Accessing the WAN

CCNA Exploration Labs and Study Guide

John Rullan

Cisco | Networking Academy
Mind Wide Open

Accessing the WAN

CCNA Exploration Labs and Study Guide

John Rullan

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing April 2008

Library of Congress Cataloging-in-Publication Data
Rullan, John.
Accessing the WAN : CCNA exploration labs and study guide / John Rullan.
p. cm.
ISBN-13: 978-1-58713-201-8 (pbk. w/cd)
ISBN-10: 1-58713-201-X (pbk. w/cd)
1. Wide area networks (Computer networks)—Examinations—Study guides. I. Cisco Systems,
Inc. II. Title.
TK5105.87.R85 2008
004.67—dc22
2008013029

ISBN-13: 978-1-58713-201-8

ISBN-10: 1-58713-201-x

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Cisco Representative
Anthony Wolfenden

Cisco Press Program Manager
Jeff Brady

Executive Editor
Mary Beth Ray

Production Manager
Patrick Kanouse

Senior Development Editor
Christopher Cleveland

Project Editor
Seth Kerney

Copy Editors
Keith Cline
Gayle Johnson

Technical Editors
Roderick Douglas
Lee Hilliard
Wayne Jarvimaki

Editorial Assistant
Vanessa Evans

Book and Cover Designer
Louisa Adair

Composition
Bronkella Publishing, Inc.

Proofreaders
Water Crest Publishing, Inc.
Debbie Williams

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.

Introduction

The Cisco Networking Academy is a comprehensive e-learning program that provides students with Internet technology skills. A Networking Academy delivers web-based content, online assessment, student performance tracking, and hands-on labs to prepare students for industry-standard certifications. The CCNA curriculum includes four courses oriented around the topics on the Cisco Certified Network Associate (CCNA) certification.

Accessing the WAN, CCNA Exploration Labs and Study Guide is a supplement to your classroom and laboratory experience with the Cisco Networking Academy. To succeed on the exam and achieve your CCNA certification, you should do everything in your power to arm yourself with a variety of tools and training materials to support your learning efforts. This Labs and Study Guide is just such a collection of tools. Used to its fullest extent, it will help you acquire the knowledge and practice the skills associated with the content area of the CCNA Exploration Accessing the WAN course. Specifically, this book helps you work on these main areas:

- WAN technology concepts
- PPP concepts and configuration
- Frame Relay concepts and configuration
- Network security threats and mitigation techniques
- Access control list operation and configuration
- Broadband services and technologies
- Network Address Translation concepts and configuration
- DHCP operation and configuration
- IPv6 concepts
- Troubleshooting methodologies and tools

Labs and Study Guides similar to this one are also available for the other three courses: *Network Fundamentals, CCNA Exploration Labs and Study Guide*; *Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide*; and *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide*.

Audience for This Book

This book's main audience is anyone taking the CCNA Exploration Accessing the WAN course of the Cisco Networking Academy curriculum. Many Academies use this book as a required tool in the course, and other Academies recommend the Labs and Study Guides as an additional source of study and practice materials.

Goals and Methods

The most important goal of this book is to help you pass the CCNA exam (640-802). Passing this foundation exam means that you not only have the required knowledge of the technologies covered by the exam, but that you can plan, design, implement, operate, and troubleshoot these technologies. In other words, these exams are rigorously application-based. You can view the exam topics any time at **http://www.cisco.com/go/certifications**. The topics are divided into eight categories:

- Describe how a network works
- Configure, verify, and troubleshoot a switch with VLANs and interswitch communications
- Implement an IP addressing scheme and IP Services to meet network requirements in a medium-size Enterprise branch office network
- Configure, verify, and troubleshoot basic router operation and routing on Cisco devices
- Explain and select the appropriate administrative tasks required for a WLAN
- Identify security threats to a network, and describe general methods to mitigate those threats
- Implement, verify, and troubleshoot NAT and ACLs in a medium-size Enterprise branch office network
- Implement and verify WAN links

The Accessing the WAN course focuses on the third, fifth, sixth, seventh, and eighth topics.

The Study Guide portion of each chapter offers exercises that help you learn the Accessing the WAN concepts as well as the configurations crucial to your success as a CCNA exam candidate. Each chapter is slightly different and includes some or all of the following types of exercises:

- Vocabulary matching and completion
- Skill-building activities and scenarios
- Configuration scenarios
- Concept questions
- Internet research

Packet Tracer
□ **Activity**

In the configuration chapters, you'll find many Packet Tracer Activities that work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available on this book's CD-ROM; Packet Tracer software, however, is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.

The Labs and Activities portion of each chapter includes all the online Curriculum Labs, some additional supplemental labs that you can perform with Packet Tracer, and a Packet Tracer Skills Integration Challenge Activity. The Curriculum Labs are divided into three categories:

- **Basic**: The Basic Labs are procedural in nature and assume that you have no experience configuring the technologies that are the topic of the lab.
- **Challenge**: The Challenge Labs cover implementations and assume that you have a firm-enough grasp on the technologies to "go it alone." These labs often give you only a general requirement that you must implement fully without the details of each small step. In other words, you must use the knowledge and skills you gained in the chapter text, activities, and Basic Lab to successfully complete the Challenge Lab. Avoid the temptation to work through the Challenge Lab by flipping back through the Basic Lab when you are unsure of a command. Do not try to short-circuit your CCNA training. You need a deep understanding of CCNA knowledge and skills to ultimately be successful on the CCNA exam.
- **Troubleshooting**: The Troubleshooting Labs ask you to fix a broken network. These labs include corrupted scripts that you purposely load onto the routers. Then you use troubleshooting techniques to isolate problems and implement the solution. By the end of the lab, you should have a functional network with full end-to-end connectivity.

Packet Tracer
□ **Companion**

Most of the Hands-on Labs include Packet Tracer Companion Activities, in which you can use Packet Tracer to complete a simulation of the lab.

Packet Tracer
□ **Challenge**

Each chapter ends with a Packet Tracer Skills Integration Challenge. These activities require you to pull together several skills learned from the chapter—as well as previous chapters and courses—to successfully complete one comprehensive exercise.

A Word About Packet Tracer

Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and they have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This “e-doing” capability is a fundamental component of learning how to configure routers and switches from the command line.

Packet Tracer version 4.*x* is available only to Cisco Networking Academies through the Academy Connection website.

How This Book Is Organized

Because the content of this book and the online curriculum is sequential, you should work through this book in order, beginning with Chapter 1.

The book covers the major topic headings in the same sequence as the online curriculum for the CCNA Exploration Accessing the WAN course. This book has eight chapters with the same numbers and names as the online course chapters.

If necessary, a chapter uses a single topology for the exercises in the Study Guide portion. This single topology allows for better continuity and easier understanding of switching commands, operations, and outputs. However, the topology is different from the one used in the online curriculum and the Companion Guide. A different topology affords you the opportunity to practice your knowledge and skills without just simply recording the information you find in the text.

- **Chapter 1, “Introduction to WANs”**: The exercises in the Study Guide portion of this chapter focus on LAN design concepts, including vocabulary and the three-layer hierarchical model. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 2, “PPP”**: The exercises in the first part of this chapter help you understand basic Ethernet and switching concepts, including building the MAC address table and collision and broadcast domains. Then the Packet Tracer exercises cover, in detail, how to configure a switch, including basic switch management and configuring switch security. The Lab portion of the chapter includes two Basic Labs, a Challenge Lab, and a Packet Tracer Skills Integration Challenge activity.

