|  |
| --- |
| What protocol is used for Ping and Trace Route?  |
|   | DHCP  |
|   | IP  |
|   | ICMP  |
|   | TCP  |
|   | UDP  |
|   |
|   | Feedback ICMP (Internet Control Message Protocol) is the correct answer for the question. ICMP is a network protocol that is used for diagnostic and control purposes. It is primarily used for Ping and Trace Route utilities. Ping uses ICMP Echo Request and Echo Reply messages to test the reachability of a network host. Trace Route uses ICMP Time Exceeded and Destination Unreachable messages to trace the route taken by packets through an IP network. DHCP (Dynamic Host Configuration Protocol) is used for assigning IP addresses to devices on a network. IP (Internet Protocol) is the network layer protocol responsible for addressing and routing packets. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are transport layer protocols used for data transmission.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 86% got this correct |  |

|  |  |
| --- | --- |
| **2)**  | Which default route will be active? /ip route add disabled=no distance=10 dst-address=0.0.0.0/0 gateway=1.1.1.1 add disabled=no distance=5 dst-address=0.0.0.0/0 gateway=2.2.2.2  |
|   | Route via gateway 1.1.1.1  |  |
|   | Route via gateway 2.2.2.2  |  |
|   | Route via gateway 1.0.1.1  |  |
|   | None of the above    |  |
|   |
|   | Feedback The default route that will be active is the one with a lower distance value. In this case, the route with a distance of 5 (via gateway 2.2.2.2) has a lower distance value than the route with a distance of 10 (via gateway 1.1.1.1). Therefore, the route via gateway 2.2.2.2 will be active.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 85% got this correct |  |

|  |  |
| --- | --- |
| **3)**  | How many different priorities can be selected for queues in Mikrotik RouterOS?  |
|   | 8  |  |
|   | 16  |  |
|   | 0  |  |
|   | 1  |  |
|   |
|   | Feedback In Mikrotik RouterOS, there are 8 different priorities that can be selected for queues. This means that when setting up queues for managing network traffic, there are 8 different priority levels available to assign to each queue. These priority levels help determine the order in which packets are processed and ensure that higher-priority traffic gets processed before lower-priority traffic.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 82% got this correct |  |

|  |  |
| --- | --- |
| **4)**  | In case when router login password is lost, it is necessary to reinstall RouterOS or use hardware reset function.  |
|   | True  |  |
|   | False  |  |
|   |
|   | Feedback When the router login password is lost, reinstalling RouterOS or using the hardware reset function is necessary. This is because the login password is a security measure to prevent unauthorized access to the router's settings and configuration. If the password is lost, reinstalling the operating system or performing a hardware reset will reset all settings and configurations, including the password, allowing the user to regain access to the router.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 81% got this correct |  |

|  |  |
| --- | --- |
| **5)**  | You have a router with configuration -Public IP :202.168.125.45/24 -Default Gateway :202.1687.125.1 -DNS Server :248.115.148.136, 248.115.148.137 -Local IP :192.168.2.1/24 Mark the connection configuration on client PC to access the internet.  |
|   | IP:192.168.2.115/24 gateway:192.168.2.1  |  |
|   | IP:192.168.0.1/24 gateway:192.168.2.1  |  |
|   | IP:192.168.1.223/24 gateway:248.115.148.136  |  |
|   | IP:192.168.2.253/24 gateway:202.168.0.1  |  |
|   |
|   | Feedback The correct answer is IP:192.168.2.115/24 gateway:192.168.2.1. This is the correct configuration because the client PC should have an IP address in the same subnet as the router's local IP address, which is 192.168.2.1/24. The gateway should also be set to the IP address of the router, which is 192.168.2.1. This configuration allows the client PC to communicate with the router and access the internet.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 77% got this correct |  |

|  |  |
| --- | --- |
| **6)**  | Nstreme works only on 40mhz Channel width.  |
|   | True  |  |
|   | False  |  |
|   |
|   | Feedback Nstreme is a proprietary wireless protocol developed by MikroTik. It is designed to improve the performance and efficiency of wireless communication. Nstreme can work on various channel widths, including 20MHz, 40MHz, and even higher. Therefore, the statement that Nstreme works only on a 40MHz channel width is incorrect.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 77% got this correct |  |

