



AAA Identity Management Security

Vivek Santuka Premdeep Banga Brandon J. Carroll

ciscopress.com

AAA Identity Management Security

Vivek Santuka, Premdeep Banga, Brandon J. Carroll

Copyright © 2011 Cisco Systems, Inc.

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

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing November 2010

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58714-144-7

ISBN-10: 1-58714-144-2

Warning and Disclaimer

This book is designed to provide information about AAA Identity Management Security. 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.

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.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: International Sales international@pearsoned.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.

Publisher: Paul Boger	Cisco Representative: Erik Ullanderson
Associate Publisher: Dave Dusthimer	Cisco Press Program Manager: Anand Sundaram
Executive Editor: Brett Bartow	Senior Development Editor: Christopher Cleveland
Managing Editor: Sandra Schroeder	Technical Editors: Rohit Chopra, JesseDubois, Chris Murray
Project Editor: Seth Kerney	Proofreader: Leslie Joseph
Editorial Assistant: Vanessa Evans	Copy Editor: Mike Henry
Book and Cover Designer: Louisa Adair	Indexer: Tim Wright
Composition: Mark Shirar	



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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Stadium/Vision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registra, Aironat, AsyncOS, Bringing the Weberling To You, Catalysti, CCDA, CCDP, CCIE, CCIP, CCNA, CCAPP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork: ExpertIqued Cisco Store are service marks; and Access Registra, Aironat, AsyncOS, Bringing the Weberling To You, Catalysti, CCDA, CCDP, CCIE, CCIP, CCNA, CCAPP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork: ExpertIqued Cisco Cisco Stade, Catalysti, CCDA, Cole, CCIP, CCIP, CCNA, CCAPP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork: ExpertIqued Cisco Cisco Stade, Cisco Stade, Cisco Stade, Cisco Mexico, Stady Stade, Cisco Charle, Colexo, Cisco, The Cisco Certified Internetwork: ExpertIqued Cisco, Cisco Cisco, Stade, Cisco Cisco, Cisco Mexico, Stady, ConPort, the ton-Port logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace, Chine Sound, MGX, Networkers, Networking Academy, Network: Registrat, FONow PK, PowerPanel, ProConnect, ScriptShare, SoneGaleta, Bcisco Cisco, Markine, TanaPath, WebEx, and the WebEx logo are registered tadamistic of Cisco Systems. Inc. And/or is difficult in the Contifient Countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Contents at a Glance

Introduction xxii

- Chapter 1 Authentication, Authorization, Accounting (AAA) 1
- Chapter 2 Cisco Secure ACS 21
- Chapter 3 Getting Familiar with ACS 4.2 57
- Chapter 4 Getting Familiar with ACS 5.1 85
- Chapter 5 Configuring External Databases (Identity Stores) with ACS 123
- Chapter 6 Administrative AAA on IOS 151
- Chapter 7 Administrative AAA on ASA/PIX 179
- Chapter 8 IOS Switches 195
- Chapter 9 Access Points 253
- Chapter 10 Cut-Through Proxy AAA on PIX/ASA 281
- Chapter 11 Router 309
- Chapter 12 AAA of VPN and PPP Sessions on IOS 331
- Chapter 13 AAA of VPN on ASA 353
- Chapter 14 ACS 4.2 Advanced Configuration 371
- Chapter 15 ACS 5.1 401

Index 433

Contents

Introduction xxii

Chapter 1 Authentication, Authorization, Accounting (AAA) 1 Authentication Overview 2 Authentication Example 4 Authorization Overview 4 Authorization Example 5 Accounting Overview 6 Accounting Example 7 Overview of RADIUS 8 RADIUS in Detail 9 RADIUS Operation 10 RADIUS Encryption 11 RADIUS Authentication and Authorization 11 RADIUS Accounting 12 Overview of TACACS+ 13 TACACS+ in Detail 13 TACACS+ Communication 14 TACACS+ Format and Header Values 14 15 Encrypting TACACS+ TACACS+ Operation 16 TACACS+ and Authentication 17 TACACS+ and Authorization 18 TACACS+ Accounting 19 Summary 20 Chapter 2 **Cisco Secure ACS** 21 Introduction to ACS 21 Overview 22 AAA Client-Server Framework 22 Cisco Secure Access Control Server Release 4.2 Characteristics and Features 23 Policy Model 23 Platform 24 Protocol Compliance 25 Features Available 26

Cisco Secure Access Control System Release 5.1 Characteristics and Features 28 Policy Model 28 Platform 29 Protocol Compliance 29 Functions and Features 31 Installing Cisco Secure Access Control Server 4.2 32 Installing Cisco Secure Access Control Server for Windows 4.2 32 Installing Cisco Secure Access Control Server Solution Engine 38 Initial Setup of Cisco Secure Access Control System 5.1 47 Cisco Secure Access Control System Appliance 5.1 48 Installing Cisco Secure Access Control System 5.1 49 Installing Cisco Secure Access Control System 5.1 on VMware 50 Licensing Model of Cisco Secure Access Control System 5.1 51 Type of License 51 Base License 51 Add-on License 52 Evaluation License 52 Not-For-Resale (NFR) License 52 Common Problems After Installation 52 ACS Solution Engine Does Not Respond to Pings 52 No Proper Cisco Secure Access Control Server GUI Access 53 Remote Administration Access to Cisco Secure Access Control Server 53 ACS Folder Is Locked During Upgrade or Uninstall 54 TACACS+/RADIUS Attributes Do Not Appear Under User/Group Setup 54 Key Mismatch Error 54 ACS Services Not Starting 55 ACS 5.1 Install Failing on VMWare 55 Summary 55 Chapter 3 Getting Familiar with ACS 4.2 57 The Seven Services of ACS 58 CSAdmin 59 CSAuth 59 CSDBSync 59 CSLog 60

CSMon 60 CSRadius 60 CSTacacs 60 The Grand Tour of the ACS Interface 61 Administration Control 61 Securing Access to ACS 62 Network Configuration 64 Network Access Profiles 65 Interface Configuration 66 TACACS+ Settings 68 Advanced Options 69 User Setup: Managing Users 70 Customizing User Attributes 72 Group Setup: Managing User Groups 74 System Configuration 76 Shared Profile Components 78 External User Databases 78 Reports and Activity 79 Summary 83 **Getting Familiar with ACS 5.1** 85 My Workspace 86 Welcome Page 86 Task Guide 87 My Account 87 Network Resources 87 Network Device Groups 88 Network Devices and AAA Clients 90 Default Network Device 92 External RADIUS Servers 93 Users and Identity Stores 94 Identity Groups 95 Adding a User in the Internal Identity Store 96 Adding a Host in the Internal Identity Store 97 Policy Elements 98 Session Conditions: Date and Time 101 Session Conditions: Custom 102 Session Conditions: End Station Filters 103

Chapter 4

Session Conditions: Device Filters 104 Session Conditions: Device Port Filters 105 Access Policies 105 Service Selection Rules 106 Access Services 107 Creating an Access Service 107 Configuring Identity Policy 110 Configuring Authorization Policy 113 Creating Service Selection Rules 115 Monitoring and Reports 117 ACS 5.1 Command-Line Interface (CLI) 120 Summary 122 Chapter 5 **Configuring External Databases (Identity Stores) with ACS** External Databases/Identity Stores 123 External Databases/Identity Stores in Cisco Secure Access Control Server 4.2 123 External Databases/Identity Stores in Cisco Secure Access Control System 5.1 126 Configuring Active Directory 128 Active Directory Configuration on Cisco Secure Access Control Server 4.2 128 Active Directory Configuration on Cisco Secure Access Control System 5.1 132 Configuring LDAP 134 LDAP Configuration on Cisco Secure Access Control Server 4.2 134 Domain Filtering 134 Common LDAP Configuration 134 Primary and Secondary LDAP Server 135 LDAP Configuration on Cisco Secure Access Control System 5.1 137 Configuring RSA SecureID 139 RSA SecureID Configuration on Cisco Secure Access Control Server 4.2 140 RSA SecureID Configuration on Cisco Secure

123

- Access Control System 5.1 140
- Group Mapping 141
 - Group Mapping on Cisco Secure Access Control Server 4.2 141
 - Group Mapping on Cisco Secure Access Control System 5.1 142

Group Mapping with LDAP Identity Stores 143
Group Mapping with AD Identity Stores 144
Group Mapping with RADIUS Identity Stores 145
Group Mapping Conditions for LDAP, AD, and RADIUS Identity Databases 146
Summary 149

Chapter 6 Administrative AAA on IOS 151

Local Database 151

Privilege Levels 152

Lab Scenario #1: Local Authentication and Privilege Levels 154

Lab Setup 154

Lab Solution 154

Lab Verification 155

Using AAA 155

Configuring Authentication on IOS Using AAA 157 Configuring ACS 4.2 and 5.1 for Authentication 159 Verifying and Troubleshooting Authentication 159 Authorization of Administrative Sessions 161 Configuring ACS 4.2 and 5.1 for EXEC Authorization 162 Verifying and Troubleshooting EXEC Authorization 166 Command Authorization 166 Configuring ACS 4.2 and 5.1 for Command Authorization 168 Verifying and Troubleshooting Command Authorization 172 Accounting of Administrative Sessions 173 Configuring ACS for Accounting 174 Lab Scenario #2: Authentication, Authorization, and Accounting of Administrative Sessions Using TACACS+ 174 Lab Setup 174 Lab Solution 175 Lab Verification 175 Lab Scenario #3: Authentication and Authorization of HTTP Sessions 176 Lab Setup 176 Lab Solution 176 Lab Verification 177 Summary 177

Chapter 7	Administrative AAA on ASA/PIX 179							
	Local Database 180							
	Privilege Levels 180							
	Lab Scenario #4: Local Authentication and Privilege Levels on ASA 183							
	Lab Setup 183							
	Lab Solution 183							
	Lab Verification 184							
	Using AAA 184							
	Configuring Authentication on ASA Using AAA 186							
	Configuring ACS 4.2 and 5.1 for Authentication 186							
	Verifying and Troubleshooting Authentication 187							
	Authorization of Administrative Sessions 188							
	Configuring ACS 4.2 and 5.1 for EXEC Authorization 188							
	Verifying and Troubleshooting EXEC Authorization 189							
	Command Authorization 189							
	Accounting of Administrative Sessions and Commands 191							
	Lab Scenario #5: Authentication, Authorization and Accounting of Administrative Sessions on ASA using TACACS+ 192							
	Lab Setup 193							
	Lab Solution 193							
	Lab Verification 194							
	Summary 194							
Chapter 8	IOS Switches 195							
	Introduction to 802.1X, EAP, and EAPOL 195							
	EAP 197							
	EAPOL 199							
	Message Exchange in 802.1X 200							
	EAP Types 201							
	PEAPv0/EAP-MSCHAPv2 203							
	PEAPv1/EAP-GTC 203							
	EAP Authentication Type Summary 204							
	802.1X Configuration on a Cisco Switch 204							
	802.1X Host Modes 206							
	Single-Host Mode 206							
	Multiple-Host Mode 207							
	Multidomain Authentication Mode 207							

Pre-Authentication Open Access 208 Multiauthentication Mode 208 802.1X Authentication Features 208 Guest VLAN 209 Restricted/Authentication Failed VLAN 209 MAC Authentication Bypass 210 VLAN Assignment 211 802.1X Timers 212 Quiet Period 212 Switch-to-Client Retransmission Time (tx-period) 213 Switch-to-Client Retransmission Time for EAP-Request Frames (supp-timeout) 213 Switch-to-Authentication-Server Retransmission Time for Layer 4 Packets (server-timeout) 213 Switch-to-Client Frame Retransmission Number (max-reauth-reg) 213 Configuring Accounting 214 Certificate Installation on ACS 214 Certificate Installation on ACS 4.2 215 Certificate Installation on ACS 5.1 219 Configuring EAP-MD5 on ACS 222 EAP-MD5 Configuration on ACS 4.2 2.2.3 EAP-MD5 Configuration on ACS 5.1 223 Configuring PEAP on ACS 224 PEAP Configuration on ACS 4.2 225 PEAP Configuration on ACS 5.1 225 Configuring EAP-TLS on ACS 226 EAP-TLS Configuration on ACS 4.2 226 EAP-TLS Configuration on ACS 5.1 226 Dynamic VLAN Assignment: ACS Configuration 228 Dynamic VLAN Assignment for ACS 4.2 228 Dynamic VLAN Assignment for ACS 5.1 229 Lab Scenario #7: Configuring Switch, ACS, and Windows XP for 802.1X Authentication Using EAP-MD5 230 Lab Setup 231 Lab Solution 231 ACS 4.2 Configuration Requirement 232 ACS 5.1 Configuration Requirement 233