- **Chapter 3, “Frame Relay”**: The exercises in the first portion of this chapter focus on the concepts of VLANs, including benefits of VLANs and types of VLANs. The exercises then cover VLAN trunking concepts before moving into a section devoted to a VLAN and trunk configuration Packet Tracer exercise. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 4, “Network Security”**: The exercises in this chapter focus on key network security threats, tools, and mitigation techniques for Cisco routers. Configuration practice is provided for router security tasks. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 5, “ACLs”**: Exercises in this chapter focus on the concept of redundant LAN topologies, using STP and its variants to stop loops, and the commands to manipulate root bridge elections. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 6, “Teleworker Services”**: This short chapter focuses on how to configure inter-VLAN routing, including two Packet Tracer exercises. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 7, “IP Addressing Services”**: The exercises in this chapter include several matching term activities, multiple choice questions, fill-in-the-blank exercises, and concept questions that test your knowledge on DHCP and scaling IP addresses with the use of NAT and PAT. It also tests your knowledge of IPv6 and routing using the next generation of RIP. The Lab portion of this chapter includes all the online curriculum labs for DHCP and NAT as well as four additional Packet Tracer activities that test your knowledge and skills in complex configurations using DHCP, Static NAT, PAT, and double NAT. A Packet Tracer Skills Integration Challenge ties all of these concepts together.
- **Chapter 8, “Network Troubleshooting”**: The exercises in this chapter begin with wireless LAN concepts, including standards, operation, and security. The exercises then cover wireless configuration for LAN access using a Linksys WRT300N, including a Packet Tracer exercise. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Appendix, “How to Install SDM”**: Cisco Router and Security Device Manager (SDM) is used in the security labs for this course. This appendix describes and illustrates how to install SDM on a Cisco router or PC.

About the CD-ROM

Packet Tracer
□ Activity

Packet Tracer
□ Companion

Packet Tracer
□ Challenge

The CD-ROM included with this book contains all the Packet Tracer Activity, Packet Tracer Companion, and Packet Tracer Challenge files that are referenced throughout the book, as indicated by the Packet Tracer Activity, Packet Tracer Companion, and Packet Tracer Challenge icons.

You can find updates to these files on this book’s website at **http://www.ciscopress.com/title/9781587132018**.

CHAPTER 5

ACLs

The Study Guide portion of this chapter uses a combination of matching, multiple-choice, and open-ended question exercises to test your knowledge of the various types of access control lists (ACL). You will also learn how to configure and where to place ACLs to properly secure and control traffic patterns in and out of networks.

The Labs portion of this chapter includes all the online curriculum labs. The Challenge and Troubleshooting labs are added to ensure that you have mastered the practical, hands-on skills needed to configure, place, and troubleshoot ACLs.

As you work through this chapter, use Chapter 5 in the *Accessing the WAN, CCNA Exploration Companion Guide*, or use the corresponding Chapter 5 in the *Accessing the WAN* online curriculum, for assistance.

Study Guide

Using ACLs to Secure Networks

ACLs are used to secure and control traffic into and out of networks. ACLs filter traffic based on rules you set in your ACL statements. The rules determine if packets are permitted or denied, what service they are allowed to use, and who they can communicate with. An example of this is whether a host is allowed to access the Internet or have access to a particular server on the network.

Access to services is filtered based on port numbers. Ports 0 to 1023 are called well-known ports. These include common services such as Telnet port 23 and HTTP, which uses port 80. Companies may request a port number from IANA between 1024 and 49,151 to identify a specific application. For example, Shockwave uses port number 1626. Ports 49,152 to 65,535 are dynamically assigned to end devices and are temporary, lasting only the duration of a connection.

When configured, an ACL turns a router into a firewall and checks all traffic against each statement before it can be forwarded to its destination. This process controls traffic patterns and helps secure your network but definitely adds latency. Packets are checked against ACL statements in the order in which they are configured, from top to bottom, one statement at a time. When the first match occurs, whether it is permitted or denied, that action occurs. If each statement is a permit action, an implicit "deny any" at the end of the statement list is not seen and does not need to be configured. Any packet that does not match any of the permit statements is automatically denied. Therefore, if all statements are deny actions, a permit any must be the last statement written, or all traffic is denied! This is a very common mistake for novice network administrators to make.

Standard and extended access lists can be named or numbered. Standard ACLS are simple statements that permit or deny traffic based on the source IP address. They should be configured on the router as close to the destination as possible. Extended ACLs can filter traffic using multiple variables such as protocol, source and destination IP address, and port number based on the service or application being filtered. Because they are precise, they are configured on the router closest to the source being filtered. This prevents denied traffic from consuming bandwidth.

Standard and extended ACLs can be configured to be named or numbered. ACLS generally are given a number to identify their type—1 to 99 for standard IP and 100 to 199 for extended IP. Named ACLs have no limit, but, more importantly, they can be modified without starting over from the beginning. Sequence numbers can be used when you want to add a statement to the middle of the list without starting over.

As mentioned, packets are processed against ACLs in the order in which they were created. This means that if you make a mistake and put a statement first that should have been last, you cannot simply remove it; you must start from the beginning. This is why it is recommended that you write out your ACL statements in Notepad and have someone check them over before you drop them into your configuration. If you use named ACLs, you are not limited as to how many statements you can create, and you also can tweak your configuration without removing it and starting over. After you create the access list that serves its purpose, the next and last step is to apply it to an interface. You must apply an ACL to an interface for it to work. Without this, the ACL is useless and is the same as having no security as all.

Multiple-Choice Questions

1. What is the well-known port number range?

A. 0 to 1023
B. 1 to 1023
C. 0 to 1024
D. 1 to 1024

2. Which of the following is a port used by TCP and UDP?

A. 23 Telnet
B. 25 SMTP
C. 53 DNS
D. 69 TFTP

3. Which port is used by secure websites using HTTPS?

A. 161
B. 443
C. 520
D. 694

4. Why are ACL numbers 200 to 1299 skipped?

A. They are reserved.
B. The are used by well-known ACLs.
C. They are reserved for loopbacks.
D. They are used by other protocols.