|  |  |
| --- | --- |
| **7)**  | What kind of users are listed in the Secrets window of the PPP menu?  |
|   | PPTP users    |  |
|   | Winbox users  |  |
|   | L2TP users    |  |
|   | Wireless users  |  |
|   | PPPOE users    |  |
|   | Hotspot users (Your Answer)  |  |
|   |
|   | Feedback The Secrets window in the PPP menu lists PPTP users, L2TP users, and PPPOE users. These are the different types of users that can be authenticated and authorized to access the network through PPP protocols. The Secrets window allows the network administrator to manage and configure the settings for these specific types of users, such as setting up their login credentials, IP addresses, and other authentication parameters.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 76% got this correct |  |

|  |  |
| --- | --- |
| **8)**  | An IP address pool can contain address from more than one subnet.  |
|   | True  |  |
|   | False  |  |
|   |
|   | Feedback An IP address pool is a range of IP addresses that are available for assignment to devices on a network. It is possible for an IP address pool to contain addresses from more than one subnet. This allows for greater flexibility in assigning IP addresses to devices, as different subnets can have different ranges of IP addresses.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 75% got this correct |  |

|  |  |
| --- | --- |
| **9)**  | From which of the following locations can you obtain Winbox?  |
|   | Router webpage  |  |
|   | Files menu in your router  |  |
|   | Via the console cable  |  |
|   | Mikrotik.com  |  |
|   |
|   | Feedback You can obtain Winbox from the router webpage or from mikrotik.com. The router webpage is a common location to access and download software for the router, including Winbox. Mikrotik.com is the official website of MikroTik, where you can find various resources and downloads, including Winbox.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 75% got this correct |  |

|  |  |
| --- | --- |
| **10)**  | Can you manually add drivers to RouterOS in case your PCI Ethernet card is not recognized, and it's a driver issue?  |
|   | Yes    |  |
|   | No  |  |
|   |
|   | Feedback In MikroTik RouterOS, you cannot manually add drivers. The RouterOS operating system includes a set of built-in drivers for supported hardware, and you cannot add or install additional drivers manually. If a PCI Ethernet card is not recognized, it may indicate that RouterOS does not have the necessary driver for that specific hardware. In such cases, it's recommended to check the compatibility of the hardware with RouterOS and use supported devices.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 74% got this correct |  |

|  |  |
| --- | --- |
| **11)**  | If you need to make sure that one computer in your Hotspot network can access the internet without Hotspot authentication, which menu allows you to do this?  |
|   | Users  |  |
|   | IP bindings  |  |
|   | Walled-garden    |  |
|   | Walled-garden IP  |  |
|   |
|   | Feedback The correct answer is IP bindings. In a Hotspot network, IP bindings allow you to specify certain IP addresses that can bypass the Hotspot authentication and directly access the internet. By adding the IP address of the specific computer to the IP bindings list, you can ensure that it can access the internet without going through the authentication process. This is useful in scenarios where you need to provide unrestricted internet access to a particular device or computer within the Hotspot network.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 73% got this correct |  |

|  |  |
| --- | --- |
| **12)**  | Which of the following protocols is used by MikroTik RouterOS to distribute IP addresses automatically to network devices?  |
|   | HTTP  |  |
|   | FTP  |  |
|   | DHCP  |  |
|   | SNMP  |  |
|   |
|   | Feedback The Dynamic Host Configuration Protocol (DHCP) is used by MikroTik RouterOS to automatically distribute IP addresses to network devices. This protocol simplifies the management of IP address assignment in a network by automatically providing IP addresses and other network configuration parameters to devices.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 73% got this correct |  |

|  |  |
| --- | --- |
| **13)**  | For static routing functionality, additionally to the RouterOS system package, you will also need the following software package:  |
|   | Routing  |  |
|   | Dhcp  |  |
|   | Advance-tools  |  |
|   | None  |  |
|   |
|   | Feedback For static routing functionality in MikroTik RouterOS, you do not need an additional software package. The basic "routing" functionality is included in the RouterOS system package itself. Therefore, the correct answer is C. None.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 73% got this correct |  |

|  |  |
| --- | --- |
| **14)**  | Mikrotik RouterOS DHCP client can receive the following options:  |
|   | Byte limit  |  |
|   | IP Gateway  |  |
|   | Rate Limit  |  |
|   | Uptime Limit  |  |
|   | IP Address and Subnet  |  |
|   |
|   | Feedback The Mikrotik RouterOS DHCP client can receive the IP Gateway and IP Address and Subnet options. The IP Gateway option specifies the IP address of the default gateway that the client should use, while the IP Address and Subnet option provides the client with its own IP address and subnet mask. These options are important for the client to successfully connect to the network and communicate with other devices.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 72% got this correct |  |

