DUMPSBOSS.

MikroTik Certified Network Associate Exam

MikroTik MTCNA

Version Demo

Total Demo Questions: 25

Total Premium Questions: 255

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, MikroTik RouterOS	81
Topic 2, Firewall	37
Topic 3, QoS	14
Topic 4, Wireless	36
Topic 5, Bridging	16
Topic 6, Routing	38
Topic 7, Tunnels	14
Topic 8, Misc	19
Total	255

QUESTION NO: 1

What is marked by connection-state=established matcher?

A. Packet belongs to an existing connection,for example a reply packet or a packet which belongs to already replied connection

B. Packet is related to, but not part of an existing connection

C. Packet does not correspond to any known connection

D. Packet begins a new TCP connection

ANSWER: A

Explanation:

`connection-state=established` matches packets that belong to a connection already known to RouterOS connection tracking and for which traffic has been seen in both directions. In practical firewall use, this includes reply traffic for a connection initiated through the router, as well as subsequent packets of a connection after it has received a valid reply. For example, when a LAN client initiates a TCP session to an Internet server, the initial outbound packet is tracked as a new connection. Once the server responds, packets associated with that flow are considered established, allowing a firewall rule to recognize them as part of an ongoing, bidirectional conversation.

This matcher is fundamental to stateful firewall design because it lets administrators permit return and ongoing traffic without creating separate broad rules for every protocol or ephemeral port. A typical RouterOS filter policy accepts established traffic early in the relevant chain, then applies more restrictive policy to traffic that is attempting to create connections. RouterOS documents the available connection-tracking states and describes `established` as packets belonging to existing connections, including packets that have already received a reply. See the RouterOS Connection Tracking documentation and the Common Firewall Matchers and Actions reference.

QUESTION NO: 2

Which of the following commands will allow you to set your Telnet password on a Cisco router?

A. line telnet 0 4

B. line aux 0 4

C. line vty 0 4

D. line con 0

ANSWER: C

Explanation:

`line vty 0 4` is correct because Telnet access to a Cisco IOS router is handled through the virtual terminal (VTY) lines. Entering this command from global configuration mode selects the range of virtual terminal line configurations numbered zero through four. Within that line-configuration context, an administrator can configure a password with the `password` command and enable password checking with `login`. For example, the relevant configuration sequence is `line vty 0 4`, followed by `password <password-value>` and `login`. These virtual lines represent remote interactive management sessions, including Telnet sessions; they are not physical console connections. The selected range also permits the same remote-access policy to be applied consistently to multiple simultaneous inbound management sessions. Cisco IOS documents VTY lines as the configuration point for remote terminal access and describes applying authentication settings under line configuration mode. For current operational security, SSH with local user authentication is generally preferred over Telnet because Telnet transmits session data without encryption, but VTY line configuration remains the correct command context for a Telnet password. See Cisco's user-access security configuration guide and its terminal-services command reference.

QUESTION NO: 3

Which of the following are valid IP addresses?

A. 10.10.14.0

B. 192.168.256.1

C. 192.168.13.255

D. 1.27.14.254

ANSWER: A C D

Explanation:

An IPv4 address is written as four decimal octets separated by periods. Each octet must be an integer from 0 through 255. **10.10.14.0**, **192.168.13.255**, and **1.27.14.254** each meet that fundamental format: they contain exactly four octets, and every displayed value falls within the permitted decimal range. Therefore, each is a valid IPv4 address representation.

Whether an address is assigned to a router interface, used as a host address, or identified as a subnet's network or broadcast address is a separate question that depends on the configured prefix length (netmask). RouterOS assigns IP addresses using address/prefix notation, such as `192.168.13.255/24`; the prefix defines the network boundary and determines any special network or broadcast role. It does not change the fact that these three dotted-decimal values are syntactically valid IPv4 addresses. RouterOS IPv4 addressing concepts and prefix-based configuration are documented in the MikroTik RouterOS IP Addressing documentation. The decimal-octet IPv4 address format is also specified by RFC 791.

QUESTION NO: 4

For static routing functionality, additionally to the RouterOS 'system' package, you will also need the following software package:

A. no extra package required

B. advanced-tools

C. routing

D. dhcp

ANSWER: A

Explanation:

no extra package required is correct because static routes are a fundamental RouterOS IP-routing function and are available as part of the base RouterOS system. An administrator can create, inspect, enable, disable, and modify static routes in the routing configuration without installing an additional package. A static route defines a manually configured destination prefix and gateway or outgoing interface, allowing the router to forward traffic toward networks that are not directly connected.