5. Which criterion *cannot* be used in an ACL rule to match a packet?

A. Source address
B. Source port
C. Destination address
D. Destination port
E. Protocol
F. Direction

6. What are the “Three Ps” when configuring ACLs on a router? (Choose three.)

A. One ACL per port

B. One ACL per protocol

C. One ACL per interface

D. One ACL per direction

E. One ACL per network

F. One ACL per filter

7. Place the following actions in the correct order:

A. The packet is processed by outbound ACL.

B. The packet is processed by inbound ACL.

C. The packet is transmitted on an interface.

D. The packet is received on an interface.

E. The packet is routed to the appropriate interface for transmission.

A. A, B, C, D, E

B. E, D, B, A, C

C. D, B, E, A, C

D. C, A, D, E, B

8. What are the benefits of using named ACLs over numbered? (Choose two.)

A. There is no limit to the number of ACLs you can create.

B. They are not sequential like numbered ACLs.

C. They can be modified without starting over.

D. They are easier to configure.

9. What is the range of numbers used to identify IP standard access lists?

A. 0 to 99

B. 1 to 99

C. 100 to 199

D. 100 to 200

10. At what layer of the OSI Reference Model does packet filtering occur?

A. Data link

B. Network

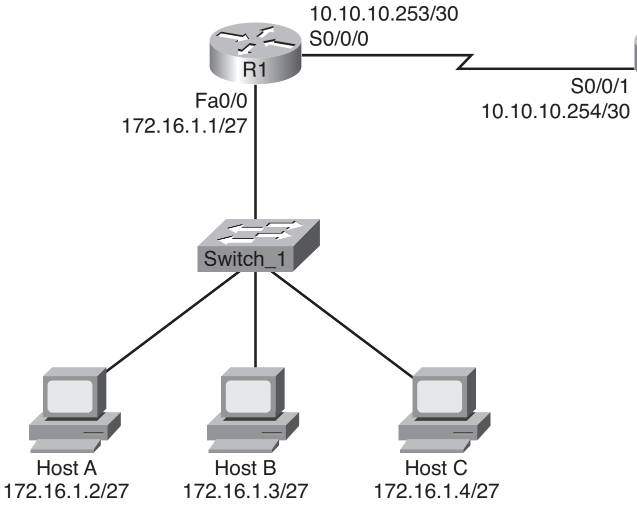
C. Transport

D. Application

Configuring Standard ACLs: Command Exercise

For question 1, refer to the topology shown in Figure 5-1.

Figure 5-1 Network Topology for Question 1



Allow only Host A to telnet to the R2 router, using **cisco** as the password. Use a standard named ACL to accomplish this task, and name the ACL **No_Telnet**. Write all the commands below.

____

____

____

____

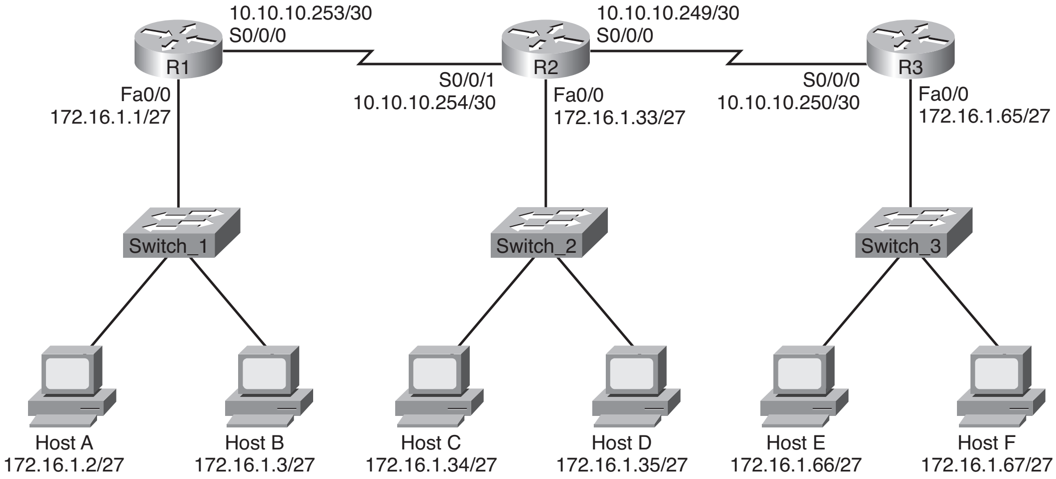
____

____

____

For questions 2 through 4, refer to the topology shown in Figure 5-2.

Figure 5-2 Network Topology for Questions 2 Through 4



Deny users from the R1 LAN access to the R3 LAN. Use a standard numbered ACL to accomplish this task, and be sure to include the appropriate wildcard mask. Configure a remark that will remind the administrator of the purpose of the ACL. Write all the commands below.

____

____

____

____

____

Permit *only* users from the R3 LAN access to the R2 LAN. Use a standard named ACL to accomplish this task, and name the ACL **R3_Only**. Write all the commands below.

____

____

____

____

____

Traffic from the R2 LAN should not be permitted to leave the LAN. Create a standard numbered ACL to accomplish this. Use the last usable number in the standard IP ACL number range. Write all the commands below.

____

____

____

Configuring Extended ACLs

Vocabulary Exercise: Matching Terms

Match the parameter on the left with its definition on the right. Use the following command syntax as a basis for your answers:

```
access?list access?list?number [dynamic dynamic?name [timeout minutes]]
  {deny ¦ permit} protocol source source?wildcard destination destination?wildcard
  [precedence precedence] [tos tos] [log ¦ log?input] [time?range time?range?name]
```

Parameter

a. Extended ACL number range
b. Dynamic
c. Protocol
d. Source/destination
e. Wildcard
f. Port
g. Log
h. Operator
i. Host
j. Any

Definition

__ Specifies the different types of traffic

__ Sends an informational message about a packet that matches the entry to be sent to the console

__ The number of the network or host from which the packet is being sent

__ Can be listed as a name or number

__ A number range from 100 to 199 or from 2000 to 2699

__ Used with lock-and-key security

__ An abbreviation for a source or destination wildcard of 0.0.0.0 255.255.255.255

__ A string of binary digits telling the router which parts of the subnet to look at

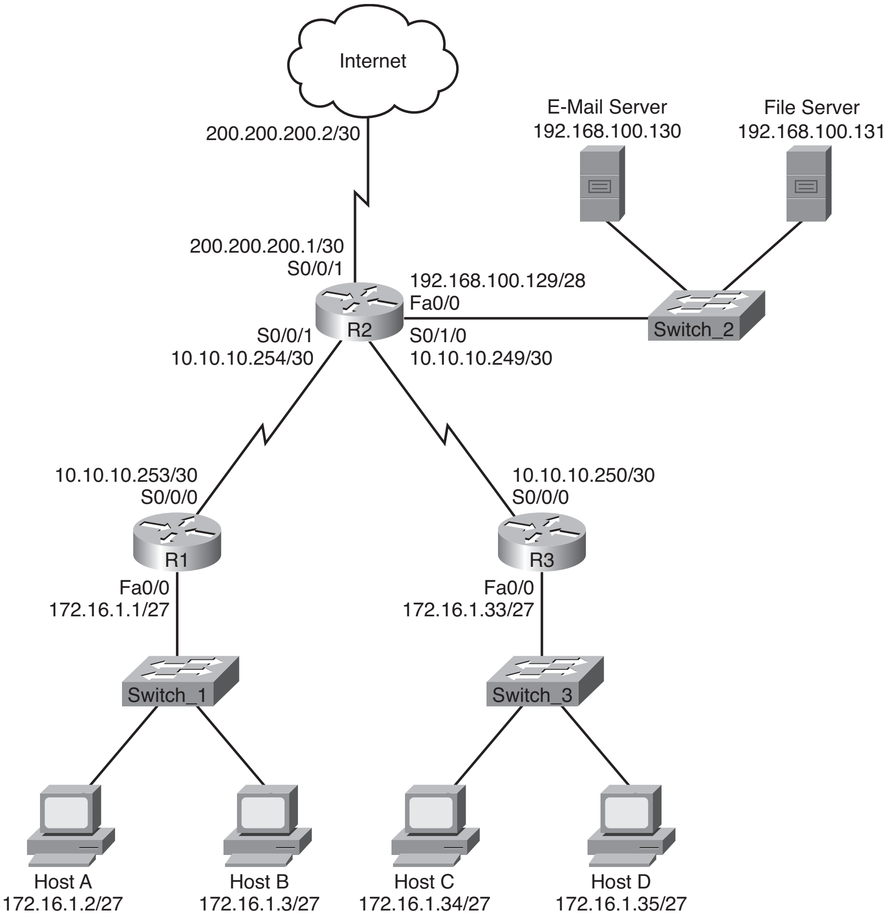
__ Equal to, not equal to, and less than

__ Abbreviation for a source or destination wildcard of 0.0.0.0

Extended ACL Command Exercise

Refer to Figure 5-3 for all the questions in this command exercise.

