

1) Which two of the following access list entries will deny DNS?

- access-list 99 deny ip any host eq dns
- access-list 101 deny tcp any any eq 21
- access-list 120 deny tcp any any eq 53
- access-list 120 deny udp any any eq 53
- access-list 120 deny tcp any any eq 23
- access-list 120 deny udp any any eq 23

2) Which router command allows you to determine if an IP access-list is enabled on a particular interface?

- show ip interface
- show access-list
- show ip access-list
- show interface ip access-list

3) The following access list has been applied to your router:

```
access-list 110 permit ip 192.168.20.0 0.0.0.255 any
```

What is the effect?

- Permit all packets matching the last octet of the destination address to any source.
- Permit all packets matching the first three octets of the destination address to any source.
- Permit all packets matching the last octet of the source address to any destination.
- Permit all packets matching the first three octets of the source address to any destination.

4) Which of the following commands will show you the access lists configured on your Cisco router?

- show access list
- show access-list
- show access-list summary
- show access-list all

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

- 0.0.0.0
- 0.0.0.31
- 0.0.0.240
- 0.0.0.255
- 0.0.15.255
- 0.0.240.255

6) Given the following criteria for granting access from a remote site to your LAN:

Restrict access on interface E1
E1=207.87.81.173
Deny access to Telnet, FTP, SNMP
Allow all other types of operations

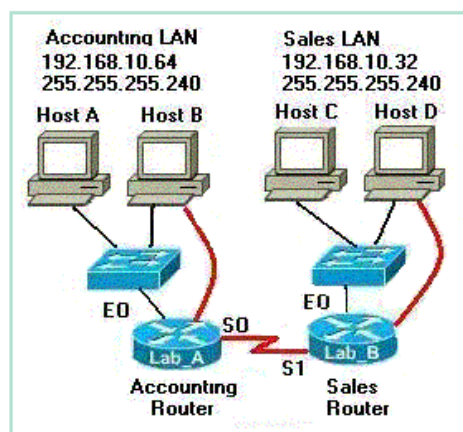
Which line should come last in configuring the access list?

- access-list 101
 - access-list 101 deny eo telnet ftp
 - access-list 101 allow all except ftp telnet
 - access-list 101 permit ip 0.0.0.0 255.255.255.255 any
 - access-list 101 deny ip 207.87.81.173 tcp eq 20 21 23
- 7) Which of the following wildcard masks is most useful for matching all IP packets in subnet 10.1.128.0 subnet mask 255.255.240.0?
- 0.0.0.0
 - 0.0.0.31
 - 0.0.0.240
 - 0.0.0.255
 - 0.0.15.255
 - 0.0.240.255
- 8) Which of the following "access-list" commands permits traffic that matches packets going to a web client from all web servers whose IP addresses begin with 172.16.5.0?
- access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
 - access-list 1951 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
 - access-list 2523 permit tcp any eq www 172.16.5.0 0.0.0.255
 - access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www 172.16.5.0 0.0.0.255
 - access-list 2523 permit tcp 172.16.5.0 0.0.0.255 eq www any

9) Refer to the exhibit. You are tasked to prevent users on the Accounting LAN from gaining access to the Sales LAN. You create the following access-list statement:

```
access-list 27 deny 192.168.10.64 0.0.0.15
```

Where would you apply this access-list?



- Outbound on E0 of the Accounting router
- Inbound on E0 of the Accounting router
- Inbound on E0 of the Sales router
- Outbound on E0 of the Sales router

10) Which of the following commands groups an access list to a vty interface?

- access-group
- access-vty
- access-list
- access-class
- access-console
- access-aux

11) Which of the following is a true statement regarding placement of access lists on an interface?

- apply as many access lists to an interface as needed
- apply only one access list to an interface
- apply one access list per direction, per protocol, on each interface
- the number of access lists applied to an interface is hardware related

12) Please review the following:

```
dublin#show access-list
Extended IP access list 110
Deny tcp any 172.16.10.32 0.0.0.15 eq 80
Deny tcp any any eq 23
```

```
Dublin# show ip interface ethernet 0
```

```
-----
```

```
outgoing access list is 110
inbound access list is not set
```

```
-----
```

What is the result of applying the access list to Ethernet 0?

- Only Telnet and HTTP traffic will be permitted out Ethernet0.
- FTP and Telnet will be denied out Ethernet0
- Telnet and HTTP will be denied out Ethernet0
- All IP traffic trying to route out Ethernet0 will be denied.
- This is not an extended access list for IP and will not function

13) What general guideline should be followed when placing IP Access Control Lists.

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

14) What does the following access-list allow?

```
access-list 1 permit 204.211.19.162 0.0.0.0
```

- Deny the network only.
- Permit a specific host.
- Permit the network only.
- None of the above.

15) Which two statements are generally true of the location of access-lists?

- Standard lists will most likely be placed close to the destination
- Standard lists will most likely be placed close to the source
- Extended lists will most likely be placed close to the destination
- Extended lists will most likely be placed close to the source
- Location of access lists is irrelevant.

16) The following access list has been applied to your router:

```
access-list 110 permit ip 192.168.20.0 0.0.0.255 any
```

What is the effect?

- Permit all packets matching the last octet of the destination address to any source.
- Permit all packets matching the first three octets of the destination address to any source.
- Permit all packets matching the last octet of the source address to any destination.
- Permit all packets matching the first three octets of the source address to any destination.

17) As a network administrator - you are tasked to deny 172.16.10.0/18 subnet access to the Accounting Server. What access list wildcard mask would perform this task?

