Navy IT Communications Part 5 Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Table of Contents

Copyright **1**

Table of Contents **2**

Introduction **3**

How to Use This Guide **4**

Questions **5**

Answers **9**

Explanations **11**

Next Steps **17**

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. What is a VPN and differentiate between IPsec tunnel mode, IPsec transport mode, and TLS VPN.

A. TLS VPN uses TLS over SSH for remote access.

B. VPN creates encrypted tunnel for remote access or site-to-site; IPsec tunnel mode encrypts entire IP packet; IPsec transport mode encrypts only the payload; TLS VPN uses TLS over TCP.

C. IPsec tunnel mode encrypts only the payload; TLS VPN uses UDP.

D. VPN is only for site-to-site connections and not remote access.

2. Which layer does 802.1Q tagging operate at?

A. Layer 3

B. Layer 2

C. Layer 1

D. Layer 4

3. A VPN tunnel is best described as which of the following?

A. A virtual link inside a LAN.

B. A physical fiber connection between sites.

C. An encrypted passage between endpoints.

D. An unencrypted channel over the Internet.

4. Non-repudiation with digital signatures: how is it achieved?

A. Non-repudiation is achieved when a digital signature created with a private key binds the signer to the data, verifiable with the signer's public key.

B. Non-repudiation is achieved by encrypting the entire message with a symmetric key.

C. Non-repudiation means anyone can deny signing; it doesn't apply to signatures.

D. Non-repudiation is achieved by hashing only.

5. Which statement correctly describes SPF's function in email authentication?

A. SPF validates the recipient's mailbox using domain reputation.

B. SPF signs messages with a cryptographic key.

C. SPF validates the sending host by checking its IP address against the domain's SPF record.

D. SPF blocks attachments using content filtering.

6. Which device operates at Layer 3 to route traffic between networks?

A. Switch

B. Bridge

C. Router

D. Hub

7. Which statement best matches common network cabling types to typical speeds?

A. UTP Cat5e up to 1 Gbps; Cat6 up to 10 Gbps short distances; fiber supports 10 Gbps+ with high distances; fiber types multimode and single-mode.

B. UTP Cat5e supports 10 Gbps; Cat6 supports 40 Gbps.

C. UTP Cat5e is fiber optic; Cat6 is copper; multimode fiber cannot be used for 10 Gbps.

D. Fiber is never used for high-speed LAN; UTP Cat6 is best for long distances.

8. What is a legitimate use case for a packet sniffer?

A. Troubleshooting network issues.

B. Hiding user activity from admins.

C. Disrupting network services.

D. Overloading a network with traffic.

9. How many memory locations are available for frequency storage in the receiver?

A. 99 memory locations and 1 manual location

B. 50 memory locations

C. 200 memory locations

D. 100 memory locations

10. Which statement about Dynamic ARP Inspection (DAI) is accurate?

A. Port security on switches cannot restrict MAC addresses.

B. ARP spoofing cannot occur if DNSSEC is enabled.

C. Dynamic ARP Inspection validates ARP packets against a trusted database to block spoofed traffic.

D. DAI replaces VLANs to isolate traffic.

Answers

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

Explanations

1. What is a VPN and differentiate between IPsec tunnel mode, IPsec transport mode, and TLS VPN.

A. TLS VPN uses TLS over SSH for remote access.

B. VPN creates encrypted tunnel for remote access or site-to-site; IPsec tunnel mode encrypts entire IP packet; IPsec transport mode encrypts only the payload; TLS VPN uses TLS over TCP.