	Switch Configuration Requirements 237				
	Client Configuration Requirements 238				
	Lab Scenario #8: Configuring Switch, ACS, and Windows XP for 802.1X Authentication Using PEAP 245				
	Lab Solution 245				
	Lab Scenario #9: Configuring Switch, ACS, and Windows XP for 802.1X Authentication Using EAP-TLS 249				
	Lab Solution 249				
	Useful show Commands 249				
	Troubleshooting 802.1X 250				
	Summary 251				
Chapter 9	Access Points 253				
	Configuring Wireless NAS for 802.1X Authentication on an AP 253				
	Configuring Wireless NAS for 802.1X Authentication on a WLC 259				
	Configuring ACS 4.2 for LEAP 263				
	Configuring ACS 5.1 for LEAP 264				
	Configuring ACS 4.2 for EAP-FAST 265				
	Configuring ACS 5.1 for EAP-FAST 266				
	Lab Scenario #10: Configure WLC, ACS and Cisco SecureServices Client for 802.1X Authentication Using LEAP269				
	Lab Setup 269				
	Lab Solution 270				
	ACS 4.2 Configuration Requirements 270				
	ACS 5.1 Configuration Requirements 271				
	WLC Configuration Requirements 273				
	Client Configuration Requirements 273				
	Lab Scenario #11: Configure WLC, ACS, and Cisco SecureServices Client for 802.1X Authentication Using EAP-FAST273				
	Lab Solution 273				
	ACS 4.2 Configuration Requirements 274				
	ACS 5.1 Configuration Requirements 274				
	Client Configuration Requirements 274				
	Troubleshooting 802.1X 275				
	Summary 279				
Chapter 10	Cut-Through Proxy AAA on PIX/ASA 281				

Cut-Through Proxy Authentication 282 Virtual Telnet, Virtual HTTP, and HTTP Redirection 285

Virtual Telnet 286 Virtual HTTP 287 HTTP Redirection 288 uauth Timer 290 Configuring ACS for Cut-Through Proxy Authentication 290 Verifying and Troubleshooting Cut-Through Proxy Authentication 291 Lab Scenario #12: Authenticating Cut-Through Traffic on ASA 292 Lab Setup 292 Lab Verification 293 Lab Solution 293 Cut-Through Proxy Authorization 294 Configuring ACS 4.2 and 5.1 for Cut-Through Proxy Authorization Using TACACS+ 295 Configuring ACS 4.2 for Cut-Through Proxy Authorization Using RADIUS 297 Configuring ACS 5.1 for Cut-Through Proxy Authorization Using RADIUS 299 Verifying and Troubleshooting Cut-Through Proxy Authorization 302 Cut-Through Proxy Accounting 303 Lab Scenario #13: Cut-Through Proxy Authentication, Authorization, and Accounting 304 Lab Setup 305 Lab Solution 305 Lab Verification 306 Summary 308 Router 309 Prerequisites for Authentication Proxy 310 Authenticating HTTP Sessions 311 Authenticating FTP Sessions 312 Authenticating Telnet Sessions 314 Configuring ACS for Authentication Proxy 315 Viewing and Maintaining Authentication Proxy Cache 315 Verifying and Troubleshooting Authentication Proxy 316 Authentication Proxy Authorization 317 Configuring ACS 4.2 for Authorization Using TACACS+ 318 Configuring ACS 5.1 for Authorization Using TACACS+ 319 Configuring ACS 4.2 for Authorization Using RADIUS 322

Chapter 11

Configuring ACS 5.1 for Authorization Using RADIUS 323 Verifying and Troubleshooting Authentication Proxy Authorization 325 Authentication Proxy Accounting 326 Lab Scenario #14: Authentication Proxy 326 Lab Setup 327 Lab Solution 327 Lab Verification 328 Summary 329 Chapter 12 AAA of VPN and PPP Sessions on IOS 331 Authenticating VPN Sessions 331 Authenticating IPsec Remote Access Sessions 331 Authenticating SSL VPN Sessions 335 Configuring ACS 4.2 and 5.1 for IPsec and SSL VPN Authentication 336 Verifying and Troubleshooting VPN Authentication 337 Authorizing VPN Sessions 337 Authorizing IPsec Remote Access Sessions 338 Configuring ACS 4.2 and ACS 5.1 for IPsec Remote Access Authorization 339 Authorizing SSL VPN Sessions 341 Configuring ACS 4.2 and ACS 5.1 for SSL VPN Authorization 342 Verifying and Troubleshooting VPN Authorization 342 Accounting for IPsec Remote Access and SSL VPN 343 Lab Scenario #15: VPN AAA 343 Lab Setup 344 Lab Solution 345 Lab Verification 345 Authenticating PPP Sessions 345 Configuring ACS for PPP Authentication 347 Verifying and Troubleshooting PPP Authentication 347 Authorizing PPP Sessions 348 Configuring ACS 4.2 and 5.1 for PPP Authorization 348 Verifying and Troubleshooting PPP Authorization 349 Accounting for PPP Sessions 350 Summary 351

Chapter 13 AAA of VPN on ASA 353

Authenticating Remote Access IPsec VPN (EzVPN Remote) and SSL VPN Using RADIUS 353 Configuring ACS for IPsec Remote Access and SSL VPN Authentication 355 Verifying and Troubleshooting VPN RADIUS Authentication 355 Authorizing IPsec Remote Access and SSL VPN Using RADIUS 356 Configuring ACS 4.2 and 5.1 for IPsec and SSL VPN Authorization 357 Verifying and Troubleshooting VPN Authorization 358 Accounting for IPsec and SSL VPN Using RADIUS 359 Lab Scenario # 16: VPN AAA Using RADIUS 359 Lab Setup 359 Lab Solution 361 Lab Verification 361 Authenticating IPsec and SSL VPN Using LDAP 362 Verifying and Troubleshooting VPN Authentication Using LDAP 363 Authorizing IPsec and SSL VPN Using LDAP 364 Verifying and Troubleshooting VPN Authorization with LDAP 366 Lab Scenario # 17: VPN Authentication and Authorization Using LDAP 367 Lab Setup 367 Lab Solution 368 Lab Verification 369 Summary 369 Chapter 14 **ACS 4.2 Advanced Configuration** 371 Network Access Restrictions 371 Backup and Restore 376 Manual Backups 377 Scheduled Backups 378 Recovering ACS from a Backup file 378 Database Replication 378 Understanding Database Replication 378 Replication Versus Backup 381 Configuring the Primary Server for Replication 381 Configuring a Secondary Server 383

RDBMS Synchronization 384 accountActions Format 385 Performing RDBMS Synchronization 387 Network Access Profiles 388 Classification of Network Request 389 Policies 389 Local Password Management 391 Remote Logging 391 Log File Management 394 CSUtil Database Utility 395 Summary 400

Chapter 15 ACS 5.1 401

Replication 401

Activating Secondary Servers 402

Dictionaries 405
Remote Logging 409

Defining a Remote Log Target 410
Specifying a Remote Log Target Under a Logging Category 411

Importing Network Resources and Users 412
Managing System Administrators 415
Backup and Restore 421

Software Repositories 422
Backing Up a Database 425

Scheduled Backups 427

Restoring Databases 429
Summary 431

Index 433

Icons Used in This Book

: 6 **Cisco Directory** Router Secure S Cerver Network Cisco ACS Access Device 000000 Wireless AAA Server LWAPP Wireless LAN Access Point Access Point Controller AGA Cerver Web Server Authentication Server Printer ∞ Relational Wireless PC Database Connection Laptop

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

This book is focused on providing the skills necessary to successfully configure authentication, authorization, and accounting (AAA) services on Cisco devices using Cisco Secure Access Control Server/System 4.2 and 5.1. This book was motivated by a desire to provide a one-stop resource for AAA solutions on Cisco devices.

Goals and Methods

The goals of this book are as follows:

- Provide an overview of the AAA architecture
- Provide detailed discussion on the TACACS+ and RADIUS protocols
- Provide detailed discussion on AAA for most common scenarios of network access
- Provide an in depth configuration and troubleshooting overview of AAA on Cisco devices
- Provide an in-depth overview of ACS 4.2 and 5.1 features and configuration to match with configuration on Cisco devices

This book discusses different means to control the access to various network resources. This is followed by configuration and troubleshooting on Cisco devices and ACS. In the end, you are given a lab scenario to reinforce the learning.

Who Should Read This Book?

This book is targeted toward the following people:

- Network security professionals tasked with the implementation and management of access control and identity management using Cisco devices and/or Cisco ACS.
- Those who are pursuing different Cisco certifications requiring knowledge of AAA, such as CCSP and CCIE.

How This Book Is Organized

This book is separated into the following six logical parts.

- Part I, "AAA and CiscoSecure ACS"—This part is designed to introduce AAA and ACS. Chapters 1 and 2 provide an overview of AAA and ACS. Chapters 3 and 4 provide an in-depth understanding of ACS 4.2 and ACS 5.1. Chapter 5 builds on the previous two chapters and dicusses various user databases which can be configured with ACS.
- Part II, "Administrative AAA"—This part is designed to discuss AAA for administrative sessions on Cisco IOS and Cisco PIX/ASA. This part is also the foundation of establishing and troubleshooting connectivity between devices and ACS. It contains two chapters and five lab scenarios.
- Part III, "802.1x"—This part is designed to discuss the IEEE 802.1x protcol and its implementation on Cisco Catalyst Switches and Cisco Access Points. In this part you will learn about different EAP types, their advantages and disadvantages, and how to configure Cisco devices, ACS, and clients running Windows XP. This part contains two chapters and five lab scenarios.
- Part IV, "Pass-Through Traffic"—This part discusses access control on traffic passing through a device running Cisco IOS and through Cisco ASA/PIX. This part contains two chapters and three lab scenarios.
- Part V, "Remote Access"—This part discusses access control on Remote Access sessions such as VPN and PPP on Cisco IOS and Cisco PIX/ASA. This part contains two chapters and three lab scenarios.
- Part VI, "ACS Advanced Configuration"—The final part of the book looks at advanced topics of ACS management such as backup, restore, remote logging, and replication. This part contains two chapters.

This page intentionally left blank

Chapter 4

Getting Familiar with ACS 5.1

This chapter covers the following subjects:

- Navigating the ACS 5.1 Graphical User Interface
- Adding Network Groups and Devices
- Adding Users to Internal Repositories
- Policy Elements and Access Services
- Monitoring and Reports
- Using the ACS Command-Line Interface

ACS 5.1 has a completely different user interface from ACS 4.2. Throughout the course of this chapter you will become familiar with the GUI and know where different functions are located. If this is your first time using ACS 5.1, it is important to take the time to learn how to navigate the interface.

The GUI is broken into two frames. You access different menu items on the left side frame (Navigation Pane) and perform configuration in the right side frame (Content Area). The Monitoring and Reports section is the only exception to this. After you launch the Monitoring and Reports Viewer, a new browser window opens. This new window has a layout similar to the original window but contains menu items related to monitoring and reporting. The left side menu is divided further into drop-down menus or drawers. Click on a drawer to expand it and see a list of options. The available drawers are as follows:

- My Workspace
- Network Resources
- Users and Identity Stores
- Policy Elements
- Access Policies

- Monitoring and Reports
- System Administration

My Workspace

The My Workspace drawer contains:

- Welcome Page
- Task Guide
- My Account

Welcome Page

The Welcome Page appears when you log in to ACS and provides links to information and shortcuts to some common tasks. Figure 4-1 shows the Welcome Page.



Figure 4-1 Welcome Page

Clicking on the links below the Getting Started section on the Welcome Page creates a new frame in the Content Area. This new frame provides help on how to get started with ACS and contains shortcuts to the initial tasks.

Clicking on any other link in the Welcome Page will open a new window containing the help section. ACS 5.1 has a comprehensive help section and can be accessed using the **Help** link in the top-right corner of the ACS GUI.

Task Guide

The Task Guide has three menu items:

- Quick Start
- Initial System Setup
- Policy Setup Steps

These items are shortcuts for the links under the Getting Started section on the Welcome Page.

