversations crossing the network
> simultaneously. These port numbers identify the source
> and destination application or process in the TCP
> segment. There are 216 = 65,536 ports available.

Question sources

Computer Science MCQ practice collection · Question 580

Question 53 | AM0581

Which service provides remote access to a network from a different location?

A. VPN

B. DNS

C. FTP

D. HTTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: VPN

A remote user can extend private-network connectivity through a VPN over another network, matching the service in the stem. DNS performs lookup, FTP transfers files and HTTP serves web resources. Those can be reachable remotely but do not by themselves extend private network access as the VPN service does.

Why each choice is right or wrong

A - Correct: A VPN extends private connectivity across another network to support remote access.

B - Incorrect: DNS supplies name resolution rather than a remote private-network connection.

C - Incorrect: FTP supplies access to a file-transfer service rather than general remote network connectivity.

D - Incorrect: HTTP supplies web-resource access rather than the private-network extension described.

Primary note proof

Study-note section NSA10

> A VPN extends private connectivity over another network; secure tunneling commonly encrypts/authenticates traffic but depends on protocol/configuration. RTP carries real-time media timing/sequence information, often over UDP; it does not guarantee timely delivery. Network printers expose services shared by clients. Provide accounts, permissions, configuration, monitoring and recovery for each service, not just its protocol name.

Study-note section NSA30

> Use authenticated protected remote administration such as SSH or properly secured management services, with restricted source access and auditing. VPNs provide protected connectivity under their defined security model; they are not packet analyzers. Firewall filtering permits/blocks traffic according to policy; it is not inherently encryption. Losing remote connectivity while changing a management route/firewall is an operational risk to plan for.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 57 | lines 78-87

Remote Administration
Remote administration is an approach being followed to control either a computer system or a network or an application or all three from a remote location. Simply put, Remote administration refers to any method of controlling a computer from a remote location. A remote location may refer to a computer in the next room or one on the other side of the world. It may also refer to both legal and illegal remote administration. Generally, remote administration is essentially adopted when it is difficult or

Data Communication and Computer Networking module | PDF page 58 | lines 22-32

The following are some of proprietary and open source applications that can be used to achieve this.
• SSH (Secure Shell)
• OpenSSH (OpenBSD Secure Shell)
• Telnet
• rlogin
• rsh
• VNC (Virtual Network Computing)
• FreeNX
• Wireless Remote Administration
• Remote Desktop Connection (RDC)

Question sources

Computer Science MCQ practice collection · Question 581

Question 54 | AM0582

Which protocol is used for real-time communication, such as video conferencing?

A. SMTP

B. DNS

C. FTP

D. RTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: RTP

NSA10 identifies RTP as carrying real-time media timing and sequence information, commonly over UDP. That is the relevant protocol for conference media among the options. The answer does not imply guaranteed deadlines: actual delivery depends on the network and application. SMTP, DNS and FTP have unrelated mail, naming and file-transfer roles.

Why each choice is right or wrong

A - Incorrect: SMTP handles mail submission/relay, not real-time conference media timing and sequencing.

B - Incorrect: DNS resolves names and is not the media transport protocol described.

C - Incorrect: FTP transfers files rather than carrying the real-time media timing/sequence service.

D - Correct: RTP carries real-time media timing and sequence information, including uses such as video conferencing.

Primary note proof

Study-note section NSA10

> A VPN extends private connectivity over another network; secure tunneling commonly encrypts/authenticates traffic but depends on protocol/configuration. RTP carries real-time media timing/sequence information, often over UDP; it does not guarantee timely delivery. Network printers expose services shared by clients. Provide accounts, permissions, configuration, monitoring and recovery for each service, not just its protocol name.

Study-note section NSA10

> DNS resolves names; DHCP supplies host configuration. SMTP sends/relays mail, while IMAP/POP retrieve it. FTP is a named file-transfer protocol; HTTP also transfers files, so “transfers files” is not an exclusive FTP description. HTTP/HTTPS serve web resources. SSH provides encrypted remote login; SFTP transfers files over SSH and differs from FTP or FTPS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 18 | lines 27-32

> Application Layer
> The Application Layer is a combination of Session,
> Presentation & Application Layers of OSI models and defines
> high level protocols like File Transfer (FTP), Electronic Mail
> (SMTP), Virtual Terminal (TELNET), Domain Name Service
> (DNS), etc.

Question sources

Computer Science MCQ practice collection · Question 582

Question 55 | AM0583

Which service, using its many-to-one address-and-port translation form, lets several private IPv4 devices share one public IPv4 address?

A. NAT

B. DNS

C. FTP

D. HTTP

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: NAT

Many-to-one NAT with port translation maintains separate bindings for internal flows. Multiple clients can therefore appear under one public address while distinct translated ports allow replies to return to the right client. This is a particular form of NAT, not a property of every NAT configuration. DNS, FTP and HTTP supply naming, file-transfer and web services rather than the address-sharing mechanism.

Why each choice is right or wrong

A - Correct: NAT in its PAT/NAPT form maps multiple internal flows to one public address.

B - Incorrect: DNS resolves names rather than maintaining address-and-port translation bindings.

C - Incorrect: FTP transfers files; it is not the address-sharing mechanism.

D - Incorrect: HTTP serves web resources; it does not provide the translation bindings.

Primary note proof

Study-note section NSA11

> Routing selects a next hop using a destination prefix; NAT rewrites addresses. Many-to-one address-and-port translation (PAT/NAPT) maps internal flows to one public address using distinct port bindings. For example, two private client sockets can appear as public-address ports 40001 and 40002, with replies translated back to the correct clients.

Study-note section NSA11

> NAT is often used when private IPv4 clients access public networks; it does not itself replace a gateway, route, firewall or authentication. One-to-one NAT and destination translation are other forms, so NAT does not always mean many hosts share one address. Public addressing inside a LAN does not automatically require NAT. Unsolicited inbound service access may require explicit mapping and filtering.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Computer Science MCQ practice collection · Question 583

Question 56 | AM0584

Which policy conflicts with restricting access to a protected internal network to authorized users, assuming the wireless service directly admits users to that network?

A. Password complexity requirements

B. Firewall configuration

C. Regular data backups

D. Open wireless network access

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer D: Open wireless network access

A protected internal network requires controlled admission. Password requirements, appropriately configured firewall rules and protected regular backups can implement security and recovery policy. Unrestricted open wireless admission to the same protected network bypasses that admission requirement. An intentionally isolated guest service would be a different case; it is excluded by the stated direct-access condition.

Why each choice is right or wrong

A - Incorrect: Password requirements support authentication and controlled access.

B - Incorrect: Firewall policy can restrict access to authorized systems.

C - Incorrect: Regular backups support recovery and availability.

D - Correct: Unrestricted open wireless admission bypasses authorization for the protected network.

Primary note proof

Study-note section NSA26

A security policy states required behavior, scope, accountable roles and enforcement. Begin with assets/service objectives, assess threats and weaknesses, choose controls, define exceptions/incident procedures, approve/communicate, monitor and periodically review. CIA means confidentiality, integrity and availability; neither sensitive-data protection nor availability alone is the universal primary goal.

Study-note section NSA26

A policy can require password controls, approved encryption, restricted administrative access, backups and patch deadlines; firewall rules implement part of it. Open unrestricted wireless access conflicts with controlled internal access unless intentionally isolated as a guest service. “Use the system passively” is not a purpose of security policy. Policies coordinate action and reduce risk; they do not guarantee every attack will fail.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 30 | lines 6-8

• Backing up the network software and data regularly to protect against the failure of network or any of its components

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Computer Science MCQ practice collection · Question 584

Question 57 | AM0585

Which purpose is directly served when a firewall applies permit/deny rules to incoming network traffic?

A. To prevent unauthorized access to the network

B. To encrypt network traffic

C. To manage network bandwidth

D. To monitor network performance

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer A: To prevent unauthorized access to the network

A firewall applies policy to allow permitted traffic and reject disallowed access. This directly supports preventing unauthorized network access. Encryption protects confidentiality, bandwidth management allocates or shapes traffic capacity, and performance monitoring measures service behavior. A device may combine these features, but the stated permit/deny operation is access enforcement rather than those separate functions.

Why each choice is right or wrong

A - Correct: Permit/deny filtering directly prevents disallowed network access.

B - Incorrect: Encryption protects confidentiality and is not inherent in traffic filtering.

C - Incorrect: Bandwidth management controls traffic capacity rather than authorization.

D - Incorrect: Performance monitoring measures behavior rather than enforcing permit/deny policy.

Primary note proof

Study-note section NSA30

> Use authenticated protected remote administration such as SSH or properly secured management services, with restricted source access and auditing. VPNs provide protected connectivity under their defined security model; they are not packet analyzers. Firewall filtering permits/blocks traffic according to policy; it is not inherently encryption. Losing remote connectivity while changing a management route/firewall is an operational risk to plan for.

Study-note section NSA28

> Encryption provides confidentiality with correct key/nonce use; authenticated encryption adds integrity/authenticity. Unspecified encryption alone does not guarantee both properties. A password hash supports verification without recovering the original password; it is not a

reversible credential store. Encryption can protect a recoverable credential only if its key is separately protected.

Study-note section NSA12

QoS classifies, queues and prioritizes traffic to meet performance objectives such as low delay or limited loss. It can operate across layers and support applications, so it is not exclusively an application-layer service. Installing a new service is an administrative action; email configuration is another action and proxies/agents are components. Distinguish service-management actions from components using a stated taxonomy.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Computer Science MCQ practice collection · Question 585

Question 58 | AM0586

Which of the following is an example of a network security vulnerability?

A. Weak password policies

B. Regular software updates

C. Use of strong encryption algorithms

D. Implementing access control lists

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer A: Weak password policies

NSA27 identifies weak passwords as exploitable weaknesses. A policy permitting them creates the corresponding vulnerability. Regular updates, appropriate encryption and access-control lists are protective measures when correctly deployed, rather than examples of the weakness requested. They are not guarantees of security, but their stated role here is defensive.

Why each choice is right or wrong

A - Correct: Weak password policy permits easily compromised credentials and creates an exploitable access weakness.

B - Incorrect: Regular updates address known software weaknesses rather than constituting the vulnerability example requested.

C - Incorrect: Strong appropriately used encryption is a protective measure rather than an example of weak authentication policy.

D - Incorrect: Access-control lists restrict permitted actions/traffic and are a defensive control when properly configured.

Primary note proof

Study-note section NSA27

> Hardening reduces exposure through unnecessary-service removal, supported patches, restricted accounts/permissions and appropriate port filtering. Blocking an unused known port can be hardening; blocking every useful port merely destroys availability. Weak passwords and unpatched exploitable software are vulnerabilities; attacks exploit weaknesses, and risk combines likelihood with impact.

Study-note section NSA28

> Encryption provides confidentiality with correct key/nonce use; authenticated encryption adds integrity/authenticity. Unspecified encryption alone does not guarantee both properties. A password hash supports verification without recovering the original password; it is not a reversible credential store. Encryption can protect a recoverable credential only if its key is separately protected.

Study-note section NSA30

> Segmentation separates groups of systems and enforces allowed flows with routing/filtering policies; VLAN membership alone does not establish complete security. NAC assesses device/user admission and can reject or quarantine unauthorized/noncompliant devices. Authentication proves an identity, while access rules decide which resources it may use.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

> • Putting security procedures in place to make
> certain that only authorized users have access to
> the network and ensuring that all security

procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 42 | lines 21-28

Administrator: The —Administrator‖ user account has complete control over the PC. He or she can install anything and make changes that affect all users of that PC.
Standard: The —Standard‖ user account can only use the software that‘s already installed by the administrator and change system settings that don‘t affect other users.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Question sources

Computer Science MCQ practice collection · Question 586

Question 59 | AM0587

What is the purpose of intrusion detection systems (IDS)?

A. To prevent network attacks

B. To monitor network traffic for suspicious activities

C. To encrypt network communications

D. To block malicious software

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer B: Monitor for suspicious activity and alert

NSA23 distinguishes detection from prevention. An IDS monitors for suspicious activity and generates detection/alerts; blocking inline is an IPS capability. Encryption is a separate data-protection mechanism. Although IDS findings can support a broader prevention program, direct prevention or malware blocking is not the defining IDS role stated here.

Why each choice is right or wrong

A - Incorrect: Direct blocking/prevention is the IPS distinction; an IDS primarily detects and alerts.

B - Correct: Monitoring traffic for suspicious behavior matches the IDS detection/alert role.

C - Incorrect: Encrypting communications is a confidentiality mechanism, not intrusion detection.

D - Incorrect: Blocking malicious software is a preventive action, not the defining monitoring/alert purpose of an IDS.

Primary note proof

Study-note section NSA23

> An IDS detects/alerts; an IPS can block inline. Scanning identifies potential weaknesses rather than proving successful exploitation. A captured packet, open port or alert needs context. Monitoring network usage is not the same as configuring access control or encrypting communications.

