CCNA Security
Portable Command Guide

All the CCNA Security 640-554 commands in one compact, portable resource

ciscopress.com

Bob Vachon

CCNA Security Portable Command Guide

Bob Vachon

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

CCNA Security Portable Command Guide

Bob Vachon

Published by:

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

ISBN-10: 1-58720-448-7

ISBN-13: 978-1-58720-448-7

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing May 2012 with corrections March 2014

Library of Congress Cataloging-in-Publication Data will be inserted once available.

Warning and Disclaimer

This book is designed to provide information about the CCNA Security (640-554 IINS) exam and the commands needed at this level of network administration. Every effort has been made to make this book as complete and as accurate as possible, fitness is implied.

The information is provided on an "as is" basis. The author, 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.

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.

Publisher
Paul Boger

Associate Publisher
David Dusthimer

Executive Editor
Mary Beth Ray

Manager Global Certification
Erik Ullanderson

Business Operation Manager, Cisco Press
Anand Sundaram

Managing Editor
Sandra Schroeder

Development Editor
Andrew Cupp

Project Editor
Mandie Frank

Copy Editor
Keith Cline

Proofreader
Megan Wade

Technical Editor
Jim Lorenz

Book and Cover Designer
Gary Adair

Publishing Coordinator
Vanessa Evans

Composition
Mark Shirar

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.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales.

For more information please contact: U.S. Corporate and Government Sales

1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the U.S. please contact: International Sales international@pearsoned.com

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.**

Contents at a Glance

Contents

About the Author

Bob Vachon is a professor in the Computer Systems Technology program at Cambrian College in Sudbury, Ontario, Canada, where he teaches networking infrastructure courses. He has worked and taught in the computer networking and information technology field since 1984. He has collaborated on various CCNA, CCNA Security, and CCNP projects for the Cisco Networking Academy as team lead, lead author, and subject matter expert. He enjoys playing the guitar and being outdoors, either working in his gardens or white-water canoe tripping.

About the Technical Reviewer

Jim Lorenz is an instructor and a senior training developer for the Cisco Networking Academy Program. He holds a bachelor's degree in computer information systems and has over 20 years of experience in networking and IT. Jim has developed course materials, including content, labs, and textbooks for the CCNA and CCNP curricula. Most recently he coordinated lab development for the CCNA Security course.

Dedications

This book is dedicated to my students. Thanks for reminding me why I do this stuff. I also dedicate this book to my beautiful wife Judy and daughters Lee-Anne, Joëlle, and Brigitte who, without their support and encouragement, I would not have been involved in this project.

Acknowledgments

I would like to start off with a big thanks to my friend Scott Empson for involving me with this project. Your *Portable Command Guide* series was a great idea and kudos to you for making it happen.

Thanks to the team at Cisco Press. Thank you Mary Beth for believing in me and to Drew and Mandie for making sure I got things done right and on time. Also thanks to my friend Jim for keeping me in check.

Special thanks to my Cisco Networking Academy family. A big thanks to Jeremy and Rob for involving me in these very cool projects. You guys keep me young.

Finally, a great big thanks to the folks at Cambrian College for letting me have fun and do what I love to do...teach!

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).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

Welcome to CCNA Security! Scott Empson had an idea to provide a summary of his engineering journal in a portable quick reference guide. The result is the *Portable Command Guide* series. These small books have proven to be very valuable for anyone studying for Cisco certifications or as a handy quick reference resource for anyone tasked with managing Cisco infrastructure devices.

The *CCNA Security Portable Command Guide* covers the security commands and GUI steps needed to pass the 640-554 IINS (Implementing Cisco IOS Network Security) certification exam. The guide begins by summarizing the required fundamental security concepts. It then provides the CLI commands and the Cisco Configuration Professional GUI screenshots required to secure an ISR. Examples are included to help demonstrate the security-related configuration.

The last section of the book focuses on securing a network using an Adaptive Security Appliance (ASA). It provides the CLI commands and the ASA Security Device Manager (ASDM) GUI screenshots required to secure an ASA 5505. Again, examples are included to help demonstrate the security-related configuration.

I hope that you learn as much from reading this guide as I did when I wrote it.

Networking Devices Used in the Preparation of This Book

To verify the commands in this book, I had to try them out on a few different devices. The following is a list of the equipment I used in the writing of this book:

- Cisco 1841 ISR running Cisco IOS advanced IP services software release 12.4(20)T1 and the Cisco Configuration Professional GUI version 2.6
- Cisco ASA 5505 running Cisco Adaptive Security Appliance software version 8.4(2) with a Base License and the ASA Security Device Manager (ASDM) GUI version 6.4(5)

Who Should Read This Book

This book is for those people preparing for the CCNA Security (640-554 IINS) exam, whether through self-study, on-the-job training and practice, study within the Cisco Academy Program, or study through the use of a Cisco Training Partner. There are also some handy hints and tips along the way to make life a bit easier for you in this endeavor. It is small enough that you will find it easy to carry around with you. Big, heavy textbooks might look impressive on your bookshelf in your office, but can you really carry them all around with you when you are working in some server room or equipment closet somewhere?