My Account

My Account provides general information regarding the ACS GUI account and assigned roles, and enables you to change the password of your ACS administrator account. No other changes to the account can be made from this section. See Chapter 15, "ACS 5.1 Advanced Configuration," for information on editing and adding GUI administrator accounts. Figure 4-2 shows the My Account pane.

Cisco Secure			
Context Reparator Welcome Task Guide Quick Staf Initial System Setup Policy Setup Policy Setup Stope Context Context	Wy Werksbeck +: My Account: General Admin Name: ACSAdmin: Description: Default Super Admin Email Address: Change Password Password must: • Contain 4 characters • Password: • New Password: • Contim • SuperAdmin		

Figure 4-2 My Account

Network Resources

AAA clients and external RADIUS servers are defined within this drawer. When ACS receives an AAA request from a network device, it searches the network device repository to find an entry with a matching IP address. If a match is not found, the request will be rejected.

This drawer has four menu items:

- Network Device Groups
- Network Devices and AAA Clients
- Default Network Device
- External RADIUS Servers

Network Device Groups

AAA clients in the ACS repository can be assigned to Network Device Groups (NDGs). NDGs are logical grouping of devices—for example, by Location or Type—which can be used in policy conditions. For example, all routers in the San Jose location can be assigned a single policy. NDGs simplify creating policies and managing device repository.

NDGs are defined under a hierarchical structure called a Device Group Hierarchy. Each device group hierarchy has a root node under which NDGs are defined. For example, Location and Device Type groups are predefined. The root node of the Location group is All Locations. New NDGs can be created under All Locations. These NDGs can further have other NDGs as child nodes. Figure 4-3 shows a sample hierarchy created under the Locations group. Notice how the NDGs are created countrywise, statewise, or citywise.

🔹 🛃 My Workspace	Network Resources > Network Device Groups > Location								
🔹 🏣 Network Resources	Network Device Groups								
Network Device Groups Location Device Type Network Devices and each Clients	Fliter. 🛛 Match if. 🔍 Go 💌								
Default Network Device External RADIUS Servers	Name Description All Locations								
+ 🎒 Users and Identity Stores	The second secon								
+ SP Policy Elements	<u>Mumbai</u> Devices in Mumbai								
+ 🌄 Access Policies	New Delhi Devices in New Delhi								
Monitoring and Reports	USA Devices in USA								
 System Administration 	California Devices in California								
	Create Duplicate Edit Delete File Operations Export								

Figure 4-3 Hierarchical Structure of NDGs

A maximum of 12 hierarchical groups can be created and each group can have a maximum of six nodes including the root node.

Note The two hierarchical groups provided—Location and Device Types—cannot be deleted or modified. This leaves 10 groups that can be added.

Clicking on the Network Device Groups menu item will display the existing groups in the Content Area as shown in Figure 4-4. The groups also appear as individual submenu items in the Navigation Pane under Network Device Groups. Click on a group name in the Content Area to edit it. New groups can be created by clicking on the **Create** button or the **Duplicate** button.

🖌 🚭 My Workspace	lietwork Resources > Network Device Groups					
👻 🚛 Network Resources	Network Device Groups	Showing 1+2 of 2 50 💌 per page Go				
Network Device Groups Location Device Type	Name Description Device Type					
Network Devices and AAA Clients Default Network Device External RADIUS Servers	Location Location					
Weers and Identity Stores Stores						
Policy Elements						
Access Policies						
 Monitoring and Reports 						
🖌 🝓 System Administration						
	Create Duplicale Edit Detete	R Page 1 of 1 P P				

Figure 4-4 Network Device Groups

To create a group, follow these steps:

Step 1. Select Network Resources > Network Device Groups.

The Network Device Groups page appears as shown in Figure 4-4.

Step 2. Click Create.

The Hierarchy - General Page appears in the Content Area. Figure 4-5 shows this page.

- **Step 3.** Enter a name; for this example, use **Routers**.
- **Step 4.** (Optional) Enter a description.
- **Step 5.** Enter a root node name. For this example, use All Routers.

Remember that this is any name that refers to all the NDGs and devices in this group.

Step 6. Click **Submit** to create the group.

The group **Routers** now appears in the Navigation Pane as a submenu item under the Network Device Group menu item.

Clicking on the group name, **Routers**, in the Navigation Page will open the Network Device Groups page in the Content Area. Because the group is new, only the root node

+ 🚓 My Workspace	Network Resources > Network Device Groups > Create
Contractive Resources Howark Resources Location Device Type Technology Migrate CNOGs Network Devices and AAA Clients Default Hetwork Device	Hierarchy - General o Name: Routers Description: Root Node Name: All Routers 0 = Required fields
External RADIUS Servers	
 B Users and Identity Stores 	
 Policy Elements 	
Access Policies	
 Monitoring and Reports 	
🖌 🤘 System Administration	
	Submit Cancel

Figure 4-5 Creating a Network Device Group

All Routers will be displayed. This page is similar to the one shown in Figure 4-3. You can add NDGs to the **Routers** group from this page. To do so, follow these steps:

- Step 1. Click Create.
- **Step 2.** Enter a name for the group; for our example, use **Core Routers**.
- **Step 3.** (Optional) Enter a description.
- **Step 4.** The root node, All Routers, is already selected in the Parent field. If other NDGs existed in the Routers group, you could have clicked on **Select** to see them and select a different parent node.
- **Step 5.** Click Submit to create the NDG.

Core Routers is now visible under the root node in the Network Device Groups page.

Network Devices and AAA Clients

It is important to remember that a device should be in the ACS repository before AAA requests from that device will be accepted. The Network Devices and AAA Clients menu item shows the repository and enables you to manage the devices. Along with the name and address, the page displays the NDG that the device belongs to. You can use the filter option to search for devices. This page is shown is Figure 4-6. To add an AAA client to the ACS database and enable communications using the TACACS+ or RADIUS protocols, you use the following steps:

- **Step 1.** Select Network Resources > Network Devices and AAA Clients.
- Step 2. Click Create.

· · ··································	Network Resources > Netw	work Devices and AAA Clients > Create		
Network Resources Network Device Groups Location Device Type Pavidere	o Name: Rou Description: Network Device Gro	ups		
Network Devices and AAA Clients	Location	All Locations:USA:California:San	Jose	Select
Default Network Device	Device Type	All Device Types	[Select
Sternal RADIUS Servers Servers Users and Identity Stores	Routers	All Routers:Core Routers		Select
Constraint Policies Constraint Policies System Administration	Single IP Ad IP: 192.168.1.0 IP: 192.168.1.0 IP: 192.168.1.0 IP: 192.168.1.0 IP: 192.168.1.0 IP: 192.168.1.0 IP: 192.168.1.0	dress () IP Range(s) Masi; 24 EditA Replace V Delete Masi: 24 24 24	 TACACS- ♥ Shared Se Single Legaco, TACAC RADIUS Shared Se 	ret Cisco Connet Device y TACACS+ Single Connet Support S-F Draft Compliant Single Connet Support cret

Figure 4-6 Adding a New AAA Device

Figure 4-6 shows the Create Network Device page.

- **Step 3.** Enter the hostname of the AAA client, or if this is going to be a group of devices, enter a name that makes it easily recognizable. For this example, use **Router1**.
- **Step 4.** (Optional) Enter a description.
- Step 5. All device groups configured in ACS are shown and their root nodes are selected. Click Select next to the group you want to change to display the Network Device Groups selection box. Click the radio button next to the desired Network Device Group and click OK. For this example, select the San Jose and Core Routers from the Location and Routers groups.
- **Step 6.** A device definition can represent a single or multiple devices. Select Single IP Address or IP Range as required. Selecting IP Range will display options for configuring a mask with the IP address. You can add multiple entries for the range. For this example, use a 192.168.1.0 address with a mask of 24.
- **Step 7.** Select TACACS+ and/or RADIUS and enter the shared secret. You have the option of selecting both protocols for a device. For this example, select TACACS+ and enter Cisco as the shared secret.
- Step 8. Click Submit

The device is now listed in the Network Devices and AAA Clients page as shown in Figure 4-7.

Note The number of devices that you can add in ACS depends on the license type. The number of devices is determined by the number of unique IP addresses that you configure.

This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.

1 Hebrork Personner	1000						
National Davida Crowas	Netwo	ork Device	5			Showing 1-1 of 1	50 💌 per page 🛛 Go
Location	Filter			Match if:	Co 🔻		
Routers		Name		IP / Mask	NDG:Location	NDG:Device Type	Description
Network Devices and AAA Clients		Router1		192.168.1.0/24	All Locations:USA:California:San Jose	All Device Types	
Default Network Device							
S Users and Identity Stores							
Sp. Policy Elements	1						
🔂 Access Policies							
Monitoring and Reports							
System Administration							
		-				1	

Figure 4-7 Network Devices and AAA Clients

Default Network Device

As mentioned previously, a device needs to be in the ACS repository before AAA requests will be accepted from it. There is an exception to this rule. You can configure a default network device. If a request comes from a device that does not specifically exist in the repository, ACS will use the default device profile. In the default network device definition, you provide a shared secret key, network device group, and the protocol(s) to be used. To configure the default network device, follow these steps:

Step 1. Select Network Resources > Default Network Device.

The Default Network Device page appears. Figure 4-8 shows this page.

- Step 2. Select Enabled from the drop-down list next to Default Network Device Status.
- **Step 3.** Click Select next to the device groups that you want to modify. For our example, select San Jose NDG from the Locations Group.
- **Step 4.** Select TACACS+ or RADIUS and enter the shared secret for the protocols. You can select one or both the protocols. For this example, select both the protocols and use Cisco as the shared secret.
- Step 5. Click Submit.

🖌 🛃 My Workspace	Network Resources > Default Network Device						
In Network Resources Network Device Groups Location Device Type Routers Network: Devices and AAA Clients	Default Network D The default device address. Default Network D Network Device G	evice definition can optionally be used in cases where no sj evice Status: Enabled 🕑 😁 roups	secific device definition is found that	matches a device IP			
Default Network Device	Location	All Locations USA California San Jose	Select				
External RADIUS Servers	Device Type	All Device Types	Select				
Bolicy Elements	Routers	All Routers	Select				
	Authentication Op TACACS+ (y) Shared Secr Eugacy T TACACS + RADIUS • RADIUS • RADIUS • Required field Submit Cancel	tions at Clace annot Device ACACS+ Single Connect Support - Draft Compilant Single Connect Support at Clace s					

Figure 4-8 Default Network Device

External RADIUS Servers

ACS 5.1 can function both as a RADIUS server and a RADIUS proxy server. When it acts as a proxy server, ACS receives authentication and accounting requests from the AAA client and forwards them to the external RADIUS server. ACS accepts the results of the requests and returns them to the client. You must configure the external RADIUS servers in ACS to enable ACS to forward requests to them. You can configure multiple external RADIUS servers. To add a server, follow these steps:

Step 1. Select Network Resources > External RADIUS Servers.

The External RADIUS Servers page appears with a list of configured servers.

Step 2. Click Create.

The Create Server page appears as shown in Figure 4-9.

- **Step 3.** Enter a name for the server. For this example, use External1.
- **Step 4.** (Optional) Enter a description.
- Step 5. Enter the server IP address. For this example, use 192.168.1.40.
- **Step 6.** Enter the shared secret. This secret is used to encrypt the RADIUS request between ACS and the external server. For this example, use Cisco.
- Step 7. Click Advanced Options.
- Step 8. Verify the authentication and accounting ports.

By default, ports 1812 and 1813 are used. If the external server uses other ports, enter them in the respective fields. This example leaves the ports set to the default values.

► 🐣 My Workspace	Network Resources > External RADR	IS Servers	ors > Create	
Hetwork Resources Network Device Groups Location Device Type	General OName: External1 Description:			
Routers Network Devices and AAA Clients Default Network Device Exempt RADIUS Servers	Server connection Server IP Address: Shared Secret	192.168	68.1.40	
Policy Elements	 Advanced Options 			
+ 🛄 Access Policies	Authentication Port:	1812		
 Monitoring and Reports 	Accounting Port:	1813		
🖌 😸 System Administration	Server Timeout	10	Seconds	
	 Connection Attempts: Required fields 	5		
	Submit Cancel			

Figure 4-9 Adding an External RADIUS Server

Step 9. Verify the server timeout value.

By default, five seconds timeout period is used. If the server fails to respond in that period, the server will resend the request as many times as specified in the Connection Attempts field. You can specify a timeout value of 1 to 120 seconds. For this example, specify 10 seconds.

Step 10. Verify the connection attempts value.