Study-note section NSA28

> Encryption provides confidentiality with correct key/nonce use; authenticated encryption adds integrity/authenticity. Unspecified encryption alone does not guarantee both properties. A password hash supports verification without recovering the original password; it is not a reversible credential store. Encryption can protect a recoverable credential only if its key is separately protected.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

> System Monitoring Software Essentials
> In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
> • Acceptable delivery speeds
> • Constant availability
> • Preventative maintenance
> • Software version monitoring and patching
> • Intrusion detection

• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Data Communication and Computer Networking module | PDF page 54 | lines 13-17

Bandwidth monitoring tools and NetFlow and sFlow based traffic analyzers help you stay aware of the activity, capacity, and health of your network. They allow you to watch traffic as it flows through routers and switches, or arrive at and leaves hosts.

Question sources

Computer Science MCQ practice collection · Question 587

Question 60 | AM0588

During troubleshooting, which action tests IP reachability with ICMP echo messages without changing the system or network configuration?

A. Configuring a firewall rule

B. Conducting a security audit

C. Installing antivirus software

D. Ping testing network connectivity

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: Ping testing network connectivity

A ping test gathers reachability evidence by exchanging ICMP echo messages. It is a diagnostic observation rather than a configuration change. Firewall rule changes can be legitimate fixes for a diagnosed filtering fault, while audits and antivirus installation serve other security purposes. None of those alternatives performs the specific echo test requested. A failed test must still be interpreted alongside filtering and loss.

Why each choice is right or wrong

A - Incorrect: Changing a firewall rule changes policy rather than performing the specified observation.

B - Incorrect: A security audit assesses controls; it is not an ICMP echo test.

C - Incorrect: Installing antivirus changes host protection rather than sending echo probes.

D - Correct: Ping performs the specified reachability test without changing network policy.

Primary note proof

Study-note section NSA08

> Define the symptom, scope, time and recent changes; gather the configuration, baseline and logs. Form a testable hypothesis, test the least disruptive explanation, isolate the failing component, apply a targeted fix, verify the user service and document the result. Change one relevant factor at a time when possible. A reboot can hide evidence and is not a diagnosis by itself.

Study-note section NSA-S04

> Ping uses ICMP echo messages to test IP reachability. A reply shows that the addressed host and path support that exchange; no reply alone does not prove the host is disconnected, because filtering or loss can suppress responses. Traceroute instead discovers responding intermediate hops through packet-lifetime expiry; it is a path-discovery diagnostic, not the same question as an end-to-end echo test.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

> Ping (Packet Internet Groper) uses ICMP echo
> messages to check the physical and logical
> connectivity of machineson a network.

Data Communication and Computer Networking module | PDF page 30 | lines 16-18

> • Diagnosing and troubleshooting problems on the
> network and determining the best course of action
> to take to solve them.

Question sources

Computer Science MCQ practice collection · Question 588

Question 61 | AM0589

Under the note’s primary tool-role classification, which is the conventional general-purpose packet capture and dissection analyzer?

A. Wireshark

B. Nmap

C. Snort

D. Nessus

Hint

Match the requested observation to the tool’s actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer A: Wireshark

Wireshark is identified as the conventional analyzer for capturing and dissecting packets. Snort also has sniffing and logging capabilities, but its primary role in this comparison is suspicious-traffic detection and alerting. Nmap discovers hosts, ports and services, while Nessus assesses vulnerabilities and configuration. The primary-role scope distinguishes the intended analyzer without incorrectly denying overlapping packet capabilities in other tools.

Why each choice is right or wrong

A - Correct: Wireshark captures and dissects packets and is a conventional general packet analyzer.

B - Incorrect: Nmap performs host, port and service discovery rather than general packet capture/dissection.

C - Incorrect: Snort can sniff and log, but is classified primarily here by suspicious-traffic detection rather than as the conventional general analyzer.

D - Incorrect: Nessus is identified with vulnerability/configuration assessment rather than the packet-analyzer role.

Primary note proof

Study-note section NSA23

> Task Manager shows running processes/resource use; Resource Monitor/Performance Monitor give more detailed counters. Wireshark captures and dissects packets. Nmap discovers hosts/ports/services. Nessus assesses vulnerabilities/configuration. Snort can detect suspicious traffic and alert, and can prevent traffic in suitable inline deployments; it also has sniffing/logging roles. Thus packet-capture capability is not exclusive to one product, although Wireshark is the conventional analyzer choice.

Study-note section NSA23

> An IDS detects/alerts; an IPS can block inline. Scanning identifies potential weaknesses rather than proving successful exploitation. A captured packet, open port or alert needs context. Monitoring network usage is not the same as configuring access control or encrypting communications.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 54 | lines 13-17

> Bandwidth monitoring tools and NetFlow and sFlow
> based traffic analyzers help you stay aware of the activity,
> capacity, and health of your network. They allow you to
> watch traffic as it flows through routers and switches, or
> arrive at and leaves hosts.

Question sources

Computer Science MCQ practice collection · Question 589

Question 62 | AM0590

Which of the following is an example of a denial-of-service (DoS) attack?

A. Man-in-the-middle attack

B. Phishing attack

C. Distributed denial-of-service (DDoS) attack

D. Brute-force attack

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer C: Distributed denial-of-service (DDoS)

DDoS is denial of service performed from distributed sources, so it is directly a type of DoS. Interception, phishing and brute force describe different attack mechanisms; each might have secondary effects, but those names alone do not identify the service-availability attack requested. NSA29 supplies the explicit DoS/DDoS relationship.

Why each choice is right or wrong

A - Incorrect: An interception attack reads or alters communications; its name does not identify denial of service.

B - Incorrect: Phishing deceives users rather than specifically exhausting or denying a service.

C - Correct: DDoS is a denial-of-service attack using distributed sources.

D - Incorrect: Brute force tries credentials; that mechanism is distinct from the denial-of-service category asked about.

Primary note proof

Study-note section NSA29

> DoS harms service availability; DDoS uses distributed sources. Phishing deceives users, brute force tries credentials and an interception attack reads/alters communications. Correlate logs using time and identity/context. Preserve relevant evidence before resetting systems. A suspicious event is not automatically confirmed compromise; record facts and uncertainty.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

> System Monitoring Software Essentials
> In order to keep your system fit for purpose, your
> monitoring activities need to cover the following
> priorities:
> • Acceptable delivery speeds

- Constant availability
- Preventative maintenance
- Software version monitoring and patching
- Intrusion detection
- Data integrity
- Security monitoring
- Attack mitigation
- Virus prevention and detection

Question sources

Computer Science MCQ practice collection · Question 590

Question 63 | AM0591

For a secure VPN tunnel already providing private connectivity, which option identifies the mechanism that keeps intercepted tunnel payloads confidential?

A. To encrypt network traffic

B. To block unauthorized access

C. To manage network bandwidth

D. To analyze network performance

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: To encrypt network traffic

A secure VPN commonly encrypts and authenticates its tunnel traffic. Encryption protects the content against disclosure to an observer who intercepts packets, assuming appropriate configuration and keys. Admission rules can restrict who connects, but that is a different question from protecting intercepted payloads. Bandwidth management and performance analysis also serve different purposes. The secure-tunnel scope avoids claiming that every unqualified VPN automatically encrypts.

Why each choice is right or wrong

A - Correct: Encryption hides tunnel payload contents from an interceptor without the required keys.

B - Incorrect: Blocking unauthorized admission is distinct from protecting the content of already intercepted packets.

C - Incorrect: Bandwidth management is QoS/traffic management, not the defining private-connectivity purpose of a VPN.

D - Incorrect: Performance analysis is monitoring; VPN connectivity does not make it a packet or performance analyzer.

Primary note proof

Study-note section NSA10

A VPN extends private connectivity over another network; secure tunneling commonly encrypts/authenticates traffic but depends on protocol/configuration. RTP carries real-time media timing/sequence information, often over UDP; it does not guarantee timely delivery. Network printers expose services shared by clients. Provide accounts, permissions, configuration, monitoring and recovery for each service, not just its protocol name.

Study-note section NSA28

Encryption provides confidentiality with correct key/nonce use; authenticated encryption adds integrity/authenticity. Unspecified encryption alone does not guarantee both properties. A password hash supports verification without recovering the original password; it is not a reversible credential store. Encryption can protect a recoverable credential only if its key is separately protected.

Study-note section NSA12

QoS classifies, queues and prioritizes traffic to meet performance objectives such as low delay or limited loss. It can operate across layers and support applications, so it is not exclusively an application-layer service. Installing a new service is an administrative action; email configuration is another action and proxies/agents are components. Distinguish service-management actions from components using a stated taxonomy.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 57 | lines 78-87

Remote Administration
Remote administration is an approach being followed to control either a computer system or a network or an application or all three from a remote location. Simply put, Remote administration refers to any method of controlling a computer from a remote location. A remote location may refer to a computer in the next room or one on the other side of the world. It may also refer to both legal and illegal remote administration. Generally, remote administration is essentially adopted when it is difficult or

Data Communication and Computer Networking module | PDF page 58 | lines 22-32

The following are some of proprietary and open source applications that can be used to achieve this.
• SSH (Secure Shell)
• OpenSSH (OpenBSD Secure Shell)
• Telnet
• rlogin
• rsh
• VNC (Virtual Network Computing)

- FreeNX
- Wireless Remote Administration
- Remote Desktop Connection (RDC)

Question sources

Computer Science MCQ practice collection · Question 591

Question 64 | AM0592

Which of the following is an example of a security incident response action?

A. Regular software updates

B. Password policy enforcement

C. Incident investigation and analysis

D. Network configuration backup

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer C: Incident investigation and analysis

PDF p.30 requires personnel to respond quickly and effectively to security failures and to diagnose and troubleshoot problems. Investigation and analysis is the option that reacts to an incident rather than routine prevention or preservation.

Why each choice is right or wrong

A - Incorrect: Regular updating is a routine patching activity (p.30), rather than investigating an incident.

B - Incorrect: Password-policy enforcement is an ongoing access-security measure, not the incident investigation requested.

C - Correct: Investigation/analysis implements diagnosis and effective response after security failure (p.30).

D - Incorrect: Configuration backup preserves data and is not the investigative response action.

Primary note proof

Study-note section NSA29

Incident response prepares, detects/analyzes, contains, removes the cause, restores service and learns from the event. Investigation is reactive response; routine patching and backup are normally preventive/preparatory operations. Document timestamps, affected systems, evidence, impact, actions, responsible people and recovery results. An incident report may record policy violations, but its scope is broader than that alone.

Study-note section NSA27

Preventive controls restrict harmful actions, detective controls expose them and recovery controls restore service. Account lifecycle, backup procedures, device configuration and traffic analysis can all be security controls under a stated objective. A vulnerability scan checks known weakness patterns, not bandwidth. Test/stage patches, prepare rollback, deploy and verify; testing and installation are both legitimate administrator duties.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 30 | lines 16-18

• Diagnosing and troubleshooting problems on the network and determining the best course of action to take to solve them.

Question sources

Computer Science MCQ practice collection · Question 592

Question 65 | AM0593

Which tool is commonly used for network scanning and host discovery?

A. Wireshark

B. Nmap

C. Snort

D. Nessus

Hint

Match the requested observation to the tool’s actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer B: Nmap

The requested scanning and discovery role directly matches Nmap in NSA23. Wireshark captures/dissects packets, Snort detects suspicious traffic and Nessus assesses vulnerabilities/configurations. These capabilities can complement discovery, but Nmap is the tool explicitly named for the requested host/port/service scan rather than those other primary purposes.

Why each choice is right or wrong

A - Incorrect: Wireshark's identified role is packet capture/dissection rather than active host and port discovery.

B - Correct: Nmap is explicitly described as discovering hosts, ports and services.

C - Incorrect: Snort's identified role is traffic inspection/detection, not the host-discovery scanning tool requested.

D - Incorrect: Nessus assesses vulnerabilities/configuration; Nmap is the note's explicit general host/port discovery tool.

Primary note proof

Study-note section NSA23

> Task Manager shows running processes/resource use; Resource Monitor/Performance Monitor give more detailed counters. Wireshark captures and dissects packets. Nmap discovers hosts/ports/services. Nessus assesses vulnerabilities/configuration. Snort can detect suspicious traffic and alert, and can prevent traffic in suitable inline deployments; it also has sniffing/logging roles. Thus packet-capture capability is not exclusive to one product, although Wireshark is the conventional analyzer choice.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 54 | lines 13-17

> Bandwidth monitoring tools and NetFlow and sFlow
> based traffic analyzers help you stay aware of the activity,
> capacity, and health of your network. They allow you to
> watch traffic as it flows through routers and switches, or
> arrive at and leaves hosts.

Data Communication and Computer Networking module | PDF page 54 | lines 49-63

> • Monitoring a range of server metrics: availability,
> CPU usage, memory usage, disk space, response
> time, and upload/download rates. Monitoring
> CPU temperature and power supply voltages.
> • Monitoring applications. Using deep knowledge
> of common applications and services to monitor
> key server processes, including web servers,
> database servers, and application stacks.

• Automatically alerting you of problems, such as servers or network devices that are overloaded or down, or worrisome trends. Customized alerts that can use multiple methods to contact you - email, SMS text messages, pager, etc.
• Triggering actions in response to alerts, to handle certain classes of problems automatically.

