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

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. The number of BGP network commands that can be added to a router is based on what?

A. A fixed limit defined by the protocol

B. Based on RAM/NVRAM

C. Equal to number of BGP neighbors

D. Unlimited

2. What is TTL Security Mechanism (TTLS) in BGP and what threat does it mitigate?

A. TTLS relays BGP sessions through TTL proxies to enhance security.

B. TTLS enables route filtering using TTL-based path vector.

C. TTLS encrypts BGP updates based on TTL.

D. TTLS requires TTL=1 for eBGP sessions; it mitigates remote spoofed connections attempting to form BGP sessions.

3. Name the three well-known mandatory attributes.

A. AS path, Next Hop, Origin

B. Local Preference, Atomic Aggregate, Community

C. Aggregator, Community, Next Hop

D. Origin, Local Preference, AS Path

4. What fields does an Update message contain?

A. Withdrawn Routes, Path Attributes and Network Layer Reachability Information

B. Version, Hold Time, Router ID

C. AS Path, Next Hop, Community

D. NLRI Only

5. What is TCP-MD5 and when should you enable it on BGP sessions?

A. TCP-MD5 is used to encrypt the BGP TCP session with a shared secret.

B. TCP-MD5 authenticates the BGP TCP session with a shared secret; enable in untrusted networks or where spoofing risk is high.

C. TCP-MD5 signs BGP messages at application layer.

D. TCP-MD5 ensures fast convergence of BGP.

6. Which attributes are considered optional transitive?

A. Aggregator and Community

B. Local Preference and Atomic Aggregate

C. AS Path and Origin

D. Next Hop and Origin

7. Which statement best describes the established state outcome?

A. Peering is established and routing begins.

B. The IP addresses are added to the IGP.

C. The BGP table is reset.

D. An update is rejected.

8. In the iBGP example, which command configures the neighbor 172.16.23.2 with remote-as 65000?

A. R3 (config)# router bgp 65000; R3 (config-router)# neighbor 172.16.23.2 remote-as 65000

B. R2 (config)# router bgp 65000; R2 (config-router)# neighbor 172.16.23.2 remote-as 65000

C. R3 (config)# router bgp 65000; R3 (config-router)# neighbor 172.16.23.2 remote-as 65001

D. R3 (config)# router bgp 65001; R3 (config-router)# neighbor 172.16.23.2 remote-as 65000

9. Which tools and data sources are commonly used to study historical BGP security incidents?

A. Packet traces.

B. DNS logs and web server access logs.

C. Firewall logs only.

D. RouteViews, RIPE RIS, BGPmon, Looking Glass, and public incident reports.

10. What is Local Preference (LOCAL_PREF) and how can it influence security-related routing decisions?

A. External attribute used by all peers to choose routes.

B. Internal attribute to prefer certain exit points; use to avoid untrustworthy peers or links.

C. Attribute that governs MED across multiple providers.

D. Deprecated attribute with no routing impact.

Answers

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

Explanations

1. The number of BGP network commands that can be added to a router is based on what?

A. A fixed limit defined by the protocol

B. Based on RAM/NVRAM

C. Equal to number of BGP neighbors

D. Unlimited

The number of BGP network statements you can configure on a router is determined by the device's memory resources. These statements are stored in the router's configuration data (RAM as the running-config and NVRAM for the startup-config), and the BGP process must keep track of them and potentially advertise them. Since the protocol itself imposes no fixed cap on how many network statements there can be, the practical limit comes from how much RAM/NVRAM is available. It's not limited by the number of neighbors, and it isn't unlimited in real hardware.

2. What is TTL Security Mechanism (TTLS) in BGP and what threat does it mitigate?

A. TTLS relays BGP sessions through TTL proxies to enhance security.

B. TTLS enables route filtering using TTL-based path vector.

C. TTLS encrypts BGP updates based on TTL.

D. TTLS requires TTL=1 for eBGP sessions; it mitigates remote spoofed connections attempting to form BGP sessions.

TTL Security Mechanism uses the IP TTL field to bind a BGP session to the directly connected neighbor, so the router only accepts BGP TCP connections that come from a one-hop path. By configuring the session to require a TTL value of 1, any attempt to form a BGP session from a remote network (i.e., more than one hop away) is dropped, because the packet would have traversed at least one router and its TTL would not match the expected value. This significantly reduces the risk of remote spoofed connections where an attacker tries to impersonate a neighbor by forging the source IP to hijack or misrepresent routes. TTLS does not encrypt BGP updates, nor does it involve TTL proxies or a TTL-based path vector; its purpose is specifically to guard against spoofed, non-direct-neighbor session attempts by leveraging the hop-count constraint.

