[Updated Constantly]

HERE

CCNA 2 (v5.1 + v6.0) Chapter 7 Exam Answers Full

How to find: Press “Ctrl + F” in the browser and fill in whatever wording is in the question to find that question/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. **In which configuration would an outbound ACL placement be preferred over an inbound ACL placement?**
   - **when the ACL is applied to an outbound interface to filter packets coming from multiple inbound interfaces before the packets exit the interface***
   - when a router has more than one ACL
   - when an outbound ACL is closer to the source of the traffic flow
   - when an interface is filtered by an outbound ACL and the network attached to the interface is the source network being filtered within the ACL

   An outbound ACL should be utilized when the same ACL filtering rules will be applied to packets coming from more than one inbound interface before exiting a single outbound interface. The outbound ACL will be applied on the single outbound interface.
2. **Which address is required in the command syntax of a standard ACL?**
   - source MAC address
   - destination MAC address
   - **source IP address***
   - destination IP address

   The only filter that can be applied with a standard ACL is the source IP address. An extended ACL can use multiple criteria to filter traffic, such as source IP address, destination IP address, type of traffic, and type of message.
3. **Which statement describes a difference between the operation of inbound and outbound ACLs?**
   - In contrast to outbound ALCs, inbound ACLs can be used to filter packets with multiple criteria.
   - Inbound ACLs can be used in both routers and switches but outbound ACLs can be used only on routers.
   - **Inbound ACLs are processed before the packets are routed while outbound ACLs are processed after the routing is completed.***
   - On a network interface, more than one inbound ACL can be configured but only one outbound ACL can be configured.
4. **Which three statements describe ACL processing of packets? (Choose three.)**
   - **An implicit deny any rejects any packet that does not match any ACE.***
   - **A packet can either be rejected or forwarded as directed by the ACE that is matched.***
   - A packet that has been denied by one ACE can be permitted by a subsequent ACE.

- A packet that does not match the conditions of any ACE will be forwarded by default.
- **Each statement is checked only until a match is detected or until the end of the ACE list.***
- Each packet is compared to the conditions of every ACE in the ACL before a forwarding decision is made.

When a packet comes into a router that has an ACL configured on the interface, the router compares the condition of each ACE to determine if the defined criteria has been met. If met, the router takes the action defined in the ACE (allows the packet through or discards it). If the defined criteria has not been met, the router proceeds to the next ACE. An implicit deny any statement is at the end of every standard ACL.

5. **What single access list statement matches all of the following networks?**
   192.168.16.0
   192.168.17.0
   192.168.18.0
   192.168.19.0
   - **access-list 10 permit 192.168.16.0 0.0.3.255***
   - access-list 10 permit 192.168.16.0 0.0.0.255
   - access-list 10 permit 192.168.16.0 0.0.15.255
   - access-list 10 permit 192.168.0.0 0.0.15.255

   The ACL statement access-list 10 permit 192.168.16.0 0.0.3.255 will match all four network prefixes. All four prefixes have the same 22 high order bits. These 22 high order bits are matched by the network prefix and wildcard mask of 192.168.16.0 0.0.3.255.
6. **A network administrator needs to configure a standard ACL so that only the workstation of the administrator with the IP address 192.168.15.23 can access the virtual terminal of the main router. Which two configuration commands can achieve the task? (Choose two.)**
   - **Router1(config)# access-list 10 permit host 192.168.15.23***
   - **Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.0***
   - Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.255
   - Router1(config)# access-list 10 permit 192.168.15.23 255.255.255.0
   - Router1(config)# access-list 10 permit 192.168.15.23 255.255.255.255

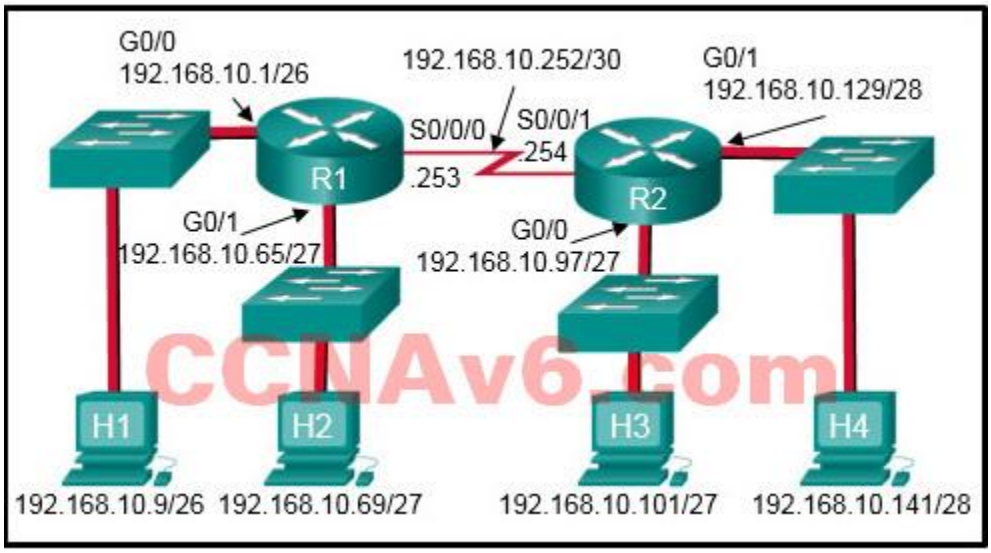
   To permit or deny one specific IP address, either the wildcard mask 0.0.0.0 (used after the IP address) or the wildcard mask keyword host (used before the IP address) can be used.
7. **If a router has two interfaces and is routing both IPv4 and IPv6 traffic, how many ACLs could be created and applied to it?**
   - 4
   - 6
   - **8***
   - 12
   - 16

   In calculating how many ACLs can be configured, use the rule of “three Ps”: one ACL per protocol, per direction, per interface. In this case, 2 interfaces x 2 protocols x 2 directions yields 8 possible ACLs.
8. **Which three statements are generally considered to be best practices in the placement of ACLs? (Choose three.)**
   - Place standard ACLs close to the source IP address of the traffic.

- Place extended ACLs close to the destination IP address of the traffic.
- **Filter unwanted traffic before it travels onto a low-bandwidth link.***
- **Place extended ACLs close to the source IP address of the traffic.***
- **Place standard ACLs close to the destination IP address of the traffic.***
- For every inbound ACL placed on an interface, there should be a matching outbound ACL.

