CCIE Professional Development

Network Security Technologies and Solutions

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

ciscopress.com

Yusuf Bhaiji, CCIE No. 9305

CCIE Professional Development

Network Security Technologies and Solutions

Yusuf Bhaiji, CCIE No. 9305

Cisco Press

Cisco Press
201 West 103rd Street
Indianapolis, IN 46290 USA

CCIE Professional Development

Network Security Technologies and Solutions

Yusuf Bhaiji

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

Printed in the United States of America

Third Printing September 2011

Library of Congress Cataloging-in-Publication Data:

Bhaiji, Fahim Hussain Yusuf.

Network security technologies and solutions / Yusuf Bhaiji.

p. cm.

ISBN 978-1-58705-246-0 (pbk.)

1. Computer networks--Security measures. I. Title.

TK5105.59.B468 2008

005.8--dc22

2008003231

ISBN-13: 978-1-58705-246-6

ISBN-10: 1-58705-246-6

Warning and Disclaimer

This book is designed to provide information about network security technologies and solutions. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Contents

Icons Used in This Book

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 comprehendible 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 andidate 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 1, “Overview of Network Security,” introduces principles of network security, security models, and a basic overview of security standards, policies, and the network security framework.
- 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.
- Chapter 23, "Security Monitoring and Correlation," covers the innovative Security Monitoring, Analysis, and Response System (CS-MARS) based on the Security Threat Mitigation (STM) System. The chapter provides key concepts of CS-MARS and deployment guidelines.

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 *x*DM 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.

å*Network Security Technologies and Solutions* is a complete reference book, like a security dictionary, an encyclopedia, and an administrator's guide—all in one.

CHAPTER 4

Security Features on Switches

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.

NOTE The configuration examples shown in this chapter are based on Cisco IOS Software syntax only (also known as native mode). Catalyst Operating System (CatOS) software-based examples are not covered.

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.

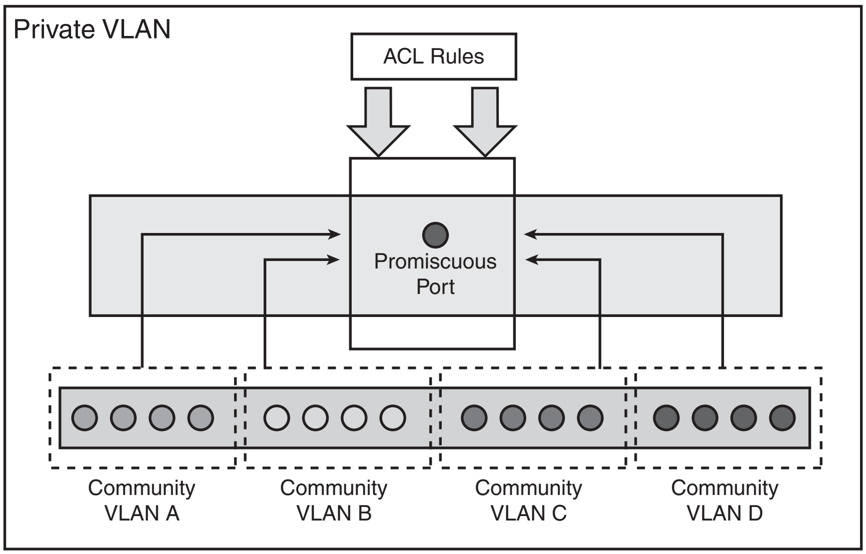
It is possible for isolated and community port traffic to enter or leave the switch through a trunk interface because trunks support VLANs carrying traffic among isolated, community, and promiscuous ports. Hence, PVLAN ports are associated with a separate set of VLANs that are used to create the PVLAN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

