NETWORK OPERATIONS: MANAGEMENT, PROTOCOLS, AND BACKUP STRATEGIES PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://netopsmgmtprotbackupstrats.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. Explain the concept of network segmentation and its security and performance benefits.

A. It increases broadcast domains and makes policy enforcement harder.

B. It has no impact on security or performance.

C. It centralizes all traffic to a single VLAN.

D. Segmentation limits blast radius, reduces lateral movement, and simplifies policy enforcement via VLANs and ACLs.

2. A disaster recovery facility that provides only space, power, and connectivity with recovery taking days to weeks is known as a

A. Hot Site

B. Cold Site

C. Warm Site

D. Hot Spare

3. Which component is a centralized platform that collects SNMP data, monitors device health, displays dashboards, and generates alerts?

A. NMS

B. SIEM

C. IDS

D. VPN

4. In network operations, what role does DNS primarily fulfill?

A. It blocks all inbound traffic to improve security.

B. It translates IP addresses to domain names.

C. It resolves domain names to IP addresses enabling reachability.

D. It maintains routing tables between autonomous systems.

5. Which network scanning tool is used to discover hosts, identify open ports, and detect running services across a network?

A. pathping

B. arp

C. nmap

D. Light Meter

6. Which protocol is a sampling-based network traffic monitoring protocol that works across manufacturers?

A. IPFIX

B. NetFlow

C. sFlow

D. Latency

7. Which tool is used to verify copper cable continuity and correct pinout before installation?

A. nmap

B. Cable Tester

C. Light Meter

D. OTDR

8. Which command-line tool queries DNS servers to resolve hostnames to IP addresses and test DNS functionality?

A. Dig

B. Traceroute

C. Netstat

D. Nslookup

9. Which open-standard FHRP is used to share a virtual IP address among routers?

A. VRRP

B. HSRP

C. GLBP

D. FHRP

10. Designing systems with redundancy to minimize downtime and keep services running continuously aims for what?

A. High Availability

B. Five Nines

C. VRRP

D. GLBP

Answers

1. D
2. B
3. A
4. C
5. C
6. C
7. B
8. D
9. A
10. A

Explanations

1. Explain the concept of network segmentation and its security and performance benefits.

A. It increases broadcast domains and makes policy enforcement harder.

B. It has no impact on security or performance.

C. It centralizes all traffic to a single VLAN.

D. Segmentation limits blast radius, reduces lateral movement, and simplifies policy enforcement via VLANs and ACLs.

Network segmentation is the practice of dividing a network into smaller, isolated segments separated by boundaries such as VLANs and firewalls. This containment means problems in one segment don't automatically affect others, and you can control who can move between segments. Security-wise, segmentation limits the blast radius and greatly reduces lateral movement. If malware or an attacker breaches one segment, they're much less able to reach critical systems in other segments. Policy enforcement becomes clearer and stronger because you can apply access controls at the segment boundaries, using VLANs to separate broadcast domains and ACLs or firewalls to filter traffic between segments. On the performance side, smaller broadcast domains mean fewer devices see each broadcast, reducing unnecessary traffic and helping with congestion. It also makes it easier to apply quality of service and troubleshoot issues because traffic is more predictable and localized. In practice, this is achieved by using VLANs to create distinct network sections and ACLs (often in combination with firewalls) to enforce who can access each segment. That combination—segment boundaries plus targeted policy—delivers the security and performance benefits described.

2. A disaster recovery facility that provides only space, power, and connectivity with recovery taking days to weeks is known as a

A. Hot Site

B. Cold Site

C. Warm Site

D. Hot Spare

Disaster recovery options are categorized by how quickly you can resume operations after a disruption. A cold site provides only space, power, and connectivity; there are no active servers or data available there, so you must bring in equipment and restore systems from backups, which typically takes days to weeks. This matches the description of a facility that offers just space, power, and network access and requires a lengthy recovery period. In contrast, a hot site has ready-to-run hardware with replicated data for near-immediate failover, and a warm site provides some pre-installed infrastructure and data but still needs setup to fully operate. A hot spare is standby hardware kept ready to replace a failed component within production, not a separate disaster recovery site.

3. Which component is a centralized platform that collects SNMP data, monitors device health, displays dashboards, and generates alerts?

A. NMS

B. SIEM

C. IDS

D. VPN

A Network Management System is designed to collect SNMP data, monitor device health, display dashboards, and generate alerts. It acts as the centralized platform that polls devices using the Simple Network Management Protocol (SNMP) to gather metrics such as CPU usage, memory, interface status, and error counts. The NMS then stores this data, provides visual dashboards to give a real-time view of network health and performance, and triggers alerts when metrics exceed thresholds or when SNMP traps indicate problems. This combination of data collection, visualization, and alerting is what makes an NMS the go-to tool for ongoing network management. SIEM focuses on security event correlation and log analysis, not routine device health and performance monitoring. IDS is about detecting suspicious activity on the network, not providing centralized device health dashboards and alerting. VPN is about creating secure connections, not monitoring or managing devices.

4. In network operations, what role does DNS primarily fulfill?

A. It blocks all inbound traffic to improve security.

B. It translates IP addresses to domain names.

C. It resolves domain names to IP addresses enabling reachability.

D. It maintains routing tables between autonomous systems.

The essential idea is that DNS turns human-friendly domain names into the IP addresses devices use to reach a target on the network. Routers and hosts route traffic by IP, not by name, so when you type a URL, your system asks a DNS resolver to translate that domain into its numeric address. Once the IP is known (and typically cached for speed), communication can proceed, making the target reachable. DNS accomplishes this through records like A for IPv4 and AAAA for IPv6, with other types such as CNAME for aliases. There's also reverse mapping (IP back to a domain) via PTR records, but that's not the primary role of DNS. The hierarchical, distributed structure of DNS ensures name resolution is scalable and efficient, enabling users to connect to services using friendly names rather than numeric addresses.