3. Name the three well-known mandatory attributes.

A. AS path, Next Hop, Origin

B. Local Preference, Atomic Aggregate, Community

C. Aggregator, Community, Next Hop

D. Origin, Local Preference, AS Path

In BGP, three attributes are required in every route update because they provide essential, universally-needed information about how the route arrived and how to reach it. The AS_PATH lists the sequence of autonomous systems the route has traversed. This helps prevent routing loops and supports policy decisions because you can see the path the update took across the Internet. The NEXT_HOP tells you the IP address of the next router to reach the destination; without this, a router wouldn't know where to forward the packets. The ORIGIN attribute indicates how the route was learned—whether from an internal IGP, an external EGP, or if the origin is incomplete—so a router can make informed decisions when comparing multiple paths. The other attributes mentioned—Local Preference, Atomic Aggregate, Community, and Aggregator—are useful for shaping routing policies and route handling, but they're not required to be present on every update. Local Preference is a local policy knob within an AS, Atomic Aggregate and Aggregator relate to how routes are summarized or who performed aggregation, and Community is a tagging mechanism for policy purposes.

4. What fields does an Update message contain?

A. Withdrawn Routes, Path Attributes and Network Layer Reachability Information

B. Version, Hold Time, Router ID

C. AS Path, Next Hop, Community

D. NLRI Only

An Update message in BGP communicates changes to the routing table. It consists of three parts: Withdrawn Routes (prefixes to remove), Path Attributes (metadata like AS_PATH, NEXT_HOP, ORIGIN, etc.), and NLRI (the new or announced prefixes). Withdrawn Routes removes previously advertised paths, Path Attributes apply to the routes being announced, and NLRI lists the prefixes that are now reachable. The Version, Hold Time, and Router ID belong to the OPEN message, not Update, and an Update message is not just NLRI alone.

5. What is TCP-MD5 and when should you enable it on BGP sessions?

A. TCP-MD5 is used to encrypt the BGP TCP session with a shared secret.

B. TCP-MD5 authenticates the BGP TCP session with a shared secret; enable in untrusted networks or where spoofing risk is high.

C. TCP-MD5 signs BGP messages at application layer.

D. TCP-MD5 ensures fast convergence of BGP.

TCP-MD5 secures the BGP session by authenticating the underlying TCP connection with a shared secret. It adds an MD5-based hash to TCP segments so both peers can verify that the other side knows the secret, preventing unauthorized peers from establishing or hijacking the BGP session. It does not encrypt BGP messages or sign them at the application layer, so confidentiality and per-message integrity beyond the TCP connection aren't provided by TCP-MD5 itself. Enable TCP-MD5 when the route between peers traverses untrusted networks or there is a higher risk of spoofing, such as across the public Internet or between operators with potential misconfigurations. Configuration requires sharing the same secret on both ends; if the secret mismatches or one side doesn't support it, the session will fail to establish. In short, TCP-MD5 protects the integrity of the TCP session used by BGP, not the content of BGP messages themselves, and is most useful where the risk of spoofed TCP connections is nontrivial.

6. Which attributes are considered optional transitive?

A. Aggregator and Community

B. Local Preference and Atomic Aggregate

C. AS Path and Origin

D. Next Hop and Origin

In BGP, path attributes are categorized by whether they are well-known or optional, and by whether they are transitive or non-transitive. Optional transitive attributes are those that aren't required to be understood by every router, but must be forwarded to the next hop along the path so that routers that do understand them can use them. Aggregator is an optional transitive attribute. It carries information about the router that performed an aggregation and the origin of the route. If a neighbor doesn't understand this attribute, it should still forward the update to the next router; if it does understand it, it can use the data for policy or troubleshooting. Community is also an optional transitive attribute. It provides a tagging mechanism to influence routing policies across multiple ASes. Networks commonly propagate communities even when downstream routers don't interpret every value, preserving the information for those that do. Other attributes listed aren't optional transitive. Some are well-known and must be understood by all routers (like AS_PATH and Origin, and Next Hop). Local Preference is a well-known discretionary attribute that is intended for use within a single AS and is not forwarded across AS boundaries. Atomic Aggregate is an optional attribute that is not transitive, so it doesn't fit the category of optional transitive.