RouterOS documentation describes static-route configuration under IP Routing, including the use of the `/ip route` menu and route properties such as `dst-address`, `gateway`, and `distance`. For example, a default route can be configured by using destination `0.0.0.0/0` with the appropriate next-hop gateway. Package modularity has varied across RouterOS releases, but static routing remains available in the core routing functionality rather than requiring a separate installable feature package. See MikroTik's IP Routing documentation and the RouterOS Packages documentation.

QUESTION NO: 5

Mark all features that are compatible with Nstreme

A. WDS between a device in station-wds mode and a device in station-wds mode

B. Encryption

C. WDS between a device in ap-bridge mode with a device in station-wds mode

D. Bridging a device in station mode with a device in ap-bridge mode

ANSWER: B C

Explanation:

Encryption is compatible with Nstreme. Nstreme is MikroTik's proprietary wireless protocol for point-to-point links and can operate while wireless security is enabled. The security profile and its selected authentication/encryption settings protect the wireless connection; administrators should select modern security settings appropriate for the RouterOS version and deployment requirements. Encryption is therefore not inherently prevented by enabling Nstreme.

WDS between a device in ap-bridge mode with a device in station-wds mode is also compatible with Nstreme. This pairing supplies the access-point and client roles required for the point-to-point Nstreme link, while `station-wds` provides the WDS functionality needed to transparently extend Layer 2 connectivity across the wireless connection. Nstreme is intended for MikroTik-to-MikroTik point-to-point operation, so both wireless peers must support and be configured for the protocol. MikroTik's wireless documentation describes the applicable wireless operating modes and WDS behavior, while its Nstreme documentation identifies Nstreme as a proprietary protocol for wireless links. See the RouterOS Wireless documentation and the MikroTik Nstreme manual.

QUESTION NO: 6

Action=redirect can be used in NAT chain src-nat

A. true

B. false

ANSWER: B

Explanation:

`false` is correct. In RouterOS NAT, the `redirect` action is a destination-NAT action: it changes the packet's destination address to an address of the router itself. Its usual purpose is transparently sending traffic received by the router to a service running locally, such as redirecting web requests to a local proxy or DNS requests to the router's DNS service. Because it operates by replacing a destination, it is used in the destination-NAT processing path, not in the `src-nat` chain.

The `src-nat` chain is for source-address translation after routing has selected the outgoing path. RouterOS uses source-NAT actions there, including `src-nat`, `masquerade`, and `same`, to modify the source address of packets leaving through an interface. This separation follows the packet flow: destination translation can affect where traffic is delivered, while source translation adjusts the return address used for traffic sent onward. MikroTik's NAT documentation identifies `redirect` as replacing the destination address with one of the router's local addresses and documents the NAT chains and actions in detail. See MikroTik RouterOS NAT and Packet Flow in RouterOS.

QUESTION NO: 7

Router A and B are both running as PPPoE servers on different broadcast domains of your network. It is possible to set Router A to use "/ppp secret" accounts from Router B to authenticate PPPoE customers.

A. true

B. false

ANSWER: B

Explanation:

false is correct because entries configured under `/ppp secret` are local RouterOS user records. Each PPPoE server consults its own locally configured PPP secrets when local authentication is used; RouterOS does not provide a setting that makes one router directly query and authenticate against the `/ppp secret` database of another router. Therefore, PPP secrets entered on Router B are not automatically available to Router A, even when both devices operate PPPoE servers in the same overall network.

To centralize credentials for PPPoE services across multiple access routers, the appropriate design is to configure an external RADIUS server and add it as an authentication source on each RouterOS device. RADIUS allows both routers to send authentication and accounting requests to the same centralized user database, so the same customer credentials can be used regardless of which PPPoE server receives the connection. MikroTik documents PPP AAA authentication and the use of RADIUS for PPP services in its PPP AAA documentation and documents RADIUS client configuration at RADIUS.

QUESTION NO: 8

What protocol is used for Ping and Trace route?