Extended ACLs should be placed as close as possible to the source IP address, so that traffic that needs to be filtered does not cross the network and use network resources. Because standard ACLs do not specify a destination address, they should be placed as close to the destination as possible. Placing a standard ACL close to the source may have the effect of filtering all traffic, and limiting services to other hosts. Filtering unwanted traffic before it enters low-bandwidth links preserves bandwidth and supports network functionality. Decisions on placing ACLs inbound or outbound are dependent on the requirements to be met.

9. **Refer to the exhibit. Which command would be used in a standard ACL to allow only devices on the network attached to R2 G0/0 interface to access the networks attached to R1?**

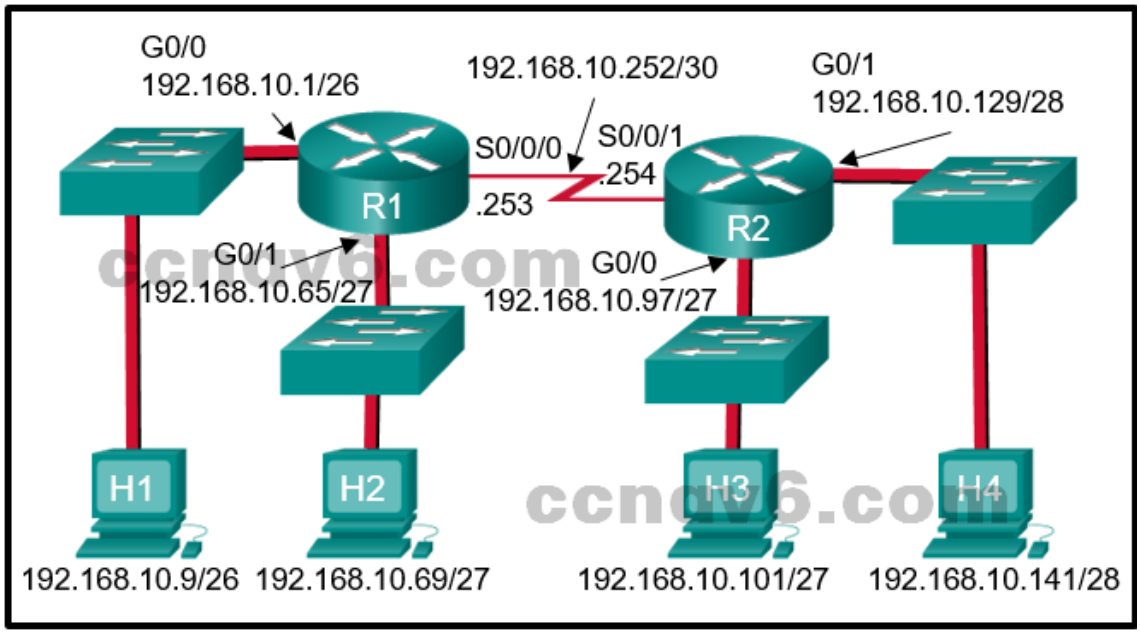


- access-list 1 permit 192.168.10.0 0.0.0.63
- **access-list 1 permit 192.168.10.96 0.0.0.31***
- access-list 1 permit 192.168.10.0 0.0.0.255
- access-list 1 permit 192.168.10.128 0.0.0.63

Standard access lists only filter on the source IP address. In the design, the packets would be coming from the 192.168.10.96/27 network (the R2 G0/0 network). The correct ACL is access-list 1 permit 192.168.10.96 0.0.0.31.

10. **Refer to the exhibit. If the network administrator created a standard ACL that allows only devices that connect to the R2 G0/0 network access to the devices on the R1 G0/1**

interface, how should the ACL be applied?



- inbound on the R2 G0/0 interface
- **outbound on the R1 G0/1 interface***
- inbound on the R1 G0/1 interface
- outbound on the R2 S0/0/1 interface

Because standard access lists only filter on the source IP address, they are commonly placed closest to the destination network. In this example, the source packets will be coming from the R2 G0/0 network. The destination is the R1 G0/1 network. The proper ACL placement is outbound on the R1 G0/1 interface.

11. **Refer to the following output. What is the significance of the 4 match(es) statement?**
    R1# <output omitted>
    10 permit 192.168.1.56 0.0.0.7
    20 permit 192.168.1.64 0.0.0.63 (4 match(es))
    30 deny any (8 match(es))
    - Four packets have been denied that have been sourced from any IP address.
    - Four packets have been denied that are destined for the 192.168.1.64 network.
    - **Four packets have been allowed through the router from PCs in the network of 192.168.1.64.***
    - Four packets have been allowed through the router to reach the destination network of 192.168.1.64/26.

    The show access-lists command shows how many packets have met the criteria for each ACE in terms of a specific number of “matches.”
12. **On which router should the show access-lists command be executed?**
    - on the router that routes the packet referenced in the ACL to the final destination network
    - on the router that routes the packet referenced in the ACL from the source network
    - on any router through which the packet referenced in the ACL travels
    - **on the router that has the ACL configured***

    The show access-lists command is only relevant to traffic passing through the router on which the ACL is configured.
13. **What is the quickest way to remove a single ACE from a named ACL?**

- **Use the no keyword and the sequence number of the ACE to be removed.***
- Use the no access-list command to remove the entire ACL, then recreate it without the ACE.
- Copy the ACL into a text editor, remove the ACE, then copy the ACL back into the router.
- Create a new ACL with a different number and apply the new ACL to the router interface.

Named ACL ACEs can be removed using the no command followed by the sequence number.