By default, ACS will attempt to connect to the external server three times. You can configure ACS to attempt up to 10 times to connect to the external server. For this example, specify five attempts.

Step 11. Click Submit.

Users and Identity Stores

To authenticate and authorize a user or host, ACS uses the user definitions stored in identity stores. There are two types of identity stores:

- Internal Identity Stores: Identity stores that ACS maintains locally are called *internal identity stores*. ACS maintains two different internal identity stores for user and host records. These stores are accessible from the Internal Identity Stores menu item in the Users and Identity Stores drawer.
- External Identity Stores: Identity stores that reside outside of ACS are called *external identity stores* (or *external user databases* in earlier versions of ACS). Each external identity store requires certain configuration before ACS can obtain information from it. The External Identity Stores menu item under the Users and Identity Stores drawer can be used to configure these stores.

In this chapter, you add a user and a host to the internal identity stores. External identity stores are discussed in Chapter 5, "Configuring External Databases with ACS."

Before adding a user or host, you should know about identity groups and how to add them.

Identity Groups

Identity groups, as the name suggests, are groups of users or hosts. As in ACS 4.2, users and hosts can be put in a group to apply a uniform policy on them.

Note A key point to remember is that ACS 4.2 is a group-based server, whereas ACS 5.1 is a policy-based server. This means that users and groups in ACS 5.1 do not have reply attributes configured in their profile. Reply attributes are derived from policy evaluation.

Identity groups are defined in a hierarchical structure like the NDGs. *All Groups* is the root of this hierarchy.

To create an identity group, follow these steps:

Step 1. Select Users and Identity Stores > Identity Groups.

The Identity Groups page appears.

Step 2. Click Create.

The Create Identity Group page appears as shown in Figure 4-10.

+ 🧬 My Workspace	Users and identity Stores > Identity Groups > Create	
In Network Resources		
Susers and identity Stores Identity Groups Internal identity Stores Users Users Hearts	o Name: Admin Description: o Parent: All Groupp Select	
External Identity Stores LDAP Active Directory RSA SecuriD Toten Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Certificate Authorities	• - Kequired helds	
> S Policy Elements		
Access Policies		
Monitoring and Reports		
🔸 💐 System Administration		

Figure 4-10 Creating an Identity Group

Step 3. Enter a unique name for the group. For our example, use Admin.

- **Step 4.** (Optional) Enter a description.
- **Step 5.** Click Select to select a parent group for this group. For this example, use the Root group.
- Step 6. Click Submit.

The Identity Group page appears with the Admin group listed under the root.

Adding a User in the Internal Identity Store

Adding a user to the internal identity store is very simple in ACS 5.1. To add a user, follow these steps:

Step 1. Select Users and Identity Stores > Internal Identity Stores > Users.

The Internal Users page appears.

Step 2. Click Create.

The User Properties page appears as shown in Figure 4-11.

 My Workspace 	Users and Identity Stores > In	ternal identity Stores	> Users > Create		
Image: Provide the second s	Constal				
Stores and Identity Stores	O Name: Use	rt	Status: Enabled		
Policy Elements	Description:				
+ 🔁 Access Policies	O Identity Group: All C	couns Admin		Select	
Monitoring and Reports					
- 💐 System Administration	Password Information Password must	n		Enable Password Information	
Administrators Accounts	Contain 4 - 32	characters		Contain 4 - 32 characters	
Roles	O Password:			Enable Password:	
 Settings 	Confirm			Confirm	
Osers Authentication Settings Operations	Password:	ord on next login		Password:	
Distributed System Management	User Information				
Software Repositories	There are no additional identity attributes defined for user records				
Scheduled Backups	0 = Required fields				
 Local Operations 					
Configuration					
 Global System Options Dictionaries 					
Protocols	4				
+ Identity					
Internal Users					

Figure 4-11 Adding a User to the Internal Identity Store

- **Step 3.** Enter a name for the user. This name will be used by the user to authenticate. For our example, use User1.
- **Step 4.** (Optional) Enter a description.
- **Step 5.** Click Select and select an identity group for the user. For this example, select the Admin group created in the previous section.

- **Step 6.** Enter the password and confirm the password. The password must match the restriction shown in the Password Information section on the page. By default, the password must be 4 to 32 characters long. For this example, use **Cisco** as the password.
- **Step 7.** (Optional) An enable password can be entered for users to log in to the privilege mode of devices. This option is enabled by default and can be disabled from the User Authentication settings section. For this example, leave this field blank.

Note Identity attributes can be used in a policy. For more information on dictionaries and identity attributes see Chapter 15, "ACS 5.1 Advanced Configuration."

Step 8. Click Submit.

The user configuration will be saved and the Internal Users page will appear with the new user listed.

Adding a Host in the Internal Identity Store

Adding a host in the ACS internal data or identity store is not a new concept. In versions of ACS prior to ACS 5.1, the MAC address of a host could be added as a user for MAC address-based authentication. ACS 5.1 provides separate user and host identity stores! Steps for adding a host in the internal identity stores are similar to that of adding a user. To add a host, follow these steps:

Step 1. Select Users and Identity Stores > Internal Identity Stores > Hosts.

The Internal Hosts page appears.

Step 2. Click Create.

The host properties page appears as shown in Figure 4-12.

Step 3. Enter the MAC address of the host. You can enter the MAC address in any of the following formats:

Although you can enter the MAC address in any of the formats in the preceding list, ACS will convert and store the MAC address in the first format. For this example, use **00-19-01-02-AA-EE**.

Step 4. (Optional) Enter a description.

▶ ⊕ ⁴ My Workspace	Users and Identity Stores > Internal Identity Stores > Hosts > Create		
🕞 🍓 Network Resources	Gameral		
Si Users and Identity Stores Identity Groups Internal Identity Stores Users External Identity Stores Certificate Authentication Profile Identity Stores Certificate Authentication Profile Identity Stores	Of MAC Address. 00-19-01-02-AA-EE Status: Enabled ♥ ⊕ Description:		
	Identity Group: All Groups:Admin Select MAC Host Information There are no additional identity attributes defined for MAC host records - Required fields		
Policy Elements			
+ 🔂 Access Policies			
Monitoring and Reports			
System Administration			
	Submit Cancel		

Figure 4-12 Adding a Host to the Internal Identity Store

- **Step 5.** Click Select and select an identity group. For our example, use the Admin group created in the previous sections.
- Step 6. Click Submit.

The host configuration will be saved and the Internal Hosts page will appear with the new host listed.

Note The Users and Identity Stores drawer contains Certificate Authority and Certificate Authentication Profiles menu items. These are used to configure ACS for Certificate based authentication. These sections are discussed in Chapter 8, "IOS Switches."

The Identity Store Sequences menu item is used to define sequences of databases to be used in a policy. This section is covered in Chapter 5, "Configuring External Databases with ACS."

Policy Elements

You know from Chapter 2 that ACS 5.x is based on a rule-based policy model. You also know that the rules are called *policies* and they consist of conditions and results, which are called *policy elements*. In this section and the next, you will learn more about policy elements and how to create them, the different types of policies, and the flow of a request through different processes in ACS.

Before creating policies, you must create policy elements, which are the building blocks of policies. Policy elements are divided into two types: *session conditions* and *authorization and permissions*.

Session conditions are conditions used to apply policies to requests. Some conditions are available by default, whereas others can be created by you. The following conditions are available by default:

- Request/Protocol Attributes: These attributes are derived from the authentication request itself.
- Identity Attributes: Identity attributes are derived from the user definition in the internal identity store or external repositories such as LDAP and Active Directory. The attributes need to be mapped in the external database configuration before they become available in the policies. See Chapter 5 for more on external databases and attribute mapping.
- Identity Groups: You can map every user and host to an identity group. This group association can be used in policies as a condition.
- Network Device Groups(NDGs): Each device is associated with an NDG. This association can be used as a condition in the policies.

The following conditions can be created by you:

- Date and Time Conditions: You can create conditions that define specific time intervals across days of the week. These conditions take into account the current date and time and return a true or false result indicating whether the condition is met.
- Custom Conditions: You can create conditions based on attributes of various identity and protocol dictionaries which are available in ACS. These conditions allow you to apply policies based on the authentication and authorization requests received from AAA clients.
- Network Conditions: You can create conditions based on the following to restrict access:
 - End Station Filters: These are based on end stations that initiate and terminate the connection. End stations may be identified by IP Address, MAC Address, or Caller Line Identification (CLI) and Dialed Number Identification Service (DNIS) fields obtained from the request.
 - Network Device Filters: Based on the AAA client that processes the request. A network device can be identified by IP address, the name of the device that is defined in the network device repository or the network device group (NDG).
 - Device Port Filters: Network device definition might be supplemented by the device port that the end station is connected to.

These filters or conditions can be included in policy conditions. This set of definitions is matched against those presented in the request. The operator that you use in the condition can either be *match* (in which case the value presented must match at least one entry within the network condition) or *no matches* (in which case it should not match any entry in the set of objects present in the filter).

Authorization and permissions are the results applied to a request that matches a condition in a policy. You can define the following types of results:

• Authorization Profiles: You can define a set of attributes and values that is returned to the device in Access-Accept responses for network access requests. These profiles

can contain common data such as VLAN information, reauthentication timer, or any RADIUS attribute.

- Shell Profiles: You can define a set of permissions that is applied to a user requesting administrative access of a device. Some of these permissions include privilege level, auto command, and custom TACACS+ attributes.
- Command Sets: You can define a list of commands that a user can execute on a device during an administrative session.
- Downloadable ACLs: You can define downloadable ACLs that can be sent to a device with an Access-Accept message.

If you have worked on previous ACS versions (4.x or 3.x), you must have noticed that many of the policy elements were available earlier in the Group Setup. The difference in ACS 5.x is that these conditions and results are now defined globally and can be used in multiple rules. Group-based configuration required configuring the conditions and results in each group even if they were similar.

Figure 4-13 shows a typical simplified flow of a request through ACS. Note the different places where policy elements are used. At this stage, do not worry about the different policies shown in the figure because they will be covered later in the chapter.



Figure 4-13 Flow of a Request Through ACS 5.x
The following sections look at creating the different policy elements.

Session Conditions: Date and Time

To create a Date and Time session condition, follow these steps:

Step 1. Select Policy Elements > Session Conditions > Date and Time.

Step 2. Click Create.

The Date and Time Properties page appears as shown in Figure 4-14.



Figure 4-14 Creating Date and Time Condition

- Step 3. Enter a name. For this example, use Work-week.
- **Step 4.** (optional) Enter a description.
- Step 5. Define start and end times for this element. During the period defined, the element can be used by policies. You can select *Start Immediately* and *No End Date* for the element to be active always or select a specific date and time during which this element will be active. This is useful when you want to provide some access or privilege for only a certain duration. For our example, select the Start Immediately and No End Date options.
- Step 6. Select the days and time during which this element will return a positive reply for access request. Each square in the grid is equal to one hour. Select a grid square to make the corresponding time active. For this example, select 7:00 to 18:00 hours, Monday to Friday as shown in Figure 4-14.
- Step 7. Click Submit.

The policy element you created will restrict access to 7:00–18:00 hours on Monday through Friday, when applied to a policy.

Session Conditions: Custom

To create a custom session condition, follow these steps:

- **Step 1.** Select Policy Elements > Session Conditions > Custom.
- Step 2. Click Create.

The Custom Condition Properties page appears. This page is shown in Figure 4-15.

► A My Workspace	My Workspace > Welcome > Create	
Network Resources	General	
 Jusers and Identity Stores 	Name: Protocol Condition	
 Specific Policy Elements 	Description:	
 Session Conditions Date and Time Custom 	Condition Dictionary: RADIUS-IETF	
 Network Conditions End Station Filters Device Filters 	Attribute: [Framed-Protocol Select]	
Device Port Filters + Authoritation and Permissions + Network Access Authoritation Profiles + Device Administration Shell Profiles Command Sets + Named Permission Objects Downloadable ACLs		
Access Policies		
 Monitoring and Reports 		
 System Administration 	Submit Cancel	

Figure 4-15 Creating a Custom Session Condition

- **Step 3.** Enter a name. For our example, use **Protocol**.
- **Step 4.** (optional) Enter a description.
- **Step 5.** Select Dictionary from the drop-down list. Different Protocol and Identity dictionaries are available in the drop-down list. For our example, select **RADIUS-IETF**.
- **Step 6.** Click Select next to the Attribute text box and select an attribute. For our example, select Framed-Protocol.