Figure 4-1b *PVLAN Traffic Flow Policies*

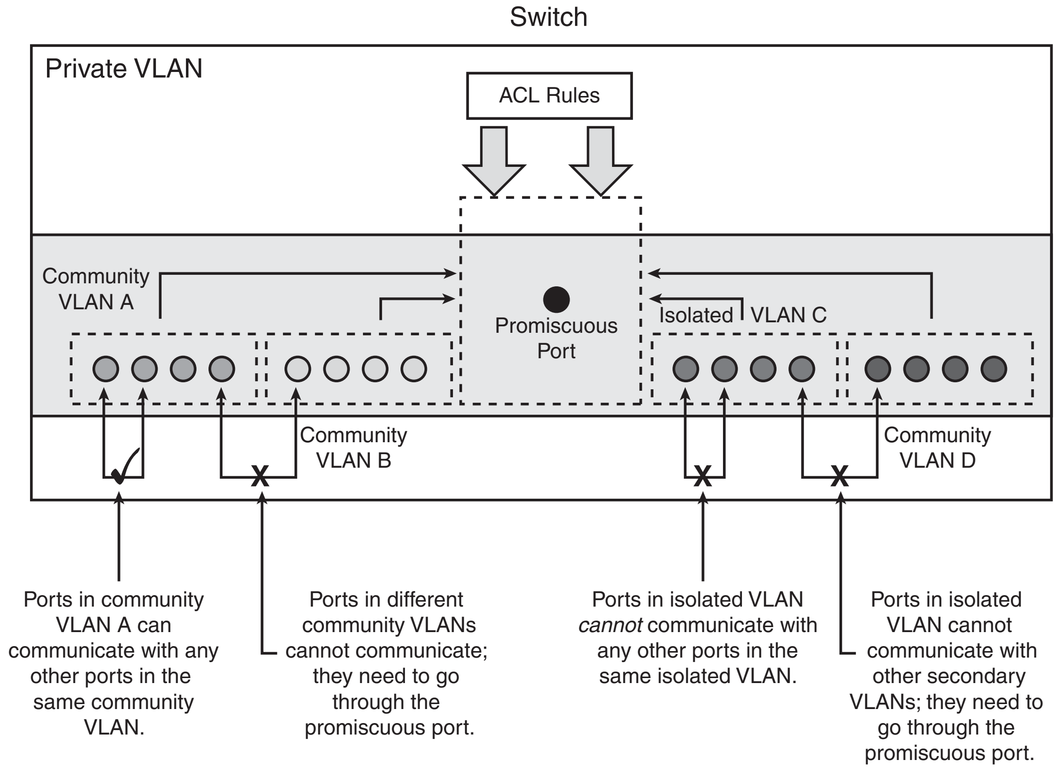


Table 4-1 shows a list of Cisco switches that support the PVLAN feature with the respective software version.

Table 4-1 *VLAN Support on Catalyst Switches*

Platform	Software Version	Isolated VLAN	PVLAN Edge (Protected Port)	Community VLAN
Catalyst 8500	Not Supported	—	—	—
Catalyst 6500/6000 — CatOS on Supervisor and Cisco IOS on MSFC	5.4(1) on Supervisor and 12.0(7)XE1 on MSFC	Yes	N/A	Yes
Catalyst 6500/6000 — Cisco IOS System software	12.1(8a)EX, 12.1(11b)E1	Yes	N/A	Yes

Table 4-1 *VLAN Support on Catalyst Switches (Continued)*

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

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.

```
Hostname(config)# interface Fastethernet 1/10
Hostname(config-if)# switchport mode private-vlan promiscuous
Hostname(config-if)# switchport private-vlan mapping 101 201-202,301
```

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)

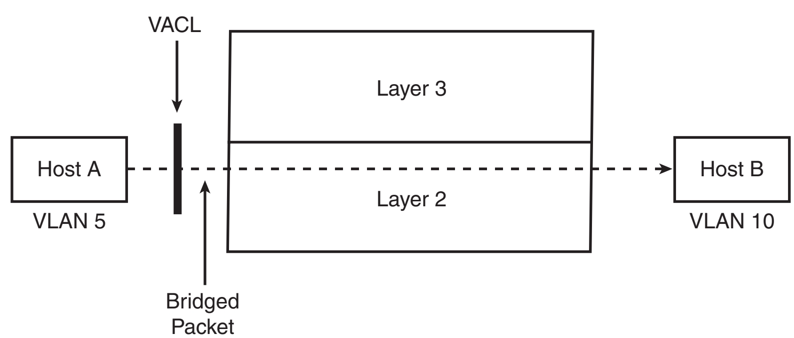
VLAN ACL (also called *VLAN map*) provides packet filtering for *all* types of traffic that are bridged within a VLAN or routed into or out of the VLAN. Unlike Router ACL, VACL is not defined by a direction (input or output). All packets entering the VLAN (bridged or routed) are checked against the VACL. 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.