14. **Which feature will require the use of a named standard ACL rather than a numbered standard ACL?**
    - the ability to filter traffic based on a specific protocol
    - the ability to filter traffic based on an entire protocol suite and destination
    - the ability to specify source and destination addresses to use when identifying traffic
    - **the ability to add additional ACEs in the middle of the ACL without deleting and re-creating the list***

    Standard ACLs (whether numbered or named) only filter on the source IP address. Having a named ACL makes it easier at times to identify the purpose as well as modify the ACL.
15. **An administrator has configured an access list on R1 to allow SSH administrative access from host 172.16.1.100. Which command correctly applies the ACL?**
    - R1(config-if)# ip access-group 1 in
    - R1(config-if)# ip access-group 1 out
    - **R1(config-line)# access-class 1 in***
    - R1(config-line)# access-class 1 out

    Administrative access over SSH to the router is through the vty lines. Therefore, the ACL must be applied to those lines in the inbound direction. This is accomplished by entering line configuration mode and issuing the access-class command.
16. **Which type of router connection can be secured by the access-class command?**
    - **vty***
    - console
    - serial
    - Ethernet

    Access to vty lines can be filtered with an ACL and applied using the access-class in command.
17. **Consider the following output for an ACL that has been applied to a router via the access-class in command. What can a network administrator determine from the output that is shown?**

```
R1# <output omitted>

Standard IP access list 2

10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)

20 deny any (1 match)
```

- Two devices connected to the router have IP addresses of 192.168.10.x.
- Traffic from one device was not allowed to come into one router port and be routed outbound a different router port.

- **Two devices were able to use SSH or Telnet to gain access to the router.***
- Traffic from two devices was allowed to enter one router port and be routed outbound to a different router port.

The access-class command is used only on VTY ports. VTY ports support Telnet and/or SSH traffic. The match permit ACE is how many attempts were allowed using the VTY ports. The match deny ACE shows that a device from a network other than 192.168.10.0 was not allowed to access the router through the VTY ports.

18. **Refer to the exhibit. A router has an existing ACL that permits all traffic from the 172.16.0.0 network. The administrator attempts to add a new ACE to the ACL that denies packets from host 172.16.0.1 and receives the error message that is shown in the exhibit. What action can the administrator take to block packets from host 172.16.0.1 while still permitting all other traffic from the 172.16.0.0 network?**

```
Router(config)# access-list 1 deny 172.16.0.1
% Access rule can't be configured at higher sequence num
as it is part of the existing rule at sequence num 10
Router(config)# exit
Router# show access-lists 1
Standard IP access list 1
    10 permit 172.16.0.0, wildcard bits 0.0.255.255
```

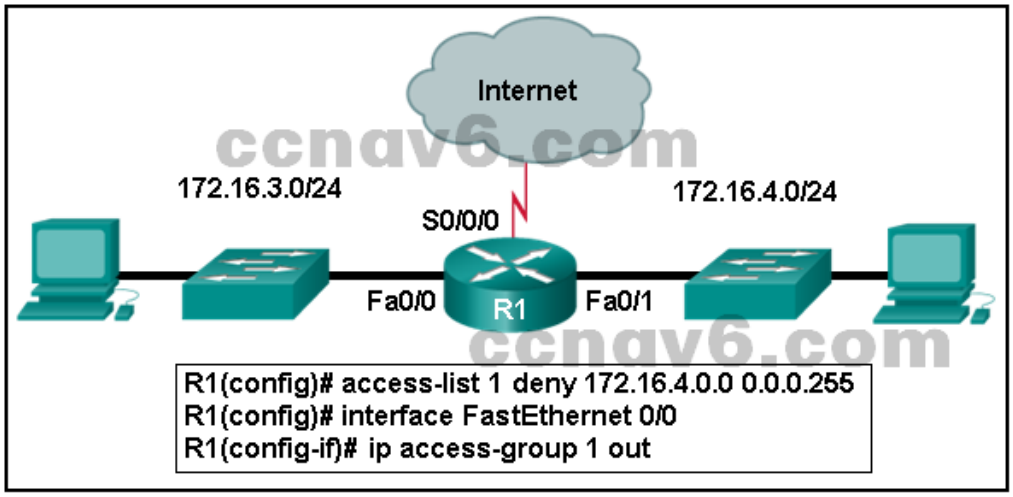
ccnav6.com

- **Manually add the new deny ACE with a sequence number of 5.***
- Manually add the new deny ACE with a sequence number of 15.
- Create a second access list denying the host and apply it to the same interface.
- Add a deny any any ACE to access-list 1.

Because the new deny ACE is a host address that falls within the existing 172.16.0.0 network that is permitted, the router rejects the command and displays an error message. For the new deny ACE to take effect, it must be manually configured by the administrator with a sequence number that is less than 10.

19. **A network administrator issues the show vlan brief command while troubleshooting a user support ticket. What output will be displayed?**
    - **the VLAN assignment and membership for all switch ports***
    - the VLAN assignment and trunking encapsulation
    - the VLAN assignment and native VLAN
    - the VLAN assignment and membership for device MAC addresses
20. **Refer to the exhibit. An ACL was configured on R1 with the intention of denying traffic from subnet 172.16.4.0/24 into subnet 172.16.3.0/24. All other traffic into subnet 172.16.3.0/24 should be permitted. This standard ACL was then applied outbound on**

interface Fa0/0. Which conclusion can be drawn from this configuration?



- Only traffic from the 172.16.4.0/24 subnet is blocked, and all other traffic is allowed.
- An extended ACL must be used in this situation.
- The ACL should be applied to the FastEthernet 0/0 interface of R1 inbound to accomplish the requirements.
- **All traffic will be blocked, not just traffic from the 172.16.4.0/24 subnet.***
  The ACL should be applied outbound on all interfaces of R1.

Because of the implicit deny at the end of all ACLs, the access-list 1 permit any command must be included to ensure that only traffic from the 172.16.4.0/24 subnet is blocked and that all other traffic is allowed.

21. **Refer to the exhibit. What will happen to the access list 10 ACEs if the router is rebooted before any other commands are implemented?**

```
Router# show access-lists
Standard IP access list 10
    50 permit 172.16.50.5
    40 permit 172.16.40.5
    10 deny   172.16.30.0, wildcard bits 0.0.0.255
    20 deny   172.16.20.0, wildcard bits 0.0.0.255
    30 deny   172.16.10.0, wildcard bits 0.0.0.255
Router# copy running-config startup-config
```

- The ACEs of access list 10 will be deleted.
- The ACEs of access list 10 will not be affected.
- **The ACEs of access list 10 will be renumbered.***
- The ACEs of access list 10 wildcard masks will be converted to subnet masks.

After a reboot, access list entries will be renumbered to allow host statements to be listed first and thus more efficiently processed by the Cisco IOS.

22. **What is the effect of configuring an ACL with only ACEs that deny traffic?**
- The ACL will permit any traffic that is not specifically denied.
- **The ACL will block all traffic.***
- The ACL must be applied inbound only.
- The ACL must be applied outbound only.

