CCIE Professional Development

Network Security
Technologies and Solutions

A comprehensive, all-in-one reference for Cisco network security

Yusuf Bhaiji, CCIE No. 9305
CCIE Professional Development

Network Security
Technologies and Solutions

Yusuf Bhaiji, CCIE No. 9305
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 e-mail 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
Associate Publisher Dave Dusthimer
Cisco Representative Anthony Wolfenden
Cisco Press Program Manager Jeff Brady
Executive Editor Brett Bartow
Managing Editor Patrick Kanouse
Development Editor Betsey Henkels
Project Editor San Dee Phillips
Copy Editor Barbara Hacha
Technical Editors Nairi Adamian, Kevin Hofstra, Gert DeLaet
Editorial Assistant Vanessa Evans
Book and Cover Designer Louisa Adair
Composition Mark Shirar
Indexer Tim Wright
Proofreader Karen A. Gill
About the Author

Yusuf Bhaiji, CCIE No. 9305 (Routing and Switching and Security), has been with Cisco for seven years and is currently the program manager for the Cisco CCIE Security Certification and CCIE proctor in Cisco Dubai Lab. Prior to this, he was technical lead for the Sydney TAC Security and VPN team. Yusuf’s passion for security technologies and solutions has played a dominant role in his 17 years of industry experience, from as far back as his initial master’s degree in computer science, and has since been reflected in his numerous certifications.

Yusuf prides himself in his knowledge-sharing abilities, which are evident in the fact that he has mentored many successful candidates, as well as having designed and delivered a number of Network Security solutions around the globe.

Yusuf is an advisory board member of several nonprofit organizations for the dissemination of technologies and promotion of indigenous excellence in the field of internetworking through academic and professional activities. Yusuf chairs the Networkers Society of Pakistan (NSP) and IPv6 Forum Pakistan chapter.

Yusuf has also authored a Cisco Press publication titled *CCIE Security Practice Labs* (ISBN 1587051346), released in early 2004. He has been a technical reviewer for several Cisco Press publications and written articles, white papers, and presentations on various security technologies. He is a frequent lecturer and well-known speaker presenting in several conferences and seminars worldwide.

About the Technical Reviewers

Nairi Adamian, CCIE Security No. 10294, has been with Cisco since 1999 and currently is a technical support manager at Cisco, Australia. She leads a team of customer support engineers at the Cisco Technical Assistance Center (TAC). She holds a bachelor’s degree in computing science from University of Technology, Sydney, and has an MBA from Macquarie Graduate School of Management.

Kevin Hofstra, CCIE No. 14619, CCNP, CCDP, CCSP, CCVP, manages a network engineering unit within the Air Force Communications Agency of the U.S. Department of Defense. Mr. Hofstra is responsible for designing, implementing, and optimizing DoD networks and has deployed as a civilian engineer to Iraq, Kuwait, and Qatar in support of Operation Iraqi Freedom. Mr. Hofstra has a computer science degree from Yale University and a master of engineering degree in telecommunications and a master of engineering management degree from the University of Colorado.

Gert DeLaet, CCIE No. 2657, is a product manager for the CCIE team at Cisco. Gert was a contributing author to *CCIE Security Exam Certification Guide* and *CCDA Exam Certification Guide* from Cisco Press. He resides in Brussels, Belgium.
Dedications
This book is dedicated to my beloved wife, Farah. Without her support and encouragement, I could not have completed this book.

Acknowledgments
I would like to thank my family for all their continuous support and encouragement, and especially my father, Asghar Bhaiji, for his wisdom. Last but not least, I reminisce about my mother, Khatija Bhaiji, whose love is ever shining on me.

I would like to especially thank the technical reviewers, Nairi Adamian, Gert DeLaet, and Kevin Hofstra, who have done an amazing job in contributing to this book. Their valuable feedback and efforts to research each topic are greatly appreciated in the accomplishment of this project.

I extend my sincere gratitude to Brett Bartow and the entire development team—Betsey Henkels, Dayna Isley, Barbara Hacha, San Dee Phillips, Chris Cleveland, and members of the Cisco Press team working on this project, whose expert guidance has been a determining factor in the completion of this book.

I would like to take this opportunity to thank my manager, Sarah DeMark, the leadership team of Learning@Cisco group, and my colleagues at Cisco for their support in writing this book and every other project. I have benefited greatly from working with them and am honored to be a member of this team.

Finally, I would like to thank you, the reader of this book, for helping me to make this book a success.
This Book Is Safari Enabled

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

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

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

- Go to http://www.ciscopress.com/safarienabled
- Complete the brief registration form
- Enter the coupon code SJGV-KMZF-ENN5-ITFN-EYIT

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

Foreword xxxii
Introduction xxxiii

Part I Perimeter Security 3
Chapter 1 Overview of Network Security 5
Chapter 2 Access Control 21
Chapter 3 Device Security 53
Chapter 4 Security Features on Switches 83
Chapter 5 Cisco IOS Firewall 113
Chapter 6 Cisco Firewalls: Appliance and Module 139
Chapter 7 Attack Vectors and Mitigation Techniques 207

Part II Identity Security and Access Management 265
Chapter 8 Securing Management Access 267
Chapter 9 Cisco Secure ACS Software and Appliance 289
Chapter 10 Multifactor Authentication 311
Chapter 11 Layer 2 Access Control 325
Chapter 12 Wireless LAN (WLAN) Security 347
Chapter 13 Network Admission Control (NAC) 373

Part III Data Privacy 405
Chapter 14 Cryptography 407
Chapter 15 IPsec VPN 423
Chapter 16 Dynamic Multipoint VPN (DMVPN) 469
Chapter 17 Group Encrypted Transport VPN (GET VPN) 503
Chapter 18 Secure Sockets Layer VPN (SSL VPN) 521
Chapter 19 Multiprotocol Label Switching VPN (MPLS VPN) 533

Part IV Security Monitoring 559
Chapter 20 Network Intrusion Prevention 561
Chapter 21 Host Intrusion Prevention 613
Chapter 22 Anomaly Detection and Mitigation 639
Chapter 23 Security Monitoring and Correlation 669

Part V Security Management 697
Chapter 24 Security and Policy Management 699
Chapter 25 Security Framework and Regulatory Compliance 747

Index 770
Contents

Foreword xxxii
Introduction xxxiii

Part I Perimeter Security 3

Chapter 1 Overview of Network Security 5
  Fundamental Questions for Network Security 5
  Transformation of the Security Paradigm 7
  Principles of Security—The CIA Model 8
    Confidentiality 9
    Integrity 9
    Availability 9
  Policies, Standards, Procedures, Baselines, Guidelines 9
    Security Policy 9
    Examples of Security Policies 10
    Standards 11
    Procedures 11
    Baselines 12
    Guidelines 12
  Security Models 13
  Perimeter Security 13
    Is Perimeter Security Disappearing? 14
    The Difficulty of Defining Perimeter 14
    A Solid Perimeter Security Solution 14
  Security in Layers 15
    Multilayer Perimeter Solution 15
    The Domino Effect 16
  Security Wheel 17
  Summary 19
  References 19

Chapter 2 Access Control 21
  Traffic Filtering Using ACLs 21
    ACL Overview 21
    ACL Applications 21
    When to Configure ACLs 23
IP Address Overview 23
  Classes of IP Addresses 24
  Understanding IP Address Classes 24
  Private IP Address (RFC 1918) 26

Subnet Mask Versus Inverse Mask Overview 27
  Subnet Mask 28
  Inverse Mask 28

ACL Configuration 29
  Creating an ACL 29
  Assigning a Unique Name or Number to Each ACL 29
  Applying an ACL to an Interface 30
  Direction of the ACL 32

Understanding ACL Processing 32
  Inbound ACL 32
  Outbound ACL 33
  Packet Flow Rules for Various Packet Types 33
  Guidelines for Implementing ACLs 36

Types of Access Lists 36
  Standard ACLs 37
  Extended ACLs 38
  IP Named ACLs 39
  Lock and Key (Dynamic ACLs) 40
  Reflexive ACLs 42
  Established ACLs 43
  Time-Based ACLs Using Time Ranges 44
  Distributed Time-Based ACLs 45
  Configuring Distributed Time-Based ACLs 45
  Turbo ACLs 46
  Receive ACLs (rACL) 46
  Infrastructure Protection ACLs (iACL) 47
  Transit ACLs 47
  Classification ACLs 48
  Debugging Traffic Using ACLs 49

Summary 50

References 50

Chapter 3  Device Security 53
  Device Security Policy 53
  Hardening the Device 55
    Physical Security 55
Passwords  55
  Creating Strong Passwords  56
  Pass-Phrase Technique  56
  Password Encryption  57
  ROMMON Security  57
User Accounts  60
Privilege Levels  61
Infrastructure ACL  62
Interactive Access Methods  62
  Console Port  62
  VTY Ports  63
  VTY Access Using Telnet  63
  VTY Access Using SSH  64
  Auxiliary Port  65
Banner Messages  65
Cisco IOS Resilient Configuration  67
Cisco Discovery Protocol (CDP)  68
TCP/UDP Small-Servers  69
Finger  69
Identification (auth) Protocol  69
DHCP and BOOTP Service  69
Trivial File Transfer Protocol (TFTP) Server  70
File Transfer Protocol (FTP) Server  70
Autoloading Device Configuration  70
PAD  70
IP Source Routing  71
Proxy Address Resolution Protocol (ARP)  71
Gratuitous ARP  72
IP Directed Broadcast  72
IP Mask Reply  72
IP Redirects  72
ICMP Unreachable  73
HTTP  73
Network Time Protocol (NTP)  74
Simple Network Management Protocol (SNMP)  75
Auto-Secure Feature  75
Securing Management Access for Security Appliance  76
  PIX 500 and ASA 5500 Security Appliance—Device Access Security  76
    Telnet Access  76
    SSH Access  77
  HTTPS Access for ADSM  77
    Authenticating and Authorizing Using Local and AAA Database  78
IPS 4200 Series Appliance Sensors (formerly known as IDS 4200) 78
  IPS Device Manager (IDM) 78
  HTTP/HTTPS Access 79
  Telnet and SSH Access 79
  Access Control List 79
  User Accounts 80

Device Security Checklist 80

Summary 81

References 81

Chapter 4

Security Features on Switches 83

Securing Layer 2 83

Port-Level Traffic Controls 84
  Storm Control 84
  Protected Ports (PVLAN Edge) 85

Private VLAN (PVLAN) 85
  Configuring PVLAN 89
  Port Blocking 91
  Port Security 92

Access Lists on Switches 94
  Router ACL 94
  Port ACL 94
  VLAN ACL (VACL) 95
    VACL on a Bridged Port 95
    VACL on a Routed Port 95
    Configuring VACL 96
  MAC ACL 97

Spanning Tree Protocol Features 98
  Bridge Protocol Data Unit (BPDU) Guard 98
  Root Guard 98
  EtherChannel Guard 99
  Loop Guard 99

Dynamic Host Configuration Protocol (DHCP) Snooping 100

IP Source Guard 102

Dynamic ARP Inspection (DAI) 103
  DAI in a DHCP Environment 105
  DAI in a Non-DHCP Environment 106
  Rate Limiting Incoming ARP Packets 106
  ARP Validation Checks 107
Advanced Integrated Security Features on High-End Catalyst Switches 107
Control Plane Policing (CoPP) Feature 107
CPU Rate Limiters 109
Layer 2 Security Best Practices 109
Summary 110
References 111

Chapter 5
Cisco IOS Firewall 113
Router-Based Firewall Solution 113
Context-Based Access Control (CBAC) 115

CBAC Functions 116
  Traffic Filtering 116
  Traffic Inspection 116
  Alerts and Audit Trails 117

How CBAC Works 117
  Packet Inspection 118
  Timeout and Threshold Values 118
  The Session State Table 118
  UDP Connections 119
  Dynamic ACL Entries 119
  Embryonic (Half-Open) Sessions 120
  Per-Host DoS Prevention 120

CBAC-Supported Protocols 121

Configuring CBAC 122
  Step 1—Select an Interface: Internal or External 122
  Step 2—Configure an IP Access List 123
  Step 3—Define an Inspection Rule 123
  Step 4—Configure Global Timeouts and Thresholds 123
  Step 5—Apply the Access List and the Inspection Rule to an Interface 125
  Step 6—Verifying and Monitoring CBAC 126

Putting It All Together 126

IOS Firewall Advanced Features 127
  HTTP Inspection Engine 127
  E-Mail Inspection Engine 128
  Firewall ACL Bypass 129
  Transparent IOS Firewall (Layer 2) 130
  Virtual Fragmentation Reassembly (VFR) 130
  VRF-Aware IOS Firewall 131
  Inspection of Router-Generated Traffic 131
Zone-Based Policy Firewall (ZFW) 132
  Zone-Based Policy Overview 132
  Security Zones 133
  Configuring Zone-Based Policy Firewall 134
  Configuring ZFW Using Cisco Policy Language (CPL) 134
  Application Inspection and Control (AIC) 136

Summary 137

References 137

Chapter 6
Cisco Firewalls: Appliance and Module 139

Firewalls Overview 139

Hardware Versus Software Firewalls 140

Cisco PIX 500 Series Security Appliances 140

Cisco ASA 5500 Series Adaptive Security Appliances 142

Cisco Firewall Services Module (FWSM) 143

Firewall Appliance Software for PIX 500 and ASA 5500 144

Firewall Appliance OS Software 145

Firewall Modes 145
  Routed Firewall Mode 146
  Transparent Firewall Mode (Stealth Firewall) 146

Stateful Inspection 148

Application Layer Protocol Inspection 148

Adaptive Security Algorithm Operation 150

Security Context 152
  Multiple Contexts—Routed Mode (with Shared Resources) 153
  Multiple Contexts—Transparent Mode 153
  Configuring Security Context 155

Security Levels 157

Redundant Interface 158

IP Routing 159
  Static and Default Routes 159
    Static Route 160
    Static Route Tracking 160
    Default Route 161
    Equal Cost Multiple Path (ECMP) Forwarding 162
Open Shortest Path First (OSPF) 163
  Configuring OSPF 164
  Securing OSPF 165
  Monitoring OSPF 166
Routing Information Protocol (RIP) 167
  Configuring RIP 167
Enhanced Interior Gateway Routing Protocol (EIGRP) 168
  Configuring EIGRP Stub Routing 169
  Securing EIGRP 169

Network Address Translation (NAT) 170
  NAT Control 171
  NAT Types 172
  Dynamic NAT 173
  Dynamic PAT 174
  Configure Dynamic NAT and PAT 176
  Static NAT 176
  Static Port Address Translation (PAT) 178
Bypassing NAT When NAT Control Is Enabled 179
  Identity NAT (nat 0 Command) 179
  Static Identity NAT (static Command) 180
  NAT Exemption (nat 0 with ACL) 182
Policy NAT 183
  Order of NAT Processing 184

Controlling Traffic Flow and Network Access 185
  ACL Overview and Applications on Security Appliance 185
  Controlling Inbound and Outbound Traffic Through the Security Appliance by
  Using Access Lists 186
    Step 1—Defining an Access List 186
    Step 2—Applying an Access List to an Interface 186
  Simplifying Access Lists with Object Groups 188

Modular Policy Framework (MPF) 190
  Configuring MPF 190
    Step 1—Identifying Traffic Flow 190
    Step 2—Creating a Policy Map 191
    Step 3—Applying a Policy 191

Cisco AnyConnect VPN Client 192

Redundancy and Load Balancing 193
  Failover Requirements 194
  Failover Link 194
  State Link 194
Implementing AAA 278
AAA Methods 279
  Authentication Methods 280
  Authorization Methods 280
  Accounting Methods 281
Server Groups 281
Service Types for AAA Functions 282
  Authentication Services 282
  Authorization Services 283
  Accounting Service 284
Configuration Examples 285
  PPP Authentication, Authorization, and Accounting Using RADIUS 285
  Login Authentication and Command Authorization and Accounting Using TACACS+ 285
  Login Authentication with Password Retry Lockout 286
Summary 287
References 287

Chapter 9  Cisco Secure ACS Software and Appliance 289
  Cisco Secure ACS Software for Windows 289
    AAA Server: Cisco Secure ACS 290
    Protocol Compliance 291
  Advanced ACS Functions and Features 293
    Shared Profile Components (SPC) 293
    Downloadable IP ACLs 293
    Network Access Filter (NAF) 294
    RADIUS Authorization Components 294
    Shell Command Authorization Sets 294
    Network Access Restrictions (NAR) 295
    Machine Access Restrictions (MAR) 295
    Network Access Profiles (NAP) 296
    Cisco NAC Support 296
Configuring ACS 297
Cisco Secure ACS Appliance 307
Summary 309
References 309
Chapter 10  Multifactor Authentication  311