Figure 5-3 Network Topology for Questions 1 Through 4



1. Allow only Host A from the 172.16.1.0/27 subnet access to the E-Mail server. Use the last usable number in the extended list range. Host A should not have access to any of the other servers. Write all the commands below.

____

____

____

____

2. Allow only Host B access to the Internet, and deny everyone else. Use an extended named ACL to accomplish this task, and name the ACL **Internet**. Write all the commands below.

____

____

____

____

____

3. No one from the 172.16.1.0/27 subnet is allowed access to the File Server, but all other traffic should be permitted. Use an extended named ACL to accomplish this task, and name the ACL **No_Access**. Write all the commands below.

____

____

____

____

____

____

4. Allow only hosts on the R3 LAN to communicate with hosts on the R1 LAN. They are allowed access to the Internet, but deny them access to the servers on the R2 LAN. Use the first usable number in the extended IP range to accomplish this task. Write all the commands below.

____

____

____

____

Configuring Complex ACLs

Review Questions

Various types of ACLs are available to secure your network and to filter traffic such as standard, extended, numbered, dynamic, lock-and-key, reflexive, and time-based. Below, write the definitions, and give an example of when you would use each kind of ACL.

Lock-and-key:

____

____

____

____

____

____

____

Reflexive:

____

____

____

____

____

____

Time-based:

Vocabulary Exercise: Matching Terms

Match the term on the left with its definition on the right.

Field

a. Standard ACL
b. Named ACL
c. Lock-and-key
d. Access class
e. Extended
f. Reflexive
g. IP access group
h. Log
i. Time-based
j. Logical operations

Definition

__ Allows you to add or delete entries within the ACL

__ Shows the ACL number and whether a packet was permitted or denied

__ Applies an ACL to a line

__ This ACL is not applied to an interface or line but is "nested" within an extended ACL

__ Equal to, not equal to, and less than

__ This feature is dependent on Telnet

__ Controls traffic based on the source and destination address

__ Controls traffic based on the source address only

__ Applies an ACL to an interface

__ This feature works best with NTP synchronization

Labs and Activities

Lab 5-1: Basic Access Control Lists (5.5.1)

Upon completion of this lab, you will be able to

- Design named standard and named extended ACLs
- Apply named standard and named extended ACLs
- Test named standard and named extended ACLs
- Troubleshoot named standard and named extended ACLs

Figure 5-4 shows the network topology for this lab. Table 5-1 provides the IP addresses, subnet masks, and default gateways (where applicable) for all devices in the topology.

Figure 5-4 Network Topology for Lab 5-1

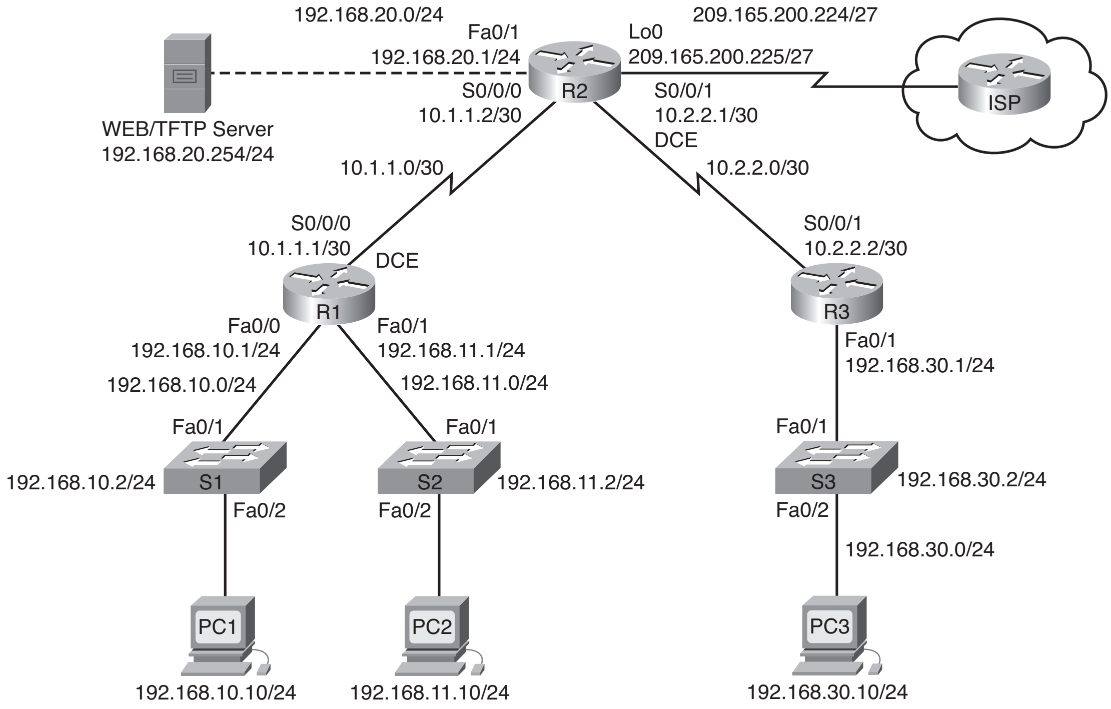


Table 5-1 Lab 5-1 Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	—
	Fa0/1	192.168.11.1	255.255.255.0	—
	S0/0/0	10.1.1.1	255.255.255.252	—

continues

Table 5-1 Lab 5-1 Addressing Table continued

Device	Interface	IP Address	Subnet Mask	Default Gateway
R2	Fa0/1	192.168.20.1	255.255.255.0	—
	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1	10.2.2.1	255.255.255.252	—
	Lo0	209.165.200.225	255.255.255.224	—
R3	Fa0/1	192.168.30.1	255.255.255.0	—
	S0/0/1	10.2.2.2	255.255.255.252	—
S1	Vlan1	192.168.10.2	255.255.255.0	192.168.10.1
S2	Vlan1	192.168.11.2	255.255.255.0	192.168.11.1
S3	Vlan1	192.168.30.2	255.255.255.0	192.168.30.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
Web Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Scenario

In this lab, you will learn how to configure basic network security using ACLs. You will apply both standard and extended ACLs.

Task 1: Prepare the Network

Step 1. Cable a network that is similar to the one shown in Figure 5-4.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: This lab was developed and tested using 1841 routers. If you use 1700, 2500, or 2600 series routers, the router outputs and interface descriptions might be different. On older routers, or those running Cisco IOS software earlier than Release 12.4, some commands may be different or nonexistent.

Step 2. Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Configure the R1, R2, R3, S1, S2, and S3 routers and switches according to the following guidelines:

- Configure the router hostname to match the topology diagram.
- Disable DNS lookup.