Question sources

Computer Science MCQ practice collection · Question 593

Question 66 | AM0594

A policy is being developed specifically to prevent disclosure of confidential records to unauthorized people. Which listed goal directly matches that objective?

A. Ensuring system availability

B. Protecting sensitive data

C. Increasing network speed

D. Enhancing user experience

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer B: Protecting sensitive data

Security policies can support confidentiality, integrity and availability, with priorities set by organizational objectives. This scenario explicitly prioritizes preventing unauthorized disclosure of confidential records, which is sensitive-data protection. Availability remains a legitimate security goal but addresses continued service rather than disclosure. Network speed and user experience have different primary objectives. The explicit policy objective determines the selection without imposing one universal priority on all policies.

Why each choice is right or wrong

A - Incorrect: Availability concerns continued service rather than the specified disclosure objective.

B - Correct: Protecting sensitive data directly addresses the stated confidentiality goal.

C - Incorrect: Network speed is a performance objective, not the security-policy priority defined in the note.

D - Incorrect: User experience can affect usability but is not the stated universal security-policy goal.

Primary note proof

Study-note section NSA26

A security policy states required behavior, scope, accountable roles and enforcement. Begin with assets/service objectives, assess threats and weaknesses, choose controls, define exceptions/incident procedures, approve/communicate, monitor and periodically review. CIA means confidentiality, integrity and availability; neither sensitive-data protection nor availability alone is the universal primary goal.

Study-note section NSA28

Encryption provides confidentiality with correct key/nonce use; authenticated encryption adds integrity/authenticity. Unspecified encryption alone does not guarantee both properties. A password hash supports verification without recovering the original password; it is not a reversible credential store. Encryption can protect a recoverable credential only if its key is separately protected.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Data Communication and Computer Networking module | PDF page 31 | lines 30-35

Principle 2 (Predictability)
The highest level aim in system administration is to work towards a

predictable system. Predictability has limits. It is the basis of reliability, hence trust and therefore security.

Question sources

Computer Science MCQ practice collection · Question 594

Question 67 | AM0595

Which of the following is an example of a security policy?

A. Setting strong password requirements

B. Monitoring network bandwidth

C. Updating software patches

D. Configuring firewall rules

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer A: Strong password requirements

A states a required behavior: passwords must satisfy specified strength requirements. That matches policy rather than an observation or operational change. Patching and firewall configuration implement controls and can be required by policy, but the options describe those actions without stating the governing requirement. Monitoring bandwidth is measurement rather than a policy statement.

Why each choice is right or wrong

A - Correct: Requiring strong passwords states mandatory behavior and is an explicit security-policy example.

B - Incorrect: Monitoring bandwidth is an operational measurement, not a stated security requirement.

C - Incorrect: Applying patches implements protection; a policy would state the required deadline/scope rather than merely the action.

D - Incorrect: Configuring rules implements policy, whereas the option does not itself state required behavior or governance.

Primary note proof

Study-note section NSA26

A security policy states required behavior, scope, accountable roles and enforcement. Begin with assets/service objectives, assess threats and weaknesses, choose controls, define exceptions/incident procedures, approve/communicate, monitor and periodically review. CIA

means confidentiality, integrity and availability; neither sensitive-data protection nor availability alone is the universal primary goal.

Study-note section NSA26

A policy can require password controls, approved encryption, restricted administrative access, backups and patch deadlines; firewall rules implement part of it. Open unrestricted wireless access conflicts with controlled internal access unless intentionally isolated as a guest service. “Use the system passively” is not a purpose of security policy. Policies coordinate action and reduce risk; they do not guarantee every attack will fail.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make
certain that only authorized users have access to
the network and ensuring that all security
procedures are followed
• Making sure the network personnel can respond
quickly and effectively in the event of a network
operational or security failure.

Data Communication and Computer Networking module | PDF page 31 | lines 17-29

Principle 1 (Policy is the foundation)
System administration begins with a
policy - adecision about what we want
and what should be, in relation to what we
can afford.
Policy speaks of what we wish to
accomplish with the system, and what we
are willing to tolerate of behavior within it.
It must refer to both the component parts and
to the environmentwith which the system
interacts. If we cannot secure predictability,
then we cannot expect
long-term conformance with a policy.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local
network to a single IP address. This address is often used
by the router that connects the computers to the Internet.
The router can be connected to a DSL modem, cable
modem, T1 line, or even a dial-up modem. When other
computers on the Internet attempt to access computers
within the local network, they only see the IP address of
the router. This adds an extra level of security, since the

router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Computer Science MCQ practice collection · Question 595

Question 68 | AM0596

Which option states the most general purpose of access control, covering user permissions on logical resources as well as physical restrictions?

A. Limiting physical access to servers

B. Controlling user access to resources

C. Monitoring network traffic

D. Performing system backups

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer B: Controlling user access to resources

Access control decides which users or other subjects may use protected resources and which actions they may perform. Limiting physical entry to a server is one particular control, but does not express the broader account-and-resource permission function. Traffic monitoring observes activity, and backups preserve recoverable data. The general resource-access description therefore best covers the stated scope.

Why each choice is right or wrong

A - Incorrect: Physical server access restriction is a valid but narrower example.

B - Correct: Controlling user access to resources expresses the general purpose.

C - Incorrect: Monitoring observes activity rather than deciding resource permissions.

D - Incorrect: Backups preserve copies for recovery rather than granting access rights.

Primary note proof

Study-note section NSA17

Create named accounts, assign only needed groups/rights, disable departed users and audit privileged activity. Authentication verifies the account; authorization permits operations. A user right such as remote logon differs from a permission on one file. Group-based administration is easier to review than many hidden individual grants.

Study-note section NSA18

Windows file/folder permissions include read, write, read/execute, modify and full control, plus more granular rights such as delete. Inherited and explicit entries, group membership, deny entries and object scope affect effective access; use the effective-access view for a real account rather than adding labels informally. Network access can be constrained by both share and filesystem permissions.

Study-note section NSA30

Segmentation separates groups of systems and enforces allowed flows with routing/filtering policies; VLAN membership alone does not establish complete security. NAC assesses device/user admission and can reject or quarantine unauthorized/noncompliant devices. Authentication proves an identity, while access rules decide which resources it may use.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 43 | lines 2-10

What is File & Folder Permissions?
Permissions are a method for assigning access rights to specific user accounts and user groups. Through the use of permissions, Windows defines which user accounts and user groups can access which files and folders, and what they can do with them. To put it simply, permissions are the operating system‘s way of telling you what you can or cannot do with a file or folder.

Data Communication and Computer Networking module | PDF page 42 | lines 36-49

All user accounts have specific capabilities, privileges, and rights. When you create a user account, you can grant the user specific capabilities by making the user a member of one or more groups. This gives the user the capabilities of these groups. You then assign additional capabilities by making a user a member of the appropriate groups or withdraw capabilities by removing a user from a group. An important part of an administrator‘s job is being able to determine and set permissions, privileges, and logon rights as necessary. Although you can‘t change a group‘s built-in capabilities, you can change a group‘s default privileges and logon rights. For example, you could revoke network access to a computer by removing agroup‘s right to access the computer from the network.

Question sources

Computer Science MCQ practice collection · Question 596

Question 69 | AM0597

Which option describes a firewall's direct traffic-enforcement role, rather than observation, auditing or confidentiality protection?

A. Monitoring network traffic for security threats

B. Encrypting network communications

C. Blocking unauthorized access to the network

D. Auditing network activity

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer C: Blocking unauthorized access to the network

A firewall enforces traffic policy by permitting authorized flows and blocking disallowed ones. Monitoring and audit records can accompany this enforcement, but observing or recording activity does not itself express the requested permit-or-block action. Encryption protects communication confidentiality and is a separate function, even when a product combines it with firewall features.

Why each choice is right or wrong

A - Incorrect: Monitoring may accompany filtering, but observation is not the requested enforcement action.

B - Incorrect: Encryption protects confidentiality rather than deciding whether a flow is permitted.

C - Correct: Blocking unauthorized access directly enforces the traffic policy.

D - Incorrect: Auditing records or reviews activity rather than directly enforcing a traffic decision.

Primary note proof

Study-note section NSA30

> Use authenticated protected remote administration such as SSH or properly secured management services, with restricted source access and auditing. VPNs provide protected connectivity under their defined security model; they are not packet analyzers. Firewall filtering permits/blocks traffic according to policy; it is not inherently encryption. Losing remote connectivity while changing a management route/firewall is an operational risk to plan for.

Study-note section NSA23

> An IDS detects/alerts; an IPS can block inline. Scanning identifies potential weaknesses rather than proving successful exploitation. A captured packet, open port or alert needs context. Monitoring network usage is not the same as configuring access control or encrypting communications.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

> Network Address Translation (NAT)
> NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Question sources

Computer Science MCQ practice collection · Question 597

Question 70 | AM0598

What is the purpose of vulnerability scanning in network and system administration?

A. Identifying security weaknesses and vulnerabilities

B. Encrypting sensitive data during transmission

C. Monitoring network bandwidth usage

D. Managing system logs

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer A: Identify potential security weaknesses

Vulnerability scanning assesses potential weaknesses and configuration problems, as NSA23 explains. It does not itself prove successful exploitation. Encryption, bandwidth measurement and log management are separate administration functions. Therefore A identifies the scan's purpose while retaining the note's caution that scan findings require contextual verification.

Why each choice is right or wrong

A - Correct: Finding potential security weaknesses and configuration vulnerabilities is the purpose assigned to vulnerability assessment.

B - Incorrect: Encryption protects data confidentiality and is not the act of checking for weaknesses.

C - Incorrect: Bandwidth monitoring measures traffic use rather than testing known vulnerability patterns.

D - Incorrect: Log management stores/organizes records and is distinct from scanning systems for weaknesses.

Primary note proof

Study-note section NSA23

Task Manager shows running processes/resource use; Resource Monitor/Performance Monitor give more detailed counters. Wireshark captures and dissects packets. Nmap discovers hosts/ports/services. Nessus assesses vulnerabilities/configuration. Snort can detect suspicious traffic and alert, and can prevent traffic in suitable inline deployments; it also has sniffing/logging roles. Thus packet-capture capability is not exclusive to one product, although Wireshark is the conventional analyzer choice.

Study-note section NSA23

An IDS detects/alerts; an IPS can block inline. Scanning identifies potential weaknesses rather than proving successful exploitation. A captured packet, open port or alert needs context. Monitoring network usage is not the same as configuring access control or encrypting communications.

Study-note section NSA27

Preventive controls restrict harmful actions, detective controls expose them and recovery controls restore service. Account lifecycle, backup procedures, device configuration and traffic analysis can all be security controls under a stated objective. A vulnerability scan checks known weakness patterns, not bandwidth. Test/stage patches, prepare rollback, deploy and verify; testing and installation are both legitimate administrator duties.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Data Communication and Computer Networking module | PDF page 53 | lines 29-43

In networking, it is typical to think of a system as a layered stack. User software sits at the top of the stack and system applications and services on the next layer down. Beneath the services and applications, you will encounter operating systems and firmware. Theperformance of software elements needs to be monitoredas an application stack. Users will notice performance problems with the software that they use, but those problems rarely arise within that software. All layers of the application stack need to be examined to find the root cause of performance issues. You need to head off problems with real-time statusmonitoring before they occur. Monitoring tools help you spot errors and service failures before they start to impactusers.

Question sources

Computer Science MCQ practice collection · Question 598

Question 71 | AM0599

Which of the following is a common vulnerability in computer systems?

A. Strong password policies

B. Regular software updates

C. Unpatched software vulnerabilities

D. Secure network segmentation

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer C: Unpatched exploitable software

NSA27 explicitly gives unpatched exploitable software as a vulnerability. Strong password policy, software updates and secure segmentation are defensive practices intended to reduce exposure. They can be imperfectly implemented, but as stated they are not the example of an exploitable weakness requested by the question.

Why each choice is right or wrong

A - Incorrect: Strong password policy is intended to reduce credential weaknesses rather than exemplify one.

B - Incorrect: Regular updates address known flaws and are a hardening practice.

C - Correct: Unpatched exploitable software contains a known weakness that an attack can exploit.

D - Incorrect: Secure segmentation restricts exposure and permitted flows rather than constituting the vulnerability example.

Primary note proof

Study-note section NSA27

> Hardening reduces exposure through unnecessary-service removal, supported patches, restricted accounts/permissions and appropriate port filtering. Blocking an unused known port can be hardening; blocking every useful port merely destroys availability. Weak passwords and unpatched exploitable software are vulnerabilities; attacks exploit weaknesses, and risk combines likelihood with impact.