7. Which statement best describes the established state outcome?

A. Peering is established and routing begins.

B. The IP addresses are added to the IGP.

C. The BGP table is reset.

D. An update is rejected.

In BGP, when the session with a neighbor reaches the Established state, peering is up and routing information can flow between the peers. This means OPEN messages were exchanged successfully, the TCP session is stable, and both sides are ready to exchange UPDATE messages. Once in this state, routes learned from the neighbor are announced and, after the decision process, can be installed into the local routing table, so actual routing can begin. The other statements don't describe the Established state. Adding IP addresses to the IGP isn't part of the BGP session becoming established—IGP operates separately. The BGP table reset happens if the session drops or restarts, not when it's established. An update being rejected can occur for various reasons, but it isn't the defining outcome of entering the Established state.

8. In the iBGP example, which command configures the neighbor 172.16.23.2 with remote-as 65000?

A. R3 (config)# router bgp 65000; R3 (config-router)# neighbor 172.16.23.2 remote-as 65000

B. R2 (config)# router bgp 65000; R2 (config-router)# neighbor 172.16.23.2 remote-as 65000

C. R3 (config)# router bgp 65000; R3 (config-router)# neighbor 172.16.23.2 remote-as 65001

D. R3 (config)# router bgp 65001; R3 (config-router)# neighbor 172.16.23.2 remote-as 65000

In iBGP, peers must reside in the same autonomous system, so the local BGP process is started with the same AS as the neighbor, and the neighbor statement uses remote-as equal to that AS. Configuring router bgp 65000 on the local router and then setting neighbor 172.16.23.2 remote-as 65000 tells the router that the neighbor is in the same AS and should be treated as an iBGP neighbor. That alignment of the local AS and the neighbor's remote-as is what makes this the correct setup. The other options would misalign the AS numbers—either using a different local AS (which would indicate eBGP) or using a different remote-as value (which would not establish an iBGP session with AS 65000). The essential point is matching the local BGP process AS with the remote-as of the neighbor for iBGP.

9. Which tools and data sources are commonly used to study historical BGP security incidents?

A. Packet traces.

B. DNS logs and web server access logs.

C. Firewall logs only.

D. RouteViews, RIPE RIS, BGPmon, Looking Glass, and public incident reports.

Studying historical BGP security incidents relies on data that directly captures how routing announcements changed over time across the internet. RouteViews and RIPE RIS are essential because they are large, multi-peer repositories of BGP updates and withdrawals from many networks, providing a time-stamped record of which prefixes were advertised and by whom. Looking Glass services let researchers query how different networks are perceiving routes at particular moments, offering additional perspectives on the routing state from various vantage points. BGPmon adds monitoring and alerting for BGP events, helping to detect and reconstruct incidents with a focus on anomalies and timelines. Public incident reports, including operator write-ups and CERT advisories, give narrative context, confirm specifics like affected prefixes and regions, and help validate findings. This combination is what makes it possible to piece together how an incident unfolded, when it started, who was involved, and how the routing state evolved across the internet. In contrast, packet traces focus on traffic flow at specific points and don't provide the global, historical view of BGP announcements; DNS logs and web server logs track domain resolution and application activity, not routing changes; firewall logs capture boundary security events but not the underlying BGP dynamics.

10. What is Local Preference (LOCAL_PREF) and how can it influence security-related routing decisions?

A. External attribute used by all peers to choose routes.

B. Internal attribute to prefer certain exit points; use to avoid untrustworthy peers or links.

C. Attribute that governs MED across multiple providers.

D. Deprecated attribute with no routing impact.

Local Preference is an internal BGP path attribute used to decide which exit point your AS should use when sending traffic to a destination. Routers within the same autonomous system compare the LOCAL_PREF values for candidate routes and pick the one with the highest value. Because it is local to the AS, this attribute isn't advertised to external neighbors—it's a tool for controlling outbound routing from inside your network. This makes Local Preference a practical lever for security-related routing decisions. By assigning higher LOCAL_PREF to routes that go through trusted, monitored, or reliable exit points, you push traffic to leave your AS via those preferred paths. Conversely, you can lower the value for routes that traverse untrustworthy or less secure links, effectively steering traffic away from them. In short, it helps you avoid paths that could be compromised or unreliable, reducing exposure to interception or manipulation of outbound traffic. It's important to distinguish this from other attributes: Local Preference is internal to the AS and not shared with other ASes, whereas features like MED are used to influence inbound traffic and involve external neighbors. And Local Preference is not a deprecated feature; it remains a standard tool for routing policy and security-focused control of egress paths.

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!