|  |  |
| --- | --- |
| **15)**  | It is impossible to delete admin user on user table MikroTik.  |
|   | True  |  |
|   | False  |  |
|   |
|   | Feedback The given statement is false. It is possible to delete the admin user on the user table of MikroTik. The user table in MikroTik allows for the management of user accounts, including the ability to delete them. Therefore, the statement is incorrect.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 72% got this correct |  |

|  |  |
| --- | --- |
| **16)**  | Which is a default baud-rate of currently manufactured RouterBOARDs?  |
|   | 115200  |  |
|   | 8291  |  |
|   | 11520  |  |
|   | 3128  |  |
|   |
|   | Feedback The default baud-rate of currently manufactured RouterBOARDs is 115200.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 71% got this correct |  |

|  |  |
| --- | --- |
| **17)**  | Action = Redirect is applied in:  |
|   | Chain=srcnat  |  |
|   | Chain=dstnat  |  |
|   | Chain=foward  |  |
|   | All of the above    |  |
|   |
|   | Feedback The Action = Redirect is applied in the chain=dstnat. This means that when a packet matches the rules in the destination NAT chain, it will be redirected to a different destination address or port. This can be useful for redirecting incoming traffic to a specific server or service.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 71% got this correct |  |

|  |  |
| --- | --- |
| **18)**  | The hotspot feature can be used only on Ethernet interfaces. You have to use a separate access point if you want to use this feature with wireless.  |
|   | Yes  |  |
|   | No  |  |
|   |
|   | Feedback The explanation for the given correct answer is that the hotspot feature is not limited to only Ethernet interfaces. It can also be used with wireless interfaces. Therefore, the statement that a separate access point is required for using the hotspot feature with wireless is incorrect.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 71% got this correct |  |

|  |  |
| --- | --- |
| **19)**  | You need to set up an E1(T1) connection with PPP configured. Which License Level is needed?  |
|   | Level 4  |  |
|   | It cannot be done in RouterOS    |  |
|   | Level 5  |  |
|   | Level 2  |  |
|   |
|   | Feedback The correct answer is CLevel 51. To set up an E1(T1) connection with PPP configured in MikroTik RouterOS, you need a license of at least Level 51. This is because Level 5 allows up to 500 interfaces, which is sufficient for most E1(T1) configurations. Please note that this information is based on the MikroTik RouterOS. Other systems may have different requirements.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 70% got this correct |  |

|  |  |
| --- | --- |
| **20)**  | The first two rules in the forward chain of the filter table are : /ip firewall filter add chain=forward connection-state=established action=accept /ip firewall filter add chain=forward connection-state=invalid action=drop connection-state=related packets are not filtered by the rules above.  |
|   | True    |  |
|   | False  |  |
|   |
|   | Feedback The first rule in the forward chain of the filter table accepts packets with a connection state of “established,” and the second rule drops packets with a connection state of “invalid.” However, packets with a connection state of “related” are also accepted by the first rule. This is because the “established” and “related” states are often grouped together in firewall rules. So, packets with a connection state of “related” are indeed filtered by the rules above.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 70% got this correct |  |

|  |  |
| --- | --- |
| **21)**  | You have an 802.11b/g wireless card. What frequencies are available to you?  |
|   | 5800MHz  |  |
|   | 2412MHz  |  |
|   | 5210MHz  |  |
|   | 2422MHz  |  |
|   | 2327MHz  |  |
|   |
|   | Feedback The given answer states that the frequencies available for a 802.11b/g wireless card are 2412MHz and 2422MHz. This is because 802.11b/g wireless cards operate in the 2.4GHz frequency range, and the frequencies 2412MHz and 2422MHz fall within this range.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 70% got this correct |  |

|  |  |
| --- | --- |
| **22)**  | Which are a necessary section in /queue simple to set bandwidth limitation?  |
|   | Target-address, max-limit, dst-address  |  |
|   | Max-limit  |  |
|   | Target-address, dst-address  |  |
|   | Target-address, max limit  |  |
|   |
|   | Feedback In the /queue simple section, the "target-address" parameter is necessary to specify the IP address or address range to which the bandwidth limitation will be applied. The "max limit" parameter is also necessary to set the maximum bandwidth limit for the specified target address. Therefore, the correct answer is "target-address, max limit". The other options either do not include both necessary parameters or include additional unnecessary parameters.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 69% got this correct |  |