Identification and Authentication  311

Two-Factor Authentication System  312
  One-Time Password (OTP)  312
  S/KEY  313
  Countering Replay Attacks Using the OTP Solution  313
  Attributes of a Two-Factor Authentication System  314
    Smart Cards and Tokens  314
    RSA SecurID  315

Cisco Secure ACS Support for Two-Factor Authentication Systems  315
  How Cisco Secure ACS Works  316
  Configuring Cisco Secure ACS for RADIUS-Enabled Token Server  317
  Configuring Cisco Secure ACS for RSA SecurID Token Server  321

Summary  322

References  322

Chapter 11  Layer 2 Access Control  325

Trust and Identity Management Solutions  326

Identity-Based Networking Services (IBNS)  327
  Cisco Secure ACS  328
  External Database Support  329

IEEE 802.1x  329
  IEEE 802.1x Components  330
  Port States: Authorized Versus Unauthorized  332
  EAP Methods  334

Deploying an 802.1x Solution  334
  Wired LAN (Point-to-Point)  334
  Wireless LAN (Multipoint)  335

Implementing 802.1x Port-Based Authentication  337
  Configuring 802.1x and RADIUS on Cisco Catalyst Switches Running Cisco IOS Software  337
    Enabling Multiple Hosts for a Noncompliant Access Point Terminating on the Switch  338
    RADIUS Authorization  338
  Configuring 802.1x and RADIUS on Cisco Aironet Wireless LAN Access Point Running Cisco IOS  342
  Supplicant Settings for IEEE 802.1x on Windows XP Client  343
IPsec Protocol Headers 432
IPsec Anti-Replay Service 434
ISAKMP and IKE 435
    Understanding IKE (Internet Key Exchange) Protocol 435
    IKEv2 (Internet Key Exchange—Version 2) 438
ISAKMP Profiles 441
IPsec Profiles 443
IPsec Virtual Tunnel Interface (IPsec VTI) 443

Public Key Infrastructure (PKI) 445
    PKI Components 446
    Certificate Enrollment 447

Implementing IPsec VPN 449
    Cisco IPsec VPN Implementations 449
Site-to-Site IPsec VPN 451
Remote Access IPsec VPN 455
    Cisco Easy VPN 456
    Dynamic VTI (DVTI) 461

Summary 465

References 466

Chapter 16 Dynamic Multipoint VPN (DMVPN) 469

DMVPN Solution Architecture 469
    DMVPN Network Designs 470
    DMVPN Solution Components 472
How DMVPN Works 473
DMVPN Data Structures 474

DMVPN Deployment Topologies 475

Implementing DMVPN Hub-and-Spoke Designs 476
    Implementing Single Hub Single DMVPN (SHSD) Topology 477
    Implementing Dual Hub Dual DMVPN (DHDD) Topology 483
    Implementing Server Load-Balancing (SLB) Topology 484

Implementing Dynamic Mesh Spoke-to-Spoke DMVPN Designs 486
    Implementing Dual Hub Single DMVPN (DHSD) Topology 488
    Implementing Multihub Single DMVPN (MHSD) Topology 498
    Implementing Hierarchical (Tree-Based) Topology 499

Summary 500

References 501
Chapter 17  Group Encrypted Transport VPN (GET VPN)  503

GET VPN Solution Architecture  503
GET VPN Features  504
Why GET VPN?  505
GET VPN and DMVPN  506
GET VPN Deployment Consideration  507
GET VPN Solution Components  507
How GET VPN Works  509
IP Header Preservation  511
Group Member ACL  512

Implementing Cisco IOS GET VPN  513

Summary  519

References  519

Chapter 18  Secure Sockets Layer VPN (SSL VPN)  521

Secure Sockets Layer (SSL) Protocol  521
SSL VPN Solution Architecture  522
SSL VPN Overview  523
SSL VPN Features  523
SSL VPN Deployment Consideration  524
SSL VPN Access Methods  525
SSL VPN Citrix Support  527

Implementing Cisco IOS SSL VPN  528
Cisco AnyConnect VPN Client  530

Summary  531

References  531

Chapter 19  Multiprotocol Label Switching VPN (MPLS VPN)  533

Multiprotocol Label Switching (MPLS)  533
MPLS Architecture Overview  534
How MPLS Works  534
MPLS VPN and IPsec VPN  536
Deployment Scenarios  538
Connection-Oriented and Connectionless VPN Technologies  539

MPLS VPN (Trusted VPN)  540

Comparison of L3 and L2 VPNs  540
Layer 3 VPN (L3VPN) 542
  Components of L3VPN 543
  How L3VPN Implementation Works 543
  How VRF Tables Work 543
Implementing L3VPN 544

Layer 2 VPN (L2VPN) 551
Implementing L2VPN 553
  Implementing Ethernet VLAN over MPLS Service—Using VPWS Based Architecture 553
  Implementing Ethernet VLAN over MPLS Service—Using VPLS-Based Architecture 554

Summary 556
References 557

Part IV  Security Monitoring 559
Chapter 20  Network Intrusion Prevention 561
  Intrusion System Terminologies 561
  Network Intrusion Prevention Overview 562
  Cisco IPS 4200 Series Sensors 563
  Cisco IDS Services Module (IDSM-2) 565
  Cisco Advanced Inspection and Protection Security Services Module (AIP-SSM) 567
  Cisco IPS Advanced Integration Module (IPS-AIM) 568
  Cisco IOS IPS 569
  Deploying IPS 570
  Cisco IPS Sensor OS Software 572
  Cisco IPS Sensor Software 574
    Sensor Software—System Architecture 574
    Sensor Software—Communication Protocols 575
    Sensor Software—User Roles 576
    Sensor Software—Partitions 577
    Sensor Software—Signatures and Signature Engines 578
    Sensor Software—IPS Events 580
    Sensor Software—IPS Event Actions 582
    Sensor Software—IPS Risk Rating (RR) 583
    Sensor Software—IPS Threat Rating 584
    Sensor Software—IPS Interfaces 585
Chapter 22  Anomaly Detection and Mitigation  639

Attack Landscape  639
   Denial-of-Service (DoS) Attack Defined  639
   Distributed Denial-of-Service (DDoS) Attack—Defined  641

Anomaly Detection and Mitigation Systems  641
Cisco DDoS Anomaly Detection and Mitigation Solution  643
Cisco Traffic Anomaly Detector  644
Cisco Guard DDoS Mitigation  647

Putting It All Together for Operation  649

Configuring and Managing the Cisco Traffic Anomaly Detector  653
   Managing the Detector  655
   Initializing the Detector Through CLI Console Access  655
   Configuring the Detector (Zones, Filters, Policies, and Learning Process)  656

Configuring and Managing Cisco Guard Mitigation  660
   Managing the Guard  661
   Initializing the Guard Using the CLI Console Access  661
   Configuring the Guard (Zones, Filters, Policies, Learning Process)  663

Summary  666

References  667

Chapter 23  Security Monitoring and Correlation  669

Security Information and Event Management  669

Cisco Security Monitoring, Analysis, and Response System (CS-MARS)  670
   Security Threat Mitigation (STM) System  672
   Topological Awareness and Network Mapping  674
   Key Concepts—Events, Sessions, Rules, and Incidents  676
   Event Processing in CS-MARS  677
   False Positive in CS-MARS  678

Deploying CS-MARS  679
   Standalone and Local Controllers (LC)  680
   Global Controllers (GC)  682
   Software Versioning Information  683
   Reporting and Mitigation Devices  684
   Levels of Operation  685
   Traffic Flows and Ports to Be Opened  687
Web-Based Management Interface 689
Initializing CS-MARS 691

Summary 693
References 694

Part V Security Management 697

Chapter 24 Security and Policy Management 699

Cisco Security Management Solutions 699

Cisco Security Manager 700
Cisco Security Manager—Features and Capabilities 700
Cisco Security Manager—Firewall Management 703
Cisco Security Manager—VPN Management 704
Cisco Security Manager—IPS Management 704
Cisco Security Manager—Platform Management 706
Cisco Security Manager—Architecture 706
Cisco Security Manager—Configuration Views 707
Cisco Security Manager—Managing Devices 710
Cisco Security Manager—Workﬂow Mode 710
Cisco Security Manager—Role-Based Access Control (RBAC) 711
Cisco Security Manager—Cross-Launch xDM 713
Cisco Security Manager—Supported Devices and OS Versions 715
Cisco Security Manager—Server and Client Requirements and Restrictions 716
Cisco Security Manager—Traffic Flows and Ports to Be Opened 719

Cisco Router and Security Device Manager (SDM) 721
Cisco SDM—Features and Capabilities 722
Cisco SDM—How It Works 723
Cisco SDM—Router Security Audit Feature 725
Cisco SDM—One-Step Lockdown Feature 726
Cisco SDM—Monitor Mode 728
Cisco SDM—Supported Routers and IOS Versions 729
Cisco SDM—System Requirements 730

Cisco Adaptive Security Device Manager (ASDM) 732
Cisco ASDM—Features and Capabilities 732
Cisco ASDM—How It Works 733
Cisco ASDM—Packet Tracer Utility 736
Cisco ASDM—Syslog to Access Rule Correlation 737
Cisco ASDM—Supported Firewalls and Software Versions 738
Cisco ASDM—User Requirements 738
Worldwide Outlook of Regulatory Compliance Acts and Legislations  765
  In the United States  765
  In Europe  766
  In the Asia-Pacific Region  766
Cisco Self-Defending Network Solution  767
Summary  767
References  768

Index  770
Icons Used in This Book

- PC
- Router
- Workgroup Switch
- Hub
- File Server
- Multilayer Switch
- Router with Firewall
- IOS Firewall
- PIX Firewall
- CS-MARS
- Access Server
- Secure Switch
- Wireless Access Point
- IP Phone
- NAC Appliance
- VPN Concentrator
- Optical Services Router
- Detector
- Web Cluster
- Secure Endpoints
- Cisco ASA 5500
- Secure Switch
- Secure Router
- Wireless Signal
- Serial Line
- Circuit Switched Line
- Line: Ethernet
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.
Foreword

With the explosion of the Internet economy, the continuous availability of mission-critical systems has never been more important. Network administrators through to business managers are expected by their customers, employees, and suppliers to provide constant network resource availability and access to critical applications and data in a completely secure environment. Not only is this a challenge, the stakes in breaching network security have never been higher.

*Network Security Technologies and Solutions* is a comprehensive, all-in-one reference for managing Cisco networks. It was written to help network security professionals understand and implement current, state-of-the-art network security technologies and solutions. Whether you are an expert in networking and security or a novice, this book is a valuable resource.

Many books on network security are based primarily on concepts and theory. *Network Security Technologies and Solutions*, however, goes far beyond that. It is a hands-on tool for configuring and managing Cisco market-leading dynamic links between customer security policy, user or host identity, and network infrastructures. The foundation of this book is based on key elements from the Cisco security solution. It provides practical, day-to-day guidance on how to successfully configure all aspects of network security, covering topics such as perimeter security, identity security and access management, and data privacy, as well as security monitoring and management.

Yusuf Bhaiji has been with Cisco for seven years and is currently the product manager for the Cisco CCIE Security certification track and a CCIE Proctor in Cisco Dubai Lab. Yusuf’s passion for security technologies and solutions is evident in his 17 years of industry experience and numerous certifications. Yusuf’s extensive experience as a mentor and advisor in the security technology field has honed his ability to translate highly technical information into a straightforward, easy-to-understand format. If you’re looking for a truly comprehensive guide to network security, this is the one!

Steve Gordon
Cisco Systems, Inc.
Vice President, Technical Services
Remote Operations Services and Learning@Cisco
Introduction

The Internet was born in 1969 as the ARPANET, a project funded by the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense. The Internet is a worldwide collection of loosely connected networks that are accessible by individual computers in varied ways, such as gateways, routers, dial-up connections, and through Internet service providers (ISP). Anyone today can reach any device/computer via the Internet without the restriction of geographical boundaries.

As Dr. Vinton G. Cerf states, “The wonderful thing about the Internet is that you’re connected to everyone else. The terrible thing about the Internet is that you’re connected to everyone else.”

The luxury of access to this wealth of information comes with its risks, with anyone on the Internet potentially being the stakeholder. The risks vary from information loss or corruption to information theft and much more. The number of security incidents is also growing dramatically.

With all this happening, a strong drive exists for network security implementations to improve security postures within every organization worldwide. Today’s most complex networks require the most comprehensive and integrated security solutions.

Security has evolved over the past few years and is one of the fastest-growing areas in the industry. Information security is on top of the agenda for all organizations. Companies need to keep information secure, and there is an ever-growing demand for the IT professionals who know how to do this.

Point products are no longer sufficient for protecting the information and require system-level security solutions. Linking endpoint and network security is a vital ingredient in designing the modern networks coupled with proactive and adaptive security systems to defend against the new breed of day-zero attacks.

Security is no longer simply an enabling technology or a one-time affair; it has become an essential component of the network blueprint. Security technologies and solutions need to be fundamentally integrated into the infrastructure itself, woven into the fabric of the network. Security today requires comprehensive, end-to-end solutions.

Goals and Methods

Cisco Network Security Technologies and Solutions is a comprehensive all-in-one reference book that covers all major Cisco Security products, technologies, and solutions. This book is a complete reference that helps networking professionals understand and implement current, state-of-the-art security technologies and solutions. The coverage is wide but deep enough to provide the audience with concepts, design, and implementation guidelines as well as basic configuration skills.

With an easy-to-understand approach, this invaluable resource will serve as a central warehouse of security knowledge to the security professionals with end-to-end security implementations.

The book makes no assumption of knowledge level, thereby ensuring that the readers have an explanation that will make sense and be comprehensible at the same time. It takes the reader from the fundamental level of each technology to more detailed descriptions and discussions of each subject.

With this definitive reference, the readers will possess a greater understanding of the solutions available and learn how to build integrated secure networks in today’s modern, heterogeneous infrastructure.
This book is comprehensive in scope, including information about mature as well as emerging technologies, including the Adaptive Security Appliance (ASA) Firewall Software Release 8.0, Cisco Intrusion Prevention System (IPS) Sensor Software Release 6.0, Host IPS, Cisco Group Encrypted Transport VPN (GETVPN), MPLS VPN technology, Cisco Distributed Denial-of-Service (DDoS) Anomaly Detection and Mitigation Solutions, Cisco Security Monitoring, Analysis, and Response System (CS-MARS), and Security Framework, Standards and Regulatory Compliance, to name a few.

Who Should Read This Book
Whether you are a network engineer or a security engineer, consultant, or candidate pursuing security certifications, this book will become your primary reference when designing and building a secure network.

Additionally, this book will serve as a valuable resource for candidates preparing for the CCIE Security certification exam that covers topics from the new blueprints.

The book will serve as a reference for any networking professional managing or considering exploring and implementing Cisco network security solutions and technologies.

How This Book Is Organized
This book is meant to complement the information already available on Cisco.com and in the Cisco security products documentation.

The book is divided into five parts, mapping Cisco security technologies and solutions into five key elements.

Part I, “Perimeter Security”: This element provides the means to control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Part I includes the following chapters:

- Chapter 2, “Access Control,” describes the capability to perform traffic filtering using access control lists (ACL). It covers numerous types of ACL, such as standard and extended ACL, Lock-and-key, Reflexive, Time-based, Receive ACL, Infrastructure ACL, and Transit ACL. The chapter addresses traffic filtering based on RFC standards and best common practices.
- Chapter 3, “Device Security,” covers some of the most common techniques used for device hardening and securing management access for routers, firewall appliances, and the intrusion prevention system (IPS) appliance.
- Chapter 4, “Security Features on Switches,” provides a comprehensive set of security features available on the switches. The chapter covers port-level security controls at Layer 2 and security features and best practices available on the switch.
- Chapter 5, “Cisco IOS Firewall,” introduces the software-based IOS firewall features, including the legacy Context-Based Access Control (CBAC) and the newly introduced Zone-Based Policy Firewall (ZFW) feature available on the router.
Chapter 6, “Cisco Firewalls: Appliance and Module,” covers the complete range of hardware-based Cisco firewall products, including Cisco PIX, Cisco ASA Firewall appliance, and Cisco Firewall Services Module (FWSM). The chapter provides comprehensive coverage of firewall operating systems (OS), software features, and capabilities.

Chapter 7, “Attack Vectors and Mitigation Techniques,” is a uniquely positioned chapter covering details of common types of attacks, and providing details of how to characterize and classify various attacks. The chapter provides mitigation techniques for a wide range of attacks at Layer 2 and Layer 3.