A. DHCP

B. IP

C. TCP

D. ICMP - ping

E. UDP – trace route

ANSWER: D E

Explanation:

Ping uses ICMP (Internet Control Message Protocol), specifically ICMP Echo Request and Echo Reply messages. A device sends an Echo Request to the destination and measures whether and how quickly an Echo Reply returns. This makes ICMP the protocol directly associated with the standard ping operation, including RouterOS `/ping`.

Traceroute commonly uses UDP probe packets. Each probe is sent with an incrementally increased IP TTL value; when the TTL reaches zero at an intermediate router, that router returns an ICMP Time Exceeded message. This reveals the successive hops on the path. RouterOS traceroute supports several probe protocols, but UDP is the default traceroute protocol and is therefore the expected answer for a question pairing the conventional protocols used by ping and traceroute. The traceroute process also relies on IP and returned ICMP control messages, but UDP identifies the usual outgoing probe protocol. See the MikroTik RouterOS documentation for Ping and Traceroute.

QUESTION NO: 9

Which of the following is true for connection tracking

A. Connection tracking must be enabled for NAT'ed network

B. Enabling connection tracking reduces CPU usage in RouterOS

C. Disable connection tracking for mangle to work

D. Connection tracking must be enabled to be able to use all firewall features

ANSWER: A D

Explanation:

Connection tracking must be enabled for NAT'ed network is correct because RouterOS NAT processing relies on connection tracking to create and maintain per-connection translation entries. When the first packet of a connection matches a NAT rule,

RouterOS records the selected translation in the connection-tracking table so that subsequent packets in both directions receive the consistent source or destination translation required for the session. RouterOS documentation explicitly states that NAT matches only the first packet of a connection and that connection tracking is required for NAT.

Connection tracking must be enabled to be able to use all firewall features is also correct. Connection tracking supplies connection state and related metadata used by stateful firewall processing, including the `connection-state` matcher commonly used to accept established and related traffic and to handle invalid traffic. It also supports functionality that depends on tracked connections, such as connection marks, NAT state matching, and FastTrack. Administrators can disable tracking for narrowly defined traffic using raw-table `notrack` rules, but that traffic cannot use connection-tracking-dependent functions. See the official RouterOS NAT documentation and RouterOS connection tracking documentation.

QUESTION NO: 10

For user in local PPP Secrets/PPP Profiles database, it is possible to

A. Allow/deny use of more than one login by this user

B. Allow login by PPPoE and PPTP, but deny login by L2TP

C. Set max values for transferred data (Rx/Tx)

D. Allow only PPPoE login

E. Deny services (like telnet) only for this user or for one group of users

ANSWER: A C D

Explanation:

Local PPP secrets and PPP profiles provide controls for an individual PPP subscriber's session behavior and accounting limits. "Allow/deny use of more than one login by this user" is supported through the PPP profile `only-one` setting. When enabled, RouterOS permits only one active session for a user at a time; the profile selected by the secret determines whether this rule applies.

"Set max values for transferred data (Rx/Tx)" is supported directly in a PPP secret with `limit-bytes-in` and `limit-bytes-out`. These values define the maximum number of bytes the subscriber may receive and transmit. They are useful for per-user traffic quotas and are separate from rate-limit settings, which control throughput rather than total transfer volume.

"Allow only PPPoE login" is also supported by the PPP secret `service` property. Assigning the service to `pppoe` restricts that credential to PPPoE authentication, rather than allowing it to be used by the general PPP service selection. These controls are part of RouterOS's local PPP AAA configuration and can be combined by assigning an appropriate PPP profile to each secret. See the MikroTik PPP AAA documentation and the PPP secret and profile property reference.

QUESTION NO: 11

On the advanced menu of the wireless setup there is a parameter called "Area", it works directly with:

A. Connect List

B. Access List

C. None of these

D. Security Profile

ANSWER: A

Explanation:

The correct answer is **Connect List**. In the legacy RouterOS Wireless package, the *area* setting on a wireless interface is a logical tag used when a station chooses which access points it is permitted or preferred to connect to. A Connect List rule can contain an area value, and RouterOS compares that value with the wireless interface's configured area while evaluating eligible wireless networks. This lets an administrator group access points into logical locations or roaming domains—such as floors, buildings, or service zones—without relying only on a specific AP MAC address or SSID.