|  |  |
| --- | --- |
| **23)**  | Which options should be used when you want to prevent access from one specific address to your router web interface?  |
|   | Group setting for System users  |  |
|   | Firewall Filter Chain Input  |  |
|   | Firewall Filter Chain Forward  |  |
|   | WWW service from IP Services  |  |
|   |
|   | Feedback The correct answer is "Firewall Filter Chain Input." This option should be used when you want to prevent access from one specific address to your router web interface. The Firewall Filter Chain Input is responsible for filtering incoming traffic to the router, and by configuring it, you can block access from a specific IP address to the router's web interface.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 68% got this correct |  |

|  |  |
| --- | --- |
| **24)**  | WPA 2 Pre Shared key (PSK) is enabled on AP, all your clients have to use the same PSK. Only Virtual AP could be used to allow clients to connect with a different PSK.  |
|   | True  |  |
|   | False  |  |
|   |
|   | Feedback The statement is false because WPA2-PSK allows each client to have a unique pre-shared key. The pre-shared key is used to authenticate and encrypt the communication between the client and the access point. Virtual APs can be used to create multiple networks with different security settings, but it is not necessary to use them in order to have different pre-shared keys for clients.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 68% got this correct |  |

|  |  |
| --- | --- |
| **25)**  | Choose all valid host address ranges for subnet 15.242.55.62/27  |
|   | 15.242.55.31-15.242.55.62  |  |
|   | 15.242.55.32-15.242.55.63  |  |
|   | 15.242.55.33-15.242.55.62  |  |
|   | 15.242.55.33-15.242.55.63  |  |
|   |
|   | Feedback The given subnet 15.242.55.62/27 has a network address of 15.242.55.32 and a broadcast address of 15.242.55.63. The valid host address range is from the first usable address after the network address, which is 15.242.55.33, to the last usable address before the broadcast address, which is 15.242.55.62. Therefore, the correct answer is 15.242.55.33-15.242.55.62.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 65% got this correct |  |

|  |  |
| --- | --- |
| **26)**  | Which queue type suits the congested environment but is not functional on UDP?  |
|   | PCQ    |  |
|   | BFIFO  |  |
|   | PFIFO  |  |
|   | RED  |  |
|   | SCQ  |  |
|   |
|   | Feedback RED (Random Early Detection) is a queue type that is suitable for congested environments. It helps to prevent network congestion by randomly dropping packets before the network becomes overloaded. However, RED is not functional on UDP (User Datagram Protocol) because it relies on TCP (Transmission Control Protocol) to provide feedback about congestion. Since UDP does not have a built-in congestion control mechanism like TCP, RED cannot effectively operate on UDP.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 64% got this correct |  |

|  |  |
| --- | --- |
| **27)**  | Router A and B are both running as PPPoE servers on different broadcast domains of your network. Is it possible to set Router A to use "/PPP secret" accounts from Router B to authenticate PPPoE customers?  |
|   | Yes  |  |
|   | No  |  |
|   |
|   | Feedback No, it is not possible to set Router A to use "/PPP secret" accounts from Router B to authenticate PPPoE customers. This is because each router is running as a PPPoE server on different broadcast domains, which means they are in separate networks and cannot directly access each other's resources. Each router will have its own set of PPPoE accounts and credentials for authentication.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 64% got this correct |  |

|  |  |
| --- | --- |
| **28)**  | Why is it useful to set a Radio Name on the radio interfaces?  |
|   | To identify a station in a list of connected clients.  |  |
|   | To identify a station in the Access List.  |  |
|   | To identify a station in Neighbor discovery.    |  |
|   | None of the above  |  |
|   |
|   | Feedback Setting a unique Radio Name on radio interfaces, such as in a Wi-Fi network configuration, helps in identifying a station (client device) in a list of connected clients. This naming convention makes it easier for network administrators to manage and monitor the devices connected to the network, troubleshoot issues, and allocate resources effectively.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 63% got this correct |  |

|  |  |
| --- | --- |
| **29)**  | "/interface wireless access list" is used for  |
|   | Shows a list of Client's MAC address that are already registered at AP  |  |
|   | Authenticate Hotspot users  |  |
|   | Handles a list of Client's MAC Address to permit/deny connection to AP  |  |
|   | Contains the security profiles settings  |  |
|   |
|   | Feedback The "/interface wireless access list" command is used to manage a list of MAC addresses that are allowed or denied access to a wireless access point (AP). This list can be used to control which clients are allowed to connect to the AP based on their MAC addresses. This helps enhance network security and manage the devices that are permitted to use the wireless network.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 62% got this correct |  |

