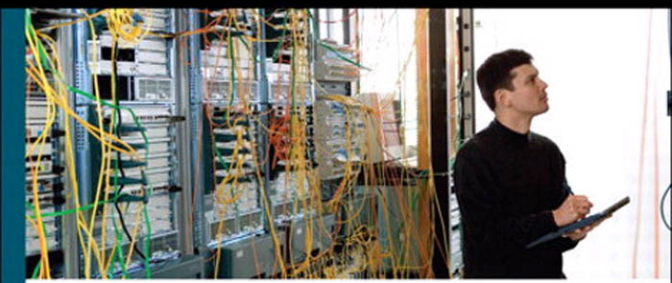


CCNP ISCW Portable Command Guide

All the ISCW 642-825 commands in one compact, portable resource

Scott Empson
Hans Roth

ciscopress.com

CCNP ISCW Portable Command Guide

Scott Empson, Hans Roth

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

Printed in the United States of America

First Printing March 2008

Library of Congress Cataloging-in-Publication Data

Empson, Scott.
CCNP ISCW portable command guide / Scott Empson, Hans Roth.
p. cm.
ISBN 978-1-58720-186-8 (pbk.)
1. Computer networks--Problems, exercises, etc. 2. Computer networks--Examinations--Study guides. 3. Packet switching (Data transmission)--Examinations--Study guides. I. Roth, Hans. II. Title.

TK5105.8.C57E57 2008
004.6--dc22

2008004857

ISBN-13: 978-1-58720-186-8
ISBN-10: 1-58720-186-0

This Book Is Safari Enabled

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

- Go to http://www.informit.com/onlineedition.
- Complete the brief registration form
- Enter the coupon code STFG-Q1KG-224L-GNGP-JWE9

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

Introduction

Welcome to ISCW! In 2006, Cisco Press contacted Scott and told him, albeit very quietly, that there was going to be a major revision of the CCNP certification exams. They then asked whether he would be interested in working on a command guide in the same fashion as his previous books for Cisco Press: the Cisco Networking Academy Program *CCNA Command Quick Reference* and the *CCNA Portable Command Guide*. The original idea was to create a single-volume command summary for all four of the new CCNP exams. However, early on in his research, Scott quickly discovered that there was far too much information in the four exams to create a single volume—that would have resulted in a book that was neither portable nor quick as a reference. So, Scott jokingly suggested that Cisco Press let him author four books, one for each exam. Well, you have to be careful what you wish for, because Cisco Press readily agreed. Realizing that this was going to be too much for one part-time author to handle, Scott quickly got his colleague Hans Roth on board as a coauthor.

This book is the third in a four-volume set that attempts to summarize the commands and concepts that you need to understand to pass one of the CCNP certification exams—in this case, the Implementing Secure Converged WANs exam. It follows the format of Scott's previous books, which are in fact a cleaned-up version of his own personal engineering journal—a small notebook that you can carry around that contains little nuggets of information such as commands that you tend to forget, the IP addressing scheme of some remote part of the network, and little reminders about how to do something you need to do only once or twice a year that is vital to the integrity and maintenance of your network.

With the creation of two brand-new CCNP exams, the amount of new information out there is growing on an almost daily basis. There is always a new white paper to read, a new Webinar to view, another slideshow from a Networkers session that was never attended. The engineering journal can be that central repository of information that won't weigh you down as you carry it from the office or cubicle to the server and infrastructure room in some branch office.

To make this guide a more realistic one for you to use, the folks at Cisco Press have decided to continue with an appendix of blank pages—pages on which you can write your own personal notes, such as your own configurations, commands that are not in this book but are needed in your world, and so on. That way this book will look less like the authors' journals and more like your own.

