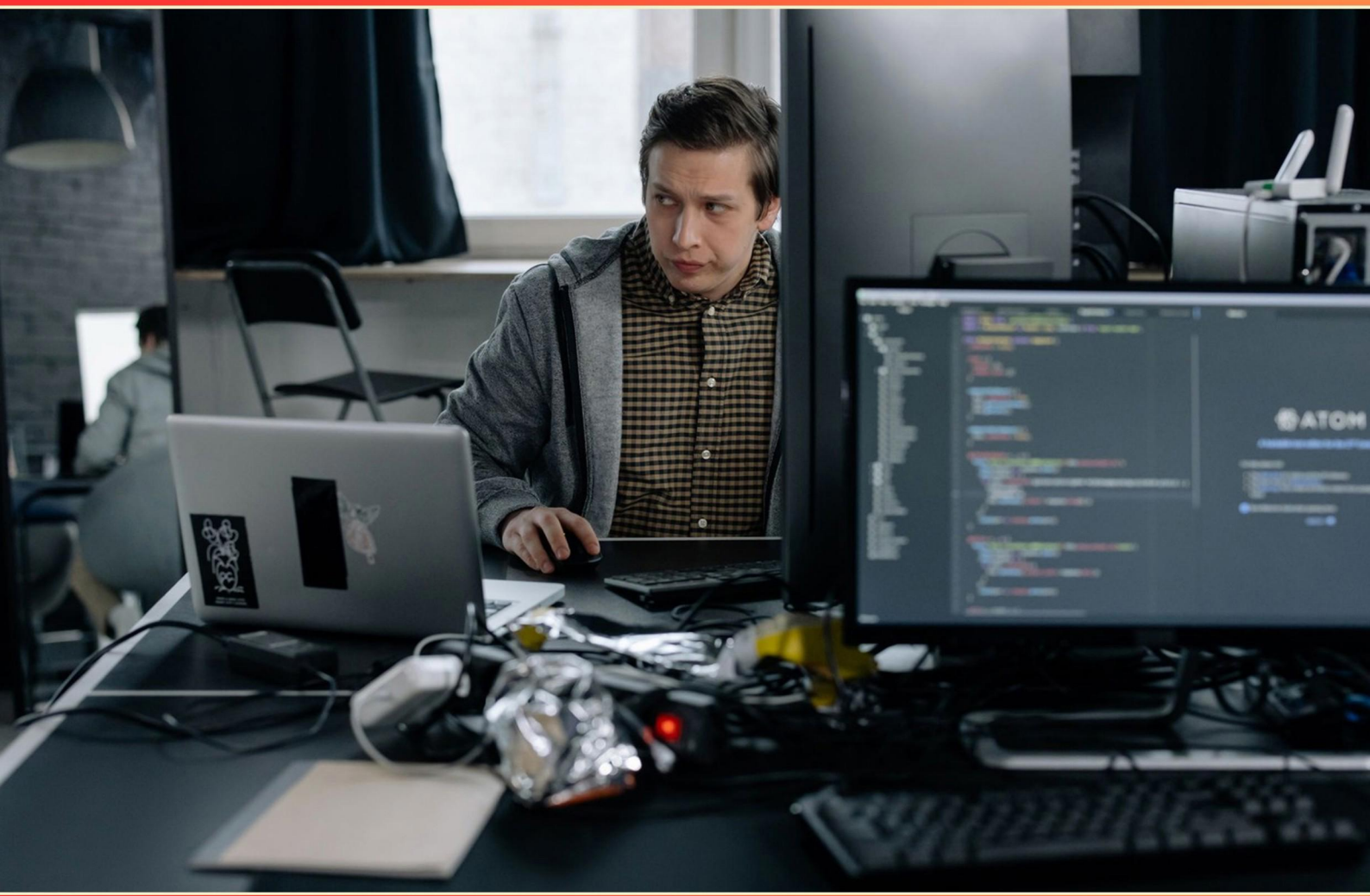
HUAWEI CERTIFIED ICT PROFESSIONAL (HCIP) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://huaweiictprohcip.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. In port mirroring, data must be collected in which manner for reliability?