5. Which network scanning tool is used to discover hosts, identify open ports, and detect running services across a network?

A. pathping

B. arp

C. nmap

D. Light Meter

The ability to map a network by finding which devices are alive, which ports are open, and what services are running on those ports is what Nmap is built to do. Nmap, short for Network Mapper, can perform host discovery to identify responsive devices, scan those devices to see which ports are open, and probe the open ports to determine the services and often the versions running on them. This combination gives a practical view of the network's active hosts and their exposed services, which is essential for inventory, security reviews, and vulnerability assessments. _pathping_ is a diagnostic tool that blends ping with traceroute to show route information and packet loss along a path; it doesn't enumerate open ports or identify the services on those ports. _arp_ resolves IP addresses to MAC addresses on a local network segment, but it doesn't provide broad network scanning for hosts or services beyond the local ARP table. _Light Meter_ isn't a standard network scanning tool used for discovering hosts or services, so it wouldn't serve this purpose.

6. Which protocol is a sampling-based network traffic monitoring protocol that works across manufacturers?

A. IPFIX

B. NetFlow

C. sFlow

D. Latency

The concept being tested is a protocol that provides visibility into network traffic by sampling packets and exporting that data in a way that works across different manufacturers. sFlow does this directly: it places a lightweight agent on devices to randomly sample packets on interfaces, pairs each sample with metadata, and sends the data to a central collector. This collector can be on gear from many vendors, giving you a unified view of traffic across a mixed network with minimal overhead. That vendor-agnostic, sampling-based approach is what makes sFlow ideal for cross-manufacturer monitoring. NetFlow is a well-established flow-export approach, and IPFIX is its standardized evolution. Both can be used for network visibility, but the key distinction here is the explicit sampling model. sFlow's design centers on sampling across devices from different vendors, which is why it's the best fit for cross-manufacturer monitoring. Latency, by contrast, is a metric, not a protocol for exporting traffic data.

7. Which tool is used to verify copper cable continuity and correct pinout before installation?

A. nmap

B. Cable Tester

C. Light Meter

D. OTDR

Testing copper cable continuity and pinout is about confirming that every conductor in the cable is connected end-to-end and that the wiring order matches the expected standard. A Cable Tester applies signals through the wires and checks each path, so you can see if there are opens, shorts, or miswired/pinout errors. This ensures that when you install the cable, the network will function correctly and you won't run into connectivity issues caused by a bad or miswired termination. Other tools don't fit this job. A network scanner like nmap is used after wiring to discover devices and services on a live network, not to verify the physical cable. A Light Meter measures light levels for fiber optic applications, not copper cables. An OTDR is designed to analyze fibers by sending pulses and detecting reflections to locate faults along a fiber, which again is not for copper cabling. So, the tool best suited for verifying copper cable continuity and correct pinout before installation is a Cable Tester.

8. Which command-line tool queries DNS servers to resolve hostnames to IP addresses and test DNS functionality?

A. Dig

B. Traceroute

C. Netstat

D. Nslookup

Dns lookup tools are used to query DNS servers to map hostnames to IP addresses and verify that DNS is functioning. Nslookup is a command-line tool that does exactly that: it asks a DNS server for DNS records that resolve a hostname to an IP address, and it can be directed to use a specific server to isolate or test DNS behavior. You can request A records for IPv4 addresses, AAAA for IPv6, or other record types, and you can perform the query against a chosen DNS server (for example, nslookup example.com 8.8.8.8) to see how that server responds. This makes it straightforward to confirm that a hostname resolves correctly and to diagnose DNS failures (like no such domain or SERVFAIL). In contrast, traceroute follows network paths rather than name resolution, netstat reveals active connections, and while dig also performs DNS lookups, nslookup is the classic, widely available tool that directly tests DNS resolution from the command line.

9. Which open-standard FHRP is used to share a virtual IP address among routers?

A. VRRP

B. HSRP

C. GLBP

D. FHRP

The concept here is providing a single, stable gateway for hosts even if a router fails. VRRP is the open-standard way to do that. In VRRP, several routers form a group and share one virtual IP address that serves as the default gateway for hosts. One router is elected as the master and actively handles traffic for that virtual IP; the others stay as backups. If the master router goes down, a backup is quickly promoted to master, and the virtual IP stays reachable, so clients don't have to change their gateway. The virtual IP is tied to a virtual MAC as well, so the switch and hosts continue to use the same gateway address during a failover. VRRP is vendor-neutral and widely implemented, which is why it's the open standard for sharing a virtual IP among routers. HSRP and GLBP are Cisco-proprietary approaches with similar goals, but they aren't open standards.

10. Designing systems with redundancy to minimize downtime and keep services running continuously aims for what?

A. High Availability

B. Five Nines

C. VRRP

D. GLBP

Designing for redundancy to keep services running continuously is about high availability. High availability describes architectures built with redundant components, health monitoring, and automated failover so services stay online even when parts fail. Five nines is a common uptime goal (99.999%), a metric of how available the system should be, but it's the target rather than the method. VRRP and GLBP are specific network mechanisms that help provide redundant gateways and load balancing; they support high availability, but the overarching objective is the continuous operation ensured by a robust HA design. In short, the aim is to design systems that stay up with minimal downtime through redundancy, monitoring, and quick recovery.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://netopsmgmtprotbackupstrats.examzify.com

We wish you the very best on your exam journey. You've got this!