Study-note section NSA30

> Segmentation separates groups of systems and enforces allowed flows with routing/filtering policies; VLAN membership alone does not establish complete security. NAC assesses device/user admission and can reject or quarantine unauthorized/noncompliant devices. Authentication proves an identity, while access rules decide which resources it may use.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 19-33

> Although the specifics of being a system administrator
> may change from platform to platform, there are
> underlying themes that do not. These themes make up the
> philosophy of system administration. The themes are:
> • Automate everything
> • Document everything
> • Communicate as much as possible
> • Know your resources
> • Know your users
> • Know your business
> • Security cannot be an afterthought
> • Plan ahead
> • Expect the unexpected
> • Backup and disaster recovery planning
> • Patching

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

> System Monitoring Software Essentials
> In order to keep your system fit for purpose, your
> monitoring activities need to cover the following
> priorities:
> • Acceptable delivery speeds
> • Constant availability
> • Preventative maintenance
> • Software version monitoring and patching

- Intrusion detection
- Data integrity
- Security monitoring
- Attack mitigation
- Virus prevention and detection

Question sources

Computer Science MCQ practice collection · Question 599

Question 72 | AM0600

What is the purpose of security incident response in network and system administration?

A. Preventing security incidents from occurring

B. Recovering data after a security breach

C. Analyzing network performance

D. Detecting and responding to security incidents

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer D: Detecting and responding to security incidents

PDF p.30 requires responding quickly and effectively to security failure, while p.54 includes intrusion detection and security monitoring. Detection and response therefore cover the requested process more fully than prevention alone or post-breach data recovery alone.

Why each choice is right or wrong

A - Incorrect: Prevention alone omits the explicit response to failures that occur (p.30).

B - Incorrect: Recovery is a narrower possible consequence; the response duty is broader (p.30).

C - Incorrect: Performance analysis addresses operational resources rather than the security-failure response.

D - Correct: Security detection/monitoring (p.54) plus responding to failures (p.30) jointly supports this.

Primary note proof

Study-note section NSA29

Incident response prepares, detects/analyzes, contains, removes the cause, restores service and learns from the event. Investigation is reactive response; routine patching and backup are normally preventive/preparatory operations. Document timestamps, affected systems, evidence, impact, actions, responsible people and recovery results. An incident report may record policy violations, but its scope is broader than that alone.

Study-note section NSA29

DoS harms service availability; DDoS uses distributed sources. Phishing deceives users, brute force tries credentials and an interception attack reads/alters communications. Correlate logs using time and identity/context. Preserve relevant evidence before resetting systems. A suspicious event is not automatically confirmed compromise; record facts and uncertainty.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Question sources

Computer Science MCQ practice collection · Question 600

Question 73 | AM0601

What protection does correctly implemented authenticated encryption provide for network data?

A. Preventing unauthorized access to the network

B. Monitoring network traffic for anomalies

C. Protecting data confidentiality and integrity

D. Performing system backups

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer C: Protecting data confidentiality and integrity

Encryption supplies confidentiality when keys and nonces are used correctly. Authenticated encryption also detects unauthorized alteration through integrity and authenticity protection. This explicit construction therefore supports both properties named together in the selected option. Network admission, traffic-anomaly monitoring and backup recovery are separate controls; none is performed merely by encrypting and authenticating a data payload.

Why each choice is right or wrong

A - Incorrect: Network admission/access control is distinct from encrypting content for confidentiality.

B - Incorrect: Anomaly detection is a monitoring function and does not describe the role of encryption.

C - Correct: Authenticated encryption combines confidentiality with integrity/authenticity protection.

D - Incorrect: Backups recover previous data and are not performed by encryption itself.

Primary note proof

Study-note section NSA28

> Encryption provides confidentiality with correct key/nonce use; authenticated encryption adds integrity/authenticity. Unspecified encryption alone does not guarantee both properties. A password hash supports verification without recovering the original password; it is not a reversible credential store. Encryption can protect a recoverable credential only if its key is separately protected.

Study-note section NSA30

> Segmentation separates groups of systems and enforces allowed flows with routing/filtering policies; VLAN membership alone does not establish complete security. NAC assesses device/user admission and can reject or quarantine unauthorized/noncompliant devices. Authentication proves an identity, while access rules decide which resources it may use.

Study-note section NSA24

> Backups recover previous data after deletion, compromise, corruption, failed upgrades/migrations or hardware loss. Authorization controls current access, a different function. A mirror/replica also copies deletions or corruption and does not replace versioned independent backups. Keep protected copies in separate failure domains, define retention and test restores.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Question sources

Computer Science MCQ practice collection · Question 601

Question 74 | AM0602

Which listed activities can be security controls when implemented for the stated purpose: A recovery, B least-privilege account provisioning, C secure device configuration, D suspicious-traffic detection? Select all that apply.

A. Data backup and recovery procedures

B. User account creation

C. Network device configuration

D. Network traffic analysis

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer A, B, C, D: Data backup and recovery procedures; User account creation; Network device configuration; Network traffic analysis

Security controls include prevention, detection and recovery rather than only one technical mechanism. Backups support recovery, controlled account creation restricts access, secure device configuration reduces exposure, and traffic analysis can detect suspicious behavior. Each listed activity therefore qualifies under its explicit purpose. Simply performing an activity without an objective would not prove effectiveness, but the question supplies the security objective needed to classify it.

Why each choice is right or wrong

A - Correct: Backups and recovery procedures restore service/data after harmful events.

B - Correct: Controlled account creation implements identity lifecycle and access restriction.

C - Correct: Secure device configuration can reduce exposure and enforce permitted network behavior.

D - Correct: Traffic analysis is a detective control when used to identify suspicious behavior.

Primary note proof

Study-note section NSA27

> Preventive controls restrict harmful actions, detective controls expose them and recovery controls restore service. Account lifecycle, backup procedures, device configuration and traffic analysis can all be security controls under a stated objective. A vulnerability scan checks known weakness patterns, not bandwidth. Test/stage patches, prepare rollback, deploy and verify; testing and installation are both legitimate administrator duties.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 6-8

> • Backing up the network software and data
> regularly to protect against the failure of network
> or any of its components

Data Communication and Computer Networking module | PDF page 42 | lines 36-49

> All user accounts have specific capabilities, privileges,
> and rights. When you create a user account, you can grant
> the user specific capabilities by making the user a member
> of one or more groups. This gives the user the capabilities
> of these groups. You then assign additional capabilities by
> making a user a member of the appropriate groups or
> withdraw capabilities by removing a user from a group.
> An important part of an administrator‘s job is being able
> to determine and set permissions, privileges, and logon
> rights as necessary. Although you can‘t change a group‘s
> built-in capabilities, you can change a group‘s default

privileges and logon rights. For example, you could revoke network access to a computer by removing agroup‘s right to access the computer from the network.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Data Communication and Computer Networking module | PDF page 54 | lines 13-17

Bandwidth monitoring tools and NetFlow and sFlow based traffic analyzers help you stay aware of the activity, capacity, and health of your network. They allow you to watch traffic as it flows through routers and switches, or arrive at and leaves hosts.

Question sources

Computer Science MCQ practice collection · Question 602

Question 75 | AM0603

What is the purpose of a security incident report in network and system administration?

A. Documenting security policy violations

B. Sharing threat intelligence with other organizations

C. Investigating network performance issues

D. Identifying system vulnerabilities

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer A: Document security incidents, including policy violations

NSA29 assigns reports the documentation of affected systems, evidence, impact, actions and recovery results, and explicitly includes policy violations within that scope. A therefore states a legitimate report purpose among the choices, although it is not exhaustive. Threat sharing, performance investigation and weakness identification are separate activities that incident findings may later support.

Why each choice is right or wrong

A - Correct: Documenting policy violations is a valid part of incident reporting, although reports also cover impact and response.

B - Incorrect: External threat-intelligence sharing is a separate activity, not the documentation purpose established for this report.

C - Incorrect: Performance investigation is broader troubleshooting and does not specifically define a security incident report.

D - Incorrect: Finding vulnerabilities is assessment; incident reporting documents observed events, evidence and response.

Primary note proof

Study-note section NSA29

> Incident response prepares, detects/analyzes, contains, removes the cause, restores service and learns from the event. Investigation is reactive response; routine patching and backup are normally preventive/preparatory operations. Document timestamps, affected systems, evidence, impact, actions, responsible people and recovery results. An incident report may record policy violations, but its scope is broader than that alone.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

> • Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
> • Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 54 | lines 49-63

> • Monitoring a range of server metrics: availability, CPU usage, memory usage, disk space, response time, and upload/download rates. Monitoring CPU temperature and power supply voltages.
> • Monitoring applications. Using deep knowledge of common applications and services to monitor

key server processes, including web servers, database servers, and application stacks.
• Automatically alerting you of problems, such as servers or network devices that are overloaded or down, or worrisome trends. Customized alerts that can use multiple methods to contact you - email, SMS text messages, pager, etc.
• Triggering actions in response to alerts, to handle certain classes of problems automatically.

Question sources

Computer Science MCQ practice collection · Question 603

Question 76 | AM0604

Which actions can be valid troubleshooting steps when supported by a tested fault hypothesis and an appropriate recovery plan? Select all that apply.

A. Rebooting the system

B. Performing a software update

C. Resetting network configurations

D. Conducting a network scan

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A, B, C, D: Rebooting the system; Performing a software update; Resetting network configurations; Conducting a network scan

Rebooting, updating software, resetting configuration and scanning can each help with an appropriate diagnosed problem. Their value depends on the hypothesis and operational context: an update may address a known bug, a reset may correct damaged settings, and a scan may gather service evidence. None should be performed blindly. The question asks which actions can belong to troubleshooting, not which one should always be tried first.

Why each choice is right or wrong

A - Correct: Rebooting can be a justified troubleshooting action, although it can hide evidence and is not itself diagnosis.

B - Correct: An update can address a diagnosed software defect affecting network behavior.

C - Correct: Resetting incorrect network settings can resolve a configuration fault after preserving needed evidence.

D - Correct: A targeted network scan can gather reachability/service evidence for diagnosis.

Primary note proof

Study-note section NSA08

Define the symptom, scope, time and recent changes; gather the configuration, baseline and logs. Form a testable hypothesis, test the least disruptive explanation, isolate the failing component, apply a targeted fix, verify the user service and document the result. Change one relevant factor at a time when possible. A reboot can hide evidence and is not a diagnosis by itself.

Study-note section NSA08

Use bottom-up checks from physical link, top-down checks from application errors, or divide-and-conquer by testing a middle layer. Divide-and-conquer narrows the working/failing boundary; it is not random trial-and-error. Rebooting, updates, resetting settings and scanning can all be troubleshooting actions in suitable circumstances; use fault evidence to choose among them.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 16-18

• Diagnosing and troubleshooting problems on the network and determining the best course of action to take to solve them.

Data Communication and Computer Networking module | PDF page 53 | lines 29-43

In networking, it is typical to think of a system as a layered stack. User software sits at the top of the stack and system applications and services on the next layer down. Beneath the services and applications, you will encounter operating systems and firmware. Theperformance of software elements needs to be monitoredas an application stack. Users will notice performance problems with the software that they use, but those problems rarely arise within that software. All layers of the application stack need to be examined to find the root cause of performance issues. You need to head off problems with real-time statusmonitoring before they occur. Monitoring tools help you spot errors and service failures before they start to impactusers.

Data Communication and Computer Networking module | PDF page 30 | lines 19-33

Although the specifics of being a system administrator may change from platform to platform, there are underlying themes that do not. These themes make up the philosophy of system administration. The themes are:
• Automate everything
• Document everything

- Communicate as much as possible
- Know your resources
- Know your users
- Know your business
- Security cannot be an afterthought
- Plan ahead
- Expect the unexpected
- Backup and disaster recovery planning
- Patching

Question sources

Computer Science MCQ practice collection · Question 604

Question 77 | AM0605

Which purposes can analysis of existing system and network logs serve? Select all that apply.

A. Identifying potential security breaches

B. Monitoring network performance

C. Configuring firewall rules

D. Encrypting network communications

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A, B: Identifying potential security breaches; Monitoring network performance

Logs can reveal suspicious activity that suggests a security breach and can also expose timing, error or workload patterns related to performance. These are complementary uses of recorded observations. Changing firewall rules may follow the analysis, but it is a separate configuration action. Encryption protects communications in transit or storage rather than emerging from analysis of past records. Both analytical purposes therefore qualify.

Why each choice is right or wrong

A - Correct: Security events in logs can reveal potential breaches and support incident investigation.

B - Correct: Log timing/errors can reveal performance faults and complement measured counters.

C - Incorrect: Rule configuration may follow findings, but is not the act or direct purpose of log analysis.

D - Incorrect: Encryption protects communications; parsing historical records does not itself encrypt traffic.

Primary note proof

Study-note section NSA35

Count the event actually requested, use timestamps/hosts to correlate, and separate absence of matches from failure to read the log. Logs support security and performance analysis, so neither purpose is universally exclusive.