A. In intervals to aggregate data

B. In real time

C. Asynchronously for later analysis

D. In a compressed format

2. Which port states are defined by RSTP?

A. Discarding

B. Learning

C. Forwarding

D. Discarding, Learning, and Forwarding

3. Which scenario does not utilize the guest access management function of the Agile Controller?

A. Customers access resources during enterprise visits

B. Citizens accessing the Internet through public utilities

C. Consumers connecting to the Internet over the enterprise network

D. Enterprise employees connecting while on business trips

4. Which technologies are part of congestion avoidance?

A. RED and WRED

B. SPF and Dijkstra

C. TCP and UDP

D. QoS and VoIP

5. During BFD session establishment between devices, which state is not involved?

A. 2-way

B. down

C. in it

D. up

6. What can help avoid information leakage on intra-nets?

A. Regular software updates

B. In-depth network auditing

C. Using VPN for all data transmission

D. Monitor incoming and outgoing MAC addresses

7. What mechanism does IS-IS use for neighbor relationship establishment reliability?

A. Status synchronization

B. Checksum verification

C. Aging timer

D. Three-way handshake

8. Which statement about the MPLS forwarding process is false?

A. The MPLS control plane can detect errors in LSP forwarding.

B. The MPLS forwarding plane adds or deletes labels from an IP packet.

C. The ingress LER adds proper labels to packets entering the MPLS network.

D. MPLS cannot use Ping or Traceroute to detect LSP errors.

9. In the context of QoS, what is often a cause of packet loss?

A. Fixed bandwidth limitations

B. Link faults

C. CPU processing speed

D. Data retransmissions

10. What is the multicast destination address of VRRP packets?

A. 224.0.0.18

B. 224.0.0.20

C. 224.1.0.18

D. 224.1.0.20

Answers

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

Explanations

1. In port mirroring, data must be collected in which manner for reliability?

A. In intervals to aggregate data

B. In real time

C. Asynchronously for later analysis

D. In a compressed format

Port mirroring, also known as SPAN (Switch Port Analyzer), is a technique used to monitor network traffic. In the context of reliability, data must be collected in real time to ensure that every packet of interest is captured without delays or losses. Real-time data collection allows network administrators and security analysts to continuously monitor and analyze the communication happening over the network. This is crucial for tasks such as troubleshooting, performance tuning, and identifying security threats, as it provides an accurate and up-to-date view of traffic patterns and issues as they occur. By capturing data in real time, any anomalies or performance issues can be addressed immediately, reducing the risk of missed critical events or reactive measures when issues escalate. Other methods such as collecting data in intervals or asynchronously can introduce a lag in the information available, which can lead to incomplete monitoring and an inability to respond swiftly to potential problems. Using a compressed format might conserve bandwidth but could obscure important details necessary for accurate analysis. Thus, real-time collection stands out as the most reliable approach in port mirroring for maintaining comprehensive and timely oversight of network activity.

2. Which port states are defined by RSTP?

A. Discarding

B. Learning

C. Forwarding

D. Discarding, Learning, and Forwarding

Rapid Spanning Tree Protocol (RSTP) is an evolution of the original Spanning Tree Protocol (STP) designed to improve the convergence time in network topologies. In RSTP, there are three definitive port states that describe how a port on a switch can handle traffic during the operation of the protocol. The discarding state is utilized when a port is not forwarding traffic; this can be due to the port being part of a redundant link that is in a standby state or simply to prevent loops in the network. In this state, the port does not send or receive frames, ensuring that there are no data packets being forwarded unnecessarily. The learning state allows a port to process incoming frames and determine the source MAC addresses for those frames. This state is critical for building the MAC address table but does not forward frames to other ports yet. This phase is essential to ensure that when a port transitions to the forwarding state, it has the necessary information to send traffic appropriately. Finally, the forwarding state is where a port actively sends and receives frames. In this state, frames can be forwarded to other ports on the network, and the port participates fully in the forwarding decisions based on its learned MAC addresses. The combination of these three states - discarding

3. Which scenario does not utilize the guest access management function of the Agile Controller?

A. Customers access resources during enterprise visits

B. Citizens accessing the Internet through public utilities

C. Consumers connecting to the Internet over the enterprise network

D. Enterprise employees connecting while on business trips

The scenario in which enterprise employees connect while on business trips does not utilize the guest access management function of the Agile Controller. The guest access management function is primarily designed to manage network access for individuals who are not part of the internal organization, such as visitors or external users. In the case of enterprise employees connecting while on business trips, they are typically existing users of the organization's network. They would have their credentials and access rights already defined within the corporate system, allowing them to authenticate and connect to the secure network without needing the guest access management protocols that are intended for temporary or external users. This contrasts with the other scenarios where guest access management is essential, as they involve individuals who are not regular users of the network and require controlled access to resources for a limited time and under specific conditions.

