CCNAv7: Enterprise Networking, Security, and Automation

Companion Guide

Networking Academy

Enterprise Networking, Security, and Automation Companion Guide (CCNAv7)

Cisco Press

Enterprise Networking, Security, and Automation Companion Guide (CCNAv7)

Cisco Networking Academy

Published by:
Cisco Press

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020935515

ISBN-13: 978-0-13-663432-4

ISBN-10: 0-13-663432-X

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Enterprise Networking, Security, and Automation (CCNAv7) course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

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.netacad.com

Editor-in-Chief
Mark Taub

Alliances Manager, Cisco Press
Arezou Gol

Director, ITP Product Management
Brett Bartow

Senior Editor
James Manly

Managing Editor
Sandra Schroeder

Development Editor
Ellie Bru

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Technical Editor
Bob Vachon

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Ken Johnson

Proofreader
Betty Pessagno

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Contributing Authors

Bob Vachon is a professor at Cambrian College (Sudbury, Ontario) and Algonquin College (Ottawa, Ontario). He has more than 30 years of computer, networking, and information technology teaching experience and has collaborated on many Cisco Networking Academy courses, including CCNA, CCNA Security, CCNP, Cybersecurity, and more as team lead, lead author, and subject matter expert. Bob enjoys playing guitar by a campfire with friends and family.

Allan Johnson entered the academic world in 1999, after 10 years as a business owner/operator, to dedicate his efforts to his passion for teaching. He holds both an M.B.A. and an M.Ed. in training and development. He taught CCNA courses at the high school level for 7 years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as Curriculum Lead.

Contents at a Glance

Contents

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Enterprise Networking, Security, and Automation Companion Guide (CCNAv7) is the official supplemental textbook for the Cisco Network Academy CCNA Enterprise Networking, Security, and Automation version 7 course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application and provides opportunities to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small to medium-sized businesses as well as enterprise and service provider environments.

This book provides a ready reference that explains the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternative explanations and examples to supplement the course. You can use the online curriculum as directed by your instructor and then use this *Companion Guide*'s study tools to help solidify your understanding of all the topics.

Who Should Read This Book

The book, like the course it accompanies, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Networking Academy courses and preparation for the CCNA certification.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following list gives you a thorough overview of the features provided in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives listed in the corresponding chapters of the online curriculum; however, the question

format in the *Companion Guide* encourages you to think about finding the answers as you read the chapter.

- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Summary:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of each chapter is a full list of all the labs, class activities, and Packet Tracer activities to refer to at study time.

Readability

The following features are provided to help you understand networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference to find the term used inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary that defines more than 1000 terms.

Practice

Practice makes perfect. This *Companion Guide* offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

Interactive Graphic

Video

- **Check Your Understanding questions and answer key:** Review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions in the online course. Appendix A, "Answers to the Check Your Understanding Questions," provides an answer key to all the questions and includes an explanation of each answer.
- **Labs and activities:** Throughout each chapter, you are directed back to the online course to take advantage of the activities provided to reinforce concepts. In addition, at the end of each chapter is a "Practice" section that lists all the labs and activities to provide practice with the topics introduced in this chapter.
- **Page references to online course:** After most headings is a number in parentheses—for example, (1.1.2). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

About Packet Tracer Software and Activities

Interspersed throughout the chapters, you'll find a few Cisco Packet Tracer activities. Packet Tracer allows you to create networks, visualize how packets flow in a network, and use basic testing tools to determine whether a 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 in the online course. Packet Tracer software is available only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Enterprise Networking, Security, and Automation v7 course and is divided into 14 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Single-Area OSPFv2 Concepts":** This chapter explains single-area OSPF. It describes basic OSPF features and characteristics, packet types, and single-area operation.
- **Chapter 2, "Single-Area OSPFv2 Configuration":** This chapter explains how to implement single-area OSPFv2 networks. It includes router ID configuration, point-to-point configuration, DR/BDR election, single-area modification, default route propagation, and verification of a single-area OSPFv2 configuration.
- **Chapter 3, "Network Security Concepts":** This chapter explains how vulnerabilities, threats, and exploits can be mitigated to enhance network security. It includes descriptions of the current state of cybersecurity, tools used by threat actors, malware types, common network attacks, IP vulnerabilities, TCP and UDP vulnerabilities, network best practices, and cryptography.
- **Chapter 4, "ACL Concepts":** This chapter explains how ACLs are used to filter traffic, how wildcard masks are used, how to create ACLs, and the difference between standard and extended IPv4 ACLs.
- **Chapter 5, "ACLs for IPv4 Configuration":** The chapter explains how to implement ACLs. It includes standard IPv4 ACL configuration, ACL modifications using sequence numbers, applying an ACL to vty lines, and extended IPv4 ACL configuration.
- **Chapter 6, "NAT for IPv4":** This chapter explains how to enable NAT services on a router to provide IPv4 address scalability. It includes descriptions of the purpose and function of NAT, the different types of NAT, and the advantages and disadvantages of NAT. Configuration topics include static NAT, dynamic NAT, and PAT. NAT64 is also briefly discussed.

- **Chapter 7, "WAN Concepts":** This chapter explains how WAN access technologies can be used to satisfy business requirements. It includes descriptions of the purpose of a WAN, how WANs operate, traditional WAN connectivity options, modern WAN connectivity options, and internet-based connectivity options.
- **Chapter 8, "VPN and IPsec Concepts":** This chapter explains how VPNs and IPsec are used to secure communications. It includes descriptions of different types of VPNs and an explanation of how the IPsec framework is used to secure network traffic.
- **Chapter 9, "QoS Concepts":** This chapter explains how network devices use QoS to prioritize network traffic. It includes descriptions of network transmission characteristics, queuing algorithms, different queueing models, and QoS implementation techniques.
- **Chapter 10, "Network Management":** This chapter explains how to use a variety of protocols and techniques to manage a network, including CDP, LLDP, NTP, SNMP, and Syslog. In addition, this chapter discusses the management of configuration files and IOS images.
- **Chapter 11, "Network Design":** This chapter explains the characteristics of scalable networks. It includes descriptions of network convergence, considerations for designing scalable networks, and switch and router hardware.
- **Chapter 12, "Network Troubleshooting":** This chapter describes how to troubleshoot networks. It includes explanations of network documentation, troubleshooting methods, and troubleshooting tools. The chapter also demonstrates how to troubleshoot symptoms and causes of network problems using a layered approach.
- **Chapter 13, "Network Virtualization":** This chapter describes the purpose and characteristics of network virtualization. It includes descriptions of cloud computing, the importance of virtualization, network device virtualization, software-defined network, and controllers used in network programming.
- **Chapter 14, "Network Automation":** This chapter explains network automation. It includes descriptions of automation, data formats, APIs, REST, configuration management tools, and Cisco DNA Center.
- **Appendix A, "Answers to the 'Check Your Understanding' Questions":** This appendix lists the answers to the questions in the "Check Your Understanding Questions" section at the end of each chapter.
- **Glossary:** The Glossary provides definitions for all the key terms identified in each chapter.