Part II, “Identity Security and Access Management”: Identity is the accurate and positive identification of network users, hosts, applications, services and resources. Part II includes the following chapters:

Chapter 8, “Securing Management Access,” covers details of the authentication, authorization, and accounting (AAA) framework and implementation of AAA technology. The chapter covers implementing the two widely used security protocols in access management: RADIUS and TACACS+ protocols.

Chapter 9, “Cisco Secure ACS Software and Appliance,” provides details of Cisco Secure Access Control Server (ACS) software that supports the AAA technology and security protocols covered in Chapter 8. The chapter highlights the commonly use ACS software functions and features.

Chapter 10, “Multifactor Authentication,” describes the identification and authentication mechanism using the multifactor authentication system. The chapter introduces common two-factor mechanisms.

Chapter 11, “Layer 2 Access Control,” covers the Cisco trust and identity management solution based on the Identity-Based Networking Services (IBNS) technique. The chapter provides details of implementing port-based authentication and controlling network access at Layer 2 using IEEE 802.1x technology.

Chapter 12, “Wireless LAN (WLAN) Security,” provides an overview of wireless LAN (WLAN) and details of securing WLAN networks. The chapter covers various techniques available to protect WLAN and expands on the various EAP protocols, including EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, and Cisco LEAP. The chapter also provides coverage of common WLAN attacks and mitigation techniques.

Chapter 13, “Network Admission Control (NAC)” provides details of Cisco Self-Defending Network (SDN) solution using the Cisco Network Admission Control (NAC) appliance-based and framework-based solutions. The chapter covers implementing the Cisco NAC appliance solution as well as the NAC-L3-IP, NAC-L2-IP, and NAC-L2-802.1x solutions.

Part III, “Data Privacy”: When information must be protected from eavesdropping, the capability to provide authenticated, confidential communication on demand is crucial. Employing security services at the network layer provides the best of both worlds. VPN solutions can secure communications using confidentiality, integrity, and authentication protocols between devices located anywhere on an untrusted or public network, particularly the Internet. Part III includes the following chapters:

Chapter 14, “Cryptography,” lays the foundation of data privacy and how to secure communication using crypto methodology and cryptographic solutions. The chapter gives a basic overview of various cryptographic algorithms, including hash algorithms, symmetric key, and asymmetric key algorithms.
• Chapter 15, “IPsec VPN,” is a comprehensive chapter covering a wide range of IPsec VPN solutions. The chapter provides various types of VPN deployment with focus on IPsec VPN technology covering IPsec protocols, standards, IKE, ISAKMP, and IPsec profiles. The chapter provides comprehensive coverage of implementing IPsec VPN solutions using various methods.

• Chapter 16, “Dynamic Multipoint VPN (DMVPN),” covers the dynamic multipoint VPN (DMVPN) solution architecture and describes the design, components, and how DMVPN works. The chapter provides coverage of implementing various types of DMVPN hub-and-spoke and spoke-to-spoke solutions.

• Chapter 17, “Group Encrypted Transport VPN (GET VPN),” covers the innovative tunnel-less VPN approach to provide data security. The chapter describes the newly introduced GET VPN technology, solution architecture, components, and how GET VPN works.

• Chapter 18, “Secure Sockets Layer VPN (SSL VPN),” describes the SSL-based VPN approach covering SSL VPN solution architecture and various types of SSL VPN. The chapter also covers the newly introduced Cisco AnyConnect VPN.

• Chapter 19, “Multiprotocol Label Switching VPN (MPLS VPN),” provides coverage of Multiprotocol Label Switching (MPLS)-based VPN technology to provide data security across MPLS networks. The chapter provides MPLS VPN solution architecture and various types of MPLS VPN technologies available. The chapter covers implementing Layer 2 (L2VPN) and Layer 3 (L3VPN)–based MPLS VPN solutions.

Part IV, “Security Monitoring”:

To ensure that a network remains secure, it’s important to regularly test and monitor the state of security preparation. Network vulnerability scanners can proactively identify areas of weakness, and intrusion detection systems can monitor and respond to security events as they occur. Using security monitoring solutions, organizations can obtain unprecedented visibility into both the network data stream and the security posture of the network. Part IV includes the following chapters:

• Chapter 20, “Network Intrusion Prevention,” covers network security monitoring using the network-based appliance sensor technology, Intrusion Prevention System (IPS). The chapter provides a comprehensive coverage of the sensor operating system (OS) software functions and features.

• Chapter 21, “Host Intrusion Prevention,” covers network security monitoring using the host-based technology, Host Intrusion Prevention System (HIPS). The chapter provides comprehensive details of Cisco Security Agent (CSA) technology providing solution architecture, components, and CSA deployment using CSA MC.

• Chapter 22, “Anomaly Detection,” provides coverage of anomaly-based security monitoring using Cisco Anomaly Detection and Mitigation Systems. The chapter covers Cisco Traffic Anomaly Detector and Cisco Guard products to provide DDoS mitigation.

Part V, “Security Management”: As networks grow in size and complexity, the requirement for centralized policy management tools grow as well. Sophisticated tools that can analyze, interpret, configure, and monitor the state of security policy, with browser-based user interfaces, enhance the usability and effectiveness of network security solutions. Part V includes the following chapters:

- Chapter 24, “Security and Policy Management,” provides comprehensive coverage of the security management solutions using the Cisco Security Manager (CSM) software and various device manager xDM tools including SDM, ASDM, PDM, and IDM.
- Chapter 25, “Security Framework and Regulatory Compliance,” provides an overview of security standards, policy and regulatory compliance, and best practices frameworks. The chapter covers the two commonly used security frameworks: ISO/IEC 17799 and COBIT. The chapter covers regulatory compliance and legislative acts including GLBA, HIPAA, and SOX.

*Network Security Technologies and Solutions* is a complete reference book, like a security dictionary, an encyclopedia, and an administrator’s guide—all in one.
This chapter describes Layer 2 security basics and security features on switches available to combat network security threats. These threats result from weaknesses in Layer 2 of the OSI model—the data-link layer. Switches act as arbiters to forward and control all the data flowing across the network. The current trend is for network security to be solidified through the support of switch security features that build feature-rich, high-performance, and optimized networks. The chapter examines the integrated security features available on Cisco catalyst switches to mitigate threats that result from the weaknesses in Layer 2 of the OSI model. The chapter also provides guidelines and recommendations intended to help you understand and configure the Layer 2 security features available on Cisco switches to build robust networks.

A summary of Layer 2 best practices is provided toward the end of the chapter.

Securing Layer 2

With the rapid growth of IP networks in the past years, high-end switching has played one of the most fundamental and essential roles in moving data reliably, efficiently, and securely across networks. Cisco Catalyst switches are the leader in the switching market and major players in today’s networks.

The data-link layer (Layer 2 of the OSI model) provides the functional and procedural means to transfer data between network entities with interoperability and interconnectivity to other layers, but from a security perspective, the data-link layer presents its own challenges. Network security is only as strong as the weakest link, and Layer 2 is no exception. Applying first-class security measures to the upper layers (Layers 3 and higher) does not benefit your network if Layer 2 is compromised. Cisco switches offer a wide range of security features at Layer 2 to protect the network traffic flow and the devices themselves.

Understanding and preparing for network threats is important, and hardening Layer 2 is becoming imperative. Cisco is continuously raising the bar for security, and security feature availability at Layer 2 is no exception. The sections that follow highlight the Layer 2 security features available on Cisco Catalyst switches.
Port-Level Traffic Controls

Port-based traffic control features can be used to provide protection at the port level. Catalyst switches offer Storm Control, Protected Ports, Private Virtual Local Area Network (PVLAN), Port Blocking, and Port Security features.

Storm Control

A LAN storm typically occurs when hostile packets are flooded on the LAN segment, creating unnecessary and excessive traffic resulting in network performance degradation. Several factors can cause a storm on a network; examples include errors in the protocol-stack implementation or a loophole that is exploited in a device configuration.

The Storm Control feature prevents regular network traffic from being disrupted by a broadcast, multicast, or unicast packet storm on any of the physical interfaces.

The traffic storm control (also known as a traffic suppression feature) monitors inbound packets over a 1-second interval and compares it to the configured storm-control suppression level by using one of the following methods to measure activity:

- The percentage of total available bandwidth of the port allocated for the broadcast, multicast, or unicast traffic
- Traffic rate over a 1-second interval in packets per second at which broadcast, multicast, or unicast packets are received on an interface

With either method, the port blocks traffic when a threshold is reached, filtering out all subsequent packets. As the port remains in a blocked state, the traffic continues to be dropped until the traffic rate drops below the suppression level, at which point the port resumes normal traffic forwarding.

To enable the traffic storm-control feature, use the storm-control {broadcast | multicast | unicast} command from the global configuration mode. By default, storm-control is disabled.

The storm-control action {shutdown | trap} command is used to specify the action to be taken when a storm is detected. By default, the storm traffic is suppressed when no action is configured.

To verify the storm-control suppression levels configured on an interface, use the show storm-control [interface] [broadcast | multicast | unicast] command.
Protected Ports (PVLAN Edge)

In some network environments, there is a requirement for no traffic to be seen or forwarded between host(s) on the same LAN segment, thereby preventing interhost communications. The PVLAN edge feature provisions this isolation by creating a firewall-like barrier, thereby blocking any unicast, broadcast, or multicast traffic among the protected ports on the switch. Note that the significance of the protected port feature is limited to the local switch, and there is no provision in the PVLAN edge feature to isolate traffic between two “protected” ports located on different switches. For this purpose, the PVLAN feature can be used. (This feature is discussed in more detail later in this chapter.)

The PVLAN edge offers the following features:

- The switch will not forward traffic (unicast, multicast, or broadcast) between ports that are configured as protected. Data traffic must be routed via a Layer 3 device between the protected ports.
- Control traffic, such as routing protocol updates, is an exception and will be forwarded between protected ports.
- Forwarding behavior between a protected port and a nonprotected port proceeds normally per default behavior.

By default, no ports are configured as protected. Example 4-1 shows how to enable and verify switch ports that are configured for the protected port feature.

Example 4-1 Configuring the Protected Port Feature

```
Switch(config)# interface Fastethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end

Switch# show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Protected: true
```

Private VLAN (PVLAN)

As discussed in the “Protected Ports (PVLAN Edge)” section, the PVLAN feature prevents interhost communications providing port-based security among adjacent ports within a VLAN across one or more switches. PVLAN provides Layer 2 isolation to quarantine hosts from one another among ports within the same PVLAN.

Access ports in a PVLAN are allowed to communicate only with the certain designated router ports. In most cases, this is the default gateway IP address. Private VLANs and normal VLANs can coexist on the same switch. The PVLAN feature allows segregating traffic at Layer 2, thereby transforming a broadcast segment into a nonbroadcast
multi-access-like segment. To prevent interhost and interserver communication, PVLAN can be used efficiently because the number of subnets or VLANs is greatly reduced, although the segmented approach within a single network segment is still achieved. The number is reduced because there is no need to create extra subnet/VLANs.

**NOTE**
The PVLAN feature is not available on all Cisco switches. Refer to Table 4-1 for a list of supported platforms.

The list that follows describes three types of PVLAN ports, as shown in Figure 4-1a:

- **Promiscuous**: A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN. The function of the promiscuous port is to move traffic between ports in community or isolated VLANs. It can use access lists to identify which traffic can pass between these VLANs. Only one promiscuous port is allowed per single PVLAN, and it serves all the community and isolated VLANs in the Private VLAN.

- **Isolated**: An isolated PVLAN port has complete Layer 2 segregation from all the other ports within the same PVLAN, but not from the promiscuous ports. Traffic from the isolated port is forwarded only to the promiscuous ports and none other.

- **Community**: Community ports are logically combined groups of ports in a common community and can pass traffic among themselves and with promiscuous ports. Ports are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

It is possible for isolated and community port traffic to enter or leave the switch through a trunk interface because trunks support VLANs carrying traffic among isolated, community, and promiscuous ports. Hence, PVLAN ports are associated with a separate set of VLANs that are used to create the PVLAN structure. A PVLAN uses VLANs in following three ways:

- **As a primary VLAN**: Carries traffic from a promiscuous port to isolated, community, and other promiscuous ports in the same primary VLAN.

- **As an isolated VLAN**: Carries traffic from isolated ports to a promiscuous port. Ports in the isolated VLAN cannot communicate at Layer 2 with any other port within the Private VLAN (either another community VLAN port or a port in the same isolated VLAN). To communicate with other ports, it must go through the promiscuous port.

- **As a community VLAN**: Carries traffic between community ports within the same community VLAN and to promiscuous ports. Ports in the community VLAN can communicate at Layer 2 with each other (only within the same community VLAN).
but cannot communicate with ports in other community or isolated VLANs. To communicate with other ports, they must go through the promiscuous port. Multiple community VLANs can be configured in a PVLAN.

Figure 4-1a depicts the basic PVLAN components and the different types of PVLAN ports.

**Figure 4-1a  PVLAN Components**

The isolated and community VLANs are also called *secondary VLANs*. PVLANs can be extended across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support PVLANs.

In summary, a Private VLAN contains three elements: the Private VLAN itself, the secondary VLANs (known as the community VLAN and isolated VLAN), and the promiscuous port.

Figure 4-1b summarizes the PVLAN components and traffic flow policies among the PVLAN ports.
Table 4-1 shows a list of Cisco switches that support the PVLAN feature with the respective software version.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Software Version</th>
<th>Isolated VLAN</th>
<th>PVLAN Edge (Protected Port)</th>
<th>Community VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 8500</td>
<td>Not Supported</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Catalyst 6500/6000 CatOS on Supervisor and Cisco IOS on MSFC</td>
<td>5.4(1) on Supervisor and 12.0(7)XE1 on MSFC</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Catalyst 6500/6000 Cisco IOS System software</td>
<td>12.1(8a)EX, 12.1(11b)E1</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 4-1  VLAN Support on Catalyst Switches (Continued)

<table>
<thead>
<tr>
<th>Platform</th>
<th>Software Version</th>
<th>Isolated VLAN</th>
<th>PVLAN Edge (Protected Port)</th>
<th>Community VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 5500/5000</td>
<td>Not Supported</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Catalyst 4500/4000 — CatOS</td>
<td>6.2(1)</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Catalyst 4500/4000 — Cisco IOS</td>
<td>12.1(8a)EW</td>
<td>Yes</td>
<td>N/A</td>
<td>12.2(20)EW</td>
</tr>
<tr>
<td>Catalyst 3750</td>
<td>12.2(20)SE—EMI</td>
<td>Yes</td>
<td>12.1(11)AX</td>
<td>Yes</td>
</tr>
<tr>
<td>Catalyst 3750 Metro</td>
<td>12.1(14)AX</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 3560</td>
<td>12.2(20)SE—EMI</td>
<td>Yes</td>
<td>12.1(19)EA1</td>
<td>Yes</td>
</tr>
<tr>
<td>Catalyst 3550</td>
<td>12.1(4)EA1</td>
<td>No</td>
<td>Yes</td>
<td>Not Currently Supported</td>
</tr>
<tr>
<td>Catalyst 2970</td>
<td>12.1(11)AX</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 2955</td>
<td>12.1(6)EA2</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 2950</td>
<td>12.0(5.2)WC1, 12.1(4)EA1</td>
<td>No</td>
<td>Yes</td>
<td>Not Currently Supported</td>
</tr>
<tr>
<td>Catalyst 2900XL/3500XL</td>
<td>12.0(5)XU (on 8MB switches only)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 2948G-L3 / 4908G-L3</td>
<td>Not Supported</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Catalyst 2948G/2980G</td>
<td>6.2</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Catalyst 2940</td>
<td>12.1(13)AY</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Catalyst 1900</td>
<td>Not Supported</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

Configuring PVLAN

NOTE  When enabling PVLAN, it is important to remember to configure the switch as VTP transparent mode before you can create a PVLAN. PVLANs are configured in the context of a single switch and cannot have members on other switches.
Perform the following steps to configure the PVLAN feature:

**Step 1** Create the primary and secondary PVLANs. For example, configure VLAN 101 as a primary VLAN, VLANs 201 to 202 as community VLANs, and VLAN 301 as an isolated VLAN.

```
Hostname(config)# vlan 101
Hostname(config-vlan)# private-vlan primary
Hostname(config)# vlan 201
Hostname(config-vlan)# private-vlan community
Hostname(config)# vlan 202
Hostname(config-vlan)# private-vlan community
Hostname(config)# vlan 301
Hostname(config-vlan)# private-vlan isolated
```

**Step 2** Associate the secondary VLANs to the primary PVLAN. For example, associate community VLANs 201 to 202 and isolated VLAN 301 with the primary VLAN 101.

```
Hostname(config)# vlan 101
Hostname(config-vlan)# private-vlan association 201-202,301
Hostname(config-vlan)# exit
```

**NOTE** Only one isolated VLAN can be mapped to a primary VLAN, but multiple community VLANs can be mapped to a primary VLAN.

