RIPE BORDER GATEWAY PROTOCOL (BGP) SECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ripebgpsecurity.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 16

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What are typical ROA validation statuses and how should each influence route acceptance?

A. Valid – accept and may prefer; Invalid – reject or deprioritize; Unknown/Not Found – follow policy (often accept with caution or reject).

B. Valid – reject; Invalid – accept; Unknown – ignore.

C. Invalid – accept; Unknown – reject; Valid – drop.

D. Valid – log; Invalid – log; Unknown – log.

2. What is a BGP Update message?

A. Only Withdrawn Routes

B. Advertises feasible routes, withdrawn routes and both. The Update message contains: NLRI, Path Attributes, and withdrawn routes or destination prefixes/lengths that have become unreachable.

C. Contains Only NLRI

D. Contains Open Messages and Keepalive Fields

3. Differentiate route leaks from route hijacks with examples.

A. Route leaks are misconfig-driven dissemination of prefixes within/among ASes; route hijacks are unauthorized announcements by a rogue AS.

B. Route leaks are deliberate blocking of routes; route hijacks are accidental misrouting.

C. Route leaks occur only at IXPs; route hijacks only involve peering.

D. Route leaks and route hijacks are the same thing.

4. Which statement about BGP prefix filtering strategies is true?

A. Prefix-lists are used to enforce explicit allow/deny rules for prefixes.

B. Prefix-lists carry ROA data in the BGP update.

C. Prefix-lists auto-generate BGP Communities.

D. Prefix-lists determine the MED value for routes.

5. What information is contained in an Open message?

A. Version, My Autonomous System, Hold Time, Router ID and Optional Parameters such as Session Authentication

B. NLRI, Withdrawn Routes

C. Version, MD5 Checksum, Path Attributes

D. Next Hop, AS Path, MED

SAMPLE

6. Which statement about keepalive messages in BGP is true?

A. BGP does not use keepalive messages.

B. BGP uses keepalive messages, but only in the initial adjacency setup.

C. BGP uses keepalive messages similar to those of OSPF and EIGRP.

D. BGP uses periodic hello messages instead of keepalives.

7. What is a typical outcome of misconfigured export policies and what mitigations help?

A. Exports leak routes to intended neighbors.

B. Export policies are irrelevant.

C. Export policies erroneously share routes with unintended neighbors; mitigations include strict filtering, staging tests, and monitoring.

D. Export policies cause BGP to crash.

8. Which address type is commonly used in the BGP neighbor command for iBGP sessions?

A. The MAC address of the neighbor's interface

B. The router ID

C. A loopback address is generally used in the BGP neighbor command

D. A multicast address

9. Which command enters BGP configuration mode?

A. Router bgp autonomous-system in global config

B. Router bgp in global config

C. bgp config enter

D. Enable BGP in interface mode

10. Which event occurs in the open confirm state?

A. The router received agreement on the parameters for establishing a session.

B. An open message was sent with the parameters for the BGP session.

C. The router found a route to the neighbor and has completed the three-way handshake.

D. Peering is established and routing begins.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What are typical ROA validation statuses and how should each influence route acceptance?

A. Valid – accept and may prefer; Invalid – reject or deprioritize; Unknown/Not Found – follow policy (often accept with caution or reject).

B. Valid – reject; Invalid – accept; Unknown – ignore.

C. Invalid – accept; Unknown – reject; Valid – drop.

D. Valid – log; Invalid – log; Unknown – log.

ROA validation statuses guide how to treat each BGP route. If a route is Valid, that prefix and AS are explicitly authorized by the ROA, so the route should be accepted and often given favorable routing priority. If a route is Invalid, the origin is not covered by any valid ROA for that prefix, so it should be rejected or deprioritized to protect against misoriginations or potential hijacks. If the status is Unknown or Not Found (no ROA entry for that prefix), there isn't enough validation evidence; handling this depends on policy—many operators either accept with caution or reject, rather than treating Unknown as simply inconsequential. The core idea is: Valid = trust and accept; Invalid = do not trust (reject or deprioritize); Unknown = policy-driven, potentially degrade or monitor.

2. What is a BGP Update message?

A. Only Withdrawn Routes

B. Advertises feasible routes, withdrawn routes and both. The Update message contains: NLRI, Path Attributes, and withdrawn routes or destination prefixes/lengths that have become unreachable.