Figure Credits

Figure 5-4, screenshot of Remote Access from PC1 © Tera Term Project

Figure 5-5, screenshot of Remote Access Attempt from PC2 © Tera Term Project

Figure 8-9, screenshot of Wireshark of Encapsulated Protocols © Wireshark

Figure 10-24, screenshot of Example of Using Tera Term to Backup a Configuration © Tera Term Project

Figure 10-25, screenshot of Example of Using Tera Term to Send a Configuration © Tera Term Project

Figure 12-16, screenshot of Wireshark Capture © Wireshark

Figure 13-1, screenshot of AWS Management Console © 2020, Amazon Web Services, Inc

Figure 14-1, screenshot of HTML Example and Resulting Web Page © WHATWG

This page intentionally left blank

CHAPTER 4

ACL Concepts

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- How do ACLs filter traffic?
- How do ACLs use wildcard masks?
- How do you create ACLs?
- What are the differences between standard and extended IPv4 ACLs?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

access control entry (ACE) *page 164*

inbound ACL *page 167*

outbound ACL *page 167*

implicit deny *page 167*

wildcard mask *page 168*

numbered ACL *page 175*

standard ACL *page 175*

extended ACL *page 175*

named ACL *page 176*

Introduction (4.0)

Say that you have arrived at your grandparents' residence. It is a beautiful gated community with walking paths and gardens. For the safety of the residents, no one is permitted to get into the community without stopping at the gate and presenting the guard with identification. You provide your ID, and the guard verifies that you are expected as a visitor. He documents your information and lifts the gate. Imagine if the guard had to do this for the many staff members who entered each day. The security department has simplified this process by assigning a badge to each employee that can be scanned to automatically raise the gate. You greet your grandparents, who are anxiously awaiting you at the front desk. You all get back into the car to go down the street for dinner. As you exit the parking lot, you must again stop and show your identification so that the guard will lift the gate. Rules have been put in place for all incoming and outgoing traffic.

Much like the guard in the gated community, an access control list (ACL) may be configured to permit and deny network traffic passing through an interface. The router compares the information within a packet against each access control entry (ACE), in sequential order, to determine if the packet matches one of the ACEs. This process is called *packet filtering*. Let's learn more!

Purpose of ACLs (4.1)

This section describes how ACLs filter traffic in small- to medium-sized business networks.

What Is an ACL? (4.1.1)

Routers make routing decisions based on information in each packet's header. Traffic entering a router interface is routed solely based on information in the routing table. The router compares the destination IP address with routes in the routing table to find the best match and then forwards a packet based on the best match route. A similar process can be used to filter traffic using an access control list (ACL).

An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. By default, a router does not have any ACLs configured. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine if each packet can be forwarded.

An ACL uses a sequential list of permit or deny statements known as ***access control entries (ACEs)***.

Note

ACEs are also commonly called ACL statements.

When network traffic passes through an interface configured with an ACL, the router compares the information within the packet against each ACE, in sequential order, to determine whether the packet matches one of the ACEs. This process is called packet *filtering*.

Several tasks performed by routers require the use of ACLs to identify traffic. Table 4-1 lists some of these tasks and provides examples.

Table 4-1 Tasks That Use ACLs

Task	Example
Limit network traffic to increase network performance	■ A corporate policy prohibits video traffic on the network to reduce the network load. ■ A policy can be enforced using ACLs to block video traffic.
Provide traffic flow control	■ A corporate policy requires that routing protocol traffic be limited to certain links only. ■ A policy can be implemented using ACLs to restrict the delivery of routing updates to only those that come from a known source.
Provide a basic level of security for network access	■ Corporate policy demands that access to the human resources network be restricted to authorized users only. ■ A policy can be enforced using ACLs to limit access to specified networks.
Filter traffic based on traffic type	■ Corporate policy requires that email traffic be permitted into a network but that Telnet access be denied. ■ A policy can be implemented using ACLs to filter traffic by type.
Screen hosts to permit or deny access to network services	■ Corporate policy requires that access to some file types (such as FTP or HTTP) be limited to user groups. ■ A policy can be implemented using ACLs to filter user access to services.
Provide priority to certain classes of network traffic	■ Corporate traffic specifies that voice traffic be forwarded as fast as possible to avoid any interruption. ■ A policy can be implemented using ACLs and QoS to identify voice traffic and process it immediately.

Packet Filtering (4.1.2)

Packet filtering controls access to a network by analyzing the incoming and/or outgoing packets and forwarding them or discarding them based on given criteria. Packet filtering can occur at Layer 3 or Layer 4, as shown in Figure 4-1.