4. Which technologies are part of congestion avoidance?

A. RED and WRED

B. SPF and Dijkstra

C. TCP and UDP

D. QoS and VoIP

The correct choice, which highlights technologies fundamental to congestion avoidance, identifies Random Early Detection (RED) and Weighted Random Early Detection (WRED) as key techniques. These algorithms are designed to proactively manage packet transmission by monitoring network traffic levels. When congestion begins to be detected, RED and WRED allow for packets to be selectively dropped before the buffer becomes completely full, effectively signaling the sending devices to reduce their transmission rates. This helps in maintaining overall network stability and performance by preventing sudden packet loss and reducing latency. In contrast, the other options focus on unrelated areas. SPF (Shortest Path First) and Dijkstra's algorithm pertain to routing protocols and pathfinding rather than congestion control. TCP and UDP are transport layer protocols, where TCP incorporates some congestion control mechanisms, but UDP does not engage in congestion avoidance. Lastly, Quality of Service (QoS) is a broader concept for managing network resources and assuring service quality, while VoIP is a communication technology. Neither of these directly addresses the specific mechanisms employed for managing congestion in networks.

5. During BFD session establishment between devices, which state is not involved?

A. 2-way

B. down

C. in it

D. up

During the establishment of a Bidirectional Forwarding Detection (BFD) session between devices, the state progression follows a specific sequence to ensure that the link is operational and that both ends can communicate effectively. The states that are typically involved in this process are "down," "up," and "init." The "down" state signifies that the BFD session has not yet been established, meaning no BFD control packets have been exchanged. The "init" state indicates that the BFD session has begun, where the device sends out BFD control packets to the other end. Once the devices recognize each other and establish a successful session, they transition to the "up" state, confirming that the BFD session is live and both devices are actively monitoring the link. On the other hand, the "2-way" state is not a recognized state in the BFD session establishment process. This terminology is more commonly associated with protocols like OSPF, which describe neighbor relationships, rather than BFD. Therefore, "2-way" is not part of the state transitions in BFD and explains why it is the correct answer to the question.

6. What can help avoid information leakage on intra-nets?

A. Regular software updates

B. In-depth network auditing

C. Using VPN for all data transmission

D. Monitor incoming and outgoing MAC addresses

Monitoring incoming and outgoing MAC addresses is an effective measure to help avoid information leakage on intra-nets. This approach provides a way to track which devices are communicating across the network, allowing administrators to see all devices connecting to and from the network. By keeping an eye on these MAC addresses, organizations can identify unauthorized devices that might attempt to access sensitive information, thereby safeguarding against potential data breaches and insider threats. This method also assists in leveraging access controls, ensuring that only recognized and approved devices have access to the internal network. It enhances security through visibility, which is crucial for quick incident response should any suspicious activity be detected. In contrast, while regular software updates can enhance overall security by patching vulnerabilities, they do not specifically target the prevention of information leakage. In-depth network auditing is beneficial for understanding network performance and security, but it is a more reactive measure rather than a proactive way to prevent data leaks. Using VPNs for all data transmission is an excellent method for secure data transfer across insecure networks, but it doesn't inherently prevent leakage within an intra-net where data is already assumed to be secure. Thus, monitoring MAC addresses stands out as a direct strategy to mitigate the risks of data leakage on intra-nets.