- Configure an EXEC mode password of **class**.
- Configure a message-of-the-day banner.
- Configure a password of **cisco** for console connections.
- Configure a password for VTY connections.
- Configure IP addresses and masks on all devices.
- Enable OSPF area 0 on all routers for all networks.
- Configure a loopback interface on R2 to simulate the ISP.
- Configure IP addresses for the VLAN 1 interface on each switch.
- Configure each switch with the appropriate default gateway.
- Verify full IP connectivity using the **ping** command.

Task 3: Configure a Standard ACL

Standard ACLs can filter traffic based on source IP address only. A typical best practice is to configure a standard ACL as close to the destination as possible. In this task, you are configuring a standard ACL. The ACL is designed to block traffic from the 192.168.11.0/24 network located in a student lab from accessing any local networks on R3.

This ACL will be applied inbound on the R3 serial interface. Remember that every ACL has an implicit "deny all" that causes all traffic that has not matched a statement in the ACL to be blocked. For this reason, add the **permit any** statement to the end of the ACL.

Before configuring and applying this ACL, be sure to test connectivity from PC1 (or the Fa0/1 interface on R1) to PC3 (or the Fa0/1 interface on R3). Connectivity tests should be successful before applying the ACL.

Step 1. Create the ACL on router R3.

In global configuration mode, create a standard named ACL called **STND-1**:

```
R3(config)# ip access-list standard STND-1
```

In standard ACL configuration mode, add a statement that denies any packets with a source address of 192.168.11.0/24 and prints a message to the console for each matched packet:

```
R3(config-std-nacl)# deny 192.168.11.0 0.0.0.255 log
```

Permit all other traffic:

```
R3(config-std-nacl)# permit any
```

Step 2. Apply the ACL.

Apply the ACL **STND-1** as a filter on packets entering R3 through serial interface 0/0/1:

```
R3(config)# interface serial 0/0/1
R3(config-if)# ip access-group STND-1 in
R3(config-if)# end
R3# copy run start
```

Step 3. Test the ACL.

Before testing the ACL, make sure that the console of R3 is visible. This allows you to see the access list log messages when the packet is denied.

Test the ACL by pinging from PC2 to PC3. Because the ACL is designed to block traffic with source addresses from the 192.168.11.0/24 network, PC2 (192.168.11.10) should not be able to ping PC3.

You can also use an extended ping from the Fa0/1 interface on R1 to the Fa0/1 interface on R3:

```
R1# ping ip

Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.11.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
U.U.U
Success rate is 0 percent (0/5)
```

You should see the following message on the R3 console:

```
*Sep  4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0 0.0.0.0 ->
192.168.11.1, 1 packet
```

In privileged EXEC mode on R3, issue the **show access-lists** command. You see output similar to the following. Each line of an ACL has an associated counter showing how many packets have matched the rule.

```
Standard IP access list STND-1
    10 deny   192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)
    20 permit any (25 matches)
```

The purpose of this ACL is to block hosts from the 192.168.11.0/24 network. Any other hosts, such as those on the 192.168.10.0/24 network, should be allowed access to the networks on R3. Conduct another test from PC1 to PC3 to ensure that this traffic is not blocked.

You can also use an extended ping from the Fa0/0 interface on R1 to the Fa0/1 interface on R3:

```
R1# ping ip

Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.10.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms
```

Task 4: Configure an Extended ACL

When greater granularity is required, you should use an extended ACL. Extended ACLs can filter traffic based on more than just source address. Extended ACLs can filter on protocol, source, and destination IP addresses, and source and destination port numbers.

An additional policy for this network states that devices from the 192.168.10.0/24 LAN are permitted to reach only internal networks. Computers on this LAN are not permitted to access the Internet. Therefore, these users must be blocked from reaching the IP address 209.165.200.225. Because this requirement needs to enforce both source and destination, an extended ACL is needed.

In this task, you will configure an extended ACL on R1 that keeps traffic originating from any device on the 192.168.10.0/24 network from accessing the 209.165.200.255 host (the simulated ISP). This ACL will be applied inbound on the R1 FastEthernet 0/0 interface. A typical best practice for applying extended ACLs is to place them as close to the source as possible.

Before beginning, verify that you can ping 209.165.200.225 from PC1.

Step 1. Configure a named extended ACL.

In global configuration mode, create a named extended ACL called **EXTEND-1**.

```
R1(config)# ip access-list extended EXTEND-1
```

Notice that the router prompt changes to indicate that you are now in extended ACL configuration mode. From this prompt, add the necessary statements to block traffic from the 192.168.10.0/24 network to the host. Use the **host** keyword when defining the destination:

```
R1(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Recall that the implicit "deny all" blocks all other traffic without the additional **permit** statement. Add the **permit** statement to ensure that other traffic is not blocked:

```
R1(config-ext-nacl)# permit ip any any
```

Step 2. Apply the ACL.

With standard ACLs, the best practice is to place the ACL as close to the destination as possible. Extended ACLs typically are placed close to the source. The **EXTEND-1** ACL will be placed on the serial interface and will filter outbound traffic.

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip access-group EXTEND-1 out log
R1(config-if)# end
R1# copy run start
```

Step 3. Test the ACL.

From PC1, ping the loopback interface on R2. These pings should fail, because all traffic from the 192.168.10.0/24 network is filtered when the destination is 209.165.200.225. If the destination is any other address, the pings should succeed. Confirm this by pinging R3 from the 192.168.10.0/24 network device.

Note: The extended ping feature on R1 cannot be used to test this ACL, because the traffic will originate within R1 and will never be tested against the ACL applied to the R1 serial interface.

You can further verify this by issuing the **show ip access-list** command on R1 after pinging:

```
R1# show ip access-list

Extended IP access list EXTEND-1
    10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)
    20 permit ip any any
```

Task 5: Control Access to the VTY Lines with a Standard ACL

It is good practice to restrict access to the router VTY lines for remote administration. An ACL can be applied to the VTY lines, allowing you to restrict access to specific hosts or networks. In this task, you will configure a standard ACL to permit hosts from two networks to access the VTY lines. All other hosts are denied.

Verify that you can telnet to R2 from both R1 and R3.

Step 1. Configure the ACL.

Configure a named standard ACL on R2 that permits traffic from 10.2.2.0/30 and 192.168.30.0/24. Deny all other traffic. Call the ACL **TASK-5**:

```
R2(config)# ip access-list standard TASK-5
R2(config-std-nacl)# permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)# permit 192.168.30.0 0.0.0.255
```

Step 2. Apply the ACL.

Enter line configuration mode for VTY lines 0 to 4:

```
R2(config)# line vty 0 4
```

Use the **access-class** command to apply the ACL to the vty lines in the inbound direction. Note that this differs from the command used to apply ACLs to other interfaces:

```
R2(config-line)# access-class TASK-5 in
R2(config-line)# end
R2# copy run start
```

Step 3. Test the ACL.

Telnet to R2 from R1. Note that R1 does not have IP addresses in the address range listed in the ACL TASK-5 permit statements. Connection attempts should fail.

```
R1# telnet 10.1.1.2

Trying 10.1.1.2 ...
% Connection refused by remote host
```

From R3, telnet to R2. You see a prompt for the VTY line password:

```
R3# telnet 10.1.1.2

Trying 10.1.1.2 ... Open
CUnauthorized access strictly prohibited, violators will be prosecuted to
  the full extent of the law.

User Access Verification

Password:
```

Why do connection attempts from other networks fail even though they are not specifically listed in the ACL?