|  |  |
| --- | --- |
| **30)**  | To make all DNS requests coming from your network to resolve on your router (regardless of client configuration), which action would you specify for the DST-NAT rule?  |
|   | Masquerade  |  |
|   | Dst-nat    |  |
|   | You can't use DST-NAT to achieve this  |  |
|   | Redirect  |  |
|   |
|   | Feedback The correct answer is "redirect." When you specify the "redirect" action for the DST-NAT rule, it will redirect all DNS requests originating from your network to resolve on your router, regardless of the clients' configurations. This ensures that all DNS traffic is directed to the router for resolution, allowing for centralized control and management of DNS requests within the network. Masquerade, on the other hand, is used for network address translation (NAT), and DST-NAT cannot achieve this objective.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 62% got this correct |  |

|  |  |
| --- | --- |
| **31)**  | Rate Flapping can be avoided by:  |
|   | Choose larger channels (40 Mhz instead of 20 Mhz)  |  |
|   | Reduce supported rates  |  |
|   | Change ap-bridge to bridge  |  |
|   | Set basic rates to only one data rate like 24 Mbps    |  |
|   |
|   | Feedback Reducing the supported rates can help avoid rate flapping. Rate flapping occurs when the wireless device constantly switches between different data rates, causing instability and poor performance. By reducing the supported rates, the device will have fewer options to choose from, reducing the chances of rate flapping. This can help maintain a more stable and reliable connection.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 60% got this correct |  |

|  |  |
| --- | --- |
| **32)**  | PPP Secrets are used for:  |
|   | L2TP clients  |  |
|   | Router users  |  |
|   | PPTP clients  |  |
|   | PPP clients  |  |
|   | IPSec clients  |  |
|   | PPPoE clients  |  |
|   |
|   | Feedback PPP Secrets are used for authenticating and authorizing clients who use various PPP-based protocols such as L2TP, PPTP, PPP, and PPPoE. These secrets contain the necessary information (username, password, and other credentials) to verify the identity of the clients and allow them access to the network. Therefore, the correct answer includes L2TP clients, PPTP clients, PPP clients, and PPPoE clients.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 60% got this correct |  |

|  |  |
| --- | --- |
| **33)**  | What Letter(s) appears next to the route, which is automatically created by ROS (RouterOS) when a user adds a valid address to an active interface?  |
|   | I  |  |
|   | D  |  |
|   | A    |  |
|   | S  |  |
|   | C  |  |
|   |
|   | Feedback In RouterOS, a route that is automatically created when a valid IP address is added to an active interface is marked with the letter "C," which stands for "connected." This indicates that the route is directly connected to a network interface.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 59% got this correct |  |

|  |  |
| --- | --- |
| **34)**  | In MikroTik RouterOS, which of the following firewall chain actions is most appropriate for preventing unauthorized external access to the router's Winbox service, while still allowing internal network management?  |
|   | Accept the connection in the input chain from all interfaces.  |  |
|   | Drop the connection in the forward chain from external interfaces.  |  |
|   | Drop the connection in the input chain from external interfaces.  |  |
|   | Reject the connection in the output chain from internal interfaces.  |  |
|   |
|   | Feedback In MikroTik RouterOS, the input chain is used to filter traffic destined for the router itself. To prevent unauthorized external access to services like Winbox, you should configure the firewall to drop connections to the input chain from external interfaces. This action ensures that only internal network management is allowed, while external attempts to connect to Winbox are blocked. The forward chain is for traffic passing through the router, and rejecting connections in the output chain would not protect the router from external access attempts.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 56% got this correct |  |

|  |  |
| --- | --- |
| **35)**  | Action=redirect allows you to make?  |
|   | Transparent DNS Cache (Missed)  |  |
|   | Foward DNS to another device IP address (Your Answer)  |  |
|   | Enable local service  |  |
|   | Transparent HTTP Proxy (Missed)  |  |
|   |
|   | Feedback The action=redirect allows you to configure a transparent DNS cache and a transparent HTTP proxy. A transparent DNS cache stores DNS responses locally, reducing the need to query external DNS servers repeatedly. This improves DNS resolution time and reduces network latency. On the other hand, a transparent HTTP proxy intercepts and forwards HTTP requests to another device's IP address, allowing for various functionalities like caching, filtering, and logging. Both of these options can be enabled using the action=redirect command.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 54% got this correct |  |