When several access points advertise a suitable network, Connect List processing can use the matching area together with other rule criteria and connection properties to control the station's association behavior. The area is therefore not a radio-frequency or regulatory setting; it is metadata that becomes meaningful through Connect List matching. Configuring consistent area names on station interfaces and the relevant Connect List entries provides a straightforward way to scope which APs should be considered for connection in a multi-AP deployment. MikroTik's Wireless documentation describes Connect List as the mechanism for selecting wireless networks and its rule matching properties: MikroTik RouterOS Wireless documentation. Additional legacy wireless configuration reference is available at MikroTik Manual: Interface/Wireless.

QUESTION NO: 12

A PC with IP 192.168.1.2 can access internet, and static ARP has been set for that IP address on gateway. When the PC Ethernet card failed, the user changed it with a new card and set the same IP for it. What else should be done? [multiple answers]

A. Old static ARP entry on gateway has to be updated for the new card

B. Nothing – it will work as before

C. MAC-address of the new card has to be changed to MAC address of old card

D. Another IP has to be added for Internet access

ANSWER: A C

Explanation:

A static ARP entry is a fixed binding between an IP address and a layer-2 MAC address on the gateway. The PC may retain 192.168.1.2 after its network adapter is replaced, but the replacement adapter normally has a different factory MAC address. For traffic sent through the gateway to reach that host, the gateway's static ARP mapping must correspond to the MAC address currently used by the PC.

Therefore, "Old static ARP entry on gateway has to be updated for the new card" is a valid way to restore connectivity: replace the MAC address in the static ARP entry while retaining the existing IP address. "MAC-address of the new card has to be changed to MAC address of old card" is also a valid alternative where the operating system and network adapter support locally administered MAC-address configuration. In that case, the replacement adapter presents the MAC address already stored in the gateway's static ARP entry, so the existing IP-to-MAC binding remains valid.

MikroTik RouterOS documents static ARP entries as manually configured IP/MAC mappings and explains ARP behavior and modes in the RouterOS ARP documentation. The underlying ARP protocol relationship between protocol addresses and hardware addresses is defined in RFC 826.

QUESTION NO: 13

Evaluate the following information:

Access Point configuration:

-- wlan1 is in 'AP-Bridge' mode

-- Bridge1 has wlan1 and ether1 as ports

CPE configuration:

-- wlan1 is in 'Station-Bridge' mode

-- Bridge1 has wlan1 and ether1 as ports

Select protocols that will pass from ether1 on the CPE to ether1 on the Access Point:

A. IPv4

B. ARP

C. USB

D. BGP

E. Firewire

F. IPv6

G. DHCP

ANSWER: A B D F G

Explanation:

IPv4, ARP, BGP, IPv6, and DHCP will pass between the Ethernet ports because this is a MikroTik-to-MikroTik wireless bridge using `ap-bridge` on the access point and `station-bridge` on the CPE. In this arrangement, each wireless interface is a bridge port alongside its local `ether1` interface. The wireless link therefore forwards Ethernet frames at Layer 2 between the two bridge domains rather than acting only as an IP-routed connection.

Transparent Layer 2 forwarding carries ordinary Ethernet traffic according to its destination MAC address, including unicast, broadcast, and multicast frames. IPv4 and IPv6 packets are encapsulated in Ethernet frames and cross the bridge normally. ARP uses Ethernet broadcast frames to resolve IPv4 addresses to MAC addresses, so it is also transported transparently. DHCP discovery and offer traffic can traverse this bridged segment because its broadcast traffic remains within the same Layer 2 broadcast domain. BGP uses TCP over IP; once IP connectivity exists across the transparent bridge, BGP packets can likewise traverse the link.

MikroTik documents `station-bridge` as a proprietary station mode intended for use with MikroTik AP modes and supporting Layer 2 bridging. See the MikroTik Wireless Station Modes documentation and the MikroTik Bridging and Switching documentation.

QUESTION NO: 14

Which is a default baud-rate of currently manufactured RouterBOARDs?

A. 9600

B. 115200

C. 38400

D. 11520

ANSWER: B

Explanation:

The correct answer is **115200**. Currently manufactured RouterBOARD devices conventionally use 115200 bits per second as the default serial-console data rate. This setting is important when connecting a computer to the RouterBOARD serial console for initial setup, recovery, troubleshooting, or observing boot output. A terminal emulator must be configured to match the device's serial parameters; the typical configuration is 115200 baud, 8 data bits, no parity, 1 stop bit, and no flow control (commonly written as 115200 8N1 with flow control disabled).