Step 7. Click Submit.

The custom condition that you just created will match the Framed-Protocol attribute in a RADIUS request when applied to a policy.

Session Conditions: End Station Filters

To create an end station filter, follow these steps:

- **Step 1.** Select Policy Elements > Session Conditions > Network Conditions > End Station Filters.
- Step 2. Click Create.

The End Station Filter Properties page appears as shown in Figure 4-16.

▶ St My Workspace	Policy Elements > Session Conditions > Network Conditions > End Station Filters > Create
In the second	General
Weers and Identity Stores	Name: HostList 1
Policy Elements	Description
 Session Conditions Date and Time 	IP Address MAC Address CLUDNIS
Custom * Network Conditions	Network Devices Showing 1-1
End Station Filters	Filter: End Station IP 😪 Match It. Contains 🐼 Clear Filter Go 🔻
Device Port Filters	End Station IP
* Authorization and Permissions	192.168.1.0/24
Network Access Device Administration Named Permission Objects	Create Duplicate Edit Delete Export to File Replace from File Page
Access Policies	
Monitoring and Reports	
🕨 💐 System Administration	
	Submit Cancel

Figure 4-16 Creating an End Station Filter

- Step 3. Enter a Name. For this example, use Host List 1.
- **Step 4.** (optional) Enter a description.
- Step 5. End stations can be filtered by IP address, MAC address, or Calling Line ID (CLI)/Dialed Number Identification Service (DNIS). The filter values are added under the respective tabs. For this example, select the IP Address tab.
- Step 6. Click Create.

A dialog box opens where you can enter an IP address or a range of addresses. For this example, select IP Range(s) and enter 192.168.1.0 in the IP text box and 24 in the Mask text box. Click Ok.

192.168.1.0/24 is now listed in the Network Devices table.

Note that the options in the dialog box will change depending on the tab selected.

Step 7. Click Submit.

The filter you created will match any host in the 192.168.1.0/24 when applied to a policy.

Session Conditions: Device Filters

To create a device filter, follow these steps:

- **Step 1.** Select Policy Elements > Session Conditions > Network Conditions > Device Filters.
- Step 2. Click Create.

The Device Filter Properties page appears as shown in Figure 4-17.

▶ St My Workspace	Policy Elements > Session Conditions > Network Conditions > Device Filters > Create	
Image: Metwork Resources	General	
Users and Identity Stores	Name: Core Routers	
* 🗫 Policy Elements	Description	
 Session Conditions Date and Time 	IP Address Device Name Network Device Group	
Custom	Network Devices Showing f	-11
End Station Filters	Filter: NDG Type 💌 Match it: Contains 🔍 Clear Filter Go 🔻	
Device Port Filters	NDG Type NDG Value	
Authorization and Permissions	Routers All Routers:Core Routers	
 Network Access Device Administration Named Permission Objects 	Create Duplicate Edit Delete (Export to File Replace from File Page	
Access Policies		
Monitoring and Reports		
🕞 😽 System Administration		
	Submit Cancel	

Figure 4-17 Creating Device Filters

- **Step 3.** Enter a name. For this example, use **Core Routers**.
- **Step 4.** You can enter the IP addresses of devices, the names of devices already in the ACS repository, or a network device group under the respective tabs. For this example, select the **Network Device Group** tab.
- Step 5. Click Create.

A dialog box appears where the NDG can be selected. Click **Select** next to the NDG Type text box and select the **Routers** group that you created earlier. Then click on **Select** next to the NDG Value text box and select the **Core Routers** group that you created earlier. Click **Ok**.

The Core Routers NDG is now listed in the Network Devices table.

Note that the options in the dialog box will change depending on the tab selected.

Step 6. Click Submit.

The device filter you created will match any device in the Core Routers NDG when applied to a policy.

Session Conditions: Device Port Filters

The steps to create a device port filter are similar to the one you followed to create device filters. The only difference is the addition of a Port text box in the dialog box where you select or enter device information. Figure 4-18 shows the Device Port Filter properties page where the Core Routers NDG is added with port 23.

🔸 🕂 My Workspace	Policy Elements > Session Conditions > Network Conditions > Device Port Filters > Create
In the second	General
3 Users and Identity Stores	Name: Core Routers - Teinet
 Sp Policy Elements 	Description
Session Conditions Date and Time Custom Network Conditions End Station Filters Device Filters Device Filters Network Access Polyce Administration Named Permission Objects	IP Address Device Name Network Device Group
	Network Devices Showing 1-1 of 1 50 V per page
	Filter: NDG Type 💌 Match it: Contains 💌 Glear Filter Go 🔻
	NDC Type NDC Value Port Routers All Routers:Core Routers 23
	Create Duplicate Edit Delete Export to File Replace from File Page 1 of 1 K + +
Access Policies	
 m) Monitoring and Reports 	
🕞 😽 System Administration	
	Submit Cancel

Figure 4-18 Creating Device Port Filters

Note Authorization and permissions policy elements are covered in later chapters.

- Authorization profiles are covered in Chapter 8, "IOS Switches."
- Shell profiles and command sets are covered in Chapter 6, "Administrative AAA on IOS."

Downloadable ACLs are covered in Chapter 10, "Cut-Through Proxy AAA on PIX/ASA."

Access Policies

Before you start creating policies, it is important to understand how ACS applies a particular policy to a request and how many policies are available. ACS uses service selection rules and access services to decide on a policy to apply to a request.

Service Selection Rules

Service selection rules decide which access service to send an authentication or authorization request to. You can configure ACS to use a single access service to process all requests or use rules based on session conditions to send requests to different access services. In the case of a rule-based selection, ACS uses the first rule from the top that matches a request.

Note When rules are used for service selection, ACS provides an option to configure a default rule. If a request does not match any rules in the table, the default rule is applied.

To further understand how this works, take a department store for example. A department store is divided into sections using product category (clothing, sporting goods, jewelry, and so on). An ACS configured to use a single access service is like the department store. All requests go to a single access service, which has different policies. The access service checks session conditions and applies the appropriate policy. Consider a grocery store for another example. A grocery store sells only groceries, but might have sections based on different categories (produce, meat, canned goods, and so on). An ACS configured for rule based service selection is similar to such a store. It will send different kinds of requests to different access services. Each access service equates to a specialized store. These access services will have different policies.

To further understand service selection rules and access services, consider another example. XYZ Inc. has five offices. Each office has routers terminating VPN connections. These routers are going to authenticate and authorize VPN sessions and administrative sessions to a single ACS. There are two ways to configure ACS for the organization:

- Method 1: Configure ACS to send all requests to a single access service and configure two policies in the access service. One policy to process all administrative session requests via the TACACS+ protocol and the other to process all VPN session requests via the RADIUS protocol.
- Method 2: Configure ACS to send all TACACS+ (administrative sessions) requests to one access service and to send all RADIUS (VPN sessions) request to another access service. Each access service can have one or more policies to process the requests.

Method 1 is easier to configure and maintain; however, it can get very complicated if different authentication or authorization methods need to be applied. For example, one site might need more stringent authorization for VPN sessions than other sites or administrators might need restricted access to remote devices. Further consider an organization with 100 sites and thousands of network devices. In such scenarios, policies will increase in the access service and soon become unmanageable. On the other hand, different access services will have a smaller number of policies and will be easier to manage.

Access Services

Access services are the most basic parts of ACS. They are sets of policies which process all authentication and authorization requests. Every authentication and authorization request has to match a policy in an access service before it is processed. As you already know, a request is sent to an access service by the service selection rules. When an access service receives a request, it checks policies in a top-down manner and applies the first policy that matches the session conditions.

Access services consist of the following types of policies:

- Identity Policy: Specifies how the user should be authenticated and includes the allowed authentication protocols and the user repository to use for password validation. Identity policies can be simple or rule based. Simple policies apply a single policy to all requests. Rule-based policies use session conditions to choose rules for requests.
- Group Mapping Policy: Specifies whether the user's ACS identity group should be dynamically established based on user attributes or group membership in external identity stores. The user's identity group can be used as part of its authorization. Chapter 5 covers group mapping in more detail.
- Authorization Policy: Specifies the authorization rules for the user. Authorization policies can only be rule based.

Note If a policy is rule based, ACS checks rules in a top-down manner and uses the first rule that matches. ACS also provides an option to configure a default rule. If a request does not match any rules in the table, the default rule is applied.

ACS has two access services by default:

- Default Device Admin: Service selection rules are configured to send all TACACS+ requests to this default access service.
- Default Network Access: Service selection rules are configured to send all RADIUS requests to this default access service.

Creating an Access Service

Access services and their policies bring together different elements from ACS. Hence, before creating an access service, you should determine the network configuration and the degree of refinement that you want individual policies to have. Depending on that, you should add devices and users or user databases. You should also create different policy elements such as session conditions and authorization and permission elements. Ensuring that you have all the required components will save you from moving back and forth between different drawers in the menu.

To create an access service, follow these steps:

Step 1. Select Access Policies > Access Services.

The Access Services page appears.

Step 2. Click Create.

The Access Service General Properties page appears as shown in Figure 4-19.

🖌 🧬 My Workspace	Access Policies > Access Services > Create
Hetwork Resources	General Allowed Protocols
 Jusers and Identity Stores 	
Policy Elements	Step 1 - General
Access Policies	
Access Services Service Selection Rules O Default Device Admin	General O Name: Remote Access VPN
Identity Authorization	Description: Access Service Policy Structure
Operault Network Access Identity Authorization	Based on service template Based on existing service Gelect
 Monitoring and Reports 	User Selected Service Type Network Access
 System Administration 	User Selected Service Type Policy Structure Oldentity Croup Mapping Authorization
	Back Next Finish Cancel

Figure 4-19 General Properties of a New Access Service

- Step 3. Enter a name. For this example, use Remote Access VPN.
- **Step 4.** (optional) Enter a description.
- **Step 5.** Select one of the following options for Access Service Policy Structure:
 - Based on service template: Creates an access service based on a predefined template. These templates are customized to use a specific condition type. To use this option, select the radio button next to it, and then click Select and select a template.
 - Based on existing service: Creates an access service containing policies based on an existing access service. The new access service does not include the existing service's policy rules. To use this option, select the radio button next to it, and click Select and select an existing access service.
 - User Selected Service Type: Provides you the option to select the access service type. The available options are Network Access, Device Administration, and RADIUS Proxy. The list of policies you can configure depends on your choice of access service type. To use this option, select the radio button next to it and select an access service type from the drop down box. Selecting this option will also display the option to enable or disable different policy types.

For this example, select User Selected Service Type and select Network Access from the drop-down box. Select Identity and Authorization in the policy structure.



Figure 4-20 Configuring Allowed Protocols in an Access Service

Step 6. Click Next.

The Allowed Protocols properties page appears as shown in Figure 4-20.

- Step 7. This page enables you to select which authentication protocols will be allowed with this access service. PAP, CHAP, MS-CHAPv1, MS-CHAPv2 and various EAP protocols are available as options. You can also enable host lookup (required for machine authentication) from this page. For this example, deselect Process Host Lookup and select Allow PAP/ASCII and Allow MS-CHAPv2.
- Step 8. Click Finish.

The access service will be saved and will appear as a menu item in the Access Services drawer. Below the menu item, selected policy types will be shown as submenu items. At this point, a prompt will give you an option to activate this service in the Service Selection Rules. For now, click **No**. The Access Services page will appear with the new access service listed in the table.

You are now ready to configure the identity rules and authorization rules for the new access service.

Configuring Identity Policy

As you already know, identity policies can be simple or rule-based. By default, identity policies are simple. When you select Identity under a new Access Service (Remote Access VPN for this example) in the Access Policies drawer, you will find that the Single result selection option is selected and Identity Source is DenyAccess.

If you want to configure a simple policy, follow these steps:

- **Step 1.** Click Select next to Identity Source and select an identity store. You can select between certificate-based authentications or different password-based internal or external identity stores.
- **Step 2.** (Optional) Click Advanced Options to display the fail-open options. Fail-open opens enable you to configure the behavior of ACS when authentication fails, the user is not found in an identity store, or there is a process failure. A process failure occurs when ACS is not able to verify the credentials, usually due to external factors such as a network failure between ACS and an external database. To understand the fail-open process, you have to remember that a device will fail over to a different AAA server if the primary server does not respond to a request. Each of the three fail-open options has three possible actions:
 - Reject: Sends an Access-Reject or Fail reply to the AAA client.
 - **Drop:** ACS drops the request, causing the AAA client to retry another fail over to another AAA server.
 - Continue: Causes ACS to try the next service or rule.