C. Contains Only NLRI

D. Contains Open Messages and Keepalive Fields

A BGP Update message is how two peers tell each other about changes in reachability. It can carry two kinds of information: routes that are being withdrawn and routes that are being announced or updated. The Update payload is structured to include the withdrawn routes first, then the Path Attributes that describe how to reach those routes, and finally the NLRI for the routes being advertised. If there are withdrawals, they appear in the Withdrawn Routes section; if there are new or updated routes, their prefixes appear in the NLRI section along with the necessary path attributes. It can do both in one message, or contain only withdrawals or only announcements if needed. Open messages and Keepalive messages are separate types used to manage the session, not Update messages. So the description that an Update message advertises feasible routes, withdrawn routes and both, and contains NLRI, Path Attributes, and withdrawn routes, is the best fit.

SAMPLE

3. Differentiate route leaks from route hijacks with examples.

A. Route leaks are misconfig-driven dissemination of prefixes within/among ASes; route hijacks are unauthorized announcements by a rogue AS.

B. Route leaks are deliberate blocking of routes; route hijacks are accidental misrouting.

C. Route leaks occur only at IXPs; route hijacks only involve peering.

D. Route leaks and route hijacks are the same thing.

Route leaks happen when routing information is shared beyond what was intended, usually due to a misconfiguration or policy mistake. This means prefixes owned by one party become visible or usable by other parts of the Internet or by other providers, not because someone is trying to do harm, but because the way routes are learned and redistributed was incorrect. For example, a network might learn a customer's prefix via an internal iBGP session and, because a route-policy or filter is misconfigured, advertise it to another provider. That unintended advertisement makes the prefix reachable through paths it shouldn't be, leading to suboptimal or unintended traffic flows. Another common case is a provider leaking routes learned from one downstream peer to another provider, broadening the visibility of prefixes that should be contained within a limited scope. Route hijacks, on the other hand, involve unauthorized announcements of prefixes by an AS that does not own them. This is about misrepresentation of ownership to attract traffic to the attacker's network, often with malicious intent. A classic example is an ASN announcing prefixes it does not own, causing traffic destined for those prefixes to route toward the rogue network. The traffic can then be intercepted, dropped, or altered. A well-known real-world instance was an incident where a route announcement caused global traffic to be misrouted through a provider's network, enabling interception of the intended destination. So, the key distinction is authorization: leaks are unintended disclosures of legitimate prefixes due to misconfiguration, while hijacks are intentional or fraudulent announcements by an actor asserting ownership of prefixes they do not own.

4. Which statement about BGP prefix filtering strategies is true?

A. Prefix-lists are used to enforce explicit allow/deny rules for prefixes.

B. Prefix-lists carry ROA data in the BGP update.

C. Prefix-lists auto-generate BGP Communities.

D. Prefix-lists determine the MED value for routes.

Prefix filtering with BGP relies on prefix-lists to enforce explicit allow/deny rules for prefixes. A prefix-list defines which prefixes (and optionally which prefix lengths) are permitted or denied, and when you apply that list to a BGP session—often through a route-map—you control which routes are accepted into your BGP table or which routes you advertise to a neighbor. This explicit allow/deny mechanism is the core purpose of prefix-lists in BGP policy. ROA data isn't carried in BGP updates. ROA information comes from RPKI validation and is used to verify that a route's origin is legitimate; it isn't transmitted as part of BGP update attributes. That's why a statement claiming prefix-lists carry ROA data isn't correct. Prefix-lists don't auto-generate BGP Communities. Communities are a separate BGP attribute that can be assigned or modified by policy (often via route-maps), but not produced merely by a prefix-list. Prefix-lists don't determine the MED value. MED is a BGP path attribute and can be set or altered by policy to influence path selection, typically via route-maps, not by the prefix-list itself. So, the statement that prefix-lists are used to enforce explicit allow/deny rules for prefixes is the accurate description.

SAMPLE

5. What information is contained in an Open message?

A. Version, My Autonomous System, Hold Time, Router ID and Optional Parameters such as Session Authentication

B. NLRI, Withdrawn Routes

C. Version, MD5 Checksum, Path Attributes

D. Next Hop, AS Path, MED

In BGP, the Open message is used to establish the session and negotiate the basic parameters for communication. The essential pieces it carries are the protocol version, the sender's Autonomous System number, the hold time (the maximum allowed time between messages before the session is considered down), and the router ID that uniquely identifies the speaker. It also includes a block of Optional Parameters, which can carry extra negotiation data such as capabilities or authentication options. This combination lets the two peers agree on who they are, how long they'll wait between messages, and what capabilities they'll use before any routes are exchanged. Route information itself does not go in the Open message. The actual route announcements and withdrawals, along with their path attributes like Next Hop, AS Path, and MED, travel in Update messages. The MD5 or other session authentication mechanism is tied to the TCP layer, not the Open message, though Optional Parameters can carry additional negotiation data in some contexts.