Organization of This Book

The parts of this book cover the following topics:

- **Part I, "Network Security Fundamentals"—**Introduces network security-related concepts and summarizes how security policies are implemented using a lifecycle approach. It also summarizes how to build a security strategy for borderless networks.
- **Part II, "Protecting the Network Infrastructure"—**Describes how to secure the management and data planes using the IOS CLI configuration commands and CCP.
- **Part III, "Threat Control and Containment"—**Describes how to secure an ISR against network threats using the IOS CLI configuration commands and CCP to configure ACLs, zoned-based firewall, and IOS IPS.
- **Part IV, "Secure Connectivity"—**Describes how to secure data as it traverses insecure networks using cryptology and virtual private networks (VPNs). Specifically, site-to-site IPsec VPNs are enabled using the IOS CLI configuration commands and CCP.
- **Part V, "Securing the Network Using the ASA"—**Describes how to secure a network using an ASA data as it traverses insecure networks using cryptology and virtual private networks (VPNs). Specifically, remote access SSL VPNs are enabled using the IOS CLI configuration commands and CCP.

This page intentionally left blank

CHAPTER 4
Network Foundation Protection

The chapter covers the following topics:

Threats Against the Network Infrastructure

Cisco Network Foundation Protection Framework

Control Plane Security

- Control Plane Policing

Management Plane Security

- Role-Based Access Control
- Secure Management and Reporting

Data Plane Security

- ACLs
- Antispoofing
- Layer 2 Data Plane Protection

Threats Against the Network Infrastructure

Common vulnerabilities and threats against a network infrastructure include the following:

Vulnerabilities	■ Design errors ■ Protocol weaknesses ■ Software vulnerabilities ■ Device misconfiguration
Threats	■ Trust exploitation ■ Login, authentication, and password attacks ■ Routing protocol exploits ■ Spoofing ■ Denial of service (DoS) ■ Confidentiality and integrity attacks

The impact of those threats and vulnerabilities includes the following:

Impact	■ Exposed management credentials ■ High CPU usage ■ Loss of protocol keepalives and updates ■ Route flaps and major network transitions ■ Slow or unresponsive management sessions ■ Indiscriminate packet drops

Cisco Network Foundation Protection Framework

The Cisco Network Foundation Protection (NFP) framework provides an umbrella strategy for infrastructure protection forming the foundation for continuous service delivery.

NFP logically divides a router and Catalyst switches into three functional areas:

Control plane	Provides the ability to route data correctly. Traffic consists of device-generated packets required for the operation of the network itself, such as Address Resolution Protocol (ARP) message exchanges or Open Shortest Path First (OSPF) protocol routing advertisements.
Management plane	Provides the ability to manage network elements. Traffic is generated either by network devices or network management stations using tools such as Telnet, Secure Shell (SSH), Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Network Time Protocol (NTP), or Simple Network Management Protocol (SNMP).
Data plane (forwarding plane)	Provides the ability to forward data. Typically consists of user-generated packets being forwarded to another end station. Most traffic travels through the router via the data plane. Data plane packets are typically processed in fast-switching cache.

Figure 4-1 provides a conceptual view of the NFP framework.

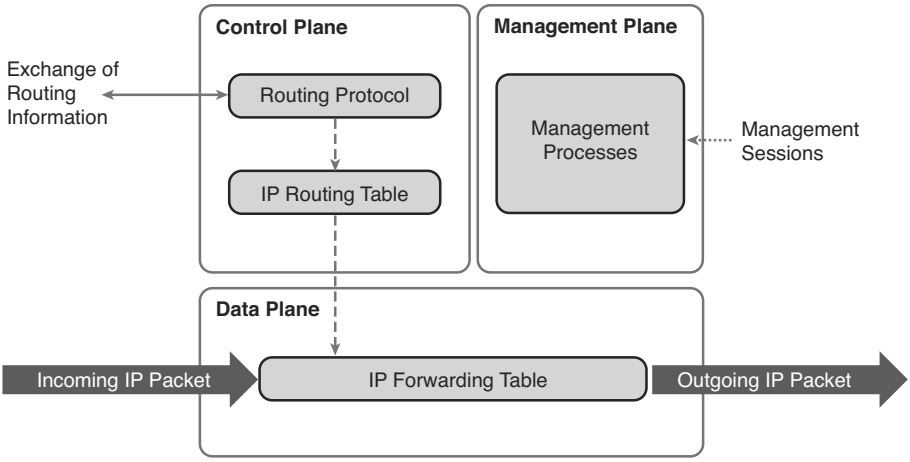

Figure 4-1 NFP Planes

Each of these planes must be protected to provide network availability and ensure continuous service delivery. The Cisco NFP framework provides the tools and techniques to secure each of these planes.