Because there is a deny any ACE at the end of every standard ACL, the effect of having all deny statements is that all traffic will be denied regardless of the direction in which the ACL is applied.

23. **Which type of ACL statements are commonly reordered by the Cisco IOS as the first ACEs?**
    - **host***
    - range
    - permit any
    - lowest sequence number

    ACEs are commonly reordered from the way they were entered by the network administrator. The ACEs that have host criteria such as in the statement permit host 192.168.10.5, are reordered as the first statements because they are the most specific (have the most number of bits that must match).

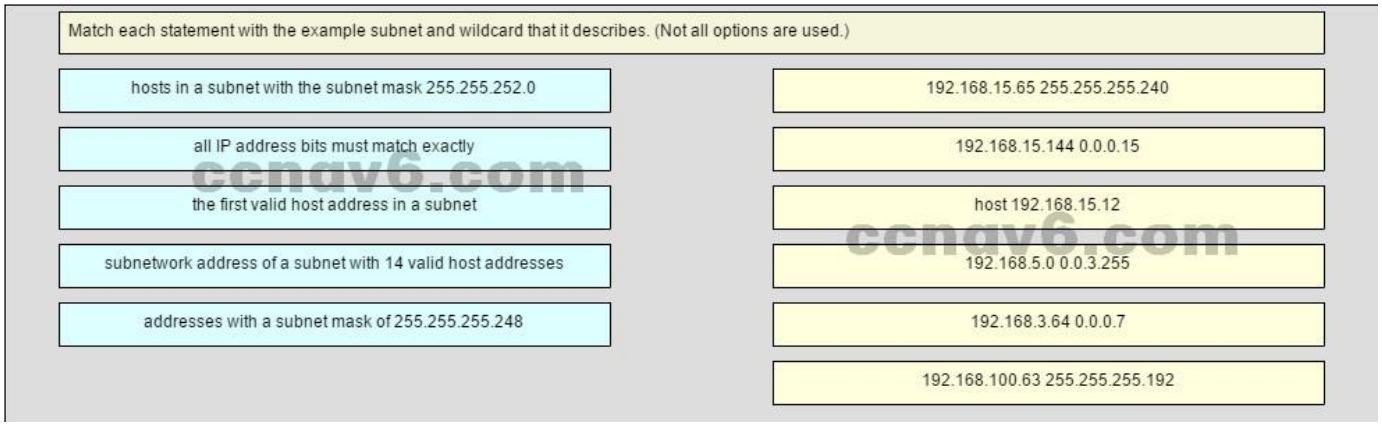
24. **A network administrator is configuring an ACL to restrict access to certain servers in the data center. The intent is to apply the ACL to the interface connected to the data center LAN. What happens if the ACL is incorrectly applied to an interface in the inbound direction instead of the outbound direction?**
    - All traffic is denied.
    - All traffic is permitted.
    - **The ACL does not perform as designed.***
    - The ACL will analyze traffic after it is routed to the outbound interface.

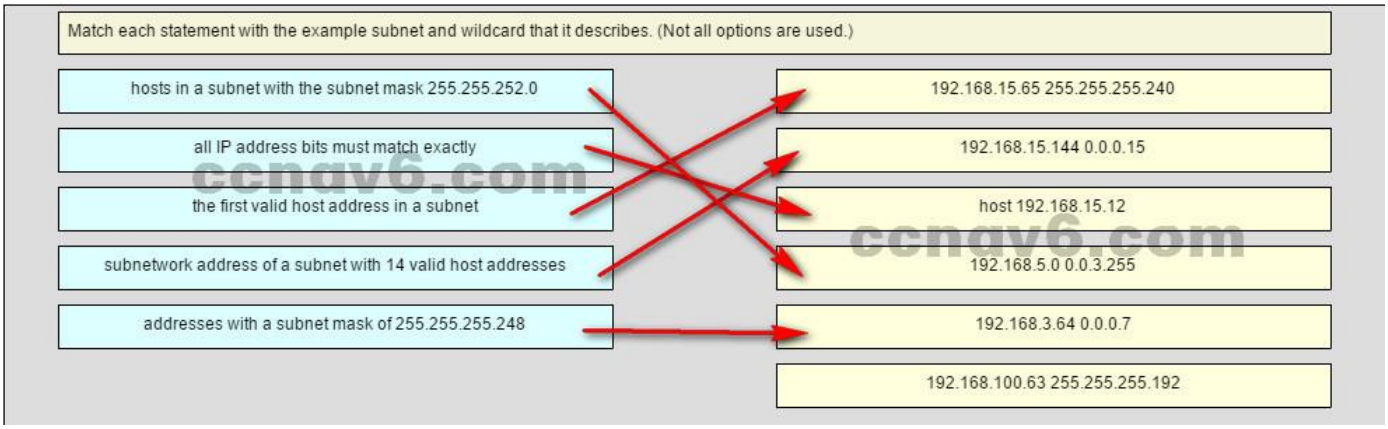
    Always test an ACL to ensure that it performs as it was designed. Applying an ACL that is applied using the ip access-group in command instead of using the ip access-group out command is not going to work as designed.

25. **When would a network administrator use the clear access-list counters command?**
    - when obtaining a baseline
    - when buffer memory is low
    - when an ACE is deleted from an ACL
    - **when troubleshooting an ACL and needing to know how many packets matched***

    The clear access-list counters command is used to reset all numbers relating to ACE match conditions that have been made within a particular ACE. The command is useful when troubleshooting an ACL that has recently been deployed.

26. **Match each statement with the example subnet and wildcard that it describes. (Not all options are used.)**





Place the options in the following order:
192.168.15.65 255.255.255.240 ==> the first valid host address in a subnet
192.168.15.144 0.0.0.15 ==> subnetwork address of a subnet with 14 valid host addreses
host 192.168.15.2 ==> all IP address bits must match exactly
192.168.5.0 0.0.3.255 ==> hosts in a subnet with SM 255.255.252.0
192.168.3.64 0.0.0.7 ==> address with a subnet 255.255.255.248

Converting the wildcard mask 0.0.3.255 to binary and subtracting it from 255.255.255.255 yields a subnet mask of 255.255.252.0.
Using the host parameter in a wildcard mask requires that all bits match the given address.
192.168.15.65 is the first valid host address in a subnetwork beginning with the subnetwork address 192.168.15.64. The subnet mask contains 4 host bits, yielding subnets with 16 addresses.
192.168.15.144 is a valid subnetwork address in a similar subnetwork. Change the wildcard mask 0.0.0.15 to binary and subtract it from 255.255.255.255, and the resulting subnet mask is 255.255.255.240.
192.168.3.64 is a subnetwork address in a subnet with 8 addresses. Convert 0.0.0.7 to binary and subtract it from 255.255.255.255, and the resulting subnet mask is 255.255.255.248. That mask contains 3 host bits, and yields 8 addresses.