Figure 4-2 *VACL on a Bridged Port*

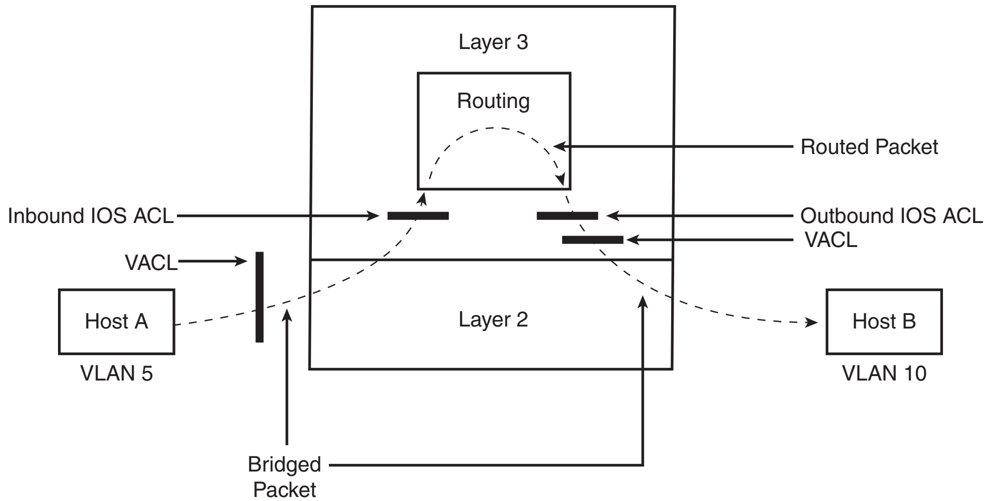


VACL on a Routed Port

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

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-access-map)#match ip address 1
Switch(config-access-map)#action drop
Switch(config-access-map)#exit
Switch(config)#vlan access-map mymap 20
Switch(config-access-map)#match ip address 2
```

Example 4-6 *VACL Configuration Example (Continued)*

```
Switch(config-access-map)#action forward
Switch(config-access-map)#exit
Switch(config)# vlan filter mymap vlan-list 5-10
Switch(config-access-map)#end

Switch# show vlan access-map
Vlan access-map "mymap"  10
  Match clauses:
    ip  address: 1
  Action:
    drop
Vlan access-map "mymap"  20
  Match clauses:
    ip  address: 2
  Action:
    Forward

Switch# show vlan filter
VLAN Map mymap is filtering VLANs:
  5-10
```

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.

Example 4-7 *MAC ACL Configuration Example*