By default ACS will reject a request if authentication fails or a user is not found, and will drop a request if the process fails. Figure 4-21 shows this page with the default Advanced options.



Figure 4-21Configuring a Simple Identity Policy

Step 3. Click Save Changes.

If you want to configure a rule-based identity policy, follow these steps:

Step 1. Select **Rule based result selection** from the Identity Properties page.

This will change the properties page to a rule-based table format shown in Figure 4-22.

🖌 🚭 My Workspace	Access Policies > Access Services > Remote Access VPN > Identity
In Network Resources	O Single result selection O Rule based result selection
By Users and Identity Stores Sto	Identity Policy
Policy Elements	Filter Status Status Match it Equals Finabled Clear Filter Go
+ 🛃 Access Policies	
Access Services El Service Selection Rules	Status Name NDG.Routers Identity Source
- O Default Device Admin	No data to display
Authorication + O Default Network Access Identity Authorication + 2 Remote Access VPN Identity Authorication	
 Monitoring and Reports 	
System Administration	Default If no rules defined or no enabled rule matches. DenyAccess
	Create_I Duplicate_I Edit Detele Move to. Customize Hit Count Save Changes Discard Changes

Figure 4-22 The Identity Policy Page for a Rule-Based Configuration

- Step 2. The rules of an Identity policy use session conditions to determine which identity store to use for a request. The session conditions available in the Rules Properties page need to be enabled from the Identity Properties page. Click Customize to open the Customize Conditions dialog box. Select the conditions that you want to use. For this example, deselect default conditions and select NDG:Routers (you created this NDG earlier in this chapter).
- Step 3. Click Create.

The Identity Rule properties page appears as shown in Figure 4-23.

- **Step 4.** Enter a name. For this example, use **Core Routers**.
- **Step 5.** Select a session condition. In this example, only **NDG:Routers** is available, so select it.
- **Step 6.** Select an operator from the drop-down box next to the selected condition. The available operators change depending on the condition selected. These are logical operators that allow matching or not matching the user-provided argument with the selected condition. For this example, select **in** from the drop-down box.
- **Step 7.** For some conditions, such as NDGs, you will see a Select button next to the condition. You can click this button to select the required element. For some conditions, you will get a drop-down box or a text box. For this example, click **Select** and select **Core Routers** NDG.

Cisco Secure ACS - Mozilla Firefox	
10.78.166.38 https://10.78.166.38/acsadmin/PolicyInputAction.do	ŵ
General Name: Core Routers Status: Enabled ● Image: Core Routers Status: Enabled ● Image: Core Routers Status: Enabled Image: Core Routers Status: Status: Image: Status: Image: Status: Conditions Image: Status: Image: Status: Status:	
OK Cancel	Help
Done	<u> </u>

Figure 4-23 Configuring the Rules of an Identity Policy

- **Step 8.** In the Results section, you can select the identity source to be used for this rule. Click **Select** next to Identity Source and select an identity store. You can select between certificate-based authentications or different password-based internal or external identity stores. For this example, use **Internal Users**.
- Step 9. (Optional) Click Advanced Options to display the fail-open options. Remember that by default, ACS will reject a request if authentication fails or a user is not found, and will drop a request if the process fails. For this example, leave them set to the default values.
- Step 10. Click OK.

The rule will be saved and the Identity Policy page will appear with the rule listed in the table.

The rule you created will use the Internal Users identity store to authenticate requests that originate from any device in the Core Routers NDG. You can add more rules to use different identity stores for different session conditions.

Now that the identity policy is configured, you can configure the authorization policy to complete the access service.

Configuring Authorization Policy

As mentioned earlier, authorization policies are rule based only. You cannot configure a simple authorization policy, but you can configure a single rule that will match all requests coming to the access service.

ACS also provides a default authorization rule. The default rule is applied if no rules are defined in an authorization policy or if a request does not match any defined rules.

Note I strongly suggest that you do not use the default rule to avoid security lapses. Using the default rule in most circumstances is like having a gate but leaving it open. You should have explicit rules for all variations of requests you get.

To configure a rule, follow these steps:

Step 1. Select Access Policies > Access Service you want to change > Authorization. For this example, select Authorization under Remote Access VPN.

The Authorization Policy page appears.

- **Step 2.** Rules of an authorization policy use session conditions to determine which authorization and permissions to use for a request. The session conditions available in the Rules Properties page need to be enabled from the Authorization Policy page. Click **Customize** to open the Customize Conditions dialog box. Select the conditions that you want to use. For this example, deselect default conditions and select **Identity Group**.
- **Step 3.** If the authorization policy for a TACACS+-based access service is being configured, then along with available session conditions, you will need to select available results in the Customize dialog box. Results can be shell profiles or command sets. For this example, you will not have an option to select results because the access service is RADIUS-based. **Authorization Profile** is the only result available with such access services.
- Step 4. Click Create.

The Authorization Rule properties page appears as shown in Figure 4-24.

- Step 5. Enter a name. For this example, use Admins.
- **Step 6.** Select a session condition. For this example, select **Identity Group**.
- **Step 7.** Select an operator from the drop-down box next to the selected condition. The available operators change depending on the condition selected. These



Figure 4-24 Creating the Rules of an Authorization Policy

are logical operators that allow matching or not matching a user-provided argument with the selected condition. For our example, select **in** from the drop-down box.

- Step 8. For some conditions, such as Identity Group, you will see a Select button next to the condition. You can click this button to select the required element. For some conditions your will get a drop-down box or a text box. For this example, click Select and select the Admin group you created earlier.
- **Step 9.** Authorization profiles require you to select a result. Results can be authorization profiles, shell profiles, or command sets depending on the access service. Click **Select** next to the result that you want to configure and select a policy element. For this example, select the **Permit Access** authorization profile, which is available by default.
- Step 10. Click OK.

The rule will be saved and the Authorization Policy page will appear with the new rule listed in the table.

You have created your first authorization rule, which permits access if the user belongs to the Admin Identity group.

Now that the access service configuration is complete, you will need to create a service selection rule so that this service is used.

Creating Service Selection Rules

As you know, service selection rules decide which access service to apply to a request. By default ACS is configured for rule-based service selection. Two rules are present by default. The first rule, named *Rule-1*, sends all RADIUS requests to the Default Network Access service and the second rule, named *Rule-2*, sends all TACACS+ requests to the Default Device Admin service. To configure ACS to use the Remote Access VPN service that you created, you need to add a new rule for service selection. You have the following choices in this situation:

- Edit Rule-1 to send all requests to the Remote Access VPN service
- Delete Rule-1 and create a new rule
- Create a new rule above Rule-1 that is specific to the Remote Access VPN service

For this example, create a new rule above Rule-1. To do so, follow these steps:

Step 1. Select Access Policies > Access Services > Service Selection Rules.

The Service Selection Policy page appears.

- **Step 2.** The session conditions available in a service selection rule properties page can be customized from this page. Click **Customize** and select the required conditions. For this example, select **NDG:Location** and **Protocol**.
- Step 3. Select Rule-1 and click the down arrow on the Create button.
- Step 4. Select Create Above.

The Service Selection Rules properties page appears as shown in Figure 4-25.

- Step 5. Enter a name. For this example, use San Jose VPN.
- **Step 6.** Select the conditions that define the rule. For this example, select **Protocol** and **NDG:Location**.
- Step 7. Select an operator from the drop-down box next to the selected condition. The available operators change depending on the condition selected. These are logical operators that allow matching or not matching a user-provided argument with the selected condition. For this example, select match for Protocol and in for NDG:Location.
- Step 8. For some conditions, such as NDG:Location, you will see a Select button next to the condition. You can click this button to select the required element. For some conditions, you will get a drop-down box or a text box. For this example, click Select and select San Jose for NDG:Location and RADIUS for



Figure 4-25 Creating a Service Selection Rule

Protocol. If you have not created the San Jose group, select the All Locations option for NDG:Location.

- **Step 9.** The result of a service selection rule is an access service or DenyAccess. You can use the drop-down box to select the result for the rule. For this example, select **Remote Access VPN** from the drop-down box.
- Step 10. Click Ok.

The rule will be saved and the Service Selection Policy page will appear with the new rule listed above Rule-1 in the table.

The rule you created will send RADIUS requests originating from devices in the **San Jose** NDG or **All Locations** NDG to the **Remote Access VPN** access service which you created earlier. The access service and policies that you created in the previous sections will authenticate RADIUS requests originating from a device in the **Core Routers** NDG using the **Internal User** identity store. If authentication is successful and the user belongs to the **Admin** identity group, the access will be permitted. Further chapters will help you create more complex access services and policies. The examples in this chapter are used to explain the basic process of creating policies and rules.

Monitoring and Reports

The Monitoring and Reports drawer replaces the Reports and Activity section of previous versions of ACS. You can now view reports based on different criteria such as Access Service, End Point, and Failure Reason, among others. ACS 5.x also introduces a configurable dashboard for reports and alarms.

Note ACS 5.x has added monitoring, reporting, and troubleshooting capabilities that are similar to those available is ACSView 4.0. ACSView is an independent reporting and monitoring platform available for ACS 4.x.

Covering the entire Monitoring and Reports section in depth is beyond the scope of this book. This section of the text will focus on the reports that are most important and touch on the rest briefly.

The Monitoring and Reports drawer contains the Launch Monitoring and Report Viewer option. Click this option to open the Monitoring and Reports Viewer in another browser window or tab. The layout of the new window is similar to the main window but contains only the following two drawers:

- Monitoring and Reports
- Monitoring Configuration

The Monitoring and Reports drawer contains the following options:

- DashBoard: ACS 5.1 provides a new customizable dashboard that contains tabs and portlets where your favorite queries, recent alarms and reports, and health status of ACS reside. Each of these tabs can have multiple portlets, with each portlet containing an application of your choice. You can select an application from the available list. Some of the important applications available in the dashboard by default are as follows:
 - Recent Five Alarms: This application is available in the General tab and shows the latest five alarms.
 - **Favorite Reports:** This application contains links to favorite reports. The favorite list is configuration from the Reports option discussed later.
 - Live Authentications: This application is available in the Troubleshooting tab and shows authentication requests received in real time. This is a very useful application for troubleshooting. By default, it refreshes every 10 seconds and is configured to monitor RADIUS requests.
 - NAD Show Command: A neat little application that can connect to a network device using SSH or Telnet and run a show command. You have to provide the login details and the show command to run. ACS will display the output in a new window. This is also a very useful application. It saves you from jumping between ACS GUI and Telnet or SSH clients.
 - ACS Health Status: Shows the health of the ACS server.

118 AAA Identity Management Security

- Alarms: ACS 5.x introduces alarms. The monitoring component retrieves data from ACS and generates alarms to notify you of critical system conditions. These alarms can be viewed in the Inbox option in this drawer or can be received through Syslog and email. There are two types of alarms in ACS: Threshold and System. Threshold alarms are defined on logs collected from ACS. You can configure a threshold alarm to notify you of different events such as authentication activity, system health, and process status, among others. System alarms notify you of critical conditions encountered during the execution of the ACS Monitoring and Reporting viewer. System alarms also provide the informational status of system activities, such as data purge events or the failure of the log collector to populate the View database. You cannot configure system alarms. This drawer contains the following options:
 - Inbox: Generated alarms can be viewed in the Inbox. After you view an alarm, you can edit the status of the alarm, assign the alarm to an administrator, and add notes to track the event.
 - Thresholds: You can configure thresholds from this page. A maximum of 100 thresholds can be configured in an ACS server. Four thresholds exist by default, out of which only the System Errors threshold is enabled.
 - Schedules: Each threshold has a schedule associated with it. The schedule defines when a threshold is run. You need to configure schedules on this page before you can use them in thresholds. By default, ACS has a nonstop schedule that monitors events 24 hours a day, seven days a week.
- **Reports:** The Reports section contains different predefined reports that you can use to monitor and troubleshoot ACS. These reports include authentication and authorization reports (similar to passed and failed reports from ACS 4.x), access service reports, ACS configuration and operation audits, and network device summary, among others. You can add any of the reports to your Favorites and those will be displayed in the General tab of the dashboard. The following report categories are available in the catalog:
 - AAA Protocol: Contains RADIUS and TACACS+ authentication, authorization (TACACS+ only) and accounting reports, AAA diagnostics, and authentication trend. Passed and failed logs from previous ACS version have been divided into protocol-specific authentication and authorization reports. Figure 4-26 shows the TACACS+ authentication report.
 - Access Service: Contains a graphical summary report and a top count report for authentication in respect to access services.
 - ACS Instance: Contains different system-related reports such as configuration and operations audit reports, health summary, administrator logins and entitlement reports, and ACS system diagnostics.
 - Endpoint: Contains MAC address-based authentication summary reports, MAC address-based top authentications reports, and machine-based top authentication reports.