Older Version: CCNA 2 Chapter 7 Exam Answers v5.1

1. **What two tasks do dynamic routing protocols perform? (Choose two.)**
   - discover hosts
   - **update and maintain routing tables***
   - propagate host default gateways
   - **network discovery***
   - assign IP addressing
2. **What is a disadvantage of using dynamic routing protocols?**
   - They are only suitable for simple topologies.
   - Their configuration complexity increases as the size of the network grows.
   - **They send messages about network status insecurely across networks by default.***
   - They require administrator intervention when the pathway of traffic changes.

3. **Which two statements are true regarding classless routing protocols? (Choose two.)**
   - **sends subnet mask information in routing updates***
   - sends complete routing table update to all neighbors
   - is supported by RIP version 1
   - **allows for use of both 192.168.1.0/30 and 192.168.1.16/28 subnets in the same topology***
   - reduces the amount of address space available in an organization
4. **An OSPF enabled router is processing learned routes to select best paths to reach a destination network. What is the OSPF algorithm evaluating as the metric?**
   - The amount of packet delivery time and slowest bandwidth.
   - The number of hops along the routing path.
   - The amount of traffic and probability of failure of links.
   - **The cumulative bandwidth that is used along the routing path.***
5. **After a network topology change occurs, which distance vector routing protocol can send an update message directly to a single neighboring router without unnecessarily notifying other routers?**
   - IS-IS
   - RIPv2
   - **EIGRP***
   - OSPF
   - RIPv1
6. **What is the purpose of the passive-interface command?**
   - allows a routing protocol to forward updates out an interface that is missing its IP address
   - allows a router to send routing updates on an interface but not receive updates via that interface
   - allows an interface to remain up without receiving keepalives
   - allows interfaces to share IP addresses
   - **allows a router to receive routing updates on an interface but not send updates via that interface***
7. **Refer to the exhibit. Based on the partial output from the show ip route command, what two facts can be determined about the RIP routing protocol? (Choose two.)**

```
     10.0.0.0/8 is variably subnetted, 4 subnets, 6 masks
C       10.0.0.0/25 is directly connected, GigabitEthernet0/1
L       10.0.0.1/32 is directly connected, GigabitEthernet0/1
C       10.0.0.128/26 is directly connected, GigabitEthernet0/0
L       10.0.0.129/32 is directly connected, GigabitEthernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
R       172.16.0.0/25 [120/1] via 192.168.1.1, 00:00:12, Serial0/1/0
R       172.16.0.128/25 [120/1] via 192.168.1.1, 00:00:12, Serial0/1/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.1.0/30 is directly connected, Serial0/1/0
L       192.168.1.2/32 is directly connected, Serial0/1/0
```

CCNA2 Chapter 7 v5.03 001

   - **RIP version 2 is running on this router and its RIP neighbor.***
   - The metric to the network 172.16.0.0 is 120.
   - RIP version 1 is running on this router and its RIP neighbor.
   - **The command no auto-summary has been used on the RIP neighbor router.***
   - RIP will advertise two networks to its neighbor.

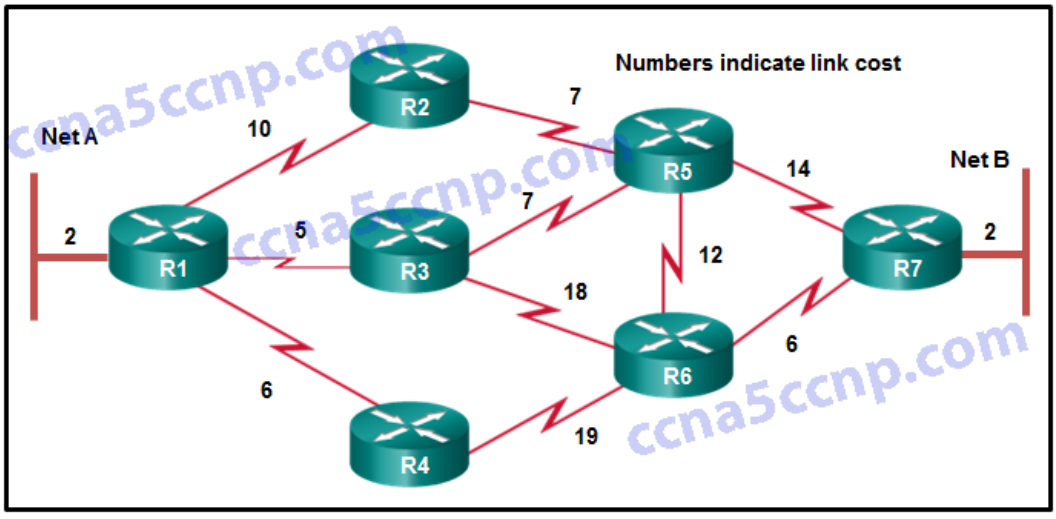
8. **While configuring RIPv2 on an enterprise network, an engineer enters the command network 192.168.10.0 into router configuration mode.**
   What is the result of entering this command?
   - The interface of the 192.168.10.0 network is sending version 1 and version 2 updates.
   - The interface of the 192.168.10.0 network is receiving version 1 and version 2 updates.
   - **The interface of the 192.168.10.0 network is sending only version 2 updates.***
   - The interface of the 192.168.10.0 network is sending RIP hello messages.
9. **Refer to the exhibit. A network administrator has issued the exhibited commands in an attempt to activate RIPng on interface gig0/0. What is causing the console message that is shown after RIP is enabled?**

```
R3# configure terminal
R3(config)# interface gigabitEthernet 0/0
R3(config-if)# ipv6 address 2001:db8:cafe:3::100/64
R3(config-if)# ipv6 rip RIP-AS enable
% IPv6 routing not enabled
R3(config-if)#
```

ccna5ccnp.com

CCNA2 Chapter 7 v5.03 004

   - Interface gig0/0 is shutdown.
   - Interface gig0/0 does not have a valid IPv6 address.
   - **IPv6 unicast routing has not been enabled on this router.***
   - IPv6 is not supported on this IOS.
10. **Refer to the exhibit. OSPF is used in the network. Which path will be chosen by OSPF to send data packets from Net A to Net B?**