MikroTik's RouterBOOT documentation identifies 115200 as the default serial-console baud rate and also documents the boot-loader configuration options through which serial-console behavior can be managed on supported hardware. The RouterOS documentation likewise describes serial terminal access and the standard settings used for console connections. Using the default speed ensures that boot messages and the RouterOS command-line interface are displayed correctly

rather than as unreadable characters. See the MikroTik RouterBOOT documentation and the MikroTik Serial Terminal documentation.

QUESTION NO: 15

Two active routes have the same destination prefix. Which route is normally preferred by RouterOS?

A. The route with the lower distance

B. The route with the higher distance

C. The route with the numerically highest gateway address

D. The route added most recently

ANSWER: A

Explanation:

The route with the lower administrative distance is normally preferred. Administrative distance expresses the preference of one route source over another when routes describe the same destination prefix. A smaller distance has higher preference.

For example, a static route with distance 1 is normally selected instead of another route to the same prefix with distance 10, provided both routes are valid and resolvable. RouterOS uses additional route-selection attributes when necessary, but distance is the primary preference value for otherwise competing routes to the same destination. See the RouterOS IP Routing documentation.

QUESTION NO: 16

What is the minimal possible wireless configuration to create an Access Point?

A. radio name

B. scan-list

C. frequency

D. band

E. ssid

F. DFS mode

G. WDS

ANSWER: C D E

Explanation:

For the wireless settings presented, **frequency**, **band**, and **ssid** are the essential radio parameters used to define an operational access-point WLAN. The frequency selects the radio channel on which the access point transmits. It must be compatible with the selected band and with the device's supported wireless capabilities. The band defines the wireless standard and frequency range in use, such as 2.4 GHz 802.11 b/g/n or a supported 5 GHz mode; this determines how the radio operates and what client capabilities can associate. The ssid is the network identifier advertised by the AP, allowing wireless clients to discover and select the WLAN.

In an actual RouterOS configuration, the wireless interface must additionally operate in an AP-capable mode, such as `ap-bridge` where supported; that mode is not among the provided choices. Within the listed parameters, frequency, band, and ssid are therefore the required minimal configuration selections. RouterOS wireless documentation describes SSID, band, frequency, and mode as key wireless-interface properties, and the MikroTik wireless guide documents configuring an interface for AP operation: MikroTik RouterOS Wireless documentation and MikroTik Wireless Interface manual.

QUESTION NO: 17

The highest queue priority is

A. 1

B. 256

C. 16

D. 8

ANSWER: A

Explanation:

The highest queue priority is **1**. In MikroTik RouterOS, the `priority` setting used by Simple Queues and Queue Trees has a range from 1 through 8. This value determines the order in which queues are considered when traffic competes for limited available bandwidth under a shared parent or interface constraint. A numerically lower priority represents a higher scheduling priority, so traffic assigned priority 1 is handled before traffic in queues assigned priorities 2 through 8, assuming the queueing conditions require prioritization.

Priority is most meaningful when multiple child queues share the same parent and there is congestion. It does not itself reserve bandwidth; guaranteed throughput is configured with parameters such as `limit-at`, while priority affects access to bandwidth that remains available after relevant guarantees and queue rules are considered. Correctly using priority 1 is useful for latency-sensitive or business-critical traffic where that traffic should receive preferential treatment during contention. RouterOS documents the priority range as 1–8 and explicitly identifies 1 as the highest priority. See the official RouterOS Queues documentation and the MikroTik RouterOS documentation portal.

QUESTION NO: 18

In RouterOS queue configurations the word "total" usually represents

A. download - upload

B. upload

C. upload + download

D. Download

ANSWER: C

Explanation:

In RouterOS queue configurations, “total” usually means the combined traffic in both directions: upload plus download. Queue statistics and related rate/byte counters can use a total value to provide one aggregate measure of traffic handled by a queue, rather than requiring the administrator to interpret each direction separately. This is particularly useful when reviewing overall client or target usage, applying accounting-oriented limits, or monitoring a queue whose traffic is relevant regardless of whether packets are entering or leaving the network.