Figure 4-26 TACACS+ Authentication Report

- Failure Reason: Contains summary and top authentication failure reports. This is one of the most important reporting sections. A close look at this section can tell you about any access attacks being carried out against your network.
- Network Device: Contains summary and top authentication reports in respect to network devices. These reports are useful in tracking which devices are generating the maximum number of requests.
- Session Directory: Contains active session, terminated sessions, and session history reports for RADIUS and TACACS+. Accounting packets received from devices are used to maintain session information.
- User: Contains summary and top authentication reports in respect to users.
- **Troubleshooting:** ACS 5.x contains some nice troubleshooting options. The following options are available in the Troubleshooting section:
- Connectivity Tests: You can run a ping, traceroute, and nslookup for a hostname or IP address to see whether the device is reachable from ACS. This is important to see whether the requests from a device and replies from ACS to the device are not getting dropped in the network.
- ACS Support Bundle: The support bundle is a zip archive of diagnostic information, including system log files. You can also choose to include ACS configuration, ACS debug log files, ACS localstore log files, and core files. This support bundle will be needed by the Cisco Technical Assistance Center (TAC) for troubleshooting.
- Expert Troubleshooter: This section contains some nice tools to check the configuration of a device and ACS. Using RADIUS Authentication troubleshooting tool, you can select a failed or passed log from RADIUS authentication report and have it check the ACS and device configuration to see why the authentication failed or passed. Figure 4-27 shows the report generated by this tool when changing the RADIUS shared key on the device. This section also contains the NAD show

command application from the dashboard and the Evaluate Configuration Validator, which checks the configuration of a device to see whether it is configured properly for a task such as 802.1x authentication.



Figure 4-27 RADIUS Authentication Troubleshooting Tool at Work

The Monitoring Configuration drawer contains various configuration options for the Monitoring and Report Viewer. Configuration of ACS View (the Monitoring and Reporting part of ACS 5.x) is out of the scope of this book.

Note The System Administration drawer contains various advanced configuration options for ACS. These options are covered in Chapter 15.

ACS 5.1 Command-Line Interface (CLI)

ACS 5.x, unlike previous versions, provides a CLI for configuration and monitoring along with a GUI. You can access the ACS CLI through a secure shell (SSH) client or the console port.

Two different types of accounts are available for accessing the CLI:

- Admin: Admin accounts have full configuration and monitoring access.
- Operator: Operator accounts have monitoring access only.

This section assumes use of an Admin account to access the CLI.

The ACS CLI is similar to IOS CLI in look, feel, modes, and command structure. You can use the question mark (?) to see the help and the Tab key to complete a command. Logging in to the ACS server places you in the Operator (user) mode or the Admin (EXEC) mode. Typically, logging in requires a username and password.

You can always tell when you are in the Operator (user) mode or Admin (EXEC) mode by looking at the prompt. A right angle bracket (>) appears at the end of the Operator (user) mode prompt; a pound sign (#) appears at the end of the Admin mode prompt, regardless of the submode.

Three command modes are available on the CLI:

- EXEC: EXEC commands primarily include system-level commands such as show and reload (for example, application installation, application start and stop, copy files and installations, restore backups, and display information). In addition, certain EXEC-mode commands have ACS-specific abilities (for example, start an ACS instance, display and export ACS logs, and reset an ACS configuration to factory default settings).
- ACS Configuration: Commands in this mode can be used to set the debug log level for the ACS management and runtime components, show system settings, reset server certificates and IP address access lists, and manage import and export processes. To access the ACS configuration mode, run the acs-config command in EXEC mode as demonstrated in Example 4-1.

Example 4-1 ACS CLI—Changing to ACS Configuration Mode

```
ACS51/admin# acs-config
Escape character is CNTL/D.
Username: ACSAdmin
Password:
ACS51/ACSAdmin(config-acs)#
```

Configuration: Commands in this mode can be used to configure various system options such as interface, repository, SNMP server, and NTP, among others. To access the Configuration mode, run the configure command in EXEC mode as demonstrated in Example 4-2.

Example 4-2 ACS CLI—Changing to Configuration Mode

```
ACS51/admin# configure
Enter configuration commands, one per line. End with CNTL/Z.
ACS51/admin(config)#
```

It is not possible to cover all the commands available in the CLI. The list that follows highlights a few important tasks and their related commands:

Starting and Stopping ACS Services: ACS services can be started or stopped from the EXEC mode using the acs {start | stop} command.

- **Reset ACS Configuration:** To reset ACS configuration to the factory default, use the **acs reset-config** command at the EXEC mode.
- **Reset ACSAdmin Password:** To reset the password of the default GUI admin, use the **acs reset-password** command from the EXEC mode.
- Verify Configuration: To see the current configuration, use the show running-config command from the EXEC mode.
- Verify Version Information: To see the current version, use the show version command from the EXEC mode.
- Verify Status of ACS Processes: To verify the status of the ACS processes, use the show application status acs EXEC command.
- **Troubleshoot Connectivity:** To troubleshoot network connectivity, use the **ping** *ip address or hostname*, **traceroute** *ip address or hostname*, and **nslookup** *ip address or hostname* commands from the EXEC mode.
- Change IP Address: To change the IP address of the interface, use the ip address *ip address subnet mask* command in the Interface mode. To go to the Interface mode, use the interface GigabitEthernet 0 command in the Configuration mode.
- Add a Route: To add a route to the routing table of ACS, use the **ip route** *networkaddress netmask* **gateway** *gateway-address* command in the Configuration mode.
- Disable ICMP Echo Response: To stop the device from sending ICMP echo responses to echo requests received, use the icmp echo off command. Use icmp echo on command to enable the device to send echo responses.
- Change Hostname: To change the hostname of the server, use the hostname *name* command in the Configuration mode.

For more details on ACS CLI commands, see the "CLI Reference Guide for the Cisco Secure Access Control System 5.1."

Summary

At this point, you should be familiar with the interface of ACS 5.1 and the process of adding and creating different elements. Remember the flow of adding network devices and users, creating policy elements and access services. You are now prepared to add external user repositories and create complex access services for different AAA scenarios.

This page intentionally left blank

INDEX

Numerics

802.1x accounting, 214 802.1x authentication, 196-197 Cisco switches, configuring, 204-206 configuring on APs, 257-258 guest VLAN, configuring, 209 MAB, configuring, 210-211 message exchange, 200-201 multidomain authentication mode, 207-208 multiple-host mode, 207 pre-authentication open access mode, 208 restricted VLAN, configuring, 209-210 single-host mode, 206-207 timers, 212-213 troubleshooting, 250-251, 275-279 VLAN assignment, configuring, 211-212

A

AAA

accounting, configuring with Cisco IOS, 173-174 authentication, configuring with Cisco IOS, 157-161 authorization, configuring with Cisco IOS, 161-166 Access Policies drawer (ACS 5.1 interface), 105-116 access services, 107-116 accounting, 6-8 ASA/PIX, configuring, 191-192 Authentication Proxy, 326 configuring, 214 configuring with Cisco IOS, 173-174 cut-through proxy accounting, configuring, 303-304 PPP sessions on Cisco IOS, 350 remote access VPNs, 342 VPNs with RADIUS, 359

ACS 4.2 (Cisco Access Control Server 4.2), 23-28 Active Directory, configuring, 128-131 Authentication Proxy authorization, 318-319 configuring, 315 backup and restore, configuring, 376-378 certificates, installing, 215-218 command authorization, configuring, 168-173 cut-through proxy authentication, configuring, 290 database replication, 378-383 EAP-FAST, configuring, 265-267 external databases, 125-126 group mapping, configuring, 141-142 identity stores, 125-126 installing, 32-47 problems, troubleshooting, 52-55 interface Administration Control. 61-64 Advanced Options section, 69-70 External User Databases section. 78-79 Group Setup section, 74-76 Interface Configuration section, 66-68 Network Access Profiles section, 65 *Network Configuration section,* 64-65 Reports and Activity section, 79-82 Shared Profile Components section, 78-79 System Configuration section, 76-79

TACACS+ Settings section, 68-69 User Setup section, 70-74 LDAP, configuring, 134-136 LEAP, configuring, 263-264 local password management, 391-392 log file management, configuring, 394-395 NAPs, configuring, 388-391 NARs, 376-376 **RDBMS** Synchronization feature, 384-388 remote logging, configuring, 391-393 RSA SecureID, configuring, 140 services, 58-61 VLAN assignment, configuring, 228 ACS 5.1 (Cisco Access Control System 5.1), 28-32 Active Directory, configuring, 132-133 Authentication Proxy, authorization, 319-321 certificates, installing, 219-223 command authorization, configuring, 168-173 cut-through proxy authentication, configuring, 290 database replication, configuring, 404-405 dictionaries, 405-409 EAP-FAST, configuring, 266-268 EAP-MD5, configuring, 223-224 external databases, 126-128 group mapping, configuring, 142-148 identity stores, 126-128 initial setup, 47-51 installation problems, troubleshooting, 52-55

interface Access Policies drawer, 105-116 CLI. 120-122 Monitoring and Reports drawer, 117-120 *My Workspace drawer*, 86-87 Network Resources drawer. 87-94 Policy Elements drawer, 98-105 Users and Identity Stores *drawer*. 94-98 LDAP, configuring, 137-139 LEAP, configuring, 264-265 licensing, 51-52 network resources, importing, 412-414 remote logging, configuring on ACS 5.1. 409-412 RSA SecureID, configuring, 140-141 scheduled backups, configuring, 427-430 software repositories, creating, 422-425 system administration, 415-422 VLAN assignment, configuring, 229 activating secondary servers on ACS 5.1. 402-406 Active Directory, configuring on ACS 4.2, 128-131 on ACS 5.1, 132-133 add-on license, ACS 5.1, 52 Administration Control section (ACS 4.2 interface), 61-64 administrative access, ASA/PIX, 180 Advanced Options section (ACS 4.2 interface), 69-70 APs, 802.1x authentication, 257-258

ASA/PIX

accounting, configuring, 191-192 authentication, configuring, 186-188 authorization, configuring, 188-191 cut-through proxy authentication, configuring, 282-285 HTTP redirection, configuring. 288-290 local database, 180 privilege levels, 180-182 Virtual HTTP, configuring, 287-288 Virtual Telnet, configuring, 286-287 authentication, 2-4 802.1x authentication, 196-197 on Cisco switches, 204-206 multiple-bost mode (802.1x), 207 single-host mode, 206-207 timers. 212-213 troubleshooting, 275-279 WLCs, configuring, 259-263 ASA/PIX, configuring, 186-188 configuring with Cisco IOS, 157-161 cut-through proxy authentication configuring, 282-285 troubleshooting, 291-292 EAP, 201-204 example, 4 IPsec VPNs with Cisco IOS, 334-335 PPP sessions on Cisco IOS, 345-347 SSL VPNs with Cisco IOS, 335-336 troubleshooting, 159-160 of VPNs with LDAP. 362-364 with RADIUS, 2001-356 troubleshooting, 337

Authentication Proxy accounting, 326 authorization ACS 4.2. 318-319 troubleshooting, 325-326 cache, maintaining, 315-316 for FTP sessions, configuring, 312-314 for HTTP sessions, configuring, 311-312 lab scenario, 326-329 prerequisites, 310-311 for Telnet sessions, configuring, 314-315 troubleshooting, 316-317 authorization, 4-6 802.1x authentication, message exchange, 200-201 ASA/PIX, configuring, 188-191 Authentication Proxy, troubleshooting, 325-326 command authorization, configuring, 166-173 configuring with Cisco IOS, 161-166 cut-through proxy authorization, 294-303 PPP sessions on Cisco IOS, 348 troubleshooting, 349-350 VPNs with Cisco IOS, 337-342 with LDAP. 364-366 with RADIUS, 356-359 authorization policies, configuring, 113-115 Auth-Proxy, 3

B

backup and restore on ACS 4.2, configuring, 376-378 on ACS 5.1, configuring, 421-427

