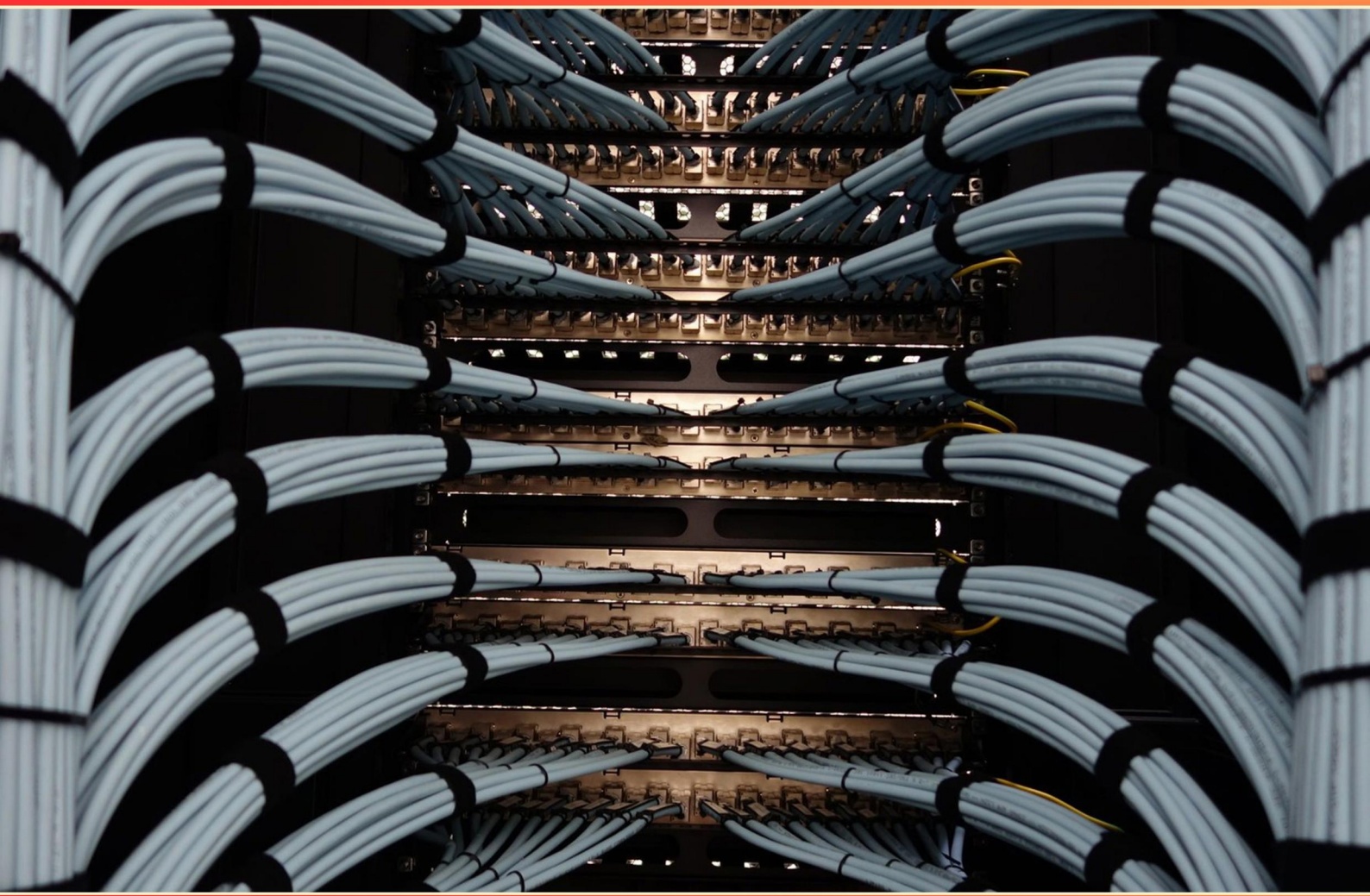
MIKROTIK CERTIFIED NETWORK ASSOCIATE (MTCNA) MODULES PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://mtcnamodules.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. What is TTL?