|  |  |
| --- | --- |
| **36)**  | Which is correct masquerade rule for 192.168.0.0/24 network on the router with outgoing interface=ether1  |
|   | /ip firewall nat add action=masquerade chain=srcnat  |  |
|   | /ip firewall nat add action=masquerade chain=srcnat src-address=192.168.0.0/24  |  |
|   | /ip firewall nat add action=masquerade out-interface=ether1 chain=dstnat  |  |
|   | /ip firewall nat add action=masquerade chain=srcnat out-interface=ether1  |  |
|   |
|   | Feedback This rule correctly specifies that any traffic originating from the 192.168.0.0/24 network (source NAT) and going out through the 'ether1' interface should be masqueraded. It ensures that the internal IP addresses are translated to the IP address of the ether1 interface when they go out to the internet.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 45% got this correct |  |

|  |  |
| --- | --- |
| **37)**  | Mark possible connection states in the connection tracking table:  |
|   | Related (Missed)  |  |
|   | Invalid    |  |
|   | Closed (Your Answer)  |  |
|   | Established    |  |
|   | Syn  |  |
|   | New (Missed)  |  |
|   |
|   | Feedback The connection tracking table is used to keep track of the state of network connections. The "Related" state indicates that the connection is related to another connection that is already established. The "Invalid" state indicates that the connection is not valid or has been terminated. The "Established" state indicates that the connection has been successfully established. The "New" state indicates that a new connection has been initiated. Therefore, the possible connection states in the connection tracking table are "Related", "Invalid", "Established", and "New".  |  |  |

|  |  |  |
| --- | --- | --- |
| **Correct**  | 44% got this correct |  |

|  |  |
| --- | --- |
| **38)**  | Possible actions of IP firewall filter are:  |
|   | Tarpit  |  |
|   | Tarp  |  |
|   | Bounce  |  |
|   | Add-to-address-list  |  |
|   | Log  |  |
|   | Accept  |  |
|   |
|   | Feedback The possible actions of IP firewall filter include tarpit, which slows down the connection to prevent malicious attacks, add-to-address-list, which adds the source IP address to a specified address list, log, which records information about the connection, and accept, which allows the connection to pass through the firewall. These actions help in enhancing the security and control of network traffic.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 43% got this correct |  |

|  |  |
| --- | --- |
| **39)**  | Which of the following actions are available for '/IP firewall mangle' (select all valid actions)  |
|   | Change MSS (Missed)  |  |
|   | Mark connection    |  |
|   | Accept (Missed)  |  |
|   | Jump    |  |
|   | Drop  |  |
|   | Mark packet    |  |
|   |
|   | Feedback The '/IP firewall mangle' table in MikroTik RouterOS allows for various actions to be performed on packets. The available actions in this case are: Change MSS (Maximum Segment Size), which modifies the TCP MSS value in the TCP SYN packet; mark connection, which marks the connection for further processing; accept, which allows the packet to pass through; jump, which jumps to a different chain for further processing; and mark packet, which marks the packet for further processing. The action drop is not available in this context.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 38% got this correct |  |

|  |  |
| --- | --- |
| **40)**  | Which software version can be installed onto the following RouterBoard types?  |
|   | Routeros-x86-x.xx.npk on a RB1100    |  |
|   | Routeros-mipsbe-x.xx.npk on a RB133 (Your Answer)  |  |
|   | Routeros-mipsle-x.xx.npk on a RB133    |  |
|   | Routeros-powerpc-x.xx.npk on a RB333  |  |
|   | Routeros-mipsbe-x.xx.npk on a RB433 (Missed)  |  |
|   |
|   | Feedback The given answer states that the software version "routeros-mipsle-x.xx.npk" can be installed on a RB133 router, and the software version "routeros-mipsbe-x.xx.npk" can be installed on a RB433 router. It implies that different RouterBoard types require different software versions for installation. The "mipsle" and "mipsbe" in the software version names refer to different processor architectures, and each RouterBoard type has a specific processor architecture. Therefore, it is important to choose the correct software version that matches the processor architecture of the RouterBoard type for successful installation.  |  |  |

|  |  |  |
| --- | --- | --- |
| **Incorrect**  | 31% got this correct |  |

|  |  |
| --- | --- |
| **41)**  | Which features are removed when advanced tools packages are uninstalled?  |
|   | Neighbors  |  |
|   | Ip-scan    |  |
|   | Netwatch    |  |
|   | LCD support  |  |
|   | Ping    |  |
|   | Bandwith-test (Your Answer)  |  |
|   |
|   | Feedback The correct answers are - ip-scan, netwatch, ping  |  |  |