7. What mechanism does IS-IS use for neighbor relationship establishment reliability?

A. Status synchronization

B. Checksum verification

C. Aging timer

D. Three-way handshake

The three-way handshake is fundamental for establishing reliable neighbor relationships in the IS-IS (Intermediate System to Intermediate System) protocol. This mechanism involves three steps: the sending of a Hello message, the response from the neighbor confirming the receipt, and finally, an acknowledgment that solidifies the relationship as being mutually recognized. This process ensures that both ends of the link agree on the existence and status of the connection before proceeding to exchange routing information. It enhances reliability by verifying that both routers are not only able to communicate but also that they recognize and accept each other as valid neighbors within the network. In contrast, other mechanisms like status synchronization, checksum verification, and aging timers serve different purposes in managing and maintaining the integrity and currency of routing information or device states but do not specifically focus on the establishment of neighbor relationships as effectively as the three-way handshake does.

8. Which statement about the MPLS forwarding process is false?

A. The MPLS control plane can detect errors in LSP forwarding.

B. The MPLS forwarding plane adds or deletes labels from an IP packet.

C. The ingress LER adds proper labels to packets entering the MPLS network.

D. MPLS cannot use Ping or Traceroute to detect LSP errors.

The correct statement regarding the MPLS forwarding process among the options provided revolves around the utilization of the MPLS control plane for error detection in LSP (Label Switched Path) forwarding. In MPLS, the control plane is responsible for establishing and maintaining the LSPs through signaling protocols like LDP (Label Distribution Protocol) or RSVP-TE (Resource Reservation Protocol - Traffic Engineering). Part of this responsibility includes the capability to detect certain errors related to LSP forwarding. For instance, the control plane can monitor pathways and verify label mappings, helping to identify any issues that may arise due to network changes or failures. Therefore, the assertion that the MPLS control plane can detect errors in LSP forwarding is accurate and reflects the intrinsic functionalities designed within MPLS architecture to ensure reliable data transmission. This reinforces the overall robustness of the MPLS network as it manages label operations effectively and maintains LSP integrity. It's also significant to note that the other provided options accurately describe aspects of the MPLS forwarding process. The forwarding plane's role encompasses adding or deleting labels and the ingress LER's responsibility for labeling packets all align with standard MPLS operations. Additionally, while MPLS can be less effective in detecting certain types of errors compared to other technologies,

9. In the context of QoS, what is often a cause of packet loss?

A. Fixed bandwidth limitations

B. Link faults

C. CPU processing speed

D. Data retransmissions

Packet loss often occurs due to various network issues, and identifying the specific causes can be crucial for maintaining quality of service (QoS). A common reason for packet loss is link faults, which can happen when there is a physical issue in the transmission medium, such as a damaged cable or a malfunctioning network interface. When a link fault occurs, packets that are sent over that link cannot reach their destination, leading to loss of data. This type of packet loss is critical because it can disrupt communication and degrade the overall performance of applications, especially those sensitive to delays, such as video streaming or VoIP. Other factors, while potentially related to packet loss, do not directly cause it in the manner that link faults do. For instance, fixed bandwidth limitations can lead to congestion, but packet loss stemming from congestion typically involves other mechanisms rather than direct link faults. CPU processing speed may affect a device's ability to process packets quickly, but it isn't a direct cause of packets being lost while in transit. Data retransmissions occur when packets that have been lost are detected and sent again, and while they are a consequence of packet loss, they don't cause the initial loss themselves. Understanding these dynamics is essential for implementing effective QoS strategies in network design

10. What is the multicast destination address of VRRP packets?

A. 224.0.0.18

B. 224.0.0.20

C. 224.1.0.18

D. 224.1.0.20

The multicast destination address for VRRP (Virtual Router Redundancy Protocol) packets is 224.0.0.18. This address is specifically designated for VRRP, allowing routers participating in VRRP to communicate effectively in a local broadcast domain. The choice of this address is important because it ensures that all devices configured to listen for VRRP advertisements will receive the packets, enabling them to coordinate in defining which router will take on the active role in providing gateway services. This plays a crucial role in maintaining network reliability and facilitating failover in case the primary router becomes unavailable. The other addresses listed are not utilized by VRRP. For example, 224.0.0.20 is generally associated with other multicast protocols, while 224.1.0.18 and 224.1.0.20 may not have specific functions related to VRRP, thereby making them unsuitable for this particular application. Thus, 224.0.0.18 is the correct multicast address to be used for VRRP communications.

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://huaweiictprohcip.examzify.com

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