RouterOS Simple Queues identify traffic by a target and process upload and download in relation to that target. Consequently, the directional figures represent the two traffic directions, while the total is their sum. For example, if a target has transferred 2 MiB in one direction and 3 MiB in the other, its total transferred amount is 5 MiB. This interpretation applies to the ordinary RouterOS meaning of total traffic and should not be confused with a rate in only one direction. MikroTik’s queue documentation describes Simple Queue traffic handling and queue properties, while its monitoring documentation covers the presentation of traffic counters and aggregate values. See the RouterOS Queues documentation and RouterOS interface statistics and monitoring documentation.

QUESTION NO: 19

Which DHCP client setting prevents RouterOS from automatically adding a default route received from a DHCP server?

A. add-default-route=no

B. use-peer-dns=no

C. disabled=yes

D. use-peer-ntp=no

ANSWER: A

Explanation:

`add-default-route=no` is correct. When a DHCP client receives gateway information from its DHCP server, RouterOS can automatically install a dynamic default route. Setting `add-default-route=no` prevents this route from being created.

This is useful when a DHCP client is used only to obtain an address or DNS information, or when default routing is controlled manually through static routes, routing tables, or another WAN connection. See the official RouterOS DHCP documentation.

QUESTION NO: 20

When VLAN filtering is enabled on a RouterOS bridge, which statements are true? Select all that apply.

A. PVID classifies untagged ingress traffic into a VLAN

B. The Bridge VLAN table controls tagged and untagged egress membership

C. All bridge ports automatically become members of every VLAN

D. Tagged frames can be allowed on a trunk bridge port

ANSWER: A B D

Explanation:

The PVID property is used to classify untagged frames received on a bridge port into a VLAN. For example, a port with `pvid=20` places untagged ingress traffic into VLAN 20.

The Bridge VLAN table controls which VLANs are permitted on bridge ports and whether frames leave a port as tagged or untagged. A VLAN-aware bridge therefore requires both suitable port PVID settings and appropriate VLAN table entries. Enabling `vlan-filtering` does not automatically make every bridge port a member of every VLAN. See the official RouterOS Bridging and Switching documentation.

QUESTION NO: 21

Consider the following diagram. We want to communicate from a device on LAN1 to a device on LAN2. Assuming that all necessary configurations are already included on R2, which of the following configurations in R1 would enable this communication?



A. /ip route add dst-address=192.168.1.0/24 src-address=192.168.0.0/24 gateway=192.168.99.2

B. /ip route add dst-address=0.0.0.0/0 gateway=Ether1

C. /ip route add dst-address=192.168.0.0/24 gateway=192.168.0.1

D. /ip route add dst-address=192.168.1.0/24 gateway=192.168.99.2

E. /ip route add dst-address=0.0.0.0/0 gateway=192.168.99.2

ANSWER: D

Explanation:

The command `/ip route add dst-address=192.168.1.0/24 gateway=192.168.99.2` adds the required static route on R1 for the remote LAN2 network. The destination prefix, `192.168.1.0/24`, represents the LAN behind R2. The gateway, `192.168.99.2`, is R2's address on the directly connected transit network shared by R1 and R2. Therefore, when a LAN1 host sends a packet to an address in LAN2, R1 matches the packet's destination against this route and forwards it to R2. R2 can then deliver the packet through its LAN2-facing interface; the premise that R2 already has all necessary configuration also includes its ability to return traffic toward LAN1. Using a specific route for the known remote subnet is the appropriate static-routing configuration because it explicitly defines the intended path between the two internal LANs. MikroTik RouterOS routes use `dst-address` to identify the destination prefix and `gateway` to identify the next-hop router. See the MikroTik IP Routing documentation and the IP Routing Configuration guide.

QUESTION NO: 22

In MikroTik RouterOS, Layer3 communication between 2 hosts can be achieved by using an address subnet of:

A. /31

B. /29

C. /32

D. /30

ANSWER: A B D

Explanation:

A **/29** subnet can provide Layer 3 communication between two hosts because it contains eight IPv4 addresses and, under conventional subnet addressing, six usable host addresses. Assigning two different usable addresses from that subnet to the two endpoints places them in the same IP network, allowing direct routed IP communication.