Study-note section NSA22

Measure a baseline, sample over an interval, compare with workload and correlate symptoms before changing hardware. CPU utilization/run queues identify processing pressure; low free memory alone is weak evidence because cache may be reclaimable. Persistent paging with high latency indicates memory pressure. Storage capacity and I/O latency are separate: a disk can be nearly empty but saturated, or nearly full while lightly loaded.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Data Communication and Computer Networking module | PDF page 54 | lines 49-63

• Monitoring a range of server metrics: availability, CPU usage, memory usage, disk space, response time, and upload/download rates. Monitoring CPU temperature and power supply voltages.
• Monitoring applications. Using deep knowledge of common applications and services to monitor key server processes, including web servers, database servers, and application stacks.
• Automatically alerting you of problems, such as servers or network devices that are overloaded or down, or worrisome trends. Customized alerts that can use multiple methods to contact you - email, SMS text messages, pager, etc.

• Triggering actions in response to alerts, to handle certain classes of problems automatically.

Question sources

Computer Science MCQ practice collection · Question 605

Question 78 | AM0606

A client has valid IP configuration. Which listed utility can send ICMP echo requests to a gateway as the next reachability diagnostic?

A. Ping

B. VPN

C. FTP

D. DNS

Hint

Match the requested observation to the tool’s actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer A: Ping

Ping sends ICMP echo requests and checks the returned replies. Testing the gateway can help isolate whether the client can exchange IP traffic with that next-hop device. A VPN provides extended protected connectivity, FTP transfers files and DNS resolves names; none is the requested echo-probe utility. Missing replies need further investigation because filtering or loss can suppress otherwise reachable devices.

Why each choice is right or wrong

A - Correct: Ping generates the requested ICMP echo probes.

B - Incorrect: A VPN provides protected connectivity rather than being an echo-test utility.

C - Incorrect: FTP transfers files rather than issuing the specified reachability probe.

D - Incorrect: DNS resolves names rather than sending ICMP echo requests.

Primary note proof

Study-note section NSA-S04

Ping uses ICMP echo messages to test IP reachability. A reply shows that the addressed host and path support that exchange; no reply alone does not prove the host is disconnected, because filtering or loss can suppress responses. Traceroute instead discovers responding intermediate hops through packet-lifetime expiry; it is a path-discovery diagnostic, not the same question as an end-to-end echo test.

Study-note section NSA10

DNS resolves names; DHCP supplies host configuration. SMTP sends/relays mail, while IMAP/POP retrieve it. FTP is a named file-transfer protocol; HTTP also transfers files, so “transfers files” is not an exclusive FTP description. HTTP/HTTPS serve web resources. SSH provides encrypted remote login; SFTP transfers files over SSH and differs from FTP or FTPS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

Ping (Packet Internet Groper) uses ICMP echo
messages to check the physical and logical
connectivity of machineson a network.

Data Communication and Computer Networking module | PDF page 28 | lines 37-45

The Process/Application Layer Protocols
• Telnet
• File Transfer Protocol (FTP)
• Network File System (NFS).
• Simple Mail Transfer Protocol (SMTP
• POP3 is used to receive mail.
• Simple Network Management Protocol (SNMP)
• Domain Name Service (DNS)
• Dynamic Host Configuration Protocol (DHCP)

Question sources

Computer Science MCQ practice collection · Question 606

Question 79 | AM0607

An administrator is monitoring network capacity and utilization, rather than conducting a vulnerability assessment. Which activity directly measures that objective?

A. Identifying security vulnerabilities

B. Tracking network bandwidth usage

C. Configuring user access controls

D. Performing system backups

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer B: Tracking network bandwidth usage

Capacity monitoring compares observed traffic with the available link rate and follows usage over time. Tracking bandwidth usage therefore measures the specified performance objective. Vulnerability assessment searches for weaknesses, access-control configuration changes permissions, and backups preserve data for recovery. All can be administration activities, but they do not measure the traffic utilization asked for here.

Why each choice is right or wrong

A - Incorrect: Vulnerability identification assesses weaknesses rather than measuring capacity utilization.

B - Correct: Bandwidth-usage tracking measures traffic utilization against available capacity.

C - Incorrect: Configuring access controls changes authorization rather than measuring traffic load.

D - Incorrect: Backups preserve recovery copies rather than observing utilization.

Primary note proof

Study-note section NSA22

> Measure interface bytes/second, errors, drops, packet delay/loss and utilization against link rate. Distinguish capacity (maximum available rate) from observed throughput. Logs can reveal both security incidents and performance faults. Performance counters expose measured events; system calls/APIs and log parsers are ways scripts can collect them.

Study-note section NSA23

> An IDS detects/alerts; an IPS can block inline. Scanning identifies potential weaknesses rather than proving successful exploitation. A captured packet, open port or alert needs context. Monitoring network usage is not the same as configuring access control or encrypting communications.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 29 | lines 44-56

> Scope of Network administration
> The management of a network, usually called network administration, consists of procedures and services that keep the network running properly. An important part of network management entails making sure that the network is available (or up and running as IT professionals say) when employees and managers need it.Other admin activities are:
> • Monitoring the network capacity to ensure that alltransmission requirements can be met.
> • Adding capacity to the network by increasing band

width interconnecting additional modes, or
creating and interconnecting additional networks.

Data Communication and Computer Networking module | PDF page 54 | lines 13-17

Bandwidth monitoring tools and NetFlow and sFlow
based traffic analyzers help you stay aware of the activity,
capacity, and health of your network. They allow you to
watch traffic as it flows through routers and switches, or
arrive at and leaves hosts.

Question sources

Computer Science MCQ practice collection · Question 607

Question 80 | AM0608

Which troubleshooting approach tests a middle layer, then narrows the working/failing boundary upward or downward?

A. Divide and conquer

B. Trial and error

C. Random testing

D. Full system restore

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: Divide and conquer

Divide-and-conquer starts with a test at a middle layer and uses the result to decide which side of the boundary needs further investigation. It therefore narrows the scope systematically. Trial-and-error is a broader description of making attempts and does not specifically name this layer-boundary method. Random testing lacks the defined decision process, and a full restore is a recovery action rather than the approach described.

Why each choice is right or wrong

A - Correct: Divide-and-conquer is explicitly supported and isolates a working/failing boundary by testing a middle layer.

B - Incorrect: Trial-and-error does not specifically identify the middle-layer boundary-isolation approach described.

C - Incorrect: Random testing lacks the testable hypothesis and controlled isolation recommended by NSA08.

D - Incorrect: A full restore is a potentially disruptive recovery action, not the routine diagnostic approach identified in NSA08.

Primary note proof

Study-note section NSA08

> Use bottom-up checks from physical link, top-down checks from application errors, or divide-and-conquer by testing a middle layer. Divide-and-conquer narrows the working/failing boundary; it is not random trial-and-error. Rebooting, updates, resetting settings and scanning can all be troubleshooting actions in suitable circumstances; use fault evidence to choose among them.

Study-note section NSA08

> Define the symptom, scope, time and recent changes; gather the configuration, baseline and logs. Form a testable hypothesis, test the least disruptive explanation, isolate the failing component, apply a targeted fix, verify the user service and document the result. Change one relevant factor at a time when possible. A reboot can hide evidence and is not a diagnosis by itself.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 53 | lines 29-43

> In networking, it is typical to think of a system as a layered stack. User software sits at the top of the stack and system applications and services on the next layer down. Beneath the services and applications, you will encounter operating systems and firmware. Theperformance of software elements needs to be monitoredas an application stack.
> Users will notice performance problems with the software that they use, but those problems rarely arise within that software. All layers of the application stack need to be examined to find the root cause of performance issues. You need to head off problems with real-time statusmonitoring before they occur. Monitoring tools help you spot errors and service failures before they start to impactusers.

Data Communication and Computer Networking module | PDF page 51 | lines 2-10

> monitoring is normally done as the first and last steps of a three-step process:
> Monitoring to identify the nature and scope of the resource shortages that are causing the performance problems.
> The data produced from monitoring is analyzed and a course of action (normally performance tuning

and/or the procurement of additional hardware) is taken to resolve the problem

Question sources

Computer Science MCQ practice collection · Question 608

Question 81 | AM0609

A static network diagram records devices, links and their arrangement for later troubleshooting. What direct purpose does creating this diagram serve?

A. Documenting network configurations

B. Identifying security vulnerabilities

C. Monitoring network performance

D. Configuring network devices

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: Documenting network configurations

A network diagram documents the arrangement of devices and links and may record configuration relationships. That record helps a troubleshooter reason about expected connectivity. An analyst might subsequently infer weaknesses from it, but creating a static diagram does not itself establish vulnerabilities, sample live performance or apply device settings. The question asks for the direct documentation purpose.

Why each choice is right or wrong

A - Correct: Documenting the network arrangement and configuration is the direct purpose.

B - Incorrect: A diagram can inform security analysis, but creating it does not itself establish vulnerabilities.

C - Incorrect: A static diagram does not measure live performance counters or traffic.

D - Incorrect: Drawing the topology does not apply settings to devices.

Primary note proof

Study-note section NSA02

Switching normally forwards frames using MAC addresses within a LAN; routing forwards IP packets between networks. TCP supplies an ordered reliable byte stream, while UDP preserves datagrams without that guarantee. Ports distinguish application endpoints, not physical connectors. Draw switches, links, subnets, gateways, service hosts and dependencies in a network diagram. A topology's shape alone does not guarantee security.

Study-note section NSA01

Use documentation, standardization, least privilege, automation and measured change. Record the current state, intended change, rollback and validation. Schedule maintenance according to service impact and urgency, not merely because a calendar date arrived. Fault management restores failures; performance management measures service behavior; configuration management tracks settings; security management controls access; accounting tracks usage.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 19-33

Although the specifics of being a system administrator may change from platform to platform, there are underlying themes that do not. These themes make up the philosophy of system administration. The themes are:
• Automate everything
• Document everything
• Communicate as much as possible
• Know your resources
• Know your users
• Know your business
• Security cannot be an afterthought
• Plan ahead
• Expect the unexpected
• Backup and disaster recovery planning
• Patching

Data Communication and Computer Networking module | PDF page 22 | lines 45-52

Inter-connectivity: components of a network, including end devices and interconnecting devices, can be connected to each other differently in some fashion. By connectedness we mean either logically, physically or both ways. Network topology refers to the shape of a network, or the network‘s layout. It is the geometric representation of the relationship of all the links and linking devices to one another. There are

Question sources

Computer Science MCQ practice collection · Question 609

Question 82 | AM0610

Which measures can provide a network security control under their ordinary stated purposes? Select all that apply.

A. Intrusion Detection System (IDS)

B. User authentication

C. Data encryption

D. Network traffic analysis

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer A, B, C, D: Intrusion Detection System (IDS); User authentication; Data encryption; Network traffic analysis

An IDS detects suspicious activity and alerts, while traffic analysis can provide additional detective evidence. User authentication establishes identity for subsequent access decisions. Correctly implemented encryption protects data against unauthorized disclosure. These mechanisms address different security needs, so all are examples of controls under the broad question. Their inclusion does not imply that any single mechanism provides complete security by itself.

Why each choice is right or wrong

A - Correct: An IDS supplies detective monitoring and alerts about suspicious activity.

B - Correct: Authentication establishes an identity before access decisions and supports controlled admission.

C - Correct: Appropriate encryption protects transmitted content against unauthorized disclosure.

D - Correct: Traffic analysis can detect suspicious behavior and is explicitly included among security controls.

Primary note proof

Study-note section NSA23

> An IDS detects/alerts; an IPS can block inline. Scanning identifies potential weaknesses rather than proving successful exploitation. A captured packet, open port or alert needs context. Monitoring network usage is not the same as configuring access control or encrypting communications.

Study-note section NSA28

> Encryption provides confidentiality with correct key/nonce use; authenticated encryption adds integrity/authenticity. Unspecified encryption alone does not guarantee both properties. A password hash supports verification without recovering the original password; it is not a reversible credential store. Encryption can protect a recoverable credential only if its key is separately protected.

Study-note section NSA30

Segmentation separates groups of systems and enforces allowed flows with routing/filtering policies; VLAN membership alone does not establish complete security. NAC assesses device/user admission and can reject or quarantine unauthorized/noncompliant devices. Authentication proves an identity, while access rules decide which resources it may use.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 54 | lines 18-30

System Monitoring Software Essentials
In order to keep your system fit for purpose, your monitoring activities need to cover the following priorities:
• Acceptable delivery speeds
• Constant availability
• Preventative maintenance
• Software version monitoring and patching
• Intrusion detection
• Data integrity
• Security monitoring
• Attack mitigation
• Virus prevention and detection

Data Communication and Computer Networking module | PDF page 54 | lines 13-17

Bandwidth monitoring tools and NetFlow and sFlow based traffic analyzers help you stay aware of the activity, capacity, and health of your network. They allow you to watch traffic as it flows through routers and switches, or arrive at and leaves hosts.

Data Communication and Computer Networking module | PDF page 16 | lines 33-42

Presentation Layer
• The communicating devices may be having different platforms. The presentation layer performs translation, encryption and compression of data.
• The presentation layer receives the data from the

application layer adds header which contains information related to encryption and compression and sends it to the session layer.
• So, the main responsibility of the Presentation layer is translation, compression and encryption.

Question sources

Computer Science MCQ practice collection · Question 610

Question 83 | AM0611

What is the direct network-structural purpose of segmentation with enforced intersegment policies? Select the most specific description.