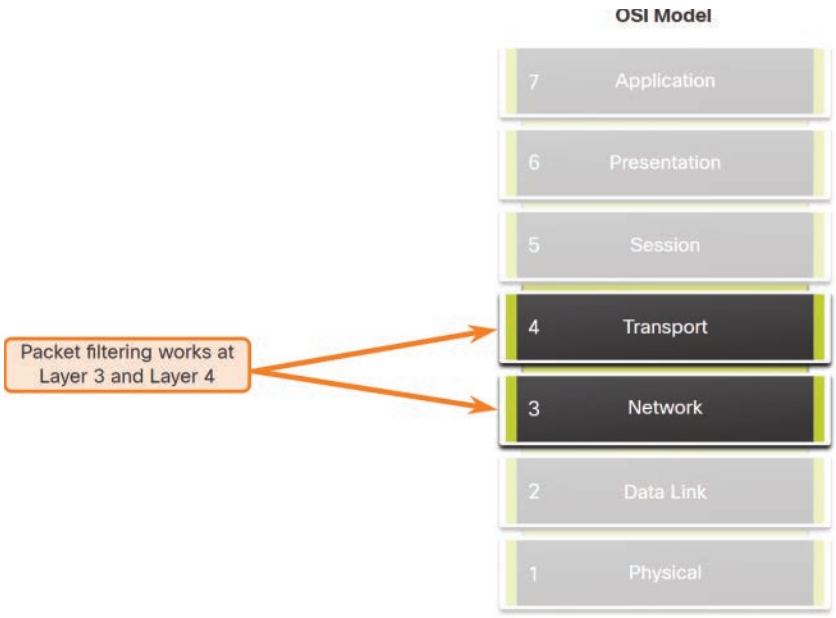

Figure 4-1 Packet Filtering in the OSI Model

Cisco routers support two types of ACLs:

- **Standard ACLs:** These ACLs only filter at Layer 3, using the source IPv4 address only.
- **Extended ACLs:** These ACLs filter at Layer 3 using the source and/or destination IPv4 address. They can also filter at Layer 4 using TCP, UDP ports, and optional protocol type information for finer control.

ACL Operation (4.1.3)

An ACL defines a set of rules that give added control for packets that enter inbound interfaces, packets relayed through the router, and packets that exit outbound interfaces of the router.

ACLs can be configured to apply to inbound traffic and outbound traffic, as shown in Figure 4-2.

Figure 4-2 ACLs on Inbound and Outbound Interfaces

Note

ACLs do not act on packets that originate from the router itself.

An *inbound ACL* filters packets before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If a packet is permitted by the ACL, it is processed for routing. Inbound ACLs are best used to filter packets when the network attached to an inbound interface is the only source of packets that need to be examined.

An *outbound ACL* filters packets after they are routed, regardless of the inbound interface. Incoming packets are routed to the outbound interface, and they are then processed through the outbound ACL. Outbound ACLs are best used when the same filter will be applied to packets coming from multiple inbound interfaces before exiting the same outbound interface.

When an ACL is applied to an interface, it follows a specific operating procedure. For example, here are the operational steps used when traffic has entered a router interface with an inbound standard IPv4 ACL configured:

Step 1. The router extracts the source IPv4 address from the packet header.

Step 2. The router starts at the top of the ACL and compares the source IPv4 address to each ACE, in sequential order.

Step 3. When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.

Step 4. If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an *implicit deny* ACE automatically applied to all ACLs.

The last ACE statement of an ACL is always an implicit deny that blocks all traffic. By default, this statement is automatically implied at the end of an ACL even though it is hidden and not displayed in the configuration.

Note

An ACL must have at least one permit statement; otherwise, all traffic will be denied due to the implicit deny ACE statement.

Packet Tracer ☐ Activity

Packet Tracer—ACL Demonstration (4.1.4)

In this activity, you will observe how an ACL can be used to prevent a ping from reaching hosts on remote networks. After removing the ACL from the configuration, the pings will be successful.

Interactive Graphic

Check Your Understanding—Purpose of ACLs (4.1.5)

Refer to the online course to complete this activity.

Wildcard Masks in ACLs (4.2)

A wildcard mask is similar to a subnet mask but the reverse. In this section, you will learn how to calculate the inverse wildcard mask.

Wildcard Mask Overview (4.2.1)

In the previous section, you learned about the purpose of ACL. This section explains how ACLs use *wildcard masks*. An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match. Wildcard masks are also used by the Open Shortest Path First (OSPF) routing protocol.

A wildcard mask is similar to a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match. However, a wildcard mask and a subnet mask differ in the way they match binary 1s and 0s. Unlike with a subnet mask, in which binary 1 is equal to a match, and binary 0 is not a match, with a wildcard mask, the reverse is true.

Wildcard masks use the following rules to match binary 1s and 0s:

- **Wildcard mask bit 0:** Match the corresponding bit value in the address.
- **Wildcard mask bit 1:** Ignore the corresponding bit value in the address.

Table 4-2 lists some examples of wildcard masks and what they would match and ignore.

Table 4-2 Examples of Wildcard Masks

Wildcard Mask	Last Octet (in Binary)	Meaning (0—match, 1—ignore)
0.0.0.0	00000000	■ Match all octets.
0.0.0.63	00111111	■ Match the first three octets ■ Match the 2 leftmost bits of the last octet ■ Ignore the last 6 bits
0.0.0.15	00001111	■ Match the first three octets ■ Match the 4 leftmost bits of the last octet ■ Ignore the last 4 bits of the last octet

Wildcard Mask	Last Octet (in Binary)	Meaning (0—match, 1—ignore)
0.0.0.248	11111100	■ Match the first three octets ■ Ignore the 6 leftmost bits of the last octet ■ Match the last 2 bits
0.0.0.255	11111111	■ Match the first three octets ■ Ignore the last octet

Wildcard Mask Types (4.2.2)

Using wildcard masks takes some practice. The following sections provide examples to help you learn how wildcard masks are used to filter traffic for one host, one subnet, and a range IPv4 addresses.

Wildcard to Match a Host

In this example, the wildcard mask is used to match a specific host IPv4 address. Say that ACL 10 needs an ACE that only permits the host with IPv4 address 192.168.1.1. Recall that 0 equals a match, and 1 equals ignore. To match a specific host IPv4 address, a wildcard mask consisting of all zeros (that is, 0.0.0.0) is required.

Table 4-3 lists, in decimal and binary, the host IPv4 address, the wildcard mask, and the permitted IPv4 address.

Table 4-3 Wildcard to Match a Host Example

	Decimal	Binary
IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard mask	0.0.0.0	00000000.00000000.00000000.00000000
Permitted IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001

The 0.0.0.0 wildcard mask stipulates that every bit must match exactly. Therefore, when the ACE is processed, the wildcard mask will permit only the 192.168.1.1 address. The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.1.1 0.0.0.0**.

Wildcard Mask to Match an IPv4 Subnet

In this example, ACL 10 needs an ACE that permits all hosts in the 192.168.1.0/24 network. The wildcard mask 0.0.0.255 stipulates that the very first three octets must match exactly, but the fourth octet does not need to match.

