MTCNA FOUNDATION DECK PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://mtcnafoundationdeck.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. Which component controls WinBox MAC connection availability on interfaces?

A. Neighbors Discovery

B. MAC Server

C. IP Services

D. Logs

2. Which tool shows the path packets travel to a destination?

A. Traceroute

B. Torch

C. Bandwidth Test

D. Packet Sniffer

3. How do you check the current time synchronization status with NTP?

A. /system ntp client enable

B. /system ntp client status

C. /system ntp client print or /system clock print to verify time

D. /system clock set

4. Which tool is used to mark packets or connections for routing, QoS, or filtering?

A. Mangle

B. Firewall

C. NAT

D. Masquerade

5. What term describes the next-hop IP used for routing traffic outside the local network?

A. Gateway

B. Distance

C. Firewall

D. NAT

6. Which command implements a basic firewall rule to drop invalid connection state packets?

A. /ip firewall filter add chain=forward connection-state=invalid action=drop

B. /ip firewall filter add chain=forward connection-state=established action=drop

C. /ip firewall filter add chain=input connection-state=invalid action=drop

D. /ip firewall filter add chain=forward connection-state=invalid action=accept

7. Which section lists software modules installed on RouterOS, such as system, wireless, and routing?

A. Packages

B. Health

C. License

D. Neighbors Discovery

8. Which MikroTik command deletes a firewall filter rule by its list number?

A. /ip firewall filter remove numbers=<number>

B. /ip firewall filter disable numbers=<number>

C. /ip firewall filter print numbers

D. /ip firewall filter remove

9. Which sequence correctly configures the input firewall to accept established/related connections and drop all other traffic?

A. /ip firewall filter add chain=input action=drop; /ip firewall filter add chain=input connection-state=established,related action=accept

B. /ip firewall filter add chain=input protocol=tcp dst-port=80 action=accept

C. /ip firewall filter add chain=input connection-state=established,related action=accept; /ip firewall filter add chain=input action=drop

D. /ip firewall filter add chain=output connection-state=established,related action=accept

10. Which section is described as controlling services such as WinBox, SSH, API, WebFig, and FTP?

A. Neighbors Discovery

B. MAC Server

C. IP Services

D. Files

Answers

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

Explanations

1. Which component controls WinBox MAC connection availability on interfaces?

A. Neighbors Discovery

B. MAC Server

C. IP Services

D. Logs

WinBox can connect to a MikroTik device over IP or directly via a MAC-level path. The MAC Server is the component that handles those MAC-based WinBox connections, controlling which interfaces will accept them. This lets you manage the device even when IP isn't configured or reachable, by enabling the MAC WinBox access on the desired interfaces. The other options don't manage MAC WinBox connections: Neighbors Discovery is about discovering devices on the network, IP Services deals with IP-based management endpoints, and Logs only records events.

2. Which tool shows the path packets travel to a destination?

A. Traceroute

B. Torch

C. Bandwidth Test

D. Packet Sniffer

To understand how data moves to a destination, you need visibility into the path the packets take. A traceroute shows each hop along the route from your device to the target, along with the time it takes to reach each hop. It works by sending probes with small, gradually increasing time-to-live values. When a router along the path receives a probe with an expired TTL, it sends back a reply (often ICMP Time Exceeded), and your system records that router's address and the round-trip time. The result is a hop-by-hop map of the route and the latency to each hop, which helps pinpoint where delays or failures occur. Other tools focus on different aspects: a packet sniffer captures and analyzes the contents of packets at a point in time but doesn't reveal the route to the destination; a bandwidth test measures the throughput between endpoints rather than the path taken; a tool like Torch analyzes live traffic on an interface but doesn't enumerate the route to a destination.

3. How do you check the current time synchronization status with NTP?

A. /system ntp client enable

B. /system ntp client status

C. /system ntp client print or /system clock print to verify time

D. /system clock set

To check time synchronization, you want to see what the NTP client is doing and what time the system has. In MikroTik RouterOS, you can quickly verify this by printing the NTP client status; it shows whether the client is enabled, which NTP servers are in use, and whether it is currently synchronized. For an extra check, you can print the system clock to see the actual time the device is reporting. Together, these commands confirm both the synchronization status and the current time. Enabling the NTP client or setting the clock are actions, not checks, which is why they don't directly answer the question about current synchronization status.

4. Which tool is used to mark packets or connections for routing, QoS, or filtering?

A. Mangle

B. Firewall

C. NAT

D. Masquerade

Marking packets for routing, QoS, or filtering is accomplished by using the mangle feature of the firewall. A mangle rule assigns a packet or connection mark to traffic, and that mark travels with the packet. Those marks then guide later decisions: routing can use routing marks to pick a path, QoS can classify and shape traffic based on packet marks, and filtering can apply rules or drive NAT decisions using the marks. Other tools like firewall rules, NAT, or masquerade handle filtering or address translation themselves, but they don't provide the labeling mechanism that makes policy-based routing, QoS, and filtering possible.

