

RADIO COMMUNICATIONS – ADVANTAGES, DISADVANTAGES, NETS, SECURITY, AND PROCEDURES PRACTICE TEST (SAMPLE) STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE**

[https://
radiocommsnetssecurityprocedures.examzify.com](https://radiocommsnetssecurityprocedures.examzify.com)



Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright	1
Table of Contents	2
Introduction	3
How to Use This Guide	4
Questions	5
Answers	8
Explanations	10
Next Steps	15

SAMPLE

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

SAMPLE

- 1. When interference or jamming is suspected, what action should the user take?**
 - A. Fill out jamming report
 - B. Ignore it
 - C. Increase transmitter power
 - D. Switch to another frequency
- 2. Which of the following is NOT a main action of electronic warfare?**
 - A. Attack
 - B. Defence
 - C. Surveillance
 - D. Frequency Hopping
- 3. Which method is used to counter electronic counter-counter measures by rapidly changing frequencies?**
 - A. Frequency Hopping
 - B. Direct Sequence Spread Spectrum
 - C. Time Division Multiplexing
 - D. Phase Modulation
- 4. Which of the following is a direct step to take when interference or jamming is suspected?**
 - A. Check radio settings
 - B. Replace the antenna
 - C. Increase power
 - D. Switch to 2m band
- 5. How many elements are in the internal triangle?**
 - A. 2
 - B. 3
 - C. 4
 - D. 5

- 6. Which term describes measures aimed at detecting and gathering information about the electromagnetic environment to support operations?**
- A. Electronic Counter Measures
 - B. Electronic Protective Measures
 - C. Electronic Support Measures
 - D. Electronic Attack Measures
- 7. What sequence best describes how stations should rejoin after a pause?**
- A. End the net immediately.
 - B. Switch to a backup frequency without notification.
 - C. Net Control calls for rejoin; stations respond with their call sign; channel is verified clear; traffic resumes.
 - D. All stations must wait until a supervisor approves.
- 8. Which of the following is a defence against enemy deception?**
- A. Authentication
 - B. Good procedures
 - C. Constant vigilance
 - D. Encryption
- 9. Does a transmission ending with 'Out' or 'Out to you' require a reply?**
- A. True
 - B. False
 - C. Depends
 - D. Not sure
- 10. Why is having pre-planned frequencies and fallback channels important, and how is this information communicated to participants?**
- A. Ensures redundancy; reduces downtime; Documented in a frequency plan; distributed to all participants via training and published SOPs.
 - B. Frequencies are chosen on the fly; fallback channels unnecessary.
 - C. Frequency plans are kept secret from participants.
 - D. Fallback channels are not tested during training.

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. When interference or jamming is suspected, what action should the user take?

- A. Fill out jamming report**
- B. Ignore it
- C. Increase transmitter power
- D. Switch to another frequency

When interference or jamming is suspected, the proper step is to file a jamming/interference report with the appropriate regulatory authority. This creates an official, traceable record that helps investigators identify the source and take appropriate action, while keeping you in compliance with regulations. Include details such as the date and time of the interference, the exact frequency and bandwidth involved, the mode you were using, and any observable signal characteristics (presence of a carrier, modulation type, tones). Note your location, the duration of the issue, and whether other stations are affected. Any directional finding results, descriptions of the environment, and logs, recordings, or spectrum captures you can provide are valuable. Also document what you did on your end (changes in frequency or power) and the outcomes. Avoid countermeasures like jamming back or routinely shifting frequencies as a long-term fix, since those actions can worsen the problem or violate rules. After filing, follow the authority's guidance and cooperate with the investigation.

2. Which of the following is NOT a main action of electronic warfare?

- A. Attack
- B. Defence
- C. Surveillance
- D. Frequency Hopping**

Electronic warfare is organized around three broad actions: attacking the enemy's systems, defending our own systems, and surveilling to understand the enemy's emissions. Attacking is about degrading or denying the adversary's radar, communications, or sensors. Surveillance involves listening to and locating emitters to gain intelligence on threat activity. Defense focuses on protecting and maintaining our own capabilities in the face of EW, including anti-jamming measures and resilience. Frequency hopping is a technique used to counter interference by rapidly changing the carrier frequency, which helps keep communications and sensors usable in a contested environment. It's a specific method employed within the defense/assurance side of EW, rather than one of the principal action categories itself. So, while useful, frequency hopping isn't considered a main action of electronic warfare, which is why it's the correct answer.

3. Which method is used to counter electronic counter-counter measures by rapidly changing frequencies?

- A. Frequency Hopping**
- B. Direct Sequence Spread Spectrum
- C. Time Division Multiplexing
- D. Phase Modulation

Rapidly changing frequencies is frequency hopping, a technique designed to defeat jamming by moving the carrier across a range of frequencies in a pseudo-random sequence shared by both ends. Because the signal only dwells briefly on any one frequency, a narrowband jammer has little time to affect it, and a jammer would have to follow the same hopping pattern or blanket a wide portion of the spectrum to be effective. This makes the communication substantially more resilient to electronic countermeasures that target a single frequency. It does require tight synchronization between transmitter and receiver and can demand more bandwidth or face regulatory constraints. Other approaches can help with jamming resistance in different ways, but the defining feature here is using rapid frequency changes to outrun interference.