____

____

Task 6: Troubleshoot ACLs

When an ACL is improperly configured or is applied to the wrong interface or in the wrong direction, network traffic may be adversely affected.

Step 1. Remove ACL STND-1 from S0/0/1 of R3.

In an earlier task, you created and applied a named standard ACL on R3. Use the **show running-config** command to view the ACL and its placement. You should see that an ACL named **STND-1** was configured and applied inbound on Serial 0/0/1. Recall that this ACL was designed to block all network traffic with a source address from the 192.168.11.0/24 network from accessing the LAN on R3.

To remove the ACL, go to interface configuration mode for Serial 0/0/1 on R3. Use the **no ip access-group STND-1 in** command to remove the ACL from the interface:

```
R3(config)# interface serial 0/0/1
R3(config-if)# no ip access-group STND-1 in
```

Use the **show running-config** command to confirm that the ACL has been removed from Serial 0/0/1.

Step 2. Apply ACL STND-1 on S0/0/1 outbound.

To test the importance of the ACL filtering direction, reapply the STND-1 ACL to the Serial 0/0/1 interface. This time the ACL filters outbound traffic, rather than inbound traffic. Remember to use the **out** keyword when applying the ACL:

```
R3(config)# interface serial 0/0/1
R3(config-if)# ip access-group STND-1 out
```

Step 3. Test the ACL.

Test the ACL by pinging from PC2 to PC3. As an alternative, use an extended ping from R1. Notice that this time pings succeed, and the ACL counters are not incremented. Confirm this by issuing the **show ip access-list** command on R3.

Step 4. Restore the ACL to its original configuration.

Remove the ACL from the outbound direction and reapply it to the inbound direction:

```
R3(config)# interface serial 0/0/1
R3(config-if)# no ip access-group STND-1 out
R3(config-if)# ip access-group STND-1 in
```

Step 5. Apply TASK-5 to the R2 serial 0/0/0 interface inbound:

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip access-group TASK-5 in
```

Step 6. Test the ACL.

Attempt to communicate with any device connected to R2 or R3 from R1 or its attached networks. Notice that all communication is blocked and that ACL counters are not incremented. This is because of the implicit “deny all” at the end of every ACL. This deny statement prevents all inbound traffic to serial 0/0/0 from any source other than R3. Essentially, this causes routes from R1 to be removed from the routing table.

You should see messages similar to the following printed on the consoles of R1 and R2 (it takes some time for the OSPF neighbor relationship to go down, so be patient):

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
  Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

After you receive this message, issue the command **show ip route** on both R1 and R2 to see which routes have been removed from the routing table.

Remove ACL TASK-5 from the interface, and save your configurations:

```
R2(config)# interface serial 0/0/0
R2(config-if)# no ip access-group TASK-5 in
R2(config)# exit
R2# copy run start
```

Task 7: Document the Router Configurations

Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Packet Tracer
□ Companion

Packet Tracer Companion: Basic Access Control Lists (5.5.1)

You can now open the file LSG04-Lab551.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for hands-on lab experience with real equipment.

Lab 5-2: Access Control Lists Challenge (5.5.2)

Upon completion of this lab, you will be able to

- Design named standard and named extended ACLs
- Apply named standard and named extended ACLs
- Test named standard and named extended ACLs
- Troubleshoot named standard and named extended ACLs

Figure 5-5 shows the network topology for this lab. Table 5-2 provides the IP addresses, subnet masks, and default gateways (where applicable) for all devices in the topology.

Figure 5-5 Network Topology for Lab 5-2

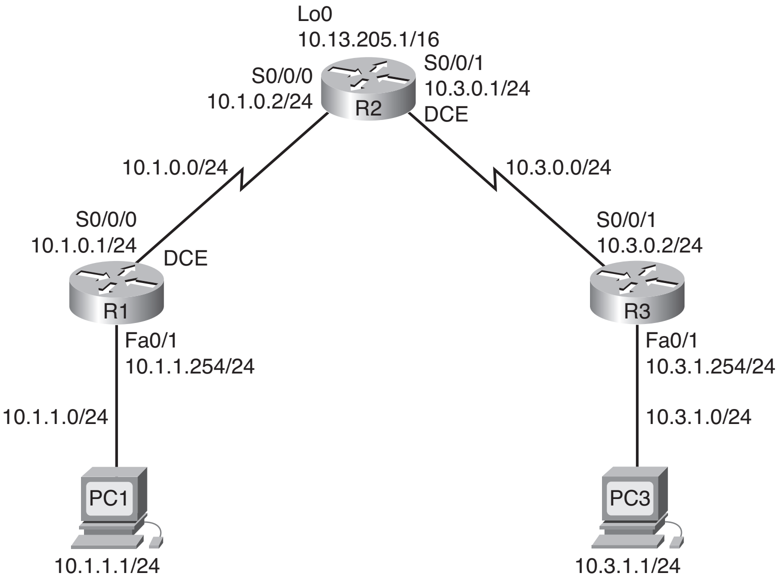


Table 5-2 Lab 5-2 Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0	10.1.0.1	255.255.255.0	—
	Fa0/1	10.1.1.254	255.255.255.0	—
R2	S0/0/0	10.1.0.2	255.255.255.0	—
	S0/0/1	10.3.0.1	255.255.255.0	—
	Lo 0	10.13.205.1	255.255.0.0	—
R3	S0/0/1	10.3.0.2	255.255.255.0	—
	Fa0/1	10.3.1.254	255.255.255.0	—
PC 1	NIC	10.1.1.1	255.255.255.0	10.1.1.254
PC 3	NIC	10.3.1.1	255.255.255.0	10.3.1.254

Task 1: Prepare the Network

Step 1. Cable a network that is similar to the one shown in Figure 5-5.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: If you use a 1700, 2500, or 2600 router, the router outputs and interface descriptions may look different.

Step 2. Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.
- Configure IP addresses on all devices.
- Create a loopback interface on R2.
- Enable OSPF area 0 on all routers for all networks.
- Verify full IP connectivity using the **ping** command.

Task 3: Configure Standard ACLs

Configure standard named ACLs on the R1 and R3 VTY lines, permitting hosts connected directly to their FastEthernet subnets to gain Telnet access. Deny and log all other connection attempts. Document your testing procedures.

____

____

____

____

Task 4: Configure Extended ACLs

Using extended ACLs on R1 and R3, complete the following requirements:

- The LANs connected to R1 and R3 are used for student computer labs. The network administrator has noticed that students in these labs are playing games across the WAN with the remote students. Make sure that your ACL prevents the LAN attached to R1 from reaching the LAN at R3 and that the LAN on R3 cannot reach the LAN on R1. Be specific in your statements so that any new LANs added to either R1 or R3 are unaffected.

- Permit all OSPF traffic.
- Permit ICMP traffic to the R2 local interfaces.
- All network traffic destined for TCP port 80 should be allowed. Any other traffic should be denied and logged.
- Any traffic not specified here should be denied.

Note: This may require multiple access lists. Verify your configuration, and document your testing procedure.

Why is the order of access list statements so important?

____

____

Task 5: Verify an ACL

Test each protocol that you are trying to block, and make sure that permitted traffic is allowed. This requires testing ping, HTTP, Telnet, and OSPF.

Step 1. Test R1 to R3 traffic and R3 to R1 traffic.

Ping from PC1 to PC3.

Ping from PC3 to PC1.

Both should fail.

Step 2. Test port 80 access.

To test port 80 functionality, enable the HTTP server on R2:

```
R2(config)# ip http server
```

From PC1, open a web browser to the R2 Serial 0/0/0 interface. This should be successful.

Step 3. Verify OSPF routes.

No routes should be lost. Confirm with **show ip route**.

Step 4. Test ping to R2.

Ping to R2 from R1 and PC1.

Ping to R2 from R3 and PC3.

Both should succeed.

Step 5. Perform other ping tests to confirm that all other traffic is denied.

Task 6: Document the Router Configurations

Task 7: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Packet Tracer Companion

Packet Tracer Companion: Challenge Access Control Lists (5.5.2)

You can now open the file LSG04-Lab552.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for hands-on lab experience with real equipment.

Lab 5-3: Troubleshooting Access Control Lists (5.5.3)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram shown in Figure 5-6
- Erase the startup configuration and reload a router to the default state
- Load routers with scripts
- Find and correct network errors
- Document the corrected network

Figure 5-6 shows the network topology for this lab. Table 5-3 provides the IP addresses, subnet masks, and default gateways (where applicable) for all devices in the topology.

Figure 5-6 Network Topology for Lab 5-3

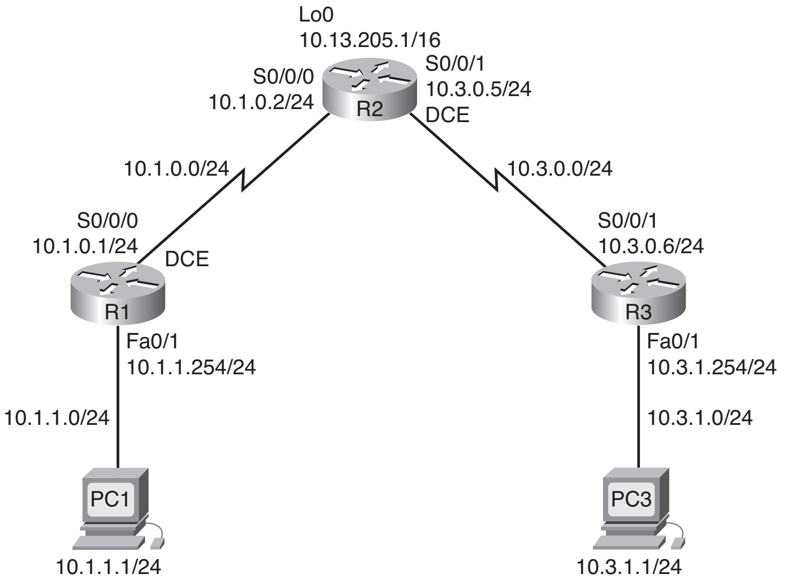


Table 5-3 Lab 5-3 Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0	10.1.0.1	255.255.255.0	—
	Fa0/1	10.1.1.254	255.255.255.0	—
R2	S0/0/0	10.1.0.2	255.255.255.0	—
	S0/0/1	10.3.0.5	255.255.255.0	—
	Lo 0	10.13.205.1	255.255.0.0	—
R3	S0/0/1	10.3.0.6	255.255.255.0	—
	Fa0/1	10.3.1.254	255.255.255.0	—
PC 1	NIC	10.1.1.1	255.255.255.0	10.1.1.254
PC 3	NIC	10.3.1.1	255.255.255.0	10.3.1.254

Scenario

You work for a regional service provider that has customers who have recently experienced several security breaches. Some security policies have been implemented that haven't addressed the customers' specific needs. Your department has been asked to examine the configuration, conduct tests, and change the configuration as necessary to secure the customer routers.

Ensure that your final configurations implement the following security policies:

- R1 and R3 customers request that only local PCs be able to access VTY lines. Log any attempts by other devices to access the VTY lines.
- R1 and R3 directly connected networks should not be allowed to send or receive traffic to or from each other. All other traffic should be allowed to and from R1 and R3.

A minimum of ACL statements should be used and applied inbound on the R2 serial interfaces. OSPF is used to distribute routing information. All passwords, except the enable secret password, are set to **cisco**. The enable secret password is set to **class**.

Task 1: Load Routers with the Supplied Scripts

Task 2: Find and Correct Network Errors

Find and correct all errors in the configuration. Document the steps you used to troubleshoot the network, and note each error found.

Task 3: Document the Corrected Network

Now that you have corrected all errors and tested connectivity throughout the network, document the final configuration for each device.

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Packet Tracer
□ Activity

Packet Tracer Exercise 5.1: Named Access Control Lists

You can now open the file LSG04-Lab0554.pka on the CD-ROM that accompanies this book to complete this activity using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for hands-on lab experience with real equipment.

Packet Tracer
□ Activity

Packet Tracer Exercise 5.2: Access Control Lists

You can now open the file LSG04-Lab0555.pka on the CD-ROM that accompanies this book to complete this activity using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for hands-on lab experience with real equipment.

Packet Tracer
□ Challenge

Packet Tracer Skills Integration Challenge

Open file LSG04-PTSkills5.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer. Upon completion of this skills integration challenge, you will be able to

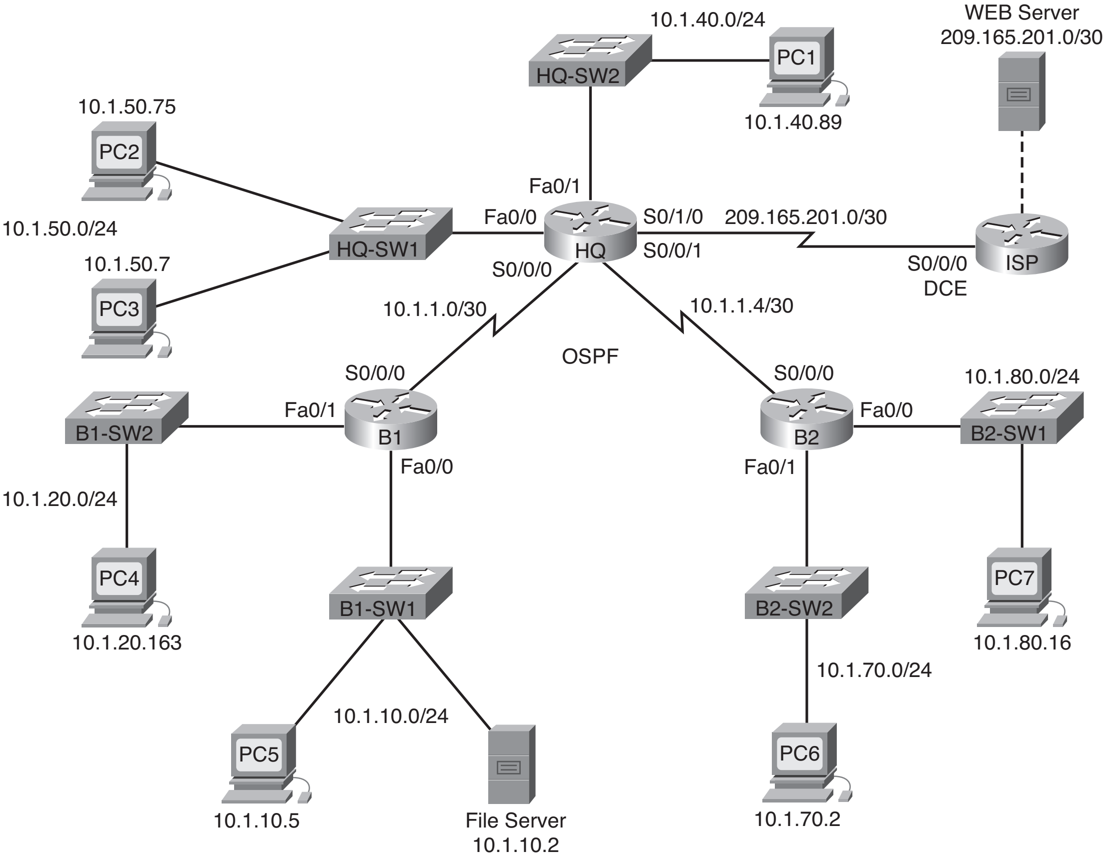
- Configure PPP with CHAP authentication
- Configure default routing
- Configure OSPF routing
- Implement and verify multiple ACL security policies

Figure 5-7 shows the network topology for this lab. Table 5-4 provides the IP addresses, subnet masks, and default gateways (where applicable) for all devices in the topology.

Table 5-4 Lab 5-6 Addressing Table

Device	Interface	IP Address	Subnet Mask
HQ	S0/0/0	10.1.1.1	255.255.255.252
	S0/0/1	10.1.1.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
	Fa0/0	10.1.50.1	255.255.255.0
	Fa0/1	10.1.40.1	255.255.255.0
B1	S0/0/0	10.1.1.2	255.255.255.252
	Fa0/0	10.1.10.1	255.255.255.0
	Fa0/1	10.1.20.1	255.255.255.0
B2	S0/0/0	10.1.1.6	255.255.255.252
	Fa0/0	10.1.80.1	255.255.255.0
	Fa0/1	10.1.70.1	255.255.255.0
ISP	S0/0/0	209.165.201.1	255.255.255.252
	Fa0/0	209.165.202.129	255.255.255.252
Web Server	NIC	209.165.202.130	255.255.255.252

Figure 5-7 Network Topology for Lab 5-6



Introduction

In this activity, you will demonstrate your ability to configure ACLs that enforce five security policies. In addition, you will configure PPP and OSPF routing. The devices are already configured with IP addressing. The user EXEC password is **cisco,** and the privileged EXEC password is **class**.

Task 1: Configure PPP with CHAP Authentication

Step 1. Configure the link between HQ and B1 to use PPP encapsulation with CHAP authentication.

The password for CHAP authentication is **cisco123**.

Step 2. Configure the link between HQ and B2 to use PPP encapsulation with CHAP authentication.

The password for CHAP authentication is **cisco123**.

Step 3. Verify that connectivity is restored between the routers.