5. What term describes the next-hop IP used for routing traffic outside the local network?

A. Gateway

B. Distance

C. Firewall

D. NAT

Gateway. The next-hop IP used to reach destinations outside the local subnet is the gateway, usually the router's address on your LAN. When a device needs to send traffic to a network beyond its own subnet, it forwards the packet to this gateway, which then routes it onward. This is often configured as the default gateway on hosts. The other terms don't describe this role: distance is a routing metric, firewall is a security device, and NAT translates addresses for outbound traffic.

6. Which command implements a basic firewall rule to drop invalid connection state packets?

A. /ip firewall filter add chain=forward connection-state=invalid action=drop

B. /ip firewall filter add chain=forward connection-state=established action=drop

C. /ip firewall filter add chain=input connection-state=invalid action=drop

D. /ip firewall filter add chain=forward connection-state=invalid action=accept

Dropping packets that have an invalid connection state is a common first-step in a stateful firewall. The command shown applies to traffic that is being forwarded through the router (not traffic destined for the router itself) by using the forward chain. It targets packets whose connection-tracking state is invalid—these are not part of any known, established connection and often indicate spoofing, misconfiguration, or malformed traffic. By setting the action to drop, these suspicious packets are discarded immediately, strengthening security without affecting legitimate traffic. Dropping such packets in the forward chain is preferable to dropping established traffic, which would disrupt valid connections, or to using the input chain, which would apply to traffic destined for the router itself rather than transit traffic. Accepting invalid state would permit potentially harmful traffic to pass through.

7. Which section lists software modules installed on RouterOS, such as system, wireless, and routing?

A. Packages

B. Health

C. License

D. Neighbors Discovery

In RouterOS, the set of software modules installed on the device is shown in the Packages section. Each package corresponds to a group of features, such as system, wireless, or routing, so this is where you can see exactly which modules are present and what version they're at. This view is also where you'd manage those modules (enable/disable or update as needed, noting that some changes require a reboot to take effect). The other sections serve different purposes: Health reports device status and performance metrics, License shows the licensing state, and Neighbors Discovery lists devices found on the network. None of these display the installed software modules like the Packages section does.

8. Which MikroTik command deletes a firewall filter rule by its list number?

A. /ip firewall filter remove numbers=<number>

B. /ip firewall filter disable numbers=<number>

C. /ip firewall filter print numbers

D. /ip firewall filter remove

The command to delete a firewall filter rule by its list number uses the remove action with the numbers parameter. When you print the rules, each one gets a numeric index (its list number). By giving that index to remove, you target exactly that rule and delete it from the list. This is the direct way to remove a specific rule without affecting others. Disabling a rule also uses the numbers parameter, but it only deactivates the rule while keeping it in place. Printing just shows the rules and their numbers without changing anything. Using remove without specifying numbers wouldn't target a rule by its list position (it would require a separate identifier), so it wouldn't accomplish deleting by the list number.

9. Which sequence correctly configures the input firewall to accept established/related connections and drop all other traffic?

A. /ip firewall filter add chain=input action=drop; /ip firewall filter add chain=input connection-state=established,related action=accept

B. /ip firewall filter add chain=input protocol=tcp dst-port=80 action=accept

C. /ip firewall filter add chain=input connection-state=established,related action=accept; /ip firewall filter add chain=input action=drop

D. /ip firewall filter add chain=output connection-state=established,related action=accept

Stateful filtering: allow established or related connections on the input path, then drop everything else. This approach relies on connection tracking so the device can recognize ongoing conversations and permit their traffic even as new attempts are blocked. The correct configuration does exactly that: it first accepts input traffic for connections that are already established or related to an existing connection, and only afterward does it drop any other input. This order is crucial because if the drop rule runs first, it will block even legitimate responses to existing connections. Why this works well here: the input chain handles traffic destined for the device itself, so you want to permit the continuation of existing conversations while denying new, unapproved attempts. A final catch-all drop rule ensures no stray traffic slips through. Contrast with the other approaches: one option drops unmatched input before allowing established/related traffic, which would inadvertently block legitimate connections. Another option accepts only traffic to a specific port and doesn't address the broader need to permit established/related sessions. A rule targeting the output chain doesn't control incoming traffic at all, so it wouldn't achieve the goal of protecting input connections. So the best pattern is to accept established/related on the input chain first, then drop other input traffic.

10. Which section is described as controlling services such as WinBox, SSH, API, WebFig, and FTP?

A. Neighbors Discovery

B. MAC Server

C. IP Services

D. Files

Access to the router's management interfaces is controlled in IP Services. This section defines which management services the device exposes and how they can be accessed, including WinBox, SSH, API, WebFig, and FTP. You can enable or disable each service and restrict which IPs or networks can reach them, as well as set their ports. The other options cover different functions: Neighbors Discovery is about finding other devices on the network, MAC Server is a separate feature not used for managing access, and Files relates to file operations, not management services.

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://mtcnafoundationdeck.examzify.com

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