```
Switch(config)# mac access-list extended my-mac-acl
Switch(config-ext-macl)# deny any any aarp
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# exit
Switch(config)# interface Fastethernet0/10
Switch(config-if)# mac access-group my-mac-acl in
Switch(config-if)# end
Switch#
```

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*

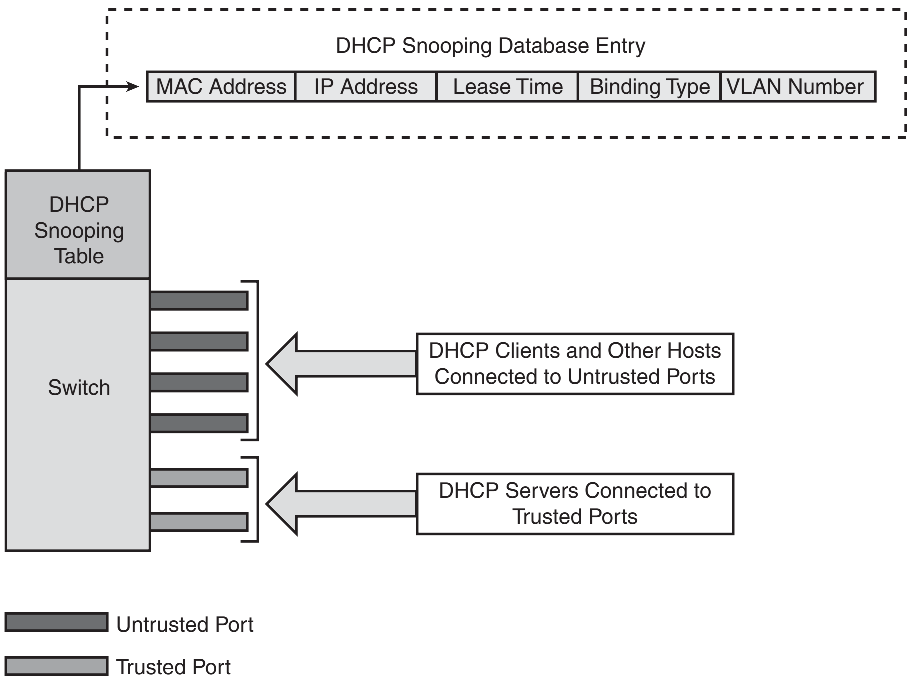
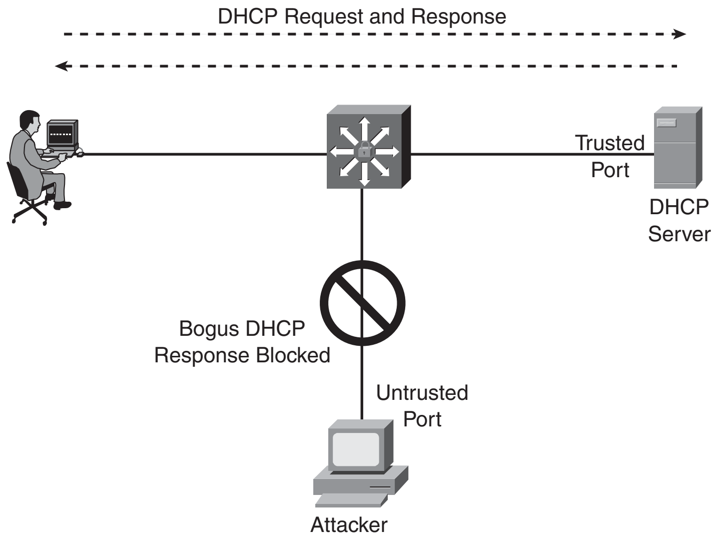


Figure 4-4b illustrates the DHCP Snooping feature in action, showing how the intruder is blocked on the untrusted port when it tries to intervene by injecting a bogus DHCP response packet to a legitimate conversation between the DHCP client and server.

Figure 4-4b *DHCP Snooping in Action*



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).

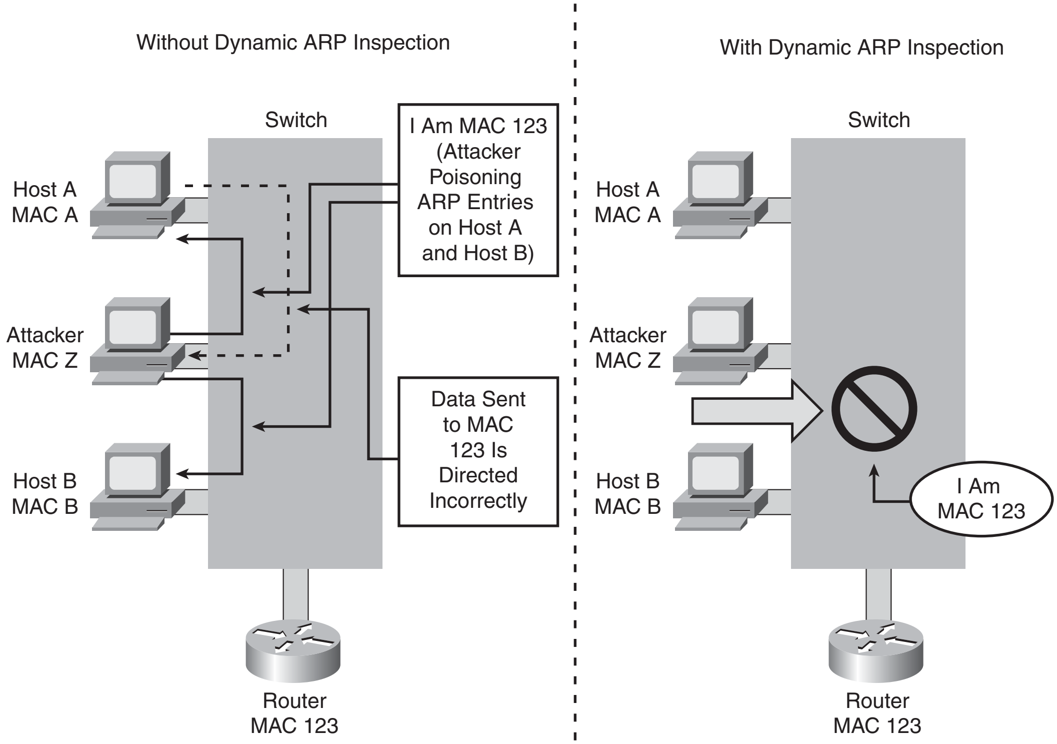
Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. A malicious user could intercept traffic intended for other hosts on the LAN segment and poison the ARP caches of connected systems by broadcasting forged ARP responses. Several 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.