Table 4-4 lists, in decimal and binary, the host IPv4 address, the wildcard mask, and the permitted IPv4 addresses.

Table 4-4 Wildcard Mask to Match an IPv4 Subnet Example

	Decimal	Binary
IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard mask	0.0.0.255	00000000.00000000.00000000.11111111
Permitted IPv4 address	**192.168.1.0/24**	**11000000.10101000.00000001.00000000**

When the ACE is processed, the wildcard mask 0.0.0.255 permits all hosts in the 192.168.1.0/24 network. The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.1.0 0.0.0.255**.

Wildcard Mask to Match an IPv4 Address Range

In this example, ACL 10 needs an ACE that permits all hosts in the 192.168.16.0/24, 192.168.17.0/24, …, 192.168.31.0/24 networks. The wildcard mask 0.0.15.255 would correctly filter that range of addresses.

Table 4-5 lists, in decimal and binary the host IPv4 address, the wildcard mask, and the permitted IPv4 addresses.

Table 4-5 Wildcard Mask to Match an IPv4 Address Range Example

	Decimal	Binary
IPv4 address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard mask	0.0.15.255	00000000.00000000.00001111.11111111
Permitted IPv4 address	**192.168.16.0/24 to 192.168.31.0/24**	**11000000.10101000.00010000.00000000 11000000.10101000.00011111.00000000**

The highlighted wildcard mask bits identify which bits of the IPv4 address must match. When the ACE is processed, the wildcard mask 0.0.15.255 permits all hosts in the 192.168.16.0/24 to 192.168.31.0/24 networks. The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.16.0 0.0.15.255**.

Wildcard Mask Calculation (4.2.3)

Calculating wildcard masks can be challenging. One shortcut method is to subtract the subnet mask from 255.255.255.255. The following sections provide examples to help you learn how to calculate the wildcard mask using the subnet mask.

Example 1

Say that you wanted an ACE in ACL 10 to permit access to all users in the 192.168.3.0/24 network. To calculate the wildcard mask, subtract the subnet mask (that is, 255.255.255.0) from 255.255.255.255, as shown in Table 4-6.

The solution produces the wildcard mask 0.0.0.255. Therefore, the ACE would be **access-list 10 permit 192.168.3.0 0.0.0.255**.

Table 4-6 Wildcard Mask Calculation—Example 1

Starting value	255.255.255.255
Subtract the subnet mask	–255.255.255. 0
Resulting wildcard mask	**0. 0. 0.255**

Example 2

In this example, say that you wanted an ACE in ACL 10 to permit network access for the 14 users in the subnet 192.168.3.32/28. Subtract the subnet (that is, 255.255.255.240) from 255.255.255.255, as shown in Table 4-7.

This solution produces the wildcard mask 0.0.0.15. Therefore, the ACE would be **access-list 10 permit 192.168.3.32 0.0.0.15**.

Table 4-7 Wildcard Mask Calculation—Example 2

Starting value	255.255.255.255
Subtract the subnet mask	–255.255.255.240
Resulting wildcard mask	**0. 0. 0. 15**

Example 3

In this example, say that you needed an ACE in ACL 10 to permit only networks 192.168.10.0 and 192.168.11.0. These two networks could be summarized as 192.168.10.0/23, which is a subnet mask of 255.255.254.0. Again, you subtract 255.255.254.0 subnet mask from 255.255.255.255, as shown in Table 4-8.

This solution produces the wildcard mask 0.0.1.255. Therefore, the ACE would be **access-list 10 permit 192.168.10.0 0.0.1.255**.

Table 4-8 Wildcard Mask Calculation—Example 3

Starting value	255.255.255.255
Subtract the subnet mask	–255.255.254. 0
Resulting wildcard mask	**0. 0. 1.255**

Example 4

Consider an example in which you need an ACL number 10 to match networks in the range 192.168.16.0/24 to 192.168.31.0/24. This network range could be summarized as 192.168.16.0/20, which is a subnet mask of 255.255.240.0. Therefore, subtract 255.255.240.0 subnet mask from 255.255.255.255, as shown in Table 4-9.

This solution produces the wildcard mask 0.0.15.255. Therefore, the ACE would be **access-list 10 permit 192.168.16.0 0.0.15.255**.

Table 4-9 Wildcard Mask Calculation—Example 4

Starting value	255.255.255.255
Subtract the subnet mask	– 255.255.240. 0
Resulting wildcard mask	0. 0. 15.255

Wildcard Mask Keywords (4.2.4)

Working with decimal representations of binary wildcard mask bits can be tedious. To simplify this task, Cisco IOS provides two keywords to identify the most common uses of wildcard masking. Keywords reduce ACL keystrokes and make it easier to read an ACE.

The two keywords are

- **host:** This keyword substitutes for the 0.0.0.0 mask and indicates that all IPv4 address bits must match to filter just one host address.
- **any:** This keyword substitutes for the 255.255.255.255 mask and indicates to ignore the entire IPv4 address or to accept any addresses.

In the command output in Example 4-1, two ACLs are configured. The ACL 10 ACE permits only the 192.168.10.10 host, and the ACL 11 ACE permits all hosts.

Example 4-1 ACLs Configured Without Keywords

```
R1(config)# access-list 10 permit 192.168.10.10 0.0.0.0
R1(config)# access-list 11 permit 0.0.0.0 255.255.255.255
R1(config)#
```

Alternatively, the keywords **host** and **any** could be used to replace the highlighted output. The commands in Example 4-2 accomplishes the same task as the commands in Example 4-1.

Example 4-2 ACLs Configured Using Keywords

```
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# access-list 11 permit any
R1(config)#
```

Interactive Graphic

Check Your Understanding—Wildcard Masks in ACLs (4.2.5)

Refer to the online course to complete this activity.

Guidelines for ACL Creation (4.3)

This section provides guidelines for creating ACLs.

Limited Number of ACLs per Interface (4.3.1)

In a previous section, you learned about how wildcard masks are used in ACLs. This section discusses guidelines for ACL creation. There is a limit on the number of ACLs that can be applied on a router interface. For example, a dual-stacked (that is, IPv4 and IPv6) router interface can have up to four ACLs applied, as shown in Figure 4-3.