A. Controlling user access to resources

B. Encrypting network communications

C. Isolating network segments for security purposes

D. Monitoring network traffic

Hint

Identify whether the task requires input/output, control flow, code organization, process execution or collection of a specific measurement.

Answer C: Isolating network segments for security purposes

Segmentation separates groups of systems and enforces permitted flows between them. This structural isolation can support access restrictions, but controlling user access is a broader result also achieved through other mechanisms. The most specific description is therefore isolating network segments for security. Encryption and monitoring are distinct controls and do not automatically follow from dividing the network into segments.

Why each choice is right or wrong

A - Incorrect: Access control may be an outcome, but this broad description does not name segmentation’s direct structural purpose.

B - Incorrect: Segmentation restricts connectivity but does not inherently encrypt the communications it permits.

C - Correct: Segmentation isolates system groups into network segments and enforces intersegment flows.

D - Incorrect: Traffic monitoring observes activity; it is distinct from establishing and enforcing segment boundaries.

Primary note proof

Study-note section NSA30

Segmentation separates groups of systems and enforces allowed flows with routing/filtering policies; VLAN membership alone does not establish complete security. NAC assesses device/user admission and can reject or quarantine unauthorized/noncompliant devices. Authentication proves an identity, while access rules decide which resources it may use.

Study-note section NSA30

Use authenticated protected remote administration such as SSH or properly secured management services, with restricted source access and auditing. VPNs provide protected connectivity under their defined security model; they are not packet analyzers. Firewall filtering permits/blocks traffic according to policy; it is not inherently encryption. Losing remote connectivity while changing a management route/firewall is an operational risk to plan for.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

• Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 22 | lines 45-52

Inter-connectivity: components of a network, including end devices and interconnecting devices, can be connected to each other differently in some fashion. By connectedness we mean either logically, physically or both ways. Network topology refers to the shape of a network, or the network‘s layout. It is the geometric representation of the relationship of all the links and linking devices to one another. There are

Question sources

Computer Science MCQ practice collection · Question 611

Question 84 | AM0612

What is the role of a Network Access Control (NAC) system in network security?

A. Managing user account credentials

B. Monitoring network bandwidth

C. Detecting and blocking unauthorized devices

D. Auditing network activity

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer C: Assess admission and reject unauthorized devices

NSA30 defines Network Access Control as assessing device/user admission and rejecting or quarantining unauthorized or noncompliant devices. C matches that admission function. Credential management, bandwidth monitoring and general activity auditing can support network operations, but they do not state the specific NAC enforcement role.

Why each choice is right or wrong

A - Incorrect: Managing account credentials is identity administration, not the complete device-admission role defined for NAC.

B - Incorrect: Bandwidth monitoring measures network use rather than deciding whether a device may join.

C - Correct: NAC can detect unauthorized/noncompliant devices during admission and reject or quarantine them.

D - Incorrect: Auditing records activity; NAC’s distinguishing role is admission assessment and enforcement.

Primary note proof

Study-note section NSA30

> Segmentation separates groups of systems and enforces allowed flows with routing/filtering policies; VLAN membership alone does not establish complete security. NAC assesses device/user admission and can reject or quarantine unauthorized/noncompliant devices. Authentication proves an identity, while access rules decide which resources it may use.

Study-note section NSA22

> Measure interface bytes/second, errors, drops, packet delay/loss and utilization against link rate. Distinguish capacity (maximum available rate) from observed throughput. Logs can reveal both security incidents and performance faults. Performance counters expose measured events; system calls/APIs and log parsers are ways scripts can collect them.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

> • Putting security procedures in place to make certain that only authorized users have access to the network and ensuring that all security procedures are followed
> • Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Data Communication and Computer Networking module | PDF page 34 | lines 7-14

> Domain Controllers
> A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing end devices to access shared domain resources. It authenticates users, stores user account information and enforces security policy for a domain. It is most commonly implemented in Microsoft

Question sources

Computer Science MCQ practice collection · Question 612

Question 85 | AM0613

In the note’s bottom-up connectivity procedure, which listed action belongs to the initial physical-link check?

A. Checking physical cable connections

B. Updating antivirus software

C. Configuring firewall rules

D. Performing system backups

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A: Checking physical cable connections

A bottom-up procedure begins with power, cable or connector condition and link state before examining interfaces, addressing, routes or application policy. Checking physical cable connections directly fits that initial stage. Firewall configuration may become relevant later when evidence identifies filtering. Antivirus updates and backups serve maintenance or recovery purposes rather than the first physical-link inspection specified in this question.

Why each choice is right or wrong

A - Correct: Cable/connector and link-state checks directly diagnose physical connectivity problems.

B - Incorrect: Updating antivirus is maintenance rather than a direct connectivity-isolation technique supported by this stem.

C - Incorrect: Firewall rules may require later inspection, but are not the initial physical-link check.

D - Incorrect: Backups support recovery but do not directly test or correct the network-connectivity path.

Primary note proof

Study-note section NSA09

Check power, cable/connector and link state, then NIC/driver state, VLAN membership, address/prefix, local gateway, route, DNS and finally application port/authentication. A recognized NIC makes a missing driver less likely, not proof of a working physical link. Ethernet commonly uses RJ45 connectors; an RJ11 telephone jack is not the expected Ethernet connection.

Study-note section NSA08

Use bottom-up checks from physical link, top-down checks from application errors, or divide-and-conquer by testing a middle layer. Divide-and-conquer narrows the working/failing boundary; it is not random trial-and-error. Rebooting, updates, resetting settings and scanning can all be troubleshooting actions in suitable circumstances; use fault evidence to choose among them.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 16-18

• Diagnosing and troubleshooting problems on the network and determining the best course of action to take to solve them.

Data Communication and Computer Networking module | PDF page 48 | lines 29-40

Network Address Translation (NAT)
NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Data Communication and Computer Networking module | PDF page 22 | lines 45-52

Inter-connectivity: components of a network, including end devices and interconnecting devices, can be connected to each other differently in some fashion. By connectedness we mean either logically, physically or both ways. Network topology refers to the shape of a network, or the network‘s layout. It is the geometric representation of the relationship of all the links and linking devices to one another. There are

Question sources

Computer Science MCQ practice collection · Question 613

Question 86 | AM0614

Which of the following scripting languages is commonly used for system administration tasks?

A. Java

B. C++

C. Python

D. HTML

Hint

Identify whether the task requires input/output, control flow, code organization, process execution or collection of a specific measurement.

Answer C: Python

NSA31 explicitly names Python among common system-administration scripting choices, along with shells and PowerShell. HTML is markup. Java and C++ are programming languages but are not the common scripting choice identified among these options. The answer concerns ordinary administration automation, not whether those languages could ever perform administrative work.

Why each choice is right or wrong

A - Incorrect: Java can implement programs, but it is not the common administration scripting choice identified in NSA31.

B - Incorrect: C++ is a compiled programming language rather than the listed common administration scripting choice.

C - Correct: Python is explicitly identified as a common language for administrative scripts.

D - Incorrect: HTML is markup and does not provide the administrative scripting control flow requested.

Primary note proof

Study-note section NSA31

> Scripts automate repeatable administration; they are not inherently faster than compiled programs or automatically secure. Python, shells and PowerShell are common choices; HTML is markup. Define inputs and outputs, use variables for state, if/elif/else for decisions, loops for repeated work and functions for reusable operations. Python indentation defines blocks; == compares while = assigns.

Study-note section NSA-S01

Least privilege limits an account or process to the rights its task needs. Agile development instead organizes frequent delivery and adaptation of software. Object-oriented programming organizes software around objects with state and behavior. Cloud computing supplies on-demand access to a shared pool of configurable computing resources. A development approach or hosting model does not itself define an access-rights principle.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 61 | lines 26-36

What is Unix/Linux?
The Unix OS is a set of programs that act as a link between the computer and the user. The computer program that allocates the system resources and coordinates all the details of the computer‘s internals is called the operating system or the kernel. Users communicate with the kernel through a program known as the shell. The shell is a command line interpreter; it translates commands entered by the user and converts them into a language that is understood by the kernel.

Question sources

Computer Science MCQ practice collection · Question 614

Question 87 | AM0615

What is the primary advantage of using scripts for system administration tasks?

A. Faster execution compared to compiled programs

B. Ability to automate repetitive tasks

C. Greater control over system resources

D. Enhanced security and encryption features

Hint

Identify whether the task requires input/output, control flow, code organization, process execution or collection of a specific measurement.

Answer B: Automate repetitive work

NSA31 identifies repeatable automation as the reason to use administration scripts. Their value is consistent execution of recurring tasks, not guaranteed speed relative to compiled code, stronger encryption or inherently greater resource control. Those properties depend on implementation and environment rather than following from the use of a script.

Why each choice is right or wrong

A - Incorrect: Scripts are not inherently faster than compiled programs; the note explicitly rejects that universal claim.

B - Correct: Automation of repetitive administrative work is the primary script benefit given in NSA31.

C - Incorrect: Greater resource control is not an inherent consequence of scripting rather than another implementation method.

D - Incorrect: Scripts are not automatically secure and do not inherently add encryption features.

Primary note proof

Study-note section NSA31

> Scripts automate repeatable administration; they are not inherently faster than compiled programs or automatically secure. Python, shells and PowerShell are common choices; HTML is markup. Define inputs and outputs, use variables for state, if/elif/else for decisions, loops for repeated work and functions for reusable operations. Python indentation defines blocks; == compares while = assigns.

Study-note section NSA31

> Make reruns predictable: compute the desired state, compare with current state and change only what differs. Validate a small dry run before mutation. Avoid requiring privilege for read-only reporting. A good script reports failures and has a meaningful exit status rather than printing success unconditionally.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 19-33

> Although the specifics of being a system administrator
> may change from platform to platform, there are
> underlying themes that do not. These themes make up the
> philosophy of system administration. The themes are:
> • Automate everything
> • Document everything
> • Communicate as much as possible
> • Know your resources
> • Know your users
> • Know your business
> • Security cannot be an afterthought
> • Plan ahead
> • Expect the unexpected
> • Backup and disaster recovery planning
> • Patching

Data Communication and Computer Networking module | PDF page 61 | lines 26-36

What is Unix/Linux?
The Unix OS is a set of programs that act as a link between the computer and the user. The computer program that allocates the system resources and coordinates all the details of the computer‘s internals is called the operating system or the kernel. Users communicate with the kernel through a program known as the shell. The shell is a command line interpreter; it translates commands entered by the user and converts them into a language that is understood by the kernel.

Question sources

Computer Science MCQ practice collection · Question 615

Question 88 | AM0616

In Python, which listed module provides an API for launching child programs and collecting their results?

A. echo

B. ifconfig

C. grep

D. subprocess

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: subprocess

Python’s subprocess module launches child programs and provides interfaces for collecting output, checking status and limiting runtime. It is a language module rather than a universal shell command. Echo prints values, ifconfig handles interface configuration, and grep searches text. Naming the language and asking for the module makes the intended process-execution abstraction precise without confusing it with one particular program a script might launch.

Why each choice is right or wrong

A - Incorrect: Echo prints values and is not a general child-process execution abstraction.

B - Incorrect: Ifconfig reports/configures network interfaces rather than generally launching arbitrary programs.

C - Incorrect: Grep searches text and is not the general program-execution mechanism requested.

D - Correct: The Python subprocess module launches child programs and returns their results.

Primary note proof

Study-note section NSA32

Python subprocess is a module, not a universal shell command. run launches a child program and returns its result; capture_output collects stdout/stderr, text=True decodes text, timeout bounds waiting and check=True raises for nonzero exit. Pass an argument list to avoid accidental shell interpretation; quote handling differs from composing a shell string.

Study-note section NSA32

Echo prints, grep searches text and ipconfig/ifconfig reports/configures networking; none is the general Python child-process abstraction. Specify the scripting language before selecting subprocess for process execution.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 61 | lines 26-36

What is Unix/Linux?
The Unix OS is a set of programs that act as a link between the computer and the user. The computer program that allocates the system resources and coordinates all the details of the computer‘s internals is called the operating system or the kernel. Users communicate with the kernel through a program known as the shell. The shell is a command line interpreter; it translates commands entered by the user and converts them into a language that is understood by the kernel.

Data Communication and Computer Networking module | PDF page 65 | lines 39-47

Network configuration commands
The ip Command
The distribution-specific scripts and graphical tools are front-ends to ip (or ifconfig and route on older systems) to display and configure the kernel‘s networking configuration. The ip command is used for assigning IP addresses to interfaces, for setting up routes to the Internet and to other networks, for displaying TCP/IP

Question sources

Computer Science MCQ practice collection · Question 616

Question 89 | AM0617

Which scripting feature is useful for handling errors and exceptions in system administration scripts?

A. Looping constructs

B. Conditional statements

C. Exception handling

D. Function definitions

Hint

Identify whether the task requires input/output, control flow, code organization, process execution or collection of a specific measurement.

Answer C: Exception handling

The NSA34 example uses try with specific exception handlers to report expected read failures while exposing unexpected programming errors. Exception handling is therefore the language feature directly intended for handling errors and exceptions. Loops repeat work, conditions choose branches and functions package reusable operations; none alone supplies exception interception.