4. Which of the following is a direct step to take when interference or jamming is suspected?

- A. Check radio settings**
- B. Replace the antenna
- C. Increase power
- D. Switch to 2m band

The key idea is that problems that mimic interference often come from how your own radio is configured. Checking radio settings is the direct, first-step action because a mis-tuned frequency, the wrong mode, improper filter selection, or an inappropriate squelch level can create symptoms that look like interference or jamming. By verifying that you're on the intended frequency and using the correct mode, with appropriate squelch, power, and any tone or filter settings, you can rule out a configuration issue and identify whether the disruption is truly external. Replacing the antenna, increasing power, or switching to a different band address different aspects of the system or the environment, but they don't diagnose or confirm the cause. They can mask or worsen the problem and may violate operating rules or degrade performance, whereas confirming settings directly targets the most common, controllable source of false interference.

5. How many elements are in the internal triangle?

- A. 2
- B. 3**
- C. 4
- D. 5

A triangle has three basic parts: three sides and three interior angles (and three vertices). An internal triangle inside another figure is still a triangle, so it also has three interior angles. Since the question is asking for how many elements are in the internal triangle, the count is three.

6. Which term describes measures aimed at detecting and gathering information about the electromagnetic environment to support operations?

- A. Electronic Counter Measures
- B. Electronic Protective Measures
- C. Electronic Support Measures**
- D. Electronic Attack Measures

The main idea here is recognizing the function of Electronic Support Measures. These are the activities that detect and gather information about the electromagnetic environment to support operations. This involves listening for and analyzing signals from radars, communications, and other emitters to understand their type, capabilities, location, and intent. This information boosts situational awareness, threat assessment, and planning, without actively interfering with the signals. As a contrast, other terms describe different parts of electronic warfare: Electronic Attack Measures use electromagnetic energy to degrade or deny enemy systems; Electronic Protective Measures focus on safeguarding our own systems from such effects; Electronic Counter Measures actively disrupt or deceive enemy EM systems.

7. What sequence best describes how stations should rejoin after a pause?

- A. End the net immediately.
- B. Switch to a backup frequency without notification.
- C. Net Control calls for rejoin; stations respond with their call sign; channel is verified clear; traffic resumes.**
- D. All stations must wait until a supervisor approves.

Rejoining after a pause requires an orderly reintegration under the control of Net Control. The best sequence is for Net Control to call for rejoin, stations to respond with their call signs, Net Control to verify the channel is clear, and then traffic to resume. This ensures Net Control knows who is present, prevents stations from talking over each other by confirming the channel is free, and provides a clean moment for everyone to listen and resume transmissions in an organized way. Ending the net immediately, switching to a backup frequency without notification, or waiting for some supervisor approval would disrupt the flow, cause confusion, or add unnecessary delays.

8. Which of the following is a defence against enemy deception?

- A. Authentication**
- B. Good procedures
- C. Constant vigilance
- D. Encryption

Authentication defends against enemy deception by confirming who is sending a message and that it originates from a trusted source. Using methods like shared secrets, call signs, challenge-response, or digital signatures lets the receiver verify identity and reject impersonations or spoofed commands. Good procedures help reduce the opportunities for deception, but they don't on their own prove who is talking. Constant vigilance is important for spotting anomalies, yet without a mechanism to verify identity, deceptive signals can still appear legitimate. Encryption protects the content of a message from being read by others, but it doesn't by itself verify who sent it (unless paired with authentication mechanisms like digital signatures).

9. Does a transmission ending with 'Out' or 'Out to you' require a reply?

- A. True
- B. False**
- C. Depends
- D. Not sure

In radio communications, ending a transmission with "Out" or "Out to you" signals that you are finished speaking and do not expect a reply. It's the opposite of ending with "Over," which indicates you're awaiting a response. So, when you hear or say "Out," you're closing the conversation on that channel. The nuance you might hear elsewhere is that "Out" can feel abrupt, but it's the standard cue that no further transmission is requested. If you need to get a reply, you would use or wait for a turn marked by "Over" instead.

10. Why is having pre-planned frequencies and fallback channels important, and how is this information communicated to participants?

A. Ensures redundancy; reduces downtime; Documented in a frequency plan; distributed to all participants via training and published SOPs.

B. Frequencies are chosen on the fly; fallback channels unnecessary.

C. Frequency plans are kept secret from participants.

D. Fallback channels are not tested during training.

Having pre-planned frequencies and fallback channels provides redundancy so operations can continue smoothly if the primary link fails. A frequency plan lays out which channels are primary and which are backups, along with the rules for when to switch and any timing or interference considerations. Communicating this plan to participants through training and published standard operating procedures ensures everyone knows exactly what to tune to and how to switch without hesitation. Relying on on-the-fly choices wastes time and can cause confusion, while keeping fallback details secret or skipping tests during training leaves teams unprepared when a failure occurs.

SAMPLE

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://radiocommsnetssecurityprocedures.examzify.com>

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

SAMPLE