Control Plane Security

Control plane security can be implemented using the following features:

Cisco AutoSecure	Cisco AutoSecure provides a one-step device lockdown feature to protect the control plane and the management and data planes. It is a script that is initiated from the command-line interface (CLI) to configure the security posture of routers and disables nonessential system processes and services. It first makes recommendations to address security vulnerabilities and then modifies the router configuration.
Routing protocol authentication	Neighbor authentication prevents a router from accepting fraudulent routing updates. Most routing protocols support neighbor authentication.
CoPP	Control Plane Policing (CoPP) is used on higher-end Cisco devices with route processors. It is a Cisco IOS feature designed to enable users to manage the flow of traffic managed by the route processor of their network devices.

Control Plane Policing

CoPP is designed to prevent unnecessary traffic from overwhelming the route processor. The CoPP feature treats the control plane as a separate entity with its own ingress (input) and egress (output) ports. Because the CoPP feature treats the control plane as a separate entity, a set of rules can be established and associated with the ingress and egress ports of the control plane.

CoPP consists of the following features:

CoPP	Control Plane Policing lets users configure a QoS filter that manages the traffic flow of control plane packets. This protects the control plane against reconnaissance and DoS attacks.
CPPr	Control Plane Protection is an extension of CoPP but allows a finer policing granularity. For example, CPPr can filter and rate-limit the packets that are going to the control plane of the router and discard malicious and error packets (or both).
Control Plane Logging	The Control Plane Logging feature enables logging of the packets that CoPP or CPPr drop or permit. It provides the logging mechanism that is needed to deploy, monitor, and troubleshoot CoPP features efficiently.

Management Plane Security

Management plane security can be implemented using the following features:

Login and password policy	Restrict device accessibility. Limit the accessible ports and restrict the “who” and “how” methods of access.
Role-based access control	Ensure access is only granted to authenticated users, groups, and services. Role-based access control (RBAC) and authentication, authorization, and accounting (AAA) services provide mechanisms to effectively authenticate access.
Authorize actions	Restrict the actions and views that are permitted by any particular user, group, or service.
Secure management access and reporting	Log and account for all access. Record who accessed the device, what occurred, and when it occurred.
Ensure the confidentiality of data	Protect locally stored sensitive data from being viewed or copied. Use management protocols with strong authentication to mitigate confidentiality attacks aimed at exposing passwords and device configurations.
Present legal notification	Display legal notice developed with legal counsel.

Role-Based Access Control

RBAC restricts user access based on the role of the user. Roles are created for job or task functions and assigned access permissions to specific assets. Users are then assigned to roles and acquire the permissions that are defined for the role.

In Cisco IOS, the role-based CLI access feature implements RBAC for router management access. The feature creates different "views" that define which commands are accepted and what configuration information is visible. For scalability, users, permissions, and roles are usually created and maintained in a central repository server. This makes the access control policy available to multiple devices using it.

The central repository server can be a AAA server such as the Cisco Secure Access Control System (ACS) to provide AAA services to a network for management purposes.

Secure Management and Reporting

The management network is a very attractive target to hackers. For this reason, the management module has been built with several technologies designed to mitigate such risks.

The information flow between management hosts and the managed devices can be out-of-band (OOB) (information flows within a network on which no production traffic resides) or in-band (information flows across the enterprise production network, the Internet, or both).

Data Plane Security

Data plane security can be implemented using the following features:

Access control lists	Access control lists (ACLs) perform packet filtering to control which packets move through the network and where.
Antispoofing	ACLs can be used as an antispoofing mechanism that discards traffic that has an invalid source address.
Layer 2 security features	Cisco Catalyst switches have integrated features to help secure the Layer 2 infrastructure.

ACLs

ACLs are used to secure the data plane in a variety of ways, including the following:

Block unwanted traffic or users	ACLs can filter incoming or outgoing packets on an interface, controlling access based on source addresses, destination addresses, or user authentication.
Reduce the chance of DoS attacks	ACLs can be used to specify whether traffic from hosts, networks, or users can access the network. The TCP intercept feature can also be configured to prevent servers from being flooded with requests for a connection.

Mitigate spoofing attacks	ACLs enable security practitioners to implement recommended practices to mitigate spoofing attacks.
Provide bandwidth control	ACLs on a slow link can prevent excess traffic.
Classify traffic to protect other planes	ACLs can be applied on vty lines (management plane). ACLs can control routing updates being sent, received, or redistributed (control plane).

Antispoofing

Implementing the IETF best current practice 38 (BCP38) and RFC 2827 ingress traffic filtering renders the use of invalid source IP addresses ineffective, forcing attacks to be initiated from valid, reachable IP addresses which could be traced to the originator of an attack.

Features such as Unicast Reverse Path Forwarding (uRPF) can be used to complement the antispoofing strategy.

Layer 2 Data Plane Protection

The following are Layer 2 security tools integrated into the Cisco Catalyst switches:

Port security	Prevents MAC address spoofing and MAC address flooding attacks
DHCP snooping	Prevents client attacks on the Dynamic Host Configuration Protocol (DHCP) server and switch
Dynamic ARP inspection (DAI)	Adds security to ARP by using the DHCP snooping table to minimize the impact of ARP poisoning and spoofing attacks
IP source guard	Prevents IP spoofing addresses by using the DHCP snooping table