CCNA2 Chapter 7 v5.03 002

   - R1, R2, R5, R7
   - **R1, R3, R5, R7***
   - R1, R3, R6, R7
   - R1, R4, R6, R7
   - R1, R3, R5, R6, R7

11. **Which two events will trigger the sending of a link-state packet by a link-state routing protocol? (Choose two.)**
    - the router update timer expiring
    - a link to a neighbor router has become congested
    - **a change in the topology ***
    - **the initial startup of the routing protocol process***
    - the requirement to periodically flood link-state packets to all neighbors
12. **Which two requirements are necessary before a router configured with a link-state routing protocol can build and send its link-state packets? (Choose two.)**
    - **The router has determined the costs associated with its active links.***
    - The router has built its link-state database.
    - The routing table has been refreshed.
    - **The router has established its adjacencies.***
    - The router has constructed an SPF tree.
13. **When does a link-state router send LSPs to its neighbors?**
    - every 30 seconds
    - **immediately after receiving an LSP from neighbors with updates***
    - only when one of its interfaces goes up or down
    - only when one of its neighbors requests an update
14. **Which routing protocol uses link-state information to build a map of the topology for computing the best path to each destination network?**
    - **OSPF***
    - EIGRP
    - RIP
    - RIPng
15. **A destination route in the routing table is indicated with a code D. Which kind of route entry is this?**
    - a static route
    - a route used as the default gateway
    - a network directly connected to a router interface
    - **a route dynamically learned through the EIGRP routing protocol***
16. **Refer to the exhibit. Which interface will be the exit interface to forward a data packet with the destination IP address 172.16.0.66?**

```
R1# show ip route
<output omitted>

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
R        172.16.0.0/26 [120/1] via 192.168.1.1, 00:00:24, Serial0/0/0
D        172.16.0.64/26 [90/2170112] via 192.168.1.6, 00:05:56, Serial0/0/1
R        172.16.0.128/26 [120/1] via 192.168.1.1, 00:00:24, Serial0/0/0
C        172.16.0.192/27 is directly connected, GigabitEthernet0/0
L        172.16.0.193/32 is directly connected, GigabitEthernet0/0
C        172.16.0.224/27 is directly connected, GigabitEthernet0/1
L        172.16.0.225/32 is directly connected, GigabitEthernet0/1
      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial0/0/0
L        192.168.1.2/32 is directly connected, Serial0/0/0
C        192.168.1.4/30 is directly connected, Serial0/0/1
L        192.168.1.5/32 is directly connected, Serial0/0/1
      192.168.2.0/30 is subnetted, 1 subnets
R        192.168.2.0/30 [120/1] via 192.168.1.1, 00:00:24, Serial0/0/0
R1#
```

CCNA2 Chapter 7 v5.03 003

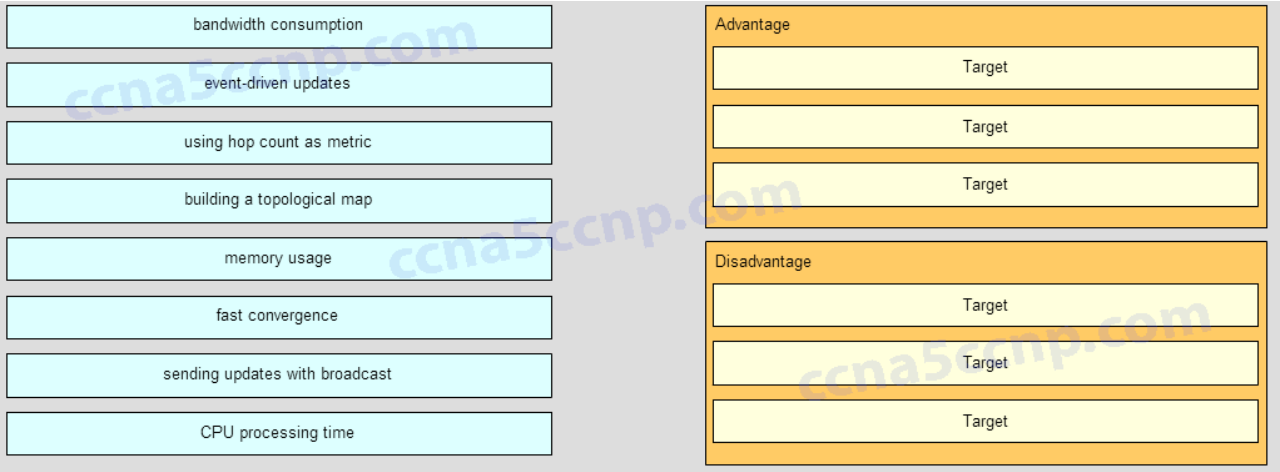
- Serial0/0/0
- **Serial0/0/1***
- GigabitEthernet0/0
- GigabitEthernet0/1

17. **Which two requirements are used to determine if a route can be considered as an ultimate route in a router's routing table? (Choose two.)**
    - contain subnets
    - be a default route
    - **contain an exit interface***
    - be a classful network entry
    - **contain a next-hop IP address***
18. **Which route is the best match for a packet entering a router with a destination address of 10.16.0.2?**
    - S 10.0.0.0/8 [1/0] via 192.168.0.2
    - **S 10.16.0.0/24 [1/0] via 192.168.0.9***
    - S 10.16.0.0/16 is directly connected, Ethernet 0/1
    - S 10.0.0.0/16 is directly connected, Ethernet 0/0
19. **Which type of route will require a router to perform a recursive lookup?**
    - **an ultimate route that is using a next hop IP address on a router that is not using CEF***
    - a level 2 child route that is using an exit interface on a router that is not using CEF
    - a level 1 network route that is using a next hop IP address on a router that is using CEF
    - a parent route on a router that is using CEF
20. **A router is configured to participate in multiple routing protocol: RIP, EIGRP, and OSPF. The router must send a packet to network 192.168.14.0. Which route will be used to forward the traffic?**
    - **a 192.168.14.0 /26 route that is learned via RIP***
    - a 192.168.14.0 /24 route that is learned via EIGRP