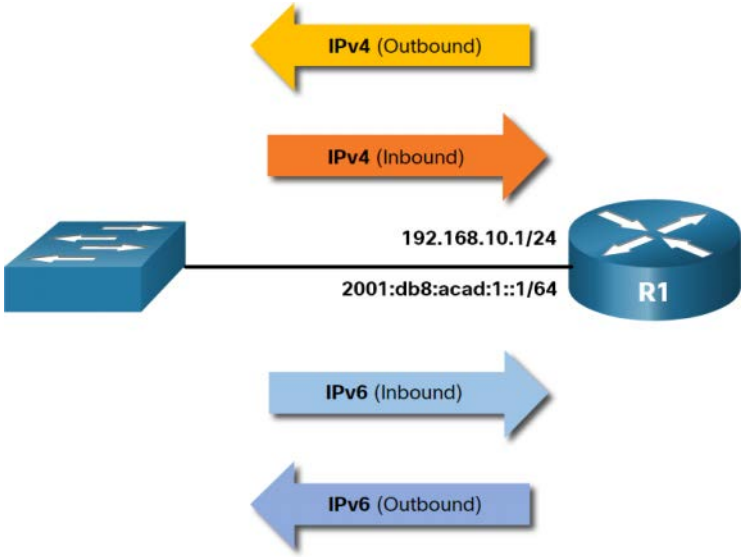

Figure 4-3 ACLs Limited on Interfaces

Specifically, a dual-stacked router interface can have

- One outbound IPv4 ACL
- One inbound IPv4 ACL
- One inbound IPv6 ACL
- One outbound IPv6 ACL

Say that R1 has two dual-stacked interfaces that need to have inbound and outbound IPv4 and IPv6 ACLs applied. As shown in Figure 4-4, R1 could have up to 8 ACLs configured and applied to interfaces.

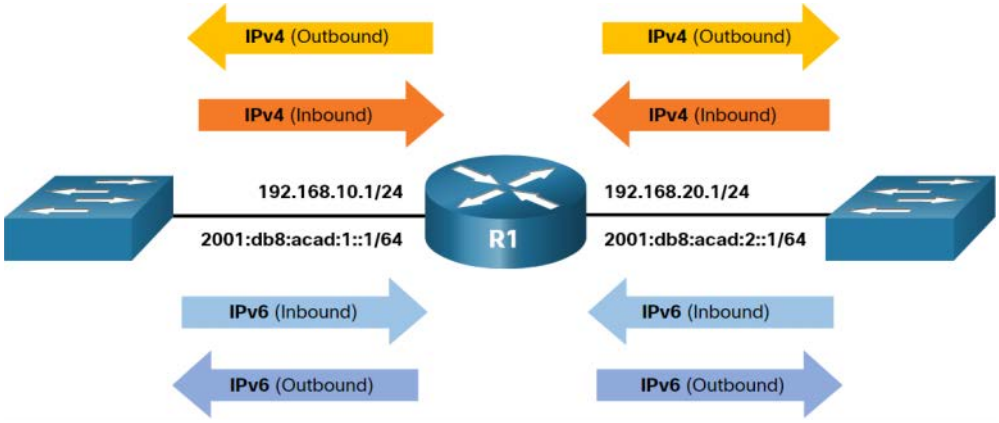

Figure 4-4 ACLs Limit Example

In this case, each interface would have four ACLs: two ACLs for IPv4 and two ACLs for IPv6. For each protocol, one ACL is for inbound traffic and one for outbound traffic.

Note

ACLs do not have to be configured in both directions. The number of ACLs and their direction applied to the interface will depend on the security policy of the organization.

ACL Best Practices (4.3.2)

Using ACLs requires attention to detail and great care. Mistakes can be costly in terms of downtime, troubleshooting efforts, and network service. Basic planning is required before configuring an ACL.

Table 4-10 presents some ACL best practices.

Table 4-10 Guidelines for ACLs

Guideline	Benefit
Base ACLs on the organization's security policies.	This will ensure that you implement organizational security guidelines.
Write out what you want an ACL to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit, and save all your ACLs.	This will help you create a library of reusable ACLs.
Document ACLs by using the **remark** command.	This will help you (and others) understand the purpose of an ACE.
Test ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

Interactive Graphic

Check Your Understanding—Guidelines for ACL Creation (4.3.3)

Refer to the online course to complete this activity.

Types of IPv4 ACLs (4.4)

This section compares IPv4 standard and extended ACLs.

Standard and Extended ACLs (4.4.1)

The previous sections describe the purpose of ACLs as well as guidelines for ACL creation. This section covers standard and extended ACLs and named and *numbered ACLs*, and it provides examples of placement of these ACLs.

There are two types of IPv4 ACLs:

- *Standard ACLs*: These ACLs permit or deny packets based only on the source IPv4 address.
- *Extended ACLs*: These ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more.

For example, Example 4-3 shows how to create a standard ACL. In this example, ACL 10 permits hosts on the source network 192.168.10.0/24. Because of the implied "deny any" at the end, all traffic except for traffic coming from the 192.168.10.0/24 network is blocked with this ACL.

Example 4-3 Standard ACL Example

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#
```

In Example 4-4, the extended ACL 100 permits traffic originating from any host on the 192.168.10.0/24 network to any IPv4 network if the destination host port is 80 (HTTP).

Example 4-4 Extended ACL Example

```
R1(config)# access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)#
```

Notice that the standard ACL 10 is only capable of filtering by source address, while the extended ACL 100 is filtering on the source and destination Layer 3 and Layer 4 protocol (for example, TCP) information.

Note

Full IPv4 ACL configuration is discussed in Chapter 5, "ACLs for IPv4 Configuration."

Numbered and Named ACLs (4.4.2)

For IPv4, there are both numbered and *named ACLs*.

Numbered ACLs

ACLs 1 to 99 and 1300 to 1999 are standard ACLs, while ACLs 100 to 199 and 2000 to 2699 are extended ACLs, as shown in Example 4-5.

Example 4-5 Available ACL Numbers

