CCNA2 Summer 2004
Module 11 STUDY GUIDE

Network administrators must figure out how to deny unwanted access to the network while allowing appropriate access. Although security tools, such as passwords, callback equipment, and physical security devices, are helpful, they often lack the flexibility of basic traffic filtering and the specific controls most administrators prefer. For example, a network administrator might want to allow users access to the Internet, but might not want external users telnetting into the LAN.

1. ACLs are lists of instructions you apply to a router's interface. These lists tell the router what kinds of packets to accept and what kinds of packets to deny. Acceptance and denial can be based on certain specifications, such as _____ _____**,** _____ _____**,** and ____ number (upper layer protocol). ACLs enable you to manage traffic and scan specific packets. Any traffic going through the interface is tested against certain conditions that are part of the ACL.

2. ACLs can be created for all routed network protocols, such as IP or (IPX), to filter packets as the packets pass through a router. ACLs must be defined on a _____ basis. In other words, you must define an ACL for every protocol enabled on an interface if you want to control traffic flow for that interface. For example, if your router interface were configured for IP, AppleTalk, and IPX, you would need to define at least three ACLs.

3. ACLs can be used as a tool for network control by adding the flexibility to filter the packets that flow ____ or ___ of router interfaces.

4. List four reasons to create ACLs
   - _____
   - _____
   - _____
   - _____

5. The _____ in which you place ACL statements is important. When the router is deciding whether to forward or block a packet, the Cisco Internetwork Operating System (IOS) software tests the packet against each condition statement, in the order in which the statements were created.

Note: After a match is found, no more condition statements are checked. If you create a condition statement that permits all traffic, no statements added later will ever be checked.

6. If you need additional statements, in a standard or extended ACL you must _____ the ACL and re-create it with the new condition statements. This is why it's a good idea to edit the router configuration on a PC using a text editor and then Trivial File Transfer Protocol (TFTP) it to the router.

7. If all the ACL statements are unmatched, an implicit "____ ___" statement is imposed. This means that even though you don't see it as the last line of an ACL, it is there and if there are no matches in the ACL statements, the packets are _____**.**

In Summary an ACL is a group of statements that define how packets:

- _____
- _____
- _____

8. There are two steps in ACLs. They are:
   - _____
   - _____

9. If you want to alter an ACL containing numbered ACL statements, you need to delete all the statements in the numbered ACL by using the command __ _____ list-number command.

10. _____ ACLs are generally more efficient than inbound, and are therefore preferred.

11. List the range of numbers that correspond with the protocol.

Protocol	***Range***
IP	
Extended IP	
Appletalk	
IPX	
Extended IPX	
IPX Service Advertising Protocol	

12. The format for creating a(n) _____ ACL is:
    _____ access-list number _____ or _____[test conditions]

13. The format for creating a(n) _____ACL is:
    _____ access-list number _____ or ____ protocol source source-mask [destination destination-mask operand port established]

14. A wildcard mask is a __**-**bit quantity that is divided into four octets, with each octet containing 8 bits. It is used like a subnet mask, but IT IS VERY DIFFERENT!

15. A wildcard mask bit _ means "check the corresponding bit value" and a wildcard mask bit **1** means "do not check (ignore) that corresponding bit value".

16. A wildcard mask is paired with an __ address. ACLs use wildcard masking to identify a single or multiple addresses for permit or deny tests.

17. Show what parts of an IP address will be checked using the following wildcard masks using C for checked and I for ignored. You may use C.C.C.I as your format or CCCCCCCC.CCCCCCCC.CCCCCCCC.IIIIIIII.

Wildcard Mask	**IP Address Checked**
0.0.0.255	I
0.0.255.255	
0.0.0.15	

Example:
Using the IP address 173.98.100.87, shown below is the result against the wildcard mask 0.0.0.255.

1st take the IP 173.98.100.87 and break it into binary.
2nd take the wildcard mask 0.0.0.255 and break it into binary.
3rd compare which bits are checked (C) and which bits are ignored (I).

1	0	1	0	1	1	0	1	0	1	1	0	0	0	1	0	0	1	1	0	0	1	0	0	0	1	0	1	0	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1

C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	I	I	I	I	I	I	I	I

OR

C	C	C	I

18. To shorten the following command: _____**,** you could use _____

19. To shorten the following command: _____**,** you could use _____

20. You use _____ ACLs when you want to block <u>all traffic</u> from a network, allow all traffic from a specific network, or deny protocol suites. These ACLs check the _____ address of packets that could be routed.

21. You use the _____ command to display the contents of all ACLs. In addition, or use the same command plus the name or number of an ACL to display the contents of one ACL.

22. Circle the correct choice to make the statement true.
The following command _____ _ will be applied to the inbound/_____ interface.

23. _____ ACLs are used most often to test conditions because they provide a greater range of control. You would use these ACLs when you want to allow Web traffic but deny File Transfer Protocol (FTP) or telnet from non-company networks. They check for both source and destination packet addresses. They also can check for specific protocols, port numbers, and other parameters. This gives you more flexibility to describe what checking the ACL will do.

24. You can have as many condition statements as you want, limited only by the available ____**.**

25. Fill in the common port numbers for the following IP protocols.

Common Port Number (decimal)	IP Protocol
	FTP data
	FTP Program
	Telnet
	SMTP
	DNS
	TFTP

26. _____ ACLs can be used to delete individual entries from a specific ACL. This enables you to modify your ACLs without deleting and then reconfiguring them.

27. You can specify only ___ ACL per protocol per interface.

28. The rule is to put the extended ACLs as close as possible to the _____ of the traffic denied.

29. The rule is to put the standard ACLs as close as possible to the _____ of the packet.

30. ACLs should be used in firewall routers, which are often positioned between the internal network and an external network, such as the Internet. The firewall router provides a point of isolation so that the rest of the internal network structure is not affected. You can also use ACLs on a router positioned between two parts of the network to control traffic entering or exiting a specific part of the internal network.

31. To provide the security benefits of ACLs, you should at a minimum configure ACLs on _____ routers, which are routers situated on the boundaries of the network. This provides basic security from the outside network, or from a less controlled area of the network, into a more private area of the network.

The _____ __ _____ command displays IP interface information and indicates whether any ACLs are set. The ____ _____ command displays the contents of all ACLs. By entering the ACL name or number as an option for this command, you can see a specific list.

Command Reference

Chapter Six

ACLs

`access-group`	Applies access control lists (ACLs) to an interface.
`access-list`	Defines a standard IP ACL.
`deny`	Sets the conditions for a named IP ACL.
`interface`	Configures an interface type and enters interface configuration mode.
`ip access-group`	Controls access to an interface.
`ip address`	Sets the logical network address of the interface.
`permit`	Sets conditions for a named IP ACL.
`show access-lists`	Displays the contents of all current ACLs.
`show ip interface`	Lists a summary of an interface's IP information and status.