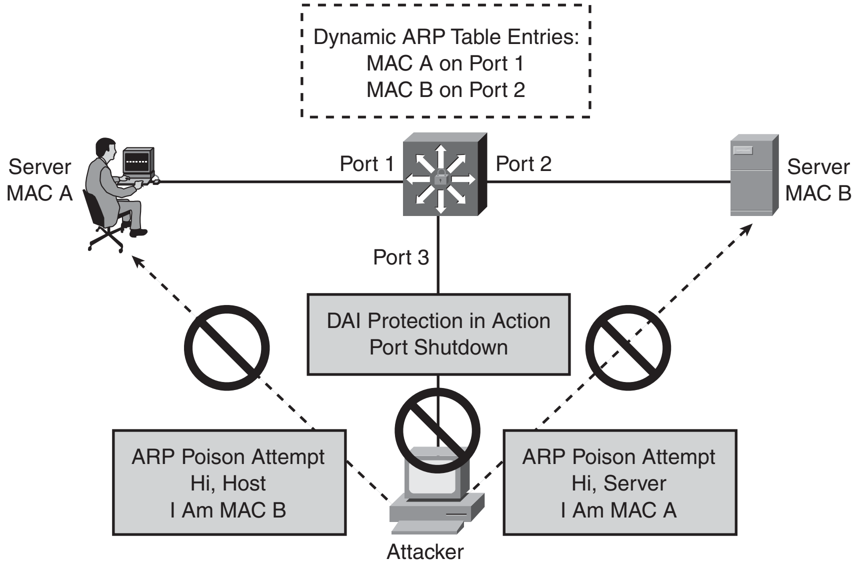
Figure 4-5a *Dynamic ARP Inspection*



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.

Figure 4-5b *DAI-in Action*



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*

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

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

http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008013565f.shtml

http://www.cisco.com/en/US/products/hw/switches/ps5528/products_configuration_guide_chapter09186a00802b7c35.html

http://www.cisco.com/en/US/products/hw/switches/ps5528/products_configuration_guide_chapter09186a00803a9a88.html

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00804357b1.html

http://www.cisco.com/en/US/products/hw/switches/ps5528/products_configuration_guide_chapter09186a00803a9a24.html

http://www.cisco.com/en/US/products/hw/switches/ps5528/products_configuration_guide_chapter09186a00803a9a23.html

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080435872.html

http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml

INDEX

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X-Y-Z