```
R1(config)# access-list ?
  <1-99>         IP standard access list
  <100-199>      IP extended access list
  <1100-1199>    Extended 48-bit MAC address access list
  <1300-1999>    IP standard access list (expanded range)
  <200-299>      Protocol type-code access list
  <2000-2699>    IP extended access list (expanded range)
  <700-799>      48-bit MAC address access list
  rate-limit     Simple rate-limit specific access list
  template       Enable IP template acls
Router(config)# access-list
```

Named ACLs

Using named ACLs is the preferred method when configuring ACLs. You can name standard and extended ACLs to provide information about the purpose of each ACL. For example, the extended ACL name FTP-FILTER is far easier to identify than the ACL number 100.

The **ip access-list** global configuration command is used to create a named ACL, as shown in Example 4-6.

Note

Numbered ACLs are created using the **access-list** global configuration command.

Example 4-6 Example of a Named ACL

```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
R1(config-ext-nacl)#
```

The following are the general rules to follow for named ACLs:

- Assign a name to identify the purpose of the ACL.
- Names can contain alphanumeric characters.
- Names cannot contain spaces or punctuation.
- It is suggested that a name be written in CAPITAL LETTERS.
- Entries can be added or deleted within an ACL.

Where to Place ACLs (4.4.3)

Every ACL should be placed where it has the greatest impact on efficiency.

Figure 4-5 illustrates where standard and extended ACLs should be located in an enterprise network.

Say that the objective is to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network. Extended ACLs should be located as close as possible to the source of the traffic to be filtered. This way, undesirable traffic is denied close to the source network, without crossing the network infrastructure.

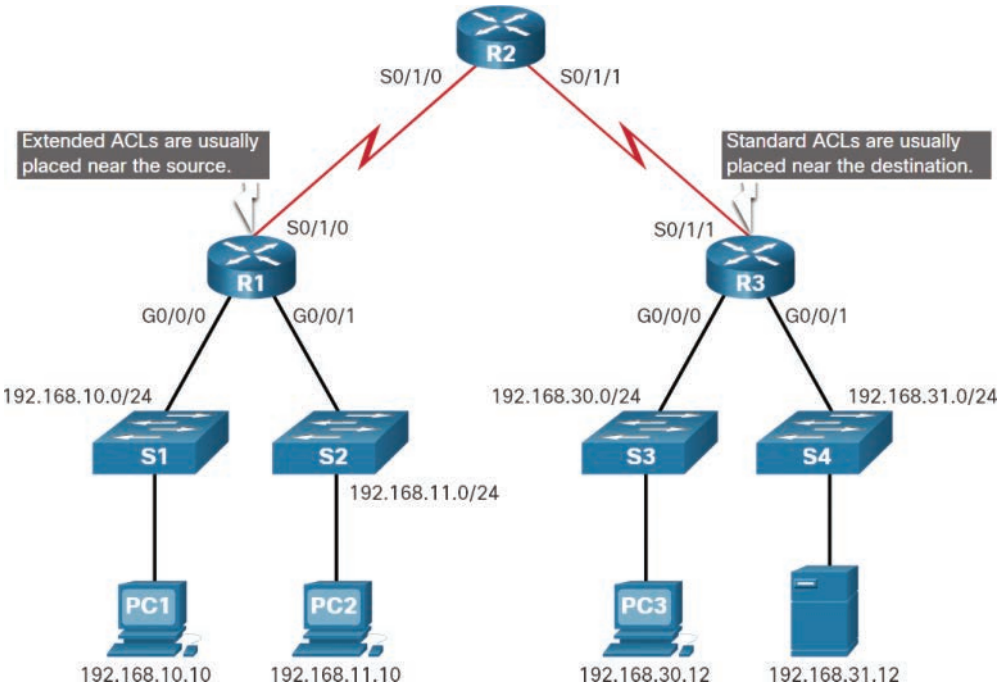

Figure 4-5 Example of Where to Place ACLs

Standard ACLs should be located as close to the destination as possible. If a standard ACL were placed at the source of the traffic, the "permit" or "deny" would occur based on the given source address, regardless of the traffic destination.

Placement of an ACL and, therefore, the type of ACL used, may also depend on a variety of factors, as listed in Table 4-11.

Table 4-11 ACL Placement Factors

Factors Influencing ACL Placement	Explanation
The extent of organizational control	■ Placement of the ACL can depend on whether the organization has control of both the source and destination networks.
Bandwidth of the networks involved	■ It may be desirable to filter unwanted traffic at the source to prevent transmission of bandwidth-consuming traffic.
Ease of configuration	■ It may be easier to implement an ACL at the destination, but traffic will use bandwidth unnecessarily. ■ An extended ACL could be used on each router where the traffic originated. This would save bandwidth by filtering the traffic at the source, but it would require creation of extended ACLs on multiple routers.

Standard ACL Placement Example (4.4.4)

Following the guidelines for ACL placement, standard ACLs should be located as close to the destination as possible.

In Figure 4-6, the administrator wants to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.

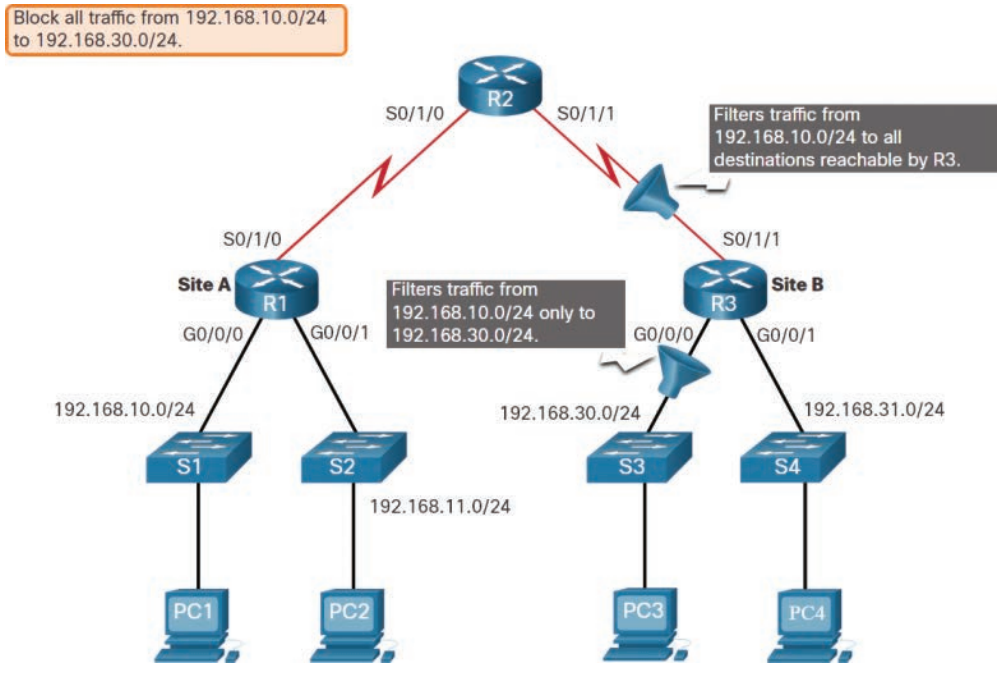

Figure 4-6 Standard ACL Example Topology

Following the basic placement guidelines, the administrator would place a standard ACL on router R3. There are two possible interfaces on R3 to which to apply the standard ACL:

- **R3 S0/1/1 interface (inbound):** The standard ACL can be applied inbound on the R3 S0/1/1 interface to deny traffic from the .10 network. However, it would also filter .10 traffic to the 192.168.31.0/24 (.31 in this example) network. Therefore, the standard ACL should not be applied to this interface.
- **R3 G0/0 interface (outbound):** The standard ACL can be applied outbound on the R3 G0/0/0 interface. This will not affect other networks that are reachable by R3. Packets from the .10 network will still be able to reach the .31 network. This is the best interface to place the standard ACL to meet the traffic requirements.

Extended ACL Placement Example (4.4.5)

Extended ACLs should be located as close to the source as possible to prevent unwanted traffic from being sent across multiple networks only to be denied when it reaches its destination.

However, an organization can only place ACLs on devices that it controls. Therefore, the extended ACL placement must be determined in the context of where organizational control extends.

In Figure 4-7, for example, Company A wants to deny Telnet and FTP traffic to Company B's 192.168.30.0/24 network from its 192.168.11.0/24 network while permitting all other traffic.

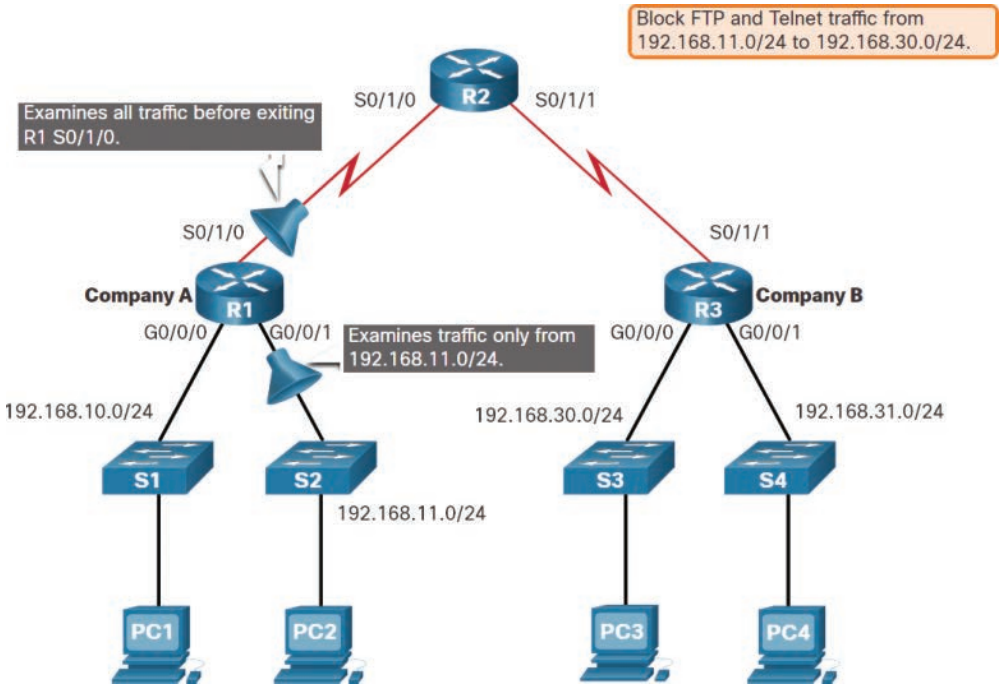

Figure 4-7 Extended ACL Example Topology