HQ should be able to ping both B1 and B2. The interfaces may take a few minutes to come back up. You can switch back and forth between Realtime and Simulation modes to speed up the process. Another possible workaround to this Packet Tracer behavior is to use the **shutdown** and **no shutdown** commands on the interfaces.

Note: The interfaces may go down at random points during the activity because of a Packet Tracer bug. The interface normally comes back up on its own if you wait a few seconds.

Step 4. Check the results.

Your completion percentage should be 29%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Default Routing

Step 1. Configure default routing from HQ to ISP.

Configure a default route on HQ using the *exit interface* argument to send all default traffic to ISP.

Step 2. Test connectivity to Web Server.

HQ should be able to successfully ping Web Server at 209.165.202.130 as long as the ping is sourced from the Serial0/1/0 interface.

Step 3. Check the results.

Your completion percentage should be 32%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure OSPF Routing

Step 1. Configure OSPF on HQ.

Configure OSPF using the process ID 1.

Advertise all subnets except the 209.165.201.0 network.

Propagate the default route to OSPF neighbors.

Disable OSPF updates to ISP and to the HQ LANs.

Step 2. Configure OSPF on B1 and B2.

Configure OSPF using the process ID 1.

On each router, configure the appropriate subnets.

Disable OSPF updates to the LANs.

Step 3. Test connectivity throughout the network.

The network should now have full end-to-end connectivity. All devices should be able to successfully ping all other devices, including Web Server at 209.165.202.130.

Step 4. Check the results.

Your completion percentage should be 76%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Implement Multiple ACL Security Policies

Step 1. Implement security policy number 1.

Block the 10.1.10.0 network from accessing the 10.1.40.0 network. All other access to 10.1.40.0 is allowed. Configure the ACL on HQ using ACL number 10.

- Use a standard or extended ACL? _______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

Step 2. Verify that security policy number 1 is implemented.

A ping from PC5 to PC1 should fail.

Step 3. Check the results.

Your completion percentage should be 80%. If not, click **Check Results** to see which required components are not yet completed.

Step 4. Implement security policy number 2.

Host 10.1.10.5 is not allowed to access host 10.1.50.7. All other hosts are allowed to access 10.1.50.7. Configure the ACL on B1 using ACL number 115.

- Use a standard or extended ACL? _______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

Step 5. Verify that security policy number 2 is implemented.

A ping from PC5 to PC3 should fail.

Step 6. Check the results.

Your completion percentage should be 85%. If not, click **Check Results** to see which required components are not yet completed.

Step 7. Implement security policy number 3.

Hosts 10.1.50.1 through 10.1.50.63 are not allowed web access to the Intranet server at 10.1.80.16. All other access is allowed. Configure the ACL on the appropriate router, and use ACL number 101.

- Use a standard or extended ACL? _______________
- Configure the ACL on which router? _______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

Step 8. Verify that security policy number 3 is implemented.

To test this policy, click PC3, click the **Desktop** tab, and click **Web Browser**. For the URL, enter the IP address for the Intranet server, 10.1.80.16, and press **Enter**. After a few seconds, you should receive a Request Timeout message. PC2 and any other PC in the network should be able to access the Intranet server.

Step 9. Check the results.

Your completion percentage should be 90%. If not, click **Check Results** to see which required components are not yet completed.

Step 10. Implement security policy number 4.

Use the name **NO_FTP** to configure a named ACL that blocks the 10.1.70.0/24 network from accessing FTP services (port 21) on the file server at 10.1.10.2. All other access should be allowed.

Note: Names are case-sensitive.

- Use a standard or extended ACL? _______________
- Configure the ACL on which router? _______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

Step 11. Check the results.

Packet Tracer does not support testing FTP access, so you can't verify this policy. However, your completion percentage should be 95%. If not, click **Check Results** to see which required components are not yet completed.

Step 12. Implement security policy number 5.

Because ISP represents connectivity to the Internet, configure a named ACL called **FIREWALL** in the following order:

1. Allow only inbound ping replies from ISP and any source beyond ISP.
2. Allow only established TCP sessions from ISP and any source beyond ISP.
3. Explicitly block all other inbound access from ISP and any source beyond ISP. Although this is not needed because of the implicit deny, having an explicit deny helps remind administrators that all other traffic is denied.

- Use a standard or extended ACL? _______________
- Configure the ACL on which router? ______________
- Apply the ACL to which interface? _______________
- Apply the ACL in which direction? _______________

Step 13. Verify that security policy number 5 is implemented.

To test this policy, any PC should be able to ping ISP or Web Server. However, neither ISP nor Web Server should be able to ping HQ or any other device behind the ACL.

Step 14. Check the results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.