С

cache (Authentication Proxy), maintaining, 315-316 certificates, installing on ACS 4.2, 215-218 on ACS 5.1, 219-223 Cisco IOS AAA authentication, configuring, 157-161 accounting, configuring, 173-174 Authentication Proxy for FTP sessions, 312-314 for HTTP sessions, 311-312 for Telnet sessions, 314-315 troubleshooting, 316-317 authorization, configuring, 161-166 command authorization, configuring, 166 - 173IPsec VPNs, authentication, 334-335 local database configuring, 151-152 privilege levels, 152-153 PPP sessions accounting, 350 authentication, 345-347 privilege levels, lab scenario, 154-155 VPNs, authorization, 342

Cisco switches, configuring 802.1x authentication, 204-206 classification of network requests, 389 CLI drawer (ACS 5.1 interface), 120-122 command authorization configuring with Cisco IOS, 166-173 troubleshooting, 172-173 commands, show commands, 249-250 configuring 802.1x authentication. 257-258 on Cisco switches, 204-206 guest VLAN feature, 209 MAB. 210-211 restricted VLAN feature, 209-210 VLAN assignment, 211-212 accounting, 214 ACS 4.2 backup and restore features, 376-378 database replication, 378-383 local password management, 391-392 log file management, 394-395 NAPs. 388-391 NARs. 375-376 **RDBMS** Synchronization feature, 384-388 remote logging, 391-393 ACS 5.1 backup and restore features, 421-427 database backup, 425-427 database replication, 404-405 dictionaries, 405-409

remote logging, 409-412 scheduled backups, 427-430 system administration, 415-422 Active Directory on ACS 4.2, 128-131 on ACS 5.1. 132-133 ASA/PIX accounting, 191-192 authentication, 186-188 authorization, 188-191 HTTP redirection, 288-290 Virtual HTTP. 287-288 Virtual Telnet, 286-287 Authentication Proxy for FTP sessions, 312-314 for HTTP sessions, 311-312 for Telnet sessions, 314-315 authentication with Cisco IOS. 157-161 authorization policies, 113-115 authorization with Cisco IOS. 161-166 Cisco IOS, local database, 151-152 cut-through proxy accounting, 303-304 cut-through proxy authentication, 282-285, 290 cut-through proxy authorization, 294-303 exec authorization, 161-166 group mapping on ACS 4.2, 141-142 on ACS 5.1, 142-148 identity policies, 110-113

LDAP on ACS 4.2, 134-136 on ACS 5.1. 137-139 RSA SecureID on ACS 4.2. 140 on ACS 5.1, 140-141 creating service selection rules, 115-116 CSAdmin service (ACS 4.2), 59 CSAuth service (ACS 4.2), 59 CSDBSync service (ACS 4.2), 59-60 CSLog service (ACS 4.2), 60 CSMon service (ACS 4.2), 60 CSRadius service (ACS 4.2), 60 CSTacacs service (ACS 4.2), 60-61 CSUtil database utility (ACS 4.2), 395-400 cut-through proxy accounting, configuring, 303-304 cut-through proxy authentication configuring, 282-285, 290 troubleshooting, 291-292 cut-through proxy authorization, 294-303

D

database replication, 378-383 on ACS 5.1, 404-405 databases, backing up with ACS 5.1, 425-427 dictionaries, configuring on ACS 5.1, 405-409

E

EAP, 197-199 types of, 201-204 EAP-FAST, 202-203 ACS 4.2, configuring, 265-267 ACS 5.1, configuring, 266-268 EAP-GTC, 203 EAP-MD5. 201 ACS 5.1, configuring, 223-224 EAPOL. 199-200 EAP-TLS. 202 ACS configuration, 226-227 evaluation license, ACS 5.1, 52 exec authorization, configuring, 161-166 external databases ACS 4.2. 125-126 ACS 5.1, 126-128 External User Databases section (ACS 4.2 interface), 78-79

F

FTP sessions, configuring Authentication Proxy, 312-314

G

group mapping, configuring on ACS 4.2, 141-142 on ACS 5.1, 142-148 Group Setup section (ACS 4.2 interface), 74-76 guest VLAN feature (802.1x), configuring, 209

H

HTTP redirection, configuring, 288-290

HTTP sessions

authentication and authorization lab scenario, 176-177

Authentication Proxy, configuring, 311-312

identity policies, configuring, 110-113 identity stores ACS 4.2, 125-126 ACS 5.1, 126-128 importing network resources (ACS 5.1), 412-414 initial setup, ACS 5.1, 47-51 installing ACS 4.2, 32-47 problems, troubleshooting, 52-55 certificates on ACS 4.2, 215-218 on ACS 5.1, 219-223 Interface Configuration section (ACS 4.2 interface), 66-68 **IPSec VPNs** accounting, with RADIUS, 359 authentication with Cisco IOS, 334-335 with LDAP, 362-364 authorization with Cisco IOS, 337-342 with LDAP. 364-366

lab scenarios 802.1x authentication configuring using EAP-FAST, 273-274 configuring using EAP-TLS, 249-250 configuring using LEAP, 269-273 configuring using MD-5, 230-245 configuring using PEAP, 245-248 AAA on ASA using TACACS+, 192-194 authentication and authorization of HTTP sessions, 176-177 Authentication Proxy, 326-329 cut-through proxy authentication, 292-294 cut-through proxy authentication, authorization, and accounting, 304-308 local authentication and privilege levels on ASA, 183-184 TACACS+ authentication. authorization, and accounting of administrative sessions, 174-176 VPN AAA with Cisco IOS, 343-345 with RADIUS, 359-361 VPN authentication and authorization with LDAP. 367-369

LDAP (Lightweight Directory Access Protocol) configuring on ACS 4.2, 134-136 on ACS 5.1. 137-139 VPNs authentication, 362-364 authorization, 364-366 LEAP. 201-202 ACS 4.2, configuring, 263-264 ACS 5.1, configuring, 264-265 licensing, ACS 5.1, 51-52 local database ASA/PIX. 180 configuring with Cisco IOS, 151-152 privilege levels, 152-153 local password management (ACS 4.2), 391-392 log file management, configuring on ACS 4.2, 394-395

Μ

MAB (MAC Authentication Bypass), configuring, 210-211 maintaining Authentication Proxy cache, 315-316 manual backups, performing on ACS 4.2, 377-378 message exchange in 802.1x authentication, 200-201 method lists, 3, 162 Monitoring and Reports drawer (ACS 5.1 interface), 117-120 multiauthentication mode (802.1x), 208 multidomain authentication mode (802.1x), 207-208 multiple-host mode (802.1x), 207 My Workspace drawer (ACS 5.1 interface), 86-87

N

NAPs (Network Access Profiles), configuring on ACS 4.2, 388-391 NARs (Network Access Restrictions), on ACS 4.2, 375-376 Network Access Profiles section (ACS 4.2 interface), 65 Network Configuration section (ACS 4.2 interface), 64-65 Network Resources drawer (ACS 5.1 interface), 87-94 network resources, importing (ACS 5.1), 412-414 NFR (Not-For-Resale) license (ACS 5.1), 52

Ρ

passwords, local password management (ACS 4.2), 391-392 PEAP, 202, 203 ACS configuration, 224-225 policies (NAP), 389-391 Policy Elements drawer (ACS 5.1 interface), 98-105 PPP sessions accounting on Cisco IOS, 350 authenticating on Cisco IOS, 345-347 troubleshooting, 347-348 authorization on Cisco IOS. 348 troubleshooting, 349-350 pre-authentication open access mode (802.1x), 208 prerequisites for Authentication Proxy, 310-311 primary servers, configuring replication, 381-382 privilege levels, ASA/PIX, 180-182 privilege levels (Cisco IOS), 152-153 lab scenario, 154-155 profiles, configuring on ACS 4.2, 388-391

R

RADIUS, 8-12

Authentication Proxy, authorization, 322-325
dictionaries, configuring on ACS 5.1, 405-409
PPP sessions, authorization, 348
VPNs, authentication, 355-356

RDBMS Synchronization feature, configuring on ACS 4.2, 384-388
recovering ACS from backup file, 378-379

remote access VPNs accounting, 343 authentication with RADIUS, 355-356 authorization with RADIUS, 356-359 remote logging configuring on ACS 4.2, 391-393 configuring on ACS 5.1, 409-412 replication versus backup, 381 **Reports and Activity section** (ACS 4.2 interface), 79-82 restricted VLAN (802.1x), configuring, 209-210 RSA SecureID, configuring on ACS 4.2, 140 on ACS 5.1, 140-141

S

scheduled backups configuring on ACS 5.1, 427-430 performing on ACS 4.2, 378 secondary servers activating (ACS 5.1), 402-406 replication, configuring, 383 service selection rules, creating, 115-116 services, ACS 4.2, 58-61 Shared Profile Components section (ACS 4.2 interface), 78-79 show commands, 249-250 single-host mode (802.1x), 206-207 software repositories, creating with ACS 5.1, 422-425 SSL VPNs accounting, 343 with RADIUS, 359 authentication with Cisco IOS, 335-336 with LDAP, 362-364 with RADIUS, 355-356 authorization with Cisco IOS, 337-342 with LDAP, 364-366 with RADIUS, 356-359 system administration on ACS 5.1, 415-422 System Configuration section (ACS 4.2 interface), 76-79

Т

TACACS+13-19

- Authentication Proxy, authorization, 318-321
- dictionaries, configuring on ACS 5.1, 405-409
- lab scenarios, authentication, authorization, and accounting of administrative sessions, 174-176

TACACS+ Setting section (ACS 4.2 interface), 68-69

Telnet

Authentication Proxy, configuring, 314-315 Virtual Telnet, 286-287

timers (802.1x), 212-213

troubleshooting 802.1x, 250-251 802.1x authentication, 275-279 ACS 4.2 installation, 52-55 authentication, 159-160 of VPNs, 337 Authentication Proxy, 316-317 authorization, 325-326 command authorization, 172-173 cut-through proxy authentication, 291-292 cut-through proxy authorization, 302-303 PPP sessions authorization, 349-350 on Cisco IOS, 347-348 VPN authentication with LDAP. 363-364 with RADIUS, 355-356 VPN authorization with Cisco IOS, 342 with LDAP. 366

U

User Setup section (ACS 4.2 interface), 70-74

Users and Identity Stores drawer (ACS 5.1 interface), 94-98

V

verifying cut-through proxy authentication, 291-292 Virtual HTTP, configuring, 287-288 Virtual Telnet, 286-287 VLAN assignment ACS configuration, 228-229 configuring, 211-212 **VPNs** accounting, 343 authentication with LDAP. 362-364 with RADIUS, 355-356 authorization with Cisco IOS, 337-342 with RADIUS, 356-359 troubleshooting, 342

W

Windows, CSUtil database utility, 395-400 wireless, 802.1x authentication configuring, 257-258 WLCs, configuring, 259-263 WLCs, configuring 802.1x authentication, 259-263 This page intentionally left blank

· **· | · · · | · ·** cisco .

ciscopress.com: Your Cisco Certification and Networking Learning Resource



Subscribe to the monthly Cisco Press newsletter to be the first to learn about new releases and special promotions.

Visit ciscopress.com/newsletters.

While you are visiting, check out the offerings available at your finger tips.

-Free Podcasts from experts:

- OnNetworking
- OnCertification
- OnSecurity

View them at ciscopress.com/podcasts.

- -Read the latest author **articles** and **sample chapters** at **ciscopress.com/articles**.
- -Bookmark the Certification Reference Guide available through our partner site at informit.com/certguide.



Connect with Cisco Press authors and editors via Facebook and Twitter, visit informit.com/socialconnect.


Try Safari Books Online FREE

Get online access to 5,000+ Books and Videos





FREE TRIAL—GET STARTED TODAY! www.informit.com/safaritrial

Find trusted answers, fast

Only Safari lets you search across thousands of best-selling books from the top technology publishers, including Addison-Wesley Professional, Cisco Press, O'Reilly, Prentice Hall, Que, and Sams.

Master the latest tools and techniques

In addition to gaining access to an incredible inventory of technical books, Safari's extensive collection of video tutorials lets you learn from the leading video training experts.

WAIT, THERE'S MORE!



Keep your competitive edge

With Rough Cuts, get access to the developing manuscript and be among the first to learn the newest technologies.

Stay current with emerging technologies

Short Cuts and Quick Reference Sheets are short, concise, focused content created to get you up-to-speed quickly on new and cutting-edge technologies.