**Step 3** Map secondary VLANs to the SVI (Switched Virtual Interface), which is the Layer 3 VLAN interface of a primary VLAN to allow Layer 3 switching of PVLAN ingress traffic.

For example, permit routing of secondary VLAN ingress traffic from VLANs 201 to 202 and 301 to the private VLAN 101 SVI (Layer 3 interface).

```
Hostname(config)# interface vlan 101
Hostname(config-if)# private-vlan mapping add 201-202,301
```

**Step 4** Configure a Layer 2 interface as an isolated or community port, and associate the Layer 2 port to the primary VLAN and selected secondary VLAN pair. For example, configure interface FastEthernet 1/1 as a PVLAN host port in community VLAN 201, map it to a private-secondary PVLAN pair, configure FastEthernet 1/2 as a PVLAN host port in isolated VLAN 301, and map it to a private-secondary PVLAN pair.

```
Hostname(config)# interface Fastethernet 1/1
Hostname(config-if)# switchport mode private-vlan host
Hostname(config-if)# switchport private-vlan host-association 101 201
Hostname(config)# interface Fastethernet 1/2
Hostname(config-if)# switchport mode private-vlan host
Hostname(config-if)# switchport private-vlan host-association 101 301
```
Step 5 Configure a Layer 2 interface as a PVLAN promiscuous port and map the PVLAN promiscuous port to the primary VLAN and to the selected secondary VLAN pair. For example, configure interface FastEthernet 1/10 as a PVLAN promiscuous port, and map it to a private-secondary PVLAN pair.

Use the `show interface private-vlan mapping` command and the `show interface [interface-id] switchport` command to verify the configuration.

Port Blocking

When a packet arrives at the switch, the switch performs a lookup for the destination MAC address in the MAC address table to determine which port it will use to send the packet out to send on. If no entry is found in the MAC address table, the switch will broadcast (flood) unknown unicast or multicast traffic out to all the ports in the same VLAN (broadcast domain). Forwarding an unknown unicast or multicast traffic to a protected port could raise security issues.

Unknown unicast or multicast traffic can be blocked from being forwarded by using the port blocking feature.

To configure port blocking for unknown unicast and multicast flooding, use the following procedures:

- The `switchport block multicast` interface configuration command to block unknown multicast forwarding to a port
- The `switchport block unicast` interface configuration command to block unknown unicast forwarding to a port
- The `show interfaces {interface} switchport` command to validate the port blocking configuration

By default, ports are not configured in blocking mode. Example 4-2 shows how to enable and verify switch ports configured for the port blocking feature.

Example 4-2 Configuring the Port Blocking Feature

```
Switch(config)# interface Fastethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
Switch# show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
... Protected: true
Unknown unicast blocked: enabled
Unknown multicast blocked: enabled
Appliance trust: none
```
Port Security

Port security is a dynamic feature that prevents unauthorized access to a switch port. The port security feature can be used to restrict input to an interface by identifying and limiting the MAC addresses of the hosts that are allowed to access the port. When secure MAC addresses are assigned to a secure port, the switch does not forward packets with source MAC addresses outside the defined group of addresses. To understand this process, think of the analogy of a secure car park facility, where a spot is reserved and marked with a particular car registration number so that no other car is allowed to park at that spot. Similarly, a switch port is configured with the secure MAC address of a host, and no other host can connect to that port with any other MAC address.

Port security can be implemented in the following three ways:

- **Static secure MAC addresses** are manually configured using the switchport `port-security mac-address [source-mac-address]` command and stored in the MAC address table and in the configuration.
- **Dynamic secure MAC addresses** are dynamically learned, stored in the MAC address table, but removed when the switch is reloaded or powered down.
- **Sticky secure MAC addresses** are the combination of items 1 and 2 in this list. They can be learned dynamically or configured statically and are stored in the MAC address table and in the configuration. When the switch reloads, the interface does not need to dynamically discover the MAC addresses if they are saved in the configuration file.

In the event of a violation, an action is required. A violation occurs when an attempt is made to access the switch port by a host address that is not found in the MAC address table, or when an address learned or defined on one secure interface is discovered on another secure interface in the same VLAN.

An interface can be configured for one of the following three security violation modes, based on the action to be taken when a violation occurs:

- **Protect**: This puts the port into the protected port mode, where all unicast or multicast packets with unknown source MAC addresses are dropped. No notification is sent out in this mode when security violation occurs.
- **Restrict**: Packets with unknown source addresses are dropped when the number of secure MAC addresses reaches the set limit allowed on the port. This continues until a sufficient number of secure MAC addresses is removed or the number of maximum allowable addresses is increased. Notification is sent out in this mode that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter is incremented.
- **Shutdown**: When a port security violation occurs, the port is placed in error-disabled state, turning off its port LED. In this mode, an SNMP trap is sent out, a syslog message is logged, and the violation counter is incremented.
To enable the port security feature, use the switchport port-security interface configuration command. The command has several options.

Example 4-3 shows how to configure a static secure MAC address on a port and enable sticky learning.

**Example 4-3  Port Security Configuration Example 1**

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0009.6B90.F4FE
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
```

Example 4-4 shows how to configure a maximum of 10 secure MAC addresses on VLAN 5 on port interface FastEthernet 0/2. The [vlan] option in this command sets a maximum value per VLAN for the specified VLAN or range of VLANs.

**Example 4-4  Port Security Configuration Example 2**

```
Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security maximum 10 vlan 5
Switch(config-if)# end
```

In addition to the configuration shown in Example 4-4, a port-security aging mechanism can be configured. By default the secure MAC addresses will not be aged out, and in normal port security configuration, the entries will remain in the MAC table until the switch is powered off. When using the sticky option, these MAC addresses will be stored until cleared manually.

There are two types of aging mechanisms:

- **Absolute:** The secure addresses on the port age out after a fixed specified time, and all references are flushed from the secure address list.
- **Inactivity:** Also known as idle time, the secure addresses on the port age out if they are idle, and no traffic from the secure source addresses passes for the specified time period.

Example 4-5 shows how to configure the aging time to 5 minutes for the inactivity aging type. In this example, aging is enabled for statically configured secure addresses on the port.

**Example 4-5  Port Security Aging Configuration Example**

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security aging time 5
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```
Access Lists on Switches

The switch supports the following four types of ACLs for traffic filtering:

- Router ACL
- Port ACL
- VLAN ACL
- MAC ACL

Router ACL

As the name implies, Router ACLs are similar to the IOS ACL discussed in Chapter 2, “Access Control,” and can be used to filter network traffic on the switched virtual interfaces (SVI). (SVI interfaces are Layer 3 interfaces on VLANs, on Layer 3 physical interfaces, and on Layer 3 EtherChannel interfaces.) Both standard and extended ACLs are supported. For more details to configure Router ACL, refer to Chapter 2.

Port ACL

Port ACLs are similar to Router ACLs but are supported on physical interfaces and configured on Layer 2 interfaces on a switch. Port ACL supports only inbound traffic filtering. Port ACL can be configured as three type access lists: standard, extended, and MAC-extended.

Processing of the Port ACL is similar to that of the Router ACLs; the switch examines ACLs associated with features configured on a given interface and permits or denies packet forwarding based on packet-matching criteria in the ACL.

When applied to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When applied to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

The main benefit with Port ACL is that it can filter IP traffic (using IP access lists) and non-IP traffic (using MAC access list). Both types of filtering can be achieved—that is, a Layer 2 interface can have both an IP access list and a MAC access list applied to it at the same time.

NOTE

Port ACLs are not supported on EtherChannel interfaces.
**VLAN ACL (VACL)**

VLAN ACL (also called *VLAN map*) provides packet filtering for all types of traffic that are bridged within a VLAN or routed into or out of the VLAN. Unlike Router ACL, VACL is not defined by a direction (input or output). All packets entering the VLAN (bridged or routed) are checked against the VACL. It is possible to filter traffic based on the direction of the traffic by combining VACLs and Private VLAN features.

VACLs are processed in hardware, so there is no performance penalty in processing them. Therefore, they are also referred to as *wire-speed ACLs*. The forwarding rate remains unchanged regardless of the size of the access list because the lookup of VACLs is performed in hardware.

**VACL on a Bridged Port**

Figure 4-2 illustrates where the VACL is processed when VACL is applied on a bridged port for traffic from Host A in VLAN 5 that is communicating to Host B in VLAN 10 through the switch.

![VACL on a Bridged Port](image)

**VACL on a Routed Port**

Figure 4-3 illustrates how IOS ACL and VACL are applied on routed packets and Layer 3 switched packets. Following is the order of processing:

1. VACL for input VLAN
2. Input IOS ACL
3. Output IOS ACL
4. VACL for output VLAN
Chapter 4: Security Features on Switches

Figure 4-3  VACL on a Routed Port

Configuring VACL

Perform the following steps to configure and apply a VACL (VLAN access map) on the switch:

1. Define the standard or extended access list to be used in VACL.
2. Define a VLAN access map.
3. Configure a match clause in a VLAN access map sequence.
4. Configure an action clause in a VLAN access map sequence.
5. Apply the VLAN access map to the specified VLANs.
6. Display VLAN access map information.

Example 4-6 shows how to define and apply a VACL to drop packets matching access list 1 from network 192.168.1.0/24; all other packets matching access list 2 are forwarded. The VACL is applied to VLANs 5 through 10.

Example 4-6  VACL Configuration Example

```
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#access-list 2 permit any
Switch(config)#vlan access-map mymap 10
Switch(config)#vlan access-map mymap 20
Switch(config)#match ip address 1
Switch(config)#match ip address 2
Switch(config)#action drop
Switch(config)#exit
```
MAC ACL

MAC ACL, also known as Ethernet ACL, can filter non-IP traffic on a VLAN and on a physical Layer 2 interface by using MAC addresses in a named MAC extended ACL. The steps to configure a MAC ACL are similar to those of extended named ACLs. MAC ACL supports only inbound traffic filtering.

To define the MAC Extended ACL, use the `mac access-list extended` command. Several non-IP protocols are supported.

After the MAC ACL is created, it can be applied to a Layer 2 interface using the `mac access-group [acl-name] in` command to filter non-IP traffic received on the interface.

Example 4-7 shows how to define and apply a MAC ACL to drop all (non-IP) AppleTalk Address Resolution Protocol (AARP) packets, allowing all other types of traffic.
## Spanning Tree Protocol Features

Spanning Tree Protocol (STP) resolves redundant topologies into loop-free, treelike topologies. When switches are interconnected via multiple paths, STP prevents loops from being formed. An STP loop (or forwarding loops) can occur when the entire network fails because of a hardware failure, a configuration issue, or a network attack. STP loops can be costly, causing major network outages. The following STP features can be used to improve the stability of the Layer 2 networks.

### Bridge Protocol Data Unit (BPDU) Guard

Bridge protocol data units (BPDU) are data messages exchanged between bridges using spanning tree protocol to detect loops in a network topology. BPDU contains management and control data information that is used to determine the root bridge and establish the port roles—for example: root, designated, or blocked port.

The BPDU Guard feature is designed to keep the active topology predictable and to enhance switch network reliability by enforcing the STP domain borders.

The guard can be enabled globally on the switch or enabled on a per-interface basis. In a valid configuration, ports with port fast enabled do not receive BPDUs. Receiving a BPDU on a port with port fast enabled signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU Guard feature puts the interface in the error-disabled state.

At the global level, BPDU Guard can be enabled on a port with port fast enabled using the `spanning-tree portfast bpduguard default` global configuration command. Spanning tree shuts down interfaces that are in a port fast operational state.

At the interface level, BPDU Guard can be enabled on an interface by using the `spanning-tree bpduguard enable` interface configuration command without also enabling the port fast feature. When the interface receives a BPDU, the switch assumes that a problem exists and puts the interface in the error-disabled state.

The BPDU Guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. In a service-provider network environment, the BPUD Guard feature can be used to prevent an access port from participating in the spanning tree.

### Root Guard

In a switched network environment with shared administrative control or in a service provider (SP) environment where there are many connections to other switches (into customer networks), it is important to identify the correct placement of the root bridge. If possible, it is also important to identify a specific predetermined location to achieve an
optimal forwarding loop-free topology. There is no mechanism in the standard STP to
enforce the position of the root bridge, as any bridge in a network with a lower bridge ID
can assume the role of the root bridge. Sometimes because of a misconfiguration, a
spanning tree may converge incorrectly by selecting an imprecise switch to be the root switch. This situation can be prevented by enabling the Root Guard feature. For example, you could enable Root Guard on SP-side switch interfaces that connect to a customer-side switch. With the Root Guard feature implemented, if a switch outside the SP network becomes the root switch, the interface is put in a blocked state, and spanning tree will select a new root switch. The customer’s switch does not become the root switch and is not in the path to the root.

With the Root Guard feature, a Layer 2 interface is set as the designated port, and if any device through this port becomes the root bridge, the interface is placed into the blocked (root-inconsistent) state. The Root Guard feature can be enabled by using the spanning-tree guard root command in interface configuration mode.

**EtherChannel Guard**

The EtherChannel Guard feature is used to detect EtherChannel misconfigurations between the switch and a connected device. An example of a misconfiguration is when the channel parameters are not identical and do not match on both sides of the EtherChannel. Another example could be when only one side is configured with channel parameters. EtherChannel parameters must be the same on both sides for the guard to work.

When the switch detects an EtherChannel misconfiguration, the EtherChannel Guard places the switch interface in the error-disabled state and displays an error message.

The EtherChannel Guard feature can be enabled by using the spanning-tree etherchannel guard misconfig global configuration command.

**Loop Guard**

The Loop Guard feature provides an additional layer of protection against the Layer 2 forwarding loops (STP loops) by preventing alternative or root ports from becoming designated ports because of a failure resulting in a unidirectional link. This feature works best when enabled on all switches across a network. By default, the spanning tree does not send BPDUs on root or alternative ports.

The Loop Guard feature can be enabled by using the spanning-tree loopguard default global configuration command.
Dynamic Host Configuration Protocol (DHCP) Snooping

The DHCP Snooping feature provides network protection from rogue DHCP servers. It creates a logical firewall between untrusted hosts and DHCP servers. The switch builds and maintains a DHCP snooping table (also called DHCP binding database), shown in Figure 4-4a. In addition, the switch uses this table to identify and filter untrusted messages from the network. The switch maintains a DHCP binding database that keeps track of DHCP addresses that are assigned to ports, as well as filtering DHCP messages from untrusted ports. For incoming packets received on untrusted ports, packets are dropped if the source MAC address does not match MAC in the binding table entry.

Figure 4-4a  DHCP Snooping Table

Figure 4-4b illustrates the DHCP Snooping feature in action, showing how the intruder is blocked on the untrusted port when it tries to intervene by injecting a bogus DHCP response packet to a legitimate conversation between the DHCP client and server.
The DHCP Snooping feature can be configured for switches and VLANs. When enabled on a switch, the interface acts as a Layer 2 bridge, intercepting and safeguarding DHCP messages going to a Layer 2 VLAN. When enabled on a VLAN, the switch acts as a Layer 2 bridge within a VLAN domain.

For DHCP Snooping to function correctly, all DHCP servers connected to the switch must be configured as trusted interfaces. A trusted interface can be configured by using the `ip dhcp snooping trust` interface configuration command. All other DHCP clients connected to the switch and other ports receiving traffic from outside the network or firewall should be configured as untrusted by using the `no ip dhcp snooping trust` interface configuration command.

To configure the DHCP Snooping feature, first enable DHCP Snooping on a particular VLAN by using the `ip dhcp snooping vlan [vlan-id]` command in global configuration mode. (Repeat this command for multiple VLANs.) Next, enable DHCP Snooping globally by using the `ip dhcp snooping` command from the global configuration mode. Both options must be set to enable DHCP snooping.

In Example 4-8, the DHCP server is connected to the FastEthernet0/1 interface and is configured as a trusted port with a rate limit of 100 packets per second. The **rate limit**
command ensures that a DHCP flood will not overwhelm the DHCP server. DHCP Snooping is enabled on VLAN 5 and globally activated.

Example 4-8  
**DHCP Snooping Configuration Example**

```
Switch(config)# interface Fastethernet0/1  
Switch(config-if)# ip dhcp snooping trust  
Switch(config-if)# ip dhcp snooping limit rate 100  
Switch(config-if)# exit  
Switch(config)# ip dhcp snooping vlan 5  
Switch(config)# ip dhcp snooping  
Switch(config)# ip dhcp snooping information option
```

Use the `show ip dhcp snooping` command to display DHCP snooping settings. Use the `show ip dhcp snooping binding` command to display binding entries corresponding to untrusted ports.

**IP Source Guard**

IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the untrusted Layer 2 ports.

The IP Source Guard feature is enabled in combination with the DHCP snooping feature on untrusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is supported on Layer 2 ports only, including access and trunk ports.

Example 4-9 shows how to enable the IP Source Guard with dynamic source IP and MAC address filtering.

**Example 4-9  IP Source Guard Configuration Example 1**