- a 192.168.14.0 /25 route that is learned via OSPF
- a 192.168.14.0 /25 route that is learned via RIP

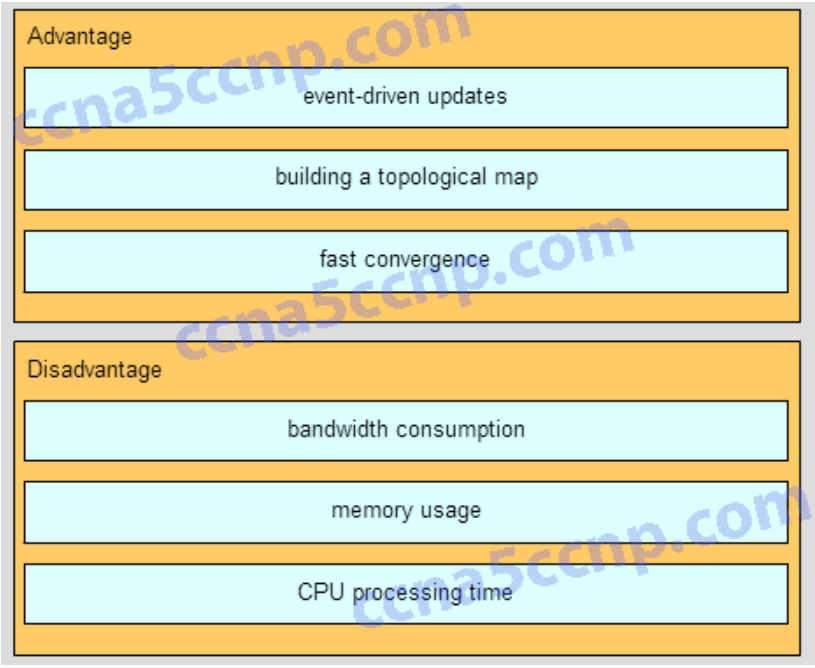
21. **Fill in the blank. Do not abbreviate.**
When configuring RIPng, the **default-information originate** command instructs the router to propagate a static default route.

22. **Match the features of link-state routing protocols to their advantages and disadvantages. (Not all options are used.)**
- Question



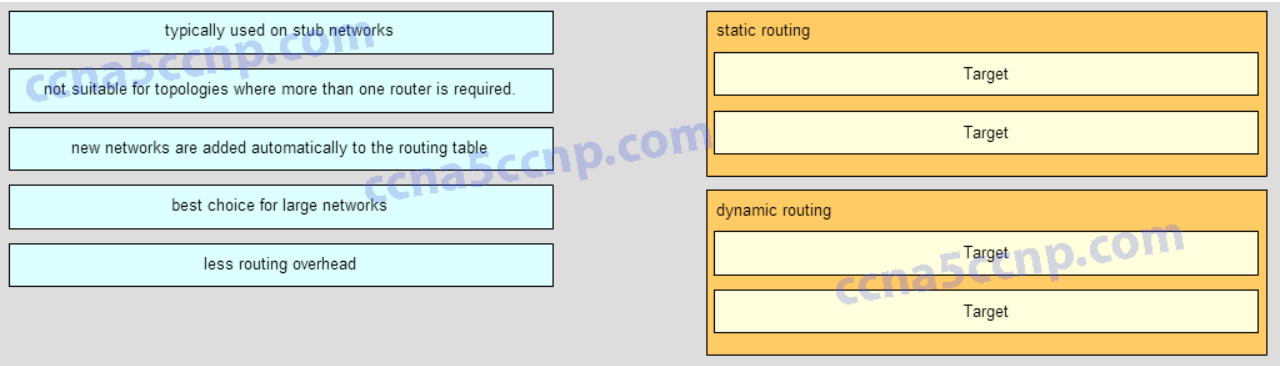
CCNA2 Chapter 7 v5.03 Question 001

- Answer



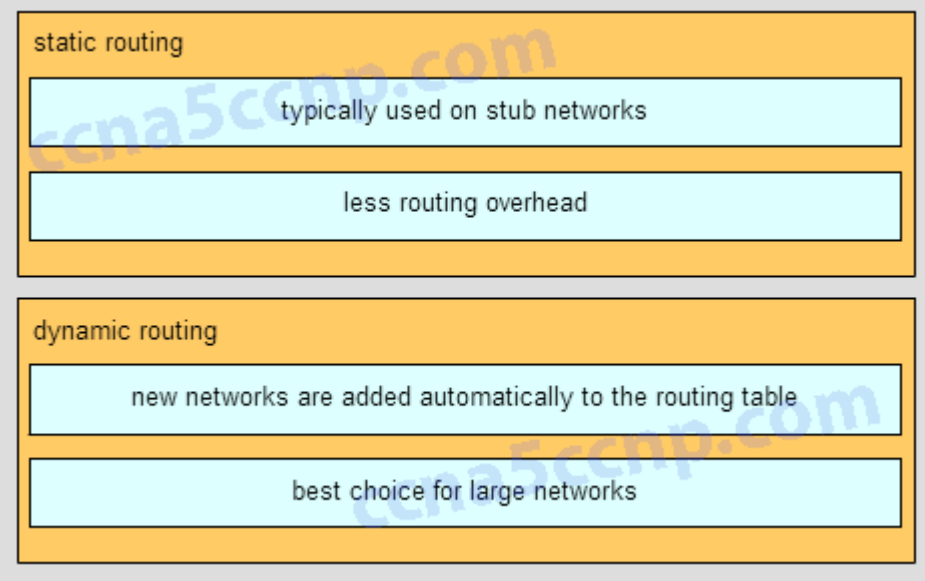
CCNA2 Chapter 7 v5.03 Answer 001

23. **Match the characteristic to the corresponding type of routing. (Not all options are used.)**
- Question