There are several ways to accomplish these goals. An extended ACL on R3 would accomplish the task, but the administrator does not control R3. In addition, this solution would allow unwanted traffic to cross the entire network, only to be blocked at the destination, which would affect overall network efficiency.

The solution is to place on R1 an extended ACL that specifies both source and destination addresses. There are two possible interfaces on R1 to apply the extended ACL:

- **R1 S0/1/0 interface (outbound):** The extended ACL can be applied outbound on the S0/1/0 interface. However, this solution would process all packets leaving R1, including packets from 192.168.10.0/24.
- **R1 G0/0/1 interface (inbound):** The extended ACL can be applied inbound on the G0/0/1, and only packets from the 192.168.11.0/24 network are subject to ACL processing on R1. Because the filter is to be limited to only those packets leaving the 192.168.11.0/24 network, applying the extended ACL to G0/1 is the best solution.

Interactive Graphic

Check Your Understanding—Guidelines for ACL Placement (4.4.6)

Refer to the online course to complete this activity.

Summary (4.5)

The following is a summary of the sections in this chapter.

Purpose of ACLs

Several tasks performed by routers require the use of ACLs to identify traffic. An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. A router does not have any ACLs configured by default. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine whether the packets can be forwarded. An ACL uses a sequential list of permit or deny statements, known as ACEs. Cisco routers support two types of ACLs: standard ACLs and extended ACLs. An inbound ACL filters packets before they are routed to the outbound interface. If a packet is permitted by the ACL, it is then processed for routing. An outbound ACL filters packets after being routed, regardless of the inbound interface. When an ACL is applied to an interface, it follows a specific operating procedure:

Step 1. The router extracts the source IPv4 address from the packet header.

Step 2. The router starts at the top of the ACL and compares the source IPv4 address to each ACE, in sequential order.

Step 3. When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.

Step 4. If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an implicit deny ACE automatically applied to all ACLs.

Wildcard Masks

An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match. Wildcard masks are also used by the Open Shortest Path First (OSPF) routing protocol. A wildcard mask is similar to a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match. However, a wildcard mask and a subnet mask differ in the way they match binary 1s and 0s. Wildcard mask bit 0 matches the corresponding bit value in the address. Wildcard mask bit 1 ignores the corresponding bit value in the address. A wildcard mask is used to filter traffic for one host, one subnet, and a range of IPv4 addresses. A shortcut for calculating a wildcard mask is to subtract the subnet mask from 255.255.255.255. Working with decimal representations of binary wildcard mask bits

can be simplified by using the Cisco IOS keywords **host** and **any** to identify the most common uses of wildcard masking. Keywords reduce ACL keystrokes and make it easier to read ACEs.

Guidelines for ACL Creation

There is a limit on the number of ACLs that can be applied on a router interface. For example, a dual-stacked (that is, IPv4 and IPv6) router interface can have up to four ACLs applied. Specifically, a router interface can have one outbound IPv4 ACL, one inbound IPv4 ACL, one inbound IPv6 ACL, and one outbound IPv6 ACL. ACLs do not have to be configured in both directions. The number of ACLs and the direction in which they are applied to the interface depend on the security policy of the organization. Basic planning is required before configuring an ACL and includes the following best practices:

- Base ACLs on the organization's security policies.
- Write out what you want the ACL to do.
- Use a text editor to create, edit, and save all of your ACLs.
- Document ACLs by using the **remark** command.
- Test the ACLs on a development network before implementing them on a production network.

Types of IPv4 ACLs

There are two types of IPv4 ACLs: standard ACLs and extended ACLs. Standard ACLs permit or deny packets based only on the source IPv4 address. Extended ACLs permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports, and more. ACLs 1 to 99 and 1300 to 1999 are standard ACLs. ACLs 100 to 199 and 2000 to 2699 are extended ACLs. Using named ACLs is the preferred method when configuring ACLs. Standard and extended ACLs can be named to provide information about the purpose of each ACL.

The following are basic rules to follow for named ACLs:

- Assign a name to identify the purpose of an ACL.
- Names can contain alphanumeric characters.
- Names cannot contain spaces or punctuation.
- It is suggested that the name be written in CAPITAL LETTERS.
- Entries can be added or deleted within an ACL.