- 255.63.0.0
- 0.0.63.255
- 0.63.255.255
- 255.255.63.0
- 0.0.0.255
- 255.255.63.255

18) Which command displays access list 111?

- show access-list 111
- show ip access list 111
- display ip address list 111
- display access-list 111 details

19) Which router command allows you to determine if an IP access-list is enabled on a particular interface?

- show ip interface
- show access-list
- show ip access-list
- show interface ip access-list

20) What type of networking device would be needed to implement access-lists to increase network security?

- Repeater
- Hub
- Switch
- Bridge
- Router
- Transceiver

21) Which of the following fields can be compared using a named IP Access Control List but not a numbered extended IP Access Control List?

- Protocol
- Source IP Address
- Destination address
- TOS byte
- All of the above
- None of the above

- 22) Which of the following wildcard masks is most useful for matching all IP packets in subnet 10.1.128.0 subnet mask 255.255.255.0?
- 0.0.0.0
 - 0.0.0.31
 - 0.0.0.240
 - 0.0.0.255
 - 0.0.15.0
 - 0.0.248.255
- 23) Access lists impart network security based on which two of the following factors?
- The data content of the packets
 - The destination subnet/host network for the packets
 - The source subnet/host network of the packets
 - The type of the network they are routed through
- 24) Which command is used to display the placement and direction of an IP access control list on a router?
- show access-list
 - show ip route
 - show ip interface
 - show extended access-list
 - show standard access-list
- 25) Where should an extended access control lists be placed?
- They should be placed as close to the source of the traffic to be denied.
 - They should be placed on the fastest interface available.
 - They should be placed as close as possible to the destination of the traffic to be denied.
 - They should be placed on the destination WAN link.
 - They should be placed on the destination LAN switch.
- 26) Which command displays the interfaces using a given access list?
- show filters
 - show ip interfaces
 - show active list
 - show interface parameters
 - configure ip access list
 - show access-list interfaces

29) Which two of the following "access-list" commands permits traffic that matches packets going to a web server from 10.1.1.1 for all web servers whose IP addresses begin with 172.16.5.0?

- access-list 101 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
- access-list 1951 permit ip host 10.1.1.1 172.16.5.0 0.0.0.255 eq www
- access list 2523 permit ip host 10.1.1.1 eq www 172.16.5.0 0.0.0.255
- access-list 2523 permit tcp host 10.1.1.1 eq www 172.16.5.0 0.0.0.255
- access-list 2523 permit tcp host 10.1.1.1 172.16.5.0 0.0.0.255 eq www

30) What does the term "any" mean in the extended list command below?

access-list 101 permit ip any 192.168.20.0 0.0.0.255 eq tcp

- Accept any source address
- Accept any destination address
- This is a standard access list and will not work
- This is a named access list and will not work.

31) Which three steps are required to configure and apply a standard access list on an interface?

- Define an access list number and its parameters.
- Enable an interface to become part of the access list group.
- Define the number of access lists to be supported on an interface.
- Copy the access list definition to each interface that will support it.
- Apply it at the source interface.
- Apply it at the destination destination.

32) Which two router CLI commands will display all access lists in a router?

- show protocols
- show version
- show access-list
- show ip route
- show running-config
- show interfaces

33) Which two steps are required to configure and apply a standard access list on an interface?

- Define an access list number and its parameters.
- Enable an interface to become part of the access list group.
- Define the number of access lists to be supported on an interface.
- Copy the access list definition to each interface that will support it.

34) Which two of the following access list entries will deny DNS?

- access-list 99 deny ip any host eq dns
- access-list 101 deny tcp any any eq 21
- access-list 120 deny tcp any any eq 53
- access-list 120 deny udp any any eq 53
- access-list 120 deny tcp any any eq 23
- access-list 120 deny udp any any eq 23

- 35) What type of access list allows more than 99 standard and 100 extended access lists to be created?
- Advanced
 - Upgraded
 - Generic
 - Destination
 - Source
 - Named
- 36) Which two of the following fields cannot be compared based on an extended IP Access Control List?
- Protocol
 - Source IP address
 - Destination IP address
 - TOS byte
 - URL
 - Filename for FTP transfers
- 37) Which two commands would allow a user who does not have the enable password find out what access lists have been configured and where they are enabled?
- show interfaces
 - show ip route
 - show access-list
 - show ip interface
 - show version
 - show flash
- 38) Which three of the following would be considered valid uses of ACLs (Access Control Lists)?
- Broadcast forwarding
 - Route table filtering
 - Logging terrabits of data sent across a WAN link
 - DDR (Dial-on-Demand Routing)
 - Classification of network traffic
- 39) Which of the following commands will show you the access lists configured on your Cisco router?
- show access list
 - show access-list
 - show access-list summary
 - show access-list all
- 40) Which range of numbers are valid in an extended IP access list?
- 100 - 199
 - 101 - 299
 - 1 - 99
 - 300 - 399
 - 400 - 499
 - 500 - 599

41) Given the following criteria for granting access from a remote site to your LAN:

Restrict access on interface E1

E1=207.87.81.173

Deny access to Telnet, FTP, SNMP

Allow all other types of operations

Which line should come last in configuring the access list?

- access-list 101
- access-list 101 deny eo telnet ftp
- access-list 101 allow all except ftp telnet
- access-list 101 permit ip 0.0.0.0 255.255.255.255 any
- access-list 101 deny ip 207.87.81.173 tcp eq 20 21 23