Why each choice is right or wrong

A - Incorrect: Loops repeat operations and do not themselves intercept raised exceptions.

B - Incorrect: Conditionals choose branches from ordinary conditions but do not replace exception handlers.

C - Correct: Exception handling catches specified failures and controls reporting or recovery when exceptions occur.

D - Incorrect: Functions organize reusable work; they still require appropriate error/exception handling inside or around calls.

Primary note proof

Study-note section NSA-S05

> Exception handling transfers control from a failing operation to a matching handler. A try block contains the attempted work; an except clause handles specified raised exceptions. A loop repeats operations, a conditional chooses an ordinary branch, and a function packages reusable work; these constructs do not by themselves intercept exceptions.

Study-note section NSA31

> Scripts automate repeatable administration; they are not inherently faster than compiled programs or automatically secure. Python, shells and PowerShell are common choices; HTML is markup. Define inputs and outputs, use variables for state, if/elif/else for decisions, loops for repeated work and functions for reusable operations. Python indentation defines blocks; == compares while = assigns.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 61 | lines 26-36

> What is Unix/Linux?
> The Unix OS is a set of programs that act as a link between the computer and the user. The computer program that allocates the system resources and coordinates all the details of the computer‘s internals is called the operating system or the kernel. Users communicate with the kernel through a program known as the shell. The shell is a command line interpreter; it translates commands entered by the user and converts them into a language that is understood by the kernel.

Question sources

Computer Science MCQ practice collection · Question 617

Question 90 | AM0618

Which concept directly reads configuration bytes from a file or writes updated content back to it, rather than interpreting or holding values?

A. File input/output

B. Regular expressions

C. String manipulation

D. Variable assignment

Hint

Identify whether the task requires input/output, control flow, code organization, process execution or collection of a specific measurement.

Answer A: File input/output

File input/output obtains configuration content from storage and persists revised content. Regular expressions and string operations can interpret or construct that content after it has been read, while variables hold values during processing. All can assist a configuration script, but only file I/O directly crosses the file-storage boundary asked about. Structured formats should still be parsed with their appropriate parsers.

Why each choice is right or wrong

A - Correct: File I/O obtains and persists the configuration content being manipulated.

B - Incorrect: Regex interprets patterns in content rather than directly reading or writing file storage.

C - Incorrect: String manipulation processes text rather than directly transferring it to or from a file.

D - Incorrect: Variable assignment holds values in program state rather than performing file I/O.

Primary note proof

Study-note section NSA33

> File I/O obtains/persists configuration; string operations parse values; regex can recognize patterns. File I/O, string operations and regex can all help manipulate configuration; choose according to the task. Use the format's parser for structured JSON/INI rather than blindly replacing every matching substring. Open text with an explicit encoding and use with so files close even when processing fails.

Study-note section NSA31

> Scripts automate repeatable administration; they are not inherently faster than compiled programs or automatically secure. Python, shells and PowerShell are common choices; HTML is markup. Define inputs and outputs, use variables for state, if/elif/else for decisions, loops for repeated work and functions for reusable operations. Python indentation defines blocks; == compares while = assigns.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 65 | lines 39-47

> Network configuration commands
> The ip Command
> The distribution-specific scripts and graphical tools
> are front-ends to ip (or ifconfig and route on older
> systems) to display and configure the kernel‘s
> networking configuration. The ip command is used for
> assigning IP addresses to interfaces, for setting up routes
> to the Internet and to other networks, for displaying
> TCP/IP

Data Communication and Computer Networking module | PDF page 64 | lines 28-31

> /var: Storage for all variable and temporary files
> created by users, such as log files, temporary files
> downloaded from the Internet, or to keep an image of a
> CD before burning it.

Question sources

Computer Science MCQ practice collection · Question 618

Question 91 | AM0619

Which scripting technique recognizes textual patterns and extracts matching fields or events from individual system-log lines?

A. Database integration

B. File compression

C. Log rotation

D. Regular expression matching

Hint

Identify whether the task requires input/output, control flow, code organization, process execution or collection of a specific measurement.

Answer D: Regular expression matching

Regular expressions describe text patterns and can capture fields from matching log lines. A script can then count events, correlate entries or report anomalies. Database integration supplies storage or query infrastructure, compression reduces data size, and rotation manages log segments and retention. Those may support an overall monitoring system, but they do not themselves perform the specific textual matching operation requested.

Why each choice is right or wrong

A - Incorrect: Database integration stores or queries information rather than specifying the requested text pattern.

B - Incorrect: Compression reduces data size rather than extracting matching fields.

C - Incorrect: Rotation manages file size and historical segments, not textual matching.

D - Correct: Regular expressions match patterns and capture requested fields or events.

Primary note proof

Study-note section NSA35

> Regex recognizes textual patterns; it does not encrypt, compress or rotate logs. search finds a match anywhere, while fullmatch requires the entire string to fit. Use raw Python strings for backslash-heavy patterns, capture only the needed fields and treat unmatched/malformed lines explicitly. Log rotation bounds file size and preserves historical segments; it is complementary to parsing.

Study-note section NSA35

> Count the event actually requested, use timestamps/hosts to correlate, and separate absence of matches from failure to read the log. Logs support security and performance analysis, so neither purpose is universally exclusive.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 64 | lines 14-17

/proc: Virtual file system containing system resources information. You can type man proc command on terminal to see more information about the meaning of the files in proc.

Data Communication and Computer Networking module | PDF page 54 | lines 49-63

• Monitoring a range of server metrics: availability, CPU usage, memory usage, disk space, response time, and upload/download rates. Monitoring CPU temperature and power supply voltages.
• Monitoring applications. Using deep knowledge of common applications and services to monitor key server processes, including web servers, database servers, and application stacks.
• Automatically alerting you of problems, such as servers or network devices that are overloaded or down, or worrisome trends. Customized alerts that can use multiple methods to contact you - email, SMS text messages, pager, etc.
• Triggering actions in response to alerts, to handle certain classes of problems automatically.

Data Communication and Computer Networking module | PDF page 64 | lines 28-31

/var: Storage for all variable and temporary files created by users, such as log files, temporary files downloaded from the Internet, or to keep an image of a CD before burning it.

Question sources

Computer Science MCQ practice collection · Question 619

Question 92 | AM0620

Which scripting language feature allows passing command-line arguments to a script?

A. Functions

B. Modules

C. Classes

D. Command-line parsing

Hint

Match the requested observation to the tool’s actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer D: Command-line parsing

NSA34 identifies command-line parsing as the mechanism for interpreting invocation arguments as named, typed inputs and options. The example uses argparse. Functions, modules and classes can organize a parser's implementation, but they do not by themselves define argument interpretation or validation; D states the requested feature directly.

Why each choice is right or wrong

A - Incorrect: Functions organize callable work but do not inherently parse invocation arguments.

B - Incorrect: Modules organize code; a parser module still needs command-line parsing behavior to interpret inputs.

C - Incorrect: Classes organize state/behavior and do not themselves define command-line argument processing.

D - Correct: Command-line parsing interprets the arguments and options supplied when invoking a script.

Primary note proof

Study-note section NSA34

> Command-line parsing converts user inputs into named, typed values and displays usage. In Python argparse, positional arguments supply required inputs and flags enable options. Validate ranges and paths before work; do not let unchecked input become executable shell text.

Study-note section NSA-S05

> A module groups definitions and statements that can be imported. A class bundles data with functionality for its objects. These organize a program, while command-line parsing interprets the arguments and flags supplied at invocation. Their implementation can use functions or classes, but organization alone does not parse arguments.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 61 | lines 26-36

> What is Unix/Linux?
> The Unix OS is a set of programs that act as a link between the computer and the user. The computer program that allocates the system resources and coordinates all the details of the computer‘s internals is called the operating system or the kernel. Users communicate with the kernel through a program known as the shell. The shell is a command line interpreter; it translates commands entered by the user and converts them into a language that is understood by the kernel.

Question sources

Computer Science MCQ practice collection · Question 620

Question 93 | AM0621

Which scripting technique is commonly used for automating system backup and restore tasks?

A. File compression

B. Version control

C. Scheduling

D. Event logging

Hint

Identify whether the task requires input/output, control flow, code organization, process execution or collection of a specific measurement.

Answer C: Scheduling

Automating recurring backup/restore work requires choosing when the operation runs. NSA37 assigns this to schedulers such as cron/systemd timers or Windows Task Scheduler. Compression packages data, version control tracks script changes and logging records outcomes. Those can support a backup process but do not themselves trigger the scheduled task.

Why each choice is right or wrong

A - Incorrect: Compression packages data but does not determine when a backup or restore operation executes.

B - Incorrect: Version control tracks changes in scripts and does not replace scheduling or data backups.

C - Correct: Scheduling triggers recurring work at configured times through the platform's scheduler.

D - Incorrect: Event logging records execution/results rather than initiating the recurring operation.

Primary note proof

Study-note section NSA37

> Schedule recurring work using cron/systemd timers on suitable Unix systems or Task Scheduler on Windows. A user crontab uses minute,hour,day-of-month,month,day-of-week then command. Use absolute paths, known environment, protected inputs, logs, bounded runtime and a lock when overlap is unsafe. Do not assume an interactive PATH, current directory or stored credentials exist in a scheduled job.

Study-note section NSA37

Compression packages data; scheduling chooses when the operation runs. Test exit status and the archive contents, then restore a sample into an isolated destination. A successful command alone does not prove a usable backup. Version control of scripts helps review but does not replace data backup.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 6-8

• Backing up the network software and data
regularly to protect against the failure of network
or any of its components

Data Communication and Computer Networking module | PDF page 30 | lines 19-33

Although the specifics of being a system administrator
may change from platform to platform, there are
underlying themes that do not. These themes make up the
philosophy of system administration. The themes are:
• Automate everything
• Document everything
• Communicate as much as possible
• Know your resources
• Know your users
• Know your business
• Security cannot be an afterthought
• Plan ahead
• Expect the unexpected
• Backup and disaster recovery planning
• Patching

Question sources

Computer Science MCQ practice collection · Question 621

Question 94 | AM0622

A script must recover a stored service credential to authenticate later. With the decryption key protected separately, which listed mechanism cryptographically protects that recoverable credential at rest?

A. Environment variables

B. Encryption algorithms

C. Hashing functions

D. Configuration files

Hint

Identify whether the task requires input/output, control flow, code organization, process execution or collection of a specific measurement.

Answer B: Encryption algorithms

The script needs the actual credential for later authentication, so a one-way password hash cannot meet the recoverability requirement. Encryption can protect the stored credential while allowing authorized decryption, provided the key is separately protected. Environment variables and configuration files describe storage or delivery choices and are not automatically encrypted. The explicit use case therefore identifies encryption without treating it as sufficient when its key is exposed.

Why each choice is right or wrong

A - Incorrect: Environment variables deliver or hold values but do not by themselves encrypt stored credentials.

B - Correct: Encryption protects a recoverable credential when its key is separately protected.

C - Incorrect: A one-way hash supports verification but cannot recover the service credential.

D - Incorrect: A configuration file is a storage choice and is not automatically cryptographically protected.

Primary note proof

Study-note section NSA28

> Encryption provides confidentiality with correct key/nonce use; authenticated encryption adds integrity/authenticity. Unspecified encryption alone does not guarantee both properties. A password hash supports verification without recovering the original password; it is not a reversible credential store. Encryption can protect a recoverable credential only if its key is separately protected.

Study-note section NSA28

> Keep reusable secrets out of source code and routine logs; obtain them from an appropriately protected credential service or restricted runtime source. Environment variables and configuration files are transport/storage choices, not automatic encryption. A script that must authenticate to another service often needs the actual credential/token, so replacing it with a one-way hash will not work. State whether the question is about password verification or recoverable service credentials.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 30 | lines 9-15

> • Putting security procedures in place to make
> certain that only authorized users have access to
> the network and ensuring that all security
> procedures are followed

• Making sure the network personnel can respond quickly and effectively in the event of a network operational or security failure.

Question sources

Computer Science MCQ practice collection · Question 622

Question 95 | AM0623

Which techniques can collect CPU or memory measurements when the relevant logs or OS interfaces expose those metrics? Select all that apply.

A. Log parsing

B. System calls

C. Signal handling

D. Performance counters

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A, B, D: Log parsing; System calls; Performance counters

Resource measurements can be recorded in logs, exposed through operating-system APIs or published as performance counters. Scripts may use any of those interfaces when the requested metrics are available. Signal handling instead reacts to process notifications and is not itself a CPU or memory measurement interface. The multiple-selection instruction preserves the complementary collection techniques without claiming one universal platform-independent API.

Why each choice is right or wrong

A - Correct: Parsing logs can collect recorded resource metrics when suitable measurements are present.

B - Correct: OS system calls/APIs can expose resource measurements used by monitoring scripts.

C - Incorrect: Signal handling manages process notifications; it is not the measurement interface for CPU/memory utilization.

D - Correct: Performance counters directly expose measured resource events and utilization-related values.