C. IPsec tunnel mode encrypts only the payload; TLS VPN uses UDP.

D. VPN is only for site-to-site connections and not remote access.

A VPN serves to create a secure, encrypted connection over an untrusted network so you can connect remotely or link separate networks as if they were directly connected. When you look at how different VPN technologies protect traffic, you see important differences in what they encrypt and where they operate. IPsec in tunnel mode protects the entire IP packet. That means both the payload and the original IP header are wrapped and carried through the VPN tunnel, which is ideal for network-to-network links or remote access where you want to shield every bit of the original packet as it traverses the public network. IPsec in transport mode, on the other hand, protects only the payload, leaving the IP header unencrypted. The header remains visible to routing devices along the path, making this mode suitable for end-to-end protection between two hosts on a shared trusted network rather than for gateway-to-gateway VPNs. TLS VPN (often called SSL VPN) uses the TLS protocol over TCP to secure the connection. This approach is typically application-oriented, enabling remote access to specific applications or networks through a browser or TLS-enabled client, and benefits from the reliability and firewall/NAT traversal characteristics of TCP. Putting these together, the description that a VPN creates an encrypted tunnel for remote access or site-to-site, that IPsec tunnel mode encrypts the entire IP packet, that IPsec transport mode encrypts only the payload, and that TLS VPN uses TLS over TCP, captures the distinct roles and protections of these technologies.

2. Which layer does 802.1Q tagging operate at?

A. Layer 3

B. Layer 2

C. Layer 1

D. Layer 4

802.1Q tagging operates at Layer 2, the Data Link layer. This tagging concerns how Ethernet frames are forwarded within a local network and how switches separate traffic into different VLANs. The tag is inserted into the frame header (between the source MAC address and the EtherType field) to carry the VLAN ID (and optional priority), enabling switches to keep broadcast domains distinct. Layer 3 handles routing between networks (IP addressing), Layer 1 covers the physical signaling, and Layer 4 deals with transport protocols like TCP/UDP. So the tagging decision and the VLAN segmentation are inherently a Layer 2 function.

3. A VPN tunnel is best described as which of the following?

A. A virtual link inside a LAN.

B. A physical fiber connection between sites.

C. An encrypted passage between endpoints.

D. An unencrypted channel over the Internet.

A VPN tunnel is about creating a secure, encrypted path between two endpoints to carry data across an untrusted network. This means the data is encapsulated and encrypted so it remains confidential and integral as it moves over the Internet or another public network, even though the underlying network isn't private. It isn't a physical link like a fiber cable, and it isn't just a virtual LAN inside a single site. It's also not an unencrypted channel—the whole purpose is to protect the data in transit with encryption and integrity checks. In practice, VPN tunnels are established between devices or networks using protocols such as IPsec or SSL/TLS, enabling secure site-to-site or remote-access connections across wide distances.

4. Non-repudiation with digital signatures: how is it achieved?

A. Non-repudiation is achieved when a digital signature created with a private key binds the signer to the data, verifiable with the signer's public key.

B. Non-repudiation is achieved by encrypting the entire message with a symmetric key.

C. Non-repudiation means anyone can deny signing; it doesn't apply to signatures.

D. Non-repudiation is achieved by hashing only.

Non-repudiation with digital signatures is achieved when the signer uses a private key to create a signature over the data, binding the signer to that data. This signature can be verified with the signer's public key, often tied to an identity via a certificate. Because only the private key holder could have generated the signature, the signer cannot credibly deny signing the data later, and the verification confirms both who signed (via the public key/certificate) and that the data hasn't been altered. Using symmetric encryption wouldn't establish who signed since the key is shared among parties, and hashing alone only ensures data integrity without proving signer's identity or involvement.

5. Which statement correctly describes SPF's function in email authentication?

A. SPF validates the recipient's mailbox using domain reputation.

B. SPF signs messages with a cryptographic key.

C. SPF validates the sending host by checking its IP address against the domain's SPF record.

D. SPF blocks attachments using content filtering.

SPF works by allowing domain owners to publish a DNS SPF record that lists which sending hosts are authorized to mail for that domain. When a message arrives, the receiving server queries the domain's SPF TXT record and compares the sending server's IP address to the authorized list. If the IP matches, the SPF check passes, indicating the mail is coming from an allowed source; if not, it fails or softfails, helping to detect spoofing. This is different from signing messages (that would be DKIM) or blocking attachments via content filters. SPF focuses on verifying the sending host by IP against the domain's published policy, not on the recipient's mailbox reputation.

6. Which device operates at Layer 3 to route traffic between networks?

A. Switch

B. Bridge

C. Router

D. Hub

Routing between networks happens at the network layer, where a device chooses paths for packets based on IP addresses. The router is the device that connects multiple networks and uses a routing table and protocols to forward each packet toward its destination, selecting the next hop that leads toward the final network. Switches and bridges operate mainly at Layer 2, handling frames within the same network by using MAC addresses, not making inter-network routing decisions. A hub is a purely physical-layer device that repeats signals to all ports without any filtering or path selection. So the device that routes traffic between networks is the router.