```
Switch(config)#interface GigabitEthernet1/0/1  
Switch(config-if)#ip verify source port-security
```

Example 4-10 shows how to enable the IP Source Guard with a static source IP address and MAC address filtering mapped on VLAN 5.

**Example 4-10  IP Source Guard Configuration Example 2**

```
Switch(config)#ip source binding 0011.0011.0011 vlan 5 10.1.1.11 interface GigabitEthernet1/0/2
```
Use the `show ip verify source` command to display the IP Source Guard configuration and the `show ip source binding` command to display the IP source bindings on the switch.

Dynamic ARP Inspection (DAI)

Address Resolution Protocol (ARP) provides IP-to-MAC (32-bit IP address into a 48-bit Ethernet address) resolution. ARP operates at Layer 2 (the data-link layer) of the OSI model. ARP provides the translation mapping the IP address to the MAC address of the destination host using a lookup table (also known as the ARP cache).

Several types of attacks can be launched against a host or devices connected to Layer 2 networks by “poisoning” the ARP caches. A malicious user could intercept traffic intended for other hosts on the LAN segment and poison the ARP caches of connected systems by broadcasting forged ARP responses. Several known ARP-based attacks can have a devastating impact on data privacy, confidentiality, and sensitive information. To block such attacks, the Layer 2 switch must have a mechanism to validate and ensure that only valid ARP requests and responses are forwarded.

Dynamic ARP inspection is a security feature that validates ARP packets in a network. Dynamic ARP inspection determines the validity of packets by performing an IP-to-MAC address binding inspection stored in a trusted database, (the DHCP snooping binding database) before forwarding the packet to the appropriate destination. Dynamic ARP inspection will drop all ARP packets with invalid IP-to-MAC address bindings that fail the inspection. The DHCP snooping binding database is built when the DHCP snooping feature is enabled on the VLANs and on the switch.

**NOTE**

Dynamic ARP inspection inspects *inbound* packets only; it does not check *outbound* packets.

Figure 4-5a shows an example of an attacker attempting to spoof and hijack traffic for an important address (a default gateway in this example) by broadcasting to all hosts spoofing the MAC address of the router (using a gratuitous ARP). This will poison ARP cache entries (create an invalid ARP entry) on Host A and Host B, resulting in data being redirected to the wrong destination. Because of the poisoned entries, when Host A sends data destined for the router, it is incorrectly sent to the attacker instead. Dynamic ARP inspection locks down the IP-MAC mapping for hosts so that the attacking ARP is denied and logged.
The dynamic ARP Inspection (DAI) feature safeguards the network from many of the commonly known man-in-the-middle (MITM) type attacks. Dynamic ARP Inspection ensures that only valid ARP requests and responses are forwarded.

Figure 4-5b illustrates the DAI feature in action and shows how the intruder is blocked on the untrusted port when it is trying to poison ARP entries.
DAI in a DHCP Environment

As mentioned earlier, DAI relies on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings. Configure each secure interface as trusted using the `ip arp inspection trust` interface configuration command. The trusted interfaces bypass the ARP inspection validation checks, and all other packets are subject to inspection when they arrive on untrusted interfaces.

Enable DAI on a per-VLAN basis by using the `ip arp inspection vlan [vlan-range]` command from the global configuration command.

Example 4-11 shows how to configure an interface as trusted and how to enable DAI for VLANs 5 through 10.

Example 4-11  DAI in a DHCP Environment Configuration Example

```
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# ip arp inspection trust
Switch(config)# ip arp inspection vlan 5-10
```
DAI in a Non-DHCP Environment

In non-DHCP environments, because there is no DHCP snooping binding database, the DAI can validate ARP packets against a user-defined ARP ACL to map hosts with a statically configured IP address to their MAC address.

Use the `arp access-list [acl-name]` command from the global configuration mode on the switch to define an ARP ACL and apply the ARP ACL to the specified VLANs on the switch.

Example 4-12 shows how to configure an ARP ACL to permit ARP packets from host IP address 10.1.1.11 with MAC address 0011.0011.0011 and how to apply this ACL to VLAN 5 with the interface configured as untrusted.

Example 4-12  DAI in a Non-DHCP Environment Configuration Example

```
Switch(config)# arp access-list arpacl
Switch(config-arp-acl)# permit ip host 10.1.1.11 mac host 0011.0011.0011
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter arpacl vlan 5
Switch(config)# interface GigabitEthernet1/0/2
Switch(config-if)# no ip arp inspection trust
```

Use the `show ip arp inspection vlan [vlan# or range]` command to verify the configuration.

Rate Limiting Incoming ARP Packets

Because the switch CPU performs the DAI, there is a potential for an ARP flooding denial-of-service (DoS) attack resulting in performance degradation. To prevent this, ARP packets can be rate limited using the `ip arp inspection limit` command from the interface configuration mode to limit the rate of incoming ARP requests and responses. By default, 15 pps (packets per second) is allowed on untrusted interfaces; however, there is no limit on trusted interfaces. The burst interval is 1 second.

When the rate of incoming ARP packets exceeds the configured thresholds, the port is placed in the error-disabled state. The port will remain in this state until the user intervenes or the `errdisable recovery cause arp-inspection interval [seconds]` command is enabled, so that ports can automatically recover from this state after a specified timeout period.

Use the `show ip arp inspection interfaces` to display the trust state, the rate limit (pps stands for packets per second), and the burst interval configured for the interfaces.

Use the `show ip arp inspection vlan [vlan# or range]` command to display the DAI configuration and the operation state of the VLANs configured on the switch.
ARP Validation Checks
Specific additional checks can be performed on incoming ARP packets to validate the destination MAC address, the sender IP address in ARP requests, the target IP address in ARP responses, or the source MAC address. Use the `ip arp inspection validate {[src-mac] [dst-mac] [ip]}` command from the global configuration mode to enable these additional ARP validation checks.

Use the `show ip arp inspection statistics` command to display packet statistics on DAI-configured VLANs.

Advanced Integrated Security Features on High-End Catalyst Switches
In addition to the features previously discussed, several integrated security features are available on high-end catalyst switches such as the Catalyst 6500 series and the Catalyst 7600 series switches. These features provide protection from excessive or unnecessary traffic and against various types of DoS attacks.

The Cisco Catalyst series switches offer a strong set of integrated security features, including the following: hardware- and software-based CPU rate limiters (for DoS protection), user-based rate limiting, hardware-based MAC learning, uRPF check in hardware, TCP intercept hardware acceleration, and most important, the Control Plane Policing (CoPP) feature. CoPP is also supported on all Cisco Integrated Services Routers (ISRs). One of the main advantages is that most of these integrated security features are based on hardware and can be enabled concurrently with no performance penalty.

Control Plane Policing (CoPP) Feature
The traffic managed by a device can be divided into three functional components or planes:

- Data plane
- Management plane
- Control plane

The vast majority of traffic flows through the device via the data plane; however, the route processor handles certain traffic, such as routing protocol updates, remote-access services, and network management traffic such as SNMP. This type of traffic is referred to as the control and management plane. The route processor is critical to network operation. Therefore any service disruption or security compromise to the route processor, and hence the control and management planes, can result in network outages that impact regular operations. For example, a DoS attack targeting the route processor typically involves high bursty traffic resulting in excessive CPU utilization on the route processor. Such attacks can
be devastating to network stability and availability. The bulk of traffic managed by the route processor is handled by way of the control and management planes.

The CoPP feature is used to protect the aforementioned control and management planes; to ensure stability, reachability, and availability and to block unnecessary or DoS traffic. CoPP uses a dedicated control plane configuration through the modular QoS CLI (MQC) to provide filtering and rate limiting capabilities for the control plane packets.

As mentioned earlier, the CoPP feature is available on all major Cisco router series including ISR. Table 4-2 provides a complete list of compatible hardware and software support.

Table 4-2  
**CoPP Support on Cisco Routers**

<table>
<thead>
<tr>
<th>Router Models</th>
<th>Cisco IOS Software Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 12000 Series</td>
<td>Release 12.0(29)S and later</td>
</tr>
<tr>
<td>Cisco 7600 Series</td>
<td>Release 12.2(18)SXD1 and later</td>
</tr>
<tr>
<td>Cisco 6500 Series</td>
<td>Release 12.2(18)SXD1 and later</td>
</tr>
<tr>
<td>Cisco 7200 Series</td>
<td>Release 12.2(18)S and later</td>
</tr>
<tr>
<td>Cisco 7500 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco 1751 Router</td>
<td>Release 12.3(4)T and later</td>
</tr>
<tr>
<td>Cisco 2600/2600-XM Series</td>
<td></td>
</tr>
<tr>
<td>Cisco 3700 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco 7200 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco 1800 Series</td>
<td>Release 12.3(8)T and later</td>
</tr>
<tr>
<td>Cisco 2800 Series</td>
<td></td>
</tr>
<tr>
<td>Cisco 3800 Series</td>
<td>Release 12.3(11)T and later</td>
</tr>
</tbody>
</table>

Perform the following steps to configure and apply the CoPP feature:

**Step 1** Define a packet classification criterion. There are a number of ways to categorize the type of traffic—for example, by using an access list or protocol or IP precedence values.

```
Hostname(config)# class-map {traffic_class_name}
Hostname(config-cmap)# match {access-list | protocol | ip prec | ip dscp | vlan}
```

**Step 2** Define a service policy. Note that flow policing is the only valid option available (as of this writing) in the policy map for CoPP.