Networking Devices Used in the Preparation of This Book

To verify the commands in this book, many different devices were used. The following is a list of the equipment used in the writing of this book:

- C2620 router running Cisco IOS Release 12.3(7)T, with a fixed Fast Ethernet interface, a WIC-2A/S serial interface card, and an NM-1E Ethernet interface
- C2811 ISR bundle with PVDM2, CMME, a WIC-2T, FXS and FXO VICs, running Cisco IOS Release 12.4(3g)
- C2821 ISR bundle with HWICD 9ESW, a WIC-2A/S, running 12.4(16) Advanced Security IOS
- WS-C3560-24-EMI Catalyst switch, running Cisco IOS Release 12.2(25)SE
- WS-C3550-24-EMI Catalyst switch, running Cisco IOS Release 12.1(9)EA1c
- WS-C2960-24TT-L Catalyst switch, running Cisco IOS Release 12.2(25)SE
- WS-C2950-12 Catalyst switch, running version C2950-C3.0(5.3)WC(1) Enterprise Edition software
- C1760 1FE VE 4SLOT DV Mainboard Port adapter with PVDM2, CMME, WIC-2A/S, WIC-4ESW, MOD1700-VPN with 32F/128D running c1700-bk9no3r2sy7-mz.124-15.T1

- C1751 1FE VE DV Mainboard with WIC-4ESW, MOD1700-VPN with 16F/64D running c1700-advsecurityk9-mz.124-5a
- Cisco 3640 with 32F/128DRAM memory, 3 Ethernet interfaces, 2-WIC-1T running c3640-jk9o3s-mz.124-12a

These devices were not running the latest and greatest versions of Cisco IOS Software. Some of the equipment is quite old.

Those of you familiar with Cisco devices will recognize that a majority of these commands work across the entire range of the Cisco product line. These commands are not limited to the platforms and IOS versions listed. In fact, in most cases, these devices are adequate for someone to continue their studies beyond the CCNP level.

Who Should Read This Book

This book is for those people preparing for the CCNP ISCW exam, whether through self-study, on-the-job training and practice, study within the Cisco Networking Academy, 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. This book 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

This book follows the list of objectives for the CCNP ISCW exam:

- **Chapter 1, "Network Design Requirements"**—Offers an overview of the two different design models from Cisco: the Service-Oriented Network Architecture and the Enterprise Composite Network Model
- **Chapter 2, "Connecting Teleworkers"**—Describes how to provision a cable modem, and how to configure a Cisco router as a PPPoE client
- **Chapter 3, "Implementing Frame Mode MPLS"**—Describes how to configure MPLS on a router, including configuring CEF, configuring MPLS on a frame mode interface, and configuring MTU size in label switching
- **Chapter 4, "IPsec VLANs"**—Describes how to configure, verify, and troubleshoot IPsec VLANs, including topics such as configuring IPsec, configuring GRE tunnels, creating High Availability using HSRP and stateful failover, Cisco Easy VPN Server and client, and configuring Easy VPN Server using Cisco SDM
- **Chapter 5, "Cisco Device Hardening"**—Includes topics such as locking down routers with AutoSecure; setting login failure rates, timeouts, and multiple privilege levels; Role-Based CLI; securing your configuration files; and configuring SSH servers, syslog logging, NTP clients and servers, and AAA
- **Chapter 6, "Cisco IOS Threat Defense Features"**—Includes topics such as configuring a basic firewall from the CLI and SDM, configuring a DMZ, and configuring inspection rules as part of an Advanced Firewall

Did We Miss Anything?

As educators, we are always interested to hear how our students, and now readers of our books, do on both vendor exams and future studies. If you would like to contact either of us and let us know how this book helped you in your certification goals, please do so. Did we miss anything? Let us know. Contact us at ccnpguide@empson.ca.

CHAPTER 3

Implementing Frame Mode MPLS

This chapter provides information and commands concerning the following topics:

- Configuring Cisco Express Forwarding
  - — Verifying CEF
  - — Troubleshooting CEF
- Configuring MPLS on a Frame Mode interface
- Configuring MTU size in label switching

Configuring Cisco Express Forwarding

To enable MPLS, you must first enable Cisco Express Forwarding (CEF) switching.