Primary note proof

Study-note section NSA36

/proc/meminfo exposes MemAvailable, an estimate of memory available without swapping; MemFree alone excludes reclaimable memory. Windows Performance Counters and OS APIs expose analogous measurements through different interfaces. System calls, counters and log

parsing can all contribute; selecting one as the only monitoring technique is unjustified without a platform/API.

Study-note section NSA-S05

A signal handler responds when a process receives a specified asynchronous event notification. Handling such a notification is distinct from reading CPU or memory measurements through an OS interface, a performance counter or a log that actually records the metric.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 50 | lines 32-43

Before you can monitor resources, you first have to know what resources there are to monitor. All systems have the following resources available:
• CPU power
• Bandwidth
• Memory
• Storage
System Performance Monitoring
System performance monitoring is normally done in response to a performance problem. Either the system is running too slowly, or programs (and sometimes even the entire system) fail to run at all. In either case, performance

Data Communication and Computer Networking module | PDF page 47 | lines 2-5

registry. The kernel, device drivers, services, Security Accounts Manager, and user interface can all use the registry. The registry also allows access to counters for profiling system performance.

Data Communication and Computer Networking module | PDF page 64 | lines 14-17

/proc: Virtual file system containing system resources information. You can type man proc command on terminal to see more information about the meaning of the files in proc.

Question sources

Computer Science MCQ practice collection · Question 623

Question 96 | CS0188

Suppose you are a network administrator and want to determine the path between two connections, which often goes through multiple routers. Which command would you use?

A. ping

B. nslookup

C. traceroute

D. All of the above

Hint

Match the requested observation to the tool's actual output; distinguish configuration, name lookup, reachability and hop discovery.

Answer C: traceroute

Traceroute discovers responding hops toward a destination by causing packet-lifetime expiry at successive distances. It is therefore the appropriate command for investigating a multi-router path. Ping checks an end-to-end echo exchange and nslookup inspects DNS resolution, which do not supply the requested hop sequence. Some intermediate devices may not reply, so the displayed trace is evidence from responding hops rather than a guarantee that every router is visible.

Why each choice is right or wrong

A - Incorrect: Ping checks end-to-end reachability, not the requested hop sequence.

B - Incorrect: Nslookup queries DNS information, not intermediate router hops.

C - Correct: Traceroute discovers responding intermediate hops along the path.

D - Incorrect: The other commands do not all perform route-hop discovery.

Primary note proof

Study-note section NSA-S04

> Ping uses ICMP echo messages to test IP reachability. A reply shows that the addressed host and path support that exchange; no reply alone does not prove the host is disconnected, because filtering or loss can suppress responses. Traceroute instead discovers responding intermediate hops through packet-lifetime expiry; it is a path-discovery diagnostic, not the same question as an end-to-end echo test.

Study-note section NSA07

> netstat displays connections/endpoints/protocols and TCP states; netstat -ano displays numeric addresses/ports and PIDs. Use the exact command name netstat rather than netstart. ping probes IP reachability; traceroute/tracert reveals responding hops using TTL/hop-limit expiry. ICMP filtering can prevent replies without proving the service is down. nslookup inspects DNS.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 27 | lines 26-28

> Ping (Packet Internet Groper) uses ICMP echo messages to check the physical and logical connectivity of machineson a network.

Data Communication and Computer Networking module | PDF page 27 | lines 29-31

> Traceroute Using ICMP timeouts, Traceroute is used to discover the path a packet takes as it traverses an Internetwork.

Question sources

Computer Science Exit Exam practice collection · Question 188

Question 97 | CS0189

Which statements correctly describe IPv4 loopback? In D, 127.0.0.1 means the conventional example rather than the entire reserved range. Select all that apply.

A. It helps to refer to the host itself

B. It allows programs to access network protocols for local services

C. It is an external pseudo address

D. It is denoted by the IP address: 127.0.0.1

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer A, B, D: It helps to refer to the host itself; It allows programs to access network protocols for local services; It is denoted by the IP address: 127.0.0.1

Loopback lets a host address its own protocol stack and reach local services without an external link. The conventional IPv4 address is 127.0.0.1, within the broader reserved 127/8 block. It is therefore local self-reference rather than an external address. The example wording permits all three true descriptions without incorrectly restricting the entire loopback range to a single address.

Why each choice is right or wrong

A - Correct: Loopback refers to the host itself rather than a remote device.

B - Correct: Programs can reach local services through network protocols using loopback.

C - Incorrect: Loopback is local and does not require an external network link.

D - Correct: 127.0.0.1 is the conventional IPv4 loopback address, although the reserved block is broader.

Primary note proof

Study-note section NSA03

127.0.0.1 conventionally names the local IPv4 loopback interface; 127/8 is reserved for loopback. Loopback tests local protocol processing, not cable, switch or remote reachability. Programs can use it for local services. Several loopback descriptions or several 127/8 addresses may be valid; compare each with the stated role.

Module passages - related reading

These source passages provide context; the primary note proof is identified separately above.

Data Communication and Computer Networking module | PDF page 65 | lines 31-38

/etc/hosts
The /etc/hosts file always contains the localhost IP
address, 127.0.0.1, which is
usedfor interprocess communication.
Never remove this line! Sometimes contains
addresses of additional hosts, whichcan be contacted
without using an external naming service such as
DNS (the Domain Name Server).

Question sources

Computer Science Exit Exam practice collection · Question 189

Question 98 | NS0296

Which listed item is a traffic-prioritization mechanism that can operate across layers, rather than an application mediator or service installation/configuration activity?

A. Proxies and agents

B. Installing a new service

C. E-mail configuration

D. Quality of service

Hint

Identify the required operational function, then compare its scope, inputs and constraints with the cited note definitions.

Answer D: Quality of service

Quality of service classifies, queues and prioritizes traffic to meet performance objectives such as low delay or limited loss. It can span layers while supporting applications. Proxies and agents are mediating components, and installing a service or configuring email are administrative activities. The revised question uses those explicit functional categories, so it does not require an unsupported taxonomy that labels every item an application-layer service.

Why each choice is right or wrong

A - Incorrect: Proxies and agents mediate requests rather than naming the traffic-prioritization mechanism.

B - Incorrect: Installing a service is an administrative activity.

C - Incorrect: Email configuration is an administrative activity.

D - Correct: QoS classifies and prioritizes traffic and can operate across layers.

Primary note proof

Study-note section NSA12

> A proxy acts on behalf of a client or backend service and can cache, filter or mediate application requests. A default IP gateway is a next-hop router; an application gateway may translate protocols. It need not be a modem/router combination. These terms describe functions that can coexist on one machine.

Study-note section NSA12

> QoS classifies, queues and prioritizes traffic to meet performance objectives such as low delay or limited loss. It can operate across layers and support applications, so it is not exclusively an application-layer service. Installing a new service is an administrative action; email configuration is another action and proxies/agents are components. Distinguish service-management actions from components using a stated taxonomy.

Question sources

Computer Science Exit Exam · 2018 · Question 13

Question 99 | NS0313

A data-center volume has exactly two equal disks and must retain service after either disk fails. One disk’s usable capacity is sufficient. Which listed RAID level meets these requirements?

A. RAID level 3

B. RAID level1

C. RAID level 2

D. RAID level 0

Hint

Compare striping granularity, redundancy placement, usable capacity and required disk-failure tolerance.

Answer B: RAID level1

With exactly two equal disks, RAID1 mirrors the data and leaves one disk's usable capacity while tolerating either disk failing. RAID0 provides no disk-failure tolerance. RAID2 and RAID3 rely on different striping and redundancy layouts rather than the two-disk mirrored arrangement that meets these requirements. The choice follows the stated disk count, capacity and failure goal rather than the institution's size or industry.

Why each choice is right or wrong

A - Incorrect: RAID3 uses byte striping with dedicated parity, not the required two-disk fault-tolerant layout.

B - Correct: A two-disk RAID1 mirror provides one disk's capacity and survives either disk failing.

C - Incorrect: RAID2 uses bit striping and Hamming redundancy rather than the required two-disk solution.

D - Incorrect: RAID0 cannot tolerate a disk failure.

Primary note proof

Study-note section NSA25

> RAID0 stripes for capacity/throughput with no disk-failure tolerance. RAID1 mirrors; a two-disk mirror has one disk's usable capacity and survives one disk failure. RAID2 uses bit striping/Hamming-code redundancy, RAID3 byte striping with dedicated parity, RAID4 block striping with dedicated parity and RAID5 block striping with distributed parity. RAID6 distributes dual parity and tolerates two disk failures. RAID10 stripes mirrored pairs; survival depends on which disks fail.

Study-note section NSA25

> With N equal disks of capacity D, RAID0 usable=ND, paired RAID1/10≈ND/2, RAID5=(N−1)D and RAID6=(N−2)D. Hardware RAID may offload work to controller resources/cache but does not universally outperform software RAID. Rebuilds consume bandwidth; parity writes have overhead. A large university/bank alone does not select a level. Striping plus parity is not uniquely RAID5 unless distributed block parity is specified.

Question sources

Computer Science Exit Exam · 2018 · Question 37

Question 100 | NS0324

A storage administrator configures four equal 2 TB disks. Each stripe stores data blocks on three disks and a parity block on the fourth; the disk holding parity changes between stripes. Ignoring metadata, which listed RAID layout provides 6 TB of usable capacity and tolerates one disk failure?

A. RAID 2

B. RAID 1

C. RAID 5

D. RAID 0

Hint

Compare striping granularity, redundancy placement, usable capacity and required disk-failure tolerance.

Answer C: RAID 5

The changing parity disk means parity is distributed across the array while data are striped in blocks, identifying RAID5. Its usable capacity is (N−1)D, so four 2 TB disks provide 6 TB and retain one disk's worth of redundancy. RAID2 uses bit striping with Hamming-code redundancy, RAID1 mirrors data, and RAID0 provides no disk-failure tolerance.

Why each choice is right or wrong

A - Incorrect: RAID2 uses bit striping with Hamming-code redundancy, not the described block stripes with rotating parity.

B - Incorrect: RAID1 mirrors data; it does not place one rotating parity block in each stripe.

C - Correct: RAID5 distributes parity across block stripes and gives (4−1)×2 = 6 TB usable capacity.

D - Incorrect: RAID0 would provide 8 TB without parity, so it fails the one-disk-failure requirement.

Primary note proof

Study-note section NSA25

> RAID0 stripes for capacity/throughput with no disk-failure tolerance. RAID1 mirrors; a two-disk mirror has one disk's usable capacity and survives one disk failure. RAID2 uses bit striping/Hamming-code redundancy, RAID3 byte striping with dedicated parity, RAID4 block striping with dedicated parity and RAID5 block striping with distributed parity. RAID6 distributes dual parity and tolerates two disk failures. RAID10 stripes mirrored pairs; survival depends on which disks fail.

Study-note section NSA25

> With N equal disks of capacity D, RAID0 usable=ND, paired RAID1/10≈ND/2, RAID5=(N−1)D and RAID6=(N−2)D. Hardware RAID may offload work to controller resources/cache but does not universally outperform software RAID. Rebuilds consume bandwidth; parity writes have

overhead. A large university/bank alone does not select a level. Striping plus parity is not uniquely RAID5 unless distributed block parity is specified.

Question sources

Computer Science Exit Exam · 2018 · Question 50

Question 101 | NS0350

Which one of the following is WRONGLY stated about an importance of security policy?

A. To help minimize risk.

B. To ensure the confidentiality, integrity and availability of data.

C. To coordinate and enforce a security program across an organization.

D. To use the system in a passive way

Hint

Distinguish the security objective from the control that prevents, detects or recovers from the stated problem.

Answer D: Passive system use is not a security-policy purpose

NSA26 assigns policies risk reduction, coordinated required behavior and CIA goals. D's passive-use statement does not describe those governance/protection purposes and is explicitly rejected here. B expresses the desired CIA objective, not a guarantee that policy alone prevents every incident. The remaining statements fit legitimate policy aims.

Why each choice is right or wrong

A - Incorrect: Reducing risk is a stated security-policy aim, so this is not wrongly stated.

B - Incorrect: CIA protection is a legitimate policy objective, with actual success depending on implemented controls.

C - Incorrect: Coordinating required behavior and enforcement across the organization is a legitimate policy purpose.

D - Correct: Passive use is not the defined purpose of security policy and does not express its governance/protection objectives.

Primary note proof

Study-note section NSA26

A security policy states required behavior, scope, accountable roles and enforcement. Begin with assets/service objectives, assess threats and weaknesses, choose controls, define exceptions/incident procedures, approve/communicate, monitor and periodically review. CIA means confidentiality, integrity and availability; neither sensitive-data protection nor availability alone is the universal primary goal.

Study-note section NSA26

A policy can require password controls, approved encryption, restricted administrative access, backups and patch deadlines; firewall rules implement part of it. Open unrestricted wireless access conflicts with controlled internal access unless intentionally isolated as a guest service. “Use the system passively” is not a purpose of security policy. Policies coordinate action and reduce risk; they do not guarantee every attack will fail.

Question sources

Computer Science Exit Exam · 2018 · Question 85