```
Hostname(config-pmap)# policy-map {service_policy_name}
Hostname(config-pmap)# class {traffic_class_name}
Hostname(config-pmap-c)# police <rate> conform-action <action> exceed-action <action>
```
Step 3  Enter control plane configuration mode using the control-plane global command. In this CP submode, the service policies are attached to the control plane.

Hostname(config)# control-plane

Step 4  Apply QoS policy configured to the control plane.

Hostname(config-cp)# service-policy {input | output} {service_policy_name}

NOTE
The CoPP feature is also available as part of the integrated Network Foundation Protection (NFP) security features on the Cisco ISR (Integrated Services Router) platforms.

CPU Rate Limiters

The Supervisor Engine 720 (SUP720) is available for high-end Catalyst 6500/7600 series switches and supports several integrated security features, including one that is important to mention. SUP720 has built-in “special case” CPU rate limiters to classify traffic that cannot be categorized otherwise. The built-in special case CPU rate limiters use an access list (examples include IP options cases, time to live [TTL] and maximum transmission unit [MTU] failure cases, and packets with errors). The CPU rate limit is mainly used for DoS protection.

Layer 2 Security Best Practices

To conclude this chapter, a list of best practices is presented here for implementing, managing, and maintaining secure Layer 2 network:

- Manage the switches in a secure manner. For example, use SSH, authentication mechanism, access list, and set privilege levels.
- Restrict management access to the switch so that untrusted networks are not able to exploit management interfaces and protocols such as SNMP.
- Always use a dedicated VLAN ID for all trunk ports.
- Be skeptical; avoid using VLAN 1 for anything.
- Disable DTP on all non-trunking access ports.
- Deploy the Port Security feature to prevent unauthorized access from switching ports.
- Use the Private VLAN feature where applicable to segregate network traffic at Layer 2.
- Use MD5 authentication where applicable.
- Disable CDP where possible.
• Prevent denial-of-service attacks and other exploitation by disabling unused services and protocols.
• Shut down or disable all unused ports on the switch, and put them in a VLAN that is not used for normal operations.
• Use port security mechanisms to provide protection against a MAC flooding attack.
• Use port-level security features such as DHCP Snooping, IP Source Guard, and ARP security where applicable.
• Enable Spanning Tree Protocol features (for example, BPDU Guard, Loopguard, and Root Guard).
• Use Switch IOS ACLs and Wire-speed ACLs to filter undesirable traffic (IP and non-IP).

Summary

This chapter presents a basic overview of Layer 2 security. The chapter gives you configuration examples and brings together the integrated-security features available on Cisco switches, such as port-level controls, port blocking, port security Private VLAN (PVLAN), and many more. The chapter discusses the various configurable ACLs that can be used on the switches, including the wire-speed ACLs. The chapter takes a quick look at the Spanning Tree Protocol features and safeguard mechanisms available to prevent STP attacks. Cisco switches offer unique features to mitigate common attacks on the services such as DHCP, DNS, and ARP-cache poisoning attacks. The chapter briefly outlines some platform-specific integrated security features available on the high-end switch platforms. The chapter concludes with the summary of Layer 2 security best practices to implement, manage, and maintain a secure Layer 2 network.
References


Numerics

3DES, 412
802.11 standards, RF bands, 348
802.1x attacks, mitigating, 254, 256
802.1x authentication, configuring
  on Cisco Aironet Wireless Access Points, 342–343
  on Cisco Catalyst switches, 337–342

A

AAA, 78, 267
  accounting, 269, 281
  services, 284
  authentication, 268, 280
  RADIUS, 270–273
  services, 282
  TACACS+, 274–277
  authorization, 269, 280
  services, 283
  dependencies, 269
  implementing, 278–279
  method lists, server groups, 281–282
AAA client server mode, AAA server, 290–291
ACCEPT response (TACACS+), 276
acceptable use policies, 10
access attacks, 208
Access Control Matrix, 13
access control process (CSA), 618
access modes (SSL VPN), 525
Access-Accept response (RADIUS), 272
Access-Request packets, 272
accounting, 269
  AAA, 281
  AAA service types, 284
ACLs (access control lists), 21, 49, 185–187
  antspoofing, 221–222
  applying to interfaces, 30–31
  classification ACLs, 48
  configuring for PVLAN attack mitigation, 249–251
  creating, 29
  directionality, 32
distributed time-based, 45
downloadable IP ACLs, 293
dynamic, 40–41
established, 43
extended, 38–39
genereal guidelines, 36
iACLs, 47
inbound, 32
infrastructure ACLs, 62
MAC ACLs, 97
named, 39
names, assigning, 29
object groups, 188–190
outbound, 33
packet flow rules, 33
Port ACLs, 94
rACLs, 46
reflexive, 42
Router ACLs, 94
standard, 37–38
time-based, 44
traffic characterization, 212–215, 218
transit ACLs, 47
Turbo ACLs, 46
VACLs, 95
  configuring, 96–97
when to use, 23
ACS. See Cisco Secure ACS
AD (anomaly detection), 597–598
Adaptive Security Algorithm, 150-152
  application layer protocol inspection, 148-150
  security levels, 157–158
  stateful packet inspection, 148
advanced Cisco IOS Firewall features
  e-mail inspection engine, 128
  Firewall ACL Bypass, 129
  HTTP inspection engine, 127
  router-generated traffic inspection, 131
  transparent IOS Firewall, 130
  VFR, 130–131
advanced level 3 operation, CS-MARS, 686
advisory policies, 749
AES (Advanced Encryption Standard), 412
agent kit management (CSA), 626, 629
Agent User Interface control page (CSA MC), 632, 634
aggressive mode (IKE), 436
aging mechanisms (port security), 93
AH, 433
AIC (Application Inspection and Control), 136, 578
AIM (Adaptive Identification and Mitigation), 142
anomaly detection and mitigation systems, 641–643, 649–650
antenna, 349
anti-replay service, IPsec VPN, 434
AP (access points), 347–349
APEC (Asia-Pacific Economic Cooperation), 766
APIPA (automatic private IP addressing), 27
application layer protocol inspection, 148–150
applying ACLs to interfaces, 30–31
ARC (Attack Response Controller), 593
ARP packets, rate limiting, 106
ARP spoofing, 209
ASDM (Cisco Adaptive Security Device Manager), 145
HTTP access, 77
ASR (Asymmetric Routing Support), 197
ASR (Attack Severity Rating), 584
assigning names to ACLs, 29
asymmetric key cryptography, 412, 416
atomic engines, 578
attack vectors, 208
attacks
access, 208
anomaly detection and mitigation systems, 641–643
DDoS, 641
DoS, 639–640
Layer 2 mitigation techniques, 242
ACLs, configuring, 249–251
BPDU Guard, configuring, 252
DAI, 245–246
DHCP snooping, configuring, 253–254
PEAP, enabling, 254–256
switch Port Security feature, 242–244
VLAN configuration, modifying, 247–249
VTP passwords, configuring, 246–247
Layer 3 mitigation techniques
CAR, 225–226
IP source tracking, 219–220
IP spoofing, 220–222
MQC, 227–228
NBAR, 230–232
NetFlow, 239–241
PBR, 234–236
TCP Intercept, 232–234
traffic characterization, 212–215, 218
traffic classification, 224
traffic policing, 229
uRPF, 236–239
reconnaissance, 208
risk assessment, 211
security incident response, 256–257
IRT, 257–261
authentication, 268. See also authentication protocols
AAA login methods, 280
AAA service types, 282
client-based, 352
MAC-based, 352
two-factor authentication systems
Cisco Secure ACS, support for, 315–316
OTP, 312–313
S/KEY, 313
smart cards, 314–315
tokens, 314–315
user accounts, 60–61
authentication protocols
RADIUS, 270
communication, 271–273
packets, 271
security, 273
TACACS+, 274
communication, 276–277
packets, 275
security, 277
authentication proxy, 114
authentication server (IEEE 802.1x), 331
authenticator (IEEE 802.1x), 330
authorization, 269
AAA, 280
AAA service types, 283
authorized port state, 332–333
autoloading device configuration, 70
Auto-Secure feature, 75–76
AUX port, interactive device access, 65
AV pairs, 269, 283
availability, 9
B

banner messages, 65–67
banner tokens, 66
baselines, 12
basic level 1 operation, CS-MARS, 685
Biba security model, 13
BLM (Bell-Lapadula Model), 13
block cipher, 411
blocking, 593–594
BOOTP, 69
BPDU Guard, 98
    configuring for STP attack mitigation, 252
BPDUs (bridge protocol data units), 98
buffer overflows, 209
bypassing NAT
    Identity NAT, 179
    Policy NAT, 183
    Static identity NAT, 180

C

CAA (Clean Access Agent), 380
cable-based failover, 196
CBAC (Context-Based Access Control), 114–115
    audit trails, 117
    configuring, 122
    dynamic ACL entries, 119
    embryonic sessions, 120
    global timeouts/thresholds, configuring, 123
    inspection rule, configuring, 123
    interface, configuring, 122
    IP access list, configuring, 123
    packet inspection, 118
    per-host DoS prevention, 120
    session state table, 118
    supported protocols, 121
    threshold values, 118
    timeout values, 118
    traffic filtering, 116
    traffic inspection, 116
    verifying configuration, 126
CDP (Cisco Discovery Protocol), 68
certificate enrollment (PKI), 447–448
challenge/response OTP, 313
Chinese Wall security model, 13
CIA model, 8–9
CIDEE (Cisco Intrusion Detection Event Exchange), 576
Cisco AIP-SSM (ASA Advanced Inspection and Prevention Security Services Module), 567
Cisco Aironet Wireless LAN Access Point, configuring 802.1 authentication, 342–343
Cisco AnyConnect VPN Client, 192, 530
Cisco ASA 5500 Series Adaptive Security appliances, 143
    software, 144
    SSH access, 77
    Telnet access, 76
Cisco ASDM (Adapative Security Device Manager), 732
    features, 732
    operation, 733, 737
    supported firewalls and software versions, 738
Cisco AutoMitigate, 672
Cisco Catalyst switches, 83
    802.1 authentication, configuring, 337–342
    ACLs
        MAC ACLs, 97
        Port ACLs, 94
        Router ACLs, 94
        VACLs, 95–97
    advanced security features, CoPP, 107–109
    FWSM module, 198
        configuring, 202–204
        installing, 200
        OS software, 199
    port-level traffic control
        protected ports, 85
        storm control, 84
    PVLANs, 85
        configuring, 89–91
        port blocking, 91
        port security, 92–93
    SUP 720, CPU rate limiters, 109
Cisco Clean Access Manager, 379
Cisco ContextCorrelation, 672
Cisco DDoS Anomaly Detection and Mitigation solution, 643, 649
    anomaly detection and mitigation process, 649–650
Cisco Guard DDoS Mitigation, 647–649
  configuring, 660–666
  initializing, 661–662
Cisco Traffic Anomaly Detector, 644–647
  configuring, 653–659
  initializing, 655–656
Cisco Easy VPN, implementing, 456–461
Cisco FWSM (Firewall Services Module), 143–144
Cisco Guard DDoS Mitigation, 647–649
  configuring, 660–666
  initializing, 661–662
Cisco IBNS (Identity-Based Networking Services), 327
  Cisco Secure ACS, 328
  external database support, 329
Cisco IDM (IPS Device Manager), 601, 740–741
  system requirements, 742
Cisco IDSM-2 (IDS Service Module), 565–567
Cisco IOS Firewalls, 113
  advanced features
    e-mail inspection engine, 128
    Firewall ACL Bypass, 129
    HTTP inspection engine, 127
    router-generated traffic inspection, 131
    transparent IOS Firewall, 130
    VFR, 130–131
CBAC, 115
  audit trails, 117
  configuring, 122–126
  dynamic ACL entries, 119
  embryonic sessions, 120
  packet inspection, 118
  per-host DoS prevention, 120
  session state table, 118
  supported protocols, 121
  threshold values, 118
  timeout values, 118
  traffic filtering, 116
  traffic inspection, 116
Cisco IOS IPS, 569–570
Cisco IOS Resilient Configuration, 67
Cisco IOS Software, Auto-Secure feature, 75–76
Cisco IPS 4200 Series sensors, 563–564
Cisco IPS appliance
  IPS inline interface pair mode, configuring, 604–608
  IPS inline VLAN pair mode, configuring, 601–603
Cisco IPS Sensor OS Software, 572–574
  AD, 597–598
  blocking, 593–594
  communication protocols, 575
  interface modes, 589–592
  interface roles, 585–589
  IPS events, 580–581
  action responses, 582–583
  IPS rate limiting, 594
  RR, 583–584
  security policies, 596
  sensor software partitions, 577
  signatures, 578–580
  TR, 584
  user roles, 576
  virtualization, 595
Cisco IPS-AIM, 568
Cisco NAC appliance, 376. See also Cisco NAC Framework solution
  comparing with NAC framework, 378
  components, 379
  deployment scenarios, 380–381
Cisco NAC Framework solution, 382–383
  components of, 386–388
  concentrator support, 390
  deployment scenarios, 391
  mechanics of, 383–384
  posture states, 385
  protocols, 385
  router support, 388
  security policy enforcement, 392
    NAC-L2-802.1x, 399–401
    NAC-L2-IP, 396–399
    NAC-L3-IP, 394–396
  switch support, 388–390
  wireless access point support, 390
  wireless LAN controllers support, 391
Cisco Network Intrusion Prevention solutions, 562
Cisco AIP-SSM, 567
Cisco IOS IPS, 569–570
Cisco IDSM-2, 565–567
Cisco IPS 4200 Series sensors, 563–564
Cisco IPS-AIM, 568
Cisco IPS Sensor OS software, 572–574
   AD, 597–598
   blocking, 593–594
   communication protocols, 575
   interface modes, 589–592
   interface roles, 585, 588–589
   IPS event actions, 582–583
   IPS events, 580–581
   IPS rate limiting, 594
   RR, 583–584
   security policies, 596
   sensor software partitions, 577
   signatures, 578–580
   TR, 584
   user roles, 576
   virtualization, 595
deploying, 570–572
high availability
   fail-open mechanism, 598–599
   failover, 599
   load-balancing, 600
Cisco PIX 500
   SSH access, 77
   Telnet access, 76
Cisco PIX 500 Series Security appliances, 140
   software, 144
Cisco SDM (Cisco Router and Security Device Manager), 721
Cisco SDN (Self-Defending Network) solutions, 373, 767
   Cisco NAC, 376
Cisco Secure ACS, 289, 328
   AAA client server model, AAA server, 290–291
   configuring, 297–301
   for RADIUS-enabled token server, 317, 321
   for RSA SecurID token server, 321–322
  Dowloadable IP ACLs feature, 293
   MAR, 295
   NAC support, 296
   NAF, 294
   NAP, 296
   NAR, 295
   protocol compliance, RADIUS, 291–292
   RAC, 294
   shell command authorization sets, 294
   SPC, 293
   two-factor authentication systems, support for, 315–316
Cisco Secure ACS SE (Cisco Secure ACS Solution Engine), 307–308
Cisco SecureVector, 672
Cisco Security Appliance
   ACLs, 186–187
   object groups, 188–190
   Adaptive Security Algorithm, 150–152
   Cisco AnyConnect VPN Client, 192
   EIGRP, configuring, 168–170
   failover, 193–195
   configuring, 195–197
   IP routing, 159
   default routes, 161–162
   ECMP forwarding, 162–163
   static route tracking, 160
   static routes, 160
   MPF, configuring, 190–192
   OS software, 145
   OSPF, configuring, 164–167
   redundant interfaces, configuring, 158–159
   RIP, configuring, 167–168
   Routed Firewall mode, 146
   security contexts, 152
   configuring, 155–157
   routed mode, 153
   transparent mode, 153–155
   Transparent Firewall mode, 146–147
Cisco Security Manager, 700
   client/server requirements, 716–718
   configuration views, 707–708
   cross launching, 713–715
   device management, 710
   features, 700–702
   firewall management system, 703
   IPS management, 704–705
   platform management, 706
   RBAC, 711–712
   supported devices, 715–716
   traffic flow requirements, 719–721
   VPN management, 704
   workflow mode, 710–711
Cisco Traffic Anomaly Detector, 644–647
configuring, 653–659
initializing, 655–656
Cisco Trust and Identity Management
Solutions, 326
Cisco IBNS, 327
Cisco Secure ACS, 328
external database support, 329
Cisco Unitified Wireless Network solution,
368–370
Clark-Wilson security model, 13
classes of IP addresses, 24–26
classification ACLs, 48
Clean Access Server, 379
clear-text passwords, 55
client authentication, 352
Client mode (Cisco Easy VPN), 458
client/server requirements, Cisco Security
Manager, 716–718
clientless Citrix support (SSL VPN), 527
Clientless Mode (SSL VPN), 525
COBIT (Control Objectives for Information and
Related Technology), 752
versus ISO/IEC 27002, 753
“Code of Practice for Information Security
Management,” 751
color-aware policing, 229
Command and Control interface (IPS), 585
command authorization, configuring with
TACACS+, 285–286
commands
show interfaces rate-limit, 227
switchport port-security, 93
community PVLAN ports, 86
comparing
Cisco NAC appliance and NAC framework
solution, 378
EAP technologies, 365–366
hardware- and software-based firewalls, 140
L2 and L3 VPNs, 540–541
MPLS VPN and IPsec VPN, 536–537
RADIUS and TACACS+, 278
VPLS and VPWS, 552
components
of Cisco NAC appliance, 379
of Cisco NAC Framework solution, 386, 388
of CSA, 622
concentrators supported on Cisco NAC
Framework solution, 390
confidentiality, 9
configuration views (Cisco Security Manager),
707–708
configuring
AAA server groups, 281–282
ACLs, 29–31
classification ACLs, 48
directionality, 32
distributed time-based, 45
dynamic, 40–41
established, 43
extended, 38–39
iACLs, 47
named, 39
rACLs, 46
reflexive, 42
standard, 37–38
time-based, 44
turbo ACLs, 47
VACLs, 96–97