A. Time to live

B. Time to login

C. Total time latency

D. Time to link

2. Is the order of Access List and Control List rules important?

A. Yes

B. No

C. Sometimes

D. Not specified

3. Where do you specify what type of encryption is used for a PPP based tunnel?

A. Manual selection

B. Highest match between client and server

C. Automatic

D. Default gateway

4. Which statement correctly matches the two RouterOS firewall sections with their chains?

A. Filter uses Forward, Input, Output; NAT uses src-nat, dst-nat

B. Filter uses src-nat, dst-nat; NAT uses Forward, Input, Output

C. Filter uses Masquerade and Jump; NAT uses Source and Destination

D. NAT uses Jump and Return; Filter uses Forward and Drop

5. What are custom chains used for?

A. Organize our rules

B. Increase throughput

C. Encrypt rules

D. Define default routes

6. Which command exports the current configuration to a file named 'config'?

A. /export file=config

B. /export

C. /import file=config

D. /backup save

7. Encryption for a PPP tunnel is configured through which setting?

A. Profile

B. Interface

C. Routing

D. DNS

8. Is a single IP pool allowed to be used for both a PPP based tunnel and DHCP address?

A. No

B. Only for VPN

C. Yes

D. Sometimes

9. Which of the following is a best practice for securing the MikroTik admin account?

A. Use a strong password, disable or restrict the default admin account, and create a separate admin-level user; enable SSH for remote management.

B. Use the default admin account with a short password

C. Disable SSH and use Telnet

D. Share admin credentials among team

10. Which IP prefix is used in a default route?

A. 0.0.0.0/0

B. 255.255.255.0/24

C. 192.168.0.0/16

D. 127.0.0.0/8

Answers

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

Explanations

1. What is TTL?

A. Time to live

B. Time to login

C. Total time latency

D. Time to link

TTL stands for Time to Live. It is a field in the IP header that determines how long a packet is allowed to live in the network, effectively limiting how many hops it can traverse. With each router the value is decreased by one, and when it reaches zero the packet is dropped to prevent endless looping. This behavior also enables network diagnostics like traceroute, which probes paths by sending packets with progressively higher TTL values. Note that TTL is not about time to login, total time latency, or time to link; it's about the maximum number of routers a packet can pass through before being discarded. In IPv6 the concept is similar and is referred to as Hop Limit.

2. Is the order of Access List and Control List rules important?

A. Yes

B. No

C. Sometimes

D. Not specified

The order of Access Lists and Control Lists determines what actually happens to traffic because rules are evaluated in sequence and the first match wins. As a packet is processed, the device checks each rule from top to bottom and applies the action of the first rule that matches. That means where you place a specific deny or permit changes the outcome for many packets. For example, if you want to block a single host but allow others, you must place that block rule before any broader permit rule; otherwise the broad permit might match first and the block would never take effect. There's usually an implicit deny at the end for anything that doesn't match any rule, which reinforces why you must be explicit about what should be allowed. This is why the order is important for implementing the intended traffic policy.

3. Where do you specify what type of encryption is used for a PPP based tunnel?

A. Manual selection

B. Highest match between client and server

C. Automatic

D. Default gateway

PPP-based tunnels establish encryption through negotiation between the two peers. Neither side fixes the algorithm in advance; instead, each end advertises its supported encryption options and the tunnel settles on the strongest common option. That's why encryption is determined by the highest match between client and server—the strongest cipher both sides support is automatically chosen during setup. You can influence the result by configuring what each side allows, but you don't pick a single cipher in the tunnel configuration itself.

4. Which statement correctly matches the two RouterOS firewall sections with their chains?

A. Filter uses Forward, Input, Output; NAT uses src-nat, dst-nat

B. Filter uses src-nat, dst-nat; NAT uses Forward, Input, Output

C. Filter uses Masquerade and Jump; NAT uses Source and Destination

D. NAT uses Jump and Return; Filter uses Forward and Drop

In RouterOS, firewall rules are organized into two sections with different purposes and chain concepts. The Filter section handles general packet filtering and uses the chains that describe where a packet is in its journey: input for traffic destined to the router, forward for traffic passing through the router, and output for traffic generated by the router itself. The NAT section deals with address translation and uses the NAT actions src-nat (source NAT) and dst-nat (destination NAT) to rewrite addresses as packets enter or leave the network. So, the correct pairing is that Filter uses Forward, Input, and Output, while NAT uses src-nat and dst-nat. The other options mix these roles, which doesn't align with how RouterOS structures firewall rules.