A **/30** subnet is the traditional IPv4 choice for a point-to-point Layer 3 link. It has four addresses, with two usable endpoint addresses in conventional addressing. Each host can receive one of those addresses, making it a compact subnet for exactly two connected devices.

A **/31** subnet is also valid for a point-to-point connection between exactly two Layer 3 endpoints. RFC 3021 permits both addresses in a 31-bit IPv4 prefix to be used on point-to-point links, avoiding the need to reserve separate network and broadcast addresses. RouterOS supports assigning IP prefixes to interfaces and can use this addressing approach where the link is point-to-point. Therefore, /29, /30, and /31 can each support communication between two hosts, with /31 and /30 being particularly efficient for point-to-point links.

See MikroTik's IP Addressing documentation and RFC 3021.

QUESTION NO: 23

It is required to make a web server on a private LAN visible on the Public Internet. Only the web server port should be visible to the public. Which of the following configuration steps must be met. (select all that apply)

A. Public IP address of the webserver must be installed on the NAT Router

B. in ip firewall NAT there should be a dst-nat between the public ip of the router and the private ip of the webserver

C. Connection Tracking must be enabled on NAT router

D. A route between the NAT Router and the webserver must exist

E. LAN address of the webserver should be routable on the internet

ANSWER: B C D

Explanation:

A destination NAT rule is required to translate traffic arriving at the router's public address and web-service port to the web server's private LAN address. In RouterOS, this is configured in `/ip firewall nat` using the `dst-nat` action. The rule should match only the intended protocol and service port, such as TCP port 80 or TCP port 443, so that the port-forwarding rule applies only to the published web service. The official RouterOS NAT documentation describes destination NAT as the mechanism used to redirect inbound connections to an internal host.

Connection tracking must be enabled because RouterOS NAT operates together with connection tracking. Connection tracking records the connection and ensures that return packets are translated consistently back through the router, allowing the Internet client to communicate with the internal server using the router's public address.

A route between the NAT router and the web server must also exist. This may be a connected route for the LAN subnet or a static/dynamic route through another internal router. The NAT router must be able to forward the translated packet to the server's private address and receive the reply traffic. See the RouterOS documentation for NAT and Connection Tracking.

QUESTION NO: 24

Which firewall chain should you use to filter clients HTTP traffic going through the router?

A. prerouting

B. forward

C. output

D. input

ANSWER: B

Explanation:

The correct firewall chain for filtering clients' HTTP traffic that passes through the router is **forward**. In MikroTik RouterOS, the forward chain processes packets that enter the router on one interface and are routed out through another interface. This is the normal path for client traffic travelling between a LAN and the Internet, including TCP traffic destined for HTTP service port 80. A firewall filter rule in this chain can match the protocol and destination port—for example, TCP with `dst-port=80`—and then allow, block, log, or otherwise control that transit traffic according to the configured action. The router is acting as an intermediary for these packets rather than as their destination or source, which is precisely the traffic scope handled by the forward chain. RouterOS documentation describes the forward chain as applying to packets passing through the router, and its packet-flow documentation illustrates this routed transit path. See the RouterOS firewall filter documentation and the Packet Flow in RouterOS reference.

QUESTION NO: 25

Select which of the following are 'Public IP addresses':

A. 172.168.254.2

B. 172.28.73.21

C. 11.63.72.21

D. 10.110.50.37

E. 192.168.0.1

ANSWER: A C

Explanation:

172.168.254.2 and **11.63.72.21** are public IPv4 addresses because neither address falls within an IPv4 range reserved for private internetworking. Public addresses are globally unique addresses that can be routed on the public Internet when they have been allocated by an appropriate Internet registry and are not subject to another special-use reservation.

RFC 1918 defines the private IPv4 ranges as 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. The 172.16.0.0/12 block extends from 172.16.0.0 through 172.31.255.255; therefore, 172.168.254.2 is outside that private block and is publicly addressable. Likewise, 11.63.72.21 is outside all RFC 1918 private ranges. In MikroTik routing and firewall configuration, addresses such as these may be used on Internet-facing links when they are assigned by an ISP or otherwise legitimately allocated. RFC 1918 also emphasizes that public Internet routes must use globally unique address space, which is the key distinction tested here. See RFC 1918: Address Allocation for Private Internets and the IANA IPv4 Special-Purpose Address Registry.