Every ACL should be placed where it has the greatest impact on efficiency. Extended ACLs should be located as close as possible to the source of the traffic to be filtered. This way, undesirable traffic is denied close to the source network without crossing the network infrastructure. Standard ACLs should be located as close to the destination as possible. If a standard ACL were placed at the source of the traffic, the "permit" or "deny" would occur based on the given source address, regardless of the traffic destination. Placement of the ACL may depend on the extent of organizational control, bandwidth of the networks, and ease of configuration.

Practice

The following Packet Tracer activity provides practice with the topics introduced in this chapter. The instructions are available in the companion *Enterprise Networking, Security, and Automation Labs & Study Guide (CCNAv7)* (ISBN 9780136634690). There are no labs for this chapter.

Packet Tracer Activity

Packet Tracer Activity

Packet Tracer 4.1.4: ACL Demonstration

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix "Answers to the 'Check Your Understanding' Questions" lists the answers.

1. What two functions describe uses of access control lists? (Choose two.)

   A. ACLs assist a router in determining the best path to a destination.
   B. ACLs can control which areas a host can access on a network.
   C. ACLs provide a basic level of security for network access.
   D. Standard ACLs can filter traffic based on source and destination network addresses.
   E. Standard ACLs can restrict access to specific applications and ports.

2. Which three statements describe how an ACL processes packets? (Choose three.)

   A. A packet is compared with all ACEs in the ACL before a forwarding decision is made.
   B. A packet that has been denied by one ACE can be permitted by a subsequent ACE.

C. An implicit deny at the end of an ACL rejects any packet that does not match an ACE.

D. Each ACE is checked only until a match is detected or until the end of the ACL.

E. If an ACE is matched, the packet is either rejected or forwarded, as directed by the ACE.

F. If an ACE is not matched, the packet is forwarded by default.

3. Which three statements are best practices related to placement of ACLs? (Choose three.)

A. Filter unwanted traffic before it travels onto a low-bandwidth link.

B. For every inbound ACL placed on an interface, ensure that there is a matching outbound ACL.

C. Place extended ACLs close to the destination IP address of the traffic.

D. Place extended ACLs close to the source IP address of the traffic.

E. Place standard ACLs close to the destination IP address of the traffic.

F. Place standard ACLs close to the source IP address of the traffic.

4. Which two characteristics are shared by standard and extended ACLs? (Choose two.)

A. Both filter packets for a specific destination host IP address.

B. Both include an implicit deny as a final entry.

C. Both permit or deny specific services by port number.

D. They both filter based on protocol type.

E. They can be created by using either descriptive names or numbers.

5. Which two statement describes a difference between the operation of inbound and outbound ACLs? (Choose two.)

A. Inbound ACLs are processed before the packets are routed.

B. Inbound ACLs can be used in both routers and switches.

C. Multiple inbound ACLs can be applied to an interface.

D. Multiple outbound ACLs can be applied to an interface.

E. Outbound ACLs are processed after the routing is completed.

F. Outbound ACLs can be used only on routers.

G. Unlike outbound ACLs, inbound ACLs can be used to filter packets with multiple criteria.

6. In which configuration would an outbound ACL placement be preferred over an inbound ACL placement?

   A. When a router has more than one ACL
   B. When an interface is filtered by an outbound ACL and the network attached to the interface is the source network being filtered within the ACL
   C. When an outbound ACL is closer to the source of the traffic flow
   D. When the ACL is applied to an outbound interface to filter packets coming from multiple inbound interfaces before the packets exit the interface

7. What wildcard mask will match networks 10.16.0.0 through 10.19.0.0?

   A. 0.252.255.255
   B. 0.0.255.255
   C. 0.0.3.255
   D. 0.3.255.255

8. What type of ACL offers increased flexibility and control over network traffic?

   A. Extended
   B. Extensive
   C. Named standard
   D. Numbered standard

9. Which statement describes a characteristic of standard IPv4 ACLs?

   A. They can be configured to filter traffic based on both source IP addresses and source ports.
   B. They can be created with a number but not with a name.
   C. They filter traffic based on destination IP addresses only.
   D. They filter traffic based on source IP addresses only.

10. What wildcard mask will match network 10.10.100.64/26?

    A. 0.0.0.15
    B. 0.0.0.31
    C. 0.0.0.63
    D. 0.0.0.127

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z