NOTE: CEF switching is enabled by default on the following platforms:

- Cisco 7100 series router
- Cisco 7200 series router
- Cisco 7500 series Internet router

dCEF Switching is enabled by default on the following platforms:

- Cisco 6500 series router
- Cisco 12000 series Internet router

`Router(config)#ip cef`	Enables standard CEF
`Router(config)#ip cef distributed`	Enables dCEF
`Router(config)#no ip cef`	Disables CEF globally
`Router(config)#interface fastethernet 0/1`	Moves to interface configuration mode
`Router(config-if)#ip route-cache cef`	Enables CEF on the interface

Verifying CEF

`Router#show ip cef`	Displays entries in the forwarding information base (FIB)
`Router#show ip cef summary`	Displays a summary of the FIB
`Router#show ip cef unresolved`	Displays unresolved FIB entries
`Router#show ip cef fastethernet 0/1`	Displays the FIB entry for the specified interface
`Router#show ip cef fastethernet 0/1 detail`	Displays detailed information about the FIB for the interface
`Router#show cef drop`	Displays packets that are dropped due to adjacencies that are incomplete or nonexistent

NOTE: CEF is not supported on logical interfaces, such as loopback interfaces.

Troubleshooting CEF

`Router#debug ip cef`	Displays debug information for CEF
`Router#debug ip cef drop`	Displays debug information about dropped packets
`Router#debug ip cef access-list x`	Displays information from specified access lists
`Router#debug ip cef receive`	Displays information about packets received by IP CEF

`Router#debug ip cef events`	Displays general CEF events
`Router#debug ip cef prefix-ipc`	Displays updates related to IP prefix information
`Router#debug ip cef table`	Produces a table showing events related to the FIB table

Configuring MPLS on a Frame Mode Interface

`Router(config)#mpls ip`	Enables MPLS globally on the router **NOTE:** MPLS is enabled by default on Cisco routers. However, if you need to re-enable it, use the global **mpls ip** command.
`Router(config)#interface fastethernet 0/0`	Moves to interface configuration mode
`Router(config-if)#mpls ip`	Enables MPLS on the specified interface
`Router(config-if)#mpls label protocol tdp`	Enables Tag Distribution Protocol (TDP) on this interface **NOTE:** TDP is Cisco proprietary. LDP is a superset of TDP. Cisco is changing from TDP to a fully compliant LDP.

`Router(config-if)#mpls label protocol ldp`	Enables Label Distribution Protocol (LDP) on this interface **NOTE:** LDP is the default protocol on Cisco IOS Release 12.4(3) and later. In older releases, TDP was the default protocol.
`Router(config-if)#mpls label protocol both`	Enables both TDP and LDP on this interface

NOTE: For backward compatibility, the **mpls** syntax will be entered as **tag-switching** syntax in the configuration by the Cisco IOS Software.

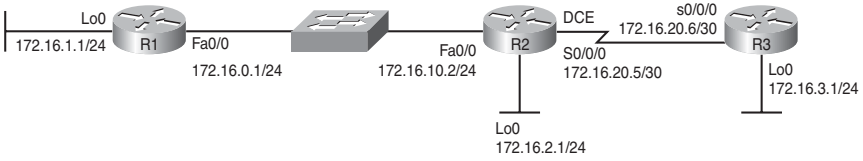
Configuring MTU Size in Label Switching

`Router(config)#interface fasthethernet 0/0`	Moves to interface configuration mode
`Router(config-if)#mpls mtu 1512`	Changes the maximum size of an MPLS-labeled packet to 1512 bytes **NOTE:** The **mpls mtu** command is an optional command when working with MPLS. But because of the addition of the label header, the MTU on LAN interfaces should be increased to prevent IP fragmentation. **NOTE:** The minimum MTU is 64 bytes. The maximum MTU depends on the type of interface medium that is being used.

Configuration Example: Configuring Frame Mode MPLS

Figure 3-1 shows the network topology for the configuration that follows, which shows how to configure Frame Mode MPLS using commands covered in this chapter.

