CCNA2 v6.0 Chapter 7 Exam Answer 2017

Posted on January 29, 2017 by Admin

CCNA2 v6.0 Chapter 7 Exam Answer 2017

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
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
3. **Which statement describes a difference between the operation of inbound and outbound ACLs?**

CCNA7

Categories

CCNA 1 v5.02 Routing and Switching 2015(100%)
CCNA 1 v5.1 Introduction to Networks
CCNA 1 v5.1 Online Assessement
CCNA 1 v6.0 Introduction to Networks
CCNA 2 v5.02 Routing and Switching 2015(100%)
CCNA 2 V5.03 Routing and Switching Essentials
CCNA 2 v6.0 Routing and Switching Essentials
CCNA 3 v5.02 Routing and Switching 2015(100%)
CCNA 3 v5.03 Scaling Networks
CCNA 4 v5.02 Routing and Switching 2015(100%)
CCNA 4 v5.03 Connecting Networks
CCNA Lab Exam
CCNA Routing and Switching Courseware
CCNA Security Exam Answer v1.2 (100%)
CCNA Security Exam Answer v2
Cisco Learning
ITE – IT Essentials v6.0
ITE v5.02 Exam 2015 100%
Linux Essentials (LPI-010)
LPIC-1 101
LPIC-1 102
Microsoft Learning
Window Tip

- 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.
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

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

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

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.

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

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

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.

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

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.

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

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

16. **Which type of router connection can be secured by the access-class command?**
    - vty
    - console
    - serial
    - Ethernet
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.
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?**
    - 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.

19. **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.
20. **Refer to the exhibit. What will happen to the access list 10 ACEs if the router is rebooted before any other commands are implemented?**
    - 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.
21. **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.
22. **Which type of ACL statements are commonly reordered by the Cisco IOS as the first ACEs?**
    - host
    - range
    - permit any
    - lowest sequence number
23. **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?

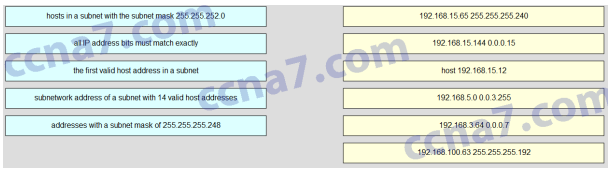
- All traffic is denied.
- All traffic is permitted.
- The ACL does not perform as designed.
- The ACL will analyze traffic after it is routed to the outbound interface.

24. **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

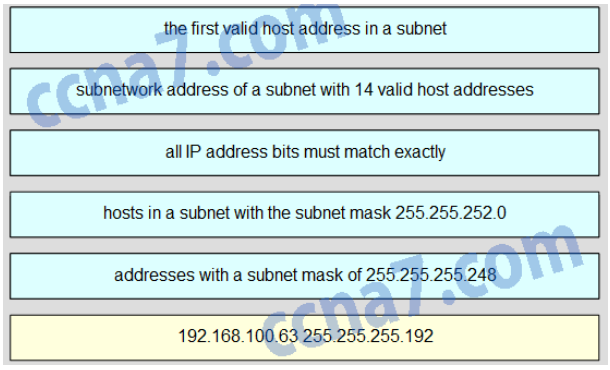
25. **Match each statement with the example subnet and wildcard that it describes. (Not all options are used.)**

- Question



CCNA2 v6.0 Chapter 7 Exam Q001

- Answer



CCNA2 v6.0 Chapter 7 Exam A001

Comments

comments


CCNA7.COM
SiteLock
MALWARE-FREE
Passed
23-Oct-2017