CAR, 226
CBAC, 122
global timeouts/thresholds, 123
inspection rule, 123
interface, 122
IP access list, 123
verifying configuration, 126
Cisco Aironet Wireless Access Points, 802.1x
authentication, 342–343
Cisco Catalyst switches, 802.1x authentication,
337–340, 342
Cisco DDoS Anomaly Detection and Mitigation
solution, Cisco Traffic Anomaly Detector,
653–659
Cisco Guard DDoS Mitigation, Cisco Traffic
Anomaly Detector, 660–666
Cisco IOS GET VPN, 513–518
Cisco IPS appliance
IPS inline interface pair mode, 604–608
IPS inline VLAN pair mode, 601–603
Cisco Secure ACS, 297–301
Cisco Security Appliance
EIGRP, 168–170
failover, configuring, 195
OSPF, 164–167
redundant interfaces, 158–159
RIP, 167–168
command authorization with TACACS+, 285–286
CoPP, 108–109
CSA, parameters, 636
CS-MARS, parameters, 691–693
custom signatures, 609–610
DHCP Snooping, 100–102
DMVPN
  DHCP topology, 483
  DHSD topology, 488–498
  hierarchical topology, 499–500
  MHSD topology, 498
  server load-balancing topology, 484–485
  SHSD topology, 477–482
ECMP forwarding, 162–163
FWSM, 202–204
interactive device access via VTY, 63
IP Source Guard, 102
IP source tracking, 220
IPS blocking, 609–610
L2VPN, 553–554
L3VPN, 544–550
login authentication
  password retry lockout, 286–287
  with TACACS+, 285–286
MPF, 190–192
MQC, 228
NBAR, 231–232
NetFlow, 240–241
PBR, 235–236
port security, 93
PPP, AAA using RADIUS, 285
PVLANs, 89–91
security contexts, 155–157
SSL VPN, 528–529
TCP Intercept, 233
traffic policing, 229
uRPF, 238–239
ZFW, 134–136
connectionless VPN, 539
connection-oriented VPN, 539
console port, interactive device access, 62
CONTINUE response (TACACS+), 277
control plane, 108

CoPP (Control Plane Policing), 107
  configuring, 108–109
correlation, 616
CPL (Cisco Policy Language), configuring ZFW, 134–136
CPU rate limiters, 109
cross launching, 713–715
crypto map table, 474
crypto socket table, 474
cryptographic VPN technologies, 421
cryptography, 408, 412
  asymmetric key cryptography, 412, 416
  symmetric key cryptography, 410–412
cryptosystems, 407
CSA (Cisco Security Agent), 614–615
  access control process, 618
  agent kit management, 626, 629
  components, 622
  configuration parameters, 636
  correlation, 616
  functional roles, 619, 622
  global correlation, 618
  group management, 630–632
  host management, 624–626
  rule modules, 635
CSA MC (Management Console), 622–623
  Agent User Interface control page, 632–634
  CSA agent kit management, 626, 629
  CSA group management, 630–632
  CSA host management, 624–626
CS-MARS (Cisco Security Monitoring, Analysis, and Response System), 669
  device support list, 675
  event processing, 677
  false positive processing, 678
  features, 670–671
  GC deployment, 682–683
  incidents, 676
  initializing, 691–693
  levels of operation, 685–687
  mitigation devices, 685
  network mapping, 674–675
  reporting devices, 684
  rules, 676
  security threat mitigation, 672–674
  sessions, 676
  software versioning, 683
standalone deployment, 680–681
topological awareness, 674–675
traffic flows, 687–689
web-based management interface, 689
custom signatures, configuring, 609–610

D

DAI (Dynamic ARP Inspection), 103
ARP packets, rate limiting, 106
ARP spoofing attacks, mitigating, 245–246
ARP validation checks, performing, 107
in DHCP environment, 105
in non-DHCP environment, 106
data link layer. See Layer 2 access control; Layer 2 attack mitigation techniques; Layer 2 security
data plane, 107
DCV (Device-Centric View), 707
DDoS attacks, 210, 641
debugging traffic with ACLs, 49
decryption, 408
default method lists (AAA), 279
default routes, 161–162
defense in depth, 15–16
deploying IPS, 570, 572
deployment scenarios
for Cisco NAC appliance, 380–381
for Cisco NAC Framework solution, 391
for CS-MARS
GC deployment, 682–683
levels of operation, 685–687
standalone deployment, 680–681
for MPLS VPN, 538
DES, 412
Detect mode (AD), 598
device management (Cisco Security Manager), 710
device security, 53
Auto-Secure feature, 75–76
banner messages, 65, 67
BOOTP, 69
CDP, 68
Cisco IOS Resilient Configuration, 67
device configuration, autoloading, 70
DHCP, 69
Finger, 69
FTP servers, 70
Gratuitous ARP, 72
HTTP, 73
infrastructure ACLs, 62
interactive access
via AUX port, 65
via console port, 62
via VTY port, 63–64
IP directed broadcast, 72
IP mask reply, 72
IP source routing, 71
IP Unreachable, 73
NTP, 74
PAD, 70
password protection, 55
cryptography, 57
ROMMON security, 57–60
strong passwords, creating, 56–57
physical security, 55
privilege levels, 61
Proxy ARP, 71
security checklist, 80–81
SNMP, 75
TCP/UDP small-servers, 69
TFTP, 70
user authentication, 60
DHCP (Dynamic Host Configuration Protocol), 69
configuring for DHCP spoofing attack mitigation, 253–254
DHCP Snooping, configuring, 100–102
DHCP spoofing attacks, mitigating, 253–254
DHDD (dual hub dual DMVPN) topology, 483
DHSD (dual hub single DMVPN) topology, configuring, 488–498
Diffie-Hellman algorithm, 414
Dijkstra algorithm, 163
directionality of ACLs, 32
distributed time-based ACLs, 45
DMVPN (Dynamic Multipoint VPN), 469–470
components, 472
data structures, 474
and GET VPN, 506
hub-and-spoke designs, 476  
DHDD topology, 483  
server load-balancing topology, 484–485  
SHSD topology, 477–482  
mesh spoke-to-spoke designs, 486  
DHSD topology, 488–498  
MHSD topology, 498–500  
network designs, 470, 472  
operation, 473  
domino effect, 16  
don’t care bits, 28  
DoS attacks, 639–640  
Downloadable IP ACLs, 293  
DSA (Digital Signature Algorithm), 415  
DVTI (dynamic VT1), 443  
implementing, 461–465  
dynamic ACLs, 40–41  
dynamic NAT, 173  
configuring, 176  
dynamic PAT, 174–176  
dynamic routing protocols, 473  

E  
EAP (Extensible Authentication Protocol), 334, 355, 385  
EAP-FAST, 359–362  
EAP-MD5, 356–357  
EAP-TLS, 357–359  
EAP-TTLS, 359  
LEAP, 364  
PEAP, 362–364  
technologies, comparing, 365–366  
EAP-FAST, 359–362  
EAP-MD5, 356–357  
EAP-TLS, 357–359  
EAP-TTLS, 359  
ECMP (equal-cost multiple path) forwarding,  
configuring, 162–163  
EIGRP (Enhanced IGRP), configuring on Cisco  
Security Appliance, 168–170  
e-mail inspection engine, 128  
e-mail policies, 10  
elite, 210  
embryonic connections, 215  
embryonic sessions, 120  
encrypted passwords, 57  
enetration, 408  
endpoint security, 613–614  
CSA, 614–615  
access control process, 618  
agent kit management, 626–629  
components, 622  
configuration parameters, 636  
correlation, 616  
functional roles, 619, 622  
global correlation, 618  
group management, 630–632  
host management, 624–626  
rule modules, 635  
endpoint software, 386  
enforcement methods (Cisco NAC Framework), 392  
NAC-L2-802.1x, 399–401  
NAC-L2-IP, 396–399  
NAC-L3-IP, 394–396  
Enterprise Mode (WPA), 354  
ERROR response (TACACS+), 276  
ESP, 432  
established ACLs, 43  
EtherChannel Guard, 99  
ethics policies, 10  
event management systems, 669  
event processing in CS-MARS, 677  
events, 676  
examples of security policies, 10  
EXEC banners, 65  
extended ACLs, 38–39  
external interfaces, 122  
external zone (AD), 597  
extranet VPN, 420, 425  

F  
failover, 193–197  
false positive processing in CS-MARS, 678  
features  
of Cisco ASDM, 732  
of Cisco SDM, 722–723  
of Cisco Security Manager, 700–702  
Finger, 69  
Firewall ACL Bypass, 129
firewall management system (Cisco Security Manager), 703

firewalls, 139
Adaptive Security Algorithm, security levels, 157–158
Cisco ASA 5500 Series Adaptive Security appliances, 143–144
Cisco FWSM, 143–144
Cisco IOS Firewall, 113
Cisco PIX 500 Series Security appliances, 140
software, 144
Cisco Security Appliance
   ACLs, 186–190
Cisco AnyConnect VPN Client, 192
   EIGRP, configuring, 168–170
failover, 193–197
   IP routing, 159–163
MPF, configuring, 190–192
OSPF, configuring, 164–167
redundant interfaces, configuring, 158–159
RIP, configuring, 167–168
   Routed Firewall mode, 146
   Transparent Firewall mode, 146–147
Cisco Security Appliance software, OS
   software, 145
FWSM, 198
   configuring, 202–204
installing, 200
   OS software, 199
Identity NAT, 179
NAT, 170–172
dynamic NAT, 173–176
dynamic PAT, 174–176
order of processing, 184
static NAT, 176
Policy NAT, 183
security contexts, 152
   configuring, 155–157
   routed mode, 153
   transparent mode, 153–155
stateful packet inspection, 148
Static identity NAT, 180

flood engines, 578
flooding, 210
fraggle attacks, 212

frameworks, 751
   COBIT, 752
   versus ISO/IEC 27002, 753
   ISO/IEC 17799, 751–752
FTP servers, 70
functional roles of CSA, 619, 622
FWSM (Firewall Services Module), 198
   configuring, 202–204
   installing, 200
   OS software, 199

G
GAME (Generic Authorization Message Exchange), 386
GC (global controller) deployment, CS-MARs, 682–683
GCKS (Group Controller/Key Server), 507
GDOI (Group Domain of Interpretation), 507–511
GET (Group Entrusted Transport) VPN, 503
   benefits of, 506
   deployment options, 507
   and DMVPN, 506
   features of, 504
   functional components, 507
   GDOI, 509, 511
   group member ACL, 512
   implementing, 513–518
   IP header preservation, 511
   versus IPsec VPNs, 504
GLBA (Gramm-Leach-Bliley Act), 754
   Cisco solutions for, 756
   penalties for violations, 756
   requirements, 755
global correlation, CSA, 618
Gratuitous ARP, 72
GRE (Generic Routing Encapsulation) protocol, 472
group management (CSA), 630–632
Group Member, 508
guidelines, 12, 750
H

hackers, 210
hardening devices
  Auto-Secure feature, 75–76
  BOOTP, 69
  CDP, 68
  Cisco IOS Resilient Configuration, 67
device configuration, autoloading, 70
  DHCP, 69
  Finger, 69
  FTP servers, 70
  Gratuitous ARP, 72
  HTTP, 73
  ICMP Unreachable, 73
  infrastructure ACLs, 62
interactive access
  via AUX port, 65
  via console port, 62
  via VTY port, 63–64
IP directed broadcast, 72
IP mask reply, 72
IP source routing, 71
NTP, 74
PAD, 70
physical security, 55
privilege levels, 61
Proxy ARP, 71
SNMP, 75
TCP/UDP small-servers, 69
TFTP, 70
user authentication, 60
with password protection, 55
  encryption, 57
  ROMMON security, 57–60
  strong passwords, creating, 56–57
hardware-based firewalls versus
software-based, 140
hash algorithms, 416–420
hash value, 409
HCAP (Host Credential Authorization Protocol), 386
hierarchical DMVPN topology, configuring,
499–500

high availability, 598
  IPS fail-open mechanism, 599
  IPS failover mechanism, 599
  load balancing, 600
HIPAA (Health Insurance Portability and Accountability Act), 757
  Cisco solutions for, 759
  penalties for violations, 758
  requirements, 758
HMAC (keyed-hash message authentication code), 418
host management (CSA), 624–626
host-based attacks, life cycle, 614
HTTP (HyperText Transfer Protocol), 73
  device access from ASDM, 77
HTTP inspection engine, 127
hub-and-spoke designs (DMVPN), 476
  DHDD topology, configuring, 483
  server load-balancing topology, configuring,
  484–485
  SHSD topology, 477–482
hybrid VPNs, 425

I

I&A (identification and authentication, 311
iACLs (infrastructure protection ACLs), 47
IBNS (Identity-Based Networking Services), 326
ICMP flood attacks, characterizing, 212–215
IDAPI, 576
IDCONF, 576
identification, 311
Identity NAT, 179
IDIOM, 576
idle time, 93
IDM (Cisco IPS Device Manager),
  78, 601, 740–742
IDS (intrusion detection systems), 561
IEEE 802.1x, 332
  components of, 330
  EAP methods, 334
  multipoint solution, deploying, 335–336
  point-to-point solution, deploying, 334
  switch port states, 332–333
IEEE 802.11 protocol standards, 348
IETF L3VPN, 550
IETF website, 534
IKE (Internet Key Exchange), 435–437
IKEv2, 438–440
illegal zone (AD), 597
implementing
   AAA, 278–279
   ACLs, 36
   Cisco IOS GET VPNs, 513–518
   IPsec VPN, 449
      remote access, 455–465
      site-to-site, 451–455
   L2VPN, 553–554
   L3VPN, 543–550
   SSL VPN, 528–529
Inactive mode (AD), 598
in-band mode (Cisco NAC Appliance), 381
inbound ACLs, 32
incidents, 676
incoming banners, 66
Information Flow security model, 13
information sensitivity policies, 10
informative policies, 749
infrastructure ACLs, 62
initializing
   Cisco DDoS Anomaly Detection and Mitigation
      solution, Cisco Traffic Anomaly Detector, 655–656
   Cisco Guard DDoS Mitigation, Cisco Traffic
      Anomaly Detector, 661–662
   CS-MARS, 691–693
inline-on-a-stick, 592
inline interface mode (IPS sensor software), 591
installing FWSM module, 200
integrity, 9
interfaces, applying ACLs to, 30–31
intermediate level 2 operation, CS-MARS, 685
internal interfaces, 122
internal zone (AD), 597
Internet VPN, 420, 425
intranet VPN, 420, 425
inverse masks, 28
IP addressing, 23
   address classes, 24–26
   inverse masks, 28
   private addresses, 26
   subnet masks, 28
IP directed broadcast, 72
IP header preservation, 511
IP mask reply, 72
IP named ACLs, 39
IP routing, 159
   default routes, 161–162
   ECMP forwarding, 162–163
   static route tracking, 160
   static routes, 160
IP Source Guard, 102
IP source routing, 71
IP source tracking, 219–220
IP spoofing, 209, 220
   using access lists, 221–222
   using IP Source Guard, 222
   using uRPF, 222
IP Unreachable, 73
IPS (Intrusion Prevention Systems), 561
   Cisco AIP-SSM, 567
   Cisco IDS-2, 565, 567
   Cisco IOS IPS, 569–570
   Cisco IPS 4200 Series sensors, 563–564
   Cisco IPS Sensor OS Software, 572–574
      AD, 597–598
         blocking, 593–594
   communication protocols, 575
   interface modes, 589–592
   interface roles, 585–589
   IPS event actions, 582–583
   IPS events, 580–581
   IPS rate limiting, 594
   RR, 583–584
   security policies, 596
   sensor software partitions, 577
   signatures, 578–580
   TR, 584
   user roles, 576
   virtualization, 595
Cisco IPS-AIM, 568
deploying, 570–572
high availability, 598
   IPS fail-open mechanism, 599
   IPS failover mechanism, 599
   load-balancing, 600
WLAN IPS solution, 367
IPS 4200 series appliance sensors, 78
  ACLs, 79
  HTTP/HTTPS access, 79
  SSH access, 79
  Telnet access, 79
user accounts, 80
IPS blocking, configuring, 609–610
IPS fail-open mechanism, 599
IPS failover mechanism, 599
IPS inline interface pair mode, configuring, 604, 606–608
IPS inline VLAN pair mode, configuring, 601–603
IPS management (Cisco Security Manager), 704–705
IPsec VPN, 425
  anti-replay service, 434
  DMVPN, 469–470
    components, 472
    data structures, 474
    hub-and-spoke designs, 476–485
    mesh spoke-to-spoke designs, 486–500
    network designs, 470–472
  operation, 473
IKE, 435
IKEv2, 438–440
implementing, 449
ISAKMP profiles, 441
phase 1 negotiation, 436
phase 2 negotiation, 437
profiles, 443
protocol headers, 432–434
remote access
  Cisco Easy VPN, 456–461
  DVTI, 461–465
  implementing, 455
RFCs, 426–430
site-to-site, implementing, 451–455
versus GET VPNS, 504
versus MPLS VPN, 536–537
versus SSL VPNS, 522
IPsec VTI, 443–445
IPv4, 23
IPv6, 23
IRT (Incident Response Team), 257–258
  5-step reaction process, 259–261
ISAKMP, 435
  profiles, 441
islands of security, 15
ISM (Industrial, Scientific, and Medical) radio spectrum, 348
ISO/IEC 17799 specification, 751–752
ISO/IEC 27001 specification, 752
ISO/IEC 27002 specification, 752
  versus COBIT, 753
isolated PVLAN ports, 86

L

L2VPN, 551
  implementing, 553–554
  service architectures, 552
  versus L3 VPN, 540–541
L3 VPN, 542
  components, 543
  implementing, 543–550
  VRF tables, 543
  versus L2 VPN, 540–541
label switching, 533
  in MPLS, 536
Lattice security model, 13
Layer 2 access control
  Cisco Trust and Identity Management Solutions, 326
    Cisco IBNS, 327–329
IEEE 802.1x, 332
  components, 330
  EAP methods, 334
  multipoint solution, deploying, 335–336
  point-to-point solution, deploying, 334
  switch port states, 332–333
Layer 2 attack mitigation techniques, 242
  ACLs, configuring, 249–251
  BPDU Guard, configuring, 252
  DAI, 245–246
  DHCP snooping, configuring, 253–254
  PEAP, enabling, 254–256
  ROOT Guard, configuring, 252–253
  switch Port Security feature, 242–244
  VLAN configuration, modifying, 247–249
  VTP passwords, 246–247
Layer 2 security, 83
    best practices, 109
Layer 3 attack mitigation techniques
    CAR, 225–226
    IP source tracking, 219–220
    IP spoofing, 220
        using access lists, 221–222
        using uRPF, 222
    MQC, 227–228
    NBAR
        configuring, 231–232
        PDLM, 231
        protocol discovery, 230
    NetFlow, 239
        configuring, 240–241
    PBR, 234
        configuring, 235–236
    TCP Intercept, 232
        as firewall feature, 234
        configuring, 233
    traffic characterization, 212
        using ACLs, 212–218
    traffic classification, 224
    traffic policing, 229
    uRPF, 236–237
        configuring, 238–239
layered security, 15–16
LC (local controller) deployment, CS-MARs, 680–681
LDP (Label Distribution Protocol), 535
LEAP (Lightweight EAP), 364
Learn mode (AD), 598
legislation for regulatory compliance, 754
    GLBA, 754
        Cisco solutions for, 756
        penalties for violations, 756
        requirements, 755
    HIPAA, 757
        Cisco solutions for, 759
        penalties for violations, 758
        requirements, 758
    in Asia-Pacific region, 766
    in Europe, 766
    in USA, 765
    SOX, 760