CCNA2 Chapter 7 v5.03 Question 002

- Answer

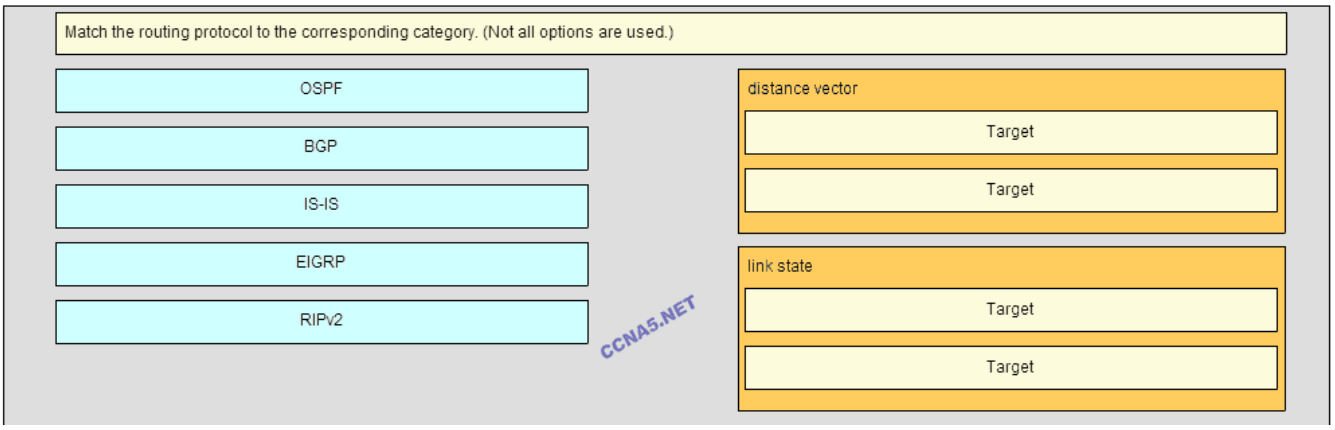


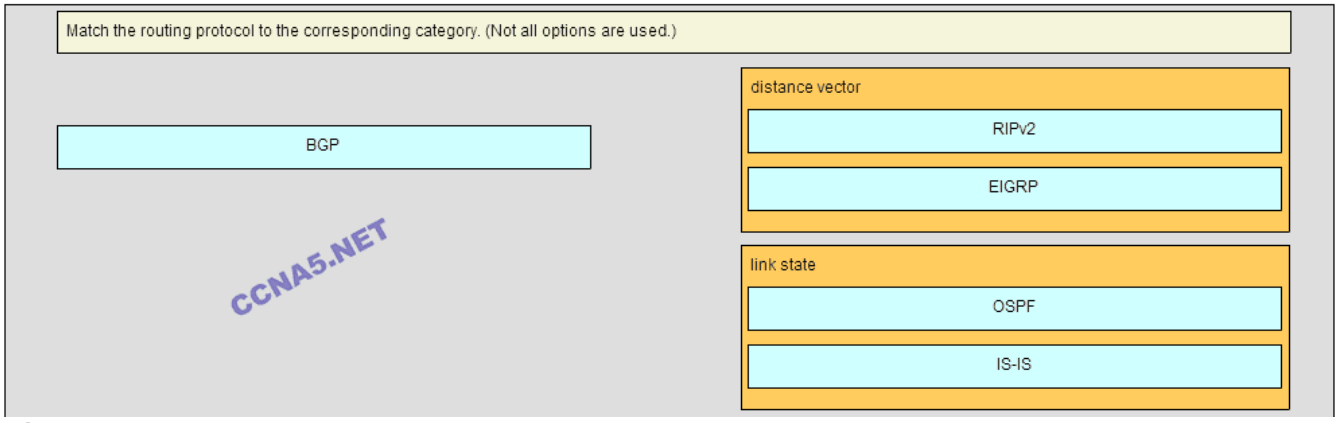
CCNA2 Chapter 7 v5.03 Answer 002

24. **Which two statements describe the OSPF routing protocol? (Choose two.)**
    - automatically summarizes networks at the classful boundaries
    - has an administrative distance of 100
    - **calculates its metric using bandwidth ***
    - **uses Dijkstra's algorithm to build the SPF tree***
    - used primarily as an EGP
25. **What two actions result from entering the network 192.168.1.0 command in RIP configuration mode on a router? (Choose two**.)
    - **The network address 192.168.1.0 is advertised to the neighbor routers. ***
    - **Routing updates are sent through all the interfaces belonging to 192.168.1.0.***
    - The routing table is created in the RAM of the router.
    - The RIP process is stopped and all existing RIP configurations are erased.
    - The neighboring routers are sent a request for routing updates. *
26. **Which dynamic routing protocol was developed as an exterior gateway protocol to interconnect different Internet provider**s?
    - **BGP***
    - EIGRP

- OSPF
- RIP

27. **In the context of routing protocols, what is a definition for time to convergence?**
    - the amount of time a network administrator needs to configure a routing protocol in a small- to medium-sized network
    - the capability to transport data, video, and voice over the same media
    - a measure of protocol configuration complexity
    - **the amount of time for the routing tables to achieve a consistent state after a topology change***
28. **A destination route in the routing table is indicated witha code D. Which kind of route entry is this?**
    - a static route
    - a route used as the default gateway
    - a network directly connected to a router interface
    - **a route dynamically learned through the EIGRP routing protocol***
29. **Match the router protocol to the corresponding category. (Not all options are used.)**





Distance vector
RIOv2
EIGRPLink state
OSPF
IS-IS

30. **Which route is the best match for a packet entering a router with a destination address of 10.16.0.2?**
    S 10.16.0.0/16 is directly connected, Ethernet 0/1

S 10.16.0.0/24 [1/0] via 192.168.0.9*
S 10.0.0.0/8 [1/0] via 192.168.0.2
S 10.0.0.0/16 is directly connected, Ethernet 0/0

31. **What is different between IPv6 routing table entries compared to IPv4 routing table entries?**
    - **By design IPv6 is classless so all routes are effectively level 1 ultimate routes.***
    - IPv6 does not use static routes to populate the routing table as used in IPv4.
    - IPv6 routing tables include local route entries which IPv4 routing tables do not.
    - The selection of IPv6 routes is based on the shortest matching prefix, unlike IPv4 route selection which is based on the longest matching prefix.
32. **Which route will a router use to forward an IPv4 packet after examining its routing table for the best match with the destination address?**
    - a level 1 child route
    - a level 1 parent route
    - a level 2 supernet route
    - **a level 1 ultimate route***