Name _____ Date _____

Module 5 - ACLs for IPv4 Configuration

Enterprise Networking, Security, and Automation– Semester 3

Student Version

Module 5 Sections:

5.0 Introduction
5.1 Configure Standard IPv4 ACLs
5.2 Modify IPv4 ACLs
5.3 Secure VTY Ports with a Standard IPv4 ACL
5.4 Configure Extended IPv4 ACLs
5.5 Module Practice and Quiz

Required Materials:

Reading Organizer

Packet Tracer Activities:
- 5.1.8 - Configure Numbered Standard IPv4 ACLs
- 5.1.9 Packet Tracer - Configure Named Standard IPv4 ACLs
- 5.2.7 Packet Tracer - Configure and Modify Standard IPv4 ACLs
- 5.4.12 Packet Tracer - Configure Extended IPv4 ACLs - Scenario 1
- 5.4.13 Packet Tracer - Configure Extended IPv4 ACLs - Scenario 2
- 5.5.1 Packet Tracer - IPv4 ACL Implementation Challenge

Labs: 5.5.2 - Configure and Verify Extended IPv4 ACLs

Module's 3 – 5 Exam

Page intentionally left blank.

Points_____ / ___100___

Name_____ Date _____

Module 5 - ACLs for IPv4 Configuration
Reading Organizer
Student Version

Note: The Reading Organizer has weighted scoring. Any question with the word **explain**, **define, or describe** in it is expected to have a longer answer and is worth two points each.

After completion of this module, you should be able to:

- Configure standard IPv4 ACLs to filter traffic to meet networking requirements.
- Use sequence numbers to edit existing standard IPv4 ACLs.
- Configure a standard ACL to secure VTY access.
- Configure extended IPv4 ACLs to filter traffic according to networking requirements.

5.1 Configure Standard IPv4 ACLs

1. List the suggested practices when configuring a complex ACL.

a.

b.

c.

d.

e.

2. Use the _____ global configuration command to remove a numbered standard ACL.

3. Describe a detailed explanation of the syntax for a standard ACL.

a. access-list-number –

b. deny –

c. permit –

d. remark text –

e. source –

f. source-wildcard –

g. log –

4. Naming an ACL makes it easier to understand its function. Write the global configuration command to create a named standard ACL.

5. ACL names are _____, _____, and must be _____.

6. _____ACL names is not required but makes them stand out when viewing the running-config output. It also makes it less likely that you will accidentally create two different ACLs with the same name but with different uses of capitalization.

7. Use the _____ global configuration command to remove a named standard IPv4 ACL.

8. After a standard IPv4 ACL is configured, it must be linked to an _____ or _____.

9. Two commands are required to completely remove an ACL from a router. What command can you use to remove an ACL from an interface?

10. Which command can you use to remove the ACL from the router after it is removed from the interface?

11. The output of the show access-lists command does not display remark statements. ACL remarks are displayed in the _____ file.

12. Which command can you use to verify if an interface has an ACL applied to it?

13. Write in the commands to create a named standard ACL called RESEARCH, with a remark, to permit host 10.25.1.1, applied outbound on GigabitEthernet0/0.

R1(config)# i_____

R1(config-std-nacl)# _____

R1(config-std-nacl)# _____

R1(config-std-nacl)# _____

R1(config)# _____

R1(config-if)# _____

R1(config-if)# _____
R1#

5.2 Modify IPv4 ACLs

14. What are the two methods to use when modifying an ACL?

a.

b.

15. Where should ACLs with multiple ACEs should be created?

16. Describe the steps required to correct an error in an ACL using a text editor.

a.

b.

c.

d.

17. Sequence numbers are automatically assigned when an ACE is entered. These numbers are listed in the _____command.

18. Does the show running-config command display sequence numbers?

19. Use the _____command to edit an ACL using sequencing numbers.

20. Explain how ACE statements can be changed using the sequence number.

21. Use the _____command to verify an ACL has a new ACE statement inserted appropriately before the permit statement.

22. Which router command shows statistics for each statement that has been matched?

23. When you show an ACLs statistics the implied deny any, the last statement does not display any statistics. Explain ho you can track how many implicit denied packets have been matched.

5.3 Secure VTY Ports with a Standard IPv4 ACL

24. Describe the two steps to secure remote administrative access to the vty lines:

a.

b.

25. The _____ keyword is the most commonly used option to filter incoming vty traffic.

26. Describe two things that need to be considered when configuring access lists on vty lines.

a.

b.

27. After the ACL to restrict access to the vty lines is configured, it is important to verify that it is working as expected. Explain how you can test this?

5.4 Configure Extended IPv4 ACLs

28. Why are extended ACLs used more often than standard ACLs?

29. What can extended ACLs filter on?

a.

b.

c.

d.

30. Use the _____access-list-name global configuration command to remove an extended ACL.

31. Match the extended ACL parameters with the description.

a. access-list-number	b. remark	c. source	d. deny	e. text
f. source-wildcard	g. permit	h. protocol	i. destination	j. source-wildcard
k. destination	l. operator	m. port	n. log	o. established
p. destination-wildcard				

_____This is the decimal number of the ACL.
Extended ACL number range is 100 to 199 and 2000 to 2699.

_____This denies access if the condition is matched.

_____This permits access if the condition is matched.

_____ (Optional) Adds a text entry for documentation purposes.
Each remark is limited to 100 characters.

_____Name or number of an internet protocol.
Common keywords include ip, tcp, udp, and icmp.
The ip keyword matches all IP protocols.

_____(Optional) A 32-bit wildcard mask that is applied to the source.

_____This identifies the source network or host address to filter.
Use the any keyword to specify all networks.
Use the host ip-address keyword or simply enter an ip-address (without the host keyword) to identify a specific IP address.

_____ (Optional) A 32-bit wildcard mask that is applied to the source.

_____This identifies the destination network or host address to filter.
Use the any keyword to specify all networks.
Use the host ip-address keyword or ip-address.

_____(Optional) This is a 32-bit wildcard mask that is applied to the destination.

_____(Optional) This compares source or destination ports.
Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).

_____(Optional) The decimal number or name of a TCP or UDP port.

_____(Optional) For the TCP protocol only.
This is a 1st generation firewall feature.

_____(Optional) This keyword generates and sends an informational message whenever the ACE is matched.
This message includes ACL number, matched condition (i.e., permitted or denied), source address, and number of packets.
This message is generated for the first matched packet.
This keyword should only be implemented for troubleshooting or security reasons.

32. Use the _____ to get help when entering a complex ACE.

33. Extended ACLs can filter on different port number and port name options. What is the port name and number for HTTP traffic?

Port Name _____ Port Number:_____

34. Explain what the TCP *established* keyword allows TCP to do.

35. If you apply the established keyword to HTTP traffic what will happen?

36. ACL names are _____, _____and must be unique.

37. The _____command is used to verify the ACL statistics.

38. What two methods are available to edit extended ACLs?

a.

b.

39. What are some of the factors to consider when applying an ACL?

a.

b.

c.

40. What are three commands you can use to verify ACLs?

a.

b.

c.