5. What are custom chains used for?

A. Organize our rules

B. Increase throughput

C. Encrypt rules

D. Define default routes

Custom chains are a way to organize firewall rules into logical blocks, making complex filtering policies easier to read and manage. In RouterOS, you can put a group of related rules into a single custom chain and use a jump from the main chains (like input or forward) to that chain. The rules inside the custom chain run, then control returns to the main chain. This modular approach lets you reuse and modify a whole set of rules in one place, or apply the same block of rules from multiple places without duplicating them. For example, you could create a custom chain for all VPN-related filtering and jump to it from several interfaces. Then you keep the VPN rules centralized in that chain, keeping the primary chains clean. Custom chains don't increase throughput by themselves, don't encrypt rules, and don't define routes. They're simply a tool for organizing and modularizing policy.

6. Which command exports the current configuration to a file named 'config'?

A. /export file=config

B. /export

C. /import file=config

D. /backup save

Exporting the current configuration to a file is done by using the export command with a file name specified. Running /export file=config writes a script that recreates the current settings into a file named config.rsc on the device. This creates a portable copy you can import later to restore the configuration. If you omit the file parameter, export outputs to the screen instead of saving to a file. Import would read from a file and apply its settings, not create a file. A backup creates a binary backup of the router, not a text config script. So the command that saves the configuration to a file named 'config' is /export file=config.

7. Encryption for a PPP tunnel is configured through which setting?

A. Profile

B. Interface

C. Routing

D. DNS

Encryption for a PPP tunnel is configured through the PPP profile. The profile stores settings that apply to all PPP connections using it, including whether the tunnel data should be encrypted (for example, enabling Use Encryption so the session negotiates MPPE for PPTP). Interfaces, routing, and DNS serve other roles and do not control PPP tunnel encryption. By placing encryption in the profile, you ensure consistent behavior across all PPP clients/servers associated with that profile.

8. Is a single IP pool allowed to be used for both a PPP based tunnel and DHCP address?

A. No

B. Only for VPN

C. Yes

D. Sometimes

IP pools are just ranges of addresses that MikroTik can hand out to clients, and they can be used by multiple services at once. You can configure a PPP profile to take remote addresses from the same pool you've defined for DHCP, so remote PPP clients and LAN clients can both receive addresses from that single pool. This simplifies address management because you're consolidating the available space in one place rather than creating separate pools for every service. The important caveat is to keep the networks on different interfaces in distinct subnets. If the PPP tunnel and the LAN were to operate in the same IP subnet across multiple interfaces, routing and reachability would become problematic. So, with thoughtful IP planning, using one pool for both PPP and DHCP is perfectly workable and commonly done.

9. Which of the following is a best practice for securing the MikroTik admin account?

A. Use a strong password, disable or restrict the default admin account, and create a separate admin-level user; enable SSH for remote management.

B. Use the default admin account with a short password

C. Disable SSH and use Telnet

D. Share admin credentials among team

Securing the MikroTik admin access relies on strong authentication, reducing the chances of unexpected intrusions, and using encrypted remote management. A strong password helps resist brute-force and guessing attacks, making it harder for an attacker to gain entry. The default admin account is a common target, so disabling it or restricting its use lowers the risk of automated login attempts finding the easiest path in. Creating a separate admin-level user lets you manage privileges more flexibly and rotate credentials without depending on a single account, which reduces the impact if one credential is compromised. Enabling SSH for remote management ensures that credentials and commands aren't transmitted in plaintext, unlike older protocols such as Telnet. Together, these practices form a layered defense for admin access. If possible, also restrict SSH access to trusted IPs or a VPN to further minimize exposure, and keep RouterOS updated to patch any known vulnerabilities.

10. Which IP prefix is used in a default route?

A. 0.0.0.0/0

B. 255.255.255.0/24

C. 192.168.0.0/16

D. 127.0.0.0/8

A router uses a catch all route to reach destinations it doesn't have a specific path for, and this catch all is denoted by 0.0.0.0/0. The /0 means "all possible IPv4 addresses," so this single prefix matches every destination and serves as the default path to the next hop when no more specific route exists. The other options don't function as a default route: 255.255.255.0/24 is effectively a subnet designation, not a universal destination prefix; 192.168.0.0/16 is a private local network range; and 127.0.0.0/8 is the loopback range used to reach the device itself. Thus, 0.0.0.0/0 is the correct default route prefix.

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://mtcnamodules.examzify.com

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