        Cisco solutions for, 764
        penalties for violations, 763
        requirements, 761–763
    LFIB (Label Forwarding Information Base), 535
    load balancing, 600
    lock and key, 40–41
    login authentication
        configuring with TACACS+, 285–286
        password retry lockout, configuring, 286–287
    login banners, 65
    Loop Guard, 99
    loop prevention, STP
        BPDU guard, 98
        EtherChannel Guard, 99
        Loop Guard, 99
        root guard, 98
    lost passwords, recovering, 56–60
    LSP (Label Switch Path), 535
    LSRs (Label Switch Routers), 534

M

    MAC ACLs, 97
    MAC authentication, 352
    main mode (IKE), 436
    management plane, 107
    MAR (Machine Access Restrictions), 295
    mathematical algorithm OTP, 312
    MD (Message Digest) algorithms, 416
    mechanics of Cisco NAC Framework solution, 383–384
    mesh spoke-to-spoke designs (DMVPN), 486
        DHSD topology, configuring, 488–498
        hierarchical topology, configuring, 499–500
        MHS topology, configuring, 498
    meta engine, 579
    method lists, configuring server groups, 281–282
    MHSMD (multihub single DMVPN) topology,
        configuring, 498
    mitigating
        replay attacks with OTP, 313
        WLAN attacks, 367–368
    mitigation devices, 685
    MITM attacks, 209
monitor mode, Cisco SDM, 728–729
MOTD banners, 65
MP-BGP Peering, 543
MPF (Modular Policy Framework), 190
configuring, 190–192
MPLS (Multi-Protocol Label Switching)
core architecture, 534
label switching, 536
LFIB, 535
LSP, 535
LSRs, 534
packet forwarding, 536
MPLS Forwarding, 543
MPLS VPN, 533
deployment scenarios, 538
L2VPN, 551
implementing, 553–554
service architectures, 552
L3 VPN, 542
components, 543
implementing, 544–550
VRF tables, 543
versus IPSec VPN, 536–537
MQC (Modular QoS CLI), Unconditional Packet Discard feature, 227
MSFC (Multilayer Switch Feature Card)
placement
in multiple context mode, 201
in single context mode, 200
multifactor authentication, I&A, 311
multilayer perimeter solution, 15
multipoint 802.1x solution, deploying, 335–336
multistring engine, 579
MVP (Multi-Verification Process)
arichitecture, 647
MyDoom worm, 619

N

NAC (Network Access Control), 296, 326, 375
Cisco NAC, 376
for WLANs, 366
noncompliant hosts, handling, 375
NAC framework, comparing with Cisco NAC
appliance, 378

NAC-L2-802.1x (Cisco NAC Framework),
security policy enforcement, 399–401
NAC-L2-IP (Cisco NAC Framework), security
policy enforcement, 396–399
NAC-L3-IP (Cisco NAC Framework), security
policy enforcement, 394–396
NAT (Network Access Filter), 294
named ACLs, 39
named method lists (AAA), 279
NAP (Network Access Profiles), 296
NAR (Network Access Restrictions), 295
NAT, 115, 170–172
dynamic NAT, 173
configuring, 176
dynamic PAT, 174
configuring, 176
Identity NAT, 179
NAT Exemption, 182
order of processing, 184
Policy NAT, 183
Static identity NAT, 180
static NAT, configuring, 176
NAT exemption, 182
NBAR (Network Based Application Recognition),
230
configuring, 231–232
PDLM, 231
protocol discovery, 230
NetFlow, 239
configuring, 240–241
Network Extension mode (Cisco Easy VPN), 458
Network Extension Plus+ mode (Cisco Easy
VPN), 459
NHRP (Next Hop Resolution Protocol), 472
NHRP mapping table, 474
noncryptographic VPN technologies, 421
nonstateful failover mode, 194
normalizer engine, 579
NTP (Network Time Protocol), 74
numbers, assigning to ACLs, 29

O

object grouping, 188–190
one-step lockdown feature, Cisco SDM, 726–728
“open-access” policy, 351
open authentication, 352
OSI model, data link layer, 83
OSPF (Open Shortest Path First), 163
  configuring on Cisco Security Appliance, 164–167
OTP (one-time passwords), 312
  replay attacks, countering, 313
  S/KEY, 313
outbound ACLs, 33
out-of-band mode (Cisco NAC Appliance), 381

P

packet classification, 224
packet flow rules (ACLs), 33
packet forwarding in MPLS, 536
packet sniffing, 210
packets
  ARP, rate limiting, 106
  RADIUS, 271
  TACACS+, 275
PACLs (per-port VLAN ACL), 223
PAD, 70
PAM (Port-to-Application Mapping), 114
pass phrases, 56
password cracking, 209
password policies, 11
password protection, 55
  encryption, 57
  ROMMON security, 57–60
  strong passwords, creating, 56–57
password recovery, 56
password retry lockout, configuring, 286–287
passwords, OTP, 312
  replay attacks, countering, 313
  S/KEY, 313
PBR (policy-based routing), 234
  configuring, 235–236
PCV (Policy-Centric View), 708
PDIOO model, 6
PDLM (Packet Description Language Module), 231
PDM (Cisco PIX Device Manager), 739–740
PE (Provider Edge) routers, 534
PEAP (Protected EAP), 362–364
  enabling for 802.1x attack mitigation, 254–256
percentage-based policing and shaping, 229
perimeter security, 13–15
Personal Mode (WPA), 354
physical security, 55
ping sweeps, 209
PKCS (Public-Key Cryptography Standards), 415
PKI (Public Key Infrastructure), 445
  certificate enrollment, 447–448
plaintext, 408
platform management (Cisco Security Manager), 706
point-to-point 802.1x solution, deploying, 334
policies, 635
  configuring on Cisco Traffic Anomaly Detector, 658
policing, 229
Policy NAT, 183
Port ACLs, 94
port blocking, 91
port scanning, 209
port security, 92–93
Port Security feature
  CAM table overflow attacks, mitigating, 242–243
  MAC spoofing attacks, mitigating, 243–244
port-level traffic control
  protected ports, 85
  storm control, 84
ports required for CS-MARS operation, 687–689
posture states (Cisco NAC Framework solution), 385
PPP (Point-to-Point Protocol), configuring AAA
  using RADIUS, 285
private IP addresses, 26
privilege levels, 61
procedures, 11, 750
professional attackers, 210
profiles
  IPsec, 443
  SPC, 293
promiscuous mode (IPS sensor software), 589
promiscuous PVLAN ports, 86
protect mode (port security), 92
protected ports, 85
protocol compliance (Cisco Secure ACS), RADIUS, 291–292
protocol headers, IPsec VPN, 432, 434
protocols in Cisco NAC Framework solution, 385
Proxy ARP, 71
PVLAN attacks, mitigating, 249–251
PVLAN edge, 85
PVLANs, 85
  configuring, 89–91
  port blocking, 91
  port security, 92–93
    configuring, 93
  secondary VLANs, 87
  support for on Catalyst switches, 88

REJECT response (TACACS+), 276
remote access IPsec VPN
  Cisco Easy VPN, implementing, 456–461
  DVTI, implementing, 461–465
  implementing, 455
replay attacks, countering with OTP, 313
reporting devices, 684
restrict mode (port security), 92
RF bands in 802.11 standards, 348
RFC 1918, 26
RFCs, IPsec VPN-related, 426–428, 430
RIP, configuring on Cisco Security Appliance, 167–168
RIRs (Regional Internet Registries), 27
risk assessment, 211
  Layer 2 mitigation techniques, 242
    ACLs, configuring, 249–251
    BPDU Guard, configuring, 252
    DAI, 245–246
    DHCP snooping, configuring, 253–254
    PEAP, enabling, 254–256
    switch Port Security feature, 242–244
    VLAN configuration, modifying, 247–249
    VTP passwords, 246–247
  Layer 3 mitigation techniques
    CAR, 225–226
    IP source tracking, 219–220
    IP spoofing, 220–222
    MQC, 227–228
    NBAR, 230–232
    NetFlow, 239–241
    PBR, 234–236
    TCP Intercept, 232–234
    traffic characterization, 212–218
    traffic classification, 224
    traffic policing, 229
    uRPF, 236–239
risk assessment policies, 11
ROMMON security, 57–60
ROOT Guard, configuring for STP attack mitigation, 252–253
root guard, 98
Routed Firewall mode (Cisco Security Appliance), 146
routed mode, multiple security contexts, 153
Router ACLs, 94

RAC (RADIUS Authorization Components), 294
rACls (receive ACLs), 46
radio waves, 347
RADIUS, 270, 385
  Cisco Secure ACS compliance with, 291–292
  communication, 271–273
  packets, 271
  password encryption, 273
  PPP, configuring AAA, 285
  security, 273
  versus TACACS+, 278
RADIUS-enabled token server, configuring Cisco Secure ACS, 317–321
rate limiting, 594
  ARP packets, 106
RBAC (Role-Based Access Control), 711–712
RDEP2, 576
reconnaissance attacks, 208
recovering lost passwords, 56–60
redundant interfaces, configuring on Cisco Security Appliance, 158–159
reflexive ACLs, 42
regulatory policies, 749
  legislation, 754
    GLBA, 754–756
    HIPAA, 757–759
    in Asia-Pacific region, 766
    in Europe, 766
    in USA, 765
    SOX, 760–764
router security audit feature, Cisco SDM, 725
router-generated traffic inspection, 131
routers supported on Cisco NAC Framework solution, 388
routers supported on Cisco SDM, 729–730
RR (Risk Rating), 583–584
RSA algorithm, 414
RSA SecurID token server, configuring Cisco Secure ACS, 321–322
RTT (Round Trip Time), 216
rule modules, 635
rules, 676

S

S/KEY, 313
Safe Blueprint, 6
script kiddies, 210
SDEE (Security Device Event Exchange), 576
SDM (Cisco Router and Security Device Manager)
  features, 722–723
  monitor mode, 728–729
  one-step lockdown feature, 726–728
  operation, 723–724
  router security audit feature, 725
  supported routers and IOS versions, 729–730
  system requirements, 730–731
SDN (Cisco Self-Defending Network), 373
Cisco NAC, 376
secondary VLANs, 87
secure VPN, 424–425, 540. See also IPsec VPN
  anti-replay service, 434
  IKE, 435
  IKEv2, 438–440
  ISAKMP profiles, 441
  phase 1 negotiation, 436
  phase 2 negotiation, 437
  profiles, 443
  protocol headers, 432–434
  RFCs, 426–428, 430
security contexts, 152
  configuring, 155–157
  routed mode, 153
  transparent mode, 153–155
security incident response, 256–257
  IRT, 257–258
  5-step reaction process, 259–261
security levels, 157–158
security models, 13, 747
security policies, 9–10, 596, 616, 749
  device security policy, 53
  security checklist, 80–81
  enforcement, Cisco NAC Framework solution, 392
  NAC-L2-802.1x, 399–401
  NAC-L2-IP, 396, 399
  NAC-L3-IP, 394, 396
security violation modes (port security), 92
security wheel, 17–18
security zones, 133
sensing interface (IPS), 586
server groups, configuring, 281–282
service engine, 579
services
  accounting, 284
  authentication, 282
  authorization, 283
sessions, CS-MARS, 676
SFR (Signature Fidelity Rating), 584
SHA (Secure Hash Algorithm), 418
shared-key authentication, 352
shell command authorization sets, 294
shift in security paradigm, 7
show interfaces rate-limit command, 227
SHSD (single hub single DMVPN) topology, 477–482
shutdown mode (port security), 92
signature engines, 578–580
signatureless endpoint security, 614
signatures, 578–580
  custom, configuring, 609–610
single-channel TCP/UDP inspection, 121
site-to-site IPsec VPNs, implementing, 451–455
SLB (server load-balancing) topology,
  configuring, 484–485
SLIP-PPP banner messages, 66
smart cards, 314–315
smurf attacks, characterizing, 212, 214–215
SNMP (Simple Network Management Protocol), 75
software versioning, CS-MARS, 683
software-based firewalls versus
hardware-based, 140
source routing, 71
source tracking, 219–220
SOX (Sarbanes-Oxley Act), 760
Cisco solutions for, 764
penalties for violations, 763
requirements, 761–763
SPC (Shared Profile Components), 293
SPI (stateful packet inspection), 114
spread-spectrum technology, 347
SSH (Secure Shell)
device access from Cisco PIX 500,
ASA 5500, 77
device access, configuring, 64
SSID (Service Set Identifiers), 351
SSL VPNs
access methods, 525
Cisco AnyConnect VPN Client, 530
Citrix support, 527
configuring, 528–529
deployment options, 524
features, 523–524
versus IPsec VPNs, 522–523
standalone deployment, CS-MARS, 680–681
standard ACLs, 37–38
standards, 11, 750
state engine, 579
stateful failover mode, 194
stateful packet inspection, 148
static identity NAT, 180
static NAT, configuring, 176
static PAT, 178
static route tracking, 160
static routes, 160
static WEP, 353
STM (security threat mitigation) systems,
CS-MARS, 672–675
storm control, 84
STP
BPDU guard, 98
EtherChannel Guard, 99
Loop Guard, 99
Root Guard, 98
STP attacks, mitigating, 252–253
stream cipher, 410
string engine, 579
subnet masks, 28
SUP 720, CPU rate limiters, 109
supplicant (IEEE 802.1x), 330
supported devices on Cisco Security Manager,
715–716
supported firewalls on Cisco ASDM, 738
supported routers on Cisco SDM, 729–730
SVTI (static VTI), 443
sweep engine, 579
switches supported on Cisco NAC Framework
solution, 388–390
switchport port-security command, 93
system requirements
for Cisco IDM, 742
for Cisco SDM, 730–731
TACACS+, 274
command authorization, configuring, 285–286
communication, 276–277
login authentication, configuring, 285–286
packets, 275
security, 277
versus RADIUS, 278
tag switching, 533
TCP hijacking, 209
TCP Intercept, 232
as firewall feature, 234
configuring, 233
TCP normalization, 145
TCP/UDP small-servers, 69
TCV (Topology-Centric View), 708
TDP (Tag Distribution Protocol), 535
telnet, configuring device access, 63
from Cisco PIX 500, 76
TFTP (Trivial File Transfer Protocol), 70
Thick Client Mode (SSL VPN), 525
Thin Client Mode (SSL VPN), 525
threat modeling, 211
time-based ACLs, 44
time-synchronized OTP, 313
TKIP (Temporal Key Integrity Protocol), 353
TLS (Transport Layer Security) protocol, 521
tokens, 314–315
  RADIUS-enabled token server, configuring Cisco Secure ACS, 317–321
  RSA SecurID token server, configuring Cisco Secure ACS, 321–322
topological awareness of CS-MARS, 674–675
TR (Threat Rating), 584
traffic anomaly engine, 579
traffic characterization, 212
  using ACLs, 212–218
traffic classification, 224, 227
traffic flow requirements, Cisco Security Manager, 719, 721
traffic flows in CS-MARS, 687–689
traffic ICMP engine, 579
traffic marking, 224
traffic policing, 229
traffic, debugging, 49
transit ACLs, 47
Transparent Firewall mode (Cisco Security Appliance), 146–147
transparent IOS Firewall, 130
transparent mode, multiple security contexts, 153–155
transport mode (IPsec), 430
tree-based DMVPN topology, configuring, 499–500
trojan engine, 579
Trojans, 209
trusted VPNs, 424, 540
  comparing L2 and L3 VPNs, 540–541
  L2VPN, 551
    implementing, 553–554
    service architectures, 552
  L3 VPN, 542
    components, 543
    implementing, 544–550
    VRF tables, 543
tunnel mode (IPsec), 430
Turbo ACLs, 46
TVR (Target Value Rating), 584
two-factor authentication systems
  Cisco Secure ACS, support for, 315–316
  OTP, 312–313
  S/KEY, 313
  smart cards, 314–315
tokens, 314–315
  Two-Rate Policing, 229
  Type 5 passwords, 55
  Type 7 passwords, 55
U
unauthorized port state, 332–333
Unconditional Packet Discard feature (MQC), 227
uRPF (Unicast RPF), 236–237
  antispoofing, 222
  configuring, 238–239
user authentication, 60
user requirements, Cisco ASDM, 738
V
VACLs (VLAN ACLs), 95
  configuring, 96–97
  verifying CBAC configuration, 126
VFR (Virtual Fragmentation and Reassembly), 130–131
virtualization, 595
viruses, 208
VLAN configuration, modifying for VLAN hopping attack mitigation, 247–249
VPLS (Virtual Private LAN Service), 552
  implementing, 554
VPN management (Cisco Security Manager), 704
VPN Route Target Communities, 543
VPNs, 420
  connection-oriented, 539
  connectionless, 539
  extranet VPNs, 420
  GET VPNs, 503
    benefits of, 506
    deployment options, 507
    DMVPN, 506
    features of, 504
    functional components, 507
    GDOI, 509, 511
    group member ACL, 512
implementing, 513–518
IP header preservation, 511
versus IPsec VPNs, 504
hybrid VPNs, 425
Internet VPNs, 420
intranet VPNs, 420
IPsec VPN, 425
anti-replay service, 434
DMVPN, 469–500
IKE, 435
IKEv2, 438–440
implementing, 449–465
ISAKMP profiles, 441
phase 1 negotiation, 436
phase 2 negotiation, 437
profiles, 443
protocol headers, 432–434
RFCs, 426–430
for WLANs, 367
MPLS VPN, 533
deployment scenarios, 538
versus IPsec VPN, 536–537
secure VPNs, 424, 540
SSL
access methods, 525
Cisco AnyConnect VPN Client, 530
Citrix support, 527
configuring, 528–529
deployment options, 524
features, 523–524
versus IPsec VPNs, 522–523
Trusted VPN technologies, 424, 540
comparing L2 and L3 VPNs, 540–541
L2VPN, 553–554
L2VPN, 551–552
L3 VPN, 542–550
VPWS (Virtual Private Wire Service), 552–553
VRF tables, 543
VTP passwords, mitigating VTP attacks, 246–247
VTY port, interactive device access, 63–64

W
web-based management interface, CS-MARS, 689
websites, IETF, 534
WEP (Wired Equivalent Privacy), 353
Wi-Fi Alliance, 348
wireless access points supported on Cisco NAC
Framework solution, 390
wireless bridges, 349
wireless LAN controllers supported on Cisco
NAC Framework solution, 391
wireless NIC, 349
wire-speed ACLs. See VACLs
WLAN IPS solution, 367
WLANs, 347
AP, 349
Cisco Unified Wireless Network solution, 368–370
components of, 349
IEEE protocol standards, 348
NAC, 366
security, 350
attacks, mitigating, 367–368
available technologies, 351
client authentication, 352
EAP, 355
EAP-FAST, 359–360, 362
EAP-MD5, 356–357
EAP-TLS, 357–359
EAP-TTLS, 359
LEAP, 364
MAC authentication, 352
“open-access” policy, 351
PEAP, 362, 364
SSID, 351
WEP, 353
WPA, 353–354
spread-spectrum technology, 347
VPN IPsec, 367
wireless NIC, 349
workflow mode (Cisco Security Manager), 710–711
worms, 208
WPA (Wi-Fi Protected Access), 353–354
WPA2, 354
X-Y-Z

zero-day attacks, MyDoom worm, 619
ZFW (Zone-Based Policy Firewall), 115, 132
  AIC, 136
    configuring, 134–136
    security zones, 133
zone filters, configuring on Cisco Traffic Anomaly Detector, 657
zones (AD), 597