7. Which statement best matches common network cabling types to typical speeds?

A. UTP Cat5e up to 1 Gbps; Cat6 up to 10 Gbps short distances; fiber supports 10 Gbps+ with high distances; fiber types multimode and single-mode.

B. UTP Cat5e supports 10 Gbps; Cat6 supports 40 Gbps.

C. UTP Cat5e is fiber optic; Cat6 is copper; multimode fiber cannot be used for 10 Gbps.

D. Fiber is never used for high-speed LAN; UTP Cat6 is best for long distances.

Understanding how common network cabling types map to speeds and distances helps you pick the right link for a given site. Copper twisted-pair cables vary by category. Cat5e can carry up to about 1 Gbps over the standard 100-meter Ethernet link. Cat6 can handle 10 Gbps, but on copper that speed is limited to shorter runs before performance degrades, so you typically see 10 Gbps on Cat6 only over shorter distances; Cat6A then extends the 10 Gbps capability to the full 100 meters. Fiber optics deliver much higher speeds and longer distances. Multimode fiber is used for shorter, inside-building links, while single-mode fiber handles very long distances; both types can support 10 Gbps and higher with the right transceivers and equipment. So the statement matches typical expectations: copper Cat5e up to 1 Gbps, copper Cat6 up to 10 Gbps on shorter runs, and fiber capable of 10 Gbps and beyond over longer distances with both multimode and single-mode fibers. Other options mix up these facts, such as claiming Cat5e can do 10 Gbps or that fiber isn't used for high-speed LAN.

8. What is a legitimate use case for a packet sniffer?

A. Troubleshooting network issues.

B. Hiding user activity from admins.

C. Disrupting network services.

D. Overloading a network with traffic.

Packet sniffers are diagnostic tools that observe network traffic to troubleshoot problems. By capturing and analyzing packets, they help you see where latency or packet loss occurs, verify that devices are communicating correctly, and confirm that protocols and configurations are behaving as intended. This passive, investigative use is legitimate when you have authorization, because it helps identify root causes and optimize performance without altering the traffic. Using the tool to hide user activity from admins or to disrupt or overwhelm the network would be misuse or harm, not a legitimate use.

9. How many memory locations are available for frequency storage in the receiver?

A. 99 memory locations and 1 manual location

B. 50 memory locations

C. 200 memory locations

D. 100 memory locations

Memory locations are the preset slots you use to store specific frequencies so you can recall them instantly. This receiver provides 100 memory locations, meaning you can save up to 100 different frequencies for quick access. That number offers a practical balance between having enough presets for typical operations and not overcomplicating the hardware. The other options are less fitting: 50 would limit how many frequencies you can store, 200 would be more than the design typically supports, and mentioning a manual location introduces a slot that isn't a true memory location, so it doesn't change the count of stored frequencies.

10. Which statement about Dynamic ARP Inspection (DAI) is accurate?

A. Port security on switches cannot restrict MAC addresses.

B. ARP spoofing cannot occur if DNSSEC is enabled.

C. Dynamic ARP Inspection validates ARP packets against a trusted database to block spoofed traffic.

D. DAI replaces VLANs to isolate traffic.

Dynamic ARP Inspection focuses on ARP security by checking each ARP packet against a trusted binding database. This database is built from DHCP snooping information and static entries, creating a map of valid IP-to-MAC addresses. When an ARP reply arrives, DAI compares the claimed IP-to-MAC pairing to that trusted map. If the pair doesn't match, the packet is dropped, effectively blocking ARP spoofing and preventing a potential man-in-the-middle scenario. This is why the statement about DAI being able to validate ARP packets against a trusted database to block spoofed traffic is the accurate description. DNSSEC deals with validating DNS responses, not ARP messages at layer 2, so enabling DNSSEC doesn't stop ARP spoofing. And DAI doesn't replace VLANs—VLANs continue to segment traffic, while DAI operates within those segments to scrutinize ARP traffic. Port security can restrict MAC addresses, so the idea that port security cannot do that isn't correct.

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://navyitcommspt5.examzify.com

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