6. Which statement about keepalive messages in BGP is true?

A. BGP does not use keepalive messages.

B. BGP uses keepalive messages, but only in the initial adjacency setup.

C. BGP uses keepalive messages similar to those of OSPF and EIGRP.

D. BGP uses periodic hello messages instead of keepalives.

The main idea is that BGP keeps an established session alive with periodic heartbeat messages known as KEEPALIVE. Once two BGP peers have completed the OPEN exchange and the TCP connection is up, they exchange UPDATE messages as routing information and periodically send KEEPALIVE messages to prove the connection is still healthy. The interval is tied to the configured hold time—the peer must see activity (any BGP message, including KEEPALIVE) within that window, or the session is considered down. This heartbeat concept serves the same purpose as the periodic liveness checks in other protocols like OSPF and EIGRP, even though BGP does not use Hello messages in the same way. So, describing BGP as using keepalive messages similar to those protocols best captures how liveness is maintained for the session. It's not only during initial setup, and it isn't about periodic Hello messages in BGP.

SAMPLE

7. What is a typical outcome of misconfigured export policies and what mitigations help?

A. Exports leak routes to intended neighbors.

B. Export policies are irrelevant.

C. Export policies erroneously share routes with unintended neighbors; mitigations include strict filtering, staging tests, and monitoring.

D. Export policies cause BGP to crash.

Export policies determine which routes a BGP speaker will advertise to each neighbor. When these policies are misconfigured, routes can be exported to neighbors that shouldn't see them, leading to leakage of prefixes and potentially exposing customer networks or altering traffic flows. That's why the described outcome—sharing routes with unintended neighbors—is the typical risk. Mitigations include strict filtering to limit what gets exported to each peer, staging tests in a controlled environment before deployment, and ongoing monitoring and auditing of route advertisements to catch and correct leaks quickly. In practice, you'd implement precise prefix-lists or route-maps to constrain exports, test policies in a lab, and use monitoring tools or route collectors to detect anomalies. Other possibilities like leaks to intended neighbors, irrelevance of export policies, or BGP crashes are not the typical, expected outcomes of misconfigurations.

8. Which address type is commonly used in the BGP neighbor command for iBGP sessions?

A. The MAC address of the neighbor's interface

B. The router ID

C. A loopback address is generally used in the BGP neighbor command

D. A multicast address

In iBGP peering, using a loopback address for the neighbor is the common practice because it gives you a stable, always-up endpoint for the BGP TCP session. Loopbacks are logical interfaces that remain up regardless of the state of any physical link, so the peering plane isn't as prone to flapping if a router interface goes down or is reconfigured. To make this work, you typically ensure reachability to the neighbor's loopback (via IGP or static routes) and configure the session to source from the loopback on both sides (often using update-source loopback). This combination keeps the session reliable and predictable. Other address types don't fit as well for this purpose. A MAC address is a layer 2 construct and isn't used to establish BGP sessions, which run over IP/TCP. The router ID is a unique identifier for BGP itself, not the address used to form a neighbor relationship. A multicast address isn't appropriate for unicast BGP peering, which relies on a specific unicast IP path.

9. Which command enters BGP configuration mode?

A. Router bgp autonomous-system in global config

B. Router bgp in global config

C. bgp config enter

D. Enable BGP in interface mode

In BGP on most IOS devices, you enter BGP configuration mode from global configuration mode by issuing the command router bgp <AS-number>. This places you into the BGP router configuration context where you define neighbors, networks, route maps, and policies. The option that matches this practice uses the router bgp syntax with the autonomous system number specified inside global config, which is why it's the best choice. The other options aren't valid: there is no bgp config enter command, you don't enable BGP from interface mode, and simply typing router bgp without the AS number isn't the correct way to enter BGP configuration in most environments.

SAMPLE

10. Which event occurs in the open confirm state?

A. The router received agreement on the parameters for establishing a session.

B. An open message was sent with the parameters for the BGP session.

C. The router found a route to the neighbor and has completed the three-way handshake.

D. Peering is established and routing begins.

OpenConfirm is reached after the BGP OPEN messages have been exchanged and the parameters are being checked and agreed upon by both sides. The key event in this state is that the router has received the neighbor's OPEN and validated the session parameters (version, AS numbers, hold time, etc.). Once that agreement is established, the session exchanges a KEEPALIVE to move toward Established, where actual routing updates begin. So the event described—receiving agreement on the parameters for establishing a session—is what defines OpenConfirm. The other events occur earlier (sending your OPEN) or later (peering and routing begin once Established), or relate to the underlying TCP connection rather than the BGP parameter negotiation.

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://ripebgpsecurity.examzify.com

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

SAMPLE