Figure 3-1 Network Topology for Frame Mode MPLS Configuration Example



R1 Router

`Router>enable`	Moves to privileged mode
`Router#configure terminal`	Moves to global configuration mode
`Router(config)#hostname R1`	Assigns hostname to router
`R1(config)#ip cef`	Enables CEF on device (enabled by default)
`R1(config)#mpls ip`	Enables MPLS globally on device (enabled by default)
`R1(config)#interface loopback 0`	Moves to interface configuration mode
`R1(config-if)#ip address 172.16.1.1 255.255.255.0`	Assigns IP address and netmask
`R1(config-if)#interface fastethernet 0/0`	Moves to interface configuration mode
`R1(config-if)#ip address 172.16.10.1 255.255.255.0`	Assigns IP address and netmask
`R1(config-if)#mpls ip`	Enables MPLS on this interface

`R1(config-if)#mpls mtu 1508`	Changes the maximum size of the packet allowed on this interface to 1508 bytes
`R1(config-if)#no shutdown`	Activates interface
`R1(config-if)#exit`	Returns to global configuration mode
`R1(config)#router eigrp 1`	Enables the EIGRP routing process for AS 1
`R1(config-router)#network 172.16.0.0`	Specifies which network to advertise in EIGRP
`R1(config-router)#no auto-summary`	Turns off the auto-summarization feature
`R1(config-router)#exit`	Returns to global configuration mode
`R1(config)#exit`	Returns to privileged mode
`R1#copy running-config startup-config`	Saves configuration in NVRAM

R2 Router

`Router>enable`	Moves to privileged mode
`Router#configure terminal`	Moves to global configuration mode
`Router(config)#hostname R2`	Assigns hostname to router
`R2(config)#ip cef`	Enables CEF on device (enabled by default)
`R2(config)#mpls ip`	Enables MPLS globally on device (enabled by default)
`R2(config)#interface loopback 0`	Moves to interface configuration mode

`R2(config-if)#ip address 172.16.2.1 255.255.255.0`	Assigns IP address and netmask
`R2(config-if)#interface fastethernet 0/0`	Moves to interface configuration mode
`R2(config-if)#ip address 172.16.10.2 255.255.255.0`	Assigns IP address and netmask
`R2(config-if)#mpls ip`	Enables MPLS on this interface
`R2(config-if)#mpls mtu 1508`	Changes the maximum size of the packet allowed on this interface to 1508 bytes
`R2(config-if)#no shutdown`	Activates interface
`R2(config-if)#interface serial 0/0/0`	Moves to interface configuration mode
`R2(config-if)#ip address 172.16.20.5 255.255.255.252`	Assigns IP address and netmask
`R2(config-if)#mpls ip`	Enables MPLS on this interface
`R2(config-if)#clock rate 64000`	Enables clock rate for this interface
`R2(config-if)#no shutdown`	Activates interface
`R2(config-if)#exit`	Returns to global configuration mode
`R2(config)#router eigrp 1`	Enables the EIGRP routing process for AS 1
`R2(config-router)#network 172.16.0.0`	Specifies which network to advertise in EIGRP
`R2(config-router)#no auto-summary`	Turns off the auto-summarization feature
`R2(config-router)#exit`	Returns to global configuration mode

`R2(config)#exit`	Returns to privileged mode
`R2#copy running-config startup-config`	Saves configuration in NVRAM

R3 Router

`Router>enable`	Moves to privileged mode
`Router#configure terminal`	Moves to global configuration mode
`Router(config)#hostname R3`	Assigns hostname to router
`R3(config)#ip cef`	Enables CEF on device (enabled by default)
`R3(config)#mpls ip`	Enables MPLS globally on device (enabled by default)
`R3(config)#interface loopback 0`	Moves to interface configuration mode
`R3(config-if)#ip address 172.16.3.1 255.255.255.0`	Assigns IP address and netmask
`R3(config-if)#interface serial 0/0/0`	Moves to interface configuration mode
`R3(config-if)#ip address 172.16.20.6 255.255.255.252`	Assigns IP address and netmask
`R3(config-if)#mpls ip`	Enables MPLS on this interface
`R3(config-if)#no shutdown`	Activates interface
`R3(config-if)#exit`	Returns to global configuration mode
`R3(config)#router eigrp 1`	Enables the EIGRP routing process for AS 1
`R3(config-router)#network 172.16.0.0`	Specifies which network to advertise in EIGRP

`R3(config-router)#no auto-summary`	Turns off the auto-summarization feature
`R3(config-router)#exit`	Returns to global configuration mode
`R3(config)#exit`	Returns to privileged mode
`R3#copy running-config startup-config`	Saves configuration in NVRAM