1. Jupiter is a host with IP address 10.1.1.1 in subnet 10.1.1.0/24. Which of the following are things that a standard IP ACL could be configured to do? (Choose two answers.)

a. Match the exact source IP address.
b. Match IP addresses 10.1.1.1 through 10.1.1.4 with one access-list command without matching other IP addresses.
c. Match all IP addresses in Barney's subnet with one access-list command without matching other IP addresses.
d. Match only the packet's destination IP address.

2. Which of the following answers list a valid number that can be used with standard numbered IP ACLs? (Choose two answers.)

a. 1987
b. 2187
c. 187
d. 87

3. Which of the following wildcard masks is most useful for matching all IP packets in subnet 10.1.128.0, mask 255.255.255.0?

a. 0.0.0.0
b. 0.0.0.31
c. 0.0.0.240
d. 0.0.0.255
e. 0.0.15.0
f. 0.0.248.255

4. Which of the following wildcard masks is most useful for matching all IP packets in subnet 10.1.128.0, mask 255.255.240.0?

a. 0.0.0.0
b. 0.0.0.31
c. 0.0.0.240
d. 0.0.0.255
e. 0.0.15.255
f. 0.0.248.255

5. ACL 1 has three statements, in the following order, with address and wildcard mask values as follows:

1.0.0.0 0.255.255.255

1.1.0.0 0.0.255.255

1.1.1.0 0.0.0.255

If a router tried to match a packet sourced from IP address 1.1.1.1 using this ACL, which ACL statement does a router consider the packet to have matched?

a. First
b. Second
c. Third

d. Implied deny at the end of the ACL

6. Which of the following access-list commands matches all packets sent from hosts in subnet 172.16.5.0/25?

a. access-list 1 permit 172.16.0.5 0.0.255.0
b. access-list 1 permit 172.16.4.0 0.0.1.255
c. access-list 1 permit 172.16.5.0
d. access-list 1 permit 172.16.5.0 0.0.0.128

7. Which of the following fields cannot be compared based on an extended IP ACL? (Choose two answers.)

a. Protocol
b. Source IP address
c. Destination IP address
d. Source Port
e. URL
f. Filename for FTP transfers

8. Which of the following access-list commands permit packets going from host 10.1.1.1 to all web servers whose IP addresses begin with 172.16.5? (Choose two answers.)

a. access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
b. access-list 1951 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
c. access-list 2523 permit ip host 10.1.1.1 eq www 172.16.5.0 0.0.0.255
d. access-list 2523 permit tcp host 10.1.1.1 eq www 172.16.5.0 0.0.0.255
e. access-list 2523 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www

9. Which of the following access-list commands permits packets going to any web client from all web servers whose IP addresses begin with 172.16.5?

a. access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
b. access-list 1951 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
c. access-list 2523 permit tcp any eq www 172.16.5.0 0.0.0.255
d. access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www 172.16.5.0 0.0.0.255
e. access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www any

10. Which of the following fields can be compared using a named extended IP ACL but not a numbered extended IP ACL?

a. Protocol
b. Source IP address
c. Destination IP address
d. TOS byte
e. None of the other answers are correct.

11. In a router running a recent IOS version (at least version 15.0), an engineer needs to delete the second line in ACL 101, which currently has four commands configured. Which of the following options could be used? (Choose two answers.)

a. Delete the entire ACL and reconfigure the three ACL statements that should remain in the ACL.
b. Delete one line from the ACL using the no access-list... global command.
c. Delete one line from the ACL by entering ACL configuration mode for the ACL and then deleting only the second line based on its sequence number.
d. Delete the last three lines from the ACL from global configuration mode, and then add the last two statements back into the ACL.

12. What general guideline should you follow when placing extended IP ACLs?

a. Perform all filtering on output if at all possible.
b. Put more general statements early in the ACL.
c. Filter packets as close to the source as possible.
d. Order the ACL commands based on the source IP addresses, from lowest to highest, to improve performance.